
GENEREX Comprehensive User Manuals

English

UPS WEB/SNMP MANAGER CS141

SENSORMANAGER & Accessories

BACS Battery Analyze & Care System

RCCMD Network Shutdown Software

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) 1995-2019 GENEREX GmbH, Hamburg, Germany. All rights reserved.

Introduction

Thank you for trusting the CS141 Webmanager – the most powerful solution for critical resource management.

Since the CS141 was designed to be a full-fledged, standalone manager, its task is not limited to gathering and sharing information. It also accomplishes numerous tasks in measurement controlling devices dealing directly with critical resource management. Furthermore, the CS141 comes with a full-featured message management system. The CS141 cannot only answer requests coming from higher-level systems - it can also independently inform responsible employees in case of an emergency incident as well as initiating emergency measures based predetermined parameters:

The CS141 can automatically activate basic or advanced emergency systems, shut down servers and workstations. Even automatic restart at predetermined conditions is configurable. In addition to standard technologies such as SNMP and Modbus, the CS141 relies on using the powerful RCCMD software solution. By doing so, even the emergency behavior of complex, fully virtualized server landscapes are realizable.

Thanks to RFC1628 the CS141 provides more flexibility than ever

This feature provides new possibilities to integrate third-party UPS systems. Thanks to the new RFC1628 compliant UPS interface, administrators can use the CS141 to poll any SNMP card that supports these standards. Simply use the SNMP-card installed inside your UPS and display the current status natively inside CS141.

This will allow administrators to use the powerful products made by GENEREX in combination of UPS-Systems that are normally not compatible.

Note

Due to the fact the CS141 Web Manager can act as a stand-alone system for managing, it can be used flexibly in many areas, even outside the functionality described in this guide. This manual therefore describes the fundamentally implemented functionality according to UPS systems. However, the enormous flexibility and the possibility of communicating with higher and lower-level systems using standardized interfaces allows the adaption to very different possibilities to use.

About this manual

This manual is more than just a small leaflet – it is written to explain and show all functions of a CS141 – you will notice, this device is very powerful and flexible, you are not limited to use this device as a UPS monitoring card. You can monitor, control, switch or communicate to any parent or child system inside complex IT systems.

This manual is written to show you what you can do with a CS141 and explains how to configure the device – in some cases you will not find some menus described in this manual. Here are possible reasons:

- The function is not enabled.
- Additional devices are needed
- Your CS141 model does not support the function you are looking for.

Basically, it is up to you to decide what you want to do...

This manual is divided into three parts:

- CS141
- BACS
- RCCMD

If this is your first CS141, this manual will guide you step by step through all menus and explain nearly everything you need to ensure emergency power and use the notification functions.

What you need to know:

Each model of the CS141 family can handle RCCMD – the CS141 is the RCCMD sender, and the RCCMD software client is the according receiver.

BACS more than just an option – it is a powerful battery management solution that may operate as a standalone system. If you are interested in battery management, this chapter is very interesting – but be careful!

Working with batteries inside a UPS system is for experienced or special trained technical who are familiar with all symbols and functions as well as how batteries work. With BACS, you can manage your batteries and optimize your entire UPS solution as well as increasing the battery performance and life time.

Table of Contents

Part 1: CS141

Introduction

- [Differences to the CS121](#)
- [Model Overview](#)
- [Delivery notes](#)
- [Function overview CS141](#)
- [Hardware Layout Appendix](#)
- [Interface Assignment](#)
- [External D-SUB 9-pin male](#)
- [Network integration of the CS141](#)

Initial Configuration

- [Preparation at the CS41](#)
- [Preparing the Workstation](#)
- [Using DHCP](#)
- [Finding CS141 in networks / MAC address](#)
- [Netfinder](#)
- [Differences in operation modes](#)

Before you start

- [Installation examples](#)
- [Required Ports](#)

CS141 Basic settings

- [Basic login passwords](#)
- [Setup Wizard](#)
- [IP-address settings and hostname](#)
- [Location and contact settings](#)
- [Provided services](#)
- [Date and time](#)
- [Tutorial: How to set up a custom time server](#)
- [User management](#)
- [System overview](#)
- [Switching to operational mode](#)

System notification

- [Email settings](#)
- [Advanced Mail Options](#)
- [Test Mail Settings](#)
- [The most common error message](#)
- [Email traps](#)
- [Modbus](#)
- [SNMP Agent](#)

UPS Configuration

- [General COM Port Settings](#)
- [The pipe through function](#)
- [Configuration of a UPS](#)
- [Battery Health Level \(%\) feature](#)
- [RFC 1628 UPS Interface](#)
- [UPS monitoring screen](#)
- [UPS functions](#)
- [UPS event handling](#)
- [The intention of a job](#)
- [Managing jobs](#)
- [Available jobs](#)
- [UPS Shutdown definition](#)
- [How to configure a job](#)
- [Time management of jobs](#)
- [Adding jobs to several events](#)
- [Delete jobs](#)
- [Counter Events](#)

Custom Thresholds

- [What are Custom Thresholds](#)
- [Difference Warning/Alarm Levels](#)
- [Example scenario: Custom Thresholds](#)
- [Exemplary excerpt: Custom Thresholds](#)
- [Tutorial: Custom thresholds](#)

CS141 RCCMD Server

[What is RCCMD](#)
[Available RCCMD Commands](#)
[Configuration of RCCMD](#)
[Setting up the IP address for RCCMD](#)
[Timing for RCCMD jobs](#)
[Variables for RCCMD traps](#)

Sensors and additional devices

[SM T H COM Standalone Sensor](#)
[General COM Port Settings](#)
[Setting up a sensor](#)
[Sensor monitoring screen](#)
[Event handling for sensors](#)
[Sensor related system events](#)
[Setting up a job for sensor events](#)

SENSORMANAGER

[SENSORMANAGER: - Sensor matrix](#)
[SENSORMANAGER - Adding analog sensors](#)
[SENSORMANAGER - Sensor event vs matrix event](#)
[SENSORMANAGER - Setting up the logical connection](#)
[SENSORMANAGER - Digital inputs](#)
[SENSORMANAGER - Linking digital inputs and analog sensors](#)
[SENSORMANAGER - Switching an output](#)
[SENSORMANAGER - Tutorial: Example scenario: aquarium](#)
[SENSORMANAGER - Possibilities of the sensor matrix](#)

[Alarm device / buzzer](#)
[GSM modem](#)
[CON_AUX4 and CON_R_AUX4](#)

Scheduler

[How the scheduler works](#)
[Setting up scheduled Jobs](#)

Web Server

[Safety instructions](#)
[HTTP settings](#)
[PORT settings](#)
[Force HTTPS](#)
[HTTP refresh time](#)
[Simple monitor](#)
[Tutorial: Creating a PEM-File](#)

Diagnostics

Logfiles

[Event Log](#)
[Data log](#)
[Data log Diagram](#)
[UPS Alert history](#)

Tools

[Reboot](#)
[Tracer](#)
[Network Scan](#)
[Privacy Notice: Network Scans](#)
[Evaluation of data](#)
[Deleting data](#)
[Tutorial: Complete data deletion](#)
[Changing Logo](#)

Data backup and updates

[Creating backups](#)
[Restore configuration from a backup](#)
[Restore network data](#)
[Performing a firmware update](#)
[Changing the OEM firmware](#)

If nothing works ...

[Rebooting without login](#)
[Performing a firmware update directly](#)
[The rescue mode on the CS141](#)
[Rescue mode on the CS141 Mini](#)

Part 2: BACS

What is BACS?

[What is BACS?](#)
[What is the advantage of BACS](#)
[EQUALIZATION: maintain individual charging / discharging](#)
[Upgrade CS141 to a BACS system](#)

BACS Installation Guide

Please read carefully before starting with working on batteries:

[How to use the BACS manual](#)
[Fundamentals when working on batteries](#)

Mandatory additional components

[BACS C module](#)
[BACS measuring cable](#)
[BACS bus cable](#)

Installation examples

[BACS installation examples](#)
[BACS Bus topology](#)
[BACS Splitting box](#)
[BACS installation with two webmanager](#)

Battery preparation

[Battery preparation](#)
[Things to be followed during initial installation](#)
[Connection BC5 measuring cables](#)
[Connecting BC4B measuring cables](#)
[Mounting BACS modules](#)
[How to replace a BACS module](#)

Initial BACS configuration

[General battery data](#)
[Number of battery strings](#)
[Basic setting of a BACS module](#)
[External current sensor](#)
[Premium feature: Ampere Multiplier](#)
[Discharge detection: Thresholds for current sensor](#)

Initial BACS module setup

[Addressing the BACS modules](#)
[BACS Programmer restart conditions](#)
[Defining an address range for module reset](#)
[General Module setup](#)
[Address range setup conditions](#)
[BACS Programmer single mode](#)
[BACS Error: HW Revision / Calibration error](#)

BACS Programmer software tool

[How to connect a computer](#)
[Preparing BACS installation](#)
[Operating modes: Automatic mode](#)
[Operating mode: Manual mode](#)
[Line check](#)
[Receive Line Check](#)

GX_R_AUX

[How it works](#)
[Connectors](#)
[Addressing the GX_R_AUX](#)
[Configuration of the GX_R_AUX](#)
[GX_R_AUX as battery breaker](#)
[Normally Open / Normally Closed contacts](#)
[Defining a job to a BACS event](#)

[Communicate with third party devices via Outputs / Inputs](#)

BACS functions

[BACS Buzzer](#)
[BACS Relay](#)

BACS alarm threshold

[Overvoltage](#)
[Deep discharge](#)
[Threshold definition](#)
[Battery voltage](#)
[Battery temperature](#)
[Internal resistance of the battery](#)
[Maximum voltage deviation between batteries](#)
[Voltage deviation per string](#)
[Current deviation per string](#)
[Alarm delay](#)

Battery strings and thermal runaway

[Define BACS battery strings](#)
[BACS strings vs battery breaker](#)
[What is a thermal runaway?](#)
[Mandatory preconditions for BACS thermal runaway functions](#)
[Max. module temperature difference](#)
[Max current per string](#)
[Above conditions are true since](#)

Initial Start up: Pause Equalizing on Schedule

[What is an unformed battery?](#)
[Why pause Equalizing during initial start up?](#)
[How to use a scheduled equalization pause](#)
[Equalization Pause Example 1](#)
[Equalization Pause Example 2](#)
[Equalization Pause Example 3](#)

Part 3: RCCMD software client

This software tool is a part of the RCCMD emergency shutdown solution

Introduction

[Welcome to RCCMD](#)

ESXi 6.5 installation guide

[Installation of the RCCMD Appliance with ESXi 6.5](#)
[Post installation console login](#)
[Gaining root privileges](#)

ESXi 6.5 vCenter installation

[Installing RCCMD with a vCenter](#)
[Starting the VM and console access using vCenter](#)

RCCMD Quick configuration guide

[RCCMD quick configuration guide](#)
[Web Login: RCCMD](#)
[The RCCMD license key](#)
[Securing the RCCMD appliance](#)
[RCCMD operation state](#)
[Allow shutdown control for RCCMD with a single host _](#)
[Handing over the shutdown control to RCCMD using a vCenter](#)

RCCMD in detail

Main section Status

[Event Log](#)
[System Status](#)
[Logout](#)

Main section Options

[Connections](#)
[Heartbeats](#)
[Redundancy](#)
[Advanced Settings](#)

[Web Access](#)
[User Settings](#)
[Dry Run installation test routine](#)

RCCMD FAQ's

[Setting up IP address data manually](#)
[Configuring RCCMD network setting](#)
[Setting up an emergency user for RCCMD on VMware](#)
[Tutorial: If your keyboard layout is wrong](#)
[CS141 FAQ section](#)

Part 4 :

Appendix

[Hardware Layout CS141](#)
[Interface Description](#)
[Pin COM2 Mini-DIN 8 pol](#)

Modbus addresses

[Section OEM: ABB/NEWAVE UPS Type Concept Power](#)
[Section OEM: MASTERGUARD](#)
[Section OEM: RITTAL PMC Extension](#)
[Section OEM: Netminder for all LT and MD types](#)
[Section OEM: Netminder EON](#)
[Section OEM: Netminder for all other types](#)
[Section OEM : AEG Protect 3. M 2.0](#)
[Section OEM: AEG Protect 3.31, 5.31, 8.31](#)
[Section OEM: AEG Protect 2.33, 3.33, 4.33, 5.33, 8.33, blue](#)
[Section OEM: POWERTRONIX](#)
[Section OEM: Socomec UPS](#)
[Section MHD Modular / Multimatic Modular / AEG Protect 1. Modular, ENIGMA](#)
[Section Borri 4000 Std. Panel / E-Tec 310 to 380 \(m\) / SALICRU SLC NX/DL/CUBE](#)
[Section Inform UPS / Pyramid DSP/Online DSP](#)
[Section Transfer Switches \(All Transfer Switch vendors, except PILLER, STS TUMEL\)](#)
[Section STS TUMEL Transfer Switch](#)
[Section OEM TRIMOD](#)
[Section: EverExceed Inverter](#)

Parameters for UPSMAN Software and BACS

[UPSMAN Status Bytes - Standard Device Status Bits](#)
[BACS Parameters](#)

Last, but not least:

[Copyright and licenses](#)

Differences to the CS121

- Complete rework of the menu structure: The simplified interface combines a powerful hardware to provide a significant performance boost:
- The powerful successor of the CS121 allows configuration in real-time - necessary system services will be started or stopped as needed. Therefore, a restart is only necessary in exceptional situations.
- Additional hardcoded user accounts according to specialized tasks:
- Engineer and Guest accounts are provided according to their tasks with limited system rights. On request the new guest account can be set up to allow external technicians a quick information overview without the need of password entry.
- The DIP switches known from the CS121 are no longer required and changed by a comfortable slide switch in the front of the device:



The easy-to-use slide switch will change the hardware configuration. Once the configuration state is chosen, a reboot can be done by the removing power connection or software triggered.

- The firmware update can now be carried out inside a common browser via drag & drop. The need for external tools and FTP access is no longer necessary.
- In case of problems with the firmware, updates or reboots can also be carried out without a complete login. To do this, use a common web browser and enter the IP of the device followed by /update. After a successful admin authentication, the firmware can now be updated and optionally resetted to factory settings.
- By default, auto logout is now enabled. On inactivity, the user is logged out of the system after 15 minutes.
- The power consumption of the CS141 has been reduced by a factor of 10 with a power increase and is well below the predecessor model.

Note:

The CS121 has been discontinued in 2015 and replaced by the powerful successor CS141. The Software development was officially discontinued in 2018 - the current firmware state is frozen. Newer UPS systems and models are not available. If you use a CS121 with a specific UPS manufacturer for many years, it may happen that your new UPS model is not natively available even if you use the latest firmware version.

In this case, it is advisable to move to the successor CS14.

Model overview

Device	Function	Remarks
CS141L	SNMP adapter	external adapter
CS141SC	SNMP adapter	Slot Adapter for UPS with slot
CS141LM	SNMP adapter	External adapter with MODBUS output (RS485)
CS141SCM	SNMP adapter	Slot adapter with MODBUS output (RS485)
CS141BL	SNMP adapter	External adapter BUDGET-Modell (No COM2- and AUX-port)
CS141BSC	SNMP adapter	Slot adapter BUDGET-Modell (No COM2- und AUX-port)
CS141R_2	SNMP adapter	Slot adapter for PILLER/CTA/RIELLO/AROS UPS Italy
CS141MINI	SNMP adapter	Slot adapter for UPS models with MINI Slot

Additional devices based on CS141:

Device	Function	Remarks
BACSKIT_B4	Battery management	External adapter
BACSKIT_BSC4	Battery management	Slot adapter

Device	Features	Supported UPS devices
CS141L	Additional Mini DIN 8 COM Port for RS232. AUX Port for Digital Input/Output. Remote RAS Management optional.	Over 1400 UPS models from over 80 different manufacturers are supported
CS141SC	Additional Mini DIN 8 COM Port for RS232. AUX Port for Digital Input/ Output. Remote RAS Management optional.	All devices with basic slot SC
CS141LM	Additional Mini device. AUX Port for Digital Input/ Output. Remote RAS Management optional.	Over 1400 UPS models from over 80 different manufacturers are supported
CS141SCM	Additional RS485. AUX Port for Digital Input/ Output. Remote RAS Management optional.	All devices with basic Slot SC
CS141BL	Slot Budget variant of the CS141. UPS Management via LAN. No AUX Port for floating contacts. No COM2 Port for Pipe-through, sensors, etc.	Over 1400 UPS models from over 80 different manufacturers are supported
CS141BSC	Slot Budget variant of the CS141. UPS Management via LAN. No AUX Port for floating contacts. No COM2 Port for Pipe-through, sensors, etc.	All devices with basic Slot SC
CS141R_2	Additional Mini DIN 8 COM Port for RS232.	Riello and Aros UPS with Netman Slot
CS141MINI	Additional Mini DIN 8 COM Port for RS232.	UPS devices with MINI Slot (Soltec, Voltronic, etc.)

All CS141s can manage UPS systems providing a native serial protocol. Furthermore, the CS141 can be easily integrated into existing SNMP systems. All models of the CS141 family provide an own unique web server with configurable event management for automating job executions based on the status of the UPS. All CS141s can manage UPS systems providing a native serial protocol. Furthermore, the CS141 can be easily integrated into existing SNMP systems.

All models of the CS141 family provide an own unique web server with configurable event management for automating job executions based on the status of the UPS, including:

- email notification
- Full RCCMD functionality
- shutdown commands,
- logfile entries, shutdown of the UPS, - graphical log files,
- shutdown and wake-up -commands (WOL)

In addition, the CS141 can also be individually configured using a scheduler to trigger job executions for many events, e.g.:

- battery testing
- calibration
- UPS or system shutdown / restore.

The CS141 provides a wide range of network management features to inform and alert required persons before a critical incident occurs. The CS141 can even monitor other SNMP devices and thanks to its built in RCCMD solution, combine them to an intelligent power resource management.

Each adapter has 2 years warranty as well as free updates for 3 years.

All devices are manufactured in Germany

Content on delivery

The scope of delivery of a CS141 includes a supplementary Software Compact Disk and additional hardware.

Note:

The budget edition does not support all features described in this manual.

Product	Included on delivery				
	External power supply	User's manual on CD	Mini-DIN-8 Connector (MODBUS)	RS-485 Via COM2	Rescue Jumper
CS141L	X	X	X		X
CS141SC		X	X		X
CS141LM	X	X		X	X
CS141SCM		X		X	X
CS141BL	X	X			X
CS141BSC		X			X
CS141R_2		X	X		
CS141MINI		X	X		

Function overview CS141

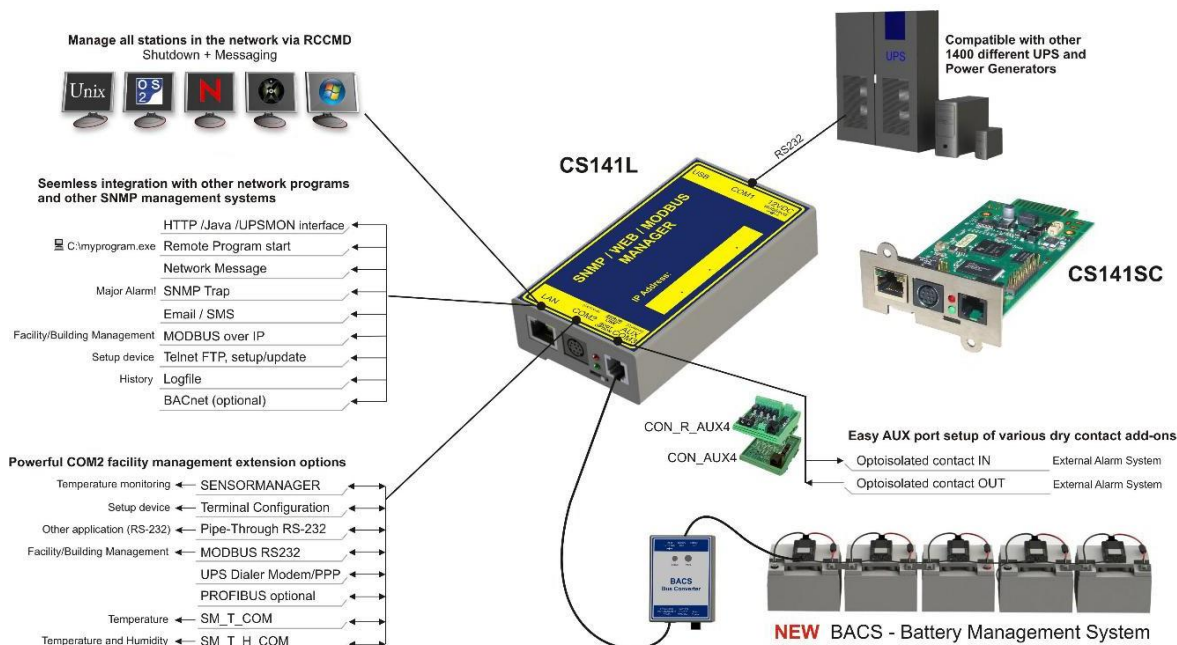
In SNMP mode, the CS141 adapter works with a preinstalled Simple Network Management Protocol (SNMP) software agent.

This agent exchanges status data with the UPS via so-called "get / set" commands and forwards them in the form of "trap messages" to predetermined recipients. These "trap messages" allow to alert necessary persons during or before critical situations happen within the UPS. Typical information can be switching to battery power or the end of a power failure.

In addition, the SNMP adapter can send RCCMD signals (Remote Control Commands):

On clients with the RCCMD software installed, freely configurable functions can be triggered – the functionality range allow nearly everything.

Administrators can run a simple system shutdown as well as a highly complex shutdown and restart routine. In addition, the web interface is also a control of the UPS possible.



In SNMP mode, the CS141 adapter works with a preinstalled Simple Network Management Protocol (SNMP) software agent.

This agent exchanges status data with the UPS via so-called "get / set" commands and forwards them in the form of "trap messages" to predetermined recipients. These "trap messages" allow to alert necessary persons during or before critical situations happen within the UPS. Typical information can be switching to battery power or the end of a power failure.

In addition, the SNMP adapter can send RCCMD signals (Remote Control Commands): On clients with the RCCMD software installed, freely configurable functions can be triggered up to complex shutdown and start routines

In addition, administrators can monitor and control their UPS possible by using the build in web interface to ensure an all-in-one solution for nearly the entire UPS system:

SNMP Trap functionality

The basic task of the adapter is to communicate alarm states of the UPS to an according monitoring station (traps) or to provide UPS data if monitoring stations poll. With this function, e.g. the power supply and battery status of a UPS are monitored by an SNMP management station.

Additionally, the CS141 provides functions for simulating and testing trap messages during configuration procedure.

Remote Control:

Due to the fact the CS141 is capable to configure it is possible to trigger different remote-controlled actions. Administrators can perform battery tests, bypass the UPS batteries or configure UPS behavior

Note:

Depending on the UPS you are using, provided functions may differ.

Compatibility according to third party network management systems

The SNMP adapter is compatible with all common network management systems. All SNMP systems providing 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 CS141.

Full RCCMD support:

Due to the fact the CS141 is a full manager and not just an SNMP-Card to collect and provide data, the entire network shutdown routine can be configured to react as fast as possible:

Thanks to integrated RCCMD support, the CS141 offers a flexible and fast way to operate even the most complex shutdown solutions. By the usage of standardized network technologies and protocols, the patented RCCMD server transfers control commands that are executed by the clients in real time.

RS-232 / pipe-through:

In some cases, different networks without any connections have to be configured to use the same UPS. With the new pipe-through capability administrators can connect two CS141 and let the communication of the UPS work with both devices:

By doing so, two different CS141 can communicate to according networks without additional hardware.

RS232 UPS interface:

The CS141 provides a standard RS232 interface to allow establishing a serial connection to any UPS providing this standard.

Note:

Please use only the original UPS communication cable supplied with the UPS. In case of using a contact UPS, choose the special designed cable of the manufacture. If you have any questions regarding special connection cables, refer your UPS dealer.

Provided real-time logfiles:

The CS141 provides a proven compilation of logfiles to reconstruct a complete timeline in case of critical incidents. This logfile is accessible via UNMS, UPSMAN, WebGUI and FTP or can be send via mail to configured mail-accounts.

Advanced mailing capabilities

Each model of the CS141 family provides the capability to connect to any mail server using standardized encryption technologies.

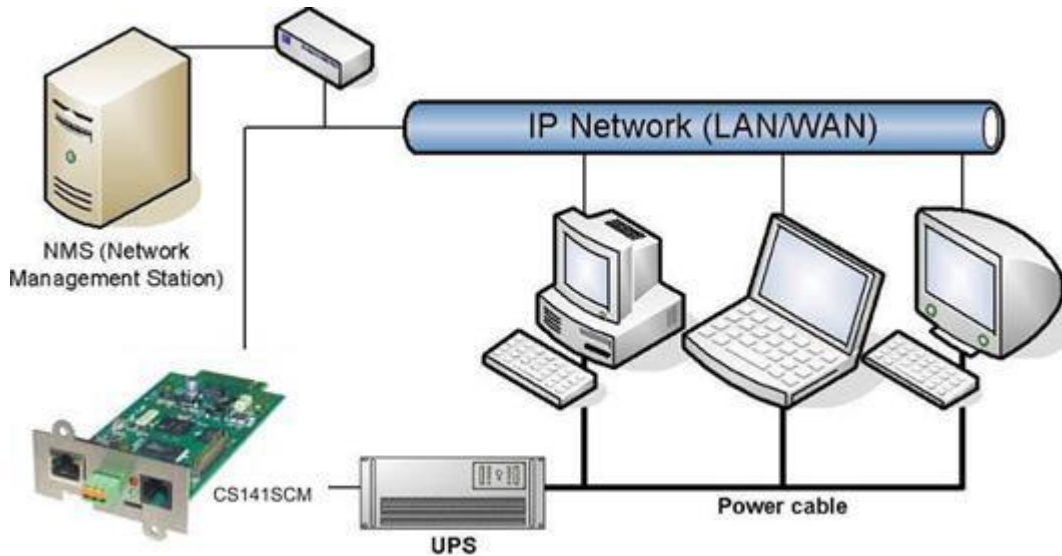
Unique web server included:

The unique build-in Web server of the CS141 displays all information about the device itself, connected sensor and external hardware. The software module UPSView inside the CS141 can also be used to display a graphical representation of these data.

To Access the web interface administrators and technicians may just use common browsers (Edge, Firefox, Chrome, Safari etc.).

Networking

Modern UPS solutions are much more than just batteries. The Cs141 takes an eye on this fact and co-operates with the UPS:



The UPS ensure power to all clients and the CS141 manages the solution to inform and finally to shut down all clients before batteries are depleted.

MODBUS:

Modbus is the standard protocol used in industrial applications for monitoring and building management.

All devices of the CS141 family therefore provide as standard a MODBUS over IP interface. In addition, CS141 with COM2 connector provide MODBUS over RS232 (CS141L & SC) and Modbus over RS485 (CS141L, SCM).

SNMP:

All models of the CS141 family communicate using SNMP via the UPS standard MIB RFC 1628.

If a system does not include this standardized MIB, administrators can download the RFC1628 data file from www.generex.de to compile the MIB at a later time.

Once you have compiled the MIB file into the appropriate MIB directories of your SNMP station, the CS141 can be used.

UPSTCP:

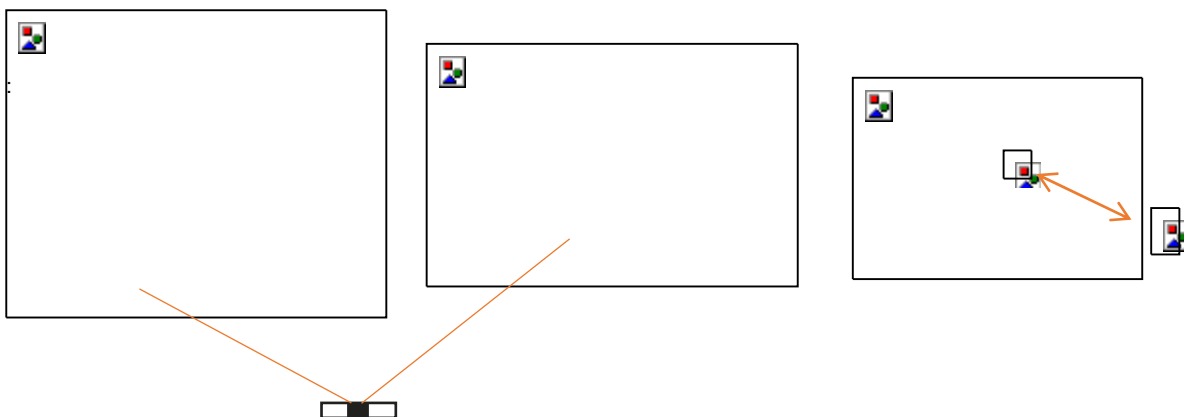
CS141 provides with UPSTCP a complete API interface to ensure optimal integration into existing networks.

Upon request, this interface specification can be supplied to manufacturers of software in order to enable their own integration.

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 is preset to the hard-coded IP address 10.10.10.10:

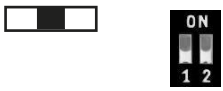





In factory default setting, the sliding switch is in the center position and the CS141 is in configuration mode. Due to its more compact design, the CS141 MINI breaks the standard and uses on-board dip switches instead of a sliding switch:

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 center position / DIP 1 + 2 OFF:</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 / Dip 1 OFF + 2 DIP 2 ON:</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 / DIP 1 ON + DIP 2 OFF:</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>	
<p>CS141 Mini special feature:</p>	
<p>Both Dip-Switches ON:</p>	
<p>Enables the rescue-mode for advanced system maintenance operation.</p>	

Initial configuration 10.10.10.10

Preparation at the CS41

Prior to commissioning, ensure the slide switch on the front is set to center position. In case of CS141Mini, both Dip switches of the CS141 MINI has to be set in OFF position. After start up, the CS141 can be runs in configuration mode, available at IP address 10.10.10.10.

Note:

Changing the mode via the hardware switches requires a reboot of the CS141. You can perform the restart in two ways:

By removing the power supply (hardware reset)
Using the Restart feature to be found inside the Tools menu (Software Reset)

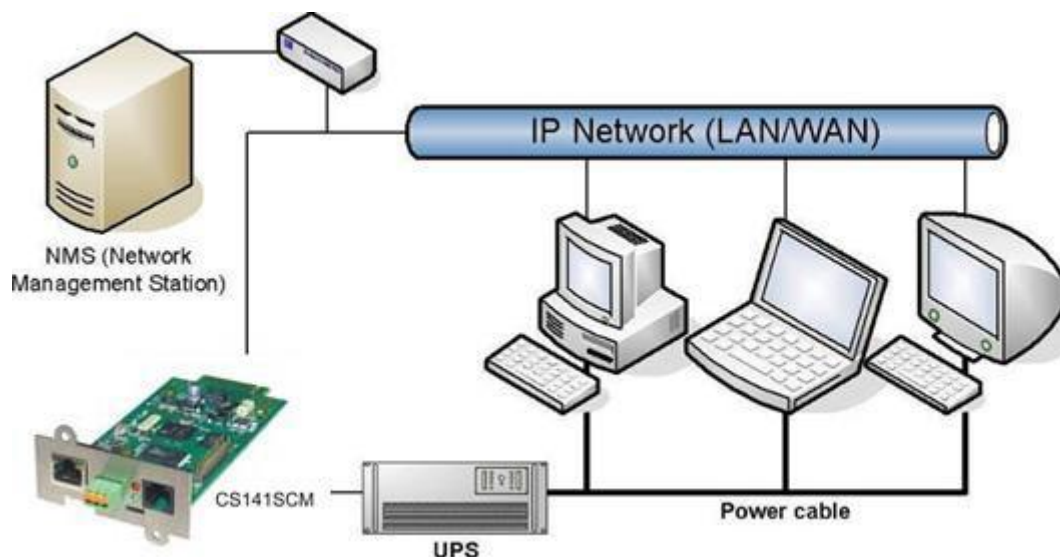
This operation does not apply the UPS the CS141 is connected to - the functionality will be kept up independently to the CS141.

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 client PC:

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

```
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>
```

PING 10.10.10.10.

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.

Using the DHCP Option

The DHCP mode

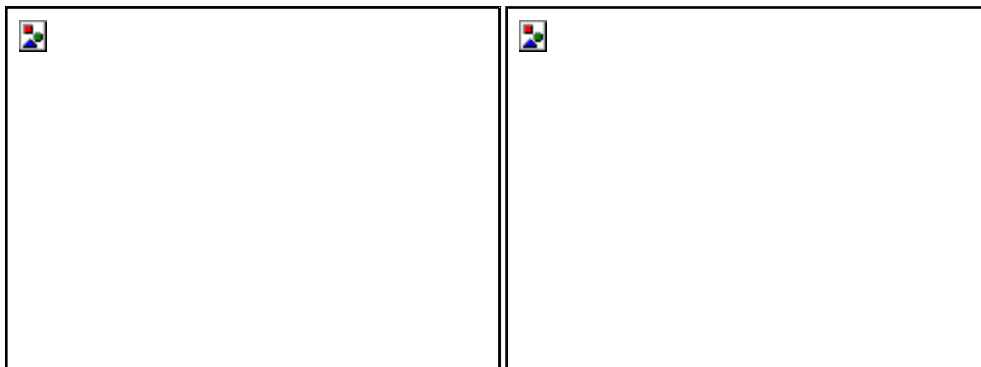
Since the models of the CS141 family can fulfill many functions due to their flexibility, it is a very realistic scenario that you need to commission several devices at the same time within an installation procedure - Unfortunately there is no fixed IP address that can be assigned for the moment.

To avoid a network conflict, activate the DHCP mode for automatic IP address assigning:

Slide the slide switch to the right, i.e. to the outer edge of the CS141. For the CS141 Mini, set dip switch 1 to OFF and move dip switch 2 to ON. Next reboot, the web manager will boot in DHCP mode according to the hardware configuration and obtain an IP address from your network.

Required information for finding CS141 in DHCP-Mode

To identify the devices, please note the MAC address including location data before proceeding hardware installation. The MAC address can be found on any CS141 web manager as a unique sticker:



Ensure a suitable DHCP server is available for this operating mode, otherwise they will not be able to get valid IP address data automatically.

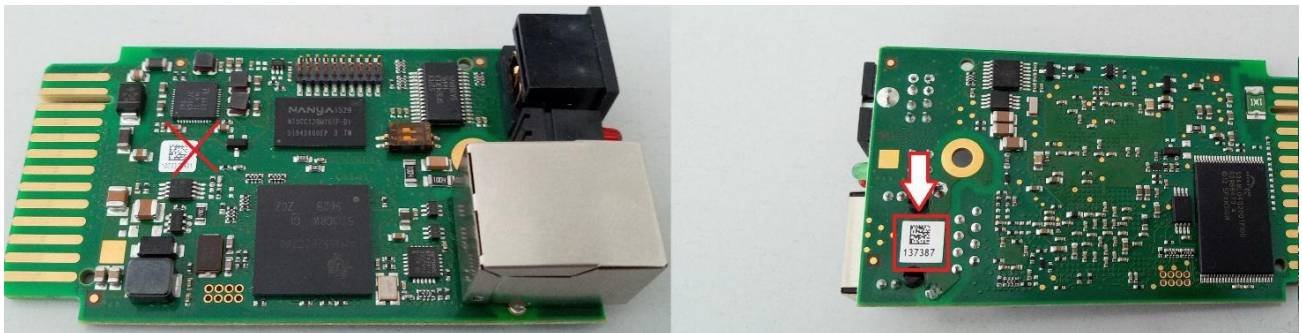
CS141 MINI and CS141 / R2

Due to the compact design, the label sticker of CS141 MINI and the CS141 / R2 differ and shows only the last three octets of the MAC address.

The MAC address of a GENEREX- network interface starts with these address values:

00-30-d6-xx-xx-xx

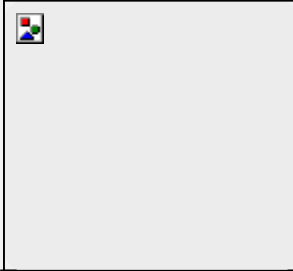
The last three values can be found at the label sticker on the back of the CS141 MINI or CS141 R2:



A common bar code scanner that can handle QR codes or a smartphone with a QR-Code app will display the complete MAC address.

Note

Please notice that you use the sticker on the back. This will show the last three octets of the MAC address. When on installation site, you can simply figure out the MAC address:

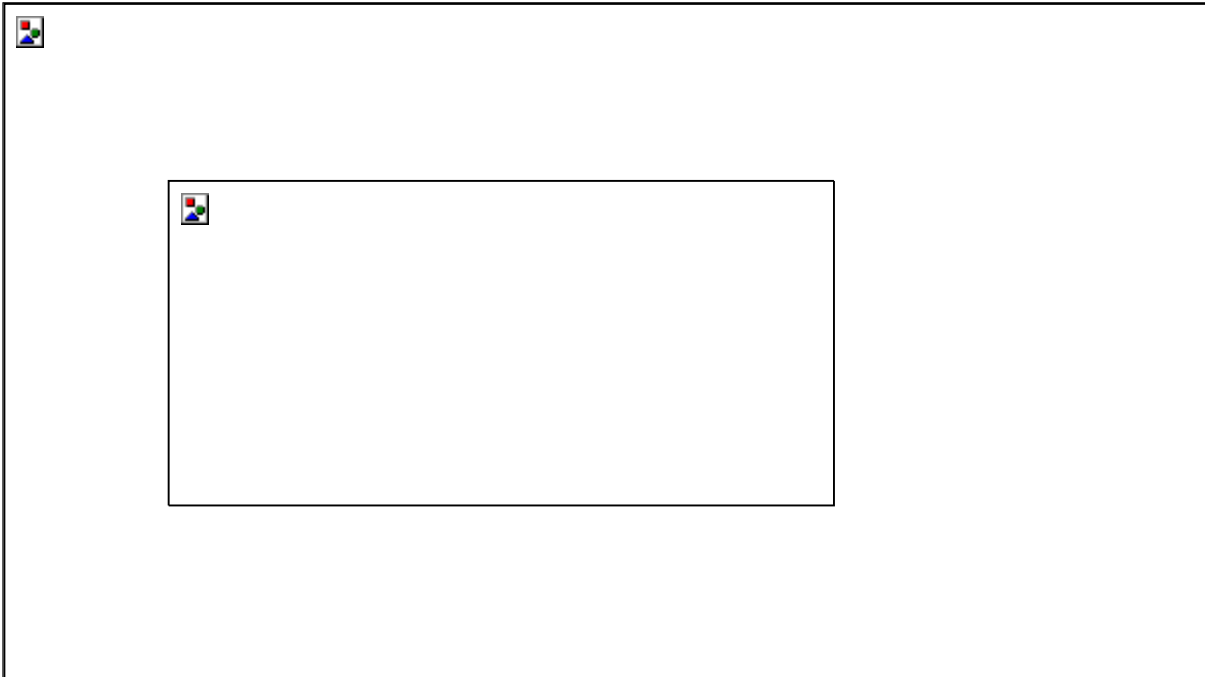


In this case, the MAC address is 00-30-d6-13-73-78

Netfinder: Search for IP-addresses used with CS141 devices

The Netfinder is a software tool that can display all CS121 and CS141 devices that can be reached inside a specific network segment. It is available at the local support CD and at www.generex.de.

To perform a quick search for valid IP addresses, use the tool Netfinder.



The default search generally refers to the network segment the service computer resides. To scan other networks and subnets for CS121 or CS141 installations, it is necessary to specify the appropriate IP address ranges.



The GENEREX Netfinder software provides a detailed overview of all devices in the network and allows quick and easy access to the web console of the respective manager.

Note:

In DHCP mode, IP addresses may change sporadically depending on the network configuration. Therefore, several Webmanager monitored by a parent system such as UNMS II should receive a fixed IP address.

In any other case, technicians can easily detect and access installed devices by using Netfinder.

Configuring the CS141 device*Differences between configuration mode, rescue mode and operation mode*

Each model of the CS141 family will be configured exclusively by an intuitive web interface. Independently to this common ground, the web managers offer four valid operating states, which fundamentally differ from each other.

1. The configuration mode

The configuration mode is the default preset on delivery:



The slide switch is in center position and the dip switches of the CS141Mini are both set to OFF. The web manager can be reached via hardware-coded preset IP address 10.10.10.10 and allows all system-relevant settings. Since the CS141 generally uses the preset IP address in configuration mode, this mode allows importing backup data and to be adjusted after restart without harming the network.

2. Operating mode

Depending on the setting, the sliding switch will be set to left or right position. In case of CS141Mini, Dip switch 1 or 2 is switched on



The CS141 can be run in two different operation modes:

In manual mode, enter the IP address information. Please note that incorrect settings may cause address conflicts on the network or the settings made may not work. The data required for manual mode can be obtained from local system administrators.

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.

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 startup 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

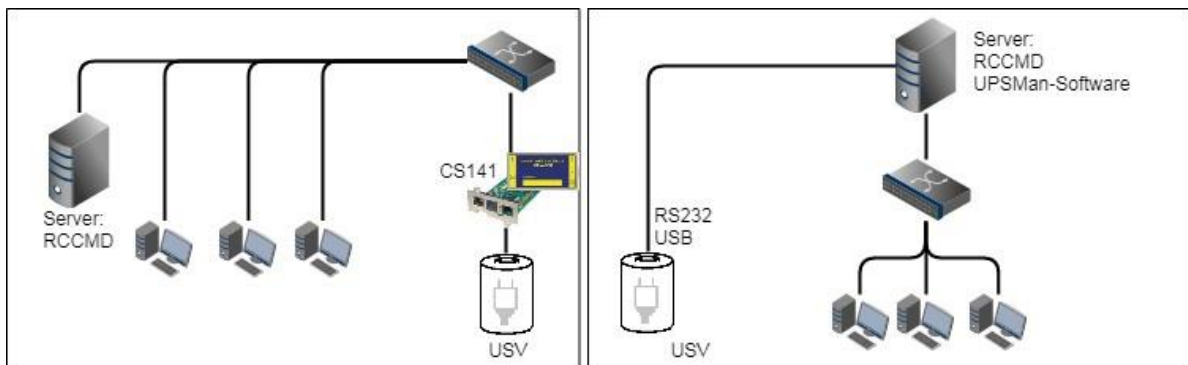
In this mode, an additional jumper is set and the slide switch center position.

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.

Before you startInstallation examples

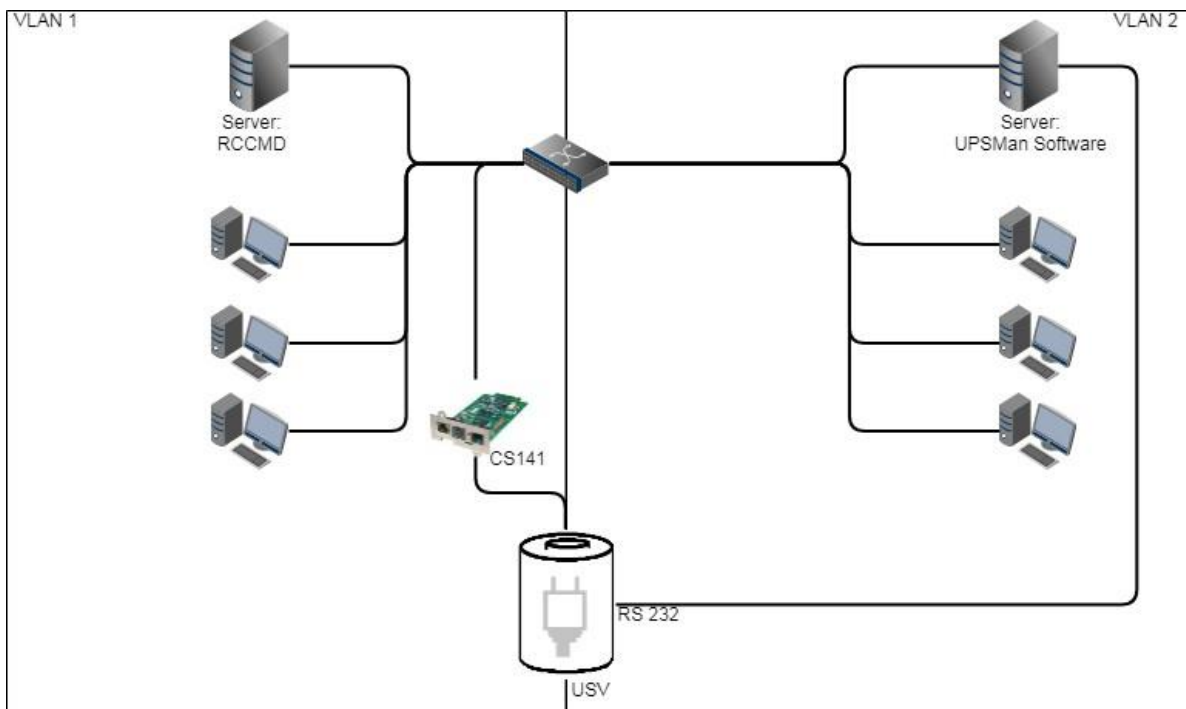
The CS141 was designed to provide a maximum of flexibility and freedom during the installation - as a result the CS141 match the tasks of modern UPS systems as well as expectations coming with it.

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:

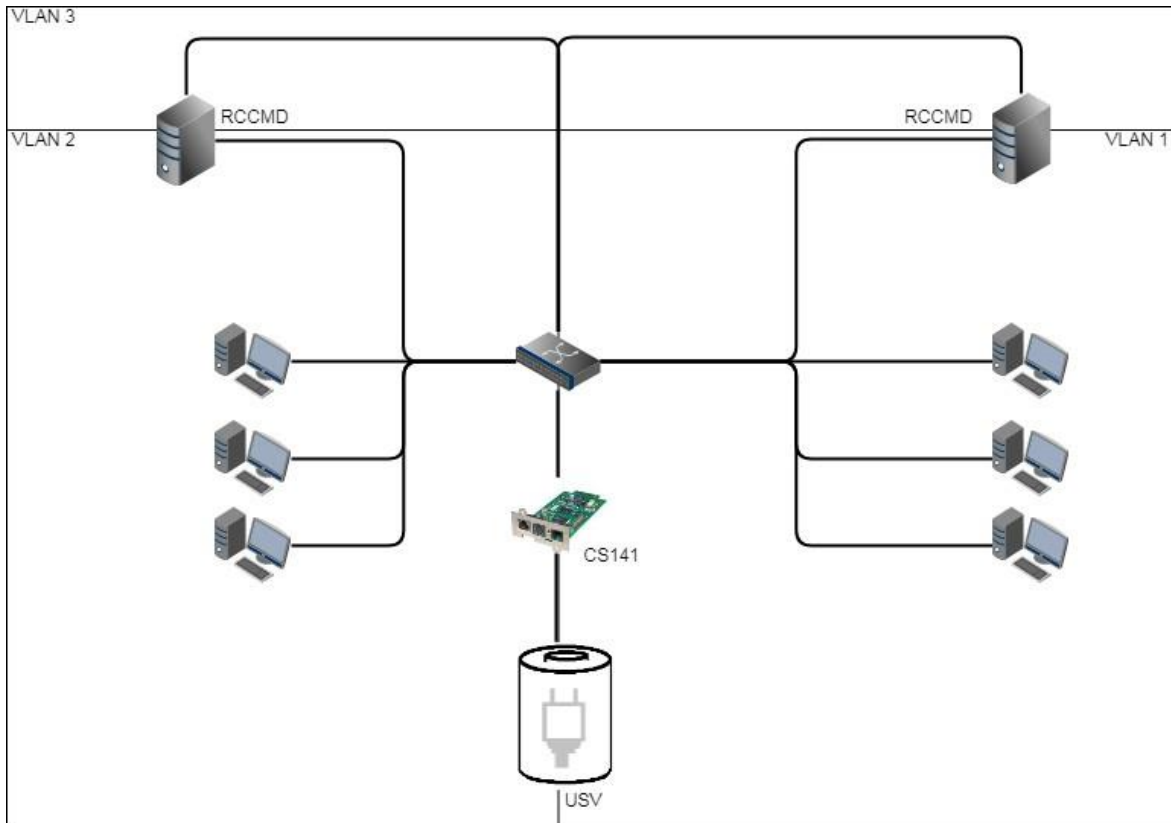


In this case, the UPS becomes a central role inside the network's emergency power security.

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:

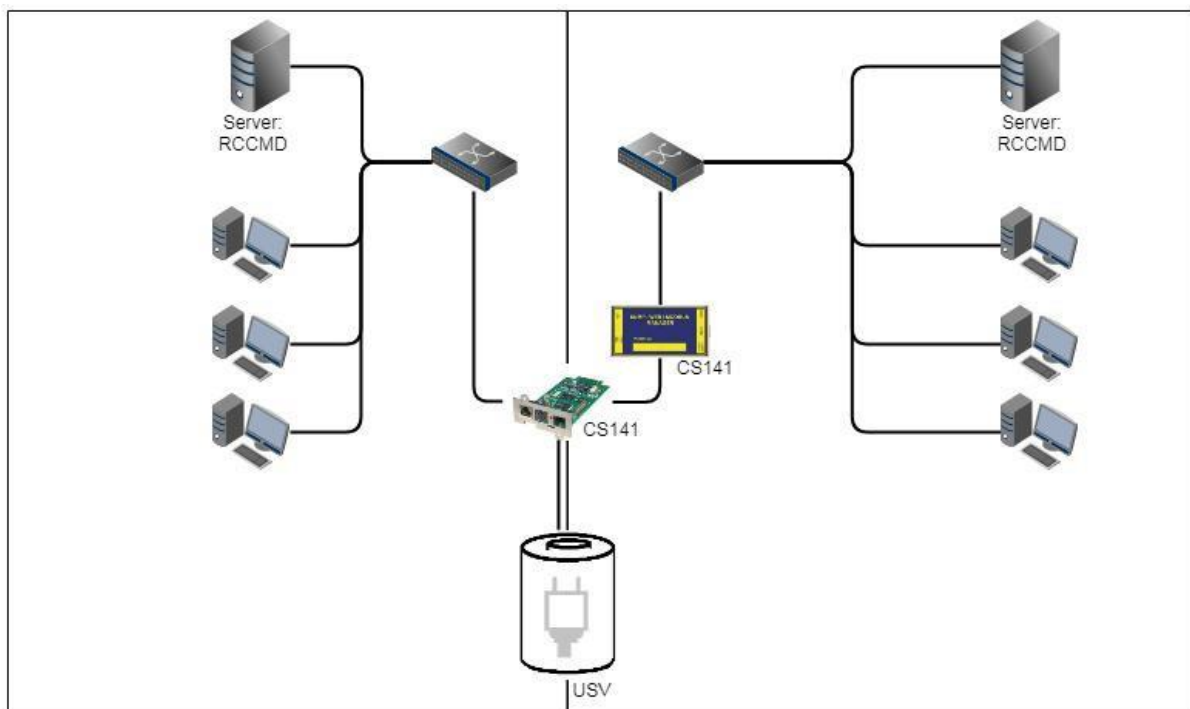
Once Installed directly on the server, it communicates with the UPS via the COM port of the server and offers the same functionality as the CS141 including a full support of RCCMD. Therefore VLAN 2 represents a "software only" solution that does not require a CS141 as additional hardware.

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



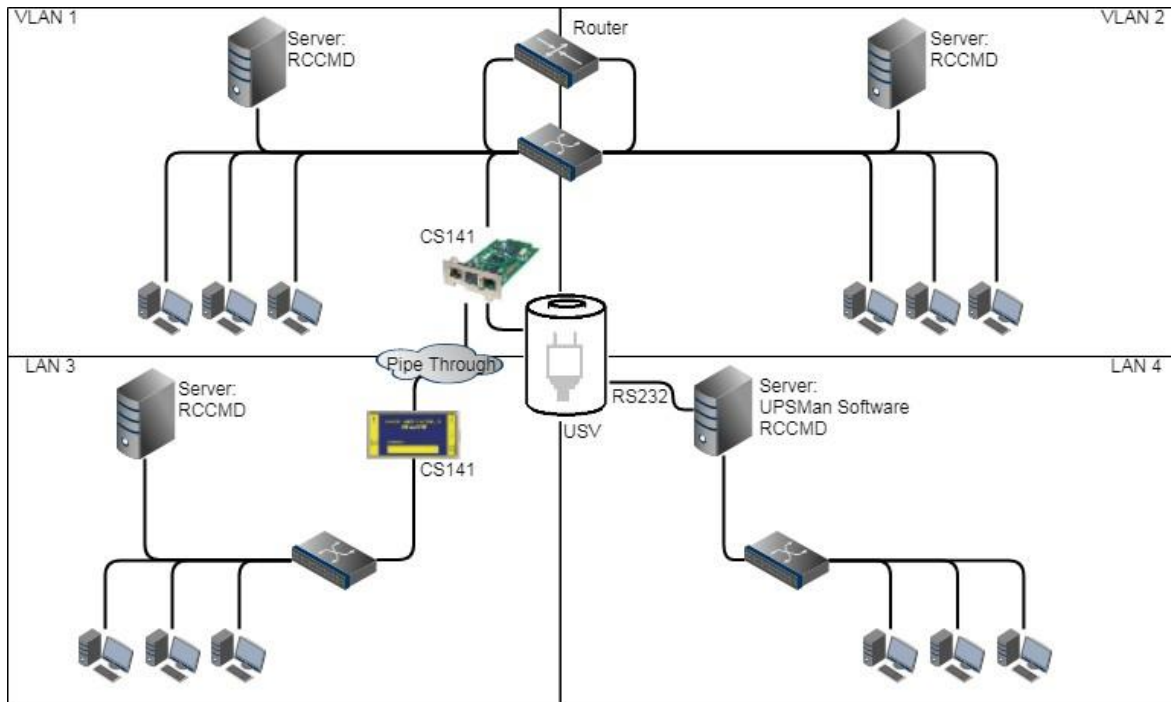
If you have chosen a solution with two network cards and the UPS provides a usable RS232 interface, this solution allows future installations - even complete closed up networks are possible.

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.

Complex 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.

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

Note

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 to configure any device of the CS141 family intuitively.

If you cannot 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

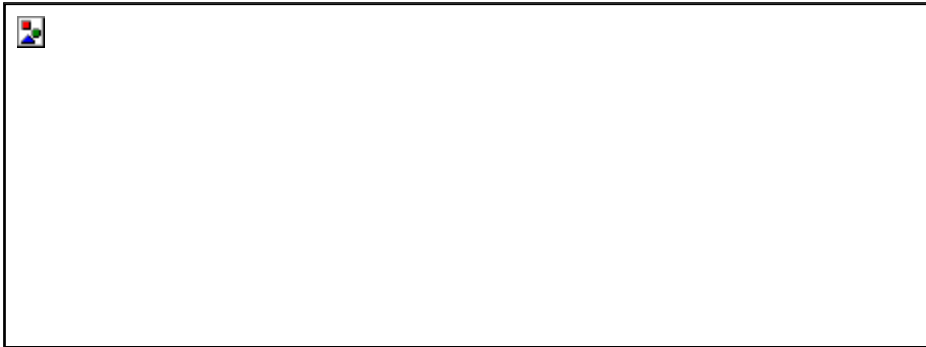
Basic settings and passwords

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-snmpp	... <i>System administrator, complete menu tree accessible</i>
User: engineer	Password: engineer	... <i>Technician, administrative restricted system access</i>
User: guest	Password: guest	... <i>guest account, only status indicators visible</i>

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

**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 behavior may result in screen errors.

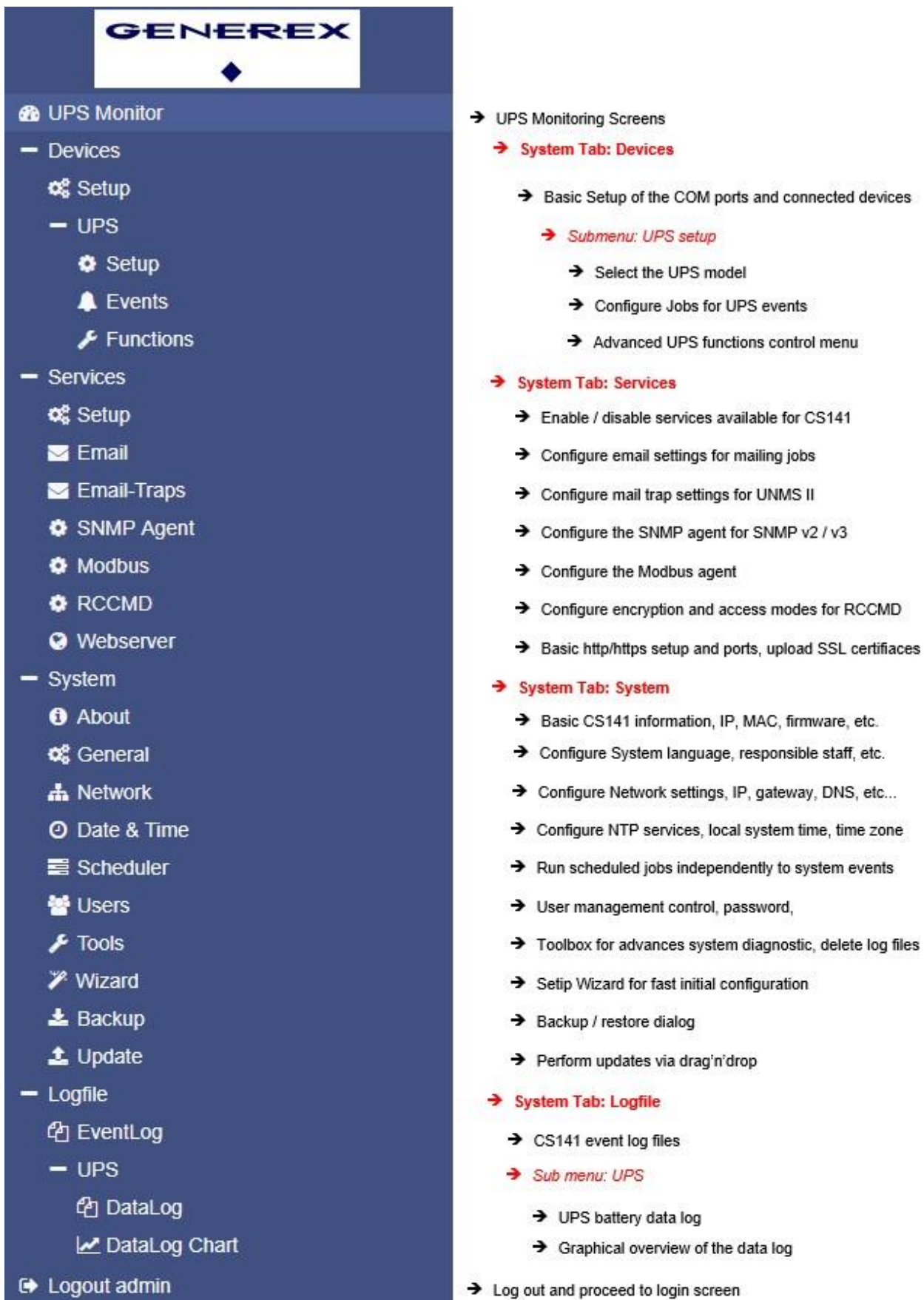
If these phenomena occur, update the browser by pressing CTRL + F5 or clear the cache of the web browser and deactivate additionally installed tools and addons, which could obstruct the presentation.

CS141 configuration menu overview for firmware 1.80

This is the CS141 menu tree without expansion modules.

If you connect additional modules in order to extend functionality, corresponding menus are automatically displayed after installing and activating the functions.

This menu tree shows all basic functions each CS141 model provides:



GENEREX

- UPS Monitor
- Devices
 - Setup
 - UPS
 - Setup
 - Events
 - Functions
- Services
 - Setup
 - Email
 - Email-Traps
 - SNMP Agent
 - Modbus
 - RCCMD
 - Webserver
- System
 - About
 - General
 - Network
 - Date & Time
 - Scheduler
 - Users
 - Tools
 - Wizard
 - Backup
 - Update
- Logfile
 - EventLog
 - UPS
 - DataLog
 - DataLog Chart
- Logout admin

→ UPS Monitoring Screens

- System Tab: Devices**
 - Basic Setup of the COM ports and connected devices
 - Submenu: UPS setup**
 - Select the UPS model
 - Configure Jobs for UPS events
 - Advanced UPS functions control menu
- System Tab: Services**
 - Enable / disable services available for CS141
 - Configure email settings for mailing jobs
 - Configure mail trap settings for UNMS II
 - Configure the SNMP agent for SNMP v2 / v3
 - Configure the Modbus agent
 - Configure encryption and access modes for RCCMD
 - Basic http/https setup and ports, upload SSL certificates
- System Tab: System**
 - Basic CS141 information, IP, MAC, firmware, etc.
 - Configure System language, responsible staff, etc.
 - Configure Network settings, IP, gateway, DNS, etc...
 - Configure NTP services, local system time, time zone
 - Run scheduled jobs independently to system events
 - User management control, password,
 - Toolbox for advances system diagnostic, delete log files
 - Setip Wizard for fast initial configuration
 - Backup / restore dialog
 - Perform updates via drag'n'drop
- System Tab: Logfile**
 - CS141 event log files
 - Sub menu: UPS**
 - UPS battery data log
 - Graphical overview of the data log

→ Log out and proceed to login screen

Extended menu trees

Depending on the CS141 model and available additional modules, additional menus are available. Please note that not every model can provide the following menus:

Sensor menus

Depending on the type of sensor, the following menus will be added automatically:

1. Standalone sensor on COM 2

After selecting sensor at COM 2 Sensor and as sensor type SM / T or the combination sensor SM / TH, following menus will appear automatically:



→ Sensor monitoring screen

→ **System Tab: Devices**

→ *Sub menu: Sensors*

- Configure measuring range, alarm marker, operating range
- Configure jobs to the alarm marker

2. SENSORMAN2 at COM 2

After selecting sensor at COM 2 Sensor and as sensor type SENSORMAN2, following menus will appear automatically:



→ Sensor monitoring screen: All sensor data in real time

→ **System Tab: Devices**


→ *Sub menu: Sensors*

- Configure up to 8 sensors, digital inputs and outputs
- Combine different sensor events to combined alarm marker
- Define Jobs to single sensor events or combined alarm marker

With the sensor matrix, an additional function is available that allows to combine single sensor events to collective events.

3. CON_AUX4 / CON_R_AUX4 selected at COM 3


The following menus are added when you connect a CON_AUX4 or a CON_R_AUX4 relay card to the COM 3 port of the CS141



- AUX monitoring screen
- **System Tab: Devices**
- **Sub menu: AUX**
 - Relay Card basic setup
 - Event handling configuration dialog CON_AUX4 or CON_R_AUX4

4. BUZZER selected at COM 3

The CS141 provides an additional buzzer for advanced acoustical alarm notifications. The following menus will appear when you choose the Buzzer at COM 3 of the CS141:



- Buzzer monitoring screen
- **System Tab: Devices**
- **Sub menu: Buzzer**
 - General buzzer setup, frequency, on / off, etc.
 - Buzzer event handling: Jobs to do because a Buzzer is active

6. BACS selected at COM 3

BACS® - the "**B**attery **A**nalysis & **C**are **S**ystem" - is the most advanced system on the market to manage stationary battery systems. It is a standalone battery monitoring and management system that can be easily integrated into your network infrastructure.

With its intelligent web-technology configurable management technology, it cyclically checks the internal resistance, the temperature and the voltage of each individual battery. In addition, it can readjust the charge voltage of each battery and manage environmental readings (temperature, humidity, hydrogen gas content) as well as loads (UPS, inverters, and other devices). The accumulators are thus always kept in the optimal working range.

Note:

Since the configuration of the system is independent to the rest of the functions, BACS functions are listed separated at Part II of this manual.

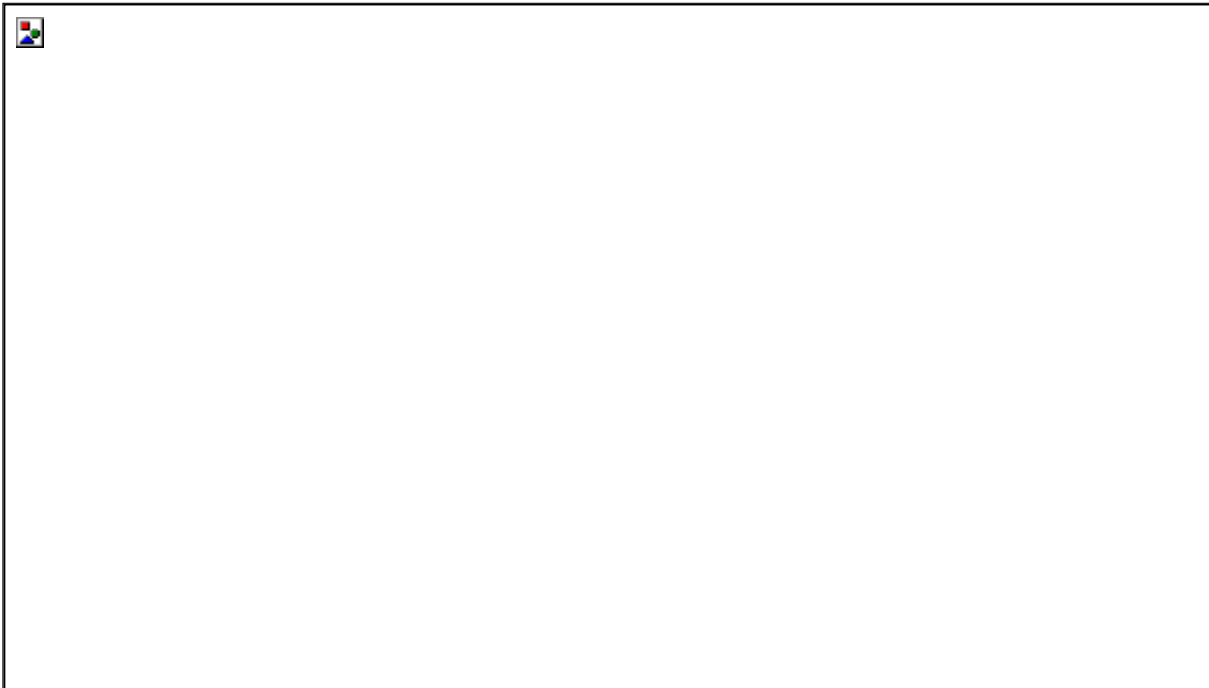
For more information and a detailed table of content about BACS, please refer to page 6 of this user guide.

The 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 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 preset 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.

How to configure network settings, open Network:

IPv4	
Configure	Active
IP Address: 10.10.10.10	IP Address: 10.10.10.10
Subnet Mask: 255.255.255.0	Subnet Mask: 255.255.255.0
Default Gateway: 10.10.10.1	Default Gateway: 0.0.0.0
DNS Server: 10.10.10.1	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 startup, 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.

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:



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:

Enter Location settings

Location data can be read by any software supporting this feature. If used in larger installations with many devices, location data will help to associate 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:



Regional settings

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 kilometers 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 ... –

Provided services

For this configuration step, navigate to the following menu:



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.



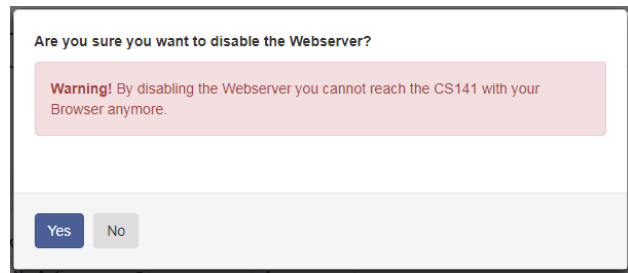
To enable or disable the according service, use the buttons.

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:

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

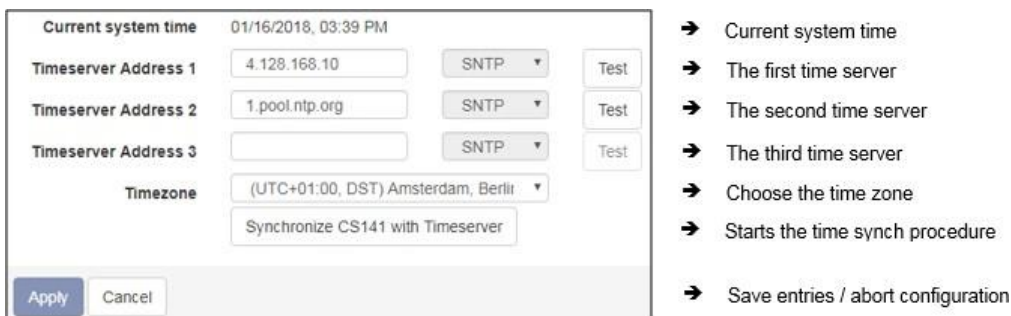
The UNMS server was specially developed to communicate with the universal network management software from GENEREX. The powerful successor UNMS 2 communicates via UPSTCP on port 5769. The UPS server service enables or disables availability through this port.

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 und 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.

Tutorial: 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

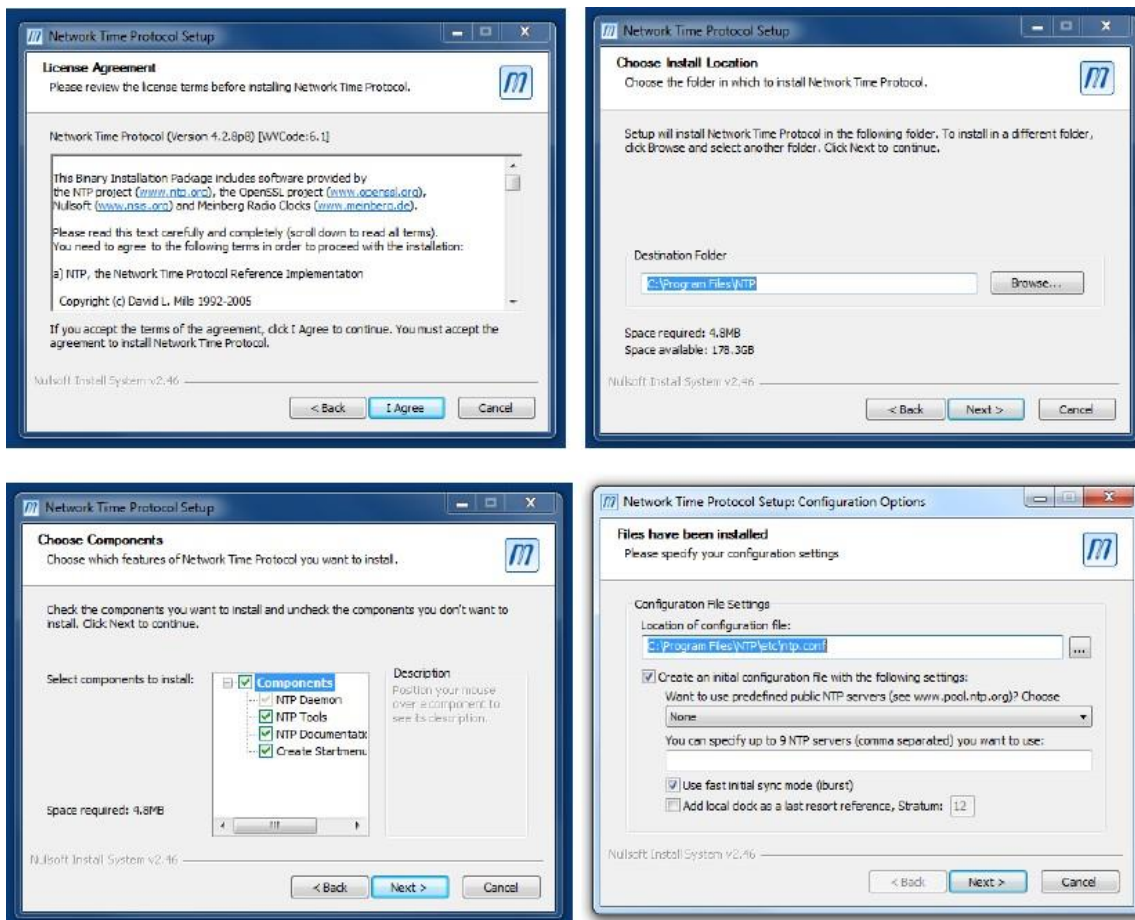
<https://www.heise.de/download/product/ntp-fuer-windows-49605/download>

Meinberg, provider of this tool:

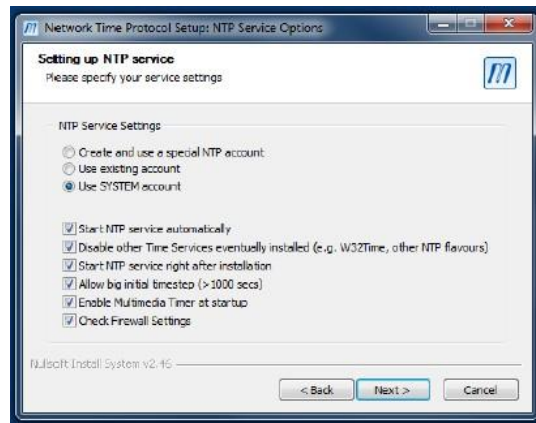
<https://www.meinberg.de/german/sw/ntp.htm>

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.

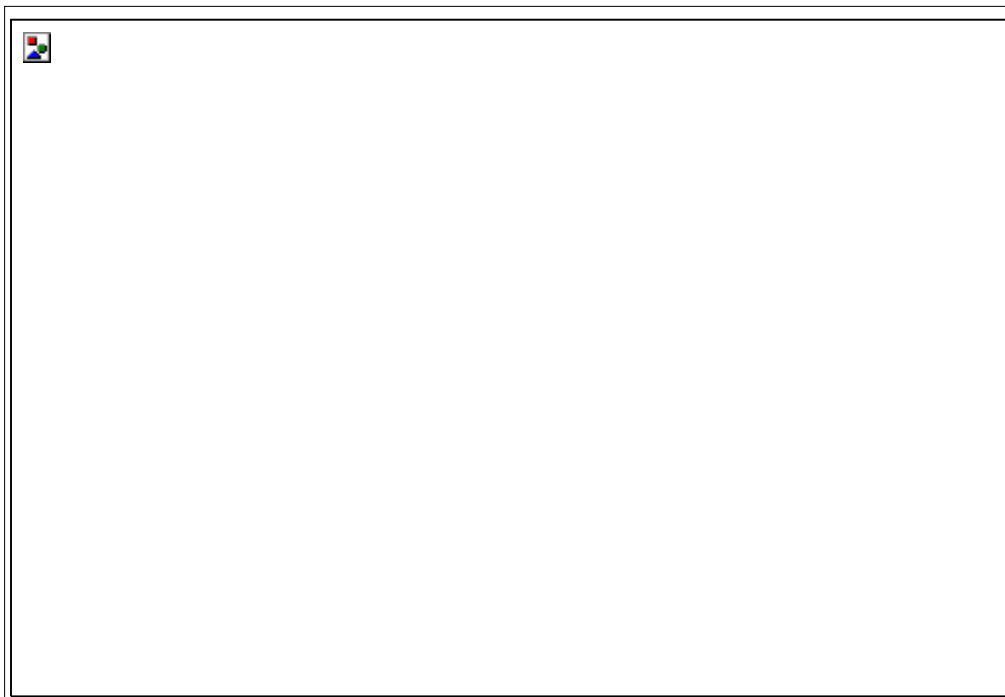
Testing the NTP server tool

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>

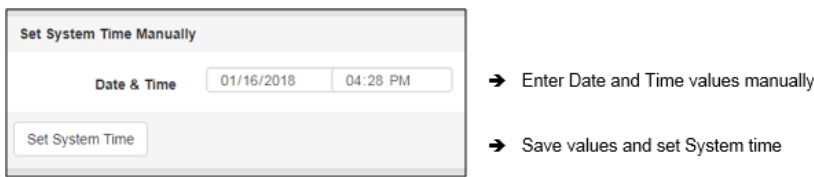
Please note that this tool only returns correct values if the following 2 conditions are completed:

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 preset 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.

The customer

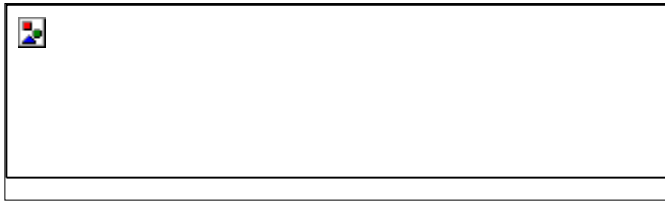
User: `customer`
Default password: `customer`

The customer has access is restricted to use the system monitors and also viewing as well as downloading a collection of log files - deleting log files is not possible.

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:

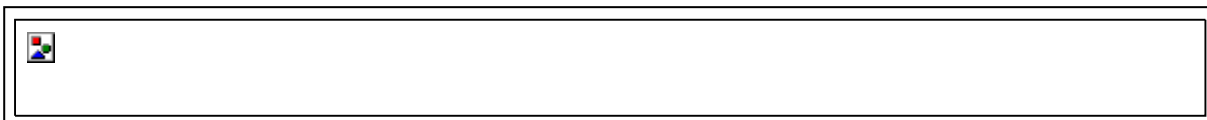
The user *admin* is allowed to manage COM interfaces, but not the user engineer. This is necessary due to the fact, attached monitoring systems may need to be prepared for a change inside the hardware landscape before local hardware or components will be disabled for local maintenance duties.

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 webside:

```
<html><head></head>
<body>
<center>
<p>l-frame according to the UPS with the IP xxx </p>
<br><hr><br>
<iframe src="http://<lhre IP>/www/devices/ups/page" width="500" height="600" name="iFrame" title="iFrame zu meiner
USV"></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 behavior is dynamically, the response page may change accordingly. However, the HTML request is standardized with these three deep links and will be served as long as the Anonymous login is active.

Advanced system 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

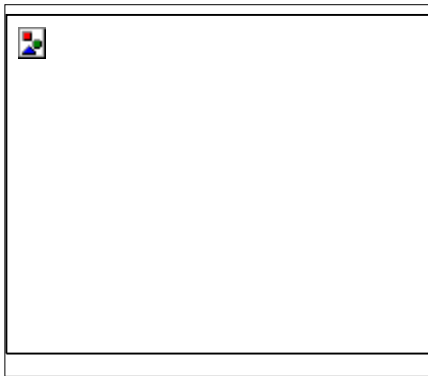
Hardware



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 *bch 8* – feature, old firmware will not run.

Network settings

- 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

- 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.

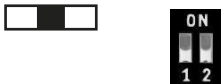

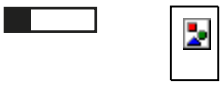
Switch to operating mode

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.

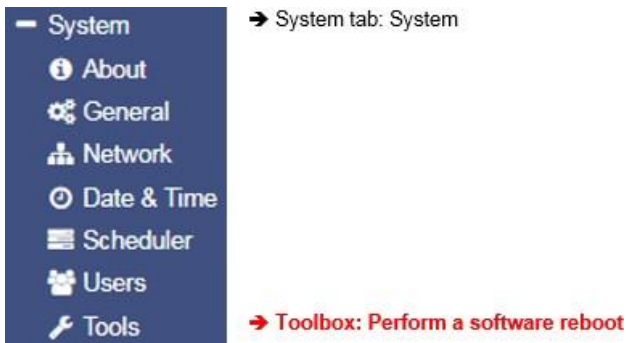
<p>Sliding switch to center position / DIP switch 1+2 OFF:</p> <p>After booting, the CS141 will run in configuration mode. Hard-coded default IP address 10.10.10.10 is active.</p>	
<p>Sliding switch to right position/ DIP 1 OFF + DIP 2 ON:</p> <p>After booting DHCP is active and IP address will be assigned automatically. To identify assigned IP address check MAC address of CS 141.</p>	
<p>Sliding switch to left position / DIP 1 to ON + DIP 2 OFF:</p> <p>After booting, manually configured network settings will take effect.</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

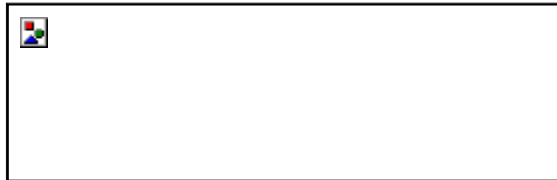
For this step, please switch to the following menu:



The toolbox is restricted for administration usage only.

After login as hard-coded user admin using default password cs141-snmp, 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**

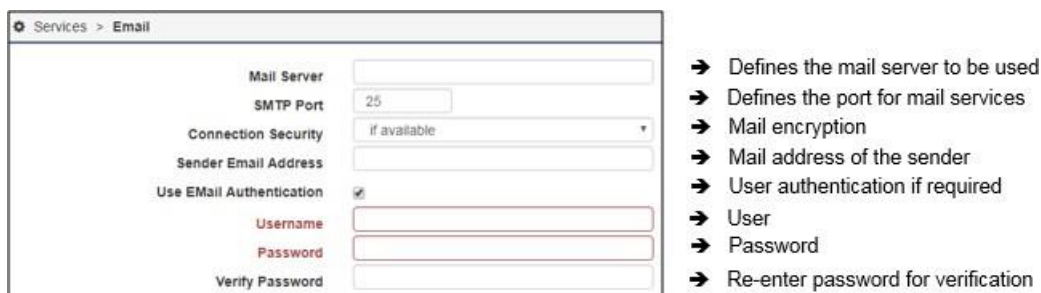
For this configuration step, navigate to the following menu:



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 use
- When it should be sent

The screenshot shows a configuration window titled 'Advanced'. It contains several settings:

- Format:** A checkbox labeled 'Database Interface Format' is checked.
- Log:** A dropdown menu is set to 'Errors only'.
- Automatically send a Copy:** A checkbox labeled 'for all sent Emails' is checked, and another checkbox labeled 'On scheduled Jobs' is also checked.
- To Receiver Email Address:** An empty text input field.

- Select the mail format
- Logging email traffic
- Additional blind carbon copy mail job
- Blind carbon copy receiving mail address

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.

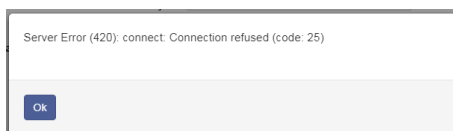
You may find a similar problem with logging the complete email traffic:

Too many entries in the event log quickly lead to 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.

Test 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:


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 behavior 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.

Problems with the mail server?

If you use your own mail server, you can usually take look at the incoming mail log. In general, the reason for rejecting an e-mail is also mentioned there. For online providers, however, the situation looks different:

You usually have no influence on the server and also no insight into the mail log.

As a result, you do everything right, but it still does not work and you cannot figure out why....

There are a couple of reasons, here are some examples:

1. The provider prohibits such service mails. The server simply rejects them automatically.
2. The mailing account must be confirmed manually. The email from unknown recources will be rejected until the user of the account validates the according sending device.
3. The frequency of mail is interpreted as spam. Mail providers react very fast and deny mails from this device even if they allow it in general.
4. Access data are basically correct but the mail server's virus guard is the opponion, the mail is used as a virus carrier. Depending on the settings of the server, the behavior may differ.

Note:

Basically, the CS141 also supports the Office365 mail server - be sure to use the correct port and encryption method!

SMTP: Server: SMTP.office365.com / Port: 587 / Encryption: STARTTLS

IMAP: Server: Outlook.office365.com / Port: 993 / Encryption: SSL / TLS

POP: Server: Outlook.office365.com / Port: 995 / Encryption: SSL / TLS

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.

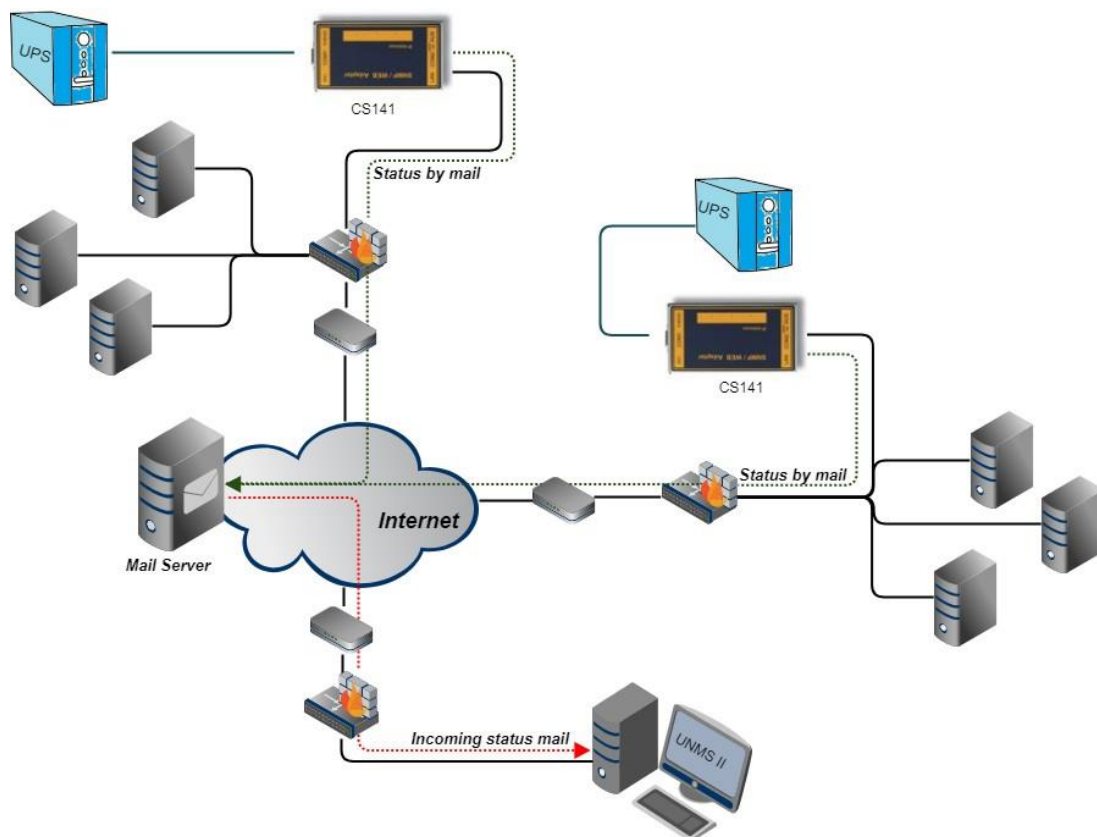
For details, please refer the Chapter *Configuring UPS*

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.

Tutorial: Email-Traps



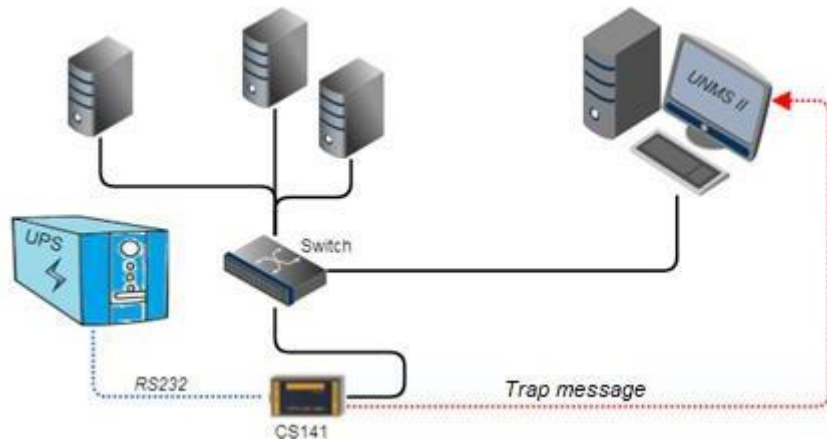
Trap messages are a very popular way to automatically get information from a network. The concept provides that a device sends its status in the form of a standardized data packet as soon as its current status changes. Among other things, the transmitted data strongly depends on the device and its function.

the key feature of a trap message:

The type of transmission is unidirectional - the packet is sent and there is no acknowledgment of receipt. If the device can send the packet, the task is completed. Since the messages are sent only in case of status changes, the destined monitoring tool normally assumes that the last received status received is valid.

Especially in weaker networks or in networks, where many messages of this kind are sent. This is an advantage as soon as either a large number of devices have to be monitored or the network is poorly developed:

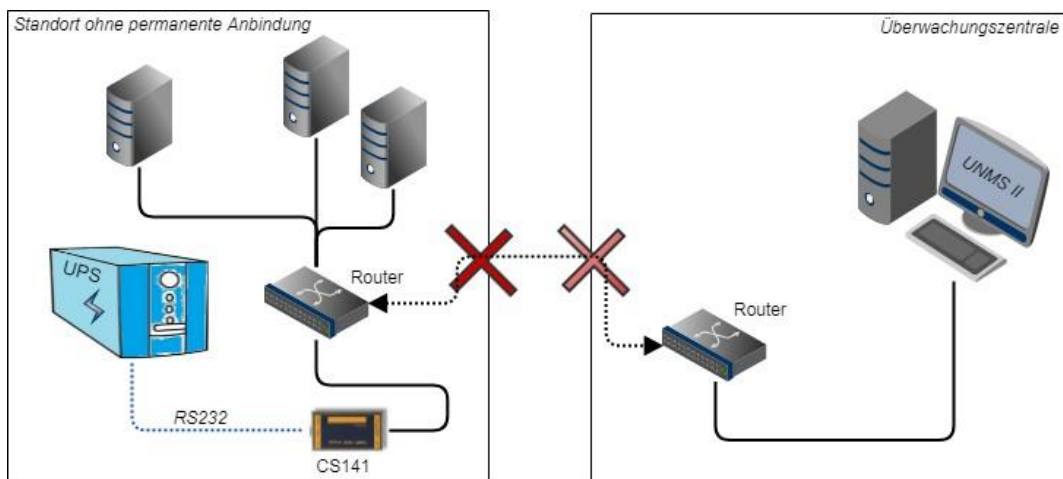
Both the required computing power and the amount of status data inside a network can be minimized.



The CS141 is capable to send trap messages to a monitoring software like the UNMS II in order to indicate a status change of a UPS.

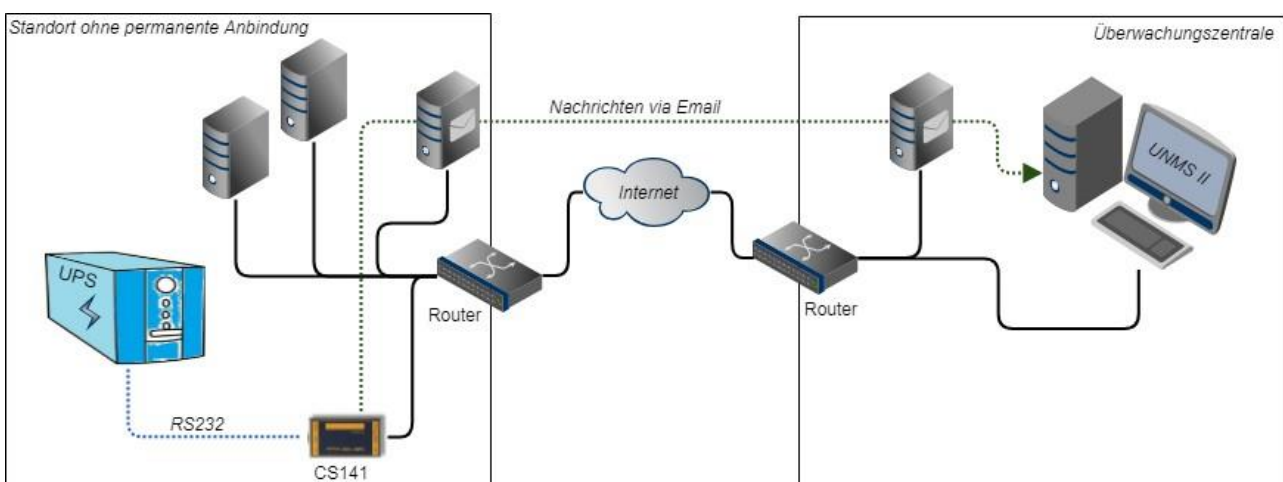
Now, there is a problem:

A network grows and for technical reasons, some segments cannot provide a permanent network connection until expensive major network installation works will be done ...



Does the argument of a better connectivity justify the costs of a network implementation or is there a better solution?

With Email-Traps, the CS141 offers an interesting way to meet this situation:



The CS141 uses the e-mail function in order to send an according message if the system status changes - a timestamp ensures that an outdated data package will be registrated but not used for the current system status monitoring. The mail server holds the e-mail until a connection is possible - and forwards this mail to a custom e-mail address UNMS II can access.

The UNMS II is the recipient. It will look for incoming mails and handle them like trap messages.

Note:

The advantage is the fact that local connection options can be used to ensure a basic communication between a device and a monitoring system. The focus is set on ensuring communication - the communication speed depends on the local infrastructure that is available:

The UNMS II displays incoming information directly on arrival, but can not determine when a valid e-mail arrives from a remote system.

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 the GENEREX website, visit 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's, 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.

Difference between CS141 Modbus and CS141 Professional

Each device of the CS41 family is capable to handle Modbus over IP. The Modbus devices have an RS485 interface instead of the standard mini-DIN connector for sensors, specially designed for Modbus infrastructures.

Modbus Pin assignment


As a default, a Modbus plug is installed od delivery. The plug can be removed and later simply assembled to ensure a fast and intuitive wiring procedure.

Please note the plug alignment:

Before wiring, ensure the terminal strips are at top of the cable slots - not below them.



By doing so, the following PIN assignment can be used:

Terminal strip	PIN	Description
	1	GND
	2	RS485 A+
	3	RS485 B -

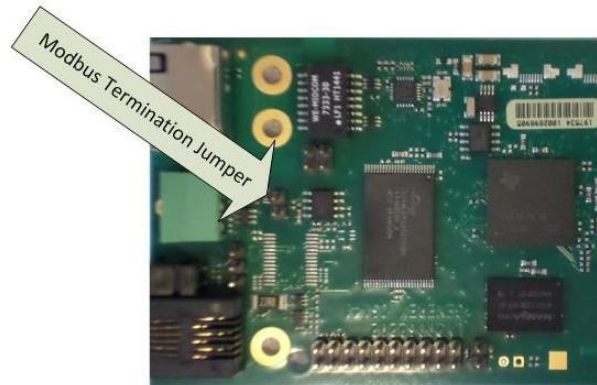
To insert an appropriate cable, pull back the spring mechanism - the clamp will automatically lock the cable at the desired position.

The Modbus Terminator-PIN

Another difference with the CS141 Professional: The CS141 Modbus adapter is capable to drive a real RS485 Modbus protocol - not only Modbus over IP. In case of operating within a real Modbus environment, you can easily integrate the CS141 Modbus adapter.

Since Modbus expects termination resistors on both the first and last devices in the bus network, the CS141 Modbus offers an optional 120-ohm resistor that can be enabled by setting a PINS.

As a default, this PIN is set to OFF - the CS141 is configured not to be the last device within the Modbus network. If required, this pin can be set manually.



Note:

In general, the CS141 MODBUS will query the UPS via SNMP and provide appropriate MODBUS addresses and values. Due to this fact, the UPS can be queried via MODBUS. Technically, the UPS is not connected to the Modbus network natively. However, the Modbus controller will not be able to recognize this fact.

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:

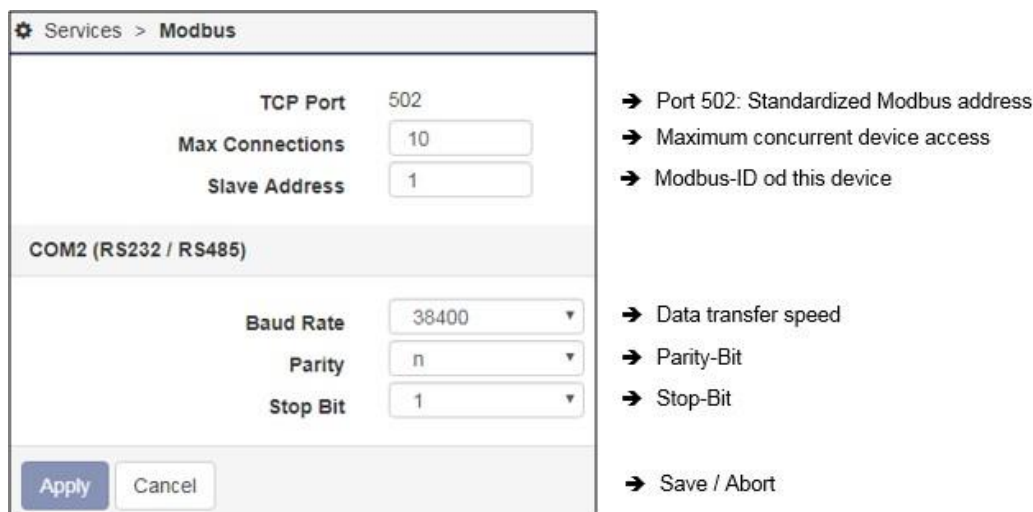
- 02H
Illegal Data Address
The address data obtained with the valid request is not a valid address servable by the slave.
- 03H Illegal Data Value
A contained value inside a valid request is not an allowed for this slave.
- 06H Slave device busy
The slave has received a valid request, but is currently 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 some time 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.



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 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 synchronization 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

For this configuration step, navigate to the following menu:



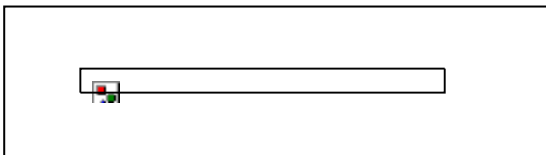
Developed by the IETF the Simple Network Management Protocol is designed for monitoring and controlling network elements from a central station. The protocol controls the communication traffic between monitored devices and monitoring stations: SNMP describes the structure of the data packets that can 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:



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

- 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

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.

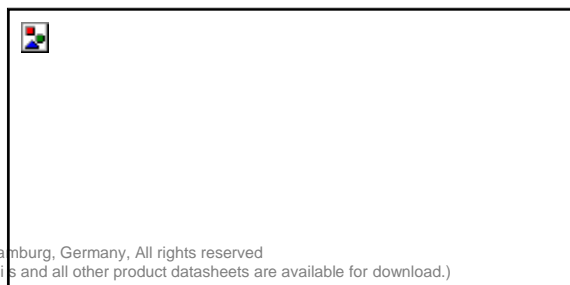
Configuring trap receivers on the CS141

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



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.

Trap receiver test



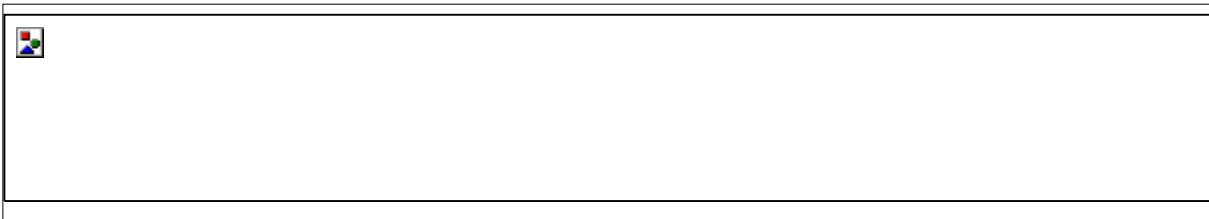
The Trap receiver can be subsequently tested by pressing the test button. The corresponding test message should be displayed directly in your management program.

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:



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

Add User

User:

Permission:

Security Level:

- ➔ 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.

Trap receiver test



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

Restarting SNMP agent

This function is available up to firmware 1.78. With firmware 1.80, this feature is an automated background process. No configuration is required.

For this configuration step, navigate to the following menu:



Within a specific and non-standard operating environment, the SNMP agent may stop responding as expected. The CS141 therefore provides a sub system to ensure the SNMP agent is running and alive.



In case of the SNMP agent suddenly dies, these options are available:

No action	the recovery service will not bother the SNMP agent with something like restarting.
Restart	the recovery service will restart the SNMP agent if it does not answer.
Delay [Min]	time delay until the Recovery service will restart the agent.

Note:

In some cases, SNMP v1 queries may cause a hung up of the SNMP agent. Although not officially supported, the CS141 can work with the appropriate SNMP v.1 queries. The agent recovery service ensures that the agent is automatically restarted in case of doubt.

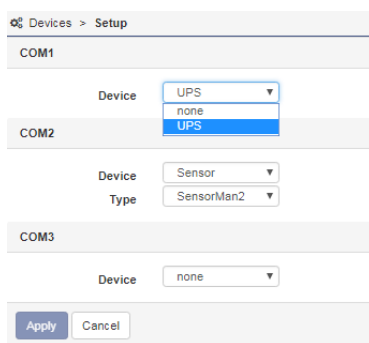
UPS Configuration

General COM Port setting

For this configuration step, navigate to the following menu:



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.



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.



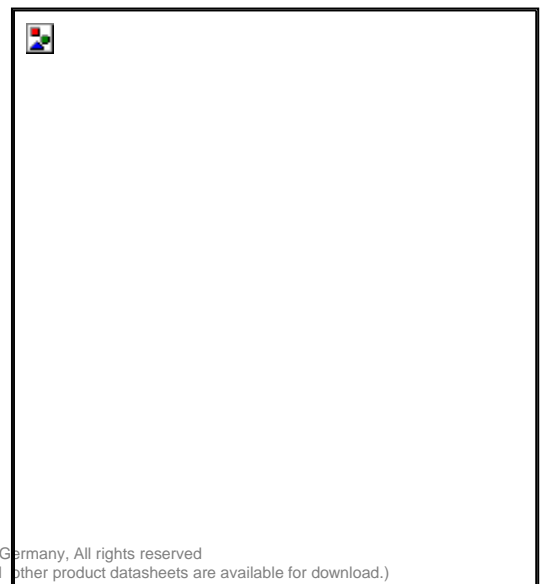
➔ UPS service start up routine in progress



menu accessible

➔ The UPS feature finished booting, the UPS

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:



UPS pipe through function

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

- Sensors
- Modbus
- External modems
- UPS Signal piping

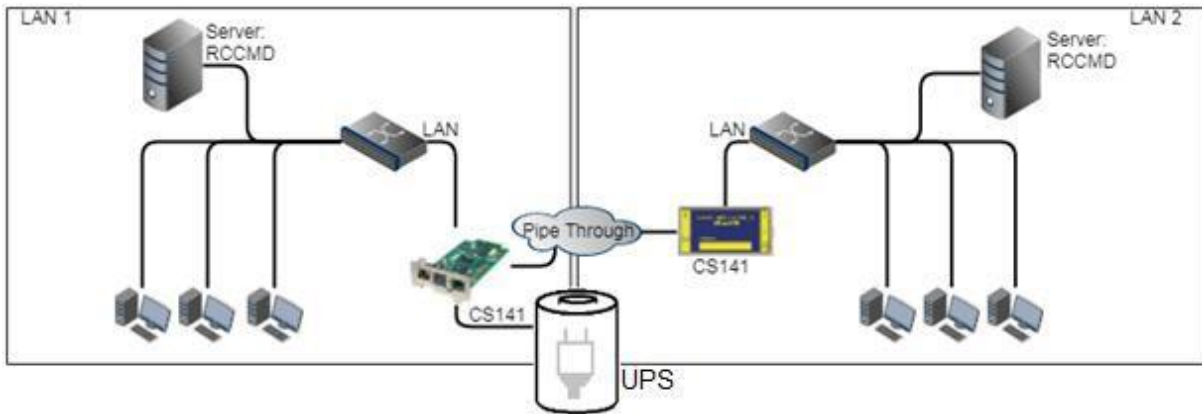
In companion to UPS configuration, the Pipe-Through functionality of the CS141 offers an advantage in UPS signal usage:

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.

Configuration of a UPS

For this configuration step, navigate to the following menus:



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

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. These cable types can be used to map different functions and switching states.

UPS-ID

If large UPS systems use more than 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(%)

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.

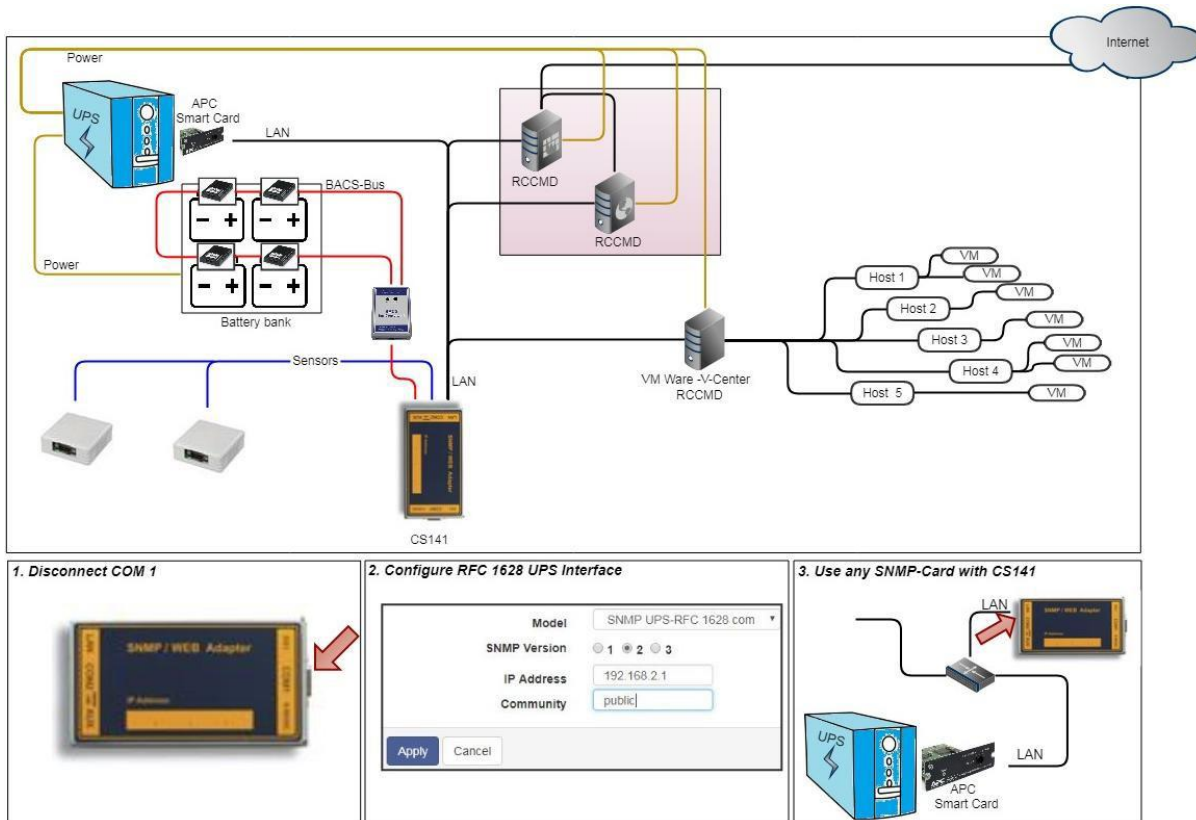
The default setting for this test is 10% deviation - but can be specified with a custom value between 5% and 30%.

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 target 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**

Devices > UPS > Setup

Model	SNMP UPS-RFC 1628 compliant
SNMP Version	<input checked="" type="radio"/> 1 <input type="radio"/> 2 <input type="radio"/> 3
IP Address	10.10.10.10 <small>IP address required</small>
Community	public

Apply Cancel

- ➔ 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 target SNMP card, choose SNMP version 1 or 2

SNMP Community

Enter the SNMP Community configured at target 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 target 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

→ 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

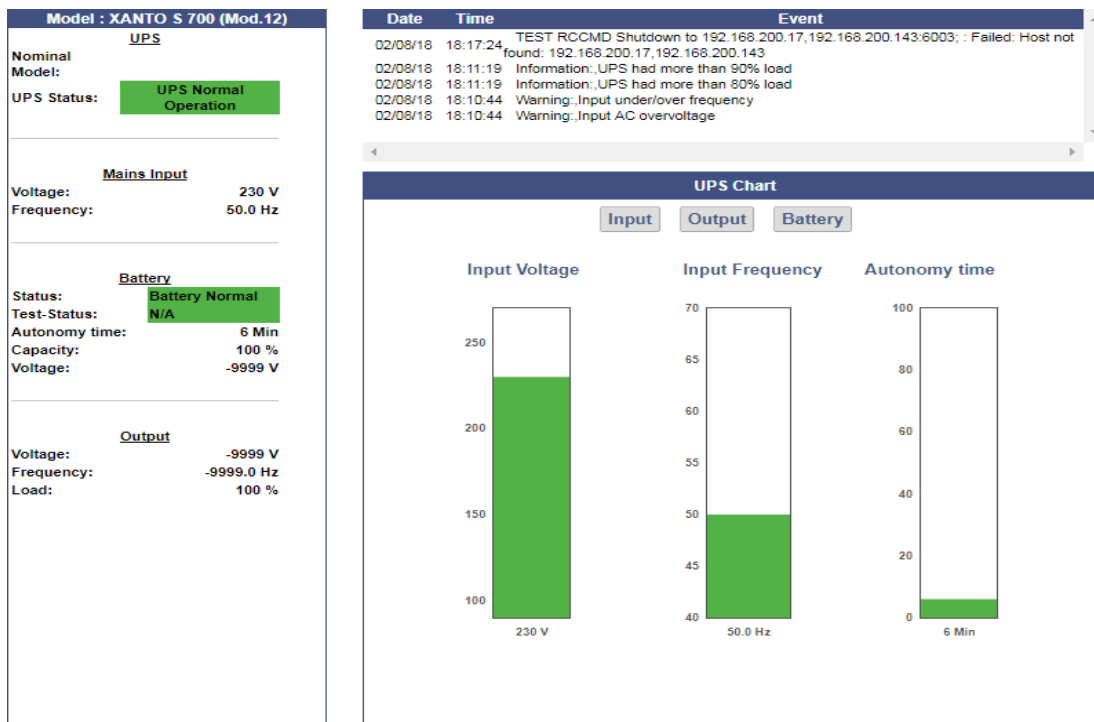
The CS141 supports SNMP v1, v2, and v3 in this mode.

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

UPS-Monitor: Checking UPS Settings



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:



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:



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:

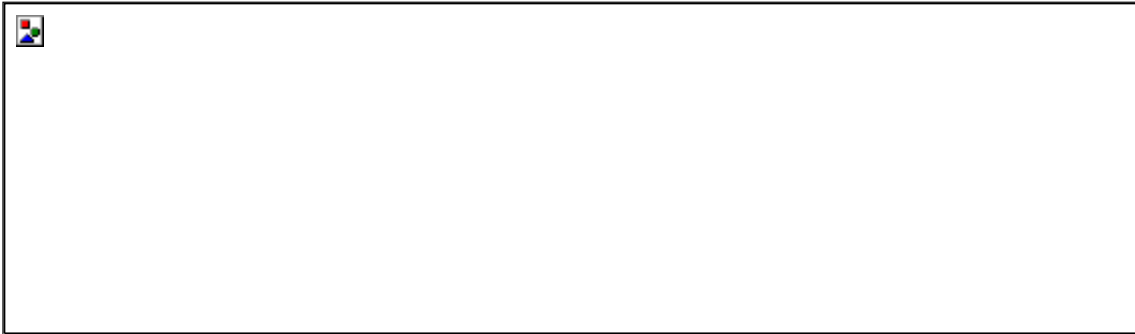
In some cases, a UPS command may seem to fail or an error message may appear. This behavior is based on the fact a UPS receives and confirms a command, but without doing it until pre-conditions are fulfilled. As an example, there must be a minimum charge for a particular battery test - otherwise the 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 behavior of a UPS system is unique and for some cases unfortunately not predictable.

UPS Control settings

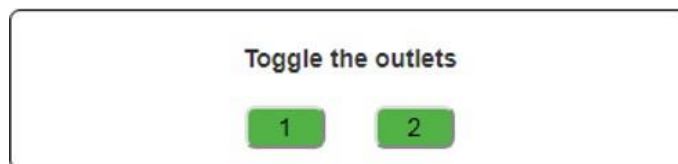
Depending on design and model, some UPS systems support additional functions to be used for verifying the performance of the UPS. The scope of functionality and configuration possibilities varies considerably and depends on both the manufacturer as well as the model to be used.

Typical functions a UPS may provide:



Switchable output

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



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.

What is the intention of a 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 fulfill 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 is appended 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.

In order to test a job, two conditions need to be adjusted according to the job:

1. Jobs according to e-mails require valid e-mail account data
2. Jobs based on the TCP / IP settings require a valid network configuration

Before continuing configuration ensure all access data are available for configuration, network settings are correct, and that the CS141 is in the regular operating mode inside 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:



Select  to open the job table:



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 cannot 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

Job	UPS Shutdown	→ Choose the job
Parameter		
Shutdown Time	<input type="text"/>	→ Time delay until system shutdown
Restore Time	<input type="text"/>	→ Time delay until system restart
Type	1	→ Toggle shutdown type

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 preset 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

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

Event contains...

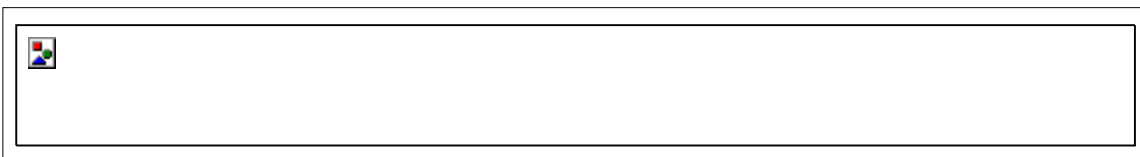
Search for a UPS event. By typing a part of an event all events according to the text fragment are listed.

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.

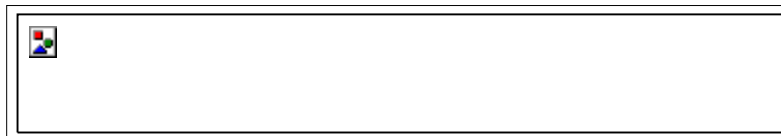
Configure a Job

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

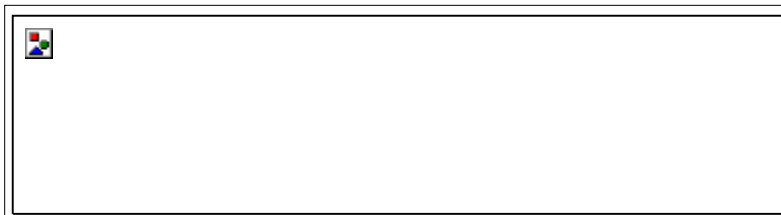


Different jobs provide different parameters to be configured

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

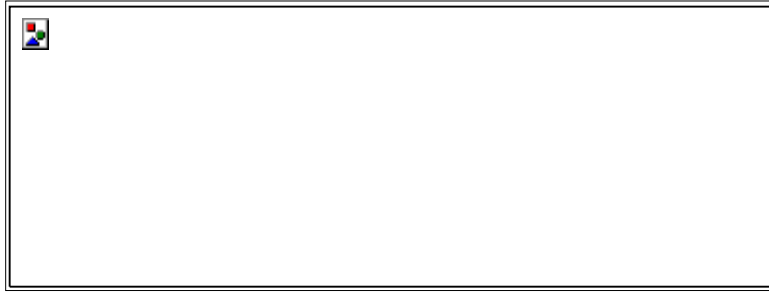


Example 2: RCCMD execute – Due to the fact RCCMD needs IP address data, the parameters will change.



Job timing

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



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 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.

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 requires 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.



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 **+**.

Delete a job

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

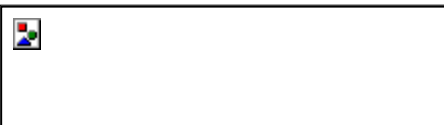
- Delete a job

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.

Counter 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 menus:

<ul style="list-style-type: none"> – Devices ⚙ Setup – UPS ⚙ Setup 🔔 Events 🔧 Functions ⚠ Custom Thresholds 	<ul style="list-style-type: none"> ➔ System tab: Devices ➔ System menu: UPS ➔ Event handling configuration dialog ➔ Custom defined system event configuration dialog
--	--

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
- vent menu to assign jobs

		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	greater 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 Threshold Warning Low On
>	+	-	Battery voltage Threshold Warning Low Off
>	+	-	Battery voltage Threshold Warning High On

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 behavior 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.

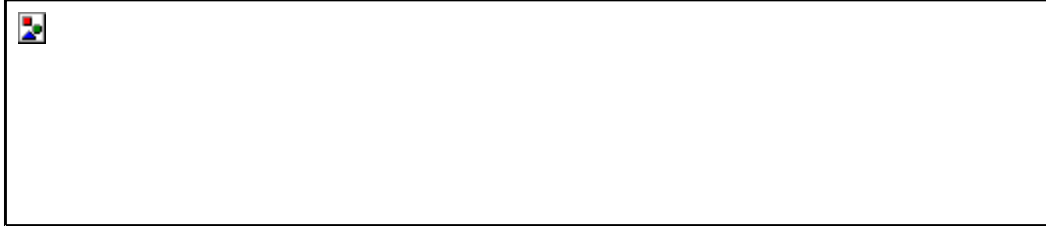
As an example, the manufacturer of a device specifies the "safe operating temperature" between + 5 ° C and + 39 ° C:

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.



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:



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

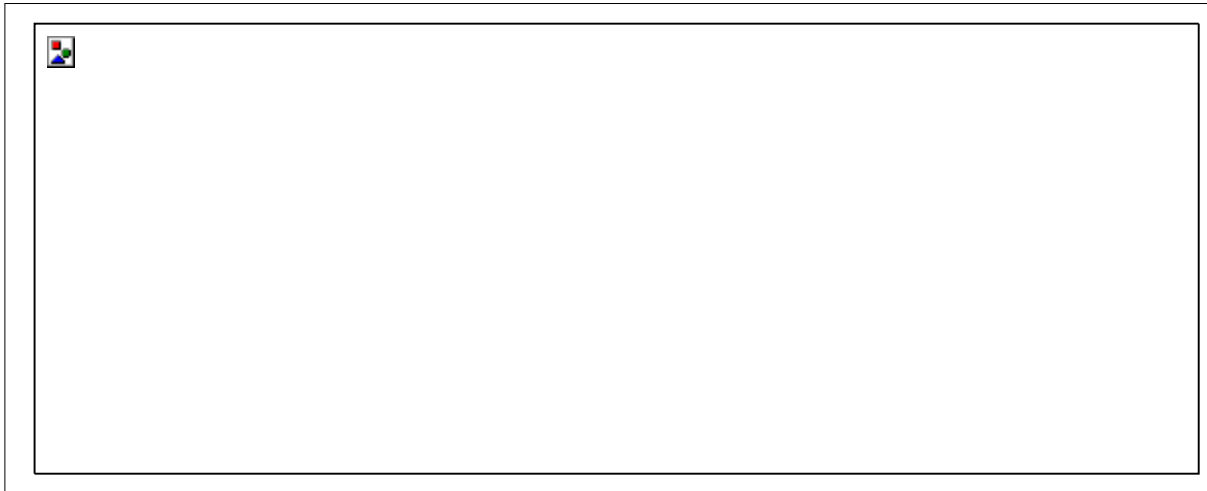
The alarm levels represent an escalation level and, if necessary, should trigger emergency measures, the values must be adjusted accordingly to warning levels.



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:



Battery Voltage <i>out of range</i> 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 <i>out of range</i> 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 <i>out of range</i> 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 behavior based on the temperature values that the UPS supplies.
UPS Autonomy <i>less than</i> XX m	in some cases, it may be useful to define additional alarm behavior about the remaining time a UPS ensure emergency power in autonomous mode - as an example if defined jobs depends on a configured time delay and due to several short power outages in a row Time is available: An emergency behavior scenario could be an alarm shutdown of systems.
Battery Charge <i>less than</i> 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 behavior can be defined using this value.
Output Load <i>less than</i> 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 behavior.
Battery Symmetry Pos./Neg. <i>greater than</i>	Some UPS systems use the positive and the negative half wave of AC to charge batteries. This setting defines the alarm behavior if the positive battery string and the negative battery string are not loaded evenly.
Seconds on Battery <i>greater than</i> 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 autonomy 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 behavior 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 ThresholdsProblem 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 behavior 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:

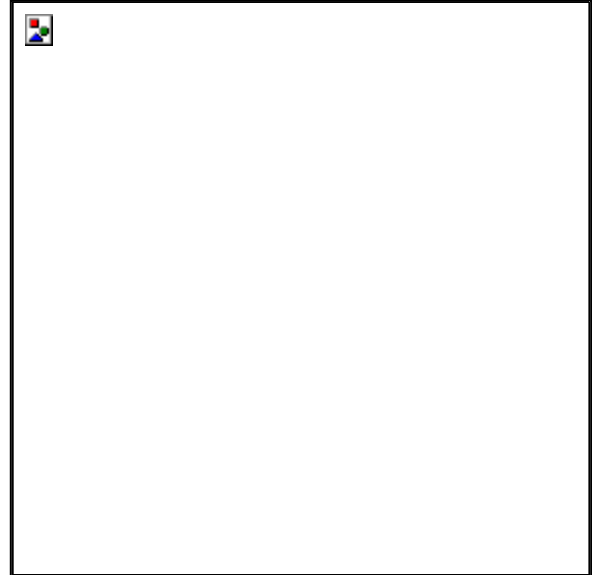
Turning off the same devices 70% and to on position at 61% could cause conflicts between events and jobs, devices should therefore be consistently configured separately

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*



CS141 as RCCMD Server deviceEver 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

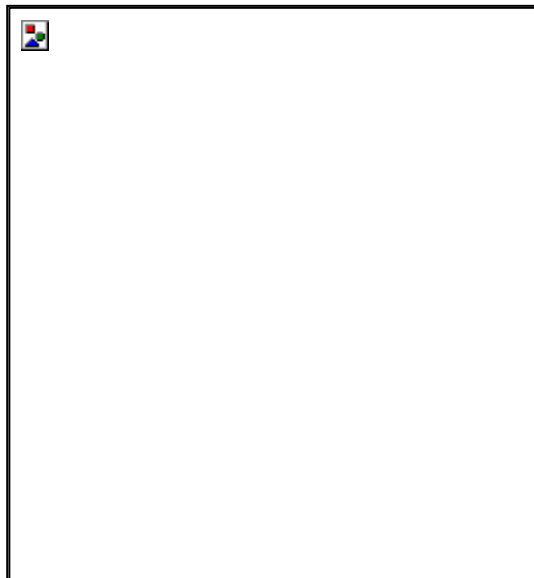
A separate license is available and can be obtained worldwide from licensed resellers, OEM partners or directly ordered at www.generex.de.

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 advice 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 advice 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.

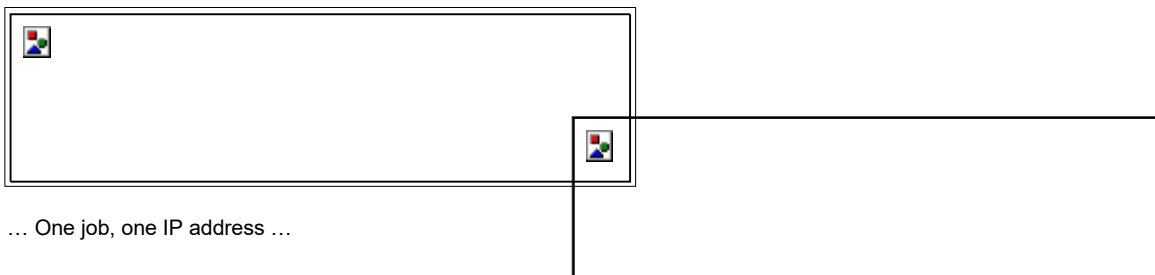
Limiting IP addressing

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.



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.

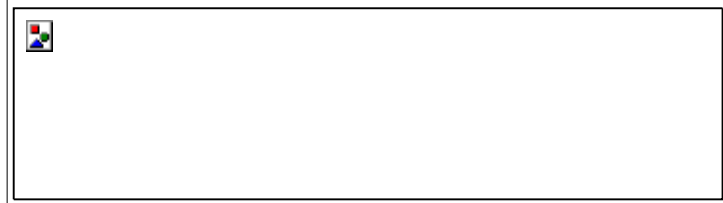
Note:

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

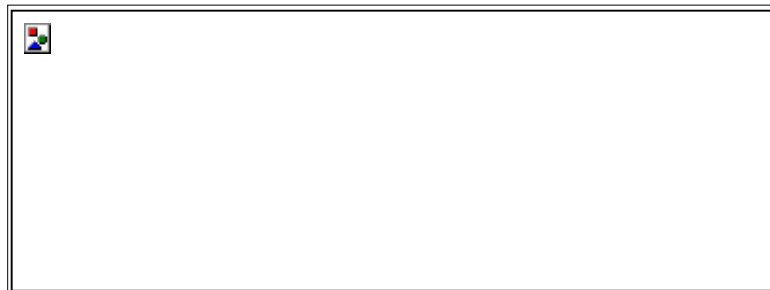
As a default port, RCCMD uses port 6003. The RCCMD client is listening on this port for a valid RCCMD command.

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



RCCMD Job Timing

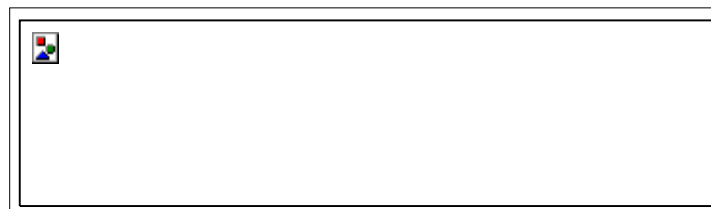
The CS141 provides many system events a job can be assigned to. Some jobs allow to configure advanced timing:



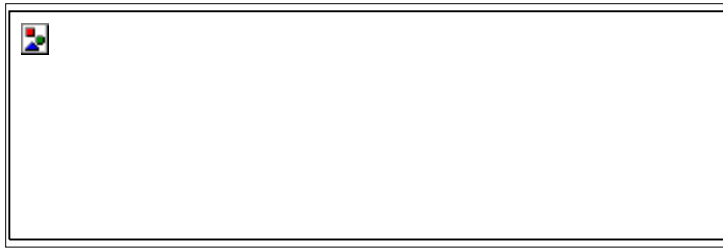
- Immediately, once as soon as an event happens, this job is executed at once and not repeated.
- After XXX seconds: The CS141 will wait a pre-defined time in seconds and then execute the job. If the event is no longer active before time is up, the job will not be executed.
- Repeat all XXX seconds: The job is repeated cyclically until the event 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

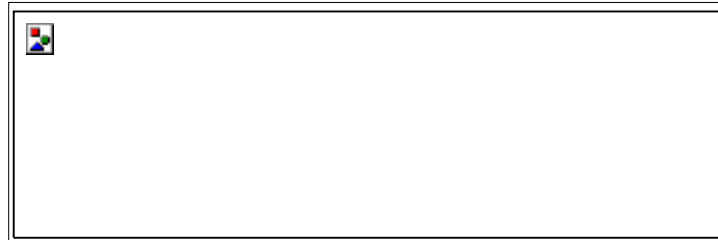
Der RCCMD Shutdown



The RCCMD shutdown is predefined and advises 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

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

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 hallowelt.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 currentstate 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:

#AGENTSOFTRREV	CS141 Firmware Version
#AUTONOMTIME	autonomy time in minutes
#BATT2OLD()	time in months until event „Please check batteries- is triggered
#BATT2OLD_YEARS	battery age in years
#BATTCAP	battery capacity in %
#BATTINSTDATE	installation date of the battery
#BATTTESTDATE	date of the last battery test
#BATTVOLT	battery voltage in V
#CHARGECCURR	momentary loading current
#CNT_BL	counter battery low
#CNT_PF	counter Powerfail
#CNT_SA	counter active shutdowns
#CNT_SD	counter shutdowns
#CNT_TF	counter testing failure
#DATE	current date
#EVENTSTATE	obstatus (idle, error, progress, success)
#FULLTESTDATE	date of the last full battery test
#GETLASTRESULT()	last test results
#HOLDTIME	hold time at 100 % load
#IDENT_NAME	name of the SNMP adapter
#INCCURR0/1/2	Eingangsstrom in A
#INFREQ0/1/2	Eingangsfrequenz in Hz
#INPHASES	Anzahl Eingangsphasen
#INPUTCURRENT0/1/2	incoming current in A
#INVOLT0/1/2	incoming voltage in V
#LASTERR	last error
#LOAD	current load
#LOCATION	Standort
#MANUFACTURER	manufacturer of the UPS
#MODEL	UPS model

#OUTFREQ0/1/2	Ausgangsfrequenz in Hz
#OUTPHASES	Anzahl Ausgangsphasen
#OUTPOWER0/1/2	Last in Prozent
#OUTPUT_VOLT0/1/2	
#OUTPUTCURRENT0/1/2	
#OVERLOAD	overload
#PHASES	phases
#POWER	power of the UPS
#RECHARGETIME	time needed for a full recharge of batteries
#RESTORETIME	restore time
#RUNTIME	uptime since last commissioning
#SECONBAT()	seconds on battery
#SELFTESTDATE	date of the last self test
#SERVER	IP address of the SNMP manager
#STATUS	system state
#SYSDATE()	system date
#SYSTEMTIME()	system time
#TEMPDEG	temperature in °Celsius
#TIMEZONE	time zone
#VOLTAVAI	USV bezogen, // USV hat eine Möglichkeit, die Inputvoltage abzufragen

Sensors and devices

For this configuration step, navigate to the following menu items:



Depending on used model, the CS141 offers to connect external sensors and devices sensors. These CS141 models support the connection of sensors:

- CS141 SC
- CS141 L
- CS141 R2
- CS141 Mini

SM_T_H_COM Standalone Sensor

This example shows how to configure the SMT_H_COM standalone sensor, a combined temperature and relative humidity sensor available for CS141.

The supplied standard length of the cable to connect the sensor to CS141 is 1.8 meters. If required, cable length up to 30m can be used.

Wiring the external sensor

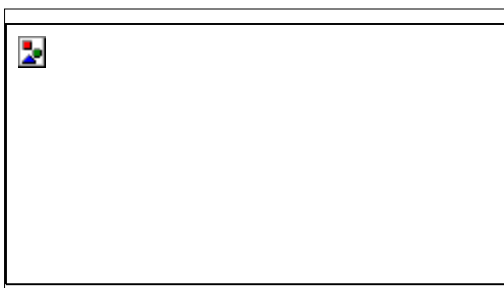
Connect CS141 COM 2 to SM_T_H_COM. CS141 does not require to reboot.

Basic Setup Configuration

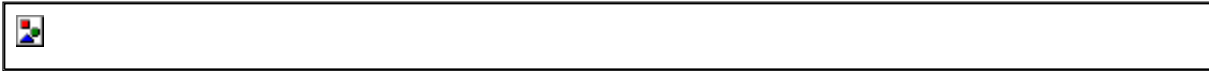
Under Devices / Setup, go to Configuration and change the setting at COM2 from none to Sensor.

After changing, define type of sensor connected to CS 141.

In this case, select SM_T_H_COM:



Press *Apply* to start the corresponding service. The status bar indicates the process.



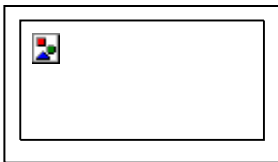
While Sensor is restarting, the according menus will be prepared. Please wait until the Sensor mark is set to -OKI before entering the configuration dialog of the sensor.

Configuration of zhe SM_T_H_COM combi sensor

Under the main tab *Devices*, open the sub menu *Sensors* and click on *Setup*. This will open the *Sensor configuration dialog*.

Name	Unit	Low PreAlarm	Low Alarm	High PreAlarm	High Alarm	Offset
Channel 1	°C ▼	10 <input type="checkbox"/>	5 <input type="checkbox"/>	80 <input type="checkbox"/>	90 <input type="checkbox"/>	0
water melon tank	% rel H	10 <input type="checkbox"/>	5 <input type="checkbox"/>	80 <input type="checkbox"/>	90 <input type="checkbox"/>	0

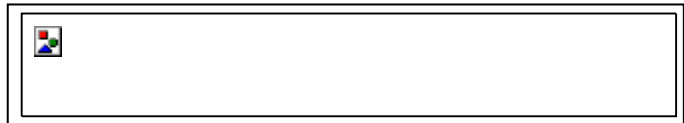
Name



At Name, enter the name, a description or an installation place of the sensor. The Name will appear at the sensor monitoring screen.

Thresholds Low / High und Alarm functions

The SM_T_H_COM combined sensor provides two different sensor types. The temperature sensor operates between -25 °C and +100 °C. The humidity sensor measures humidity range 0% and 100%. After installing the sensor, the maximum sensor range will be shown without a range restriction or notification markers. In order to define an alarm behavior, the CS141 needs information about the critical values and if necessary, a configured measuring range.



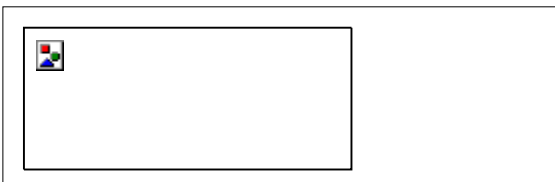
Please note the following rules during configuration:

1. The pre-alarm must be lower than the critical alarm setting.
2. The relative humidity is a minimum of 0% and a maximum of 100%
3. The coldest temperature value is -25 °C and the highest value + 100 °C

Note:

As long as the checkboxes for the according alarm is not set, the respective alarm marker. Due to this fact it is possible to configure notification and alarm values and test the settings before activating.

Offset - Settings



Although the SM_T_H_COM is already a calibrated sensor, the operating environment may require different values. The correction values will be defined via offset settings:

These values will be added or subtracted from the value the sensor provide. This allow to harmonize the sensor values with calibrated external measurings and to adapt the sensor for special operating conditions.

Sensor-related system events

The CS141 provides defining system jobs via connected sensors. The available system events refer to the measured values of the connected sensors. The following events are available for SM_T_H_COM.

SM_T_H_COM Temperature High

The value at Threshold (high) defines the upper critical temperature limit. If this temperature is exceeded, a corresponding alarm behavior can be triggered.

SM_T_H_COM Temperature Low

The value Threshold (low) defines the lower critical temperature limit. If this temperature is undershot, a corresponding alarm behavior can be triggered.

SM_T_H_COM Temperature Normal

Defined by the values for the upper and lower temperature limits. If no limits are entered, any displayed temperature will be displayed as "normal".

SM_T_H_COM Humidity High

The value is defined by Threshold (high) for the relative humidity and determines the upper critical limit for humidity. If this value is exceeded, a corresponding alarm behavior can be triggered.

SM_T_H_COM Humidity Low

The value is defined via Threshold (low) for the relative humidity and determines the lower critical limit for humidity. If this value is undershot, a corresponding alarm behavior can be triggered.

SM_T_H_COM Humidity Normal

Defined by the values for the upper and lower relative humidity. If no limits are entered, any displayed humidity will be displayed as "normal".

SM_T_H_COM Connection Lost

If the connection between the CS141 and the SM_T_H_COM tears off, a corresponding alarm behavior can be triggered via this system event.

SM_T_H_COM Connection Restored

The counter event to Connection Lost: The connection has been restored; a corresponding alarm behavior can be triggered via this system event.

Event classification

At the sub menu *Sensors*, click on the menu *Events*:

All sensor events use the same event classification:

- Temperature / Humidity High
- Temperature / Humidity HighPreAlarm
- Temperature / Humidity normal
- Temperature / Humidity LowPreAlarm
- Temperature / Humidity Low

Click **>** to open the general job list. With **+**, the job configuration dialog will be triggered to add a new job to the current job list.



Note:

For detailed information about how to manage jobs, refer the following chapter: [Managing jobs](#)

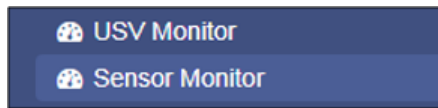
Ein Gegenjob zuweisen

Beachten Sie bitte, dass je nach Konfiguration einige ausführbare Jobs ein sog. Gegenjob benötigen, während andere Jobs lediglich nicht mehr ausgeführt werden müssen, weil das Ereignis nichtmehr ansteht. Dieser Job wird konfiguriert, indem es beim Eintritt in das entsprechende neue Ereignis ausgelöst wird – z.B. wird der Kontakt bei Erreichen von Temperature High automatisch geschlossen und als Gegevent bei Temperature normal wieder geöffnet. Unterdessen wird eine Mailbenachrichtigung so lange alle 5 Minuten gesendet, wie das Ereignis Temperature High ansteht.

Verwechseln Sie an dieser Stelle nicht ein Gegenereignis mit einem Gegenjob – das eine ist ein Ereignis, welches ansteht, das andere der entsprechende Job, der zu einem Ereignis ausgelöst werden soll – beides verhält sich relativ zueinander.

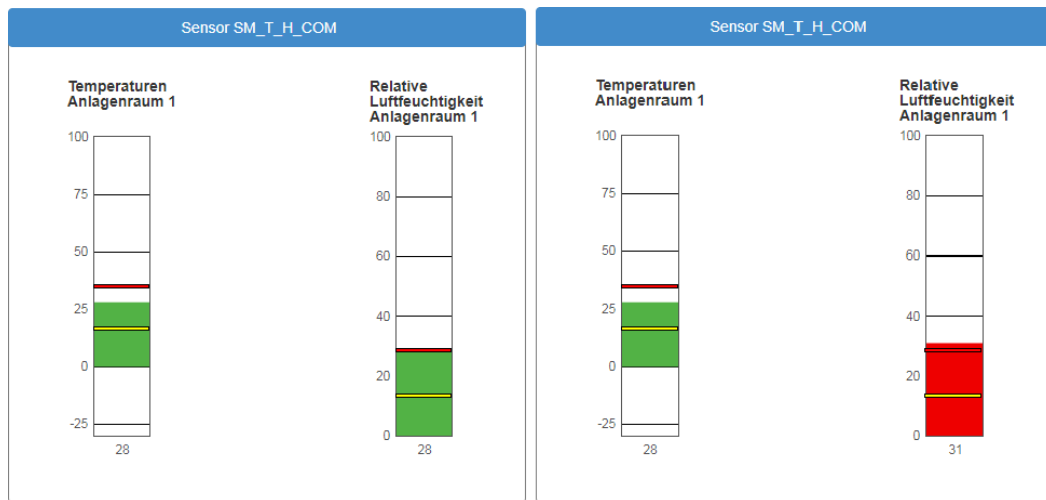
Monitor sensors: Check configuration

For this screen, open the following menu:



→ Monitoring of sensors connected to CS141

Once completed all settings, the sensor data will be shown at Sensor Monitor:



The yellow line represents the value of the Threshold (low). The upper line represents the Threshold (high). As soon as the value exceeds or falls below these lines, the color changes to red and a corresponding job can be triggered for the according sensor event. If you use pre-alarms and alarm settings, the Sensor monitor will show the according marker.

Tipp:

Sollten Sie mehrere Sensoren benötigen, bietet der CS141 über den Sensormanager die Möglichkeit, bis zu 8 Umweltkontrollsensoren zu betreiben.

Die genaue Konfiguration entnehmen Sie bitte der Installations- und Konfigurationsanleitung des SENSORMANAGERS, welche Sie unter www.generex.de im Downloadbereich erhalten können.

SENSORMANAGER

The SENSOR MANAGER is an optional accessory to extend the functionality of the CS141:

The GENEREX sensors / actuators can easily be connected to the SENSOR MANAGER, required RJ12 connection cables are included on delivery. The sensor can be configured via the web interface of the CS141 / BACSWEBMANAGER. Any third-party sensor or actuator that are conform with required specifications, can be used with the SENSORMANAGER.

SENSORMANAGER II application examples:*Monitoring of sensor data*

Temperature, humidity, electr.. Electricity, electr. Voltage, electr. performance and other analogue measurements.

Monitoring of contacts:

Door contacts, fire detectors, motion detectors, water detectors, glass breakage sensors and other potential-free signaling contacts.

Switching:

Switching of optical and acoustic actuators such as flashing lights, warning horns u. relay contacts

SENSORMANAGER II input signals:

Up to 8 analog inputs (0-10VDC o. 0 / 4-20mA)
Up to 4 digital inputs (potential-free contacts)

SENSORMANAGER II output signals:

Up to 4 digital output signals (open collector / 12VDC max 30mA)

SENSORMANAGER II PIN assignment of the Rj12 connection sockets

INPUT 1:

Pin 1	9-24VDC, output according to input of supply voltage, default delivery: 12VDC power supply
Pin 2	Analog input channel 1 (0-10VDC o. 0/4-20mA)
Pin 3	Analog input channel 2 (0-10VDC o. 0/4-20mA)
Pin 4	Ground (GND)
Pin 5	Digital output (Open-Collector 9-24VDC/max. 30mA, Default on delivery: 12VDC)
Pin 6	Digital input (min./max. 9-24V via Pin 1)

INPUT 2:

Pin 1	9-24VDC, output according to input of supply voltage, default delivery: 12VDC power supply
Pin 2	Analog input channel 3 (0-10VDC o. 0/4-20mA)
Pin 3	Analog input channel 4 (0-10VDC o. 0/4-20mA)
Pin 4	Ground (GND)
Pin 5	Digital output (Open-Collector 9-24VDC/max. 30mA, Default on delivery: 12VDC)
Pin 6	Digital output (min./max. 9-24V via Pin 1)

INPUT 3:

Pin 1	9-24VDC, output according to input of supply voltage, default delivery: 12VDC power supply
Pin 2	Analog input channel 5 (0-10VDC o. 0/4-20mA)
Pin 3	Analog input channel 6 (0-10VDC o. 0/4-20mA)
Pin 4	Ground (GND)
Pin 5	Digital output (Open-Collector 9-24VDC/max. 30mA, default on delivery: 12VDC)
Pin 6	Digital input (min./max. 9-24V via Pin 1)

INPUT 4:

Pin 1	9-24VDC, output according to input of supply voltage, default delivery: 12VDC power supply
Pin 2	Analog input channel 7 (0-10VDC o. 0/4-20mA)
Pin 3	Analog input channel 8 (0-10VDC o. 0/4-20mA)
Pin 4	Masse (GND)
Pin 5	Digital output (Open-Collector 9-24VDC/max. 30mA, Default on delivery: 12VDC)
Pin 6	Digital input (min./max. 9-24V via Pin 1)



Pin number:	Funktion:
1	9-24VDC, output according to input of supply voltage, default delivery: 12VDC power supply
2	Analog input channel x (0-10VDC o. 0/4-20mA)
3	Analog input channel x (0-10VDC o. 0/4-20mA)
4	Ground (GND)
5	Digital output (Open-Collector 9-24VDC/max. 30mA, Default on delivery: 12VDC)
6	Digitalinput (min./max. 9-24V via Pin 1)

Note:

The voltage provided by pin 1, pin 5 and pin 6 is defined by the power supply unit used on the SENSOR MANAGER. The SENSOR MANAGER itself operates at an operating voltage of 9-24V. If a 12 V power supply is connected, 12 VDC will be offered on these pins accordingly. When connecting external devices, pay attention to the maximum permissible voltage that may be applied:

Overvoltage can damage or even destroy connected devices. In case of undervoltage, however, connected devices may deliver wrong results.

On delivery the SENSOR MANAGER comes with a standard power supply providing 12 VDC.

Analog inputs:

Each of the 4 SENSORMANAGER_II physical RJ-12 connectors provide 2 analog inputs on pin 2 and pin 3.

Administrators wishing to connect a third-party device, must set the signal (0-10VDC o. 0 / 4-20mA) of the third-party device to PIN 2 or pin 3 and pin 4 (ground / GRD).

Digital inputs:

Each of the 4 physical RJ-12 connections of the SENSORMANAGER_II provides a digital input on pin 6.

For Administrators who wish to connect a third-party device:

The high signal (12VDC) from pin 1 must be routed to pin 6 via the signaling contact of the third-party device.

Digital outputs:

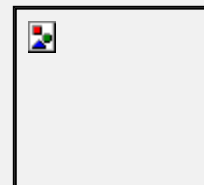
Each of the SENSORMANAGER's 4 physical RJ-12 ports provides a digital output on pin 5.

Administrators who wish to connect a third-party device:

The device must be connected to pin 5 (open collector output: + 12VDC / max.30mA) and pin 4 (Ground / GND) are connected.

Note:**How to use third-party sensors**

Due to the fact third-party devices do not have the standardized RJ12 port, our Connection Terminal SM_CON is an easy-to use possibility to connect these devices to the CS141. By using the SM_CON it is possible to adapt open line ends to the Rj12 connector directly - No custom plug

Connecting sensors / actuators to the SENSORMANAGER II

The sensors / actuators for the SENSORMANAGER II can be connected directly to the SENSORMANAGER II RJ12 sockets- ensure to use the original RJ12 cables supplied with the according sensor.

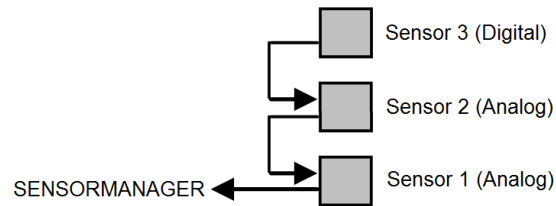
The SENSORMANAGER II provides to connect several sensors / actuators to one physical port. The system design provides following wiring options:

1. A maximum of two analog sensors per port
2. A maximum of one more digital sensor per port
3. A maximum of one digital actuator per port

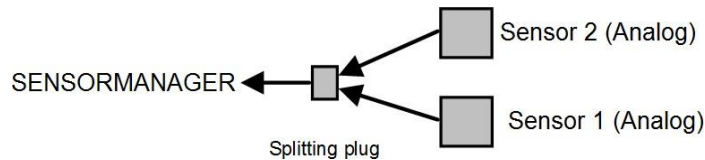
The sensor manager supports a total installation of 8 analog and 4 digital sensors as well as up to 4 digital actuators.

Sensor connection scenarios: SENSORMANAGER II.

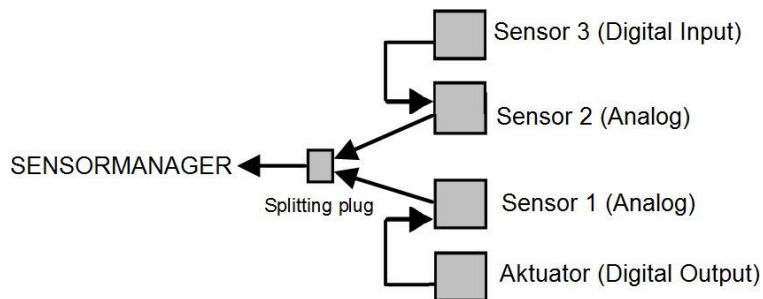
The SENSORMANAGER II provides various options to connect sensors.

The Daisy Chain: Connection

The daisy chain is a sequential arrangement of sensors and actuators. The signal is transmitted from the sensor manager through the first sensor to the second sensor. In this installation example, a digital third sensor is attached to the second sensor. Please note that no further digital sensor can be attached to the sensor 3.

The Splitting Plug SPSMRJ connection

If sensors need to be installed in different areas, the signal distribution can be splitted into two wirings. The optional splitting plug will split the signal accordingly. Please note that the sensor manager can only serve two analog sensors per port.

Combined connections: Daisy Chain and Splitting Plug SPSMRJ

This installation constellation extends the existing installation by an actuator and a digital sensor: The port on the sensor manager is maxed out utilizing a total of 4 devices:
Please note the system design:

This installation design provides the maximum of two analog sensors and one digital sensor as well as one digital output per sensor manager port.

SENSORMANAGER II: Available sensors

These sensors are currently available for SENSORMANAGER_II:

GENEREX-Analog-Sensors:

SM_T (Temperature sensor -> 1 analog channel required)
 SM_T_H (Combined sensor: Temperature and humidity -> 2 analog channels required)
 SM_VMC (True RMS AC voltage sensor -> 1 analog channel required)
 SM_CSxxxA (AC- current sensor -> 1 analog channel required)

GENEREX-Digital-Input-Sensors

SM_HYG2 (water and humidity sensor -> 1 digital input required)
 SM_Glas (Glas breach detector -> 1 digital input required)
 SM_MD (motion detector -> 1 digital input required)
 SM_SD (Smoke - und fire dector -> 1 digital input required)
 SM_DC (door contact alarm detector -> 1 digital input required)
 SM_H2 (Hydrogen Sensor -> 2 digital inputs required)

Digital GENEREX-Actuators:

SM_IO (Relais-Box -> 1 digital output required)
 SM_BUZ (accustical alarm buzzer -> 1 digital output required)
 SM_Flash (flash light -> 1 digital output required)

SENSORMANAGER II – Installation and configuration

Before you start ...

The configuration must be saved to the PIC processor of the SENSOR MANAGER. This will be done by the CS141 automatically if pressing save buttons. If a configured SENSOR MANAGER needs to be replaced, the configuration stored in the CS141 must be written to the new PIC processor by applying again. A spare parted SENSORMANAGER will not work without writing the new configuration.

SENSORMANAGER II: Connecting to CS141

Use the supplied cable to connect the COM1 of the SENSOR MANAGER II to the COM 2 of the CS141. Log into the CS141 and go to general COM port settings. Configure the comport for sensormanager usage.

Then connect the power supply to the SENSORMANAGER:

Two LED's are installed on the underside of the SENSOR MANAGER: one should now light continuously and signal the operational readiness. The second LED flashes only when the CS141 makes a request to the SENSORMANAGER.

After the SENSORMANAGER is ready for configuration, open sensor manager configuration menu at CS141 and start configuring your sensors and devices.

Note:

The CS141 will only make a request to the SENSORMANAGER if it is configured accordingly. The LED on the sensor manager will only flash when a request has been received or is answered by the SENSORMANAGER.

Please note that the sensor manager is a stand-alone device with its own power supply. In case of main power supply is not available will cause disabling the connected sensors and actuators. The CS141 will notice this fact and can be configured to send custom alarm messages for sensor lost issues.

When using a SENSORMANAGER, ensure both, CS141 and SENSORMANAGER are secured by independent power supply (UPS) for full operability in case of main power issues.

Sensor matrix

For this configuration step, proceed to the following menus



A special feature of the sensor manager is the possibility to link logically all available sensors and contacts via a matrix. Because the matrix does not tell you which sensors and digital inputs you want to use for linking to each other, there are numerous ways to map your operating scenario - as an example, a pressure sensor monitoring a pipe can be used with a temperature sensor on a corresponding pump in the first instance. With a second instance, different sets of sensor markers can be combined to trigger a unique alarm behavior.

How does the sensor matrix work?

As already described, the matrix is a link of individual instances that build on each other

1. Sensors and Inputs -> Individual single configuration and event management
2. Matrix marker -> Links logically individual sensors and digital inputs to a collective marker
3. Output switcher -> Links logically single alarm marker to switch an output

Each of these three instances has its own events, which can be assigned with jobs via the event control inside the sensor menu.:

Adding analog sensors

At system tab Sensors, open Setup to enter the sensor configuration dialog:

Sensor Inputs	Name	Sensortype	Unit	Low PreAlarm	Low Alarm	High PreAlarm	High Alarm	Sensor Range		Offset
1	Temperature	SM_T_H	°C	10	4	70	90	-5	100	
	Humidity	SM_T_H	% rel H	17	15	28	30	0	100	

Name

Enter a name or a description that will be shown at the alarm matrix as well as the sensor monitor.

Sensortype

Determine the type of sensor. To do this, select one of the predefined sensor types from the list. For third-party sensors, please consult the appropriate user manual to enable connection. Please note that some sensors are so-called combined sensors - two sensors in one housing. These require both channels and no further sensors can be connected.

Unit

With the choice of the sensor a suggestion for the indicated unit name appears. You can customize the name to your liking, but the unit that you see as a suggestion will not change itself.

Pre-alarm / alarm

Passen Sie an dieser Stelle die entsprechende Alarmstufe an. Dabei gilt folgendes Grundprinzip:

Adjust the appropriate alarm level. The following basic principle applies:

With increasing values on a measurement scale, the pre-alarm is BEFORE the actual alarm - at a temperature, e.g. the pre-alarm (pre-alarm) at 70 °C - the actual alarm is 90 °C. As the values decrease, the concept revolves: the pre-alarm must be higher than the actual alarm - in relative humidity, this means the pre-alarm is at 17% humidity during the actual alarm, which would be triggered at 15% relative humidity.

Note:

Please keep in mind, with decreasing temperatures the pre-alarm may be set with +3°C, but the actual alarm is at -5°C. From 0°C down, the numbers will start to increase with a negativ sign.

Sensor range

Many sensors have a predefined measuring range - in other cases it makes no sense to create a measuring range outside certain operating values. With this value range, it is possible to adjust the measuring range to a custom sensor as well as to specific operating environments.

Offset

Although all sensors are calibrated on delivery by GENEREX, operating conditions may use different reference values. The values may differ as a result from changing atmospheric pressure, ambient temperatures, solar radiation, etc. Use the offset values to adjust the values to fit to a local reference measuring. Simply enter the corresponding deviation:

If e.g. If your reference reading deviates downward at a temperature of 2 ° C, enter -2 as offset value.

Sensor event vs matrix event

Configured sensor alarms can be used to configure according event:

For each analog sensor, you will find 2 according events:

- Alarm Analog Input High -> Alarm: critical value reached or exceeded high alarm settings
- Alarm Analog Input High off -> Alarm: Critical value fell below high alarm settings
- Pre-Alarm Analog Input High -> Pre-Alarm: Questionable value reached or exceeded high pre-alarm settings
- Pre-Alarm Analog Input High off -> Pre-Alarm: Questionable value fell below high pre-alarm settings
-
- Normal state – no alarm -> No alarm configurable
-
- Pre-Alarm Analog Input Low off -> Pre-Alarm: Questionable value fell below low pre-alarm settings*
- Pre-Alarm Analog Input Low -> Pre-Alarm: Questionable value reached or exceeded low pre-alarm settings*
- Alarm Analog Input Low off -> Alarm: Critical value fell below low alarm settings*
- Alarm Analog Input Low -> Alarm: critical value reached or exceeded high alarm settings *

*) Please note the paradox that the value can also increase with negative values (eg at temperatures in the minus range).

For each of these events, you can configure a corresponding job to setup a specific alarm behavior. Using the alarm matrix, you can summarize the corresponding events and stitch them an event marker with coming with it's own conditions.

Open the menu Matrix to find all events as checkbox list:

Sensor Inputs	Name	Sensortyp
1	Temperature Area 51	SM_T_H
	Humidity in % Area 51	SM_T_H

	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Sensor Input 1				5	6	7	8	5	6	7	8	5	6	7	8
	Temperature Area 51				<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

At sensor configuration, you can enter a name for each channel. After entering a name press apply and change to the menu „Matrix-: The recently entered name will it will be displayed automatically as soon as you move the mouse over the according channel checkbox.

Setting up the logical connection

Using the logic link, the condition can be defined to set the marker to a logical On:

- And Both conditions must be
- Or At least on of the configured conditions are met.

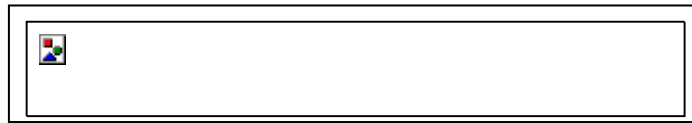
Inverted mode

As a standard, the marker is pre-configured to switch to ON as long as the conditions for ON are met. The inverted turn this switching behavior from OFF to ON: The marker ist always at High (ON) position and will will switch to Low (Off).

Digital inputs

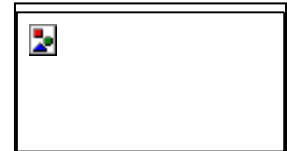
In addition to analog inputs, the SENSORMANAGER can manage up to 4 digital inputs. The inputs

Diese Eingänge werden entsprechend der Konfiguration auf Aktiv geschaltet und können im Alarmverhalten als NC (Normally Closed) oder NO (Normally Open) – Kontakt definiert werden.



Linking digital inputs

The marker only looks whether the result of the digital input is "High (On)" or "Low (Off)" - The type of contact is unimportant for the marker. Like the analog inputs, name of the digital input will be shown by mouse over action. The linking of the digital inputs follows the same principle as with the sensors.



Linking digital inputs and analog sensors

Simply select the appropriate digital inputs with the analog inputs. Press Apply to save the setting and restart the services for the sensors.

Switching an output

Outputs will be switched in case of conditions met via the defined alarm markers:

SensorMan2 Digital Outputs																		
Port	Name	Logic	Marker															
1	Output 1	And ▾	<table border="1"> <tr> <td>1</td> <td>2</td> <td>3</td> </tr> <tr> <td><input checked="" type="checkbox"/></td> <td><input checked="" type="checkbox"/></td> <td><input type="checkbox"/></td> </tr> <tr> <td><input type="checkbox"/></td> <td><input type="checkbox"/></td> <td><input type="checkbox"/></td> </tr> <tr> <td><input type="checkbox"/></td> <td><input type="checkbox"/></td> <td><input type="checkbox"/></td> </tr> <tr> <td><input type="checkbox"/></td> <td><input type="checkbox"/></td> <td><input type="checkbox"/></td> </tr> </table>	1	2	3	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
1	2	3																
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>																
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>																
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>																
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>																
2	Output 2	Or ▾																
3	Output 3	Or ▾																
4	Output 4	Or ▾																

In contrast to the markers, however, no pre-alarms are used - if the marker is set to high, the output will be switched depending on its switching logic. The CS141 matrix provides combining up to 8 markers individually and assign them with an AND / OR combination. The output will be switched:

1. As soon as only one of the configured marker are set to high. („OR-)
2. As soon as all configured marker are in high state („AND-)

Fallback of the output to normal state

the output is only switched as long as the condition has been fulfilled exactly hereby the corresponding logical link will decide which condition leads to the drop of the output:

In a restrictive AND operation, only one marker to off will force the output to off.

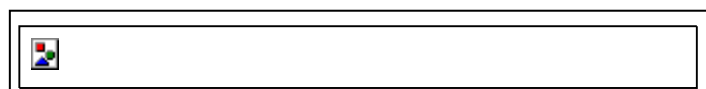
With an OR operation, the output remains at ON state until each marker is turned off.

Keep in mind that the markers conditions for an on/off state will not be checked by output switching control – This control only checks logically the markers state and act according to it.

Tutorial: Example scenario: aquarium

In this simple example the cross reference between a cracked disc and a leaking aquarium will be described. It shall show you how markers, inputs and outputs will be linked and work together. The total scope of scenarios can reach very high complexity and fitted even to very custom problems....

Huge aquariums with large glass panels are dependent on ensuring the structural integrity. If a glass panel is damaged or cracked, a

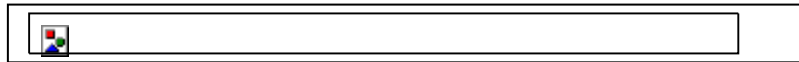


corresponding alarm must be issued automatically. For this purpose, the sensor manager offers a digital input:

The method this crack sensor uses to detect a cracked glass is a secondary question as the SENSOR MANAGER also supports the connection of third-party sensors. If necessary, connect an additional relay box to each sensor manager input: With the SM_IO box, managing all 4 inputs and outputs is made intuitive.

In this scenario, a glass crack sensor would close a switch and thus report a problem to digital input 1.

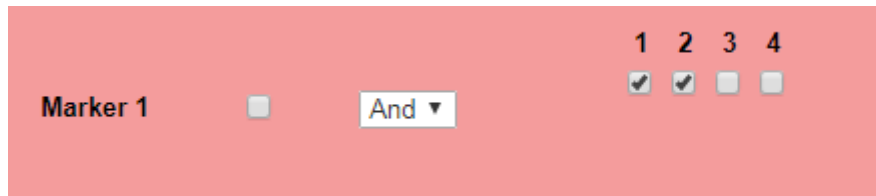
The second essential value is the water level of our aquarium, which requires intervention drops below a certain amount of water. In this case, a level sensor is used, which closes a digital contact at a filling level of 80%:



This input clearly indicates that the water level has dropped, but not why it happened - normally this will be caused by natural evaporation.

The cross reference:

Using the matrix, you can now handle both events in conjunction to each other:



In this case, marker 1 would be set active if both inputs are closed at the same time: The idea is that a glass crack alarm is present AND the level has dropped below 80% - in this case someone should be informed at once.

In the Events menu, fsearch for Alarm Marker 1:

In diesem Beispiel soll eine SMS geschrieben werden, sobald beide Bedingungen erfüllt sind:

In this example, an SMS should be sent as soon as both conditions are met:

At the moment the marker is activated, the CS141 will issue an emergency SMS if a GSM modem or alternatively an IP modem is available. Thus, both individual input events have been directly connected, other jobs are possible that will be repeated as long as this marker status is present.

The marker status will be terminated with two basic conditions:

1. The water level has been corrected
2. The glass damage has been fixed

Since these two conditions are coupled by an AND link, this marker is triggered only when both conditions are met.

Using several marker

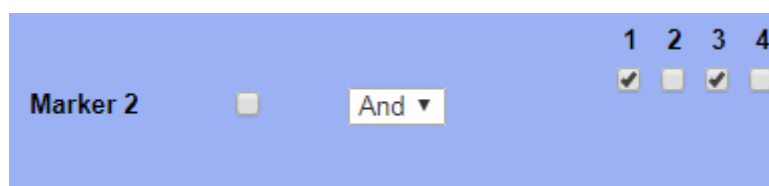
This marker can handle two basic problems:

A dropping water level below 80% and some kind of cracking glass. And yes, if this happens simultaneously, it is possible that water leaks. Due to the fact, 20% water inside an observation room can be very many water, a third sensor may be useful:



This sensor will find water or increased humidity levels at visitors observation room - something that can only be caused by a cracked aquarium windows (or something visitor- caused).

With the matrix settings, a second sensor can be configured:



This marker defines that there is a glass breach alert present and water is found at visitors observation room., dass ein Glasbruchproblem vorliegt und im Besucherraum zudem Wasser auftritt.

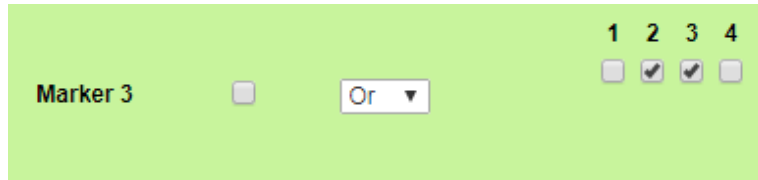
The Or connection

Okay, from now on the emergency conditions are set:

1. Glass breach and water level drops below 80%
2. Glass breach and water found at visitors observation room

Es However, it may now be the case that the water level drops and / or water is reported in the visitors' area without an obvious glass breakage. This may happen and someone need to maintenance this issue, but it is not really critical. In some cases it could be wanted.

To show this scenario, a third marker can combine both conditions with an OR:



This basic marker can be used as a non-critical overview lookup:

1. Water level below 80%
2. Unusual Humidity or liquids found at visitors observation room

With the OR operation, these two conditions can occur independently of each other - in both cases, the marker is set to high – on the other hand, this marker will only fall back to off position if all standard maintenance work is done.

Switching outputs

In this example scenario, many trigger points are included. For the matrix, these issues are configured:

- Glass breach **and** dropping water level
- Glass breach **and** water/liquids at visitors observation room
- Dropping water level **or** water/liquids at visitors observation room

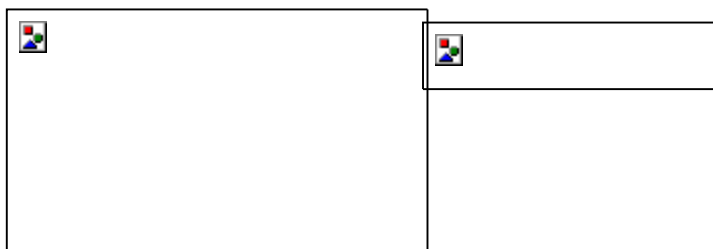
Die kritischen Probleme sind hierbei mit festen UND-Bedingungen verknüpft, da ein schnelles Handeln erforderlich ist. Die Eskalationsstufe ist, dass alle 3 Ereignisse aufeinandertreffen: Es gibt ein Glasbruchproblem, der Beobachtungsraum läuft voll Wasser und der Füllstand auf 80% gesunken ist.

The critical issues here are linked to fixed AND conditions because quick action is required. All three problems together means, visitors can be endangered: There is a glass break problem, the observation room will be filled by water and the water level has dropped below



80%. Perfect for automatic emergency procedures - all critical I markers can be summarized and linked to an output:

As long as marker 1 and marker 2 are set to ON (high), output 1 will be triggered :



This output can inform ordinate and subordinate monitoring systems via alarm contacts, switch of switch off sockets near the floor, etc. Via the event "Output 1 On", any additional job chains can be created inside for advanced automatic emergency measures.

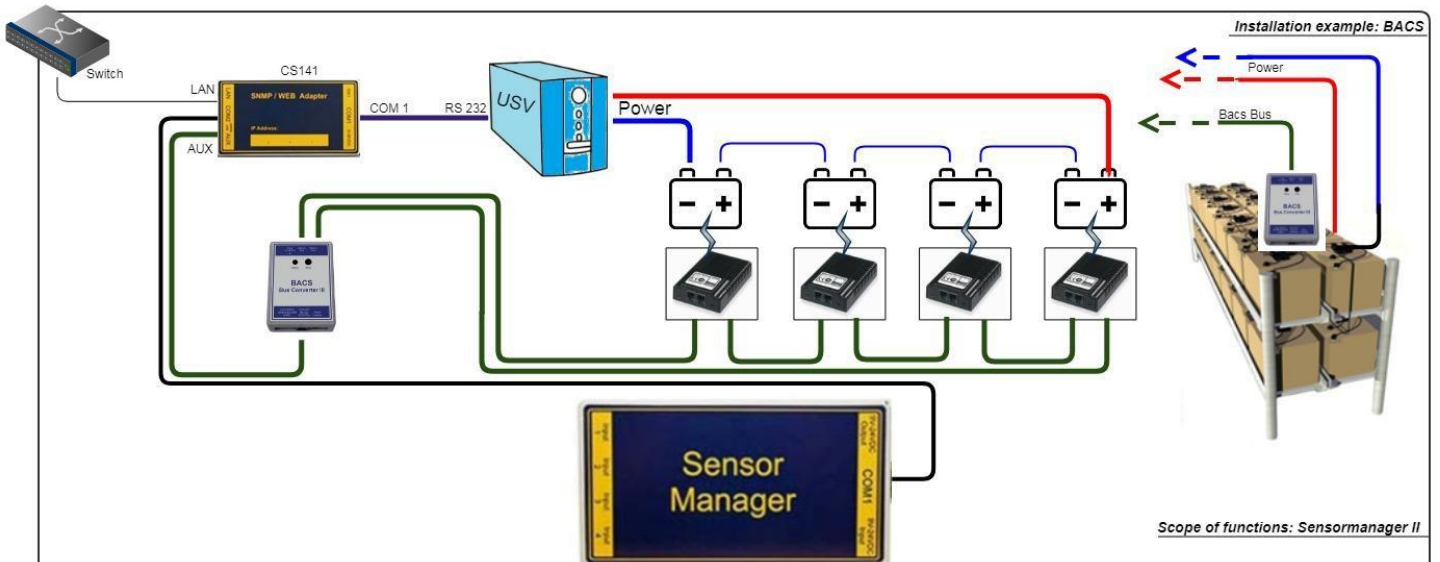
Fallback o normal state

The output will be switched off in case of one of these markers fall back to normal state.

Note

As with the configuration of the markers, you can create an And / Or dependency between up to 8 different markers. As an example, this function is useful if a machine may only be started if preconditions like pressure, temperature, etc. meet specific operating values. By using the matrix, the output that unlocks the start button will not be released until all conditions have been met..

Combination of sensors coming with the sensor matrix



Scope of functions: Sensormanager II

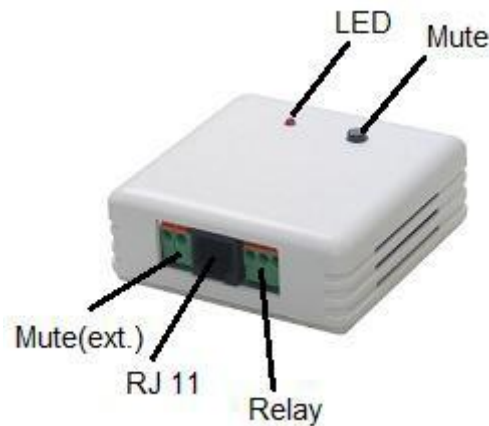
Digital output area	Digital input area	Analog input area
Active access control and warning <div style="display: flex; justify-content: space-around;"> <div style="text-align: center;"> SM_IO Relay boxes </div> <div style="text-align: center;"> SM_BUZ Acoustic alarm device </div> <div style="text-align: center;"> SM_FLASH Optic alarm device </div> </div>	Advanced access control <div style="display: flex; justify-content: space-around;"> <div style="text-align: center;"> SM_GLAS Glass breakage </div> <div style="text-align: center;"> SM_MD Motion detector </div> <div style="text-align: center;"> Any digital inputs </div> </div>	Current and voltage <div style="display: flex; justify-content: space-around;"> <div style="text-align: center;"> SM_CMC Current sensor </div> <div style="text-align: center;"> SM_VMC Voltage sensor </div> </div>
Triggering, switching, feedback <div style="display: flex; justify-content: space-around;"> <div style="text-align: center;"> SM_IO Relaisbox </div> <div style="text-align: center;"> Door buzzer </div> <div style="text-align: center;"> Switches </div> <div style="text-align: center;"> Ventiles </div> </div>	Digitale Alarmsensoren <div style="display: flex; justify-content: space-around;"> <div style="text-align: center;"> SM_SD Smoke detector </div> <div style="text-align: center;"> SM_HYG II Digital water alarm </div> <div style="text-align: center;"> Any digital inputs </div> </div>	Temperaturen und Gase <div style="display: flex; justify-content: space-around;"> <div style="text-align: center;"> SM_T Temperature </div> <div style="text-align: center;"> SM_T_H Combi sensor Temperature %Humidity </div> </div>
Open standards The digital outputs support third-party sensor contacts.	Open standards The digital inputs support third-party sensor contacts.	Open standards Full support of third-party analog sensors
<div style="display: flex; justify-content: space-around;"> <div style="text-align: center;"></div> <div style="text-align: center;"></div> <div style="text-align: center;"></div> <div style="text-align: center;"></div> </div>	<div style="display: flex; justify-content: space-around;"> <div style="text-align: center;"></div> <div style="text-align: center;"></div> <div style="text-align: center;"></div> <div style="text-align: center;"></div> </div>	<div style="display: flex; justify-content: space-around;"> <div style="text-align: center;"></div> <div style="text-align: center;"></div> <div style="text-align: center;"></div> </div>

As soon as potential-free contacts 0-10 VDC / 0-20mA are provided by the target system, the SENSORMANAGER II can establish a connection between the target system and the CS141:
 The scope of communication can be configured to interact from simple alarm wires up to complex communication structures with automatic feedback loops.

Buzzer

The CS141_BUZ is an acoustic alarm to be used with the CS141 SNMP adapter (CS141 SC or CS141 L). The CS141_BUZ is based on a piezo element using an internal power supply. Due to this fact, no separate power supply is required. The volume is about 85 db. The CS121_BUZ provides an RJ12 to be directly connected to CS141. Furthermore, an RJ12 socket for the output of PINs 1, 2, 3 to use external devices.

In addition, the acoustic signal of the buzzer can be remotely reset by closing a potential-free contact via the two-poled contact terminal block. Furthermore, a LED indicates a manually switched off alarm. This LED will stay blinking until it will be triggered by CS141 to normal state.



Technical data:

voltage usage:	12 – 15 VDC
power usage:	ca. 30mA
Volume:	ca. 85 dB
Connection type:	wired, RJ12, 6_5, 5_m
Dimensions:	70 x 70 x 40 mm

Connect to CS141:

Use enclosed cable to connect the buzzer CS141_BUZ to AUX Port of CS141.

Configure the buzzer:

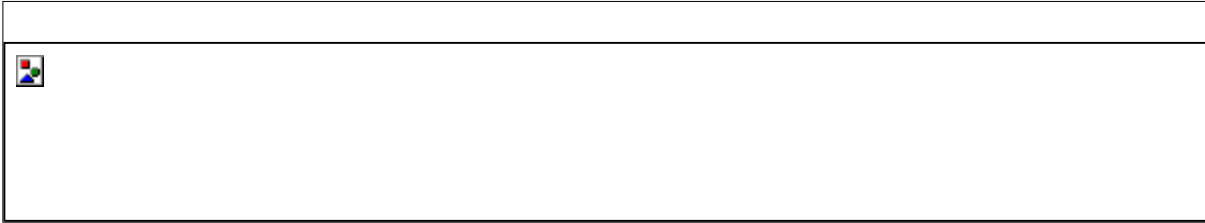
Step: 1



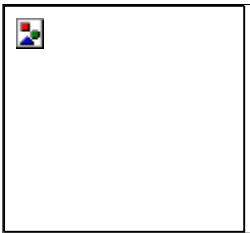
Under Devices/Setup, select Buzzer at COM and press Apply.

Step 2

Under Devices you find the buzzer alarm menu:

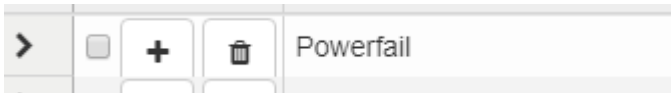


Apply transfers the current setting to the system configuration. Selected functions will be displayed at the BUZZER MONITOR. Furthermore, in the upper status bar the buzzer will be shown as operational.



Step 3:

Select an event the buzzer shall toggle – as an example buzzer alarm if recognizes a power fail



Press + to open job configuration dialog:

Under Job select Buzzer:

Relays on

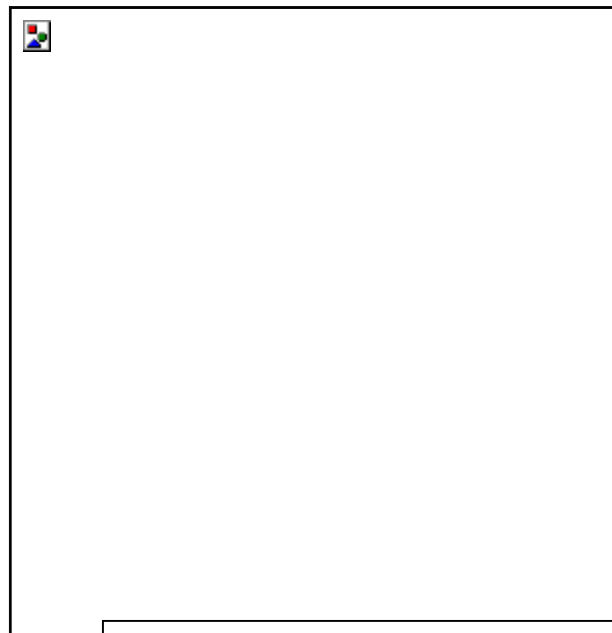
Additionally, the buzzer provides a relay for external connections to be switched.

Buzzer on

In case of a power fail the buzzer will be triggered. As soon as main power returned back, the event "Power restored" needs a job to switch off buzzer.

Events according to a buzzer

Search for the buzzer event menu:



At BUZZER ON click + to start job the configuration dialog

Choose the job to be executed, because the buzzer was triggered.

Depending on your setting, a corresponding action will be triggered in addition to the triggered buzzer and simultaneously noted in the event log.

Note:

You can define structured job chains by different devices connected to the CS141: Therefore, it is possible to select the BUZZER from inside the AUX menu and trigger it and use this system state to trigger the next event accordingly. In that case, the AUX event handling will trigger the buzzer and then the next event.

Events related to other devices

Events for this device can be performed by any device connected to the CS141. As example, an SMS is triggered by an alarm transmitter - a buzzer - because the alarm relay has jumped to ON:



At the event RELAIS ON, click + to start the configuration dialog:

Under Job, select the job to be executed because the buzzer's relay has been triggered.

Depending on your setting, a corresponding action will be triggered in addition to the triggered buzzer.

Note:

If installed, you can also select the BUZZER via the AUX menu and may it have triggered accordingly. In that case, the AUX event will trigger the buzzer. The fact the buzzer is triggered will be able to trigger the next event. This behavior allows you to define as many individual events as well as event chains. You can even configure time delays ...

GSM-Modem

A GSM modem provides the ability to notify responsible persons via SMS as an additional security measure. This is useful to help staff reducing response time.



GSM-T61

3GT61

*Technical data:***GSM-T61**

Power supply:	12 – 15 VDC
Power consumption:	ca. 30mA
Dimensions:	70 x 70 x 40 mm

3GT61

Power supply:	12 V
Power consumption:	ca. 50mA
Dimensions:	70 x 70 x 40mm

Set up SIM cards

Both - The CS141 as well as GSM cannot deal with dial-in data of your service provider. The SIM card must be preconfigured according to your service provider in a network-enabled device so that it does not require dial-in data for operation. For detailed instructions how to configure your SIM card, please refer your mobile service provider.

Insert SIM card to GSM modem

Insert the SIM card. Ensure the contacts of the SIM card is upside. Insert the card into the device under light pressure until it locks in place. To remove, press the SIM card. The spring mechanism unlocks and the card can be removed.

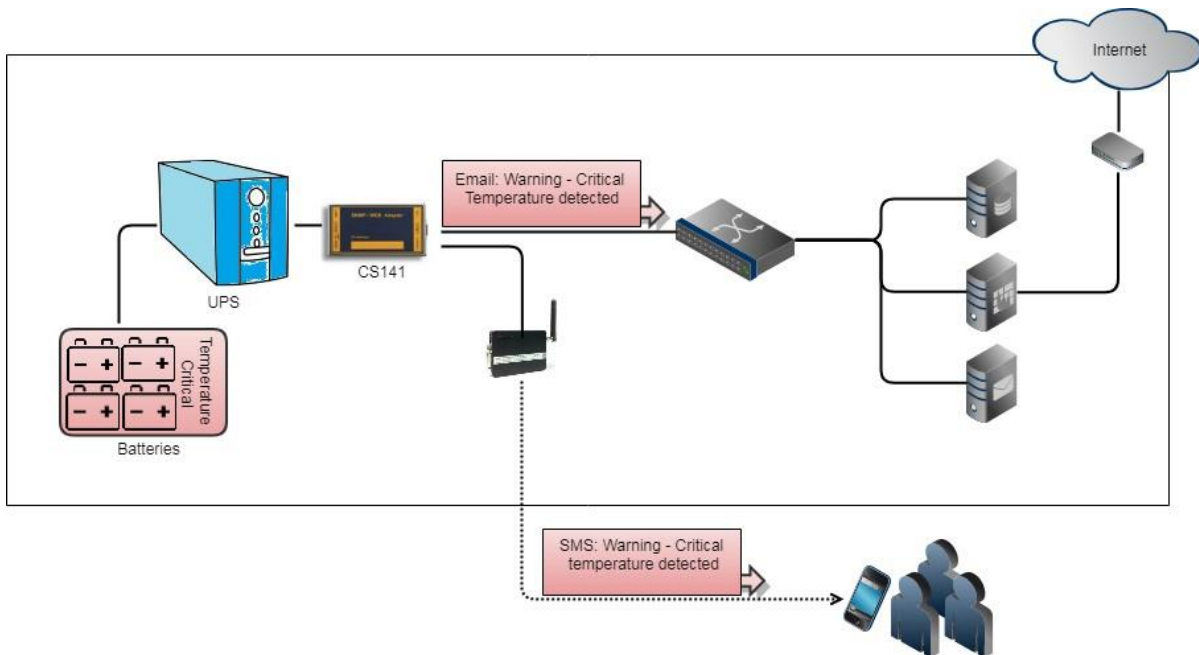
Connect to CS141:

Connect the COM port of the modem directly to the COM2 port of the CS141. Connect the power adapter.

How the GSM modem works

SMS modems provide the ability to notify responsible contact persons or administrative personal independently to any other automatic notification procedures in a very direct way. Due to the fact the GSM modem is a standalone device, it will work even in worst case scenarios when the intranet of a company is not available.

If emergency situations occur, it will help to shorten reaction time chain essentially.



In cooperation with other auxiliary devices, the GSM modem can be configured for numerous events:

- Critical temperature measurements
- Door contacts / access control and unauthorized entry
- Parent and child system failures
- Emergency ventilation usage
- ...

Please note that a GSM modem is intended for sending short messages and is not designed to connect to the CS141 via the local mobile network. Currently the following options are supported:

- A GSM-Modem as serial standalone device
- IP/SMS-Gateway SMS communication

Setting up the SIM card

There is no option to store access data for the SIM card inside the GSM modem or at the CS141. The SIM card must be configured accordingly by a network-compatible device to ensure no dial-in data ("without PIN") will be required for operation: The corresponding configuration guide for your SIM card can be obtained from your mobile service provider as well as from the operating instructions of the device selected for the configuration.

Insert / remove the SIM card

Once the SIM card has been configured appropriately to be used with the GSM modem, it can be inserted into the device. Please note that you insert the SIM card with the contacts upwards with slight pressure until it locks in place by a spring mechanism. To remove, press the SIM card to unlock the mechanism:

The card pops out and can be removed.

CS141: Setting up the GSM modem for serial usage

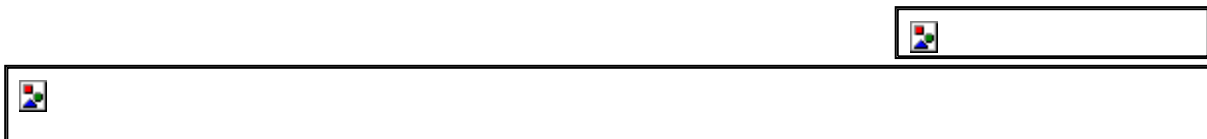
For this configuration step, navigate to the following menu



Connect the COM port of the modem to COM2 interface of the CS141 and connect the power adapter. After connecting, open the CS141 system tab Devices. At COM-Port 2, Select GSM Modem



The GSM modem symbol should appear in the upper bar and show the quality of the signal accordingly:



In addition, the CS141 will display the system tab GSMModem:



Serial COM port connection

To use a serial connected GSM modem, select com as operating mode.

If necessary, adjust the values for baud rate parity and stop bit. Please default values in normally represent the optimal setting and do not need to be changed.



note:
be

Using an IP modem



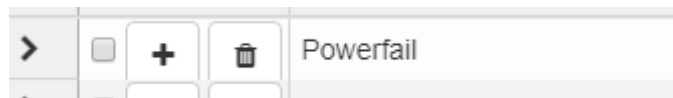
As special feature the CS141 is the support of a connection via LAN. COM2 is not necessary and can be used for other external devices. Under Mode, select IP. Enter the IP address and port number the CS141 will be able to access the IP modem.



Valid IP address can be obtained by local administrators. If used, the CS141 will pass the data to the IP modem.

Job configuration using an SMS

Under UPS event handling, choose the event *Powerfail*.



Press **+** to begin with the job configuration dialog

Add Job to Event Powerfail

Job: Send SMS

Parameter

Text: Powerfail ... warning!

Phone: +494012334567

Timing

Immediately, once

After seconds

After seconds, repeat all seconds

After seconds on Battery

At seconds remaining time

Choose the job Send SMS.

SMS text allows you to enter a small text message.

Under Phone, enter the mobile phone number of the SMS receiver. Ensure there are no spacers at the phone number you entered.

Use Timing to configure how often an SMS should be sent.

Press Save to finish job configuration.

The example dialog screenshot job will be triggered in case of a power fail occurs and send an SMS. If several parties need to be informed, define a separate job for each mobile number.

When you need an sms if other devices are triggered

Any device that is listed with a system event can be used to trigger an sms job. In this example, a buzzer will be used to trigger an sms.

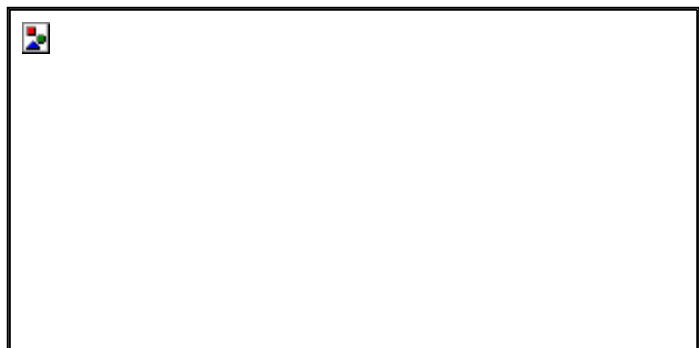


At the event *RELAY ON*, click **+**

As Job, choose SMS, enter the text message and a valid phone number.

As a consequence, the event chain will be shown as followed:

Because there is a power fail, the buzzer is on and the relay is on. Because the Relay is on, the SMS will be sent with a custom text and logged accordingly



Note:

These event chains are very capable: In theory, it is possible to set up very complex event chains, where a job triggers the next event, etc. – you can use inputs and outputs to communicate all over the IT without the need of a network: -High/LowI or -ON/OFFI can trigger many things and produce complex notification alerts.

But be careful when using long event chains: They may brake if a single device is not available or configured accordingly.

CON_AUX4 and CON_R_AUX4

There is more than one method to communicate with parent and child systems: The external devices CON_AUX4 and CON_R_AUX4 provide input as well as outputs to get information as well controlling third-party devices:

To start configuration, define COM3 as AUX port. Type will be used to toggle between CON_AUX4 and CON_R_AUX4.

Configuration

Once the AUX service has been started, the general operability is displayed accordingly in the upper bar. Please wait until the service is ready to use before accessing the configuration menu - it will appear automatically as a sub menu at Devices.

Depending on whether a CON_AUX4 or CON_R_AUX4 has been connected, the configuration screen will differ:

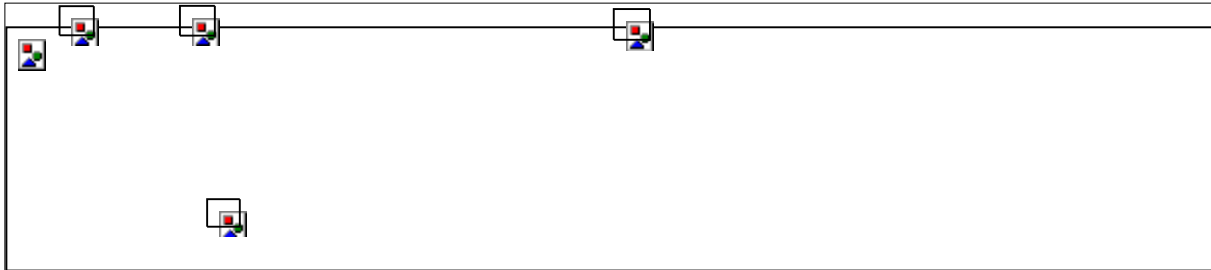


Figure 1: Configuration menu – CON_AUX4

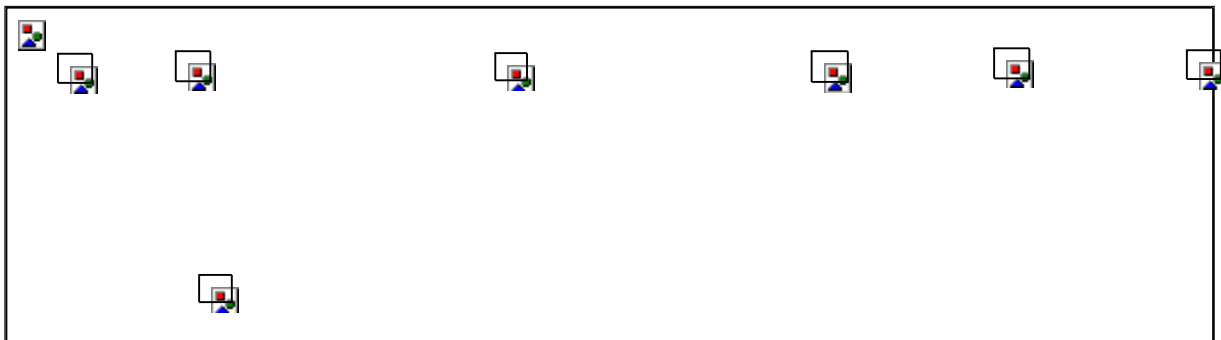


Figure 2: Configuration menu – CON_R_AUX4 Port

1: Port

Current port number

2 Name

Since the cable of the target device can be up to 60 meters, define a name or location. The field Name is freely editable.

3 Output

The ports can be configured as an output to switch potential-free contacts. This function is only available at CON_R_AUX4.

5 NC normally closed

Determine if the input / output normally contains an open or closed contact. Among other things, this function defines the alarm behavior

Switch on cs141 Powerup

The port is automatically switched on if the CS141 is starts or after reboot.

7 Power up delay

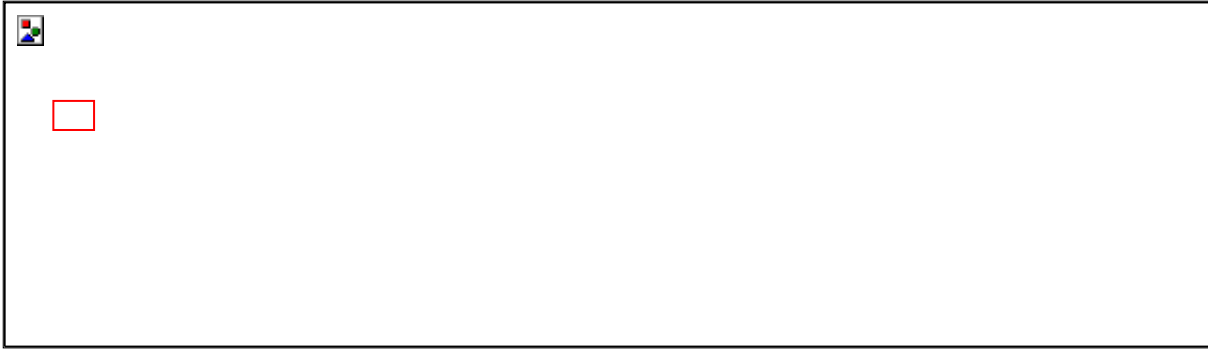
During CS141 boots, the port will be turned on after predefined seconds. This allows a time-delayed startup or switching through potential-free contacts during a restart.

8 Apply / Cancel

Apply will save the configuration and restart the service – a reboot is not necessary. Cancel will abort configuration dialog without saving data.

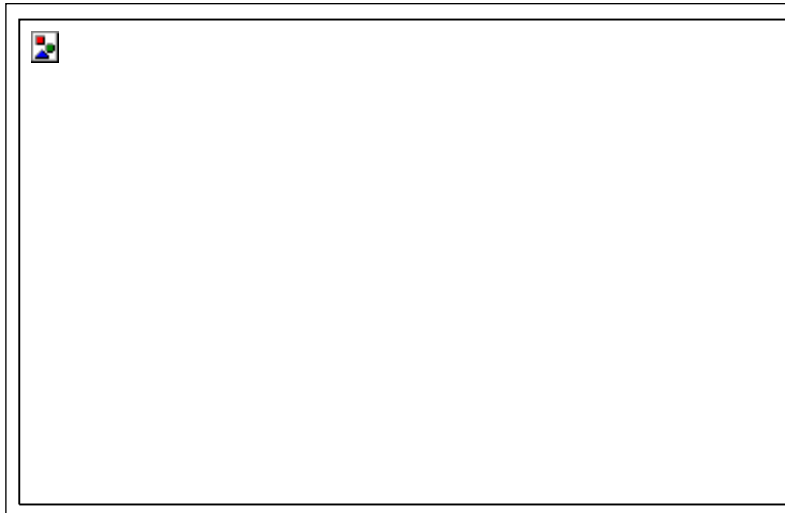
Define jobs to an AUX-Port

Under devices, navigate to AUX Event configuration menu:



Click + to start the configuration dialog.

Possible jobs and timing configuration is similar to UPS event configuration



This example will trigger a job in case of AUX Port 1 is set to high. (on)

Trigger AUX Ports to high/low (on/off):

The AUX ports can be triggered as a job:



As an example, open Event Powerfail at UPS event handling. Select job AUX. Choose the port number that should change a state in case of a power fail occurs. Under Command, select the state the AUX port should be switched to.

Note:

The port state to be switched to is completely independent to the actual switching state. If the port is set to high/on and you switch the port to high, it will be switched accordingly again. Timing configuration is similar to other jobs

Switch an output

With CON_R_AUX 4, it is possible to switch a potential-free relay contact on activation:

Manually switched



→ Manual switching on / off of a port

Each channel defined as output can be manually switched by pressing the Switch on button at AUX monitor.

AUX status monitor

For monitoring, CS141 provides an AUX Status Monitor. To open the AUX Status Monitor, select AUX Monitor from the top-level menu:

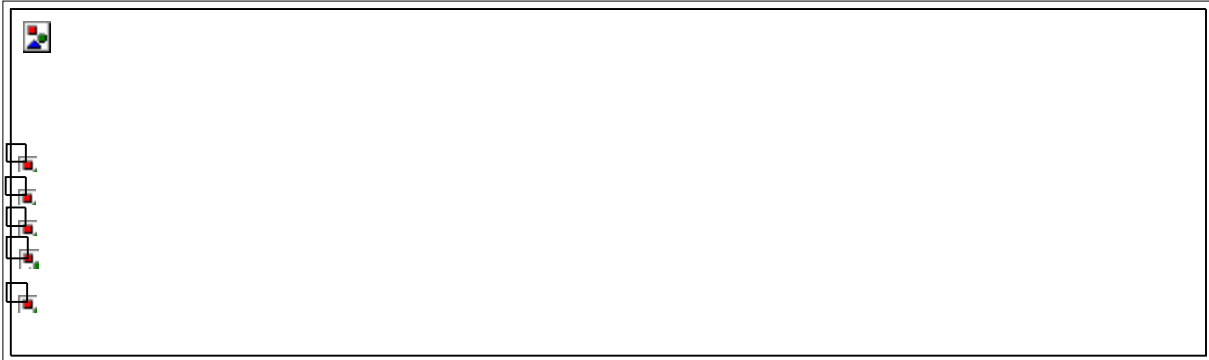


Figure: CON_R_AUX 4 AUX Monitor: Port 1 is inverted, port 2 is output and port 3/4 is default

1: Port

Port number shows the current port.

2: Usage

Usage shows whether the used port is configured as input or output.

3: Inverted

Inverted provides information about the behavior of how the connected device should be interpreted.

There are two valid states:

Inverted: No

The connected contact must normally be closed.

Inverted: Yes

The contact is normally considered "open". This function can thus be used to invert the alarm behavior.

4: State

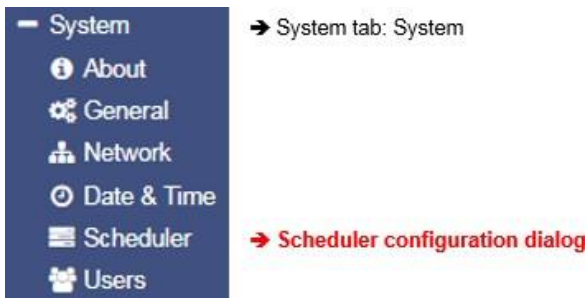
State displays the current switching state. Please note this state will change according to the LEDs at CON_AUX4 and CON_R_AUX4. Due to the fact web technology is used, there is a time delay based on refreshing time of the browser.

5: Switch on /off

If a port is defined as output, this button will toggle the current state of the output.

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 behavior

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

Timing	
Start	08.03.2018 10:52
Repeat	One Time ▼
Triggers	At 10:52 on 3/8/18 one time

Note:

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

Webserver Settings

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.

- Disable http web console
- Current http – port
- Use HTTPS for browser
- Select current HTTPS – Ports
- Time until a refresh will be forced
- Welcome screen after login
- Toggle between simple and advanced screen
- Enable/disable Tooltips
- Time until CS141 automatic logs out
- Save settings / Cancel configuration

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.

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

HTTPs Port

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

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.

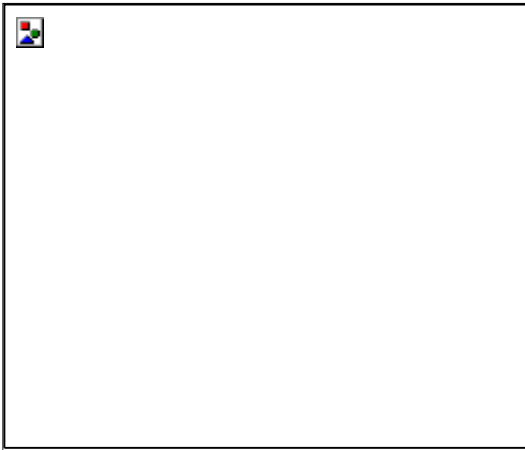
HTTP Refresh time

The CS141 will automatically return an updated page showing, among other things, the status of UPS systems or other available status monitors.

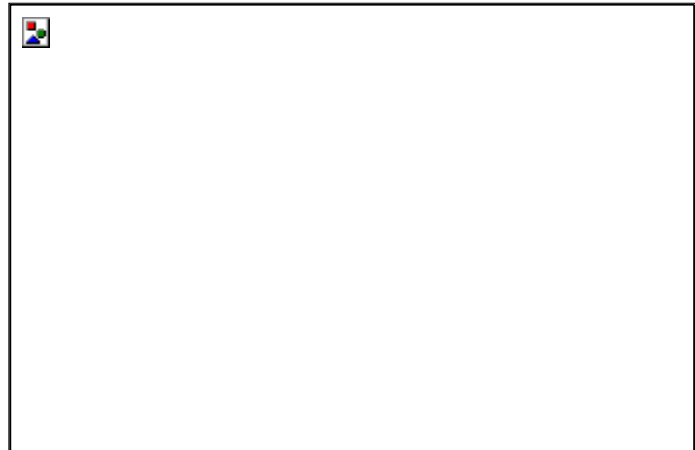
This value defines how often an automatic page refresh is performed. By default, the CS141 updates these displays every 10 seconds.

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 .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)

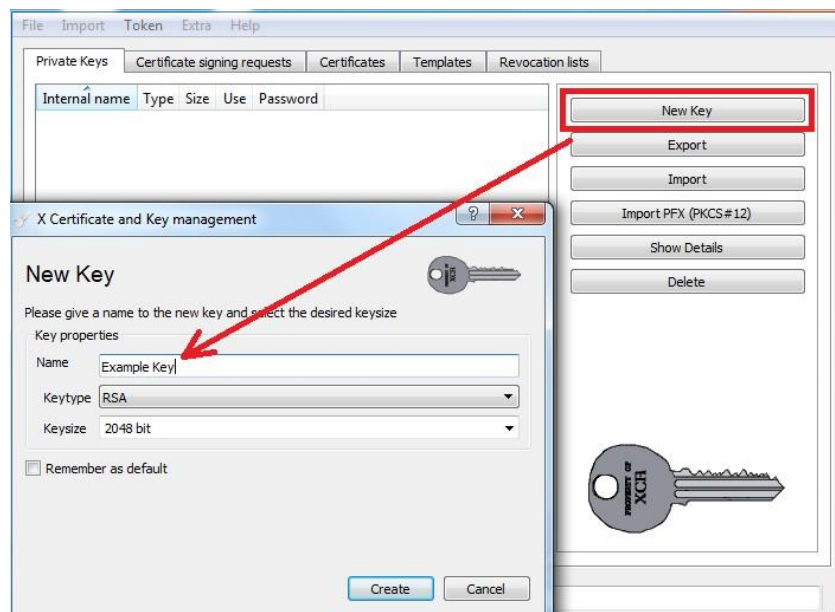
After installation, click on File and create a new database. It is not necessary to enter a password to protect the database

WOLZ	15.02.2018 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.

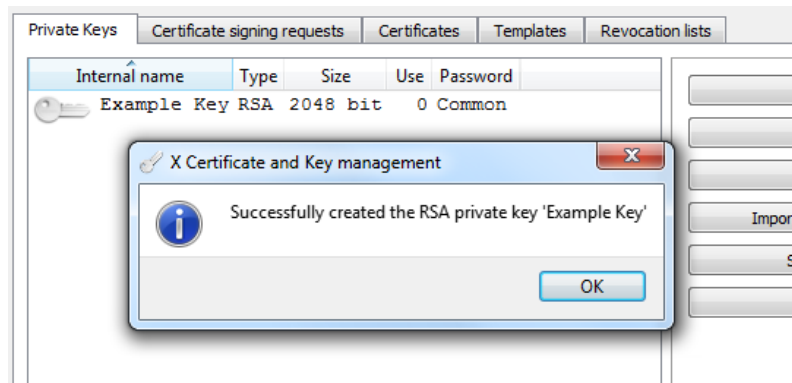
Step 3: Create and export a private key

Go to private Keys and press the button New Key:

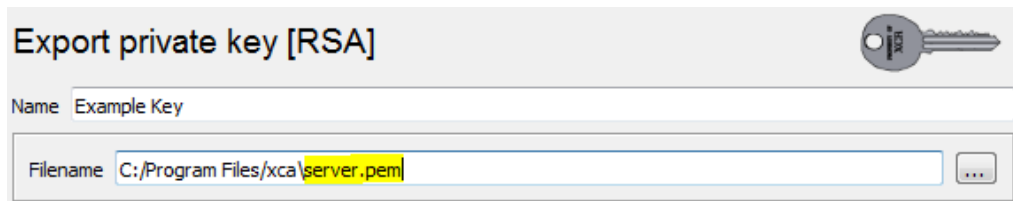


Click Create to complete this process. The key will be provided in the database containing a corresponding message.

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 certificates owner data. Adjust the data according to your company. With Add you hand over these data inputs to the database of the tool.

Extensions

With extended functions, you can set the validity of the certificate:

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"/>

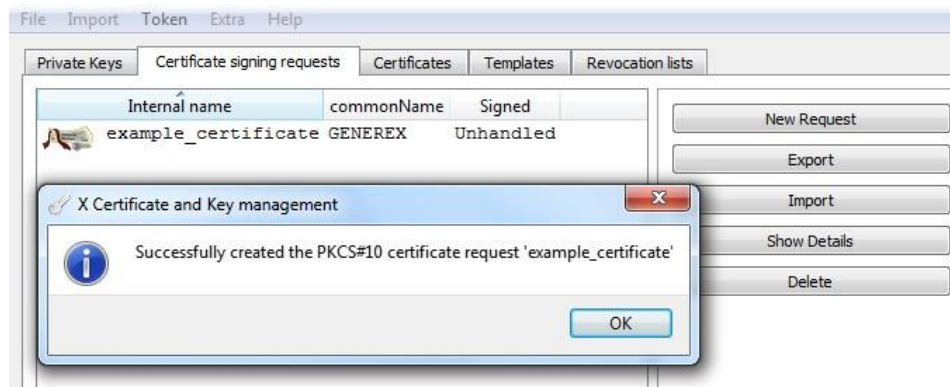
Passen Sie diese Daten an, um die Dauer Customize this data to determine the duration of the certificate. Apply with Complete this process.

Key Usage.

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

X509v3 Key Usage	X509v3 Extended Key Usage
<input checked="" type="checkbox"/> Critical	<input checked="" type="checkbox"/> Critical
<input type="checkbox"/> Digital Signature <input type="checkbox"/> Non Repudiation <input type="checkbox"/> Key Encipherment <input type="checkbox"/> Data Encipherment <input type="checkbox"/> Key Agreement <input type="checkbox"/> Certificate Sign <input type="checkbox"/> CRL Sign	<input type="checkbox"/> TLS Web Server Authentication <input type="checkbox"/> TLS Web Client Authentication <input type="checkbox"/> Code Signing <input type="checkbox"/> E-mail Protection <input type="checkbox"/> Time Stamping <input type="checkbox"/> Microsoft Individual Code Signing <input type="checkbox"/> 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-----
MIIEoDCCA4igAwIBAgIBATANBgqhkiG9w0BAQsFADCBjTElMAkGA1UEBhMCSEgx [...]
hQ9t4jtit2VSTnv4rIrHoT8j5/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  RmkXwyQQgoTJuknaDLAFXFQV4XBPpEC6N5/zvNj1LKYGKik4ibwlyF52CqhPtii
26  DOPUGYKLeDfEAXNK5mKq349qC5C177YYFDEFrAtiZdysh2KgRR0kCg==
27  -----END RSA PRIVATE KEY-----
28
29  -----BEGIN CERTIFICATE-----
30  MIIEoDCCA4igAwIBAgIBATANBgqhkiG9w0BAQsFADCBjTElMAkGA1UEBhMCSEgx
31  CzAJBgNVBAGTakhIMRUwEwYDVQHDxHRU5FUkVYX0R1bW8xEDAoBgNVBAoTB0dF
32  TkVSRVgxZzARBgNVBA5TCkdFTkVSRVgtSVQxEDAoBgNVBAMTB0dFTkVSRVgxITAf
33  BekahkiG9w0BCOEWEN1cHBvcnRAZ2VuZXJleC5kZTAeFw0xODA3MDkxND0zMDBa
```

Save this file without changing the file name, the file extension or file type.

CS141: Inserting the .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>

Upload

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, take a look at the two LEDs in front of the CS141:


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 behavior. 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

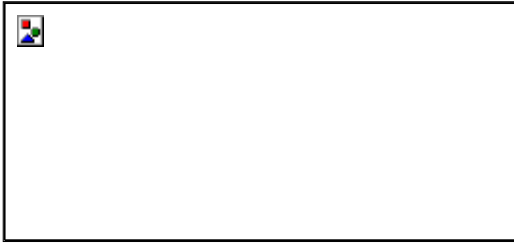
A blue marker indicates that the device was probably configured correctly, but no initial communication has been established.

Sensor:  Disabled

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

Example: Quick diagnosis using LEDs and marker

At the front of the CS141 both, red and green LED's, are on, but they should be off or just the green one flashing slowly. The UPS is definitely recognized ... and seems to work normally.

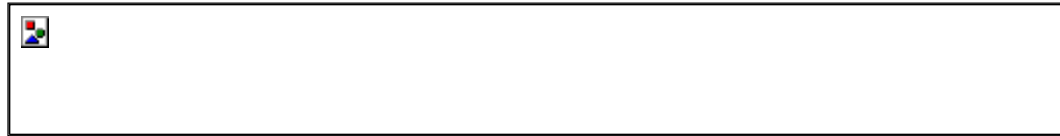


As you can see the red and the green LEDs are lit statically. Since it is a slot card, it is plugged into the UPS and is supplied with the necessary information about it.

The yellow plug is the ethernet cable to connect the CS141 to the local network

In this example scenario, the AUX port is the cause of a communication error:

After logging into the CS141, the top status bar displays the following information about enabled devices:



The UPS is set correctly and has made the communication accordingly. The AUX port, on the other hand, is set to initializing. However, since the AUX port has no device connected to CS141, the yellow marker will change from yellow to blue in time, while the LEDs on the front of the CS141 continue to glow green and red statically.

Due to the fact the UPS indicates a green marker and other devices are set to disabled, the AUX-Port will cause trouble.

What you can do:

Once a CON_AUX4 or CON_R_AUX4 device has been connected to the AUX port of the CS141 and successfully initialized, the marker in the status bar will turn to green and provide feedback with OK. Furthermore, the LED status at CS141 will indicate normal operating mode.

If no AUX device is to be used, you can set the AUX port at COM3 to none in the general configuration menu. In this case, the AUX port will be disabled as well as the AUX marker will be removed from the top status bar.

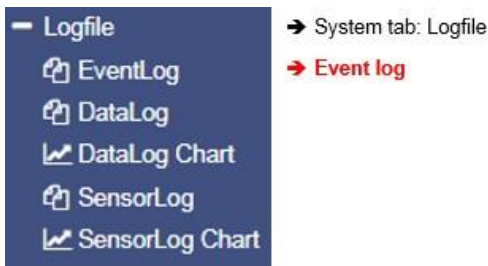
As a consequence, the LED at CS141 will indicate normal operating mode.



Logfiles

Event Log

Since this is not a configuration step, just navigate to the following menu:



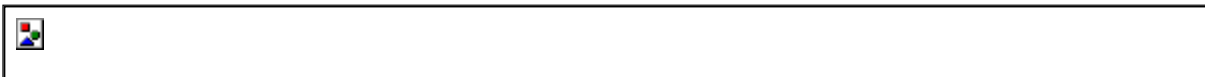
The event log contains all actions concerning the CS141 and the UPS are recorded. The event history will be written by any event containing a log job. The most significant jobs are included by default settings. Administrators may create, edit and delete default settings as well as creating custom log entries.



After reboot the first entry is a message by CS141 with its OEM ID:



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:



Any program that can deal with CSV files can be used to open the event log.



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 startup.

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:



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.

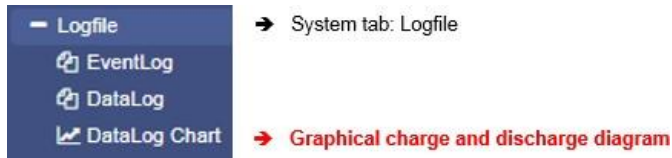
Like the event log, data log can be exported as CSV file as data backup. The data log stores the entries every 3 minutes and keeps the entries 8 weeks as the current data log file. After that the actual data log will be moved to an archive file and a new data log for the current data is opened.

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 Diagram

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:



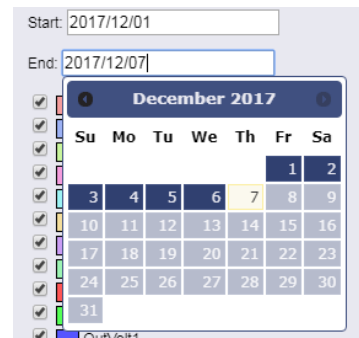
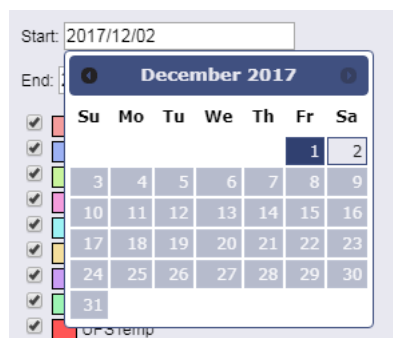
In addition to the current values, the CS141 provides selecting specific values from current databases.

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 of existing time periods that are selectable. Click the date field to bring calendar:

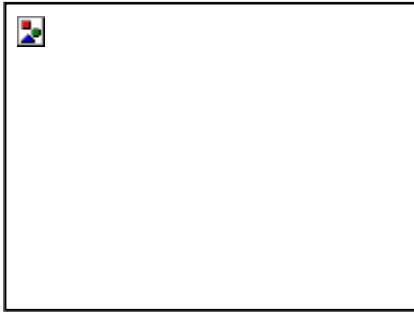
The dates of the corresponding period automatically loaded and displayed main window.



overview
up the
are
inside the

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.



The zoom function allows an enlargement of the timeline up to 2 minutes.

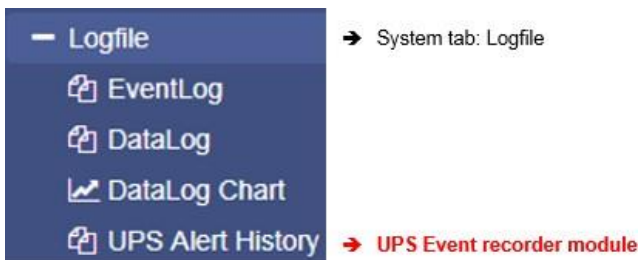
This function resets the zoom back to the original scope.



This function updates the current data shown and refocuses 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.



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



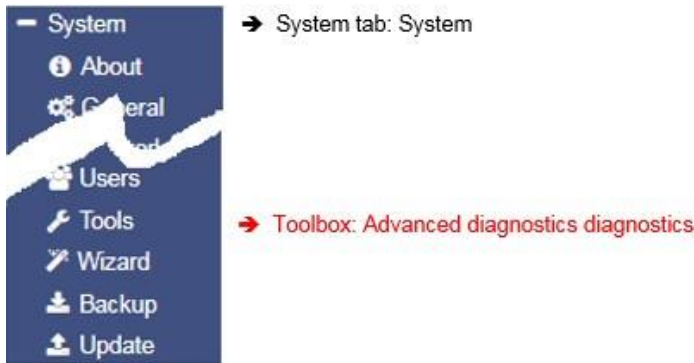
Note:

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.

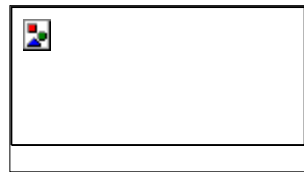
Tools

The GENEREX system tools are a collection of useful utilities to help in case of diagnostic problems. To ensure authorized access only, this menu acquire administrative credentials:

To open the Toolbox, 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 / GSMModem 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 with Trace starts the process. Depending on your browser's configuration an open 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

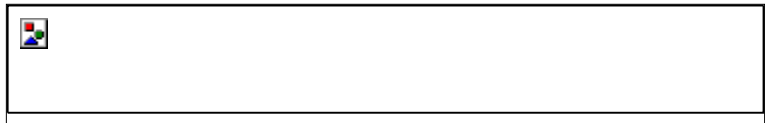
Open the saved text file. Please note the extended text formatting - Ensure to use a text editor mastering extended text formatting. As an example, typical applications would be editors like sublime or the editor write by Microsoft Windows.

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

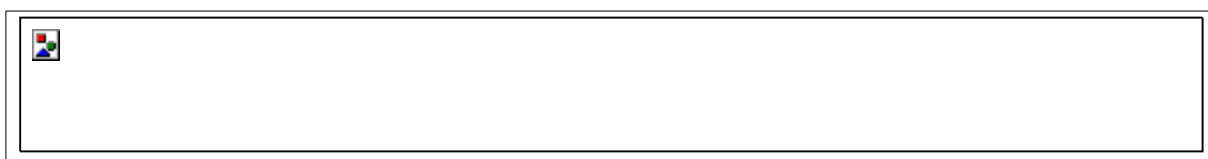
As special feature the CS141 provides an integrated network scanner to examine the LAN for issues and errors. The network scan provides extensive information for evaluation about the network the CS141 is connected to. All data packets are collected in a log file. After network scan, the network log can 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 behavior. 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.

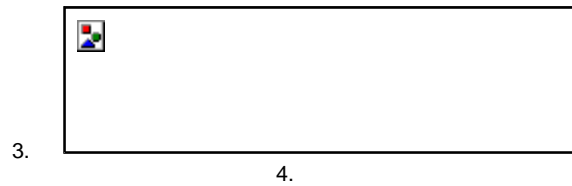


The Tracer logs packet data within the LAN segment in real-time and stores it locally on the CS141. The tracer will quit if there are two conditions:

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 analyzed via diagnostic tools such as Wireshark *:



Downloaded data can be read and analyzed by special diagnostic tools such as Wireshark *:



*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 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.



it
tools.
it is

Networklog

Deletes any network trace data

Eventlog

Deletes all logged data according to events

Datalog

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 center 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

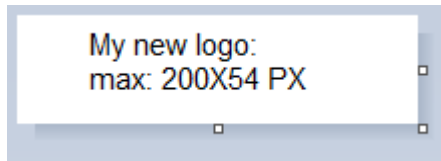
Type `http://10.10.10.10/update` in the browser and run the flash update after entering the current administrator password. On the second pass, the default password `cs141-snmp` is active

Change the 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



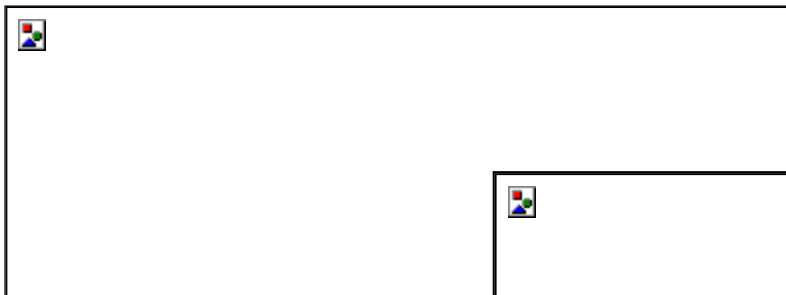
3. Edit the logo as your wish
4. When finished, save the logo with filename logo.gif – otherwise it will not work.
5. Open CS141 Toolbox:

Under Tools, you will find the configuration screen:

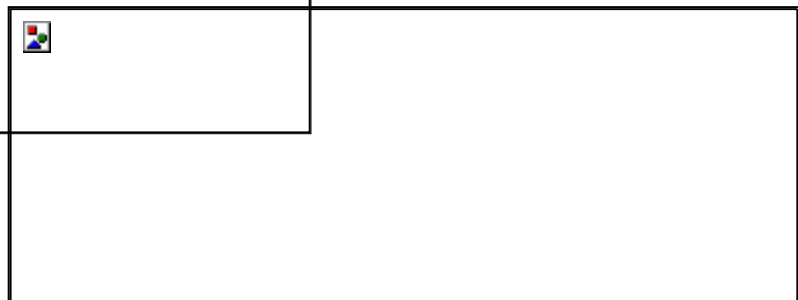


Use drag and drop to insert the new logo or click to select from a list.

6. Press Upload to insert the new logo.



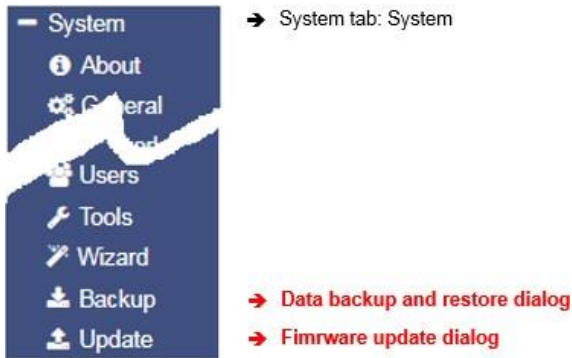
Before...



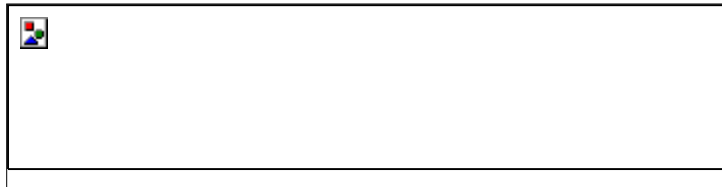
... and after

Data backup and firmware update

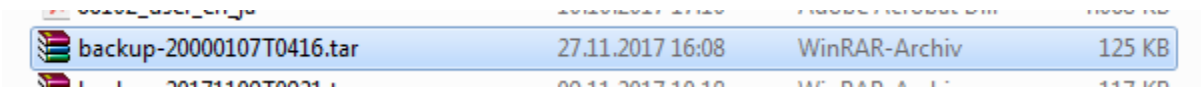
For this configuration step, navigate to the following menus



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.

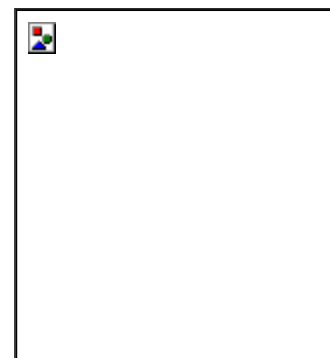


This data backup can be run with any CS141 using a similar or higher OEM firmware version. Please note changing the file name will cause the backup file to lose its validity. As a consequence, CS141 will show an error message.

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.

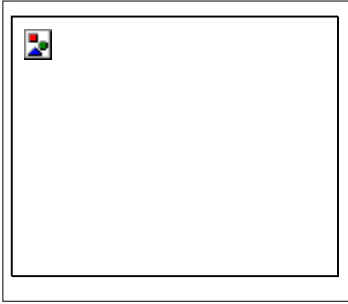
Restoring network data

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 behavior 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.

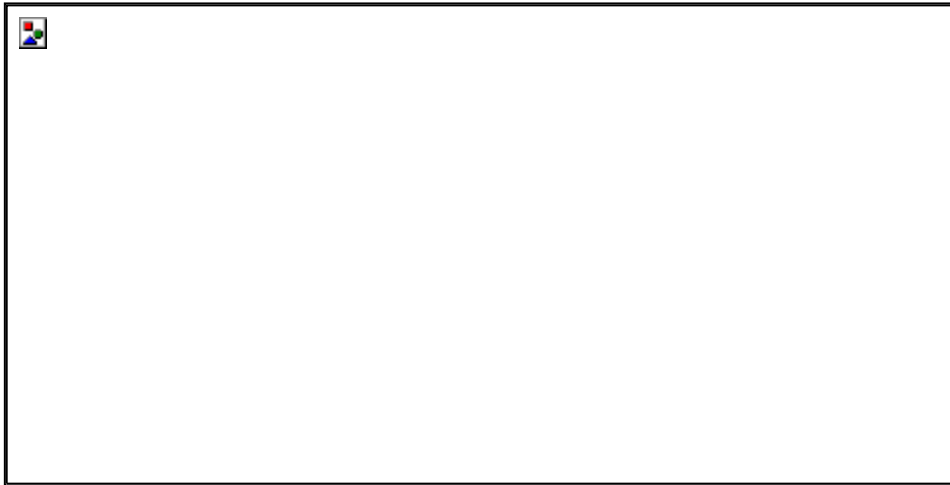
By default, the OEM ID 12 / GENEREX is preinstalled on delivery.

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:

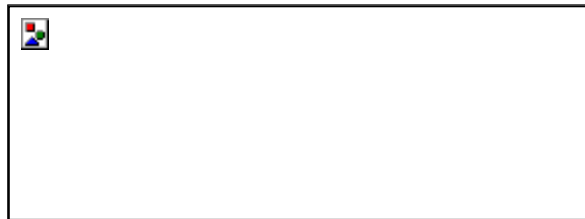
- GENEREX - ID 12
- OEM version of the manufacturer of your UPS

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

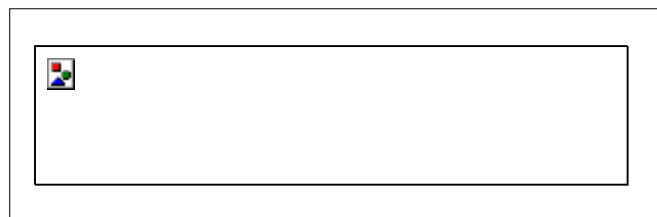
You can see the current firmware by the logo in the top left corner:



Depending on the manufacturer, you will find the corresponding logo.

Checking firmware version

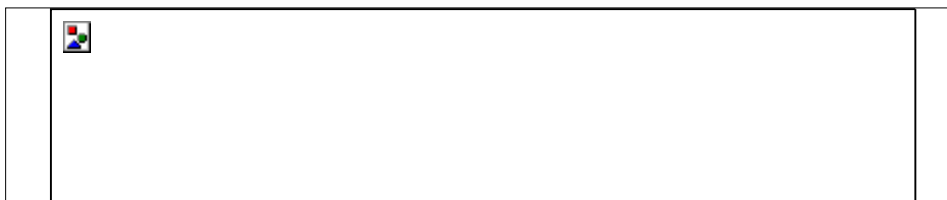
In the general system information, you will find this entry



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 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' behavior. 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 behavior 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 behavior 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. Please note, this function is a rescue system, the CS141 will reset all settings except the IP address. All configurations are deleted and the device is set to startup 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 center 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!.

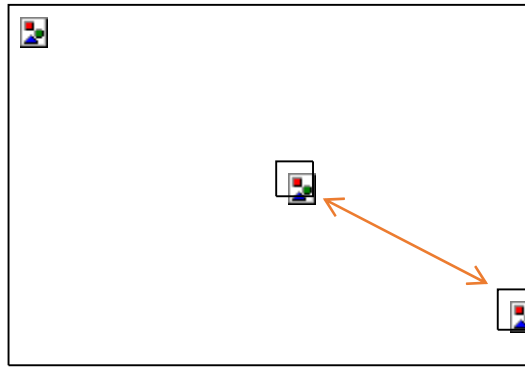
This version can be activated by setting the following jumper:



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.

Rescue mode on CS141 mini

Due to its compact design, the CS141 Mini has no jumper that can be set. To activate the rescue mode, set both DIP switches to the ON position:

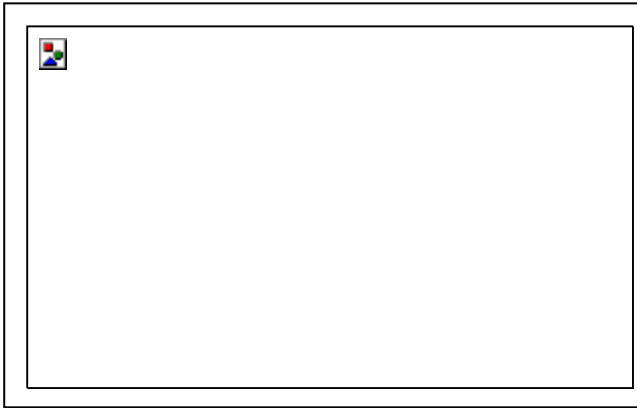


Run a firmware update and reset the adapter to factory settings. Please note you are not flashing the operating system of the rescue mode:

You will not see the result until you return to normal operating mode and restart the CS141.

PART II - BACS[®] Battery Analysys & Care System

Users manual

What is BACS®?

BACS® - the "Battery Analysis & Care System" - is the most advanced system on the market to manage stationary battery systems. It is a standalone battery monitoring and management system that can be easily integrated into your network infrastructure. With its intelligent web-technology configurable management technology, it cyclically checks the internal resistance, the temperature and the voltage of each individual battery. In addition, it can readjust the charge voltage of each battery and manage environmental readings (temperature, humidity, hydrogen gas content) as well as loads (UPS, inverters, and other devices). The accumulators are thus always kept in the optimal working range. The ongoing monitoring and limiting of the individual charging voltages of each block ensures the estimated maximum battery availability at any time. After installation, BACS® will significantly find a way to increase and secure the performance at all lead-based, closed and sealed

batteries (AGM, GEL, wet batteries, maintenance-free), nickel cadmium and lithium-based cells.

The BACS system was designed for the individual monitoring and to control each single accumulator inside a battery system. BACS regulates the voltage symmetry during charging and provides individual scalable notification options in case of an asymmetric discharge or similar faults:

- It stops the overcharging of individual batteries and warns in case of pending deep discharges.

The problem that weak accumulators may be damaged by unrecognized overcharging or deep discharging is now observed. Notifications in time allow counter measures before an incident occurs.

- The BACS unique system architecture provides active charge / Discharge control for each accumulator

The patented GENEREX BACS EQUALIZATION distributes evenly

the voltage from the charger / UPS is evenly distributed to all accumulators. As a result, a homogeneous voltage is present across all batteries inside the system. Due to this fact, average lifetime and capacity will be increased significantly.

- Sulfation problems are no longer a creeping threat

BACS EQUALIZATION minimizes the problems of sulfation through a constant trickle charge. In case the sulfation is in progress, BACS can detect this as a problem and ask for further assistance by the operator in good time. As a result, countermeasures like controlled discharging or removal of sulfation can be initiated before the accumulator is severely damaged.

What is the advantage of BACS?

Manual monitoring and maintenance are expensive and complex - With BACS, they are no longer necessary. Since the individual data of the accumulators are now available it is possible to maintain each accumulator individually at any time. If the BACS EQUALIZATION repair procedure does not work on one or more accumulators or irreparable defects are detected on a battery, it is possible to change one cell before the defect has a negative effect on the neighboring cells. The precautionary replacement of all batteries inside the system is therefore no longer necessary. By doing so, BACS ensures more than the availability of the battery system:

Its unique technology provides by the constant monitoring and managing of the batteries, the optimum capacity to ensure emergency operating time.

The data and experiences gained through our patented BACS since 2004 on the realistic behavior of battery systems shows how to double the average service life time of rechargeable batteries that are installed into UPS systems and why the UPS usage differs from a single rechargeable battery usage: The estimated life of a single accumulator is determined by the manufacturer - As an example, he states an estimated life time for a special battery model as 10 years. Since inside large UPS systems very many accumulators are interconnected, the single battery behavior will change according to the number of batteries in use:

The number of weak batteries with negative influences to neighbored ones will increase statistically.

Due to this fact, the overall behavior of all batteries leads into a significantly reduced time for active usage inside a UPS - the so-called service life. Astonishingly, this active service time is usually half of the stated battery life time. With BACS, it is possible to extend the life of any battery running inside a UPS to the manufacturer's stated battery lifetime. BACS offers more than best economical possibilities in single battery monitoring - it provides reliable data for extensive analysis and long-term studies.

BACS systems are available in 4 versions (2V, 4V, 6V and 12V) for a range of uses ranging from small 7 Ah batteries to large stationary lead-acid batteries up to 6000 Ah.

In addition, the BACS system has a state-of-the-art alarm threshold system that is continuously under development. BACS collects readings inside specially designed internal database for battery histories:

The device determines and stores individual battery values like internal resistance, temperature and voltage. With the optional BACS CSxxx current sensor, the scope of measured data will be enhanced with additional charge and discharge current measurements, valuable data for comprehensive long-term analysis. Collected sensor data will be sent directly via its own bus system to the central control unit, the BACS® WEBMANAGER.

All incoming information will be stored and processed:

After processing sensor data, the BACS® WEBMANAGER provides an intuitive well-structured interface to present the measurements. In companion to the data presentation and configurable notifications, additional alarm LED and alarm buzzer ensures that the UPS will be save during operation. Finally, the BACS® WEBMANAGER has an intuitive user interface via web browser, which also contains a clearly arranged configuration menu.

EQUALIZATION: How to maintain individual charging / discharging of accumulators

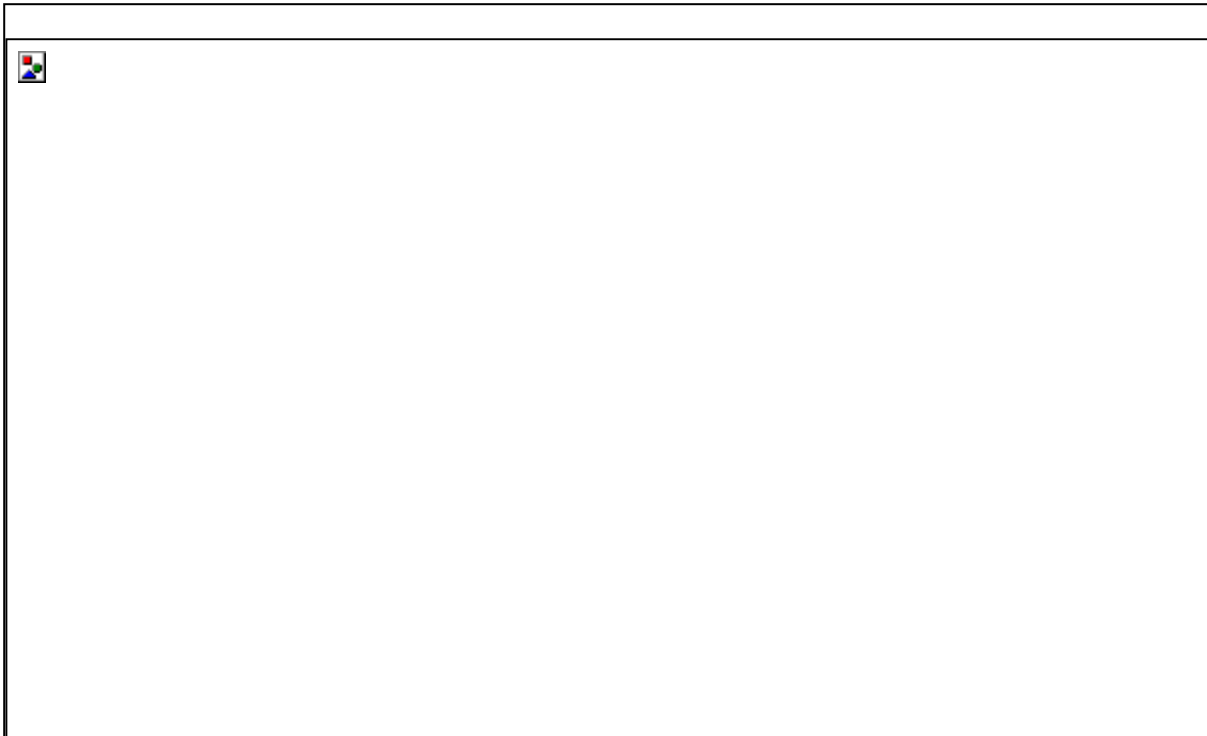
As a continuously running background process, the BACS® WEBMANAGER calculates a so-called "charging voltage point" - A value each block should have at the instantaneous total voltage. If an accumulator deviates from this average charging voltage, the BACS WEBMANAGER sends a command to the corresponding BACS module that manages the accumulator. The BACS Module will manage to adjust the charging voltage to the calculated charging voltage point.

As mentioned, many different values are recorded and monitored - even the average activity and the number of charging and discharging cycles. If an event occurs during the monitoring which can be classified as serious or dangerous, the BACS WEBMANAGER can manage alarm notifications provided by direct network alarms as well as email, SMS, SNMP or RCCMD. If available, even an optional Modem can be used for customizable SMS alarming. In case of being operated inside a Modbus system, BACS Webmanager will also serve the MODBUS format via one of the serial interfaces and / or via MODBUS over IP

Additional Features

Thanks to optimized memory routines, the BACS WEBMANAGER is capable to record battery data for up to 3 years by using reliable 32MB internal flash memory. All stored data can be downloaded and archived:

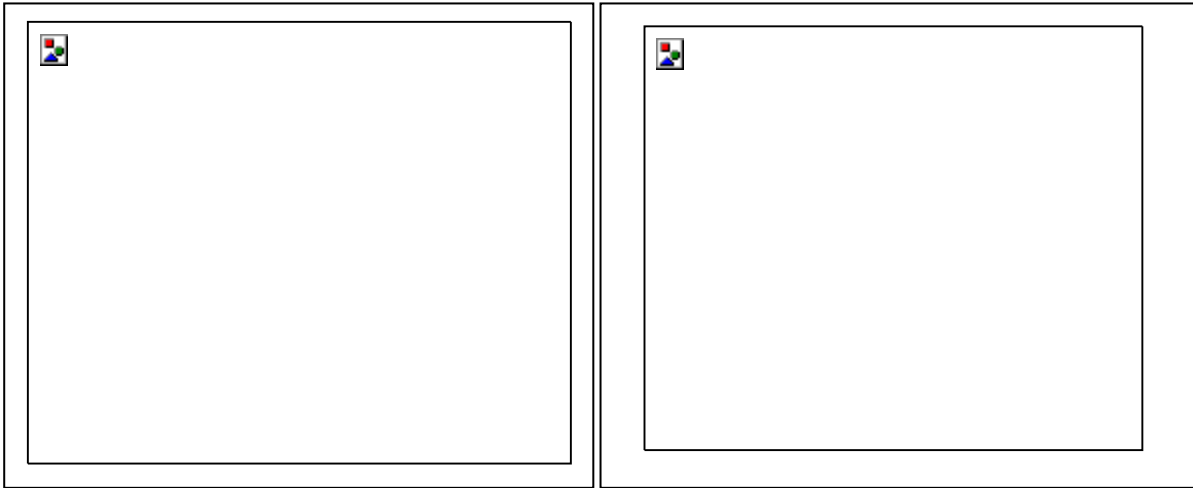
Alarms from the batteries or other devices connected to the UPS are logged with a timestamp - in order to ensure data and time allocation, the BACS® WEBMANAGER provides automatic time synchronization with free definable time servers as well as second clock inside the BACS BUS CONVERTER.



Picture: typical setup of a BACS

CS141 and BACS

To upgrade the CS141 into a full BACS system, you need the BACS Bus Converter



In case of your project involves larger installations with more than 50 batteries, we recommend the BACS Splitting Box. The Splitting Box allows to divide the installation into individual strings. A further application is the possibility to realize well-structured clear cabling of the BACS modules.

These devices can be ordered separately, among others, via the GENEREX web shop as well as comfortably worldwide via a certified GENEREX partner.

What is the difference between the BACS Webmanager Budget and the CS141 in companion with a BACS Bus Converter?

First of all: both devices fulfill exactly the same functions.

The difference is that the combination of a CS141 BACS and a Bus Converter is modularly composed of two separate devices, while the BACS Webmanager Budget consists of a complete device: While the single device has a more compact design, the modular solution allows to separate the BACS BUS Converter: Take it along while the CS141 will continue in place its monitoring and managing works.

In both cases, it is possible to connect a computer in order to use the BACS tools.

BACS WEBMANAGER Kits



The BACS WEBMANAGER BUDGET is the central control unit for all batteries connected to the BACS bus. The BACS WEBMANAGER KIT contains a BACS WEBMANAGER, a BACS CONVERTER, all necessary cables as well as power supply.

The BACS WEBMANAGER can be configured via a special BACS data cable as well as via a network interface.

Each BACS WEBMANAGER system includes a full-featured SNMP / Web UPS Manager on COM 1 and offers a variety of sensors for access control, temperature and humidity as well as versatile environmental sensors. Even customer-specific sensors can be used via the optional SENSORMANAGER.

Upgrade your CS141 into a full-featured BACS Webmanager:

For this configuration step, navigate to the following menu:



General COM port settings

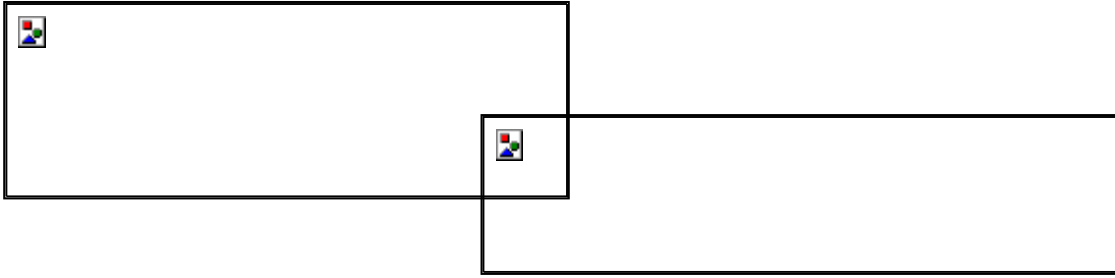
Under Devices, click on the menu Setup. This will allow to activate the BACS capability and is necessary for further configuration. Without this setting, the BACS menu is not accessible.

Note:

An easy method to figure out if your CS141 model can be used as a BACS Webmanager.

As soon as your CS141 provides an AUX-Port, your CS141 will support a BACS BUS Converter in general. You just need to look at the ports. If you cannot access the device physically, you can take a look at the General COM Port settings. If your CS141 model does not provide an AUX port, COM3 is not available.

BACS can be operated a completely standalone system - independently of your previous UPS configuration. Even it is useful for BACS to know the current UPS state, it is not required. If you just want to monitor the batteries in standalone mode, you can disable the UPS functionality by setting COM 1 from UPS to none.



If you want to monitor the alarm behavior of the UPS and already manage your network, let COM 1 be on UPS - BACS will be operated like an additional feature. These basic settings are mandatory to be set for both - slot card versions and the external versions of the CS141.

Note:

The UPS with their connected batteries generally stay together!

You can not monitor a UPS and connect the BACS-monitored batteries to another UPS. The power source is not important for CS141 as long as the correct UPS is queried:

it is crucial that the charge / discharge detection is configured to UPS as well as the associated batteries.

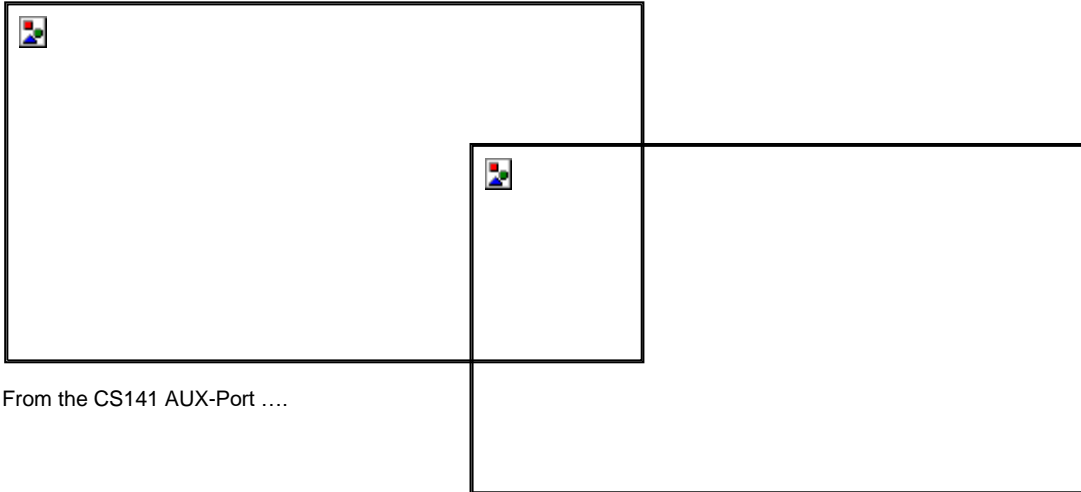
Since the BACS Webmanager provides different possibilities to query a UPS it is possibly it is up to you to select the best power source as well as to configure the correct target. You can not use one BACS Webmanager for different Battery sites.

When saving, necessary services are started. After finishing this process, a new BACS menus will be accessible:



Hardware precondition: Connecting the BACS Bus Converter to the CS141

Even the menus are accessible, the BACS Bus Converter needs to be connected to CS141 before starting configuration. Use the AUX-Port of the CS141 and the COM 3 Port of the BACS Bus converter to establish a connection between the devices:



From the CS141 AUX-Port

... to the COM 3 port of the BACS-Bus Converter

Since the cables are coded, a wiring failure should not be possible. During installing, ensure neither to jam the connectors nor to use brute force - the contacts may be damaged.

Once communication has been established between the devices, a relay will click inside the BACS Bus Converter and a red LED will light up on top, followed by a buzzer.

Press Mute to temporarily switch off the alarm. You can not switch off the alarm permanently, after some time it will be automatically fall back to active state.

In addition, the upper status bar inside the CS141 web interface will show a "Communication Lost" issue - This status is normal in this configuration state since there are no modules installed or something is configured.



Using the BACS capabilities of a CS141 SC slot card



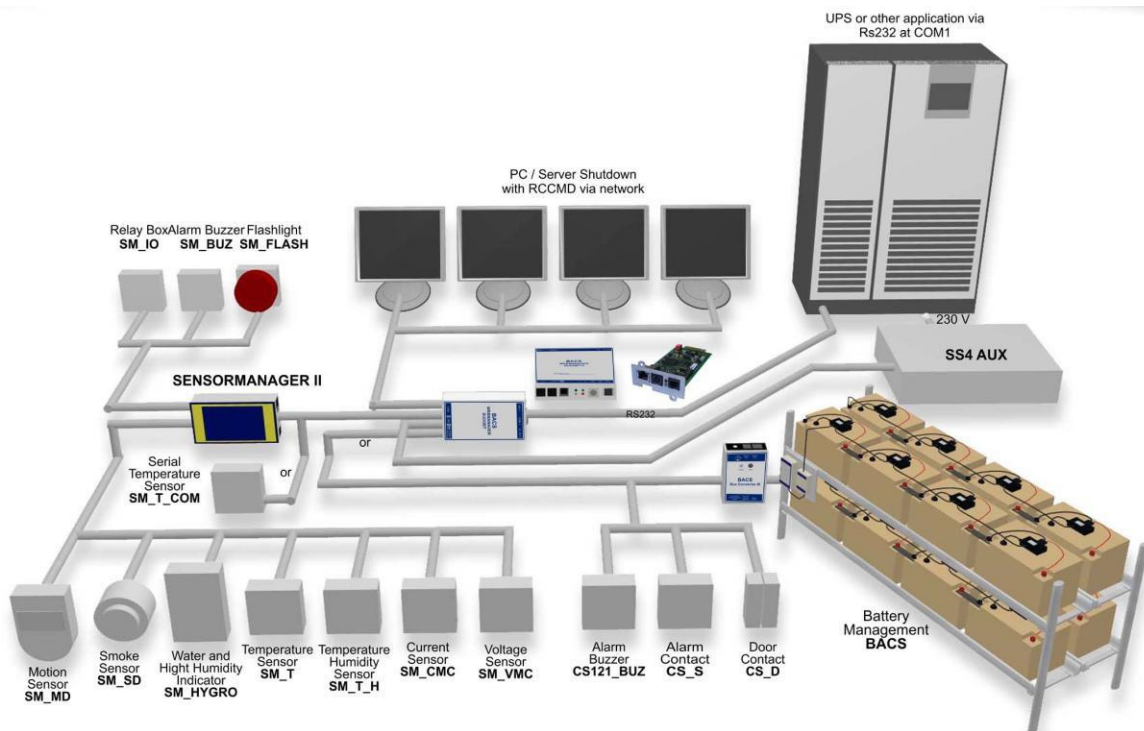
Connect the AUX-Port of the CS141 SC with COM 3 of the BACS Bus Converter. At CS141 SC, configure the COM-Ports as described. You do not need to restart the CS141 SC.

Note

If the menu does not appear even though you have switched COM3 to BACS, your web browser may use old files stored at an internal browser cache. Modern web browsers use caching technologies to increase the display speed of web-based content: As an example they store alleged static contents for further usage or may pre-cache complete webside contents before displaying them. In this case, it may lead into presentation failures like missing links or even wrong menus if they has been moved by a firmware update.

Please clear the browser cache and press CTRL + F5 to refresh the display and the menu should appear.

Now let us talk about your brand-new, worldwide unique BACS® - the "Battery Analysis & Care System":



This graphic illustrates a full-featured and fully equipped BACS system. Due to the fact BACS is scalable it can grow with your UPS and even easily ported to a new system – if you decide to purchase a new UPS, you can take all the modules from your old BACS – equipped UPS and install it on your new batteries.

After a quick reconfiguration, BACS will automatically start to learn how your batteries work and what they really need for best performance.

How to read and use the BACS manual

Since BACS is a complete stand-alone system, it can operate on it's own, too. You do not need to read the complete CS141 manual, but it will help you to understand how the menu structure works and all about the icons used. If you want to use a UPS and the RCCMD environment, we recommend to start with the CS141 configuration guide and than moving on to your BACS installation.

If you have worked with the CS141 before

If you are familiar with the menus of the CS141 and know how to add a job as well as how to set up mails, mailtraps, etc. ... well, you do not really need the first part of the manual and will be able to understand and configure the BACS system quickly:

- Events
- Jobs
- Mail / Mailtraps
- Discharge detection

The BACS web interface is designed to provide a fast way to configure it intuitively. And like the CS141 part inside this manual – this manual is written to explain. ...

DANGER:

Please keep in mind that batteries, battery racks and current-carrying equipment may be under high voltage - there is a real danger to life when touching high-voltage components! Working with batteries need your total attentions and following the rules. „Short cuts“ are just a method to figure out if you can survive your mortal incident...



In the case of non-expert or appropriate handling, there is an acute danger to life when handling modern battery systems. There are also numerous legal requirements that personnel must meet during installation, operation and maintenance of electrical systems. For this reason, we ask you to read the following safety instructions carefully and consult in case of doubt experts or at least specially trained professionals:

Fundamentals when working on battery systems

Make sure that the environmental conditions for installing BACS is met.

An incorrect handling can lead to personal and material damage! GENEREX is not responsible or liable for any direct or indirect damage caused by incorrect handling.

Risk of explosion and fire

Avoid short circuits! Caution: Metal parts of a battery are always charged, so never put metal objects or metal tools on the battery!

Elektrolyte are extremely corrosive liquids.

Leaking electrolytes in a battery are harmful to the health of the eyes and the skin. Heat fumes can be easily inhaled and cause severe damage to the lungs.

Ask trained and qualified personnel only

Working with batteries installed inside high voltage areas are dangerous and always need special attention. Especially installation and maintenance procedures should only be performed by these trained personnel or by personnel authorized by the battery manufacturer - the personnel must be familiar with the handling of batteries as well as necessary precautionary measurements.

Non-expert staff can run into situations with acute danger to their life due to high voltage!

Follow the legal regulations carefully

- ZVEI publication "Instructions for the Safe Handling of Electrolyte for Lead-acid Accumulators."
- ZVEI publication "Safety Data Sheet on Accumulator Acid (Diluted Sulfuric Acid)." VDE 0510 Part 2: 2001-12, in accordance with EN 50272-2:2001: "Safety Requirements for Secondary Batteries and Battery Installations - Part 2: Stationary Batteries".
- IEEE Standard 450-2002: "Recommended Practice for Maintenance, Testing and Replacement of Vented Lead Acid Batteries for Stationary Application."
- IEEE Standard 1375-1998: "Guide for Protection of Stationary Battery Systems"

Note

The legal requirements may vary depending on country and state. Furthermore, the current legal requirements may be adapted or even changed completely by local regimes over time to include new technologies and scientific findings or as a direct reaction of incidents dealing with a special technology:

If in doubt, contact the local authorities before determining any safety precautions for the installation or operation of a system.

Obey the safety rules when handling electrical conductors and components

- Ensure that all electrical loads and power supplies (chargers) are switched off as well as required fuses and switches are secured before starting maintenance work. This must be done by qualified or specially trained /certified staff.
- Remove all wristwatches, rings, chains, and other metal objects before and working on batteries until work is done and you enter secure marked area.
- Use insulated tools that are certified for the work.
- Wear insulated rubber gloves as well as rubber shoes
- Never place tools or metallic components on the batteries.
- Make sure that the batteries are not accidentally grounded. If the system is grounded, release the connection: Touching grounded batteries may lead to an electric shock accident.
- Check the correct polarity before wiring a battery. Wrong polarity will lead into damaging including the possibility fire, explosion, corrosive hot gas

- Stuffed lead acid batteries contain high explosive gas (hydrogen / air mixture). Never smoke and or provoke sparks near the batteries. Avoid electrostatic discharges - wear cotton clothing and, if necessary or required by local law, ground yourself before maintenance work.
- Always wear the appropriate clothing and take care they are suited to statutory safety and protective arrangements.

Avoid areas that are not suited for battery installations

Standard modules shall not be used in case of ...

- outdoor or open space usage as well as non-water protected, enclosed spaces.
- dusty rooms or places with high levels of dust.
- in areas of high concentration of saline as well as oxidizing gases.
- the place is next to open fire, spark zones, heat sources or inside heat extreme zones.
- areas that are known for high temperature fluctuations that cannot be normalized by environmental control systems.
- areas that are known for with high vibration or mechanical movements
- areas that are known for gas concentration or other flammable substances

Note

In some cases, there is a small and fluently defined borderline that decides about a location is appropriate or inappropriate for installing and operating a BACS system. If in doubt, please contact the GENEREX Support Team, we are happy to advise you about the possibilities as well as environmental conditions to be met.

Just write a small mail to our support team: BACS@generex.de.

if you need to install BACS and the area is known to deviate from a standard installation for technical or environmental reasons:

GENEREX offers especially insulated and sealed modules to handle these installation scenarios.

To be noted during installing a BACS

1. *High voltage danger*

Do not open the BACS sensor; Do not attach objects to the battery or to the BACS modules! The BACS modules and cables could be under high voltage!

2. *Magnetic fields*

Keep in mind that every live wire creates a magnetic field around it. The strength of the magnetic field depends on the current: a large If insufficient shielded, a UPS system can generate very high electromagnetic interference (EMI). Therefore, avoid the installation or operation of technical equipment that is susceptible to electromagnetic fields.

Take care for technical staff using a cardiac pacemaker - Magnetic interferences may harm regular functions and even destroy these vital devices!

3. *Trained and BACS qualified technical staff only!*

BACS is installed on batteries that can be under high voltage during installation. As soon as the BACS measuring and connecting cables are connected to the batteries, they may be under high voltage, too. To prevent short circuits, ensure the system is disconnected before performing any maintenance or installation work in companion with BACS cables. Since a certain order must be adhered to, special trained and certified BACS technicians are required..

Note

Need a BACS training for your technical staff? Speak to us – our BACS training team will be pleased to advise you the best way to get a BACS certification training.

4. *Replace damaged batteries before installing BACS for the first time*

Damaged are batteries often not determinable by a mere visual inspection. A damage can be found during a measuring the internal resistance - the higher the internal resistance, the worse the current condition of the battery.

The problem:

If a battery is highly damaged that the internal resistance exceeds maximum possible highness, the charge / discharge current will no longer be able to pass through the battery. Because the charge/discharge current must find a way it would seek the path of least resistance: The BACS module. As a consequence, unplanned heat will be generated that can damage or destroy the BACS module over time. Due to this fact, do not continue and use batteries in a battery bank that are already detected externally as defective or if the BACS module measures a very high internal resistance!!

5. *Never mix different BACS module versions as well as BACS types of measurement cables.*

BACS modules differ technically within the revisions. The according measuring cables were specially adapted to the corresponding revision of the BACS module. If you mix different BACS modules, it will not work in general. In addition, an unfortunate combination of different modules may lead into irreversible damages to the cables and BACS modules.

Before starting to install cables and modules, ensure that you do not have mixed your stock for installation:

Sort modules and measuring cables beforehand.

Rework, maintenance and care

Regularly check the measured values of the modules and the temperature development of the batteries

- ... during installation and during the first charge / discharge cycle

During its initialization, BACS performs its own diagnostic measurements to find hidden defects that may occur within combination of used and new batteries. Until BACS has fully captured the batteries in order to provide a reliably report defective batteries:

As soon as unusual temperature fluctuations and unusual increases are noticed, the according battery should be replaced immediately.

- ... up to 12 hours after complete discharge until depleted

Followed by a regular discharge from a power outage, the most common "thermal runaways" occur - a massive increase in temperature on damaged batteries that can become so hot that leads into acute fire hazard. Statistically there is the highest risk of battery failure with damage to the electrolyte within the battery can be found significantly inside a time window of 0 to 12 hours after discharge. If the temperature of the battery continues to increase after a discharge instead of staying the same or slowly decreasing, the charging cycle should be stopped immediately and the affected battery replaced.

On passing this time window, a battery pack can be regarded as stable - it can be reintegrated into the normal chain of alarm states.

The warnings and issues BACS provides should be taken seriously - Respond in good time!

BACS was designed and developed to extend the service life of accumulators in multiples. BACS will not only inform you with cyclically status messages that something was wrong after deviated behavior is detected at the monitored systems. Thanks to the unique control technology combined with efficient early warning and alarm functions, BACS will inform you before an incident can harm your system:

You can react before a real incident occurs that may damage your entire system.

Please keep in mind that the patented technologies behind BACS will cushion battery or charge control errors over a period of time from the first warning, but will not be able to permanently compensate for real defects.

Additional components required to assemble a BACS:*BACS Battery C-Module*

The control of the charging and discharging processes of each accumulator during the EQUALIZATION procedure as well as the measurement of the actual battery state are carried out by so-called BACS® battery C-modules. These modules are mounted on each individual accumulator. The according C module to be used in your battery system depends on the battery used and must be dimensioned accordingly.

The key figures of the available C modules are documented in the current BACS data sheets

BACS measuring cable

This cable is used to measure the voltage and impedance of the connected battery. It is a 4-pin cable with 2 fuses in the positive cable (red) to protect the BACS system against high currents or short circuits. When installing, the connection order is important: This cable must be firmly connected to the battery poles BEFORE connecting the BACS modules:

With wrong handling, the integrated fuse is sensitive and may trigger.

BACS bus cable

The patented BACS bus allows high-speed communication between all BACS modules within a battery system. This cable is specially designed for use with BACS only. It is shielded and calibrated against EMI to ensure communication even in harsh environments.

Before you start ...

like the CS141, when using BACS there are many things that should be considered before starting an installation - there are many individual installation options to be used. One of the most important thoughts coming with this context, is whether and how to extend the technical possibilities of existing systems. Eine der größten Probleme ist hierbei, dass unter Umständen völlig unterschiedliche Systeme miteinander koordiniert werden müssen, um gemeinsam auf dasselbe Ziel hinzuarbeiten.

One of the biggest problems is that different systems may have to be coordinated with each other in order to work together. In fact, the BACS system makes it easy to be added:

It does not care whose batteries should be managed unless different UPSs are combined to charge the batteries - this should be avoided, because a BACS Web Manager will expect one UPS for the connected batteries is responsible. Otherwise the measurements are strange and not suitable analyses. However, as long as this framework condition is met, it would be a quite useful information if the UPS could communicate its own operating state, but it is not needed.

Due to this fact, a BACS system can be fitted seamlessly into almost any infrastructure in order to manage the batteries *The*

Central task of BACS inside an existing infrastructure

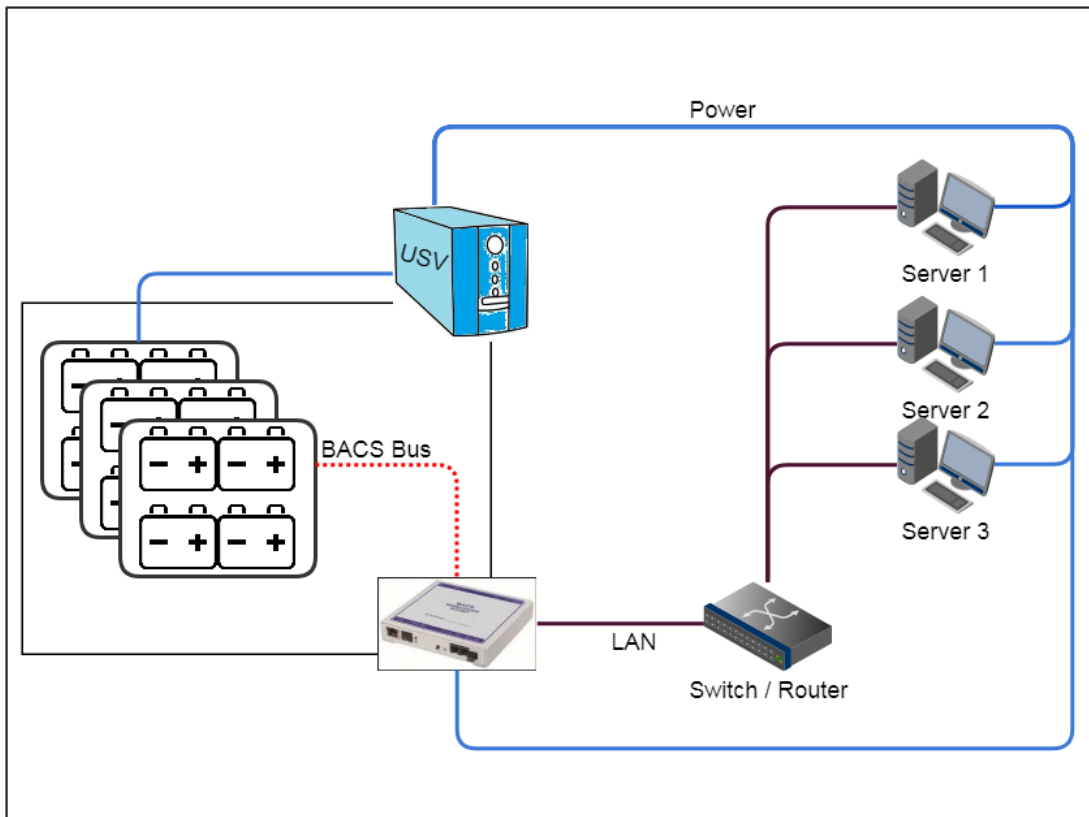
In addition to the monitoring of the battery conditions, the central task is care and active regulation of the batteries during the complete charging / discharging cycle. Thereby BACS takes into account the needs of each individual battery in relation to the overall system in order to ensure improved lifetime as well as maximum performance if an emergency situation occurs.

For the operation of BACS, it is not important to know UPS that will charge the batteries or which discharge circuit will be used - as a standalone system, BACS can detect the basic system states with its own sensors inside each BACS module:

- charge status
- discharge
- trickle charging status

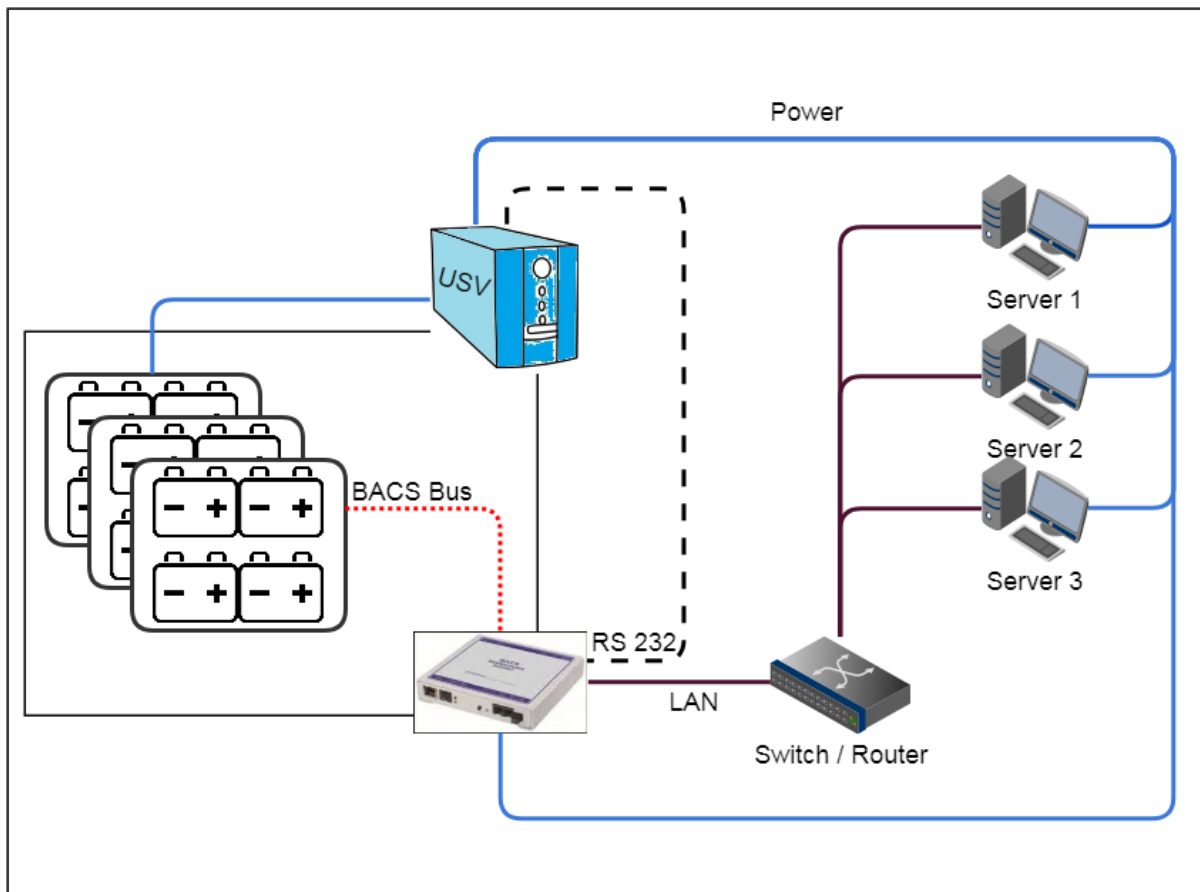
The following installation examples may give you an insight overview about installation possibilities:

Installation example 1: BACS as a standalone system



BACS is not able to get system states from the UPS and is limited to the core task of monitoring connected batteries and regulating charging cycles. The sensors of the BACS modules, which are individually connected to each battery, can detect charging / discharging cycles and provide the necessary data for the control to the BACS. If individual batteries with deviations become noticeable, the BACS Web Manager can automatically inform about this battery condition before a dangerous incident occurs. The disadvantage is that the general UPS functions and system status are not available:

BACS can detect that the batteries are discharging but fails to inform about the reason, why this happens.

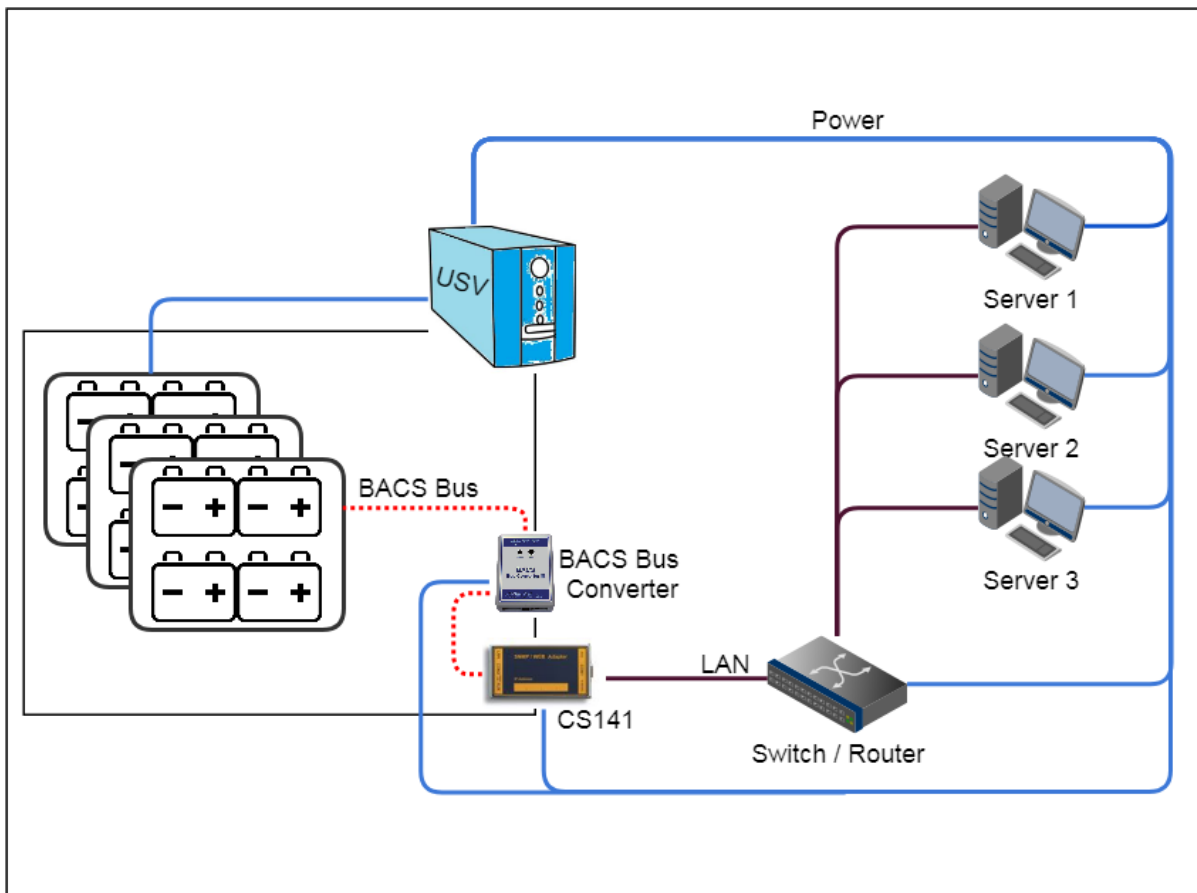
Installation example 2 – the complete solution: BACS is connected to the UPS via RS232

The BACS Webmanager budget is connected to the UPS via the RS232 interface. The BACS modules are supervised by the BACS Webmanager budget. With this solution all options of BACS and the CS141 are available:

- Extended UPS management
- Freely configurable emergency behavior
- Connection of external sensors
- Emergency server shutdown management
- External Input / Output management

While the UPS monitoring is fully featured, the BACS Webmanager can handle complex jobs according to system events to protect the entire IT infrastructure, the integrated BACS system protects the batteries from dangerous charging currents to ensure a reliable and solid emergency power supply.

The BACS Webmanager budget is an all-in-one solution for your entire network.

Installation example 3: A modular solution that grows with your IT infrastructure

The modular BACS solution provides more than just installable in case of realigning by installing a new UPS controlled emergency power solution. The modular version can be installed as a UPS manager, and then grows with the tasks even to a fully featured BACS system that always fits to your UPS. As the modular installation example shows, a BACS bus converter is set between the BACS modules and the CS141 and activate the according COM Port inside the CS141. The CS141 will start the BACS capability and provide all menus of a full-fledged BACS System.

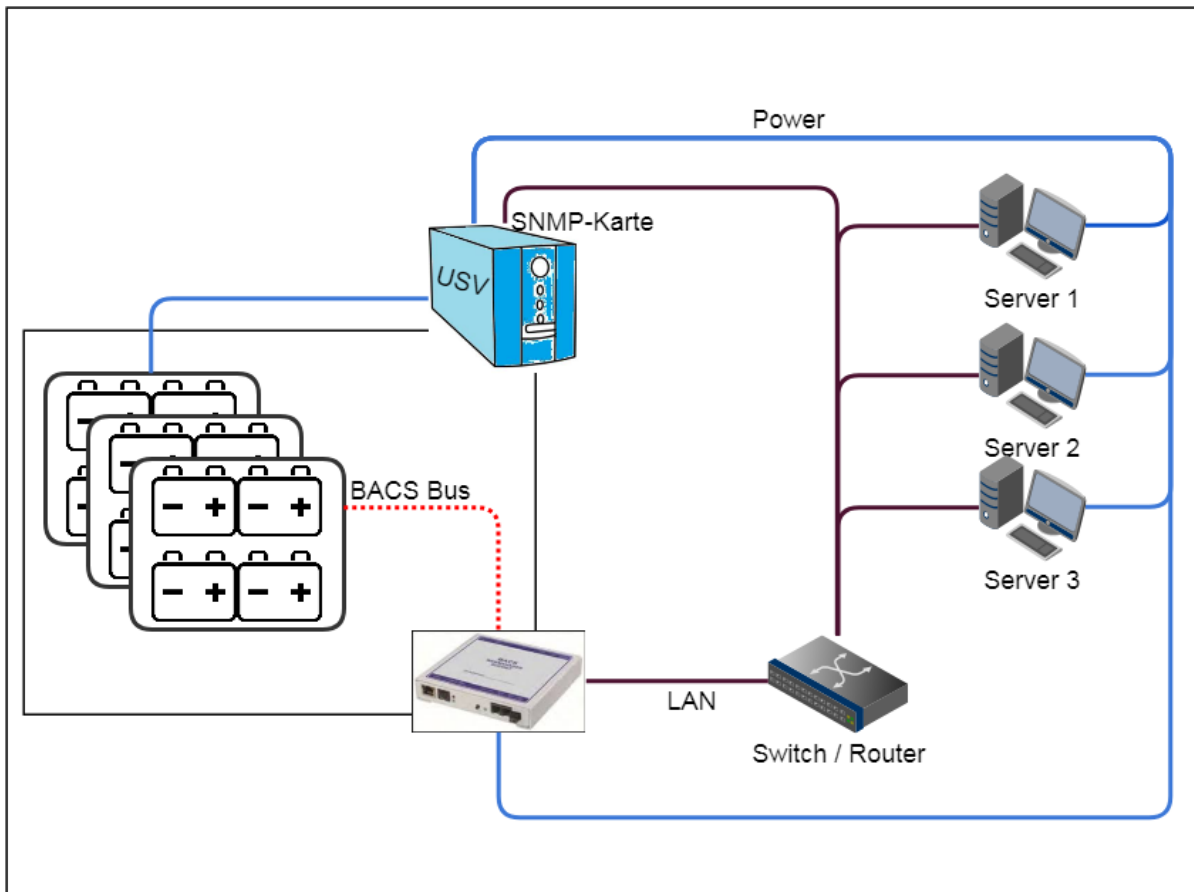
The BACS Bus Converter is needed to establish a communication between CS141 and BACS modules. The peculiarity here is that you can "reuse" already purchased parts, which minimizes the acquisition costs for a full-fledged BACS system.

The existing UPS configuration with the alarm behavior will be enhanced by battery monitoring and management capabilities.

It is up to you to decide ...

If you prefer the the CS141 as a slot card or as an external box - once the CS141 provides the AUX interface, it can be upgraded to a BACS system.

With BACS, you can plan your emergency power solution and adapt it to future trends as required.

Installation example 4: The LAN SNMP solution – if you need UPS information without a direct connection

If you have read the CS141 manual, you will notice this feature at the latest at this point:

Unfortunately, some UPS models are not compatible with the CS141. Causes are, for example, that the interfaces do not exist or are otherwise occupied, existing slots of the UPS have a different design or simply the manufacturer wants to use their own system cards. If your UPS uses its own SNMP card or a similar solution, you can use the UPS settings in the BACS Web Manager to query the signals via SNMP and manage all UPS functions based on this data - each CS141-based model provides this feature.

Since BACS can use this UPS information as "Discharge Detection", this data is not only interesting for general monitoring, but also a reliable means to detect the current UPS state:

All you need to do is:

- Open UPS configuration dialog
- Select RFC 1628 smart interface as UPS model
- Enter IP address of the target SNMP card
- Enter SNMP v1 / 2 / 3 credentials
- Configure an according SNMP user at the target card.

The SNMP card will be queried by the CS141 / BACS Webmanager budget and presented at the UPS monitoring screen.

Note

Yes, this feature can be used with the predecessor CS121 or an existing CS141 that is already installed but does not provide an AUX port, too – if the BACS Webmanager cannot be fitted directly to the UPS, you may use this powerful feature to adapt the BACS Webmanager fitting to your existing UPS solution.

The BACS Bus topology

As well-known from network technology, there are always different ways to connect nodes and devices with each other. You need to choose the best solution for the according task and take care not to connect all nodes in a way to set up a network short circuit...

When connecting BACS modules, there are less things to be obeyed - the wiring of the BACS modules follows two simple rules:

Rule 1: Each ID can only be assigned once

One single Strain:

On delivery, BACS module and BACS sensors use the basic ID 0. When the BACS Web Manager calls the address 0, all modules are addressed. During initialization via BACS Programmer, the individual BACS modules receive a single unique ID. This ID is once inside this BACS installation. The module installation order does not follow the according row of address ID's: After initialization, the BACS Web Manager queries individual addresses and the addressed module will respond accordingly.

Two or more strains:

Inside the strain, the ID's have to be sorted by a specific order. Between different strains, the pool of numbers must be sorted:

Strain 1: Module-ID 1 – 10

Strain 2: Module-ID 11 – 20

Strain 3: Module-ID 21 – 30

Never mix ID module pools between strains!

Rule 2: Obey the maximum cable length

The better the signal, the more stable the entire BACS system will finally work

Rule 3: Obey magnetic interferences

Any live wire produces a magnetic field that affects other metallic objects and conductors. Although the BACS cables are specially shielded against magnetic influences, the installation site can strongly take effect to the quality of the data signal. If you have a lot of interference, test for these magnetic interferences.

Connection examples

In general, BACS does not tell you how to connect all modules each other - a structured wiring method will help you to do maintenance work as well as finding problems during installation. Furthermore, well-structured connection methods will help to improve reliability when operated. Due to this fact, there are some hints you should need to before wiring. Both, the BACS Bus Converter as well as the BACS Webmanager Budget provide two ports for a BACS bus. The possibility to select the appropriate installation type allows different setup scenarios

1. The classic ring topology:

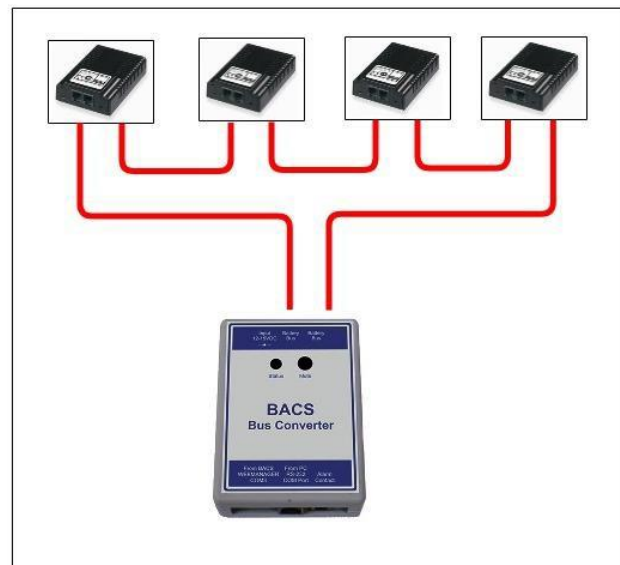
The advantage in the ring topology is a high reliability:

The BACS webmanager can use different cable routes to query a BACS module. The target BACS module can answer the same way. Should a cable fail, there is a second redundant connection that can compensate this for some time. The entire system is still fully operable.

A disadvantage of this design is that the arrangement of the batteries in must meet certain characteristics, since the first and the last battery must be connected to the BACS Web Manager, otherwise the ring can not be closed.

Furthermore, you need to stop at the maximum length to reach the last module in a row from both sides:

If there is a problem with the first cable, the signal needs to be routed through the last module to to the first module. If the maximum length is exceeded, it will not work.



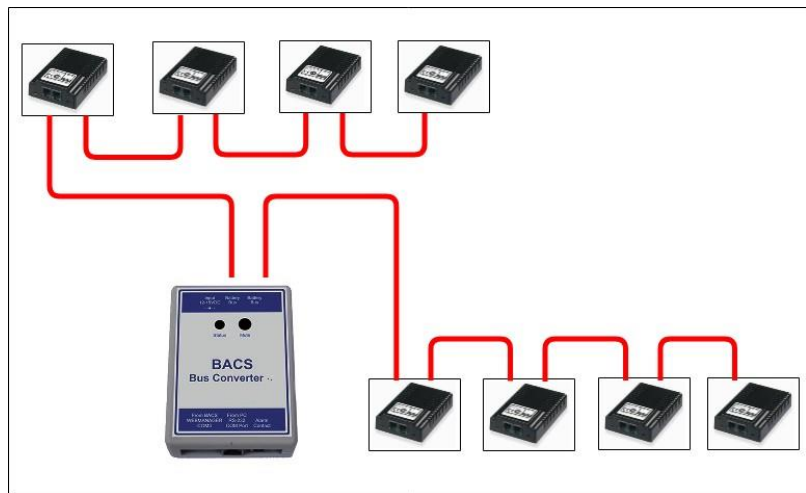
2. The classic star cabling:

With this topology, the bus cabling runs in different directions from a central point. It's advantage is the more flexible design of the wiring and the resulting usability of premises.

Since you are not bound by certain conventions, the batteries can be arranged flexible and adapted to the environment:

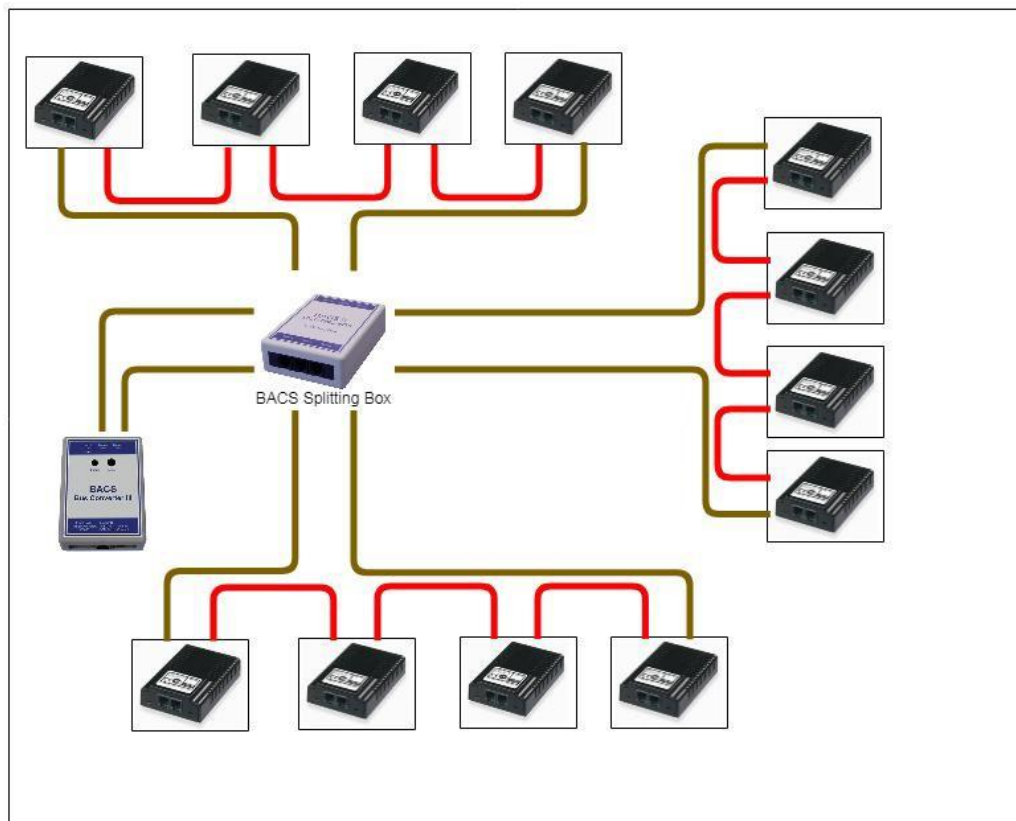
Each single strain may use the maximum available length.

Due to the fact, a star uses a single line connection type, a cable problem will lead into connection lost alerts.



The Splitting Box

A good tool for a well-structured cabling is the separate available BACS splitting box. This box allows splitting a cabling strain into different smaller strains to realize well-structured cabling and to avoid loss of signal due to the longer cable increasing resistance:



Each box provides eight ports and allow several configuration methods. In this example there is a ring-topology with 3 strains – but finally it is up to you how to set up the wiring:

- Ring topology
- Star cabling – connect up to 7 single strains
- Both of them – two ports for a ring two ports for the BACS webmanager, 4 ports for single strain
- Mixed up – Port 1 of the BACS webmanager for starting a ring, one port for the BACS Splitting box, at splitting box 6 Ports for single strains and one port to close the ring from the BACS webmanager, ...

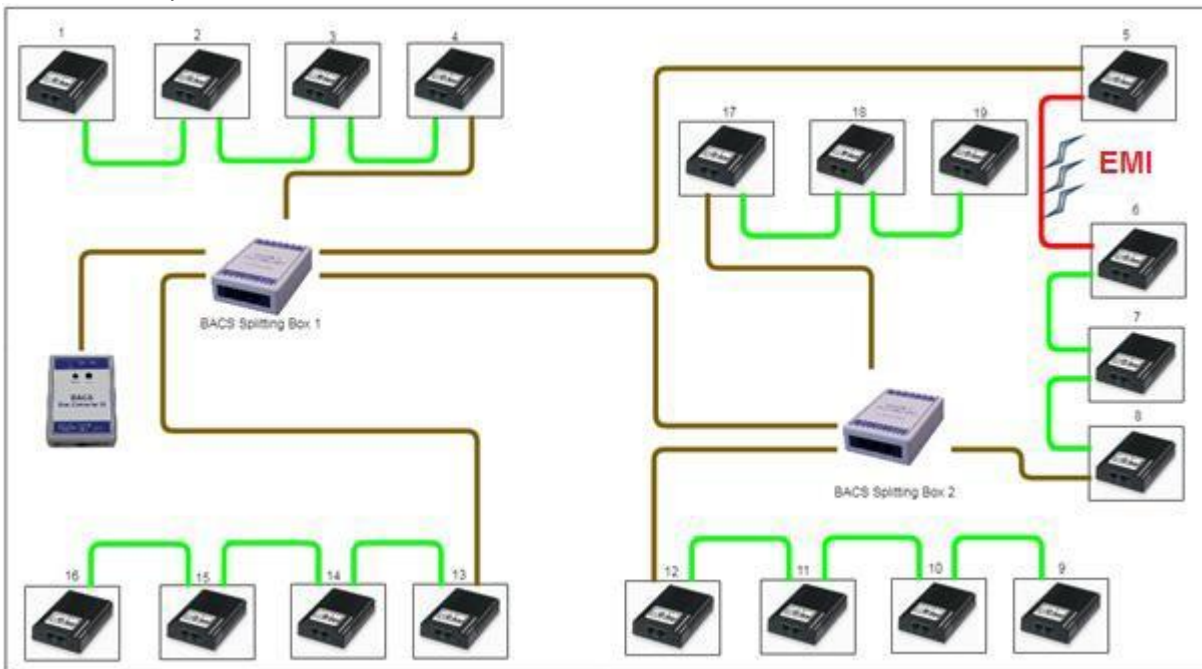
Only the use of one single splitting box will enhance you options to connect BACS bus cables.

How to use more than one BACS Splitting Box

The BACS splitting box is a flexible device. With this device, it is possible to:

- Create partial redundancies
- Create partial ring cabling
- Create ring cabling with different splitting boxes

This flexibility allows technicians to be structured as well as flexible about the locations and technicalities of a BACS installation to maximize reliability:



This installation example shows a combined bus cabling method:

Due to EMI irradiation, the data line between module 5 and 6 is compromised, which leads to sporadic failures. As a consequence, BACS would have problems with modules 6, 7 and 8, as these modules are subsequently connected via a data line. Therefore, modules 5-8 were connected via a second BACS splitting box, creating ring cabling.

Even if EMI interference would compromise the data line between modules 5 and 6, the BACS Web Manager would reliably reach all modules and report no errors.

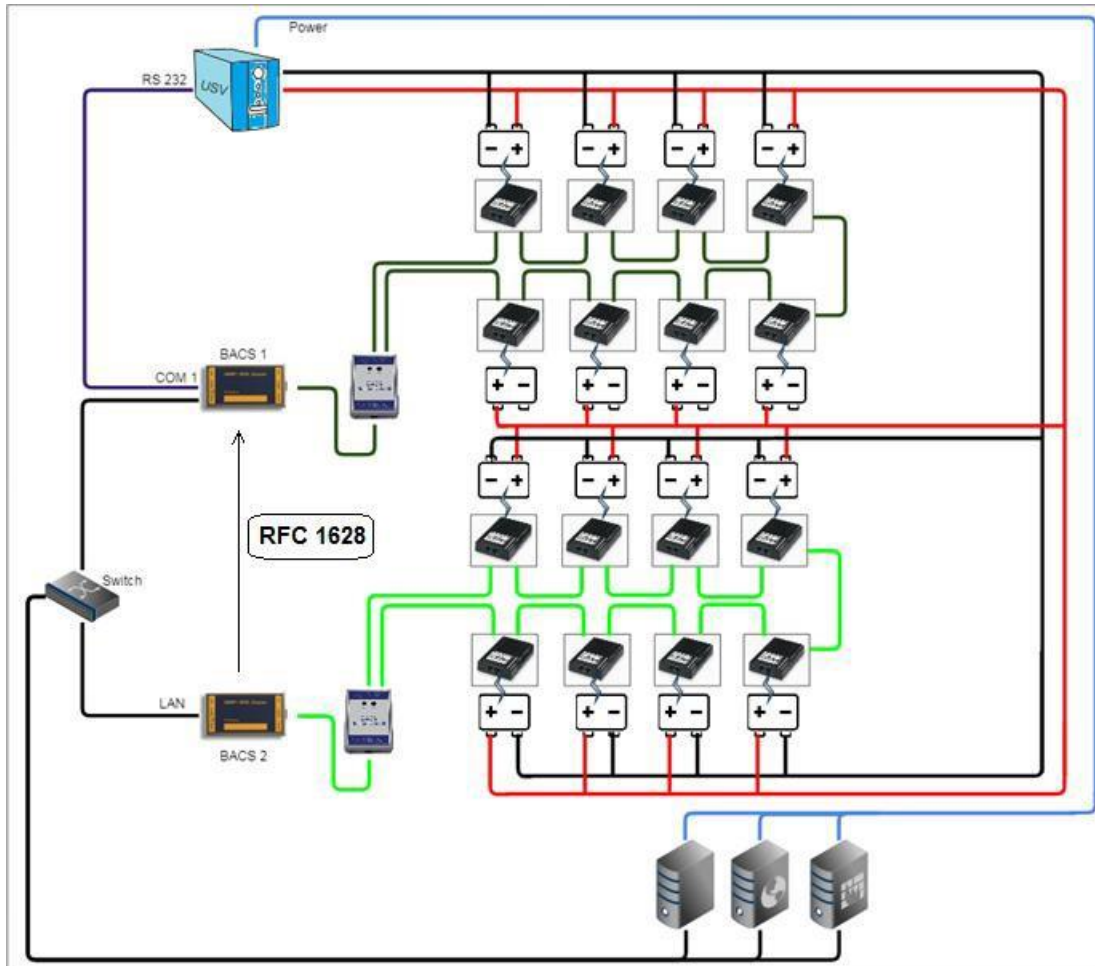
Side effect of this topology:

The BACS Splitting Box 2 is connected directly to Splitting Box 1. If this connection is lost, Splitting Box 2 would automatically try to route the signal via the BACS wiring of the modules 5 - 8. Without EMI it will work properly. Therefore, the modules 9-12 and 17 - 19 are closely connected to the Web Manager via ring cabling, even if it does not seem to be at first view

Note

The BACS Webmanager is the central unit that controls the monitoring and control. If possible, use a ring topology to ensure the best possible connectivity and reliability. The BACS bus is designed to exclude a network short-circuit and ensure any number of redundancies - nevertheless, structured cabling is recommended for maintenance and traceability of an installation.

BACS – Installation with 2 or more BACS Webmanagers



The number of batteries a single BACS installation supports is limited to 500 batteries. If more than 500 batteries are in use, BACS supports the installation and coordination of several BACS webmanagers. In this installation example, two BACS systems were coordinated with each other to jointly manage a large battery field.

Following this installation method, there are two basic things you need to consider:

- 1- Each BACS Bus has to be run with it's own BACS Webmanager

Two BACS web managers are not allowed to address and govern the same BACS modules - they would interfere with each other. If you have more than one BACS Web Manager in use, make sure that each BACS network forms a closed system for itself. The BACS bus itself will not work with an uplink to two different BACS Webmanager.

- 2- All Batteries inside a BACS installation have to be charged / used by the same UPS

As soon as the batteries of different UPS systems are charged and discharged, they are completely independent UPS systems. It would be an invalid battery condition if e.g. A UPS indicates a discharge state, but the monitored battery is actually charging because it belongs to a completely different UPS with it's own circuit.

In this example one UPS loads all batteries. To unleash the full regulation power of BACS, BACS 1 is connected to the UPS via RS232 cable while BACS 2 receives UPS data from BACS 1 by LAN via the RFC 1628 smart UPS interface. By doing so, a numerous redundant reactions and very complex configuration options are possible to think about.

Note

Each BACS Web Manager is also a complete system for UPS and building monitoring. Since an emergency can be more than just a power outage, you can control all installations like lifts, access control, lights, lifts, etc... A CS141 based system can perform emergency management of an entire IT network, co-ordinate communication with parent and child systems, and much more.

With each additional web manager that joins your network, connectivity, control, and monitoring will be increased.

Preparing batteries

Before you can connect the BACS modules, the batteries must be prepared. In addition to the general safety guidelines for work on live components and live cables, please note the following when handling the BACS power cables: Each BACS measuring cables provides an own fuse, integrated in the positive pole of the cable.

As soon as faulty currents leave the tolerance range, these fuses trip in order to interrupt the contact between the BACS module and the associated battery. By doing so, the BACS module will be protected from damage.

Please note, this fuse is not designed to be removed or repaired. The entire cable need to be changed during maintenance work at the according battery:



Short circuits inside large battery systems are very dangerous depending on battery type, it can lead to explosive gases, escaping high corrosive acids as well as acid gas. It may also lead into fire feeded by chemistry.

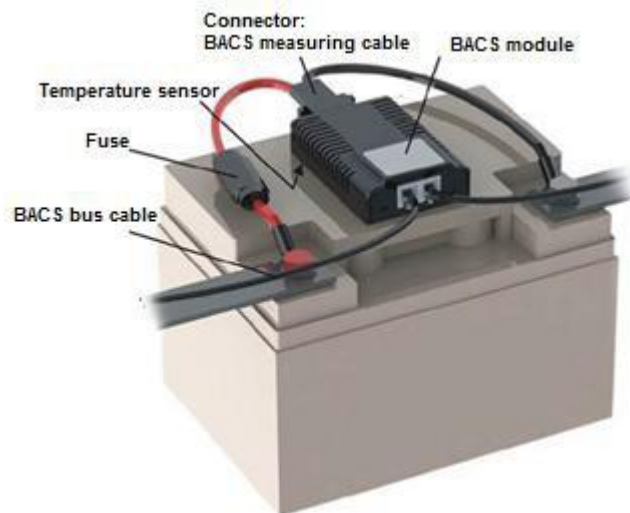
Never try to replace or repair the fuse!

During initial installation, please obey following:

Once load is connected to the BACS cable, current will inevitably flow when as soon as contact with the battery poles is established. During installation work, an unnoticed repeated brief touching of the battery poles can may trigger fuse while connecting to the battery. In some cases, the fuse will continue working for the moment but is permanently damaged and will trigger short time later. For this reason, there is an installation row to be followed:

First connect the cables to the battery poles and then connect the BACS modules to the pre-coded connector. This will prevent such an internal damage at the fuse.

Since battery connectors may vary depending on model and manufacturer, the basic connection procedure is always the same



procedure:

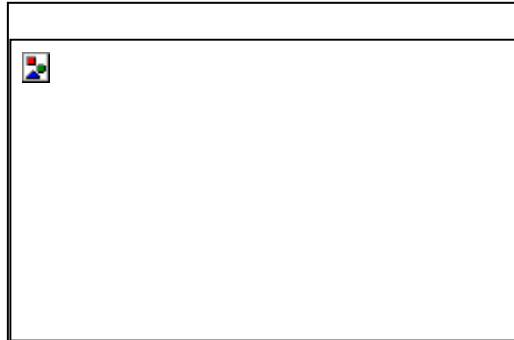
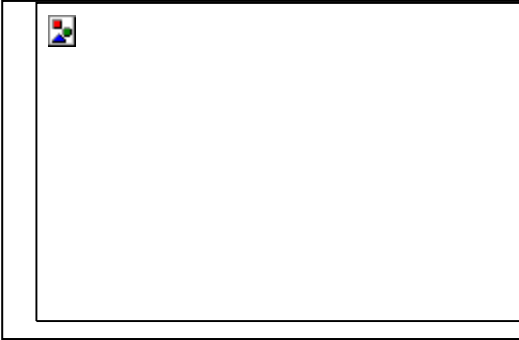
Connect the BACS measuring cables to the poles of the battery. Ensure not reversing the polarity of the cable, the fuse in the measuring cable will be triggered immediately and the cable need to be exchanged:

- | | |
|--------------|------------------------------|
| Red cable: | Positive pole of the battery |
| Black cable: | Negative pole of the battery |

When fitting measuring cables, keep in mind to grant enough space for the later installation of the BACS module:

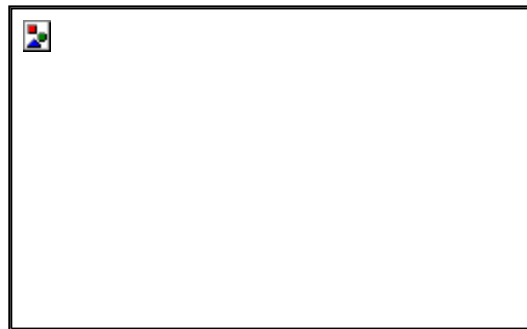
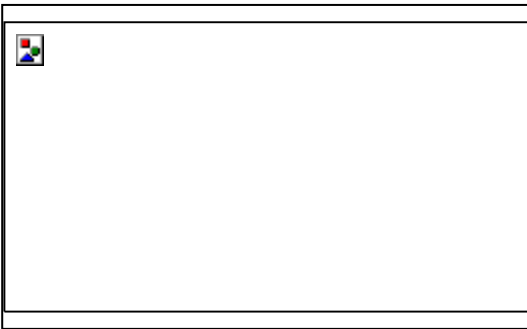
As the BACS module among other things provides a built-in temperature sensor the module must be attached to the battery in a way that the internal sensor is placed about 1-4mm from the battery case. By doing so, the module will be able to measure the air temperature close to the battery.

Connecting a BC5 measuring cable to terminal ports of batteries at 6V - 16V



When connecting the battery terminals, please observe the torque values specified by the manufacturer, as otherwise you may damage both the battery and the terminals. Furthermore, please refer the manual of the battery model - depending on the manufacturer, there may be design differences to the installation examples in this manual.

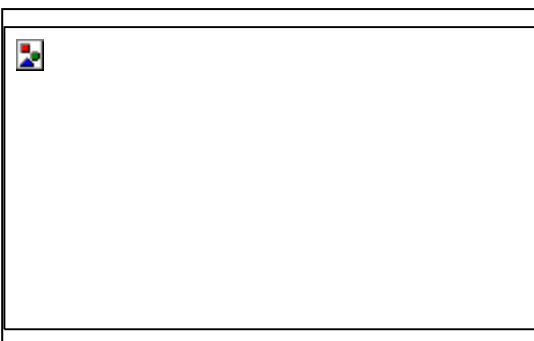
How to connect the BC4B test cables to 1.2V - 2V bipolar batteries



The BC4B measuring cable provides 4 connectors: two for the positive pole and two for the negative pole. When installing, pay attention to the color coding as well as the correct connection. Wrong wiring will trigger the measuring cable built-in fuse - the fuse cannot be repaired or replaced. To avoid damaging the battery as well as the measurement cable, use the torque ratings tested by the according manufacturer.

How to connect the BC4B test leads to four-pin 1.2V - 2V batteries.

Some manufacturers use batteries with four contact points. Coming with this design, two contact points are assigned to a positive or negative pole. Since the BACS measuring cable provides 4 connectors, they must be fitted accordingly to the battery.



Mounting the BACS module at the battery

Please note the preconditions

- there is no dirt on the surface.
- The surface is free from fats, silicone or other coatings.
- The site is easily accessible for maintenance or subsequent service
- If possible, do not cover any valves or cooling fins
 - o In the case of sealed batteries, velcro tape can also be attached directly on it if there is no other way. An AGM valves would in case of opening separate the velcro connection and the pressure escapes.
- For low maintenance batteries and wet cells, keep at least 10 cm distance to the vent pipe

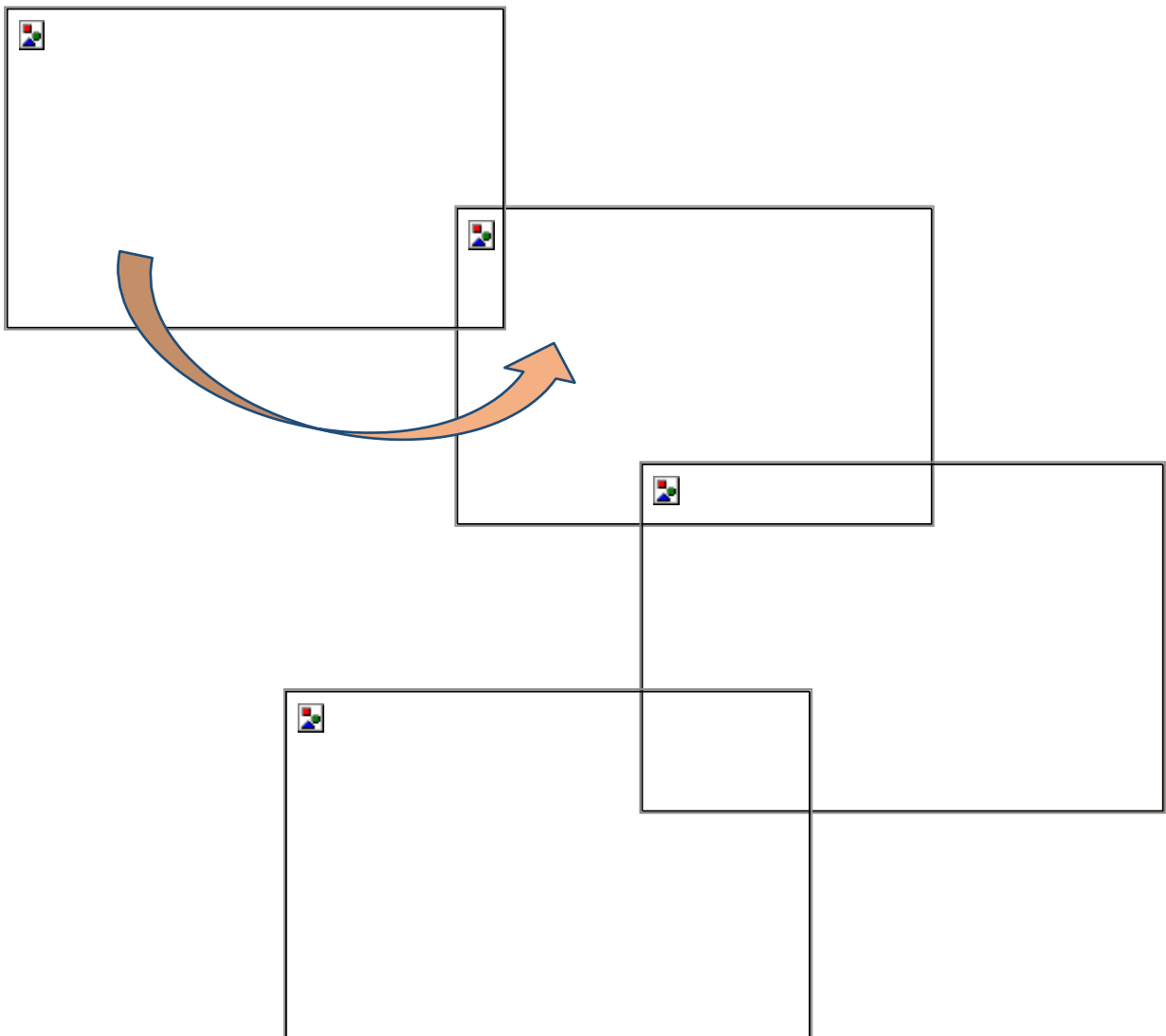
Before installing the BACS modules, carefully read the installation and maintenance instructions for the corresponding battery.

Wiring the BACS module



The BACS cables are coded and standardized, an erroneous connection is normally not possible.

Connect the BACS bus cables to the modules:



For larger cable lengths and installations, please take care for ...

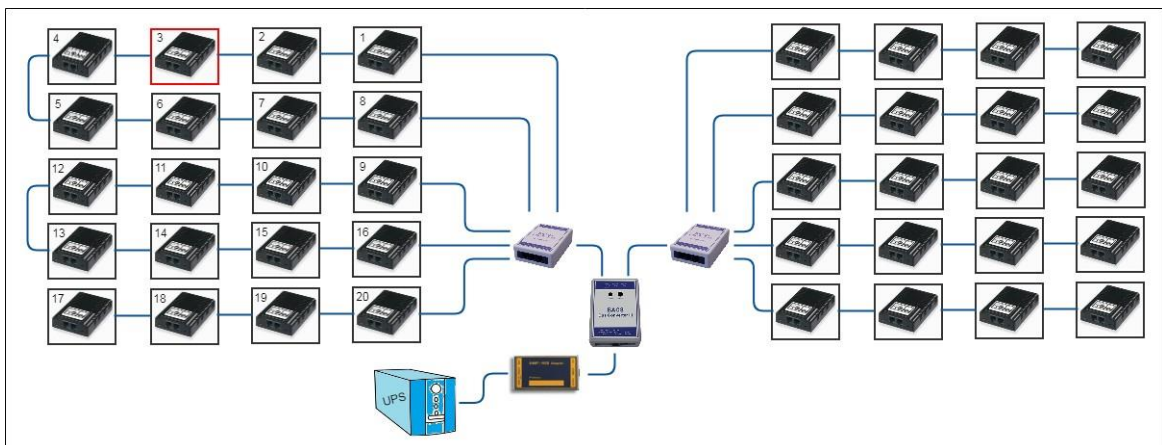
- the maximum cable length including all modules must not exceed 50 m
- Do not install more than 50 modules per cable harness- If more than 50 batteries are in use, a plitting box is mandatory to split the battery site into two different strangs.
- not exceeding the total number of 500 modules.
- installing the modules that the connection sockets are not live after connecting the cables.
- avoiding excess cable lengths

Note

keep an eye on logical cable sequences when connecting - BACS does not tell you how to connect all modules or in which order you address the modules. For technical reasons, a network short circuit is not possible by placing rings within an installation. Structured cabling and related documentation, however, facilitates system maintenance, especially when individual modules need to be replaced within the installation.

Furthermore, if using a splitting box and set up several strings, a structured hardware configuration is mandatory to set up the BACS configuration.

Maintenance: Replacing a single a BACS module



This example describes a problem with BACS module 3. Since the module 3 comes with a ring wiring, the modules 2 and 4 are still available and work properly. By comparison, if module 19 would fail, modules 17 and 18 would have been equally affected - the connection design is not a ring structure.

However, in case of a failure, the BACS webmanager will report a problem at module 3.

How to proceed: First open the battery separator to avoid an electric shock, safe your work place and take enough time to obey the security rules for working on live parts.

1. Identify the harmed BACS module

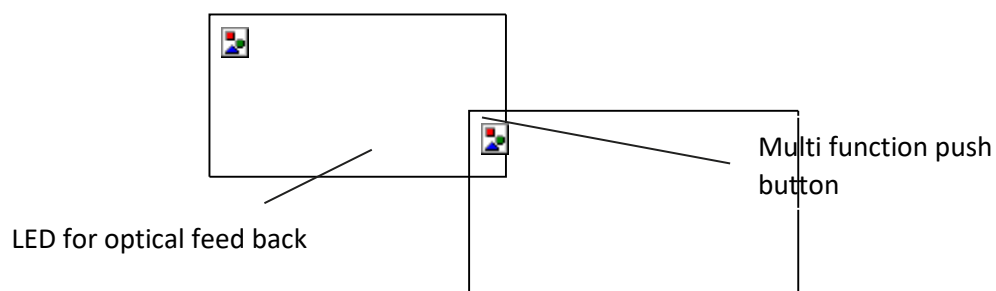
Locate the BACS module with the associated battery and remove the BACS data cable. It is important in this context that the exact ID of the BACS module is known so that you do not accidentally replace the wrong module.

2. Remove the BACS data and measurement cables

Remove the BACS data cable as well as the measurement cable. Please note that the BACS measuring cables installed on battery side do not need to be removed - the changed BACS module will be re-connected.

3. Install the spare BACS module

First connect the BACS module to the measuring cables and proceed to connect the BACS data cables. After the module has been initialized, press the button on the BACS module for about 10-15 seconds:



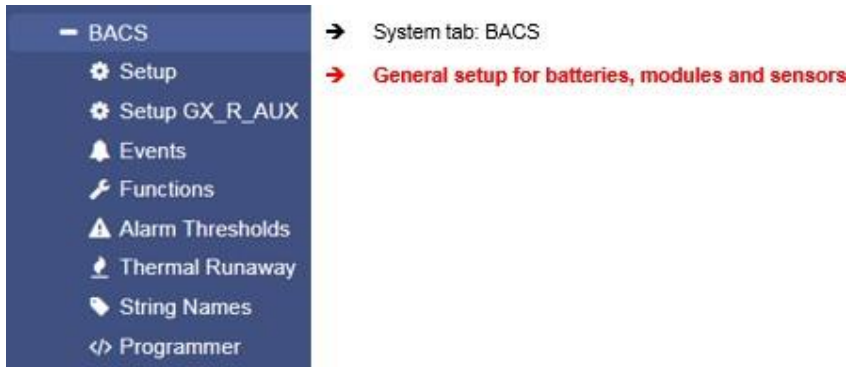
This forces the replaced module into a reset and it reverts to ID 0. This procedure will have effect on this specific spare module and not the entire BACS installation. After reset, the module should now slowly flash red as an indication that its now running on ID 0.

4. Open the build-in BACS programmer and configure the spare module

The module is currently with ID 0 in factory default state. Due to the fact there is only one module that provides ID 0, it is possible to set manually ID 0 to the ID of the broken BACS module. After leaving the BACS programmer mode, BACS will initiate and the new module is active.

Initial BACS Installation: Configuration of BACS

General battery data



Open the general battery configuration dialog and enter required battery data:

Nominal Battery Voltage	12	→ What is the battery voltage of used batteries?
Nominal Capacity per Battery	7 Ah	→ What capacity provide the batteries?
Number of Batteries	1	→ How many batteries are installed?
Number of Battery Strings	1	→ How many strings do you want to set up?

During installation and configuration process, you may choose between different procedures - Since each procedure comes with its specific advantages and disadvantages:

In this case, it is up to you to decide whether first configure the BACS modules and then set the number of batteries or first configure the number of batteries and set up the ID of the BACS modules during installation.



How to find general battery data:

Since these data are mandatory for BACS module configuration, please refer the data sheets of the batteries as well as the name plate attached to the batteries:

In this configuration example, the voltage is 12V with a capacity of 7Ah

Nominal Battery Voltage

Define the voltage each single battery provides. Please note that you may choose between different battery models as long as the voltage is identical:

it is not possible to combine different cell voltages!

Capacity per Battery

Enter the capacity of the batteries in ampere hours. Please note that manufacturers decide how to specify this value inside datasheets. If necessary, convert the values beforehand. This value defines the level of Equalization:

According to the AH value, the BACS modules will be allowed to roll out a maximum Equalizing:

An AH value under 150AH will limit the provided Equalizing power to the size of such smaller batteries, beyond 150AH BACS will use its full Equalizing power which is available for this module type.

Number of batteries

Define the total number of batteries within your BACS installation.

As an example, if you use 40 batteries inside your system, enter 40. Since each battery gets its own BACS module, The BACS webmanager will search for a total of 40 BACS modules, starting with ID 1. The ID 0 is not allowed during normal operation.

Number of battery strings

Number of battery strings defines a logical assignment of the configured batteries in combination with built-up batteries. Among other things, the number of strings is defined by the physical wiring of the batteries. As an example, 20 batteries may be installed into one positive string and 20 into the according negative string. Such a middle point battery setup requires in BACS a configuration as -2 strings- since the charger handles the positive and the negative string separately. Other installation types would be in this case of 10 batteries in string 1, 10 batteries in string 2, etc.

According to this context, it is important the physical wiring of the batteries match the logical structure of the strings. The BACS system uses the sequential numbering of the BACS modules during initialization and divides them by the number of battery strings..

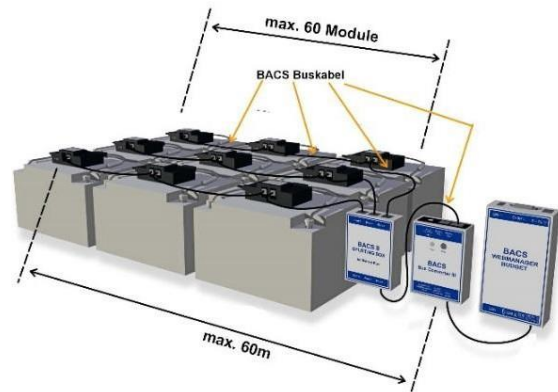
If arbitrarily connecting the BACS modules to the batteries and activate BACS, BACS will logically initialize the BACS modules into a string with IDs 1-10, followed by IDs 11-20, ...

Physically the BACS modules may form up a shredded string that is logically correct. As a consequence, BACS would receive wrong readings and possibly not even start: The strings will be displayed separately in the BACS monitor and treated accordingly during regulation.

When assigning the BACS modules, pay attention to the position or numbering of the batteries in the battery compartment itself to match the logical assignment with the current installation: Ideally battery no. 1 also received the BACS module with the number 1.

Something more to take an eye on

For technical reasons, it is not possible to connect and manage an unlimited number of batteries to a single string. From 50 batteries onwards, we recommend to "split" the BACS bus, ie to define two different cable strings per definition in order to keep the cable length as short as possible.



Note

With String Names it is possible to enter a freeform label for the battery string. you enter a name for up to 16 battery strings before configuring the BACS modules. However, the number of strings will be define at Number of battery strings. that will be shown. Entering a name does not automatically increase the number of battery strings.

Helpfull information about the BACS system

Information		
Battery Manufacturer	<input type="text"/>	→ Manufacturer of the battery
Battery Type	<input type="text"/>	→ Installed battery type
Battery Location	<input type="text"/>	→ Where are the batteries installed?
Battery Installation Date	<input type="text"/>	→ Installation date of the batteries
Contact Person	<input type="text"/>	→ Responsible staff
Contact Person Phone	<input type="text"/>	→ Direct phone contact data of staff

Battery manufacturer and type

Enter the designation as free form text. If usefull, add some information about it's function or the intention of this battery system or in special cases chemistry used for this battery room. If an incident occurs and rapid interaction is mandatory, this information can increase the average response time. On the other hand, misleading or poorly documented terms can cost valuable time.

Battery installation date

The battery installation date indicates the date of initial battery installation. Since a system can be upgraded with BACS at any time, it is important to be familiar with the difference of a battery installation date and the installation date of BACS.

You will usually find the battery installation date on the battery itself as "date of manufacture"

Contact person and phone contact

In case of maintenance work or incidents, responsible staff can be contacted to shorten response time.

Note

If wanted, BACS can send general contact information to a custom mail address and contact responsible staff directly. However, your entry at contact phone cannot be used for automatic SMS notifications - An SMS modem or IP modem must be configured separately.

BACS module basic setting

Module	C20	→ Choose the module
Equalizing on	<input checked="" type="checkbox"/>	→ Enable / Disable BACS
Optimize Scan	<input type="checkbox"/>	→ Optimize Equalizing scan
Choose Discharge Detection Source	Automatic	→ What to use as discharge detection?

Module

Different voltages on the batteries require different BACS modules - please ensure to select the BACS module type fitting to your batteries. Depending on the voltage selected for the batteries, it will display modules fitting to the voltage. Currently the following modules and voltages are available:

Cell Voltage	Selectable module
2 V	C40 / C42
4 V	C41
6 V	C30
12 V	C20 / C21 / CSYM
16 V	C23
24 V	CSYM

The screenshot shows a configuration window with the following fields:

- Nominal Battery Voltage: 2 (dropdown)
- Nominal Capacity per Battery: 7 Ah
- Module: C40 (dropdown, with C40 and C42 also visible in the expanded list)
- Equalizing on:
- Optimize Scan:
- Choose Discharge Detection Source: Automatic (dropdown)

Obey the correct settings. An unsuitable combination of UPS, modules and batteries may lead into system failure and damage.

Equalizing on

Equalizing is a patented voltage distribution control system inside a battery pack, the batteries will differ from each other. As a consequence, they need individual regulation of charging voltage to reach the target charging voltage of the charge controller.

Since Equalizing intervenes in the charging circuit and actively regulates,

it may be necessary for new installations to operate the batteries for some time without this regulation. This will allow batteries to "form" up each other. During this time window, new batteries will be operated without regulation, the voltage differences need to be tolerated. Please contact your battery manufacturer if their battery products need such a time window and how long it should take until Equalizing can take over in order to protect your batteries.

The installation of the BACS modules as well as fetching measuring data with the BACS system is completely independent to equalizing - you can install and operate all BACS modules without charging control and active regulation. Equalizing can be activated at any time. If activated, BACS will take over the care of the batteries.

Optimize Scan

Normally, only a small amount of data is collected and stored during trickle charging. Since the parameters of the battery will not change very much during a trickle charge, only a small amount of data is collected and stored. This will change during discharging:

When discharging, considerable amounts of data are generated. Furthermore, BACS increases the sampling rate in order to record the event as accurately as possible during an evaluation by additional freewaer tool BACS VIEWER. The scan optimization reduces the data points to the measurement of voltage values. by doing so, changes in a discharge cycle can be recorded much more accurately.

Discharge Detection source

BACS offers alternative options to differentiate between a charge and discharge cycle. By default, BACS will automatically select the best source and, if necessary, query alternative sources:

- UPS

The UPS provides the fastest and most reliable detection rate due to the fact it will switch in case of a powerfail to battery mode. Depending on the design, the BACS system can use the CS141 slot card, an RS232 interface or even the RFC1628 network interface in the network to obtain the information, amon other useful information, about detecting a discharge.

- *Current sensors*

The direction of the magnetic field induced by current flow is a probate method to figure out if the batteries are currently in state charge, trickle charge or discharging. Although the detection rate is slower than querying the UPS. Current sensors provide additional measurements of the quality of the discharge current. The current sensor selection would be the best detection source if a UPS state query is impossible.

- *BACS sensors*

The BACS sensors can also perform a discharge detection:

The modules measure the battery voltages - from the moment the voltage drops below the rated voltage, BACS will assume a discharge is in progress. Since the batteries take a while to fall from the trickle charge to the rated voltage and stay there for a while before dropping below this value, it is a reliable but very slow option to figure out if a discharge is in progress.

Normally, this detection source is selected if neither UPS nor current sensors are available.

Note

A rechargeable battery needs some time to fall from trickle charge values to it's rated voltage. This natural process can be misinterpreted as "discharge". For this reason, a battery monitoring or management system needs the ability to differ between this natural process and a battery discharge:

BACS can do this job and will increase the detection and logging rate only if a real discharge is confirmed.

To improve detection rate, additional current sensors are recommended- if BACS detects a voltage loss as well as current flow, the discharge status is confirmed.

Offset values

Offset Values	
Temperature Offset	<input type="text" value="0"/> °C
Impedance Offset	<input type="text" value="0"/> mΩ

→ Enter temperature differences
→ Enter impedance differences

BACS modules are calibrated on delivery and will give an exact value related to the calibration. However, the BACS system can not know the general installation location and it may be possible that the calibrated measurement results differ from external reference measurements due to the installation site. Air pressure, humidity, ambient temperature and other environmental variables can distort the values collected by BACS:

The calibrated values need to be corrected if necessary.

With the offset values, it is possible to enter correction values coinciding with measurements at the installation location.

Current Sensor

BACS CS Current Sensor Connected	<input checked="" type="checkbox"/>	→ Enable / Disable BACS current sensor
Only One Current Sensor For All Strings	<input type="checkbox"/>	→ Number of installed current sensors
Reverse Current Direction	<input type="checkbox"/>	→ Direction of installation
Ampere Multiplier	<input type="text" value="1"/>	→ Multiplier

Each BACS module already provides its own charge / discharge detection.

The detection by the BACS modules arises from the need for batteries to generally have a slight discharge curve and lose their charge over time.

However, this charge / discharge detection is realized by voltage measurements of the cell. If the voltage drops below a rated voltage, BACS assumes a discharge is in progress. What the BACS module does not measure is the current flowing through the individual strings during a battery discharge cycle.

In addition to the charge / discharge detection, the current sensor can also be used to check whether the currents are divided equally between the parallel battery strings as well as the average quality and stability of the current.

Installing the current sensor

If you want to use a BACS Current Sensor, enable the BACS CS Current Sensor Connected:

By default, the BACS Web Manager searches for one current sensor per battery string - the number of BACS strings will reflect the number of sensors that need to be found. At BACS monitor, the result will be displayed below the according string.

18	13.58	30.2	18.85		
19	13.58	29.9	18.63		
20	13.58	30.0	18.84		
Σ Spannung 271.65 V					
13.58 [V] Target Voltage					
0 [A] Strom 0.00 [KW] Reale Leistung					

→ Current sensor

Premium feature: Only One Current Sensor for All Strings

Usually each battery string get its own current sensor to get information about real current flow on all strings. In some cases it is desirable by customers to use only one current sensor for a general charge / discharge detection. By doing so, BACS need to know that only one current sensor is installed:

Enable "Only One Current Sensor for All Strings" and press apply to restart BACS.

After restarting BACS, only one sensor will be automatically displayed. If the current sensor is installed on a string, the ampere multiplier value will get approximate overall current value.

Premium feature: Ampere Multiplier – how it works

The ampere multiplier multiplies the measured current by a theoretical factor in order to draw conclusions about the entire system. The multiplier value to be entered depends two factors:

1. There are several strings in the BACS system - the number of strings determines the multiplier.
2. For various reasons only one current sensor is available

The multiplier can be used this way:

Main string: The current sensor measures main current value = 1

Single string: The current sensor measures the partial current of the string value = Number of strings

Since the measurements are not very exact in the end, this solution serves only the more accurate charge / discharge detection. It is not designed to determine more information than an exact charge/discharge detection as well as basic information about estimated current flow.

Note

You will get the *best* results with a combination of current sensors inside each individual BACS string as well as using the sensors coming with BACS modules. By doing so, more data can be collected and analyzed:

- General voltage
- Internal resistance of the batteries
- temperature of the batteries
- quality and uniformity of the discharge current itself

However, BACS offers you different graduated possibilities for discharge detections:

1. UPS status

The UPS knows the current charge or discharge status and will provide this information for the BACS Webmanager. To choose this option, the BACS Web Manager must be connected to the UPS. Depending on the BACS design, you can choose between a single device or a modular solution. Even the combination CS141 slot card with BACS BUS Converter can be used.

In other cases the connection is possible via the RS232 interface. If you use a UPS with SNMP access, it is also possible to configure an access via the RFC1628 interface and query the data directly via LAN. Current sensors provide additional current quality detection

2. If no communication to the UPS is possible, you can get accurate information via the current sensors and the BACS modules.
 - a. Charge-/Discharge detection
 - b. Accurate readings on consistent charge and discharge cycles as well as quality and fluctuations of the current.

In this setup, the BACS modules provide voltage values across the batteries and the current sensors provide values about the current that actually flows per string.

3. If, for logistical reasons, you can only use one current sensor, it will in principle provide an exact charging and discharging detection source. But with one current sensor, it is just possible to provide a theoretical overview of the quality of the current that will flow during charge- / discharge processes.

Obey that the current sensors can be used either on the main line before splitting into single strings or inside a single string after splitting.

a. The main string

At the main string, the total current is measured. You will recognize a very accurate charge / discharge detection as well as information about internal fluctuation in the current flow, but you will not be able to get informations about the strings that may trigger current flow problems.

b. At the single string

Like a main string installation type, you will find a very accurate charge/discharge detection. The difference is, that the single string installation will measure the real current at this strand the current sensor is installed to. You can use the multiplier to approximate the value to reality, but it remains as some kind of rough estimate. What you can see accurate:

If the value for current drops, the problem has to be found in the string where the sensor is installed to. On the other hand, if the value increases dramatically, there is a problem in one of the other strings. Technically, a more exact limitation feasible in this constellation is not possible and the accuracy depends on the number of strings you have installed - With two strings, it is easy to figure out which string causes trouble. With three strings, two strings you have possible candidates...

4. You can also completely dispense the connection of a UPS as well as the use of current sensor. The charge / discharge detection can be fully mapped by the BACS modules. The modules measure the internal resistance and the voltage of the batteries they are installed on. The modules can measure if a charge cycle or discharge cycle is in progress. But it will need some time. This possibility, however, ignores the current that will flow during charging and discharging.

Reverse Current Direction

The current sensor measures the induced magnetic field coming with directed electron migration through a conductor. Due to the fact the current sensor can measure bi-directional, the installation direction is crucial:

The magnetic field of this directed electron motion provides information about the direction of electron migration.

With this function, the real magnetic field recognition can be inverted - thus will place charge and discharge recognition into a correct context. If the current sensor has been installed incorrectly, this function can be used to reverse the current direction and the sensor can remain in this installation direction.

Thresholds for current sensor discharge detection

Thresholds	
Discharge	-1 A
Charge	1 A

The direction of current flow indicates whether the batteries are charging or discharging. In principle, you need to differ between three charging or discharging states:

1. Discharging

The batteries discharge while granting emergency power.

2. Charging

If batteries drop below a certain voltage level, they must be charged. This battery state can be reached via a natural discharge process over time or in case of emergency power usage. The charging process is always initiated and terminated by the UPS / Charger. By "Equalizing", BACS distributes the existing charging current and voltages - Each battery charge is considered individually to ensure the optimal charging.

3. Trickle charging

Batteries tend to self-discharge over time. This process can not be prevented, but slowed down by proper storage. The trickle charge hereby serves to maintain the current state of charge. Normally, a trickle charging will not be displayed.

Depending on the charging behavior of a UPS, certain currents always flow within a system. Due to this fact, it cannot generally be assumed that a current flow is automatically a charge / discharge cycle. Since only two of the possible states are important for the current sensor to detect a charge or discharge cycle, it is necessary to define a fixed point at the current intensity for a charge/discharge cycle.

With the "Thresholds", the values can be adapted to the environment that a clear charge or discharge cycle can be assumed.

The negative sign defines the discharge cycle and the positive sign the charge cycle.

How to configure the BACS modules

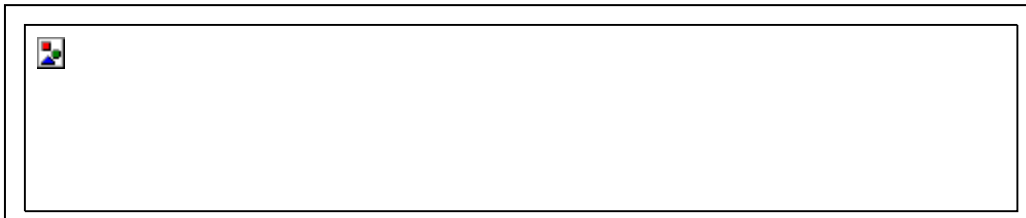
Addressing BACS modules: The BACS programmer

The BACS modules can be configured by using the WINDOWS program BACS PROGRAMMER or via the web interface in the CS141 / BACS WEBMANAGER.

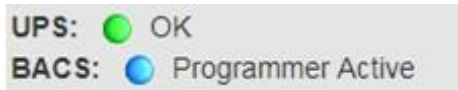
To use the BACS programmer in the web interface, navigate to the following menu:



To install, configure, or remove new BACS modules, the BACS system must be put into standby for this time window. First set the Programmer Input Capability to "On":



Please note that the button generally describes the state that is currently available. While the Programmer is active, BACS pauses – the current system state can be seen at the top status bar of the Webmanager:



The top bar shows that the BACS Programmer is now active and normal BACS operation is paused.



The top bar shows that BACS has started and is in regular operation and the BACS programmer is off.

Two conditions will disable the BACS programmer and enable regular BACS functions:

1. Cold start or reboot

During a cold start, the device is de-energized briefly and then reboots. A reboot will be advised by an administrator via tools or directly via the web browser reboot command. In both cases, the default startup setting will start without the BACS programmer set to on.

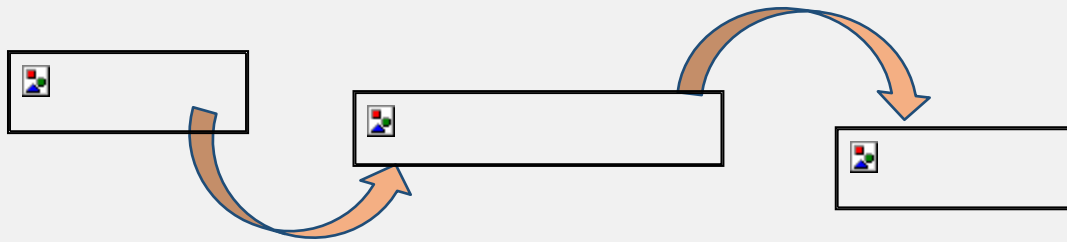
2. Enable or disable manually

The BACS Programmer does not have an automatic activation function - it is started manually by an authorized user and must be terminated accordingly. If you log off as an administrator from the system, the BACS Programmer remains active, even if you subsequently log in as an engineer.

Note

Always remember to disable the BACS programs after using. An internal watchdog will permanently look if there is activity on the BACS bus. *After 15 minutes without some kind of activity*, this watchdog will assume something is wrong and trigger reboot.

Once you enable the feature, the BACS Web Manager will adjust its BACS status accordingly:



Normal operation and any communication on the BACS bus is paused by user for maintenance work. After finishing maintenance work, the BACS programmer will be disabled and normal operation starts. The BACS bus watch dog is not part of the CS141 - it is placed on the BACS Bus Converter and will interpret the entire communication between CS141 and the BACS modules - and restart the CS141 in case of a communication failure.

Addressing modules*Change the ID*

During initial commissioning, the BACS modules must receive a unique ID in order to be able to register with the BACS Web Manager. In general, these addresses are static, but each BACS module can be reset to factory default or programmed to any other ID.

Because reprogramming is possible, setting up an ID follows specific installation rules:

1. Each ID is unique and it is not allowed to set up one ID twice.

Duplicate registrations will produce errors when initializing BACS because the modules can not be uniquely assigned to a battery.

2. Only sequentially numbered IDs are allowed inside the BACS network.

The IDs are assigned to a specific battery a BACS module is connected to. If 25 BACS modules are expected, 25 batteries are mandatory. You can not "turn on" module ID 26 with a new battery and "turn off" the battery with the BACS module ID 17. You need to reassign the module-ID 17 to the new battery.

3. The highest ID number defines the number of batteries you want to install.

BACS will not scan for 25 batteries with a connected BACS modules, it will exclusive look for 25 batteries with the BACS modules ID's 1-25.

Define an address range

Please remark, resetting modules may be necessary as of an initial installation - reusing modules for another BACS installation is possible. In that case, the existing modules may still have arbitrary ID's from older installations. On initialisation, all modules need the ID 0.

First define the module ID range you want to reset. You free to choose a complete range from 0 - 600 or - if wanted - limit their range: 250 - 450.

Check "Reset" and press the Start button to begin. The BACS Webmanager will reset all modules and set them 0. The modules will visually display this process by slowly flashing red.

Range

[Help](#)

Reset

Start

End

Note

In some cases, the modules may not have been reset by the BACS Web Manager, as an example, if a cable is damaged or individual modules are not properly accessed due to external interferences. You can manually reset these modules by holding down the button on the module itself for about 20 seconds.

Set up all modules

When configuring the BACS modules, please note that one BACS module must have ID 1, otherwise the entire BACS communication will not start after configuration. At Start, enter the first ID number you

want to assign. With End, enter the last ID number you want to assign. Pressing Start will start the configuration process:

You will notice that all modules will begin to flash fast. The fast red blink indicates that the modules are in addressing mode and ready to confirm the ID number.

Start addressing by pressing the programmer button at the BACS module. The module LED will change the color and blinking frequency into a slowly blinking green state. With each module button press, the BACS Webmanager will count up until all numbers are set and the Webmanager shows the message: "succeeded"

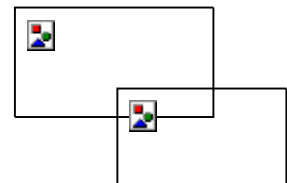
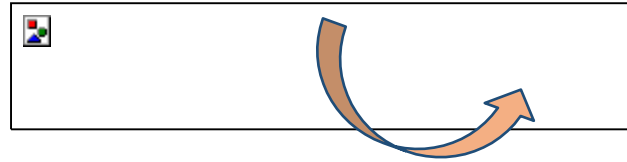


Assigning address ID's can be stopped, if...

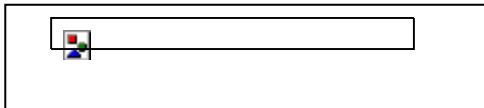
1. The number of ID's previously entered are confirmed
2. you press the Stop button.

The BACS module programmer button

You assign the IDs by pressing the button on the BACS modules. The module will acknowledge receipt of the ID by flashing from fast red into a slowly green. At the same time, the process bar in the web interface of the BACS Web Manager will count up one ID. Please ensure not pressing the LED - this is not the button! You will find the button on the other side of the BACS bus data cable connectors.



Audible confirmation



On request, an acoustic confirmation can be set when assigning the BACS Module ID. By doing so, the BACS webmanager will generate an additional audio signal from every button operation..

Define different address ranges

In larger installations with a huge number of modules, addressing modules is still mandatory. To increase clarity, it may be recommended to assign ID's to the BACS modules step by step. For this reason, you can address different address areas one after the other.

Just divide the BACS modules into individual address ranges:

Addressing sequence 1:	Address range 1-50,	Start-ID: 1 / Final ID 50
Addressing sequence 2:	Address range 51 – 100,	Start-ID: 51 / Final ID 100
Adressierungsdurchgang 3:	Address range 101 – 150,	Start-ID 101 / Final ID 150

Use the module addressing dialog Start and End to define a unique address range.

Note

The individual BACS modules can be combined in so-called strings - the modules are logically divided into individual groups and displayed and measured accordingly. This logical assignment works on this principle:

Number of registered modules divided by number of strings gives the number of modules per string.

When setting up the modules, make sure that the logical assignment matches the physical structure:

The order of the modules within a string are less important for the function of BACS, but if the modules' position differs physically and logically, measurement and control errors will occur. Due to a wrong construction, the strings can be randomly thrown together and lead into problems with battery string breakers, current sensors, etc.

Changing a single ID of a BACS module

The "Single" function allows you to set and change individual module IDs of BACS modules.

This function provides 3 different options:

- Switch an ID to another
- Switch an ID to 0
- Switch an ID from ID 0 to a target ID

The procedure is identical to all three options:

Single

Connect only one Module to the bus to avoid undetermined behaviour of the system.

Old

New

Under Old, enter the current ID that you want to change. Under New, enter the target ID to which you want to set the BACS module. Unlike standard addressing, this mode requires no action on site at the BACS module.

Resetting module ID's

If necessary, the BACS modules can be returned individually or completely to the delivery state. Depending on the procedure, only the ID will be changed or by pressing the modules button for 20 seconds, the modules will perform a hardware reset and falls back to the default ID 0.

Resetting all modules or an address range to factory default

This action will reset all specified ID's directly to factory default 0 as soon as you press Start. The modules will visually confirm the reset with flashing slowly red.

Setting one single ID back to 0

Resetting a single module can be done by two different methods:

1. Use the BACS programmer

You can specifically reset a BACS module to 0 in this way. As a consequence, the BACS module will slowly flash red. This is useful if you want to swap a module, but you want it to be reset to the factory default state for later use within other installation.

By doing so, it is ensured that the ID is no longer in use before you remove the module..

2. Press the BACS module button for about 20 seconds

With this option, the BACS module will be forced to reset on the hardware side. Accordingly, all information contained in the module is deleted.

Finding modules

Large BACS installations can be very confusing for new guys.

In order to locate a specific BACS module within all the strings, the programmer offers a fast and convenient solution:

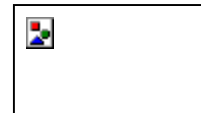
Under Query you can optically flash individual modules with a red flashing. This will help you to find the according battery you wish to maintenance.

Simply enter the ID of the module you are looking for and click on "Show" - the module will start blinking slowly red/green.

The module you are looking for will blink accordingly. You can choose between these two options

1. Go to the BACS module and press the button.

Pressing the confirmation button on the module itself will release the search function and the module falls back to normal operation mode.



2. At BACS Webmanager, press OK to confirm search is over.

The module will be triggered by the BACS webmanager to fall back to normal operation.



Check for module with red/green blinking led. Address: 2 Acknowledge having found the module and quit search by clicking "Ok".

BACS programmer Single mode

The single mode is an option to program one single BACS module or change module ID's inside an existing BACS installation.

Please note for this function it is mandatory to know the exact ID of the according module you wish to program.

If you are unsure about the current ID, please reset the module to factory default ID 0. If you know the module's ID, you may skip resetting the module and use the current ID.

At „Old-, enter the current module ID. With „New-, the new module ID

Single

Connect only one Module to the bus to avoid undetermined behaviour of the system.

Old

New

can be entered. Set will start the programming procedure. By doing so, it is not required to push the confirmation button at the BACS module.

The BACS module will confirm the setting by flashing slowly green.

Using single mode inside a BACS installation

This function can be used to change module ID's inside an existing BACS installation – this will allow to resort BACS-Modules according to the physical wiring. The according module can be logically set to a string it is physicalle installed. Please note: You can program two modules with the same address. As a consequence, BACS will not start because of an address conflict. if you set up two modules with the same address, you need to seperate the ID's with a hard reset of one of these modules or by disconnecting on module. Otherwise these modules will receive and confirm the new ID simultanously.

Checking ID programming:

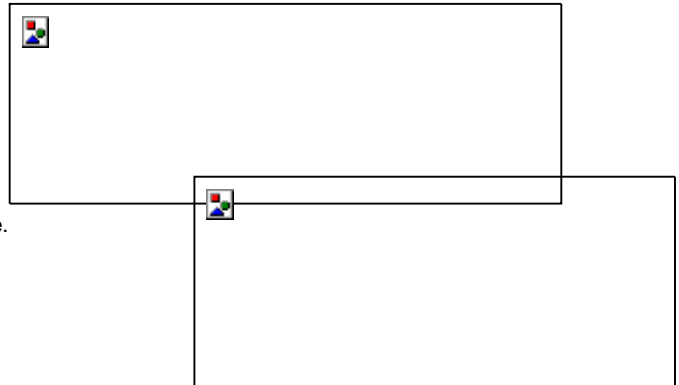
If unsure, it is mandatory to check the ID's of the modules. With this tool you can check ...

- If the module responds to the intended ID
- If there are two modules with the same ID inside a BACS installation.

Search a BACS module

Under Module, enter the ID you want to find and press show:
All modules will start blinking green, with one extention:
The module with the entered ID will blink red/green.
The blinking will stop by pressing the confirmation button of the module or at the BACS programmer pop up confirmation dialog.

If you set up an ID twice, both modules will start blinking this way.
If BACS cannot find the module, it will display an according message.



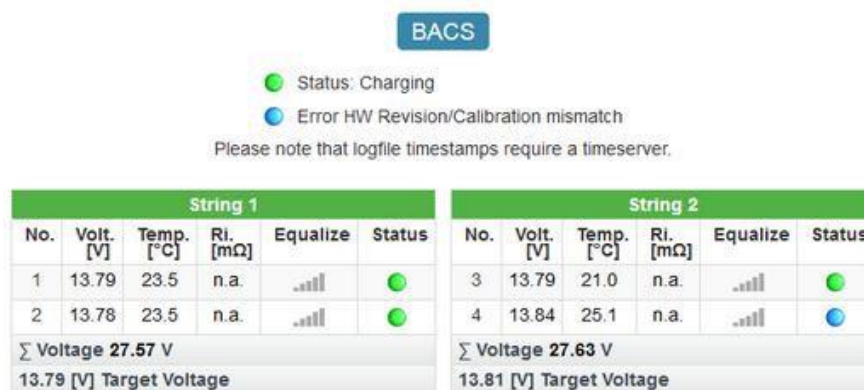
BACS Error: HW Revision / Calibration error

Once all modules are set up correctly and the BACS programmer mode is disabled, the BACS system boots and initializes the modules according to their configuration.

The result can be observed within the BACS Monitor Screen:

After validating the entire configuration, all modules will jump to "green" - The system will be ready for use.

In some rare cases, however, this system message occurs:



BACS

● Status: Charging
● Error HW Revision/Calibration mismatch

Please note that logfile timestamps require a timeserver.

String 1						String 2					
No.	Volt. [V]	Temp. [°C]	Ri. [mΩ]	Equalize	Status	No.	Volt. [V]	Temp. [°C]	Ri. [mΩ]	Equalize	Status
1	13.79	23.5	n.a.		●	3	13.79	21.0	n.a.		●
2	13.78	23.5	n.a.		●	4	13.84	25.1	n.a.		●
Σ Voltage 27.57 V						Σ Voltage 27.63 V					
13.79 [V] Target Voltage						13.81 [V] Target Voltage					

HW Revision Mismatch

On initialization, the BACS Webmanager assumes that the hardware revision for the module coming with ID 1 (The first module) is the reference for all subsequent modules. The Webmanager compares the hardware revisions with the revision number found at ID 1. If one of the following modules show different hardware revision, the module is marked accordingly:

BACS modules from different installations can be combined as required. After adjusting the ID of the according module, the module can be inserted e.g. as a spare part. Different hardware revisions are not allowed - they cannot be combined with each other. If a module does not fit the BACS system, it must be replaced by a corresponding module with a hardware revision that fits to it. In case of maintenance works inside larger BACS systems containing several BACS Web Managers, keep an eye on possible compatibility issues between the individual BACS modules

Note

If ALL modules show this issue on initialization but not the first module, take a look at the module with the hardware ID 1:

It is probably be affected and the following modules use the correct hardware revision.

In this case, exchange the ID 1 with a different ID via the BACS Programmer and repeat the boot process. Normally, all modules should now have the status green and this one module should be marked accordingly.

If you have just been supplied with a single BACS system, please contact your local dealer: It is possible that this shipment contains a wrong BACS module.

HW Calibration Mismatch

The second test validates if the modules are calibrated:

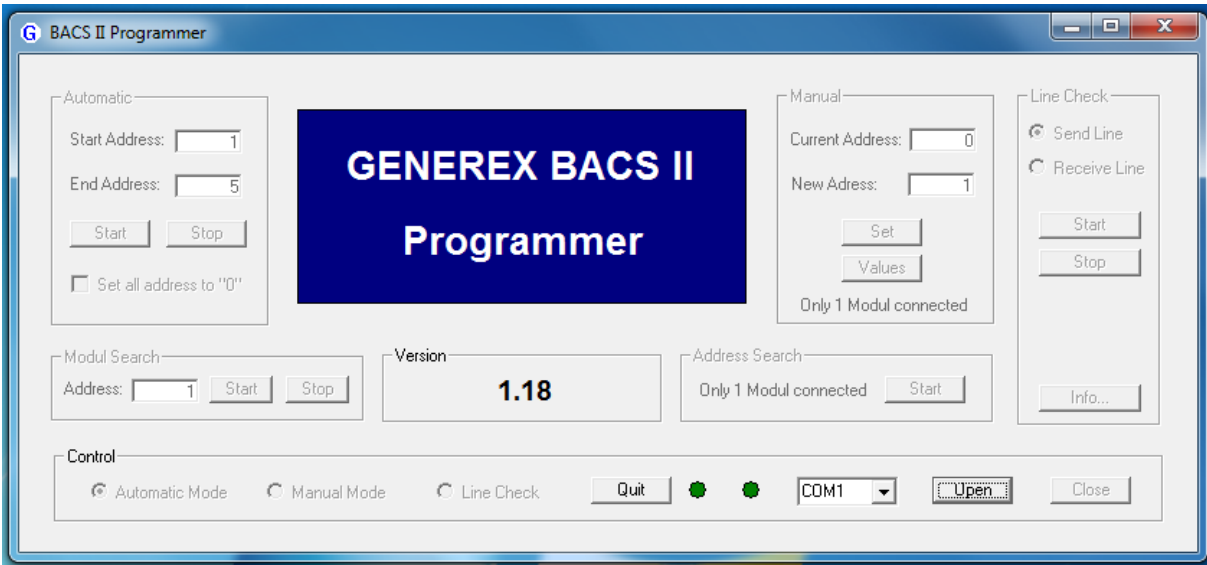
First of all: you cannot re-calibrate them manually. The calibration is performed during production at the factory. Because the BACS Webmanager needs exact values for its reliability, it checks if this calibration has been performed during initializing phase. If a module does not pass this test, it is not suitable for operation:

Unlike the Mismatch Error revision, the Calibration Mismatch Error is a hardware failure that affects the module itself. Unfortunately, this issue cannot be fixed by porting module to another BACS system:

In this case, the module must be replaced by a corresponding replacement module.

The alternative method: Using the BACS Programmer Windows software

The BACS Programmer software can be used with both, the BACS Webmanager budget as well as the BACS Kit. In addition to the core function of addressing modules and preparing them for operation, the BACS Programmer software also offers interesting features helpful for error diagnostic and the detection of individual modules within a very large installation.



Preparation

This software is not a network software, you need to connect the BACS Bus Converter to the COM port of your computer.

Note

Modern laptops often do not provide a native COM port anymore. Before your on-site visit, check if your mobile device provides such a port. If this is not the case, a suitable adapter cable can be used. Normally, this cable will be connected to the USB port and thus establish a connection between your computer and the BACS Bus Converter.

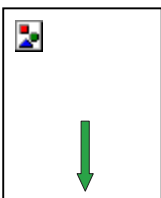


This standardized accessory for your computer is usually available from specialist retailers.

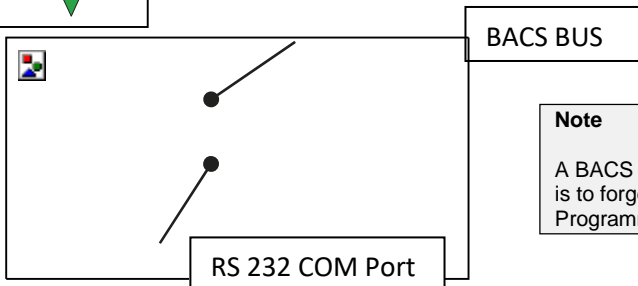
Ensure to use the supplied cable, a standard cable may fit to the ports but may have internal differences - the software would consequently suggest problems caused by an inappropriate cable:

Not every Mini-DIN / Sub D 9 pin cable can be used to communicate with the BACS Bus Converter. Mark your cables to be used to avoid confusion during maintenance work.

Connecting the BACS Bus Converter



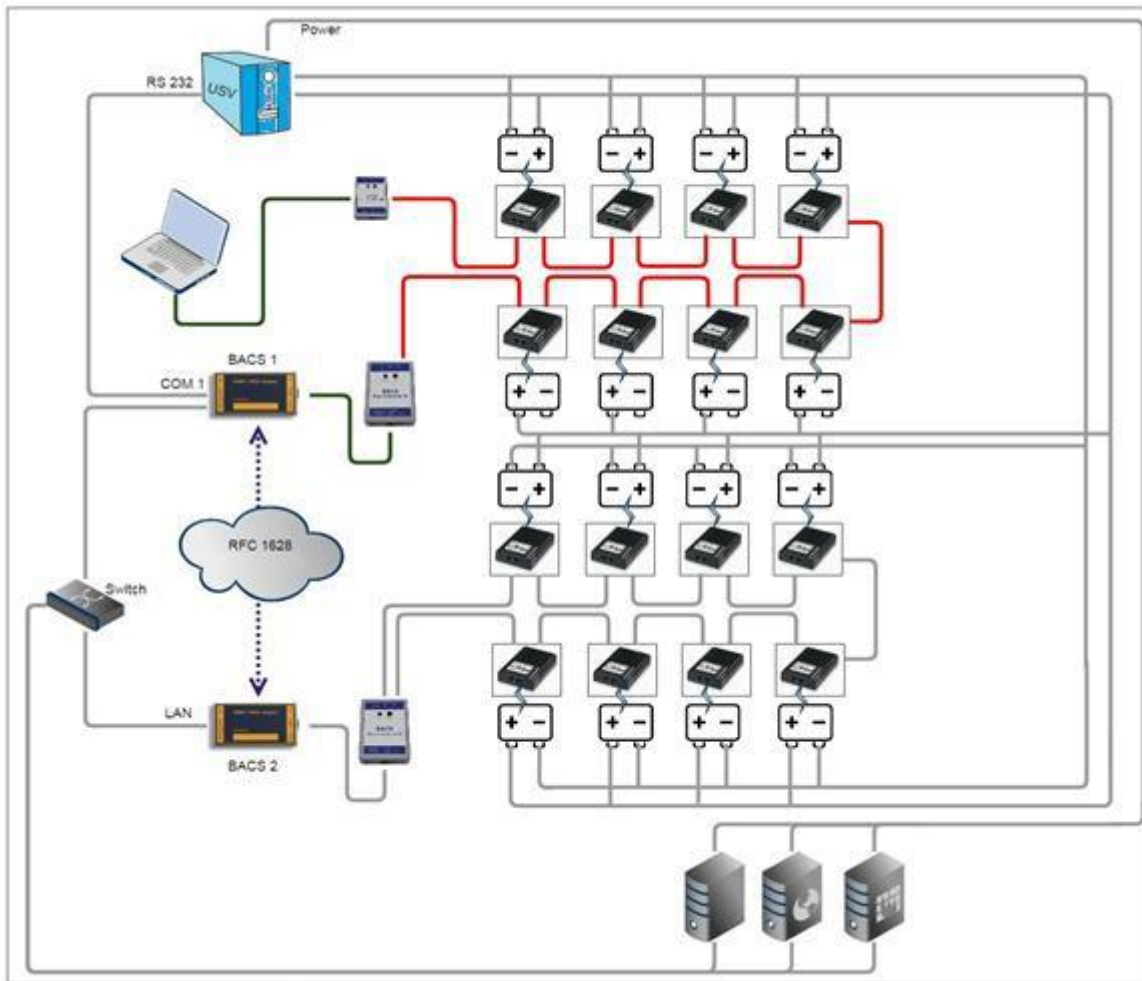
First remove the connection between the CS141 and the BACS Bus Converter. Then connect the COM port of your computer to the BACS bus converter. The port is labeled on the BACS Bus Converter with From PC RS232 COM Port.



Note
A BACS Bus Converter requires its own power adapter. A popular mistake is to forget this when connecting ... As a consequence, the BACS Programmer will not establish any communication.

Pay attention to possible redundancies when connecting.

You do not necessarily have to decouple the entire BACS system if you want to specifically check a specific section within a large system - but you need to ensure only one BACS Bus Converter will access the tested modules:



In this example, a cable was taken from the BACS 1 and connected via a BACS bus converter to the COM port of the laptop. In this constellation, both BACS bus converters would disturb each other until the segment to be tested is completely decoupled and separated:



The number as well as the module ID's of BACS modules that can be tested is determined by the technician who interrupts the data connection.

Note

WIf you are looking for a fault in the cabling, you should check with both, a simple and a ring cabling. If several modules are affected in the middle, you can determine the source of the error exactly from both sides. This allow you to find the affected section. However, if there is only one cable faulty, you will need the simple wiring to locate the faulty cable or module.

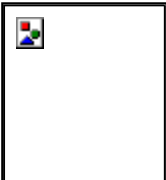


At BACS II Programmer Tool, select the according COM-Port of your Computer the cable is connected to and press Open.

The button label will change to "close" and the BACS Programmer will try to establish a connection to the BACS Bus Converter via the serial connection.

Toggle operating mode

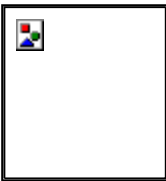
Automatic Mode



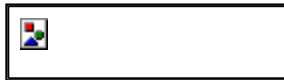
By default, the BACS Programmer starts in Automatic Mode.

In order to prevent accidental incorrect entries, only the functions assigned to a specific operating mode are enabled. The automatic mode is designed for the automatic addressing of BACS modules, the functionality is the same as in the BACS Webmanager

Manual Mode



This mode describes similar functions like the single module address and search tools running on the BACS Webmanager. Search for an address ID of a single module or change module addresses.



Searching for an installed module



This feature will be interesting if you are inside a very large BACS installation and, as an example, you are looking for the BACS module with ID 378.

In this case, enter 378 and press Start. The requested module will respond with a red flash within the BACS installation until you click Stop.

Line Check

A premium feature of the BACS programming software is the Line Check:



With the Line Check, BACS cabling can be tested.

This test can help you to find points of weakness inside a cabling concept. As an example, this test is helpful, if

- the signal is partial disturbed caused by electromagnetic interferences (EMI) or other influences during installation not all modules are addressable.
- All modules are addressable but not found during initial start up.
- sporadic communication lost occurs

Operation modes of the line check

The BACS Line Check offers two basic functional checks.

- Send Line Check
- Receive Line Check

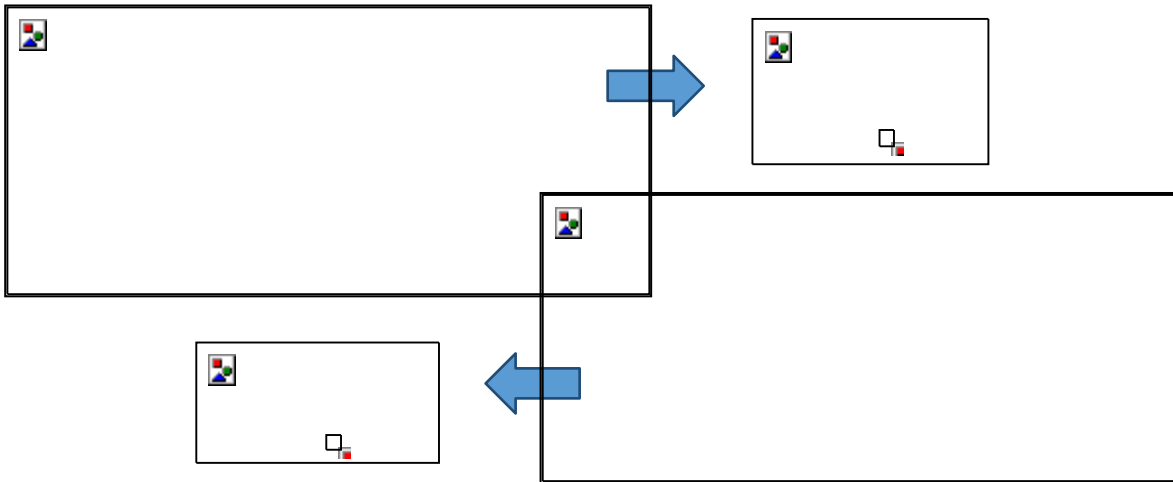
Note

For the line check tool, it is mandatory that all modules are set to factory default ID 0.

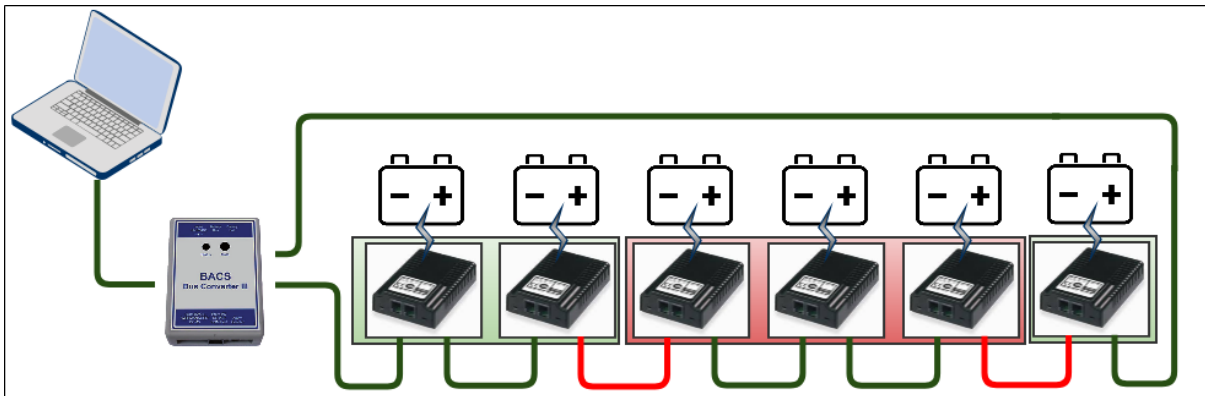
How the send line test works

The Send Line Check is a test procedure in which all modules are addressed via a broad cast signal, starting from the BACS BUS Converter.

As soon as you start this test, the Send Line Check specifies a current state that the LEDs on the BACS modules should show:



Modules that do not adhere to this guideline can be found easily. If several faults are found within a ring cabling, the outermost fault as well as a non-responding module chain is visible:



in this example, the red marked modules will show connection problems - everything between the broken cables will not be reachable. With this test, one can narrow down the sources of error, but do not clearly determine the reason for this problem. It may be...

- a broken cable
- a broken module port
- a broken port of the module before the error
- a broken module itself

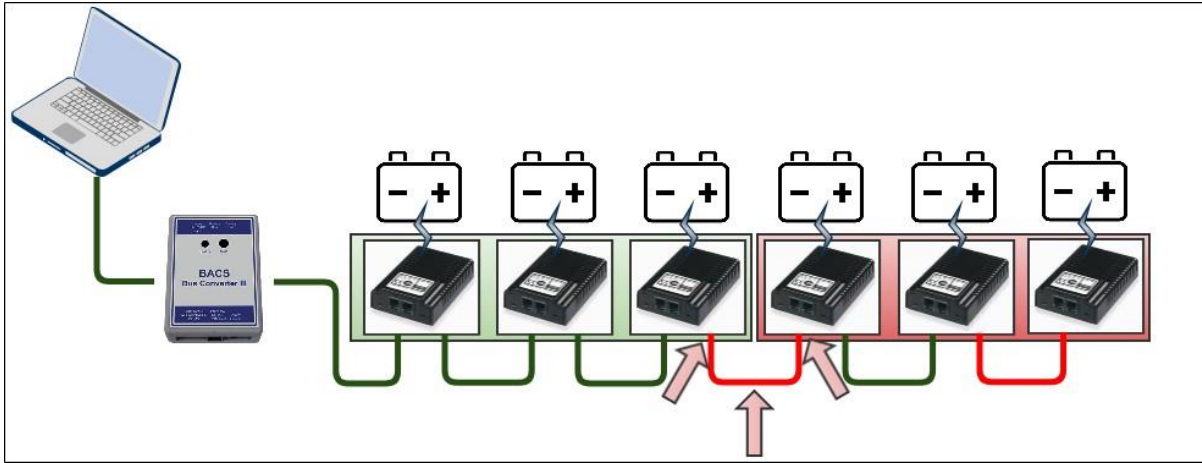
The disadvantage of ring cabling while running this test, is the fact that a defective BACS module would immediately attract attention, but a single defective cable or a BACS module with a defective cable socket cannot appear. you need at least a completely broken module or two "half-broken" parts to find an issue:

By a single cabling defect, the redundancy behavior of the ring cabling would inevitably find all modules in the query.

What you can do

You can perform a redundancy test on known defects and determine a general availability of all modules. By contrast, the same test running on a simple wiring:

You would only reveal the first problem inside a BACS string.



Again, you need to check whether the reason for the error can be found at the modules or the bus cables. This test reliably detects weaknesses inside an installation and will find all problems. The disadvantage is, you will always find only one problem after the other - this can take a long time.

Note

Both tests have their specific advantages and disadvantages. The send test coming with a ring cabling will show the general behavior and conveniently, but can only be used to find failures moderate system failures as well as broken single modules. The same test coming with a simple cabling method without a ring topology can then be used to find all problems but only the first issue in a row.

In combination, technicians can first ensure basic operations and guarantee basic availability.

The Receive Line Test

While the Send Line test will take care for general availability of modules and helps to find cabling issues, the Receive Line Test will take care for the quality of the data signal that will reach the BACS Bus Converter:

In some cases, the cabling is well done, but the communication does not start or interrupts sporadically. This may cause as an example by strong electromagnetic interferences: EMI – In this case, the signal itself will be compromised by electromagnetic fields that will harm the conductor inside the cable and produces error bits that cannot be compensated. With the receive line test, you can take a look what happens if the last module far away from the BACS Webmanager will send a data package.

Preconditions of the test

Please note that all modules must use the ID "0"! Otherwise this test will not work properly. If in doubt, use the Automatic Mode to set all modules to the ID "0" in advance. After resetting, proceed to the receive line test



Starting the Receive Line test

The receive line test is a passive testing mode. The BACS Programmer will not query but wait for a specially coded incoming data packet.

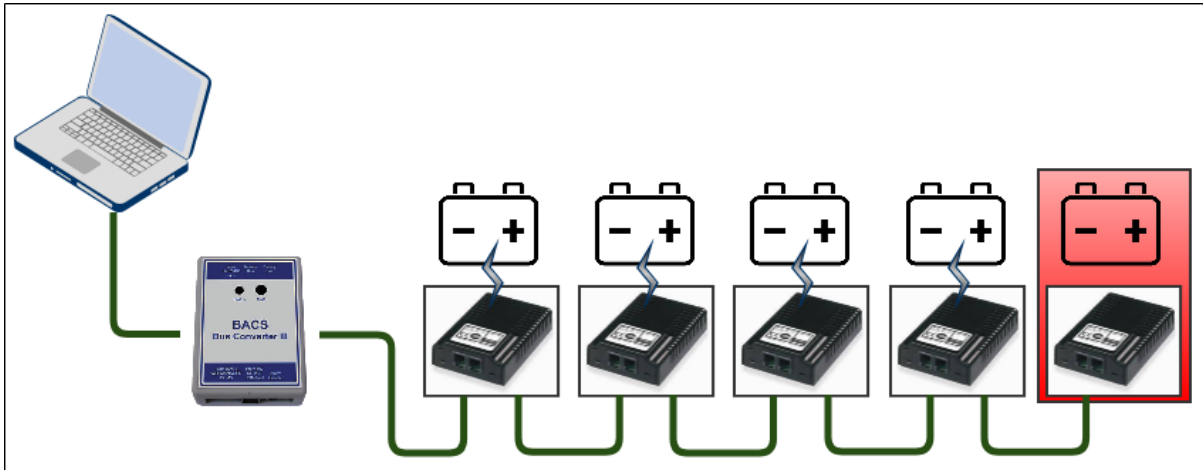
When you start the test, you will not see animations or something like that, BACS programmer will only show a blue center screen with white letters:



Performing a Receive Line Check

Because you want to know something about a specific route to the BACS programmer, this test will only run with a simple chain connection without any ring wiring.

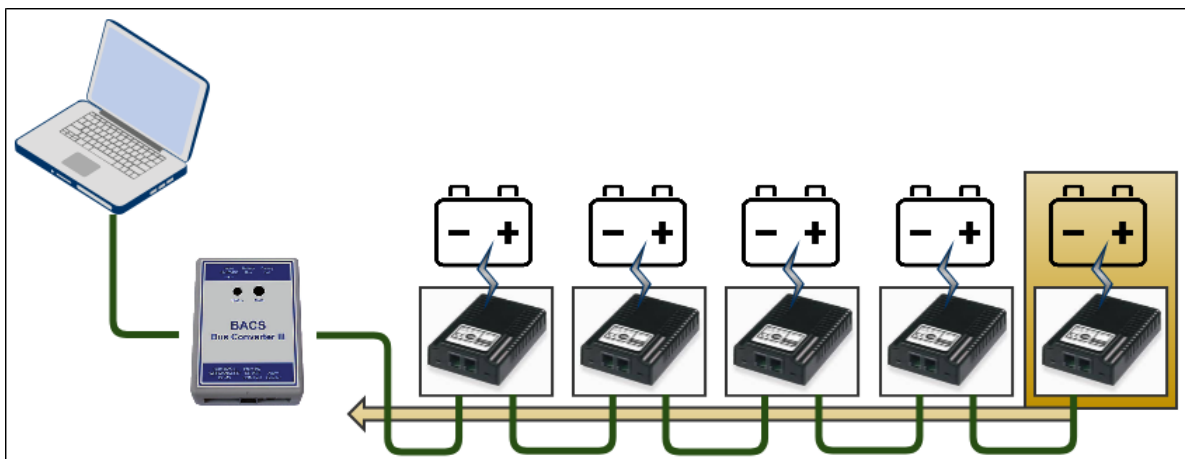
1. To start the test, unplug the measuring cables to depower the BACS module.



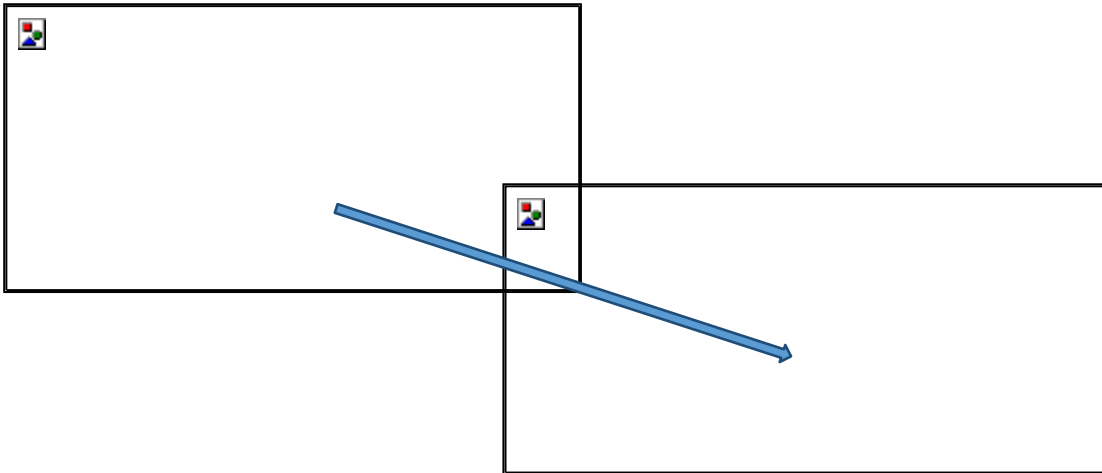
2. Press the button (yes dude, this is not the LED ...) and hold it.
3. Repower the module while holding the module button pressed.
4. Release the button. This will start the test.

What happens:

This BACS module will start sending 300 signatred data through the cables to the BACS Webmanager or a BACS Bus Converter. This will be done sequential and evenly.



The BACS programmer will notice this incoming data packets and show the number signature:



Due to the fact the data packages are signed with a unique number, it is possible to examine the quality of the data signal. In case the data packet is broken or invalid, it will be rejected.

Due to the fact you will notice following:

- The counter does not start, the screen is blank

In this case, no incoming data packets are noticed. If the send line test works as expected, please check if all modules are at default ID 0. Most common problem: Starting this test is a little bit tricky – you need to hold the button while inserting the measuring cables to repower the module. When you release the button, the test starts. If the test does not start, you cannot receive data packets.

- Jumping numbers

Yes, the test started and the last module inside the chain sends his 300 data packets. In this case there are missing or broken data packets. These packets are lost and will show, in general it may work but there is something wrong inside the cabling. To find the reason why, you may spit the bac modules in two different strings and repeat the test until all numbers will be shown evenly.

- It starts counting evenly, but it suddenly stops.

This means, the chain is interrupted physically or something will block all data packets.

- It runs as expected

The numbers will be shown evenly and the countdown starts at 299 and stops with 0. Data quality is OK, all modules will respond.

Since the data packages are signed, a fault in the data line can be diagnosed very quickly because the display window counts irregularly or displays jumping numbers. If the meter stops at a number, it can be assumed that the data connection has collapsed.

Note

This test starts only if the trigger timing on the last BACS module is consistent. If the test does not start, first make sure that the test was triggered correctly. Otherwise, the Receive Line Check will indicate a fault in the BACS cabling.

GX_R_AUX

The GX_R_AUX is the digital BACS version of the former CON_R_AUX for the CS121 series, which can be connected directly to the CS141. This device offers switching relays as Output and dry contacts as Input to connect external devices to the BACS/CS141 system.

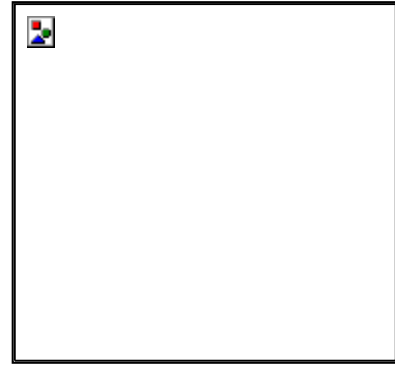
The overall configuration process is similar, but the GX_R_AUX provides some advantages like the option to integrate up to 4 of these devices into one BACS bus - this will allow up to 16 inputs and outputs in total.

Due to the fact they are freely configurable, that can be used to switch and monitor many functions including other systems.

The GX_R_AUX devices are designed to be used a modular. They do not need to be installed all together at a single place - Install or move them during maintenance work anywhere within the installation inside the BACS bus.

Due to the fact the GX_R_AUX is supplied with the necessary operating voltage via the BACS bus cabling, there are no further live cables that need to be installed separately*.

Thanks to the modular concept, the GX_R_AUX is an optional accessory to extend the scope of functions and activities of your BACS installation by many additional possibilities and can be used for both – the BACS installation as well as advanced CS141 configuration to communicate with child- and parent surveillance and monitoring systems as well as to trigger and monitor third-party devices. All you need to do is to put the GX_R_AUX to its own little BACS strain.

**Note**

The GX_R_AUX makes it possible to configure battery systems according to the US standard "International Fire Code IFC 608.3". This standard defines, in case of a malfunction in coming with a possible impending Thermal Runaway threat, the batteries have to be completely isolated automatically. The use of the GX_R_AUX allows activation of battery separators and thus meets the requirements of the US Standard International Fire Code IFC 608.3. In case of an impending Thermal Runaway, the GX_R_AUX can trigger

battery separators or send an opening signal through alarm contacts in order to disconnect the battery system from the charger so the batteries cannot heat up anymore.

**) For more information, please refer the BACS FAQ at the end of this manual.*

Connectors

Screwed Connections 1-14:

Ports 1-14 are located on the side marked as input. Port 1 is located on the left side when viewed directly from above.



Screw terminal layout pins 1 - 14

1. Reserved for future developments.
2. Reserved for future developments
3. Digital Input 1
4. +12V (voltage for input 1)
5. Digital Input 2
6. +12V (voltage for input 2)
7. Digit input 3
8. +12V (voltage for input 3)
9. Digital input 4
10. +12V (Versorgung für Eingang 4)
11. Alternative BACS bus +12V voltage
12. Alternative BACS bus data input
13. Alternative BACS bus data output
14. Alternative BACS bus ground

Pin 11 – 14: Alternative BACS Bus

In some cases, it may be necessary to connect BACS devices directly via contacts. To provide this additional function, ports 11 to 14 can be used in case of the device is not connected to the BACS bus via the "BUS 1" or "BUS 2" plug.

Center console

The address switch: The DIP bank "Address"



In contrast to the BACS modules, the GX_R_AUX must be configured to its own ID. This will be done via the DIP switches.

The following DIP settings are valid:

DIP 1	DIP2	DIP 3	DIP3	GX_R_AUX device ID
off	off	off	off	GX_R_AUX will be set to ID 1
ON	off	off	off	GX_R_AUX will be set to ID 2
off	ON	off	off	GX_R_AUX will be set to ID 3
ON	ON	off	off	GX_R_AUX will be set to ID 4

Please note that the ID, like a BACS module, requires a unique ID, which must be set consecutively starting with ID 1. The difference to the BACS module is that the GX_R_AUX ID is set directly via the DIP bank and can not be managed via the BACS Web Manager - whereby the base address range used differs from the BACS modules.

Therefore, the BACS module with the ID 1 cannot be confused with the GX_R_AUX ID 1.

Connecting the GX_R_AUX to the BACS Bus

The GX_R_AUX can be used everywhere inside a BACS bus - Simply connect the module between two BACS modules. The GX_R_AUX fits seamlessly into the BACS bus and can be used immediately.

Output connectors

Screwed connectors 15-28

The ports 15-28 are on the side marked as output. Terminal 15 is in direct view from the top on the left side, in opposition to input 1.



Screwed connectors 15 - 28

- 15. Relay contact 1 No*
- 16. Relay contact 1 NC**
- 17. Relay contact 1 Common
- 18. Relay contact 2 NO*
- 19. Relay contact 2 NC**
- 20. Relay contact 2 Common
- 21. Relay contact 3 NO*
- 22. Relay contact 3 NC**
- 23. Relay contact 3 Common
- 24. Relay contact 4 NO*
- 25. Relay contact 4 NC**
- 26. Relay contact 4 Common
- 27. Relay contact zukünftige Entwicklungen
- 28. Relay contact zukünftige Entwicklungen

*NO: normally open contact

**NC: normally closed contact

Note

If the labels and labels have been removed, you can still clearly identify the numbering of the screw terminals based on the position of the LEDs: On one side you have 5 LEDs - 4 grouped and one separated. The separate LED is the status indicator.

Align the GX_R_AUX in a way that the 5 LED's are in the upper side.

From now, you can easily numerate the terminals you are looking for:

The upper screw bar is numbered from left to right in ascending order, the first connection on the left outside defines 1. Furthermore, the upper bar defines the input bar.

The DIP switches are numbered from left to right in this orientation, from left to right: 1, 2, 3, 4

The bottom screw bar starts on the left side with the number 15 and is incremented to the right continuously. the bottom screw bar defines the outputs

GX_R_AUX Configuration guide

For this configuration step, navigate to the following menu:

**Step 1 - Setting up a mandatory GX_R_AUX ID**

Set up a corresponding ID - the ID's you choose hast to start with 1 and ends with a number according to the number of GX_R_AUX you wish to use. Please note the following conditions:

- An ID may only be assigned once
- The first device receives the ID 1, then it is consecutively numbered
- Do not use more than the maximum of 4 GX_R_AUX within one BACS installation.

Step 2 - At BACS Webmanager, open the GX_R_AUX configuration dialog

In the configuration dialog, you can use the BACS Webmanager to specify the number of installed modules:



Enter "0" to disable the function. Otherwise, set the number of used GX_R_AUX modules and click Apply. Due to the fact new devices have been added to the BACS bus, the web manager must reboot BACS to find and initialize the new devices accordingly. This procedure will only restart required services, neither the Webmanager itself nor the UPS will reboot.

Note

The BACS Webmanager will program the ID of a GX_R_AUX - the ID will be set by the DIP switch bank. After setting up the hardware ID of the GX_R_AUX, the Webmanager will be configurated to search for the specific number of GX_R_AUX that are placed inside the BACS installation. If the estimated number of GX_R_AUX is not found, a corresponding error message will occur.

You can follow the success of the initialization in the upper task bar.



How to set up the outputs of a GX_R_AUX as battery breaker

Under Thermal Runaway, activate the battery breaker functionality

Before configuring the GX_R_AUX outputs and associated events, you need to decide if and how many battery breakers you need. Open the Thermal Runaway configuration dialog - the battery breaker configuration is mostly done automatically, which manifests itself in subsequent configurations:

1. According outputs will be labeled automatically
2. Events and jobs assigned to a Thermal Runaway are automatically entered

The total number of required battery breaker depends on the number of strings you configured at BACS general setup.



If you want to use one battery breaker for the complete installation, select the option *Trip single Battery-Breaker for all strings*.

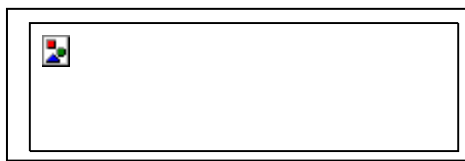
If you want to use a single battery System, select the option „Trip separate



breaker for each string installed in your BACS Battery-Breaker for each string

Press *Apply* when ready.

Under Setup GX R AUX, you will find new entries:



As you can see, BACS auto-labeled your GX_R_AUX Outputs according to your settings. You cannot re-label them - they are reserved for the battery breaker. Please note: If you use battery breaker, ensure, the NC Contact Flag is not set!

Again, press *Apply* when ready

How the BACS Webmanager will count the battery breaker:

The first battery breaker will be associated with output 1. From there onwards, all battery breaker will be counted one by one. If several AUX are in use, the 5th battery interrupter is configured on the 2nd AUX, Port 1. The classification as battery breaker will exclude any existing configuration - the configured output can only be used for the according battery breaker. Furthermore, depending on the number of GX_R_AUX devices, an individually configured additional configuration dialog will appear:

Name the inputs and outputs in free text. These labels can be found next to the inputs and outputs at the GX_R_AUX - Monitor:

GX_R_AUX Status						
GX_R_AUX 1						
Input	Name	Status	Output	Name	Status	
1	test	●	1	Trip Battery-Breaker String 1	<input type="radio"/>	Switch On
2		●	2	Trip Battery-Breaker String 2	<input type="radio"/>	Switch On
3		●	3	Trip Battery-Breaker String 3	<input type="radio"/>	Switch On
4		●	4		<input type="radio"/>	Switch On

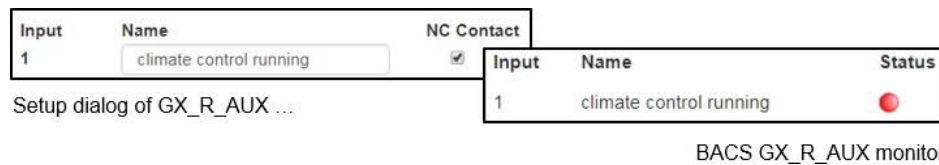
Normally Open / Normally Closed

If you do not use battery breaker you may use the outputs freely. Depending on your settings, the behavior of the BACS Webmanager changes when dealing with contacts:

NC / NO input configuration

The inputs provide to connect any potential-free switch contacts. It can be distinguished whether a contact must normally be closed (NC) or open (NO). By Changing from NO to NC behavior, it is possible to harmonize the contacts to third party devices.

A switching state in opposition to the configuration is provided with a red alarm marker:



In this case, the climate control will close the contact if running. Otherwise the Status is marked red – the climate control is off.

NC / NO output configuration

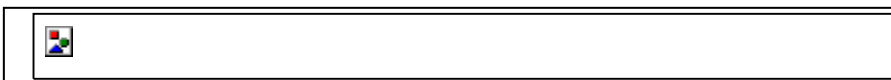
The outputs can be assigned via the terminal strips 15-26. This option defines if a contact is generally closed and needs to be opened or open and has to be closed. During the BACS initialization, the switches automatically take the correspondingly configured switching states.

Please note:

A NO - normally open - contact is open at system startup and **must be closed / turned on** accordingly:



An NC - normally closed - contact is closed at start up and **must be switched to off / open** accordingly



Depending on the configuration, the marker is green (active) or grey (disabled).

Defining jobs to GX_R_AUX input events

BACS use a stand-alone event and job management.

This allows to use a BACS system completely without a UPS connection in stand-alone operation and use its own sensors.

To define a job, open the events menu in the BACS configuration menu and search for the following entry:

>	<input type="checkbox"/>	+	<input type="checkbox"/>	BACS GX_R_AUX 1 Input 1 Alarm Off	3	1	0	1	0
>	<input type="checkbox"/>	+	<input type="checkbox"/>	BACS GX_R_AUX 1 Input 1 Alarm	3	1	0	1	0
>	<input type="checkbox"/>	+	<input type="checkbox"/>	BACS GX_R_AUX 1 Input 2 Alarm Off	3	1	0	1	0
>	<input type="checkbox"/>	+	<input type="checkbox"/>	BACS GX_R_AUX 1 Input 2 Alarm	3	1	0	1	0

BACS GX_R_AUX 1 defines the module assigned with the ID 1 via the DIP bank. If you have more modules in use, they will be listed automatically as AUX 2, AUX 3, and AUX 4 inside the event menu.

The current alarm ON/Off state will be determined by NO / NC contacts definition at GX_R_AUX setup. At the event handling, it is possible to configure what will happen at the current contact state.

Note

The word "alarm" itself is relative meaning in this context. You can also communicate with other devices through the inputs and, for example, get switching confirmations - you are not forced to use this as an "alarm" notification.

Setting up a job

In this example, a log entry job is set to Input Port 1.

To enter a new job, select **+** at Input 1 Alarm – this will open the job configuration dialog:

1. As Job, choose „Log -“:

The screenshot shows a dialog box with a label 'Job' and a dropdown menu. The dropdown menu is open, showing 'Log' as the selected option.

With the job type, the parameters will be adapted automatically. In this case, you can type a free text messages that will appear at the event log if GX_R_AUX 1 input port 1 reports a closed alarm contact position:

The screenshot shows a dialog box with a label 'Parameter' and a text input field. The text input field contains the text 'Input 1 contact set to closed position'.

Timing will allow to define when this job shall be executed. In this case, the job is executed once, at the precise moment when the defined alarm behavior occurs. For more information, please refer to the chapter event handling at part 1 of this manual.

The screenshot shows a dialog box with a label 'Timing'. It has five radio button options:

- Immediately, once
- After [] seconds
- After [] seconds, repeat all [] seconds
- After [] seconds on Battery
- At [] seconds remaining time

With save, the job will be written to the configuration file and executed as soon as the according event occurs. You do not need to restart the CS141 / BACS Webmanager.

Checking the job configuration:

To test the job, unfold the event *BACS GX_R_AUX 1 Input 1 Alarm* by clicking 

Your new job will be displayed:

The screenshot shows a menu item with a small icon on the left and a large empty rectangular box on the right, representing the configuration area for the selected event.

At this menu, you can edit, delete or test the job. More information can be found at event handling configuration in part 1 of this manual.

Communicate with third party devices via GX_R_AUX outputs

In this example, a third-party monitoring device shall be triggered by AUX output port 1.

1. Choose the event that shall trigger the output and press **+** to start the job configuration dialog
2. As job, choose AUX:

The screenshot shows a dialog box with a label 'Job' and a dropdown menu. The dropdown menu is open, showing 'AUX' as the selected option.

Depending on the number of installed GX_R_AUX modules, you can select an individual port from the list: In this example, GX_R_AUX 1, Port 3 is selected.

By doing so, use at GX_R_AUX output screw bar these screw connectors:

- 21 Relay contact 3 NO*
- 22 Relay contact 3 NC**
- 23 Relay contact Common

The wiring method determines what will happen in case of the command „Set High (On) -“:

NO <-> Common
 NC <-> Common

On trigger, the contact will be closed
 On trigger, the contact will be opened

The standard configuration for these contacts is NO <-> Common. For this example, Port 3 will be closed as soon as the according event will occur.


Parameter	
Port Number	GX_R_AUX 1, Port 3
Command	Set High (On)

Timing will allow to define when this job shall be executed. In this case, the job is executed once, at the precise moment when the defined alarm behavior occurs. For more information, please refer to the chapter for advanced event handling at part 1 of this manual.

Timing	
<input checked="" type="radio"/>	Immediately, once
<input type="radio"/>	After <input type="text"/> seconds
<input type="radio"/>	After <input type="text"/> seconds, repeat all <input type="text"/> seconds
<input type="radio"/>	After <input type="text"/> seconds on Battery
<input type="radio"/>	At <input type="text"/> seconds remaining time

With save, the job will be written to the configuration file and executed as soon as the according event occurs. You do not need to restart the CS141 / BACS Webmanager.

Checking the job configuration:

At the according event, click  to unfold the job list configured to this event:

The new job should be added accordingly:



From here, you can edit, delete and test the job. Results can be seen at the GX_R_AUX monitor as well as event chains may be triggered.

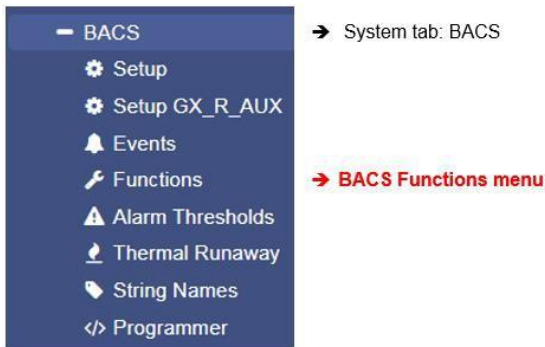
Note

For the complete description of event handling including all symbols, please refer to page 58 of this manual, chapter:

System event handling

BACS Functions

For this configuration step, navigate to the following menu:



Each BACS Webmanager offers basic functions that can be switched on or off remotely via the web interface.

BACS Buzzer

This internal alarm provides a clear audible warning signal as soon as there is a problem with your BACS system or the connected sensors occurs or in the case of a so-called General Alarm.

As a default, the buzzer will be triggered in case of the event „BACS General Alarm -“.



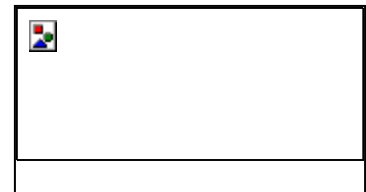
BACS Relay

Parallel to the alarm buzzer, BACS provide an internal relay:

With this relay external monitoring systems can be informed that something went wrong. The internal BACS alarm relay is linked to a general alarm and cannot be configured:

The relay is a pre-defined normally closed contact, which automatically picks up about 15-20 seconds after system startup and is only reopened in case of a system fault:

1. A BACS General Alarm is in progress
2. The BACS Webmanager or BACS Bus Converter is depowered.



Master alarm will start, if ...

- Voltage alarm high/low,
- Temperature alarm high/low
- Impedance alarm high/low
- Communication lost to one or more modules or a system alarm is in progress
- Thermal Runaway alarm
- Equalizing / Balancing Error alarm
- String voltage alarm

Note:

If you manually open the relay, it remains open until one of the following conditions is met:

- The device restarts (by rebooting via software button or in case of a cold boot).
- An active BACS-alarm falls back to normal state (voltage measurements reach alarm levels and drops below).
- It will be closed via BACS relays functions menu.

BACS alarm thresholds

In principle, there are two points during usage, that may heavily damage the batteries of a UPS system:

Overvoltaged batteries

The overvoltage occurs if a UPS initiates a boost charging cycle to restore emergency power time as fast as possible after a discharge. As an example, the charging process will be done with a boost charge or operates with predefined charging voltage.

In both cases, the reference charging point is the slowest loading battery to rule the entire charging process.

As result, normal or fast charging batteries are consequently overcharged, leading into average temperature issues and as a long-term consequence, overcharging the cells in the battery are damaged through the dehydration process coming with abnormal temperature usage. Overcharging will damage the battery, but this is not enough:

As a consequence of an overcharge, a battery will heat - this may lead into a dangerous battery overheating and fire issue. Conversely, a battery damaged by overvoltage can subsequently not meet the requirements set, which leads to different behavioral characteristics:

- Extended loading time
- Permanently performance decrease
- Temperature increasing with each charge/discharge cycle
- Sporadically dropping below the discharge end voltage
- Lapsing service time

- Overheating and acute fire hazard.

Which defects occur exactly depends on the type of battery as well as the basic conditions. Overloading should, if possible, be avoided for these reasons.

Deep discharge

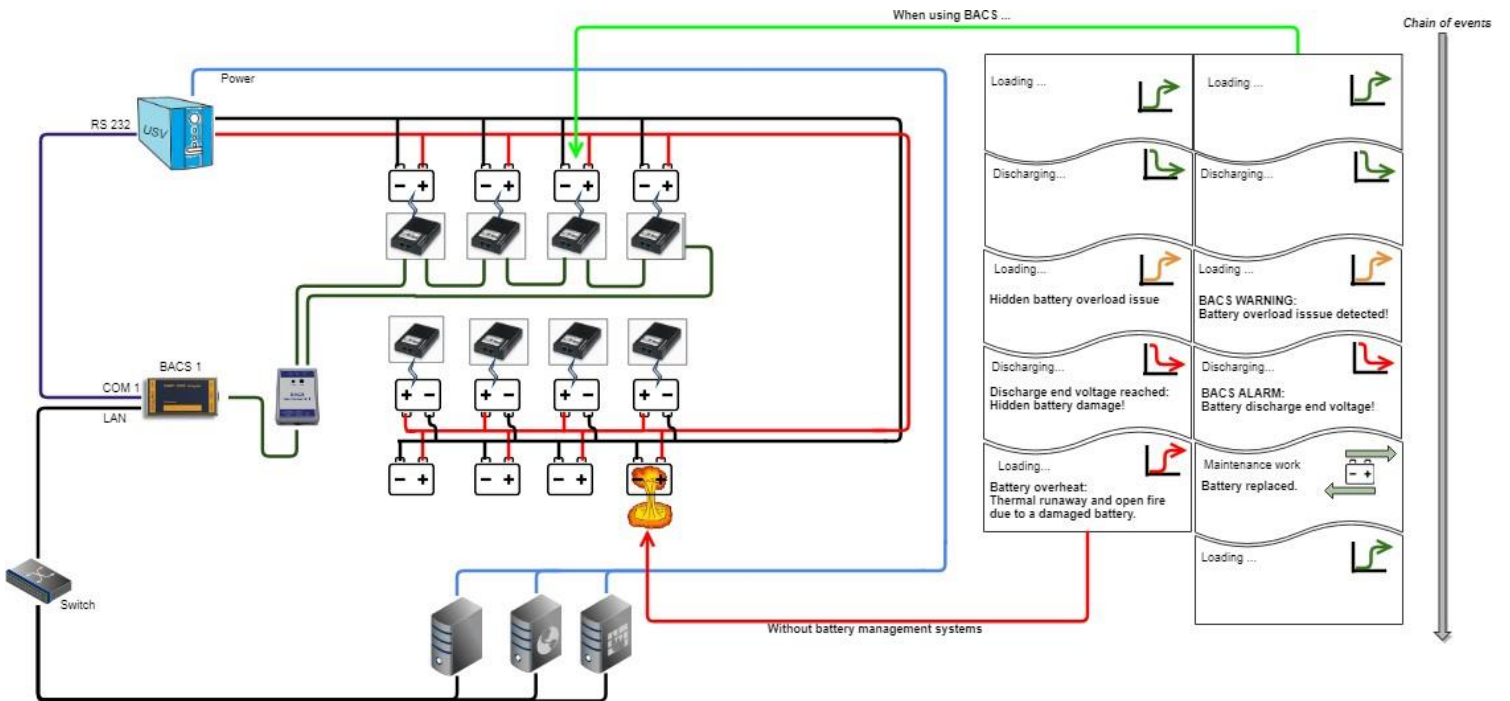
During deep discharge, a cell of a battery is discharged during use until a complete depletion. In case of a deep discharge, the voltage drops below the final discharge voltage, a condition in which a wide variety of defects may occur. Depending on the type of battery even a single deep discharge can damage the battery internally so that it can lead into a total failure or even a polarity reversal of the battery contacts.

Reloading damaged battery can be very dangerous because the reaction to the charging current unpredictable:

Although the battery is faulty, it initially appears to be responding normally to the charging process initiated by the UPS - a creeping malfunction can appear up to 16 hours after charging is complete. Everything may happen, starting at an acute overheating when starting or during charging process as well as a seemingly sporadic phenomenon during charging that leads creeping into a fire issue many hours later.

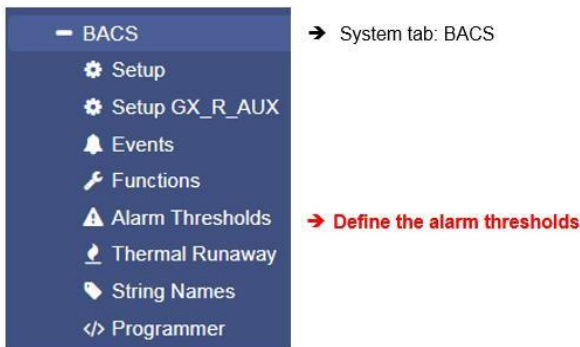
Note

Typically, a UPS will stop operating in time to avoid this deep discharge, but overvoltage or undervoltage that weaken the cells, cannot be detected the UPS.



Threshold definitions

For this configuration step, navigate to the following menu:



The BACS thresholds define fixed points within the charge / discharge cycle where intervention becomes necessary before an acute incident arises.

The following values are monitored during the discharge / charge cycles:

Warning Levels		Min	Max	
Voltage	<input type="text" value="10,5"/>	V	<input type="text" value="14,1"/>	V → Battery voltage
Temperature	<input type="text" value="10"/>	°C	<input type="text" value="30"/>	°C → Battery temperature
Impedance	<input type="text" value="1,2"/>	mΩ	<input type="text" value="40"/>	mΩ → Internal resistance of the battery
Enable Max. Voltage Difference	<input checked="" type="checkbox"/>		<input type="text" value="0"/>	V → Voltage deviation between batteries
Baseline Impedance	<input type="text" value="25"/>	%		% → Baseline Impedance in %
Enable String Thresholds	<input type="checkbox"/>			
String Voltage	<input type="text" value="0"/>	V	<input type="text" value="1000"/>	V → Voltage deviation between battery strands
Enable Current Thresholds	<input type="checkbox"/>			
String Current	<input type="text" value="-10"/>	A	<input type="text" value="10"/>	A → Current deviation between the battery stands

Battery voltage

The voltage measured by a battery during the charge / discharge cycle indicates whether the battery will soon become overcharged or will run into a deep discharge. These values may differ depending of the specifications made by the battery manufacturer. In case of the measurements exceed or drop below the pre-defined values, a warning will be issued.

Please note, the limits specified by the BACS are correct for most batteries and should only be changed after consultation with the battery manufacturer.

Battery temperature

The temperature of a battery will influence the performance and the life of a battery. A battery will heat up during the charge and discharge cycle. However, if the temperature exceeds the limits, it may lead into different defects. How and when these defects will manifest, depends on the type of battery.

Internal resistance of the battery

Depending on the design of the battery, the internal resistance changes, in some cases it increases abruptly, in other cases it drops abruptly. In case of using new batteries, measured values of the internal resistance should always be equal at all batteries. Thereby the measured value is determined by its carrier material - the type of battery. This means, a deviation of the internal resistance to other batteries indicates a battery fault.

Why not using voltage measurements?

The voltage is not suited to be used as an indicator for battery failure, because measured voltages of the battery reacts and follows during a trickle charge the voltage behavior of the charger. With internal resistance (and the indicator for equalizing) measured values will indicate a problem of the batteries' chemistry and thus allow to warn in case future problems can be assumed.

The internal resistance of a battery indicates upcoming problems and should be used for long term monitoring.

For warning level, we recommend 25% deviation from the average value of all batteries.

For alarm levels, we recommend 50 % deviation from the average value of all batteries.

Attention:

Each battery manufacturer uses an own measuring method to get the impedance values for a data sheet. As a consequence, it is possible that taking impedance values from the battery manufacturer's data sheet is not suitable to configurate BACS thresholds:

To ensure save operation, determine impedance values for BACS as described in this manual.

Maximum Voltage deviation between batteries

Batteries must be used regularly, the charge / discharge process is very important for optimal operation.

Despite equalizing / balancing, an unused battery loses its target voltage over time, although it receives a trickle charge from the UPS. This is a natural process and not a malfunction:

If the fluids in the battery come to rest, gravity affects the fluids inside the battery:

Basically, liquids of different molecular weight in a standing system tend to be arranged according to their molecular weight over time. The heavy liquid slowly sinks down while the light liquid migrates upwards. As a consequence, the overall concentration ratio of liquids changes, which impairs the efficiency. How much this natural process will take effect, depends strongly on the chemicals used as well as the size of a battery - as bigger the battery as stronger this phenomenon will take effect.

The target voltage can be normalized by regular battery use due to the fact the chemical processes cause a circulation and even distribution of all chemicals. The BACS Webmanager can measure the deviation in 0.1-volt increments and give an indication if the measured voltage and the target voltage are too drifting apart.

Voltage deviation per string

This feature is similar to comparing individual BACS voltage measurements. However, this function compares the individual strings within a BACS installation.

Current deviation per string

Unlike the voltage, the charging current divides evenly into the different strings - but the total current will not change. Since all battery strings work evenly in the network, defects in one string will have a negative impact on all strings. BACS can be advised to measure this effect and give feedback to technical staff.

Please note, this setting requires current sensors on each string

Note

What is the difference between warning and alarm?

BACS distinguish between a definitive alarm that requires intervention and a warning:

Both states are quite similar, the different jobs can be freely defined for the corresponding warning or alarm level. Depending on optional parts and devices attached to BACS as well as the configuration, very delicate automatic processes can be initiated, ranging from information to the initiation of active emergency measures up to switching and controlling of systems, etc.

In the event of an alarm condition, the acoustic alarm is additionally activated, the alarm LED changes its status and the alarm contact on the BACS Webmanager is actively opened.

The values are freely definable, but care should be taken to ensure that the values for the warning are always reached well in advance of the values for an alarm so that there is still enough time for an adequate response.

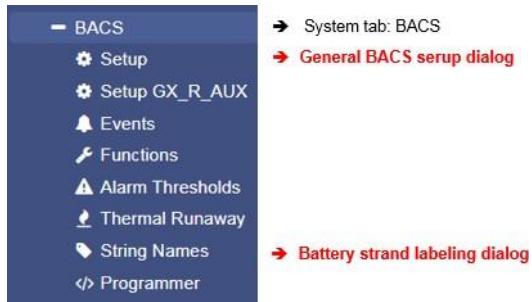
Alarm Delay

As a consequence of a used emergency power or an extended battery test, battery voltage is in low condition. If the UPS takes the maximum time for autonomous operation, it possible that the minimum values for the BACS alarm will be triggered.

This option allows to set up an alarm time delay to prevent BACS from sending a false alarm.

Define BACS Battery strings

For this configuration step please navigate to the following menus



BACS offers the logical assignment of the individual batteries to so-called Battery strings.

The number of batteries is divided by the number of specified strings. The result is the logical assignment of the BACS module in single strings.

Example:

They have 72 batteries and define 6 single strings. The BACS system will present you with 6 battery strings of 12 batteries each, as entered after initialization. Basically, the assignment is made according as followed:

72 batteries divided by 6 strings will take 12 batteries per stand

Batteries 1 - 12	String 1
Batteries 13 - 24	String 2
Batteries 25 - 36	String 3
Batteries 37 - 48	String 4
Batteries 49 - 60	String 5
Batteries 61 - 72	String 6

After initialization, you will notice that BACS has renamed the modules:

If you have successfully included module 49, it would now be listed at battery strings 5 as module 1.

Note

The ID of the module has not changed, it remains the BACS module with the unique ID 49. What changed is the display context at the monitoring screen as well as general presentation of the data. Usually, the installation site and the string are coordinated so that module and string accordingly fit together.

If no project documentation exists, you can use this to identify the individual strings and search via the BACS Programmer.

Please note: The numbers of current sensors will be defined by the number of strings you define and label. You cannot define a specified number of current sensors, but you can:

- Use a current sensor for each single BACS string
- Use one current sensor for all BACS strings if installed at the master string
- Use one current sensor installed in one single string and use the multiplicator to get information about all strings

BACS strings vs battery breaker

Furthermore, setting up BACS strings will harm the battery breaker setup:

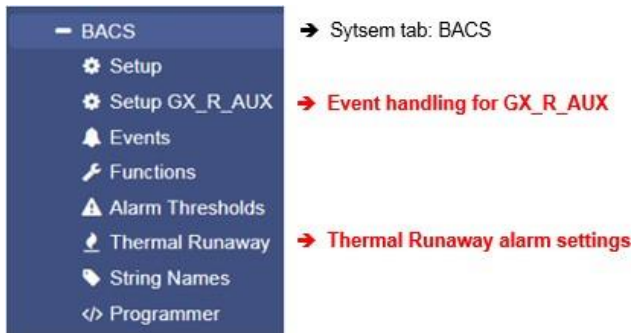
The BACS Webmanager offers two options:

- One battery breaker for all strings
- One battery breaker for each string

Please note, depending on the number of strings, you may need up to 4 GX_R_AUX modules. The maximum number of battery breaker is 16.

Thermal Runaway

For this configuration step, navigate to the following menu:



A "Thermal Runaway" is one of the most dangerous events that can happen when using battery systems:

The battery overheats. This incident leads into trouble with unpredictable effects:

Overheated batteries can expel explosive, corrosive, or oxygen-displacing gases, catch fire, explode as well as damaging neighboring batteries. Furthermore, battery caused fire also contains toxic and unpredictable mixture of chemicals, whose combustion gases, in addition to special extinguishing agents, make special protective clothing indispensable.

For this reason, some countries all around the world require in case of clear signs for a beginning thermal runaway, the batteries can be completely separated from the UPS or the battery charging system.

How to configure a thermal runaway

For this step, the following pre-conditions are mandatory:

1. The number of batteries is configured
2. The number of battery strings is configured
3. Ideally, the strings are named
4. All BACS modules are registered, found and BACS is initialized and running.
5. Battery breaker are installed
6. GX_R_AUX are installed and ready to use

Open the tab „Thermal Runaway“ :-

At first, define the condition a BACS Webmanager shall assume a Thermal Runaway:

Max. Module Temperature Difference	<input type="text" value="20"/>	°C	→ temperature difference between BACS modules
Optional: Max. Current per String	<input type="text" value="10"/>	A	→ Current difference between strands*
Optional: Above Conditions Are True Since	<input type="text" value="30"/>	Minutes	→ Reference time: above should be fulfilled*

* Additional options based on the configuration and hardware-level of your BACS system

Max. Module Temperature Difference

Problems usually indicates in dramatic temperature increasments of individual batteries. The BACS Webmanager therefore measures the temperature of the individual batteries on each module.

This results in a basic statistical value from which individual batteries can deviate.

If boundary conditions are met, there is a clear indication of a thermal runaway. Depending on the hardware constellation, the protection circuitry physically disconnects affected string or all batteries from UPS / battery charger.

Max Current per String

Optionally, an additional conspicuousness can be included in the thermal runaway detection as soon as each string can use its own current sensor. Via the current sensor, a deviation of individual strings in relation to other strings can be measured:

Ideally, the strings are evenly loaded and unloaded. Irregularities and short-term deviations are familiar phenomena when dealing with batteries, large and long-term deviations are an indication of a broken battery, endangered for leading into a thermal runaway...

Above Conditions Are True Since

This feature defines timer that must be expired before the BACS Webmanager considers a thermal runaway is proven. Among other things, this feature can be used to calculate local peculiarities and roughly predictable environmental influences.

When finished with configuration, open the GX_R_AUX configuration dialog

Your settings changed the entries and fixed them to a special functionality:

GX_R_AUX 1					
Input	Name	NC Contact	Output	Name	NC Contact
1	Warpkern	<input type="checkbox"/>	1	Trip Battery-Breaker String 1	<input type="checkbox"/>
2	Materie Injektor	<input checked="" type="checkbox"/>	2	Trip Battery-Breaker String 2	<input type="checkbox"/>
3	Antimaterie Injektor	<input type="checkbox"/>	3	Trip Battery-Breaker String 3	<input type="checkbox"/>
4	Magnetische Eindämmung	<input checked="" type="checkbox"/>	4	Captain Picard fragen...	<input type="checkbox"/>

Apply Cancel

All you need to do is the definition whether the battery breaker you are using are Normally Open (NO) Contacts or Normally Closed (NC) contacts. Due to the fact, both concepts are in use, BACS cannot know which type of battery breakers are currently in use.

Open BACS event handling and search for BACS thermal Runaway String 1, 2 and 3 and unfold them:

Job Type	When	Parameter
Log	Once, immediately	{"text":"BACS Thermal Runaway String 1"}
RCCMD Trap	Once, immediately	{"text":"BACS Thermal Runaway String 1 in #LOCATION"}
Email Trap	Once, immediately	{}
AUX	Once, immediately	{"port":"100","on_off":"1","text":"BACS Thermal Runaway String 100"}

The BACS Webmanager automatically added an AUX-Job to switch the battery breaker.

Press the test button to check whether the battery breaker will be triggered and opens accordingly. If not, you need to configure the NC/NO-Contacts of the BACS GXR_AUX to the correct position and check wiring at the device itself.

Note

If you configure the Thermal Runaway after configuring GX_R_AUX outputs, be sure to check for previously entered events for plausibility:

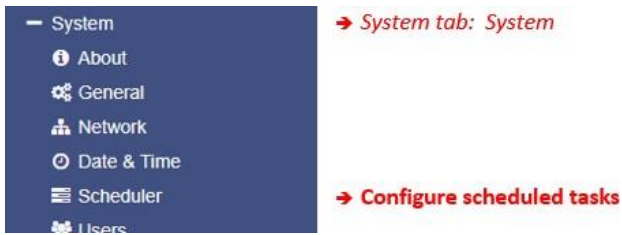
You may also need to open the battery interrupters for other reasons, the Thermal Runaway configuration dialog will only work on a specific scenario and configuration routine automatically:

The outputs are renamed and a preconfigured job is automatically added to the corresponding events. Since the BACS Web Manager cannot know why you entered these additional conditions, BACS will not remove all your configurations automatically-

It is up to you to check them manually.

Pause Equalization on schedule

For this configuration step, you need the following menu:



This hidden function is a little bit difficult to explain without basic information about the production process of a battery – please read the following information carefully, it will explain you why this function is very powerfull and how set up the most effective configuration that fits to your batteries ...

Depending on the manufacturer and production process, AGM batteries require a few charge / discharge cycles to achieve the optimum performance for a standby mode of a UPS. The number of chards / discharge cycles you need to form up your batteries is a technical puzzler:

Basically, there are two different production methods for batteries:

Formed accumulators

As a post production process, formed accumulators were repeatedly charged and discharged. By doing so, the battery chemistry itself will perform a so-called recombination. Caused by the entropy during the charge / discharge cycle, the recombination of the battery chemistry will stabilize the internal resistance of the entire accumulator. As a side effect, the accumulator's capacity will be maximized.

Unformed accumulators

These batteries are produced, packed and sold directly without any post production service. The entire forming process is a part of the final installation on site. The forming process will be performed by the customer during first months of usage - as an example, while running battery stress tests or by random power failures. In the end, these batteries will also reach full capacity as well as a stabilized internal resistance, but it will take much longer than batteries that are formed before installation on site.

OK, but why does unformed accumulators exist?

There is no legal standard that dictates forming - accordingly, it is a service of battery manufacturers and is a quality feature of recently produced batteries. As a consequence, it is up to the manufacturer how he wants to produce and sell his batteries:

While some manufacturer only supplies formed batteries as a quality standard, other manufacturer design two different product lines or produce as cheap as possible.

Note

From a technical point of view, no differences can be observed between the formed and unformed batteries during commissioning - all accumulators that have been assembled to a battery system have to perform such a formation process. The difference is that already pre-formed accumulators can finish this process much faster. Please note, the "formation is finished" can only be seen when evaluating the battery data collected by BACS.

In principle, BACS eliminates generally harmful voltage fluctuations.

As a result, formed batteries are spared and can be used over a very long time - sometimes even beyond the manufacturer's specifications about the design life of a battery. However, if batteries are unformed at start-up, balancing or equalizing, especially in the early days, could slow down the formation process enormously, because the accumulators need these voltage fluctuations.

Determining the optimal time from to hand over the equalization of your BACS system completely, depends, among other things, on the basic operating mode:

Scenarios with a cyclic usage

In the case of cycling applications, formation takes place automatically as there is generally a regular charge / discharge cycle. This means BACS can run immediately and your batteries will reach their maximum capacity very quickly.

Scenarios with a stand-by usage

In case of standby applications, the situation differs:

Because there is no cyclic discharge, the formation is carried out by natural voltage fluctuations of the UPS. As a consequence, a system that mostly eliminates voltage fluctuations slows down the entire formation process.

How to use „Pause Equalization“

As you can see, only Chuck Norris has an automatic battery forming process because his roundhouse kick will teach the batteries what they want to do... In all other cases it is technically not possible because the batteries can vary enormously depending on batch, grade, manufacturer, chemical composition, storage time after production, storage location, etc. It can actually happen that two batteries from the same manufacturer need completely different time windows until they reach the formed state - New BACS-controlled UPS systems must be observed individually.

Pause Equalization is thus a kind of "pause function" to facilitate the structured formation or reformation of batteries. To use this function, open the scheduler and select the job Pause Equalizing:

Add/Edit Scheduler Task		
Job	<input type="text" value="Pause Equalizing"/>	→ Select the job "Pause Equalization"
Parameter		
Hours	<input type="text" value="2"/>	→ Toggle the time in hours the equalization process shall pause
Timing		
Start	<input type="text" value="09/03/2019 02:50 PM"/>	→ Set up the job timing
Repeat	<input type="text" value="One Time"/>	
Triggers	At 02:50 PM on 09/03/2019 - one time	
<input type="button" value="Save"/> <input type="button" value="Cancel"/>		→ Save changes / discard changes

Setting up Hours and job timing

How many hours you want to pause equalizing is difficult to answer - BACS can facilitate and accompany the formation process in many ways. Here are 3 examples how to configure the BACS function pause equalizing:

Method 1: As easy as possible

Pause Equalizing for 5 days and repeat the job:

In this case, choose 120 hours and advise the CS141 to repeat once in a week:

The BACS Webmanager will pause equalizing for 120 hours or 5 days. The UPS is this given the chance to advance the battery formation 5 days a week. Then the BACS Webmanager will enable Equalizing for 2 days and generate comparable data. After an overall period of 7 days, the job will be re-run ... The BACS Web Manager Monitoring will always inform you if something with the batteries is not working as expected, even if Equalizing is temporarily disabled or pausing.

Use a second job to get status information about the forming process:

On initial start, the BACS Webmanagers integrated monitoring system starts collecting all required battery data for a detailed forming status evaluation. Just add a scheduled mail and the BACS Webmanager will send your regular status reports including necessary log files. You do not need daily reports, getting a status mail once a month should be enough to decide if the forming process is finished. If there an additional problem occurs:

BACS will inform you immediately...

During data evaluation, what are you looking for?

As an example, if you start with 40 unformed batteries, you will notice that each battery will show individual charge/discharge voltages. This is not an issue, it is natural for both, pre-formed and unformed batteries. With each discharge / charge cycle, the voltage curves of all batteries approach each other until they are only about 1V apart. If this can be seen, batteries are in sync and the forming process is largely completed. You may quit and delete the scheduled job "Pause Equalizing" and BACS begins its work.

With this method, you can evaluate the battery data once a month and are informed about the current state of health of the batteries. As soon as the battery data reaches formation parameters and indicates that the formation has been completed successfully, the Pause Equalizing job can be adjusted or removed accordingly.

Add/Edit Scheduler Task	
Job	<input type="text" value="EMail"/>
Parameter	
Receiver	<input type="text" value="techniker@tardis.de"/>
Text	<input type="text" value="Job Pause Equalizing läuft aus..."/>
	<input checked="" type="checkbox"/> Use text as subject
	<input checked="" type="checkbox"/> Eventlog
	<input checked="" type="checkbox"/> Datalog
	<input checked="" type="checkbox"/> Bacsllog

Method 2 – during running – faster but time-consuming

You can also instruct the BACS web manager to take control step by step.

If you choose running this way, equalizing is configured to pause each day for a specific time window. The advantage is that your UPS system is not on its own for the first few weeks. BACS has an eye on it and equalizing is most of the week enabled.

This method allows to plan special charge/discharge cycles without BACS equalizing provides and speed up the forming process. As an example, if your batteries have a discharge/charge cycle of about 6 hours, you can plan a -not-equalized time window of 6 hours daily, weekly – you can customize this time window to fit to your conditions.

In this example, the job Pause Equalizing will stop the equalizing process from 6:00pm Uhr to 11:00pm.

This will provide a unique time window to run a custom discharge / charge cycle and log the voltage behavior of the batteries. This method could be very interesting if you change some batteries and mix some new with old batteries. Equalizing will save your existing, already formed batteries and your new batteries have the chance to form up with all other batteries.

Timing	
Start	<input type="text" value="06:00 PM"/>
Repeat	<input type="text" value="Daily"/>
Triggers	At 06:00 PM - every day

In this example, we will use a periodic message reporting - if you know that equalizing pauses from 6:00 pm to 11:00 pm, you could create a "formation report" and get the according log files by mail:

Timing	
Start	<input type="text" value="23:15 PM"/>
Repeat	<input type="text" value="Weekly"/>
	<input type="checkbox"/> Sun <input checked="" type="checkbox"/> Mon <input type="checkbox"/> Tue <input checked="" type="checkbox"/> Wed <input type="checkbox"/> Thu <input checked="" type="checkbox"/> Fri <input type="checkbox"/> Sat
Triggers	At 11:15 PM - every Monday, Wednesday, Friday

In this case, set the je-mail job timing to Weekly and instruct the BACS WEBMANAGER to generate a status mail with the current battery data at 23:15 on Mondays, Wednesdays and Fridays.

As a consequence of a scheduled hour-by-hour formation of batteries, the entire formation process will take some more time:

Technically, the internal battery chemistry is calmed by eliminating the necessary voltage fluctuations associated with equalization - this will slow down the forming process.

On the other hand, evaluating of data is easier because you can directly compare how the batteries behave. This will allow you to determine very precisely when there will be no improvement in the voltage values and fully activate the equalization with pinpoint accuracy. As a side effect, you may train to spot strange measuring data.

Method 3 – Completely scheduled with unique single jobs

If you choose to climb this way, you need some experiences about using batteries and their behavior when equalize them. In general, the sense of scheduled tasks is to plan jobs and execute them automatically when the time has come to trigger a function. You may choose between cyclic jobs like sending mails with log files or single jobs like a small text message to your RCCMD client to remember yourself a single event is pending.

However, the advantage of this method is, that you can design and configure a general road map to form the batteries. As an example, it may look like this job list:

- Enable Equalizing for 2 days
- Send an email with log files for data evaluation
- Pause Equalizing for 7 days
- Send an email for data evaluation
- Enable Equalisation for 3 days
- Pause Equalizing for 5 days
- Send a mail with log files for data evaluation
- Pause Equalizing the next 7 days for some hours
- Send a mail with log files for data evaluation
- [...]

This will allow you to create a normalized 6-month battery forming procedure. To abort this scheduled task list because the forming process is finished earlier than expected, just delete this job list.

Note:

Forming new battery systems is an individual matter that largely bases on experience. In general, you can say:

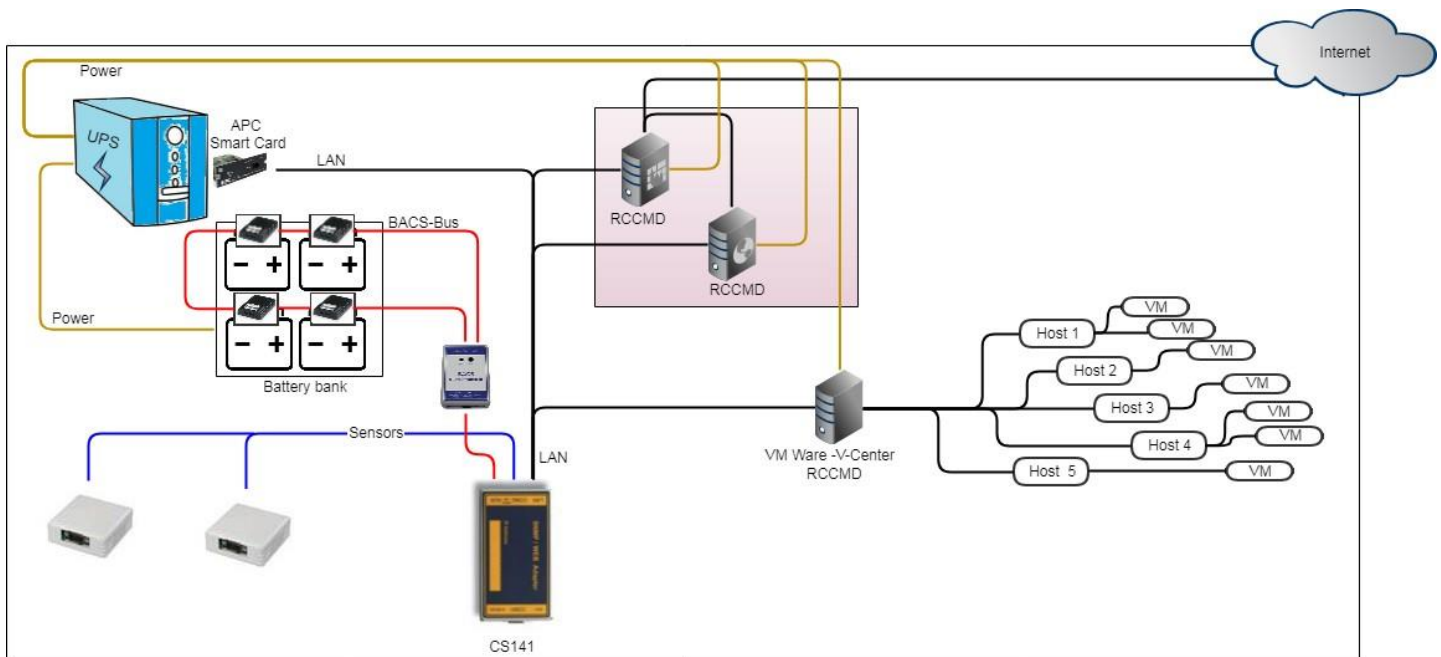
Unformed high-quality batteries reach the final operating state faster than unformed less-quality batteries. But it is also possible that pre-formed low-quality batteries may surprise you very much.

Please keep in mind, each battery system is a unique installation that needs an individual point of view.

RCCMD – Multiple Server Shutdown Software

Users Manual

Welcome to RCCMD



RCCMD is designed to shut down your systems in case emergency. In this case, an RCCMD server - usually a UPSMan or CS141 / CS121 - sends a shutdown command to the clients. The clients react to this signal accordingly.

Several basic conditions must be fulfilled for operation:

1. The RCCMD client needs a fixed IP address

This IP address must be communicated to the RCCMD server so that a unique command can be sent. If the IP address changes dynamically or there is no DHCP server available during system critical situations, RCCMD can also be addressed directly by IP address.

2. The corresponding RCCMD server must be authorized to send.

By default, RCCMD accepts any broadcast issued by an RCCMD server. If this reception behavior is not desired, an authorized RCCMD transmitter can be defined. The client will log all further commands but will no longer execute them.

3. The following ports must be available on your network:

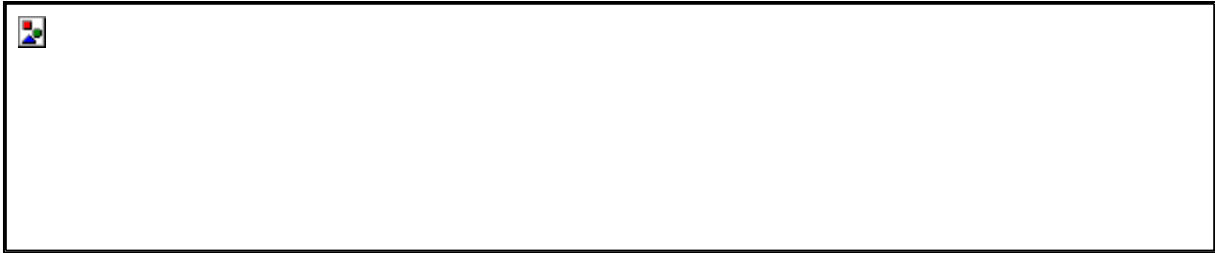
Port 8080 This port is used to call the local RCCMD web interface

Port 8443 This port is used to access the RCCMD web interface on another computer / server

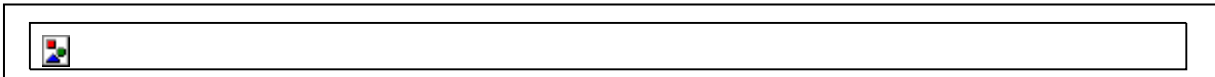
Port 6003 The RCCMD client communicates via this port

Installation of the RCCMD Appliance with ESXi 6.5:

Open your VMware ESXi – Host and login as root:

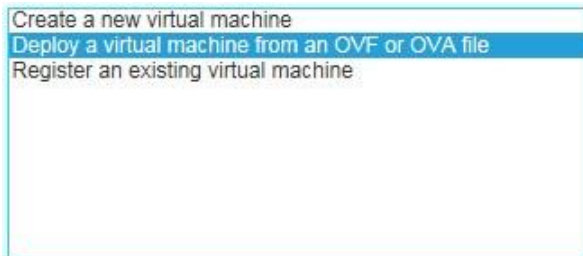


After successfully logging in create a new VM - For ESXi 6.5 you will find the corresponding tab in the upper bar:



Then select the following option:

Deploy a virtual machine from an OVF or OVA file:

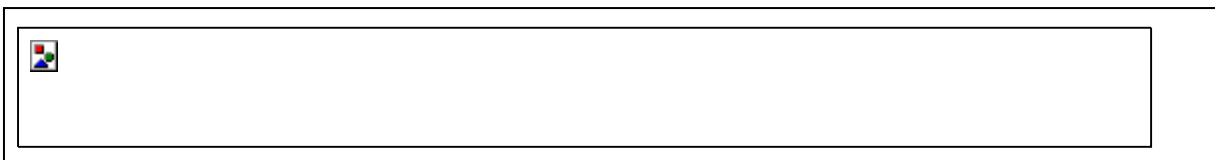


This option guides you through the process of creating a virtual machine from an OVF and VMDK files.

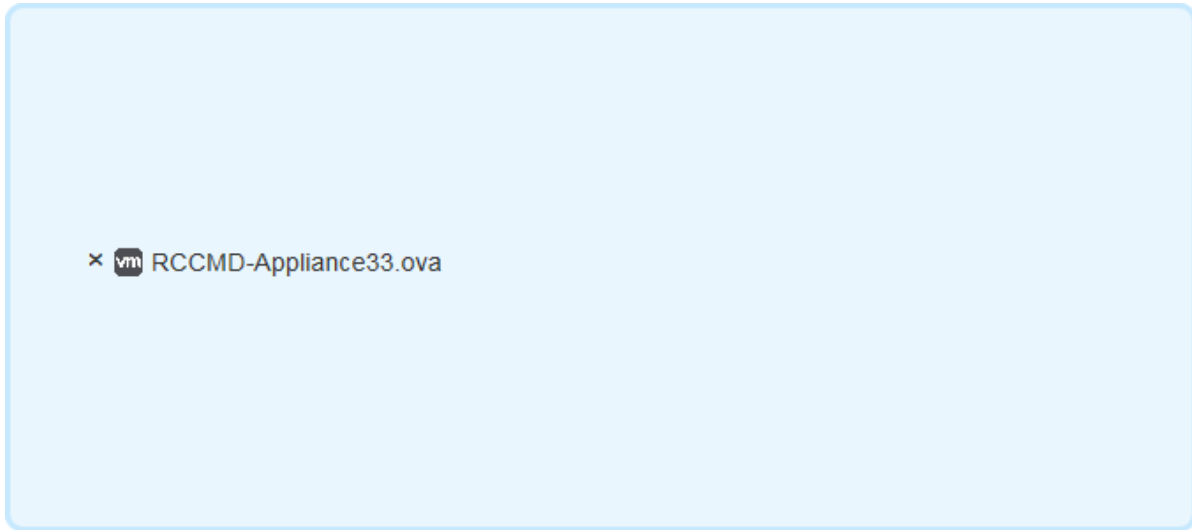
Click next to proceed to the next configuration dialogue:



Give your new RCCMD machine a unique name:



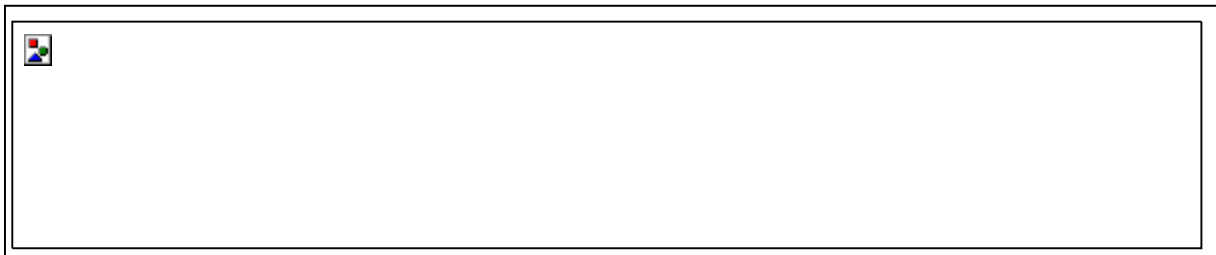
Place the OVA file into the necessary ESXi host window using drag and drop ...



... and click Next:



The OVA file is preconfigured, there is no need to do any additional settings:



Due to this fact, just click on next:



The RCCMD client will be managed by an according RCCMD server device. Therefore, this server device must be able to reach your RCCMD client over local network structures. In general, you can accept the preconfigured settings.

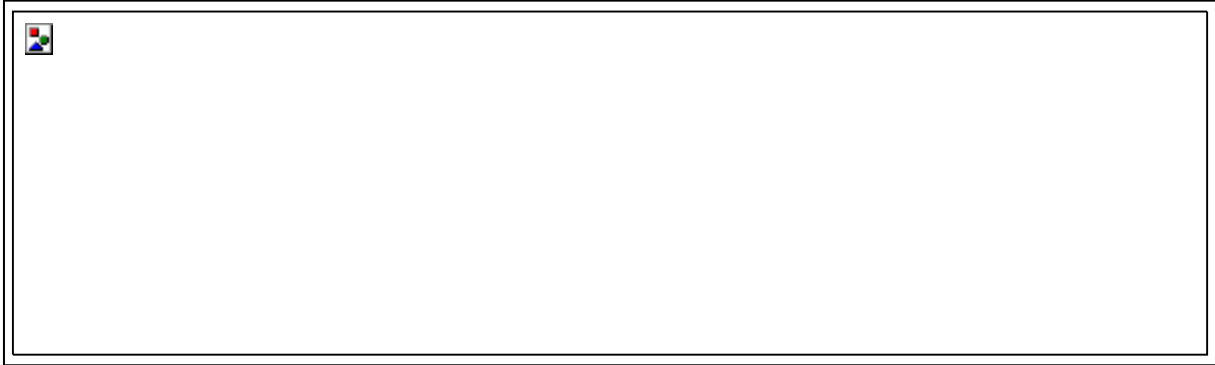
Network mappings	bridged	VM Network
Disk provisioning	<input checked="" type="radio"/> Thin <input type="radio"/> Thick	

The same works for provisioning of the hard disk space. The RCCMD OVF file is preconfigured for best use unless your hardware platform differs from standard installation routines.

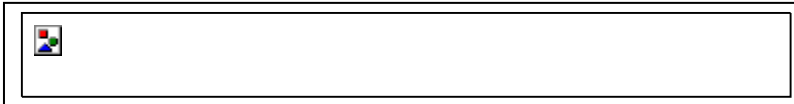
Once you have made the settings as you like, click *Next* to go to the next step:



This is the final step:
Please review all settings before clicking Finish:



Obey the special notification carefully to prevent damaging RCCMD during installation routine is running.



VMWare responds sensitive to browser updates during installation process. If the browser will be refreshed before installation is finished, the process will be aborted, rendering the virtual machine unusable.

Click finish to start the installation process:



The automatic installation

Results and Completed shows the current installation state and proper success.

Task	Target	Initiator	Queued	Started	Result	Completed
Destroy	RCCMD_Easy_Install	root	05/15/2018 13:32:17	05/15/2018 13:32:17	Completed successfully	05/15/2018 13:32:17
Shutdown Guest	RCCMD_Easy_Install	root	05/15/2018 13:31:53	05/15/2018 13:31:53	Completed successfully	05/15/2018 13:31:53
Upload disk - RCCMD-Appliance33-dis...	RCCMD Easy Install	root	05/15/2018 12:37:10	05/15/2018 12:37:10	<div style="width: 61%; background-color: #4f81bd; height: 10px;"></div>	Running... 61 %
Import VApp	Resources	root	05/15/2018 13:43:10	05/15/2018 13:43:10	<div style="width: 56%; background-color: #4f81bd; height: 10px;"></div>	Running... 56 %

Obey the Daleks:
The administrator will wait for the installation to complete before updating this browser window.

Note:

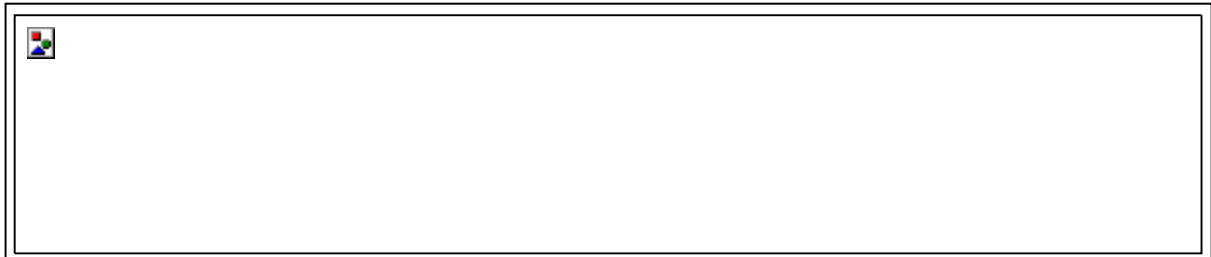
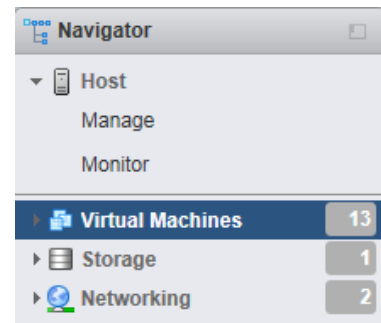
Use tabbed browsing to keep working. VMware will automatically detect the current session. By doing so, administrators will be allowed to continue working on the system while waiting for a finished RCCMD installation.

The Installation progress

On the left side you want to find a tool called navigator. The navigator displays an overview of all virtual machines installed on the system. This installation example is called

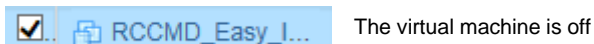
RCCMD_Easy_Install

Search for virtual machine including the RCCMD appliance.
Clicking on it will open advanced system information about the virtual machine.

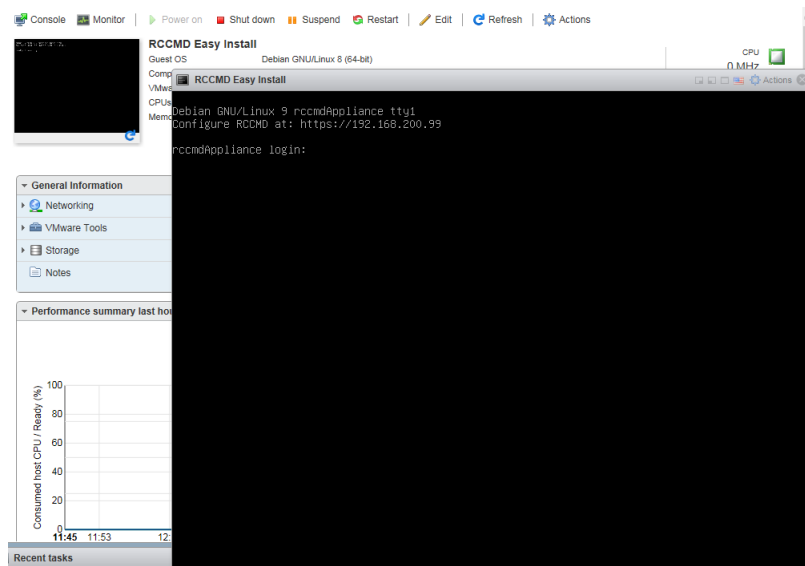


Open console

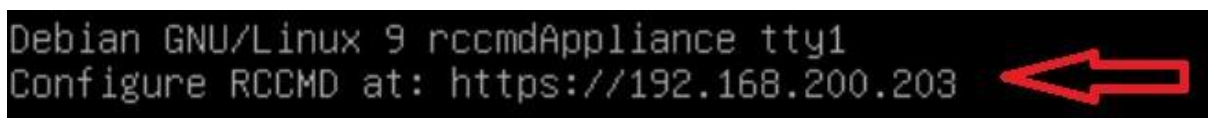
Ensure the virtual machine is running. Take a look at the list of all virtual machines and search for the RCCMD Appliance



Click on the virtual machine you have installed for more detailed information.
By pressing the console screenshot, the web console for the virtual machine will be opened:



As a default, the appliance will ask for a valid IP address. If your network provides a DHCP server, RCCMD will automatically display the current IP address.



If there is no valid IP address by DHCP, it is necessary to manually assign an IP address. in the appendix, you will find information about the procedure

Post installation console login

You can log on to the RCCMD appliance directly from the web console:

User: admin
Password: RCCMD

Gaining root privileges

The VMware Appliance is based on a Linux Debian 9 - The root privileges allow the manual re-installation of official packages as well as advanced configuration of the network interfaces.

```
admin@rccmdAppliance:~$ sudo su
[sudo] password for admin:
root@rccmdAppliance:/home/admin#
```

command: `sudo su`

by default settings, admin has not been granted system privileges to make changes - you need to assign increased system privileges by using the Linux command `sudo su`.

The installation of the RCCMD appliance is now complete. For further configuration, refer the web interface. A configuration guide for assigning an IP address manually can be found in the appendix to this manual.

Installing RCCMD with a vCenter

At VCenter context menu, start the RCCMD installation routine by choosing *Deploy OVF Template ...*:



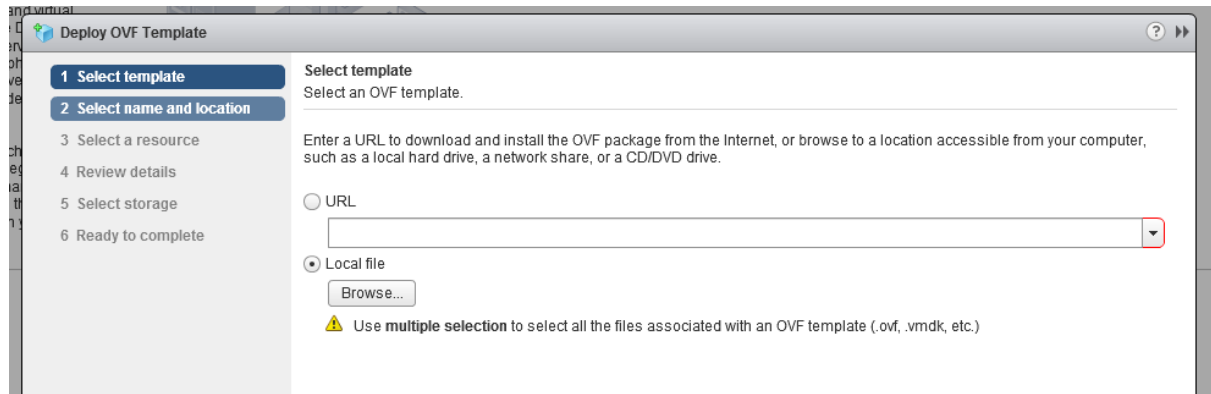
First, select the necessary file. vCenter provides two options:

URL:

If the OVF file is provided by web resources, specify the appropriate path.

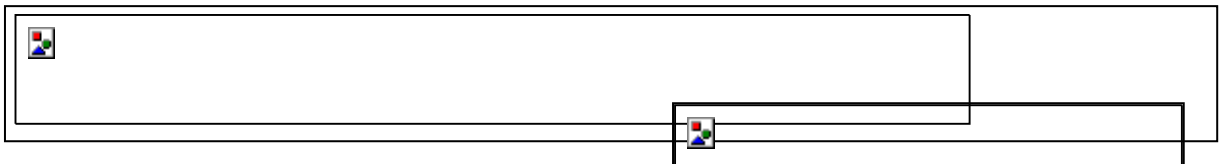
Local File

If you have saved the OVF file as a local file, select the file directly.



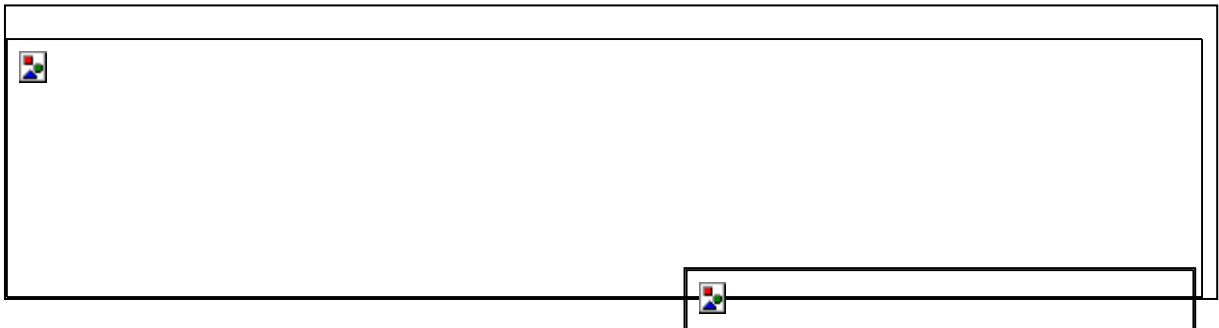
In this example installation, the local file will be used to install the RCCMD Appliance:

After selecting the local file, press Next to proceed to the next installation step:

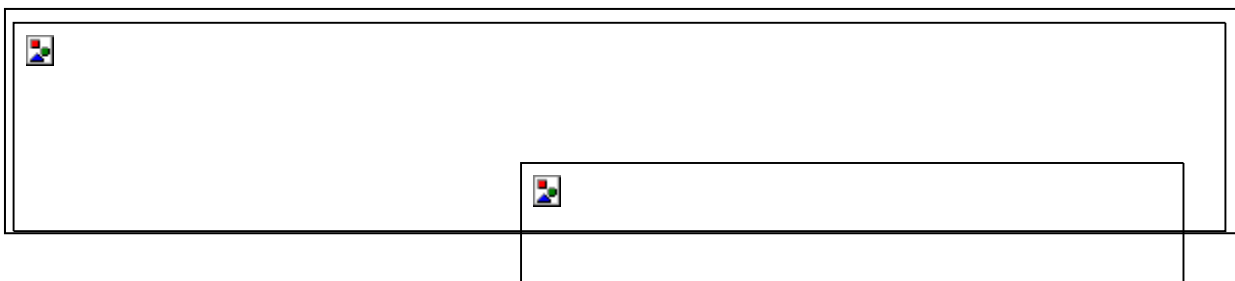


The next step asks you to name the virtual machine VM a uniquely. This name is needed in the later configuration steps of RCCMD.

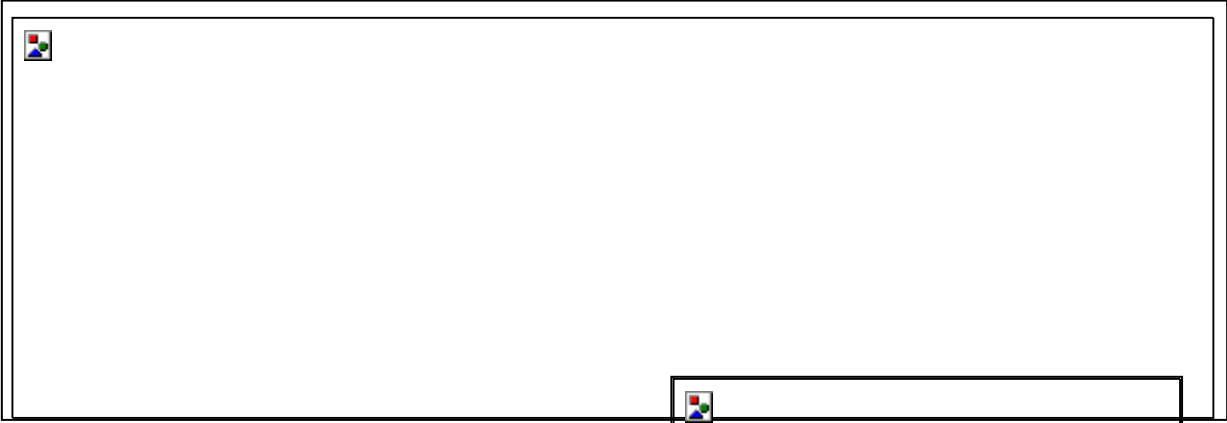
Click Next to proceed to next configuration step.



vCenter needs to know the destination host to set up and install the virtual machine

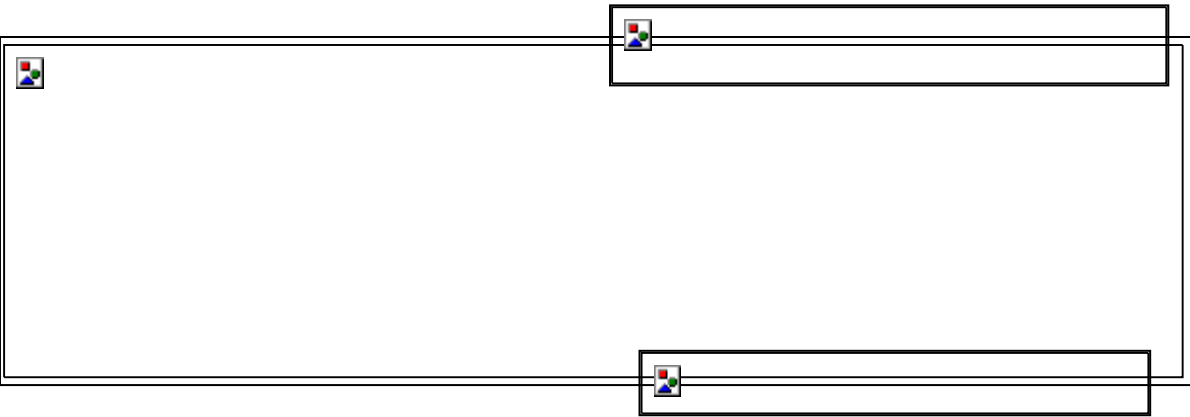


vCenter will provide a general overview of the settings according to the virtual machine. Press Next to continue.



Please note that there is no way but confirming the copyright terms...

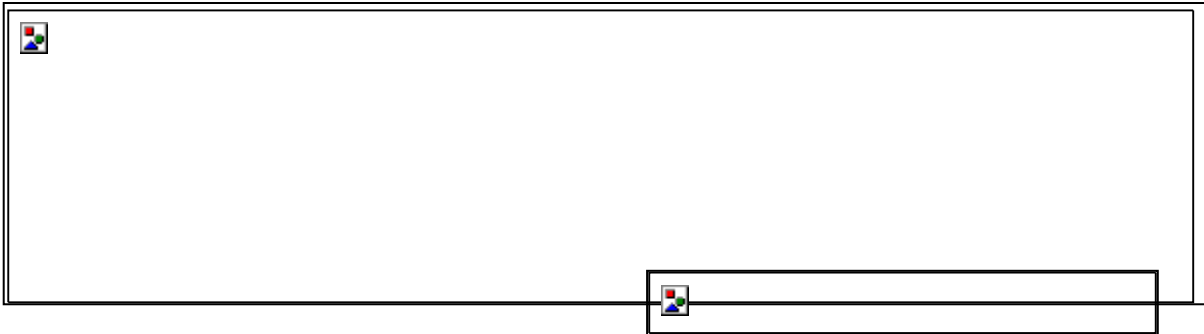
Please press Accept before proceeding the installation - the Next button will not work unless this has been happened.



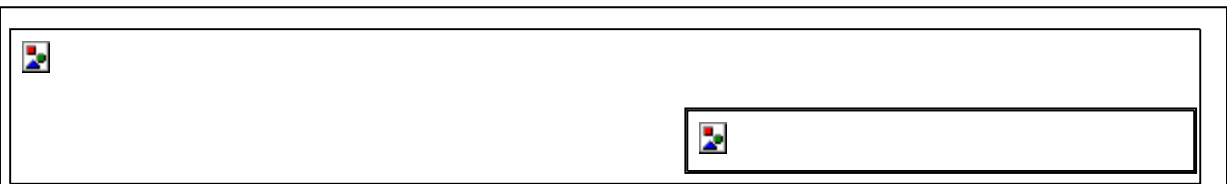
Disk usage may vary depending on the configuration of your system:

Please refer to local system administrators to get the correct setting.

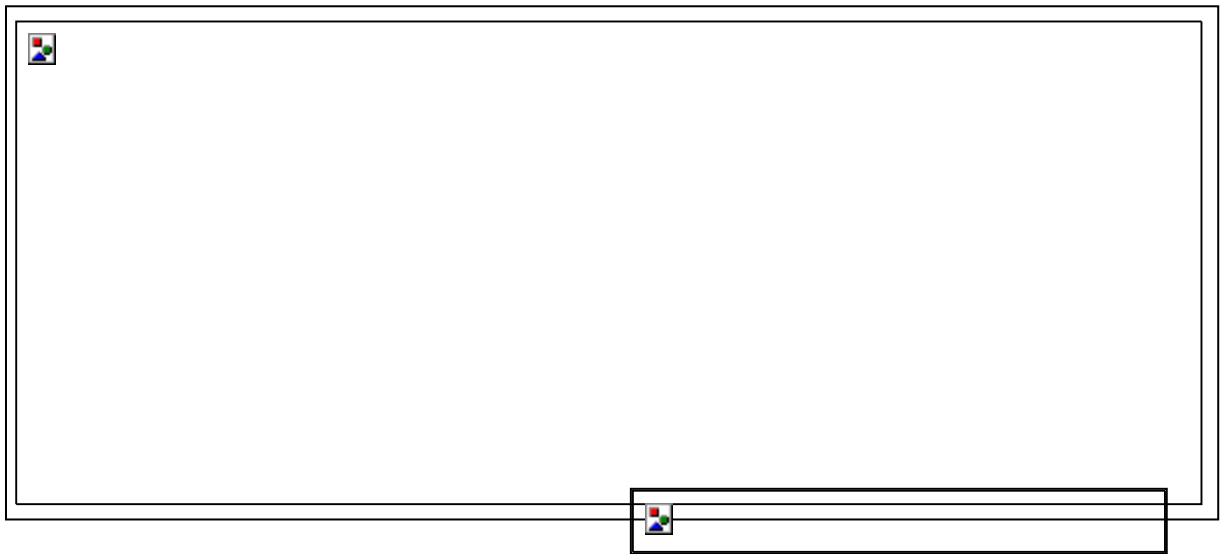
If you are unsure, select Thin provision and as VM storage policy none.



The appliance needs access to the network. Again, please refer your local system administrator...If you are unsure, first select VM Network in bridged mode. In this installation example, we use VM Network to correctly connect the VM to the network.



Take some time to review your settings: you will be shown an overview of your configuration. If the settings are to your liking, proceed by clicking *Finish*. This button will quit the configuration dialog and triggers the RCCMD appliance automatic installation routine.



How to observe the installation progress

Under Recent Tasks, you can track the current installation progress:

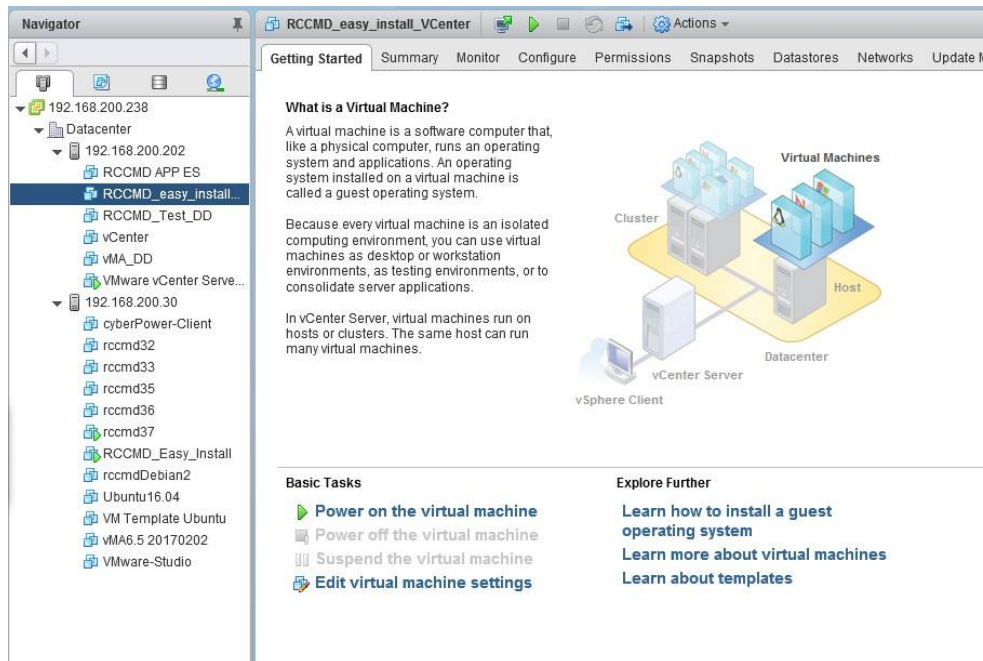
Recent Tasks							
Task Name	Target	Status	Initiator	Queued For	Start Time	Completion Time	Server
Deploy OVF template	RCCMD_easy_inst...	10 %	VCENTER6.7.GENE...	3 ms	5/31/2018 10:22:19 ...		192.168.200.238
Import OVF package	192.168.200.202	10 %	Administrator	140 ms	5/31/2018 10:12:11 ...		192.168.200.238

Please wait until the complete installation process is done and the status is set to *Completed*:

Target	Status
RCCMD_easy_inst...	✓ Completed
192.168.200.202	✓ Completed

Starting the VM and console access using vCenter

At navigator, search for the corresponding virtual machine and power it up.



Console login after installation

After the VM boots successfully, you can access the console directly from the vCenter console menu:



```
Debian GNU/Linux 9 rccmdAppliance tty1
Configure RCCMD at: https://192.168.200.203

rccmdAppliance login: admin
Password:
Last login: Wed May 30 16:10:37 CEST 2018 from 192.168.200.40 on pts/0
Linux rccmdAppliance 4.9.0-6-amd64 #1 SMP Debian 4.9.88-1+deb9u1 (2018-05-07) x86_64


The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.

Welcome to RCCMD-Appliance.
To configure RCCMD point your web browser to: [https://192.168.200.203]!
admin@rccmdAppliance:~$ _
```

As a default, the appliance will ask for a valid IP address. If your network provides a DHCP server, RCCMD will automatically display the current IP address.

```
Debian GNU/Linux 9 rccmdAppliance tty1
Configure RCCMD at: https://192.168.200.203
```



If there is no valid IP address by DHCP, it is necessary to manually assign an IP address. in the appendix, you will find information about the procedure

Post installation console login

You can log on to the RCCMD appliance directly from the web console:

User: admin
Password: RCCMD

Gaining root privileges

The VMware Appliance is based on a Linux Debian 9 - The root privileges allow the manual re-installation of official packages as well as advanced configuration of the network interfaces.

```
admin@rccmdAppliance:~$ sudo su
[sudo] password for admin:
root@rccmdAppliance:~/home/admin#
```

command: sudo su

by default settings, admin has not been granted system privileges to make changes - you need to assign increased system privileges by using the Linux command sudo su.

The installation of the RCCMD appliance is now complete. For further configuration, refer the web interface. A configuration guide for assigning an IP address manually can be found in the appendix to this manual.

Overview: The RCCMD menu structure

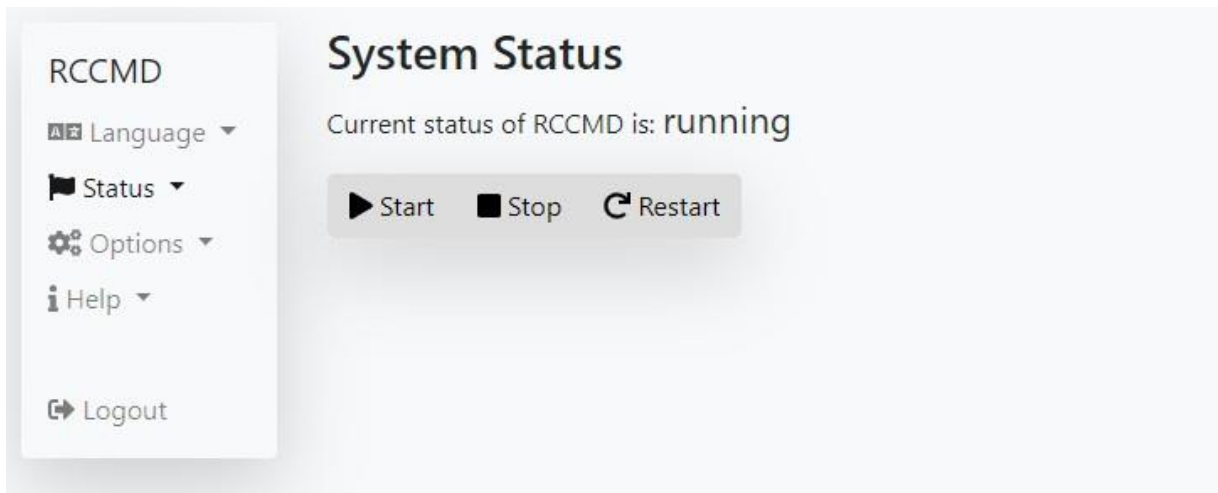
The RCCMD appliance provides a web console for comfortable access and configuration. The web configuration dialog uses the following menu structure:

Login mask

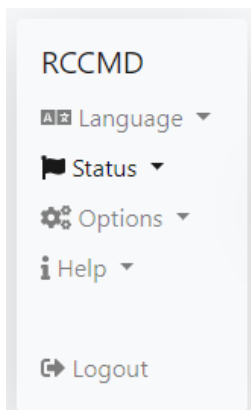
The login page shows a basic system status, the current version of the RCCMD appliance and the System login dialog.

Configuration dialog

After Login, RCCMD will show the configuration dialog:



On the left side, you will main categories. On click they will unfold and show sub menus:



- Language selection
-
- Main system status and log files
-
- RCCMD configuration dialog
-
- Help topics, maunals and links

→ Logout and return to the login mask

RCCMD quick configuration guide

Web Login: RCCMD

To access configuration screen of RCCMD, open a web browser and proceed to the IP address of you RCCMD installation:

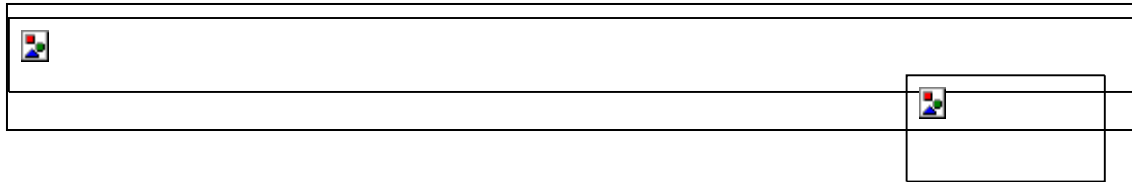
<https://<IP address of the RCCMD appliance >>



Use the default credentials to log in:

User: *admin*
Password: *RCCMD*

Before starting any configuration, RCCMD displays the current terms of use. Accepting them is required for using RCCMD software.



You may read the end user conditions and then click on the Accept button. The configuration dialog will proceed after accepting the end user license agreement

Next, RCCMD will prompt you to enter a valid license key:

Please note that the key used by RCCMD installation will work with these conditions:

1. One Key – one RCCMD installation

You can use any number of RCCMD clients in your system. In general, the prerequisite is that only one unique key will be used for one RCCMD client. If a key will be accidentally assigned twice, the RCCMD client that launches first will claim the license. The following RCCMD clients starting up will recognize a claimed license and will show an according log entry:



2018-05-30 09:17:51 rccmd[00490]: Licence fraud from IP address 192.168.200.144 detected. Functionality will deteriorate.

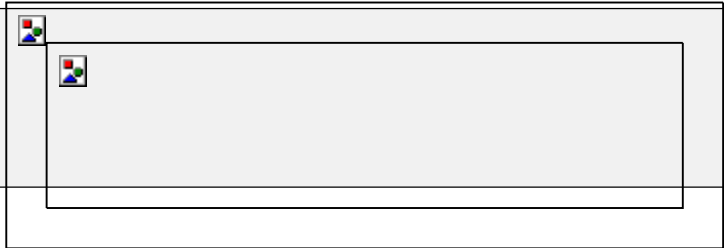
In case of using a key valid for a certain number of installations, only the according number of RCCMD installations will be activated with this appropriate key.

Please note, the demonstration key itself is a unique basic key that will be used for any installation:
You cannot use more than one RCCMD trial versions in one network.

2. If there is no valid key present, RCCMD will run in trial version mode

If you do not have the key or want to test the product, do not enter a key. By doing so, RCCMD will assume that you will use an initially a full-featured trial installation and uses a build-in 30-day evaluation key. RCCMD provides a configuration dialog for changing the key at any time.

Note
RCCMD offers you within the Web console on a dialogue to change the key:
Open Advanced Settings and click Update License Key

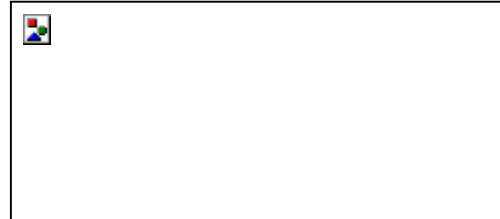


Please restart after essential configuration work

During the configuration of RCCMD a custom restart of the service is necessary:

Whenever a change has been made to the configuration, it is required to restart the RCCMD service. Otherwise the data is saved but not transferred to the active configuration.

If you activate Do not ask again, RCCMD will not inform you about the fact a restart is required.



Securing the RCCMD appliance

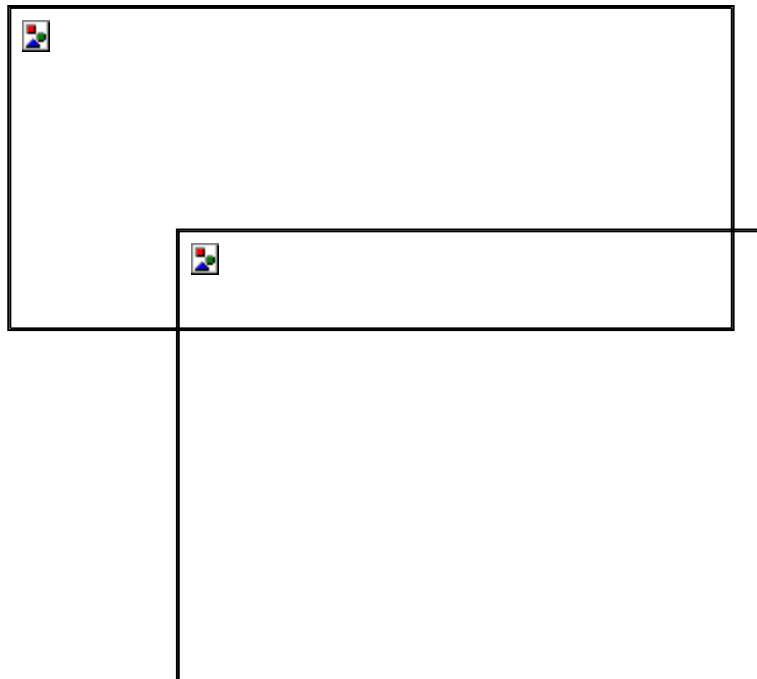
Menu: Open Options click on Connections

Protection against accidental server shutdown

Currently, each RCCMD transmitter can trigger a shutdown that cannot be taken back. The RCCMD client therefore offers you to limit these commands to specific stations.

Under Options, click on *Connections* to open the corresponding dialog. With *Insert* you can add a new IP address:

Enter the IP address expressly entitled to send an RCCMD shutdown command.



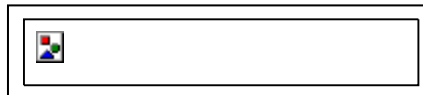
Activating RCCMD encryption

If your network requires to use an SSL encryption, RCCMD can be advised use SSL encryption.



To force SSL encryption, enable Accept only SSL connections. In case of up-to-date certificates only, RCCMD can be forced to reject outdated certificates.

With Save Changes, the IP address settings will be insert into the corresponding configuration script.



Checking current RCCMD system state

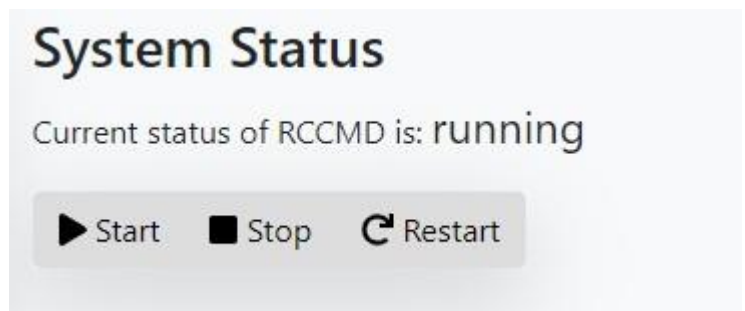
Menu: Status

Click System Status and press Restart.

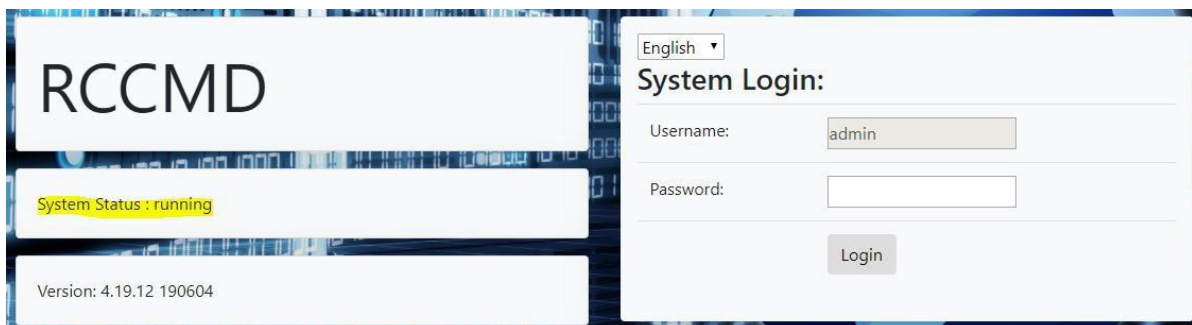
The Current status of RCCMD is used to detect the now active operating state.

The following status messages indicates the current RCCMD operating state:

- not running RCCMD is offline
- running RCCMD is online



RCCMD running status at the login screen

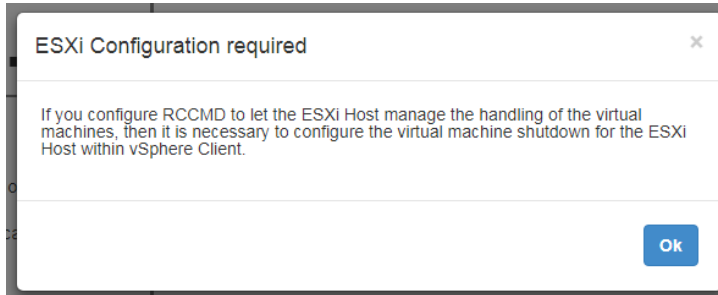


Passing the shutdown control to RCCMD when using a single host

Menu: VMware Settings

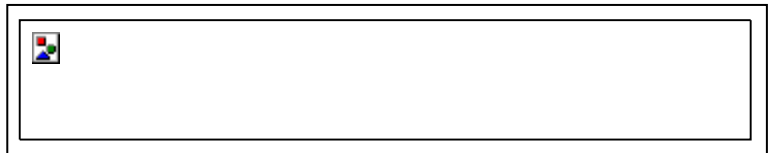
Go to VMware Settings:

If you have not yet made any settings, RCCMD will inform you that RCCMD needs additional information:



Although RCCMD is installed as a virtual machine and is already ready for use, it cannot yet fulfill its actual function since the necessary access authorizations have not yet been stored. Confirm this message with OK to open the VMware settings:

When using a single host is, virtual machines can be powered off before the ESXi host itself shuts down.

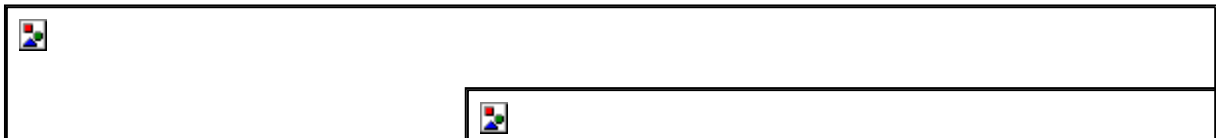


Note

The regular shutdown routine requires the virtual machines to be shut down and the host itself to be shut down. In this case, the shutdown duration merely defines the time window that the virtual machines have to shut down immediately after the RCCMD shutdown signal is received. The Maintenance Mode timeout defines the time window that RCCMD grants vMotion before the regular shutdown routine of the hosts takes effect. The maintenance mode in the shutdown behavior can therefore also be used to trigger a shut down for different hosts including a time delay.

For Virtual Machine Management, select *by RCCMD*. As Virtual Machine Behavior *Shutdown Virtual Machines*.

To prevent RCCMD from shutting itself down, the VMware host must know what the machine running the RCCMD Client itself is:



... RCCMD at the ESXi ...

... the current RCCMD client

RCCMD requires the following information:

HOST / IP name

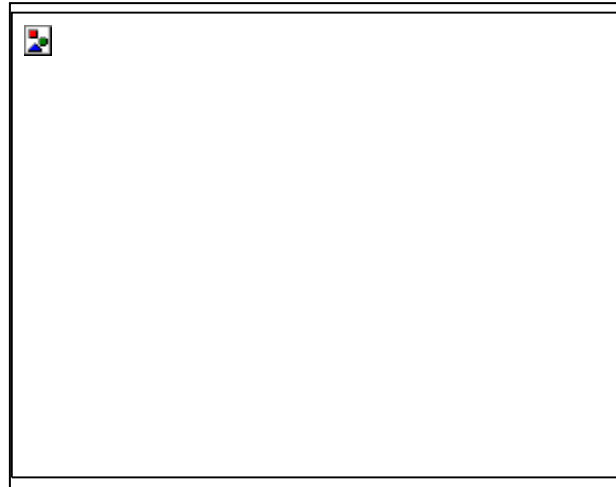
Normally, we recommend using the IP address of the RCCMD host here. You can, however, also enter the host name itself.

User

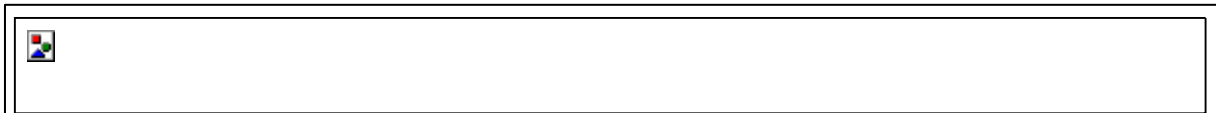
A user with the appropriate system privileges to shut down the VMware environment accordingly.

Password

The password assigned to the user that allows RCCMD to authenticate itself as authorized.



The next step will determine how much time RCCMD should allow the virtual machines to quit before the ESXi host powers down:

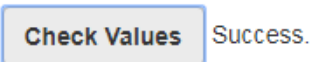
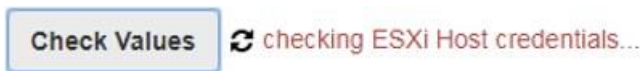


Virtual machines take different amounts of time to shut down and shut down properly. The exact time, how long a machine needs, is very individual and depends strongly on the task and the promised hardware. To prevent data loss or damage to the virtual machine, the host can be instructed to give the machines a proper time window to shut themselves down before shutting down itself.

Shutdown delay indicates the time in seconds that the host waits before being turned off.

The Default setting is 90 seconds - virtual machines taking more will be turned off due to the fact the ESXi host powers down.

You can check the access data with Check Values:



If the test was successful, press Save Changes to exit the configuration dialog.

Click on Verify to confirm the entered ESXi data as verified server.



You will notice that at the bottom right the Save Changes has changed color:



You will notice that at the bottom right the Save Changes has changed color:

You have made a change that requires RCCMD to be restarted to permanently save the inputs and apply them to the active configuration. This process is indicated by the green button.

Handing over the shutdown control to RCCMD using a vCenter

Menu: VMware Settings

The vCenter differs with its operating modes from a standalone host. While the Standalone Host works on its own and shuts down virtual machines as needed, vCenter provides the so-called vMotion: The HA - High Availability - of vMotion allows virtual machines to be moved from one host to another before the host is intentionally powered down.

Please note:

Before you can use the RCCMD appliance with vMotion, the Distributed Resources Scheduler DRS must be configured to use the fully automatic mode.

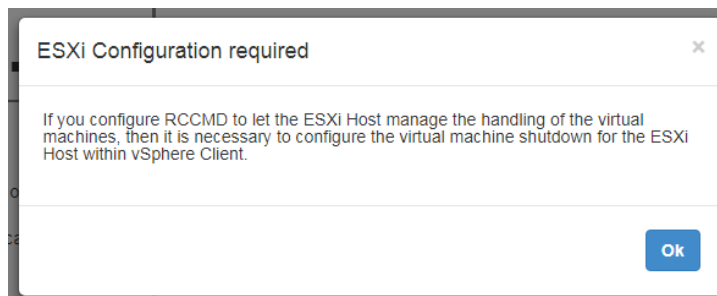
Note

Before using RCCMD in conjunction with vMotion, ensure to verify that each virtual machine running on the host has been tested working with the maintenance mode. If maintenance mode fails, non-migrated virtual machines will be switched off when the host is powering down.

Open VMware Settings:

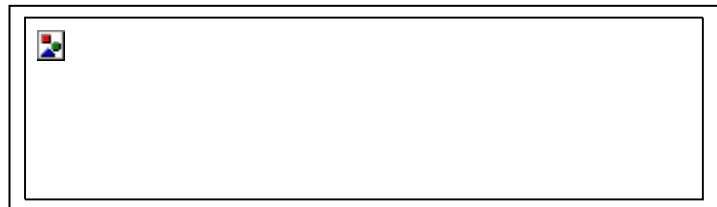
If you have not yet made any settings, RCCMD will inform you that RCCMD needs additional information:

Although RCCMD is installed as a virtual machine and is already ready for use, it cannot yet fulfill its actual function since the necessary access authorizations have not yet been stored. Confirm this message with OK to open the VMware settings:



While using a vCenter, virtual machines can migrate to another host before the original host powers down. The virtual machines themselves will continue working seamlessly. Please note the different access data:

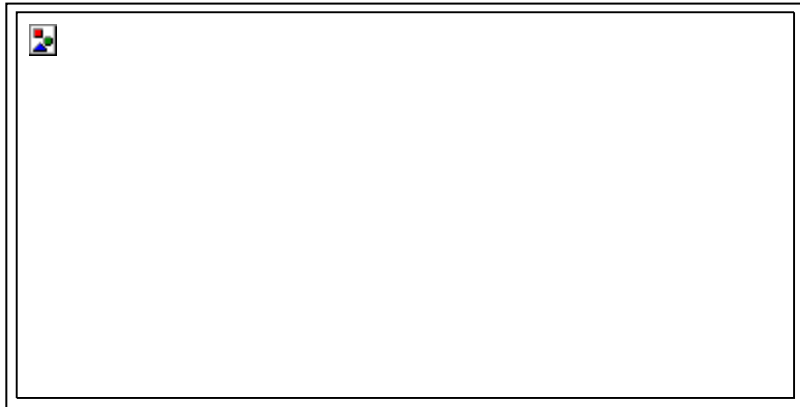
Under Virtual Machine Behavior, select Maintenance Mode (vMotion).



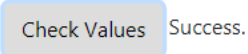
The Maintenance Mode time out in Seconds defines the time vCenter is given to move a virtual machine to another host. The behavior of vMotion is configured within the high availability (HA) within the vCenter. As soon as time is up, the standard shutdown procedure will be initiated:

remaining virtual machines will shut down due to the fact the host powers down.

Unlike the standalone host, RCCMD requires user data with the corresponding authorizations of the vCenter:

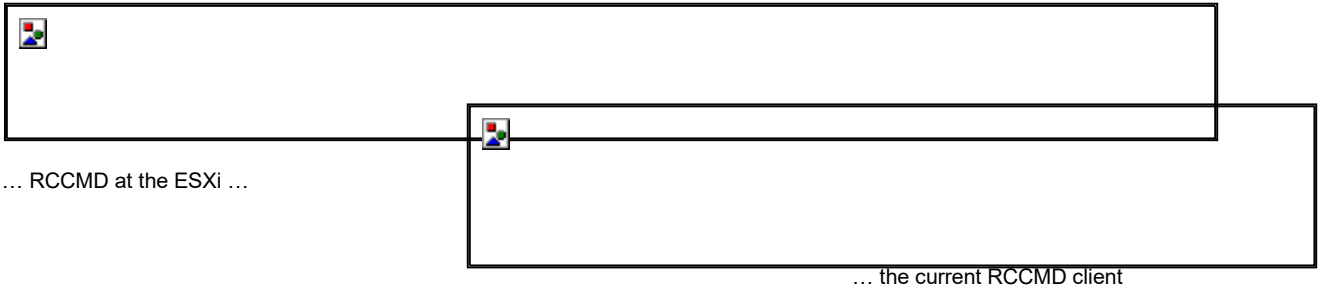


Use Check Values validate the credentials of the vCenter - Check values will display whether the vCenter is reached and the access data has been entered correctly:



If RCCMD cannot reach the vCenter correctly, it will show a corresponding error message.

To prevent RCCMD from shutting itself down, the VMware host must know what the machine running the RCCMD Client itself is:



RCCMD requires the following information:

HOST / IP name

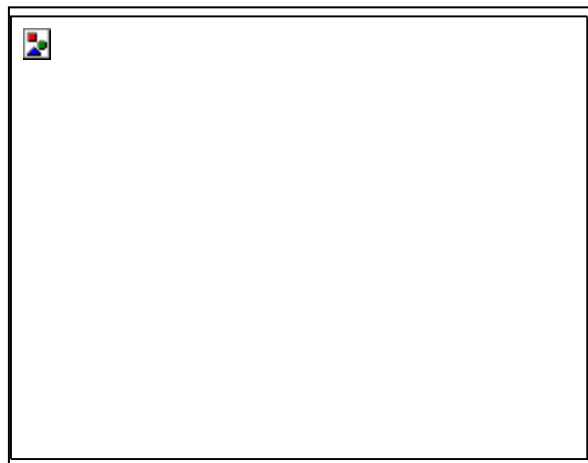
Normally, we recommend using the IP address of the RCCMD host here. You can, however, also enter the host name itself.

User

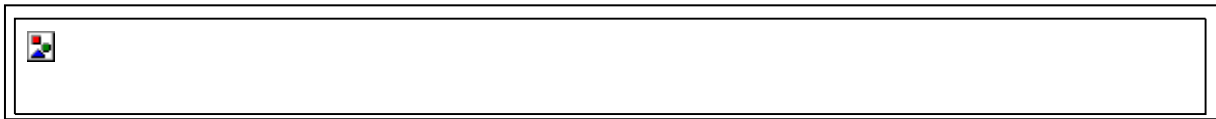
A user with the appropriate system privileges to shut down the VMware environment accordingly.

Password

The password assigned to the user that allows RCCMD to authenticate itself as authorized.



The next step will determine how much time RCCMD should allow the virtual machines to quit before the ESXi host powers down:



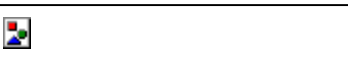
Virtual machines take different amounts of time to shut down and shut down properly.

The exact time, how long a machine needs, is very individual and depends strongly on the task and the promised hardware. To prevent data loss or damage to the virtual machine, the host can be instructed to give the machines a proper time window to shut themselves down before shutting down itself.

Shutdown delay indicates the time in seconds that the host waits before being turned off.

The Default setting is 90 seconds - virtual machines taking more will be turned off due to the fact the ESXi host powers down.

You can check the access data with Check Values:



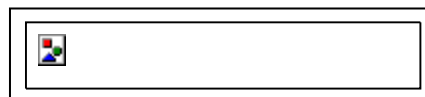
If the test was successful, press Save Changes to exit the configuration dialog.

Click on Verify to confirm the entered ESXi data as verified server.



You will notice that at the bottom right the Save Changes has changed color:

bottom right the Save Changes



You will notice that at the bottom right the Save Changes has changed color:

You have made a change that requires RCCMD to be restarted to permanently save the inputs and apply them to the active configuration. This process is indicated by the green button.

Enabling shutdown control when using a vSAN

Before starting, please read the following configuration notes carefully to prevent shutdown issues caused by a wrong configuration of RCCMD.

RCCMD can handle vSAN VMware environments. Due to the fact, a vSAN is very complex and the operating conditions of a vSAN differs when compared with a single host or a standard cluster, there are some pre-conditions that must met before RCCMD can shut down a vSAN:

The RCCMD client that handles the vSAN cannot be installed inside a vSAN

Due to the fact, each host of a vSAN must be set to in maintenance mode before the can be switched off. As long as one virtual machine is running, it is not possible to switch off the hosts.

The vCenter that handles the vSAN is the first virtual machine that starts and the last virtual machine that shuts down.

The vCenter is the control unit of a vSAN. It is allowed to install the vCenter inside the vSAN as well as running it on a single host that is not part of the cluster. The essential function of the vCenter is managing the all data synchronization inside a vSAN after all other virtual machines are down. You need to ensure that the vCenter can complete this operation.

If you run a Witness-Server as a virtual machine inside a vSAN

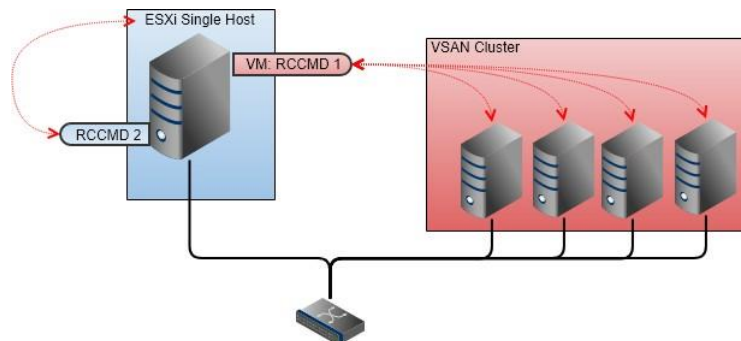
The Witness Server has a special task If two hosts do not match which host holds the most recent data, they ask the witness server. The witness server acts like a complete host, but cannot maintain virtual machines.

Due to this fact, the witness server can also be virtualized in the vSAN and still acts as a stand-alone host. In that case, you need to differ between the Witness server's IP address and the host's virtual machine where the witness server's virtual machine is located:

The witness server is shut down regularly within the vSAN cluster.

The host that maintains the virtual machine that contains a witness server, needs a second RCCMD client for enabling the maintenance mode after the witness server is switched off.

Technically, an RCCMD client can only handle the vSAN or the host it runs on



As a consequence, if you have single hosts AND a VSAN cluster, you will need at least 2 RCCMD clients: RCCMD 1 manages the shutdown of the VSAN cluster and RCCMD 2 manages the shutdown of the single host. The shutdown routine is then divided into 2 different commands for the CS141:

- o Shutdown the VSAN cluster
- o Shutdown of the single host

Since the two RCCMD clients run side by side:

When choosing the correct time window for shutdown tasks, ensure the VSAN has turned off all hosts completely before turning off the last remaining single host - otherwise the RCCMD client that manages the shutdown of the VSAN may not be able to complete the shutdown routine because the second RCCMD client performs a local virtual machine shutdown.

Note

Appliance vs Appliance - What is the Virtual Machine and what is "the RCCMD client"

Basically, the two appliances do not differ from each other: Both are virtual machines. However, because you use two appliances, the name of the virtual machine they run themselves on, will differ. Entering the name of the virtual machine will prevent that an RCCMD client will shut down itself first. So, if you tell RCCMD 2 the name of his own virtual machine, it will consider that RCCMD 1 is just another "guest VM" and will shut down it. When using a vSAN, the shutdown commands of the CS141 will harmonize the shutdown behavior of both appliances.

if you use a vSAN, take care for the time windows required by the modified shutdown sequence

The reason for using a vSAN is to combine a maximum data redundancy with a most possible availability of servers: Basically, there is no reason for a regular vSAN cluster shut down.
A complete shutdown is an emergency issue, and should be handled accordingly:
It is difficult to predict how much time the vCenter will take within a vSAN to bring the hosts into maintenance mode. In principle, the vSAN shutdown will be performed in three steps:

Shutdown of all virtual machines

In this step, all virtual machines will shut down.

Post synchronization phase

At this stage, all hosts synchronize their current datasets.

Switching into maintenance mode

All virtual machines are shut down and the datasets are up to date. The hosts can be switched off.

The critical system stage is the post synchronization phase. This process is difficult to assess:

The maintenance mode can only be assumed as soon as the synchronization of the data between all hosts has been completed. Unfortunately, this process is dynamic and the time needed to fulfill this process depends on the level of used hardware, the number of virtual machines as well as the amount and type of data that exists within the virtual machines.

To make it trickier, this process takes place within the vSAN without any information about the current data synchronization state - at some point, the hosts are in maintenance mode, which means that the process is complete.

However, available time is determined by the maximum operating time of the UPS:

RCCMD needs validated timer settings that not only use the calculated times for a shutdown but also respects the granted uptime of the UPS:

Ensure this time window ...

allows to shut down the vSAN in good times.

contains some extra time if the post synchronization phase suddenly needs more time than expected

stays within the security range of the UPS's uptime,

ensures a shut down of other hosts and clusters, too.

System critical note:

Before you start to configure the shutdown of your vSAN, the following information are mandatory:

1. an overview of the time window that a UPS can grant for an orderly shutdown?
2. How long do you need for a manual shutdown?

Please note:

Due to the fact a vSAN is sensitive to shut down fails a vSAN is technically a very system critical process that needs your attention.

Preparing RCCMD for the vSAN

At vmware settings, enable "Hosts are also vSAN nodes"



To manage the shutdown routine, ensure that the RCCMD appliance must be located outside the VSAN cluster.

Once you have activated the vSAN mode, you will get additional menus:

vSAN Timeouts
Ensure all operations complete within their timeouts! Integrity of vSAN Objects will break if any timeout interrupts a running operation.

Mode for decommissioning vSAN nodes:	<input type="text" value="No data evacuation"/>	<input type="button" value="Info..."/>
vSAN Resync timeout in Seconds:	<input type="text" value="200"/>	<input type="button" value="Info..."/>
Seconds to wait before setting Maintenance Mode for vSAN:	<input type="text" value="100"/>	<input type="button" value="Info..."/>

Mode for decommissioning vSAN nodes

Leave the decommissioning mode on No data evacuation - this mode is the fastest method to shut down a vSAN cluster: The virtual machines are shut down in a structured way and then all data will be synchronized on all affected hosts.

Definition of the vSAN Resync timeout

Unlike the default procedure, the vCenter becomes active after the virtual machine shut down and start synchronizing all records within the cluster.

This post synchronization phase defines the critical phase of the shutdown procedure:

All datasets from the virtual machines must be in sync with mirrored data stored on other hosts. As long as this synchronous system state is not reached, the Maintenance mode cannot be taken by any host.

Note:

This process is very dynamic and depends on the type of data that needs to be synchronized. You may have created several new virtual machines and the synchronization time will only change marginally. However, it can also happen that you create a virtual machine and thus radically increase the post-sync time. In other scenarios, the data within the virtual machine may grow organically cause by the usage, which in turn affects the time required:

This value cannot be determined once during the first installation as a fixed value, it must be regularly checked for up-to-datedness and adjusted if necessary.

The vCenter takes all the time needed for this process. Unfortunately, this relative amount of time is in direct contrast to a clearly defined time window that can be provided by the UPS during an emergency power operation. You need to calculate a sufficiently large time window to give the vCenter a time reserve in case of the calculated period is insufficient.

Defining maintenance mode for the vCenter.

This setting defines how much time the vCenter has to shut itself down after synchronizing data. If the vCenter runs as a virtual machine within the vSAN, this point in time becomes interesting: After this time window, the hosts are put into maintenance mode and the vCenter is switched off by its host.

Enter data for the vSAN managing vCenter

Enter the vCenter Server credentials:

Host name or IP:

User name:

Password:

Since RCCMD must coordinate with the vCenter over the entire process, the access data for the vCenter, which manages the vSAN, is mandatory.

At this configuration dialog, do not enter credentials for individual host.

Define the vSAN managing RCCMD client:

RCCMD has the task of shutting down all virtual machines and turning off the hosts at the end. Since within a vCenter not only a vSAN but further hosts can be mapped, RCCMD can shut them down, too. There are two exceptions that need more attention:

Information about the virtual machine running RCCMD

The virtual machine that runs RCCMD must not be shutdown. Or else RCCMD cannot shutdown the other virtual machines and hosts. Enter the virtual machine's name on which RCCMD runs.

VM running RCCMD:

Although RCCMD itself cannot run in the vSAN that should be shut down, the vCenter that manages the vSAN may include additional hosts in its list. The RCCMD appliance is a virtual machine that must comply with the control commands of the host on which it is running itself - if the host advises a shutdown, the appliance will do it. To prevent RCCMD from inadvertently giving itself a shutdown command, enter the name of the virtual machine you chose for RCCMD. When entered, the virtual machine that holds this name will be excluded from the shutdown process.

Define the virtual machine that contains the vSAN managing vCenter

The virtual machine that runs vCenter must not be shutdown. Or else vSAN Hosts cannot be decommissioned properly. Enter the virtual machine's name on which vCenter server runs. If vCenter Server is not shut down by RCCMD, or is not running on a virtual machine, then ignore this field.

VM running vCenter:

Within the vSAN system, the vCenter performs special administrative tasks, but is also a virtual machine. During the shutdown, RCCMD first gets an overview of active virtual machines and then shuts them down, migrates them, etc. With this setting, RCCMD will know which of the virtual machines is the vCenter and will shut down it exclusively as the last machine in the vSAN shutdown procedure.

Definition of the vSAN ESXi host nodes

Define the hosts to be shut down by RCCMD. The virtual machines can be moved to other hosts via the vCenter. To shut down a host, RCCMD requires the following information:

HOST / IP name

We recommend using the IP address of the host at this point to avoid addressing problems when parts of the IT infrastructure are down.

Due to the fact RCCMD supports host names, you may enter a host name, too.

User

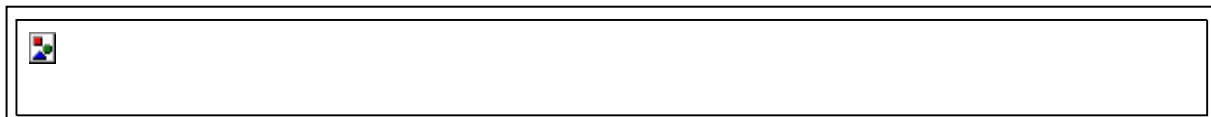
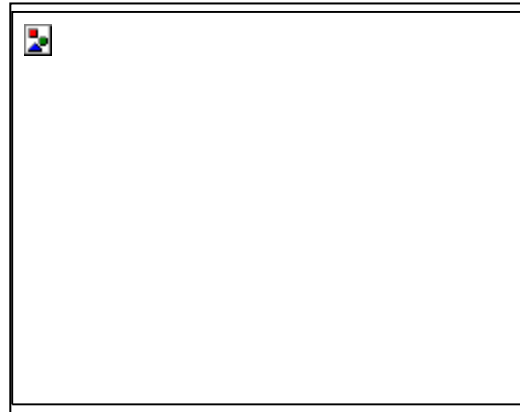
A user with the appropriate system rights to shut down the VM Ware environment accordingly. Normally, it is the local host administrator

Password

The password assigned to the user that allows RCCMD to authenticate itself as authorized.

Shutdown delay

The next step is to determine how much time RCCMD should allow the virtual machines to shut down before the before the ESXi host will quit all operation and switches off:



The vSAN has a special feature compared to other operating modes:

The shutdown duration typically defines the time window that a host grant the operating systems within virtual machines before the virtual machine is simply powered off. Thereby it does not matter if a vCenter has previously tried to migrate machines or not.

When this command is issued to the hosts running in a vSAN, there are no more virtual machines that need to be powered off:

- All hosts must be in maintenance mode
- A host can only be in maintenance if all virtual machines are moved or switched off.

For the hosts in vSAN, this means that the shutdown time of virtual machines can be set to 1 second:

The shutdown routine on a vSAN has already brought all hosts into maintenance mode. Consequently, no time window is required to grant operating systems within a virtual machine for a shut down.

Add... Remove Edit... Verify ESXi Hosts to shutdown		
ESXi Address	Shutdown duration	Verified
192.168.200.107	1 Seconds	
192.168.200.124	1 Seconds	
192.168.200.156	1 Seconds	

Special role: The witness server

Small vSAN systems lack the necessary resources to be able to independently adjust all data stocks.

To prevent problems with data synchronization in minimalist vSAN systems, a witness server is used:

This witness server acts as a stand-alone host in vSAN, but is not responsible for hosting and managing virtual machines - as soon as hosts are unable to agree with the timeliness of their datasets, the witness server decides which host has to synchronize the data.

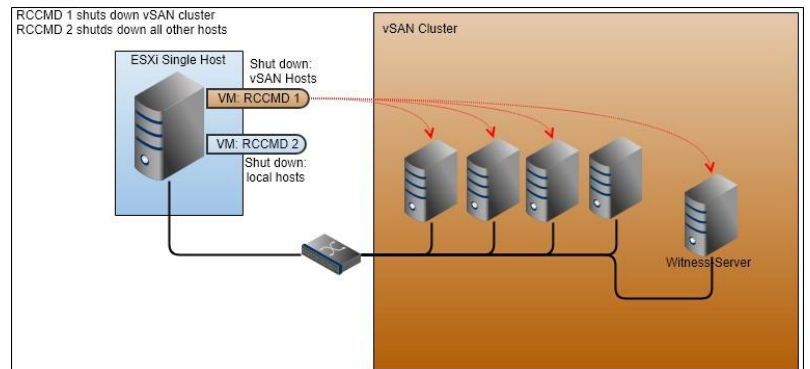
The witness server can be both, a real physical machine with its own hardware as well as acting like a physical host but running within a virtual machine. The vSAN knots cannot see the difference between the different setup strategies of a witness server.

But this difference affects the RCCMD configuration:

If running a real witness server as a standalone machine:

In this case, assign the witness server and any hosts that you want to shut down. The hosts will go into maintenance mode accordingly:

- Shut down virtual machines
- The vCenter will perform the reSynch
- The hosts switch into maintenance mode
- The hardware can be switched off.



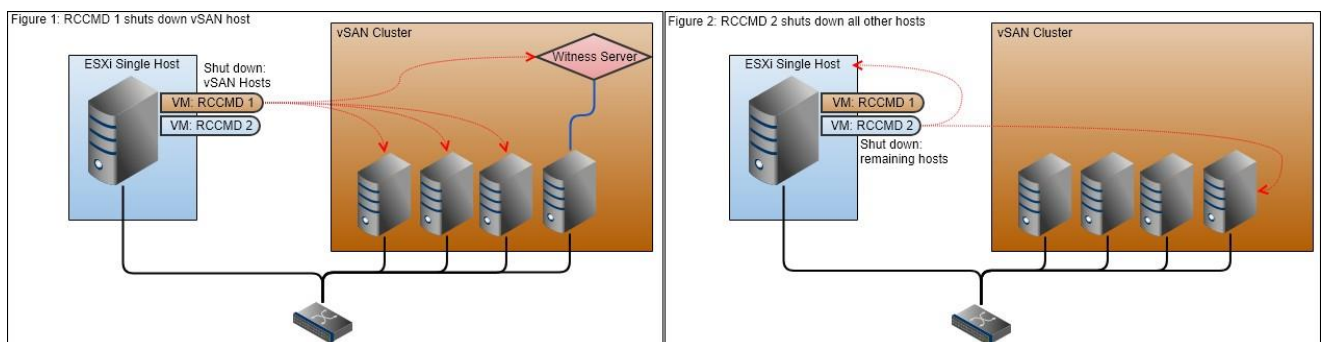
When using a virtual machine to run a witness server

If you run the witness server as a virtual machine in the vSAN, you must differ between the host on which the witness server is stored and the witness server as a stand-alone host. Since the witness server acts like a host within the vSAN, it is perceived and treated accordingly - The installation type does not matter:

While the host that maintains the virtual machine of the witness internally perceives only one virtual machine running "some kind of system", it accepts the witness server as a standalone host and network node on the network. If the wrong IP address has now been specified, the host responsible for the virtual machine will respond correctly:

- The host will stop running the virtual machine
- The host changes to Maintenance Mode

However, since the (albeit virtualized) witness server represents a full-fledged host and network node, it must consequently be treated as a real host and put into maintenance mode before being turned off. Formally, you need two RCCMD appliances to shut down a vSAN. If you use a virtualized witness server, you can use the second RCCMD to regularly switch off the host that manages the virtual witness server.



How long is the estimated shutdown time?

Basic shutdown time

After entering all the data, an estimate time will be shown RCCMD may be need for a full shutdown.

You can see the estimated shutdown time below the ESXi host settings.



Please note that this value is a guideline calculated by entered data.

This value is intended to help you to find the optimized trigger time to run an emergency shutdown routine if a power failure occurs.

Note:

Each UPS can only grant a pre-defined time window emergency power. When the batteries are depleted, the UPS will shut down itself to avoid damaging the batteries. In general, it will not help if you just play with the numbers within RCCMD until the estimated shut down time matches the data sheet of the UPS:

Furthermore, these values are just a snapshot of your system based on the data you entered! Please check regularly whether the entered values meet the real shut down condition in case of an emergency.

Keep in mind that between two shutdown tests the shutdown conditions may change. When calculating and adapting the average shutdown time, we recommend to take some extra time than the minimum time requires..

The configuration of RCCMD is now complete and RCCMD will be able to shut down your system in an emergency. Please note that RCCMD does not become active automatically - it needs a valid RCCMD shutdown command. The transmitter is usually an SNMP card or a software tool that can handle RCCMD shutdown signals.

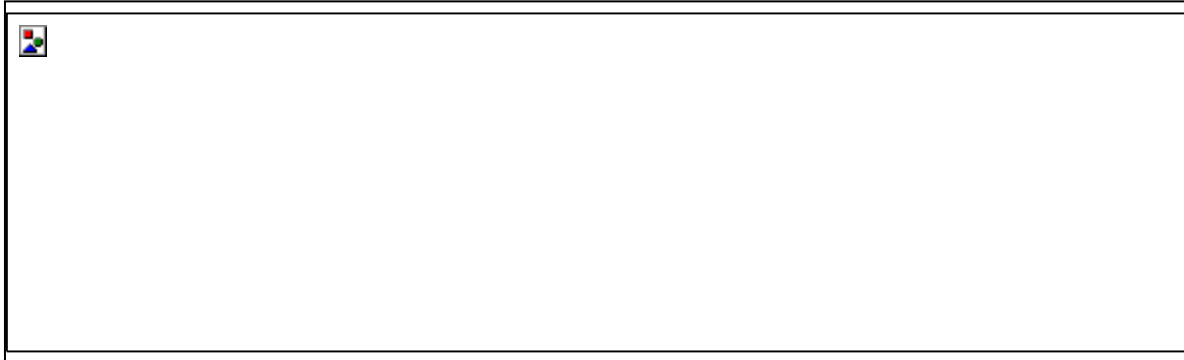
On the following pages all configuration menus are explained in detail in the order of appearance.

RCCMD - Web interface options in detail

In the following, we will introduce you to the functional elements of the RCCMD client and explain the settings that are available for the RCCMD web interface.

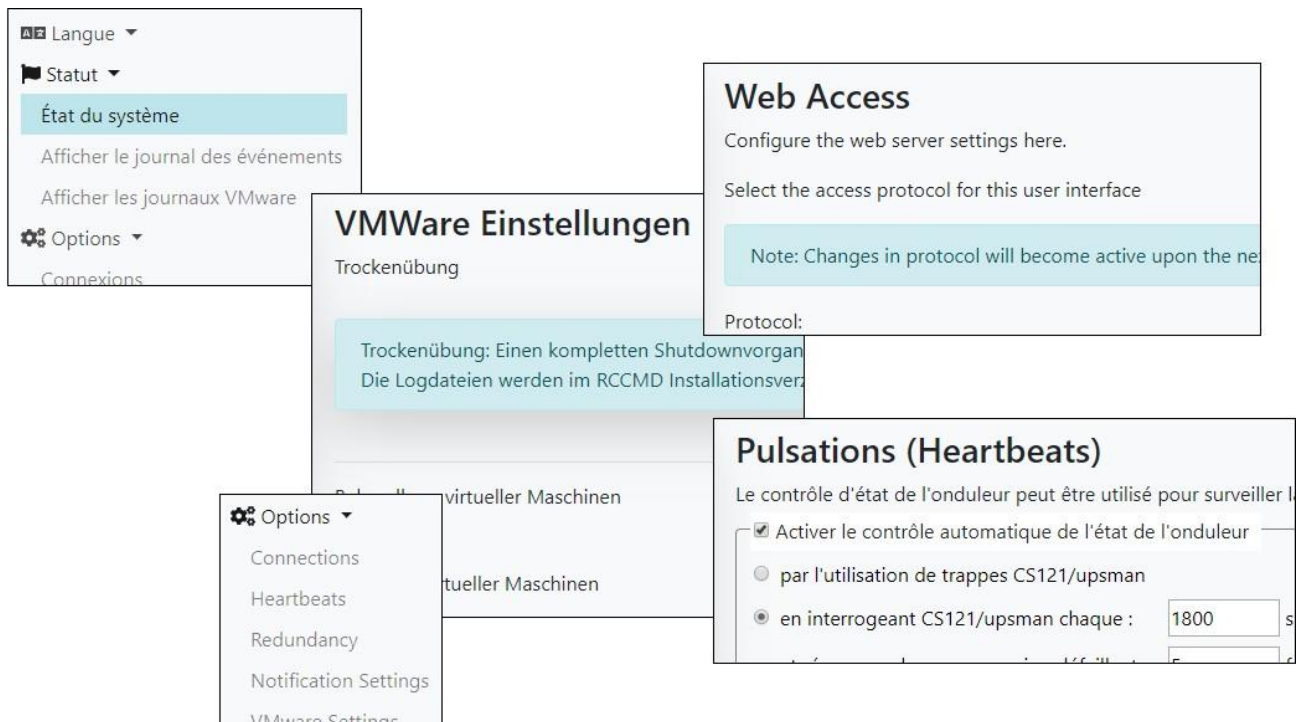
System tab Language

For language options, select the system tab -Language



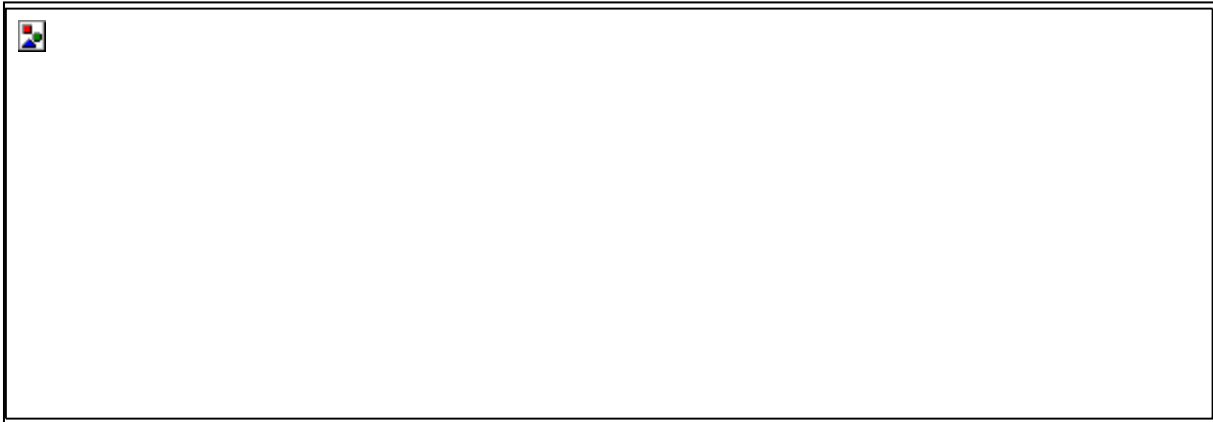
RCCMD supports the languages German, English and French.

To switch to the corresponding language pack, select the appropriate language. RCCMD will switch to the language at once without a restart.



System tab: Status

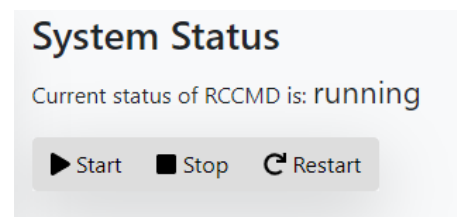
This menu contains general information about the RCCMD operating state and all available log files.

*System Status*

The system status is an interactive dialog which provides immediate information about the current operating status of RCCMD:

The buttons provide the following actions:

Start	Starts RCCMD when stopped
Stop	Stops RCCMD when starts
Restart	Stops and Restart RCCMD



Depending on the current action, the Current status of RCCMD will be shown:

Not running

Current status of RCCMD is: **not running**

RCCMD is disabled and will not protect your server.

Running

Current status of RCCMD is: **running**

RCCMD is online and waits for incoming signals.

The peculiarity of this function

All settings during configuration will be cached temporarily, RCCMD will continue to work in the background with the configuration of the last system start.

To activate the new configuration, it is mandatory to stop, start or restart the RCCMD service.

Event Log



RCCMD logs events concerning the RCCMD service:

- Notifications
- System Events
- Actions
- Executed scripts

RCCMD logging includes these information

- Date of the event
- Time when the event arrived
- IP address of the sending device
- Success / failure while executing a job

Using this event report, complex event chains can be traced back in individual steps and evaluated in conjunction with the event logs of the associated CS141.

By doing so, it is possible to track:

- When a server shuts down
- Why a server shuts down
- How fast a system reacted to an incident.

Event reports help to break down complicate issues and may show futural problems.

Downloading an event log

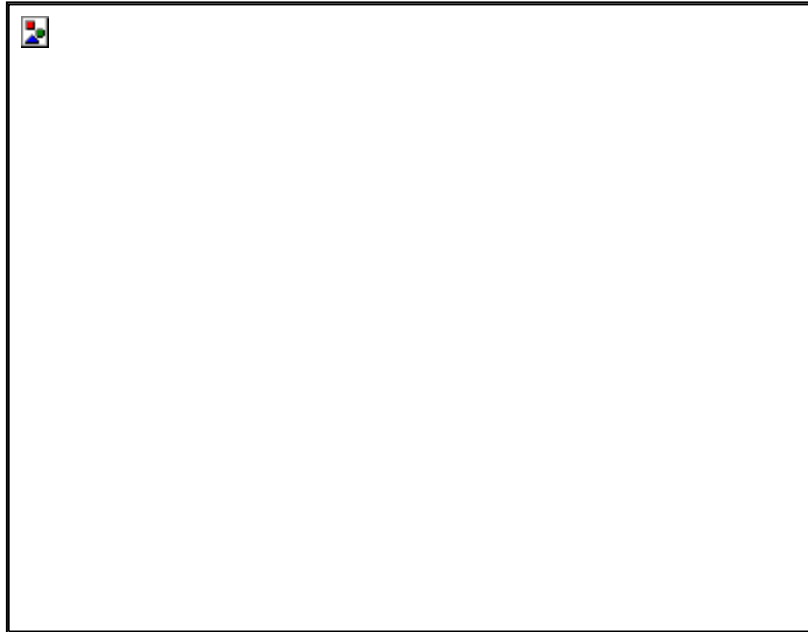
Larger companies require regular status reports on IT security.

RCCMD therefore allows you to download and export the log files to a CSV file that is integratable into external monitoring systems and databases.

You will find the download link below the last log entry:



View VMware Logs



The RCCMD Appliance provides extensive log files to assist with the recovery of an incident.

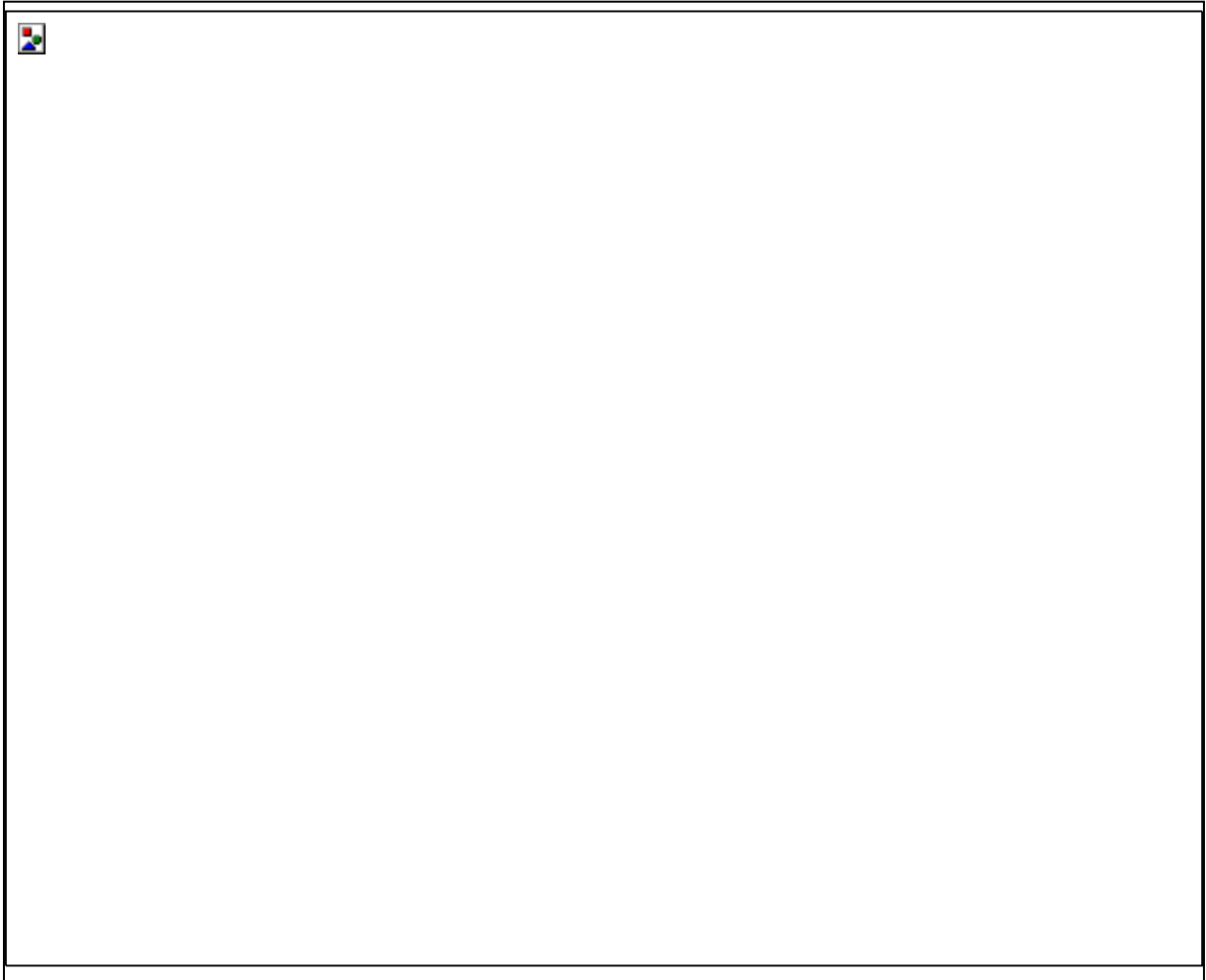
RCCMD logs the following information:

- ✓ Date
- ✓ Time
- ✓ Received signals
- ✓ Own communication attempts
- ✓ Executed scripts
- ✓ Dry run results

Depending on the depth of detail of the evaluations, you can use these log files to trace the path of a shutdown even over complex network nodes and compare them with other log files.

System tab: Options

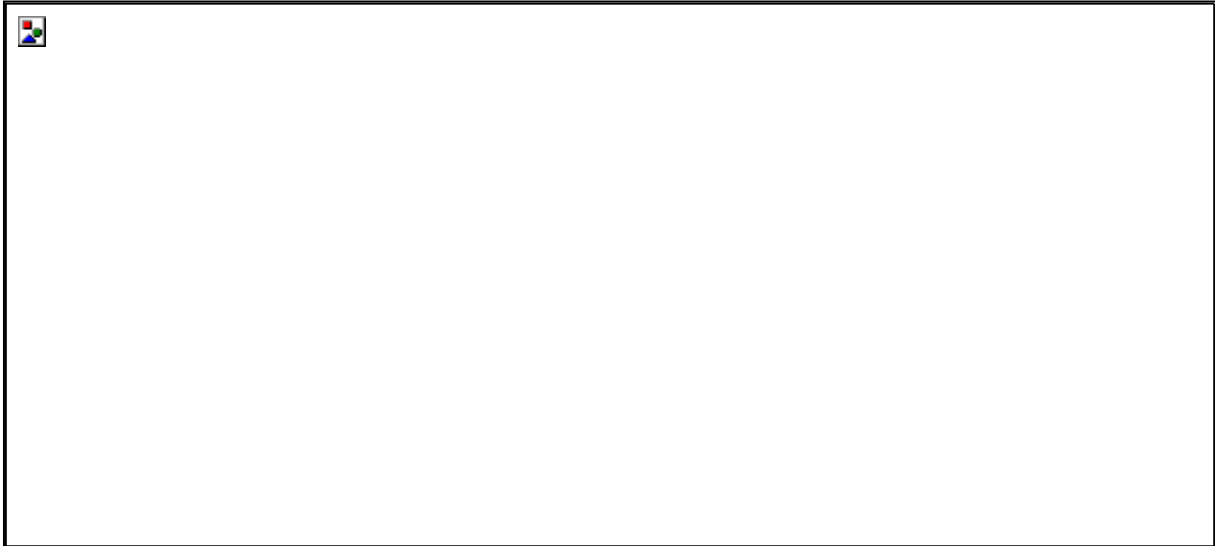
Under Options, you will find all the settings you need to configure RCCMD.



Connections*Define the permitted inbound connections*

If you leave this field empty, all incoming RCCMD shutdown signals may trigger a shutdown. As a surprise, this is an unfavorable condition that should be changed. By entering a sender IP, you limit which devices are in principle authorized to send a command to this RCCMD client.

RCCMD commands from unauthorized devices are logged, but the RCCMD denies an execution.



The Connections configuration dialog

Insert and Edit

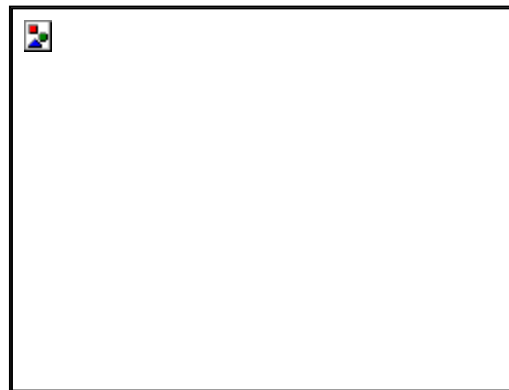
With insert, add a new IP address.

Save Changes will add the IP address to IP white list. Close aborts the process and exits the configuration dialog. Repeat the process until all RCCMD authorized stations have been recorded.

If the settings change over time, they can be edited:

Select an IP address and press Edit. The selected IP address is offered to you in the configuration dialog and can be changed by you according to your ideas. Save Changes complete the process.

Close cancels the process and terminates the configuration dialog.

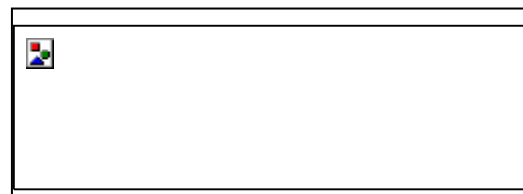


Valid is both, the IP address of the sender as well as a valid host name

Working with hostnames is always tricky:

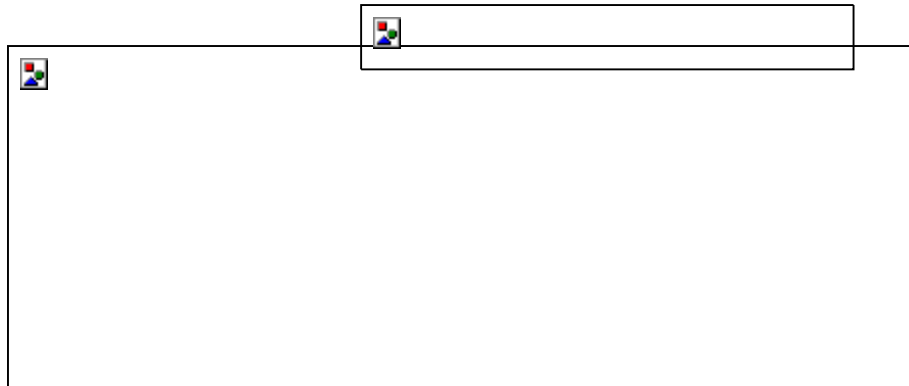
you also need a DNS server for translation between hostname and IP address this hostname is associated with. If the DNS server is down or the communication to the server is broken, RCCMD will not be able to contact the according host and manage a shut down.

RCCMD supports host names, but in order to avoid the issue described above, we recommend to use an IP address.



RCCMD is a client that will always wait for an incoming signal! You need to configure an RCCMD sender like the CS141 Web manager:

At UPS event management, select as job *RCCMD Shutdown* – you may choose between the IP address or the host name of the RCCMD client.



In critical resource management, it is advisable to eliminate as many interfering possibilities as possible.

As an example, if you need a server that can resolve the hostnames into IP addresses, the communication between client and sender will stop working as soon as the server is unavailable.

Therefore, the general recommendation is to use a manual IP addresses: by doing so, all devices inside a network segment can communicate with each other without additional server.

Note

If you configure the CS141 and want to see if the jobs you have configured are correctly received by RCCMD, you can use connections to create an inbound log. As long as the sender is not explicitly included in Connections, RCCMD will log the execution but refuse to execute it.

However, at least one IP address must be entered in order to activate this filter function.

Preparing UPS redundancy

Some settings depend on each other. If you have several UPS systems paired in operation in order to secure the server infrastructure, it may be necessary to specify more than one UPS to trigger a shut down command.

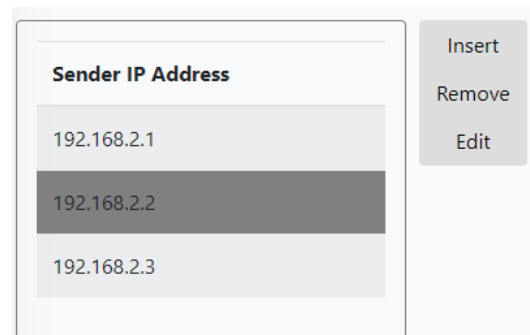
If you enter two or more valid IP addresses for a valid RCCMD signal, the "Redundancy" menu is automatically activated and can be used.

RCCMD can be configured to manage valid RCCMD shutdown signals from different sources. For details, refer to the menu "Redundancy".

How to delete an IP address

Click on the IP address and press Remove.
This will delete the IP address.

Remember to press Save changes at the upper right position to save your settings permanently.



Increase the connection security



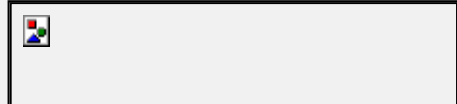
This feature adds security to your network, but conversely also increases administration overhead:

You can instruct the RCCMD to explicitly accept SSL-encrypted communication with a valid certificate. If a sender does not have an SSL certificate to identify itself, the connection is terminated.

In addition to this feature, you can instruct RCCMD to check SSL certificates are up-to-date. If the certificate becomes expired, it is considered invalid and the connection is terminated accordingly.

Note

Surely you have already noticed how often we point out that the save function changes the color.

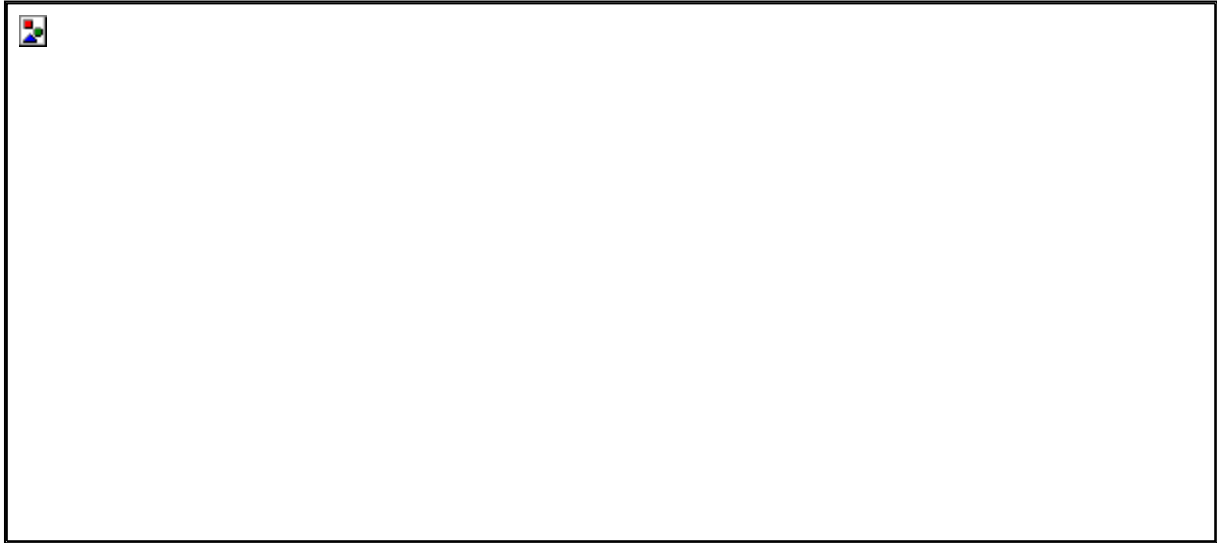


If you enter or change data within a configuration dialog, data are saved temporary, without any impact on current configuration. If your configuration work is done, you need to write your local settings to the RCCMD configuration file.

To activate the new configuration, RCCMD needs to be restarted - just press at Status stop / start or restart. RCCMD will re-read the new configuration and take over the new configuration.

Heartbeats

The heartbeats function provides an availability lookup. The communication between RCCMD client and the associated server can be monitored and logged:



In principle, two basic sources of interference are checked:

1. The general network accessibility
2. The UPSMan service of the CS141

This test is not designed to run complex network diagnostics. RCCMD can use this test to find out if the RCCMD signal sending device is available and as well as working properly.

The RCCMD client offers two basic options:

- Automatic mode

Enable automatic UPS alive check

- by the use of CS121 / UPSMAN Traps
- by polling CS121 / UPSMAN every: seconds
and retry each failed connection: times

You can choose between two different options:

UPSMAN Traps

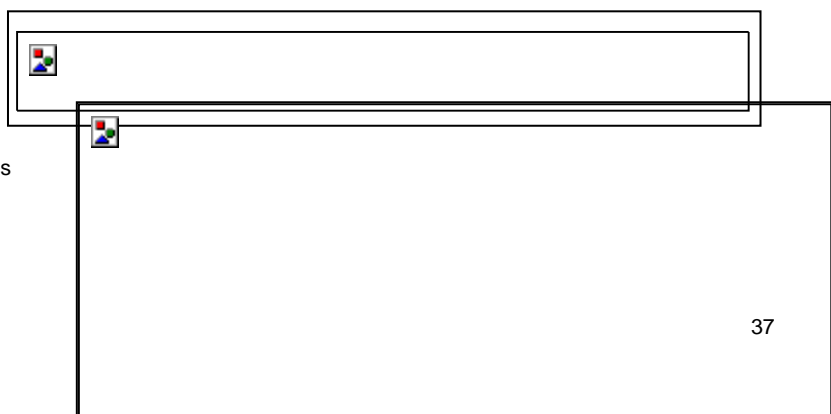
An RCCMD server sends a trap message to the RCCMD client. The receipt of this message is logged accordingly.

By Polling

The RCCMD client cyclically requests a message from the RCCMD server and logs the reachability of the remote station. In case of connection lost, the queries can be repeated as often as configured. If polling ends unsuccessful, an automatic script can be started.

This script can be customized freely to your needs. With Edit File ... you can directly edit and adapt the file in the web browser.

To edit this file, Linux scripting knowledge is mandatory.



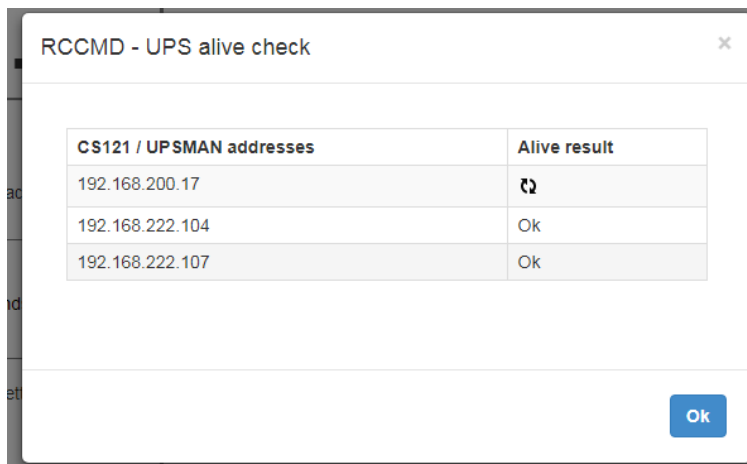
The Manual mode

With Test UPS connections, RCCMD provides a tool that enables quick accessibility lookup test.

Run alive check now ...

opens an additional window. All RCCMD devices entered at Connections are listed and will be queried.

Lack of communication readiness and missing availability will be displayed accordingly:



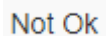
CS121 / UPSMAN addresses	Alive result
192.168.200.17	🔄
192.168.222.104	Ok
192.168.222.107	Ok



... Testing in progress



... Testing complete, device is available und UPSMan service is running



... Testing complete, device not found.

Please note: RCCMD will show the result for information and troubleshooting purposes.

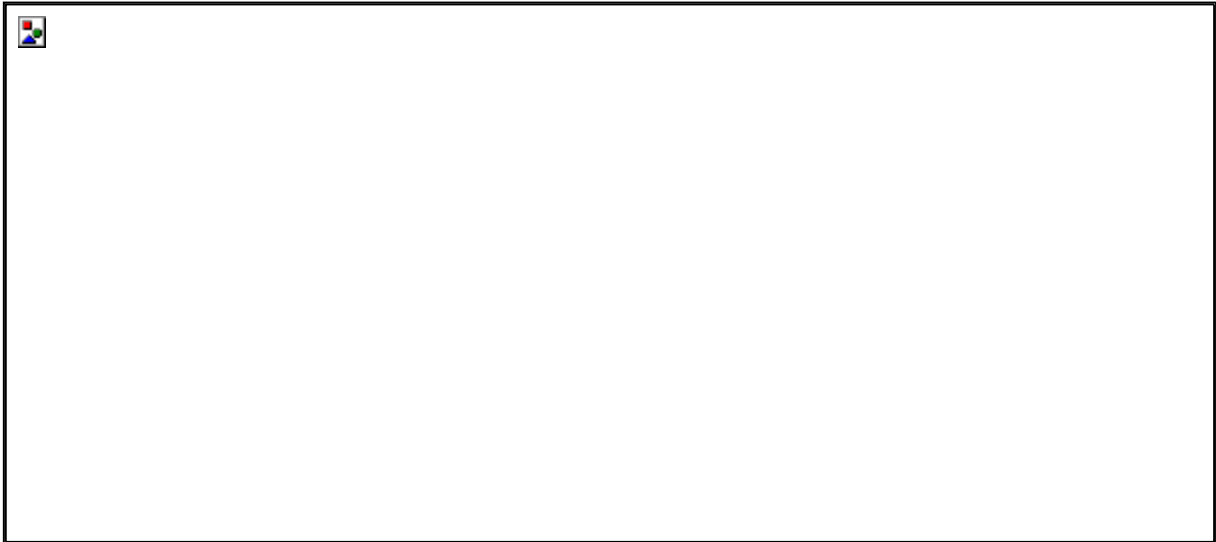
An Alive Check may fail under the following conditions:

- Network failure or broken infrastructure
- Target device is switched off
- Locked or misconfigured ports
- incorrect routing
- UPSMan service does not answer

Unlike automatic polling, no automatic script is executed on failure, as RCCMD assumes that an authorized administrator is monitoring this manual lookup process.

Please note that the configuration will only take effect after you have pressed the green Save Changes, as the RCCMD Client must be restarted for this function.

**Redundancy**



The redundancy behavior depends on the settings of Connections and Heartbeats:

For the redundancy behavior to work properly, two preconditions must be met:

1. Two valid IP addresses must be specified under Connections.

At least two IP addresses must be stored and allow inbound RCCMD commands.

Redundancy means, RCCMD should not shutdown the server until at least two transmitters have instructed to power down the host.

2. The heartbeats must be set to "Automatic UPS alive check by polling"

RCCMD is instructed by the heartbeats to automatically check the availability of registered IP addresses:

Should a registered UPS become unreachable and the redundancy system shuts down, RCCMD will assume that there is a serious problem and shut down the system ignoring the redundancy setting.

Note:

Keep in mind that the intervals between lookups can be crucial for a shutdown.

Note: The redundancy behavior refers exclusively to the RCCMD command shutdown

Other commands are handled individually and logged accordingly. With the ability to run your own scripts, RCCMD offers options to bypass the standard procedures in case of an emergency.

Defining redundancy levels

First activate the RCCMD redundancy function.
Then select the IP addresses that are allowed to send a shutdown signal.

The Redundancy Level is depending on the number of selected devices:

Number of selected units X -1

By using two devices, both need to send an RCCMD shutdown signal.

Since only two systems have been selected, only a maximum of one additional system can send this command. Thereby it is not important, which device is the first sender - this may change dynamically.

For 3 selected systems, the maximum value is 2:

If 1 unit + 2 other units instruct the shutdown, it will be executed. RCCMD does not differ which of the three systems sends the first shutdown.

Using 3 systems, you can also change the Redundancy Level to 1:

Enable RCCMD redundancy function

Group	Sender Addresses
<input checked="" type="checkbox"/>	192.168.200.17
<input checked="" type="checkbox"/>	192.168.222.104
<input type="checkbox"/>	192.168.222.107

Redundancy Level:

As a consequence, two out of three systems are needed for RCCMD to shut down the server. The combination may change dynamically. If you just want to pair 2 of 3 UPS systems, it is recommendable to select them and set the redundancy level to 1. By doing so, the shut down will only be done if both selected UPS's will send a shutdown command.

Keep in mind:

With redundance, you combine several devices. Under connections, you allow general incoming shut down signals. As a consequence, it is possible to configure one redundancy shutdown as well as several single shutdown sender.

Note

Please keep in mind that a shutdown instruction remains active until the system which has instructed the shutdown explicitly withdraws it. This is controlled via the RCCMD Custom Command *wakeup*.

Shutdown behavior with two UPS systems

In case of a shutdown signal, The redundancy will check the connectivity and the availability of the second UPS system are. If it answers properly, the shutdown signal will be suppressed with reservation until further notice:



As soon as the second system instructs a shutdown, this command is executed and the system shuts down. If a shutdown signal is sent by the first system and the second system is not reachable, RCCMD shuts down the system - in this case, RCCMD assumes that the second system is not available.

Shutdown behavior with three valid devices

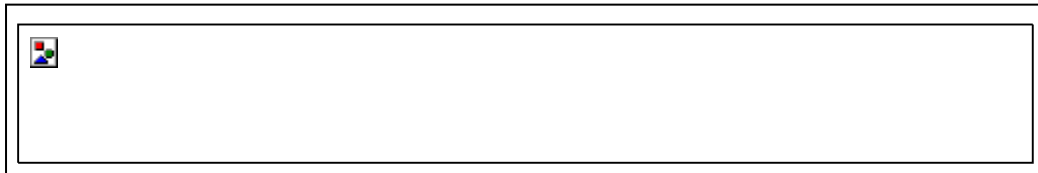
From three devices onwards, the redundancy behavior can be individually adjusted to necessary conditions:

1. If one of three systems send a shutdown
2. When two out of three systems send a shutdown
3. All three systems must decide the shutdown together.

Each system can individually instruct and withdraw its shutdown via the RCCMD Custom command *wakeup*. In general, RCCMD will not execute the shutdown until the exact shutdown condition is met.

Redundancy-related scripting

If you use redundancy behavior, the RCCMD client waits to execute the shutdown until the appropriate number of devices also instruct the shutdown.



Because this process has a direct impact on the operation of the servers being monitored by RCCMD, a script will be launched to indicate an incident.

Use Edit File ... to customize and adapt this script to your individual requirements.

Abort will close the editor and withdraw all changes you made.

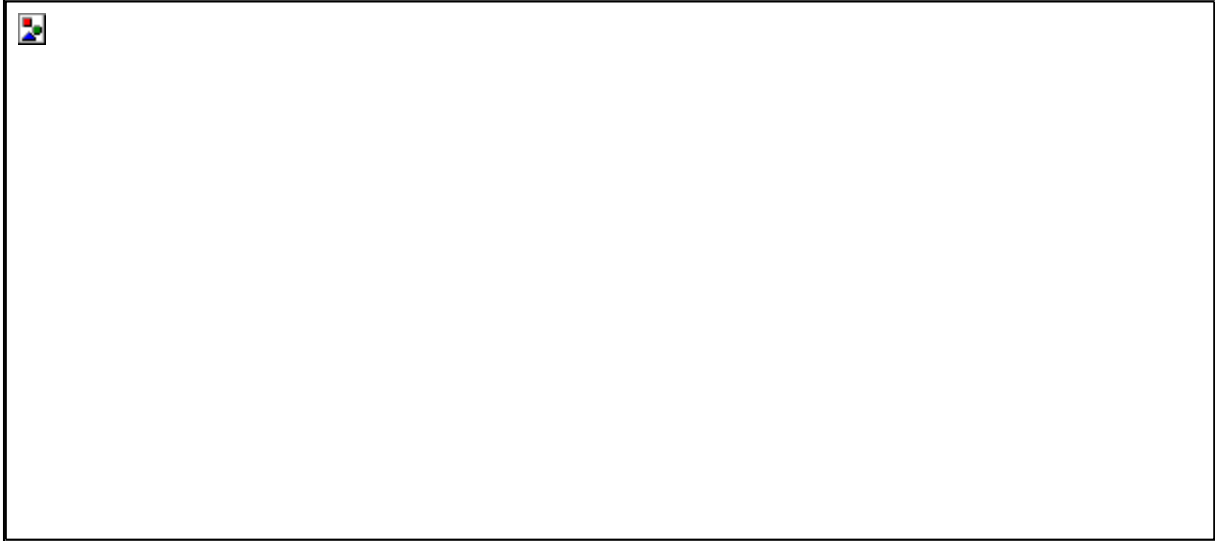
As a default, a text notification is pre-defined to indicate a redundancy-based shutdown behavior.

```

/usr/rccmd/ShutdownSuppressed.sh

/usr/rccmd/ShutdownSuppressed.sh
#!/bin/bash
#
/usr/rccmd/rccmd_message.sh "Alarm ! RCCMD Shutdown Signal received -
Shutdown is pending as long as redundancy is present. NOTE: Please stop/restart
RCCMD service when problem has been solved to reset the alarm. This restart
avoids unwanted shutdown at the next alarm situation."
  
```

Abort Save Changes

Notification Settings

Depending on which command is received by a valid RCCMD transmitter, three basic scripts are executed automatically. Each script triggers an RCCMD functions. The RCCMD routines are preconfigured and normally there is no need to edit them.

However, if you want to execute your own scripts by RCCMD,

you can either write these scripts directly to the appropriate .sh - script and execute them as a custom command or you may edit these basic files.

Warning:

If you modify, customize, or extend these scripts, you change the overall behavior of RCCMD within your system. Be sure to make a backup before editing the scripts to find back to the original system state. Changes to the original configuration may result in unpredictable behavior of RCCMD and may cause system-wide problems.

Edit these scripts at your own risk!

When will these scripts be executed?

RCCMD differs between three different scripts:

Email notification

The CS141 will normally rely on its own mail client - this is also the recommended way. However, in some high-security networks, it may not be desirable for the web manager to be able to send their own mails. The RCCMD client can be used as an interface to forward short mail messages.

You can also use this script to trigger additional scripts:

Send an email AND execute the following script ...

for this function, the freeware Linux tool send mail is installed, which allows RCCMD to send e-mails. You can configure the tool at any time by logging in via a console on the Linux interface of the RCCMD client.

To forward an email from a CS141, use the Custom Commands and enter the following command by entering the IP address:

Mail targetmailaddress@targedmailserver.com <Text message>

At the Cs141, you will enter:

mail Kirk@enterprise.de Jean-Luc Picard was here

RCCMD would take over and write a mail to kirk@enterprise.de with the topic „Jean-Luc Picard was here-.

Is the only function of this script the trigger of an email?

No, this script can be edited to do everything. ...

- changing the complete script will cause changing the behavior and may cause RCCMD will not run as expected.
- Edit it at your own risk.

Message Notification

This script controls the receipt of messages and is responsible for displaying them on the monitor. Because the RCCMD appliance is a non-graphical server program that runs without permanent a permanent monitoring, you should leave this script simple as it is:

Since it is triggered by each incoming RCCMD notification signal, additional content would also be executed each time.

Due to the fact, this is mostly without a function (no graphical interface) you may use it for routine scripting

- changing the complete script will cause changing the behavior and may cause RCCMD will not run as expected.
- Edit it at your own risk.

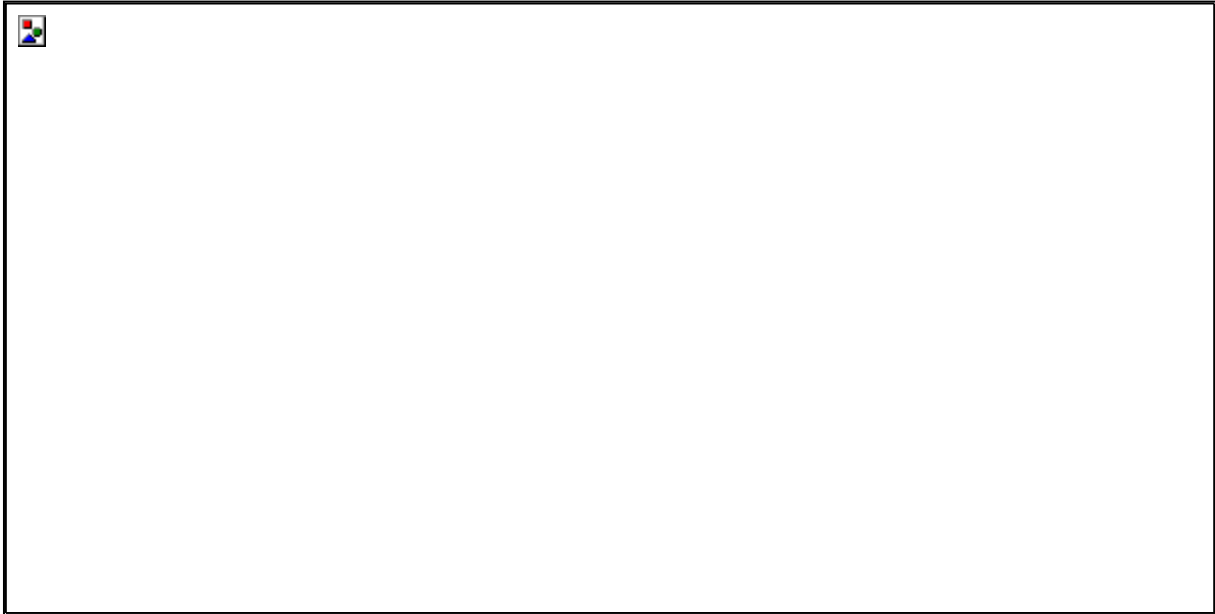
Execute Notification

This script is interesting:

This script executes all valid incoming commands a CS141 may send. This script triggers the complete shut down routine RCCMD provides

With this script, RCCMD will provide you the unique option to add and trigger your very own customized shutdown scripting solution and even program an additional non-standard routine that specifically met exactly your network.

- This script is a very powerful option as well as dangerous because changes directly interfere with all functions of the RCCMD. Any changes and enhancements you make will directly affect the shutdown behavior.
- Advanced scripting skills in Linux are essential for changes to this script!

VMWare Settings

The VMWare settings control the overall shutdown behavior of servers and hosts within VMware. Depending on the configuration level and configuration type, different types of configuration are necessary in order to manage a VMware based infrastructure. In addition to the mandatory basic data like IP addresses user credentials, you may need, among other things, more specific knowledge about the shutdown behavior of your IT landscape.

Please note, some data are not static. Values may change and should be adjusted during regular system checks..

→ RCCMD evaluates and displays estimated shutdown times according to entered data.

Part 1: Basic setup

The basic settings assume that you are running hosts without vCenter. You can shut down as many hosts as you want with one RCCMD appliance:

Virtual Machine Management

This menu defines whether you want the hosts and virtual machines to be managed by RCCMD or by a vCenter. If you operate the hosts in lock-down mode, e.g. the control commands are exclusively approved by a vCenter. Even if you enter the credentials correctly, the host will deny command execution.

In the default setting, "from RCCMD" is preset.

Virtual machine behavior

Use this setting to define whether you want to use vMotion or just shut down your machines. A virtual machine shutdown will be controlled directly by the host:

the virtual machines are shut down normally, and then the host is turned off.

If you enable vMotion, local shutdown of virtual machines is the secondary protocol. First, the vCenter will try to move the virtual machines to another host.

The default setting is "Shut down virtual machines".

→ If maintenance mode is selected, additional information are required like credentials of the vCenter as well as a time window that should be available for the vCenter to move virtual machines to another host.

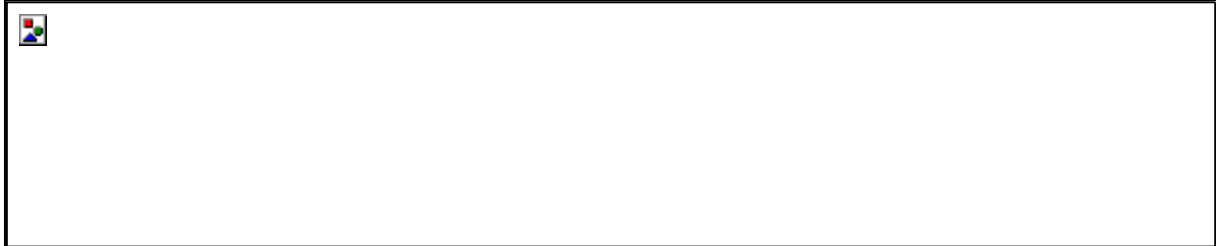
Safely decommission vSAN nodes auf no vSAN in use

This setting defines the shutdown behavior in case of a vSAN is in use - The vCenter provides different basic settings, to be selected at this configuration point. If you want to use an RCCMD-managed vSAN, refer to the basic requirements that must be met.

The default setting is "No vSAN in use".

VMware running RCCMD

RCCMD needs to know the name of the virtual machine that contains the RCCMD appliance. This setting prevents a shutdown of the RCCMD Client.

*Tell RCCMD all ESXi Hosts to shut down*

With this configuration dialog, declare which ESXi hosts has to be shut down by RCCMD:

The menu bar provides several functions:

- Add: Add another host. To remove a host
- Remove: Select a host and click Remove to remove it from the current list
- Edit: Select a host. With Edit you can edit the access data.
- Verify: If you press this button, the current configuration will be saved and the login data will be validated. At verified, RCCMD shows the connection attempt.

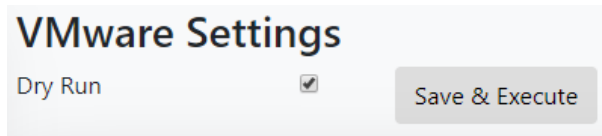
Estimated shutdown time

After the configuration job is done, RCCMD shows an estimated shutdown time:



This is the current average shut down time of your IT infrastructure. Please note, this shut down time is calculated and can be used to compare it with the emergency power time granted by the UPS.

Due to the fact this is a calculated value: Please test you shutdown setting before activating!

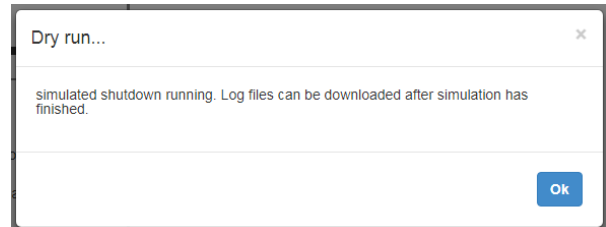
Dry Run installation test routine

With the Dry Run RCCMD offers a unique function within the VMware settings:

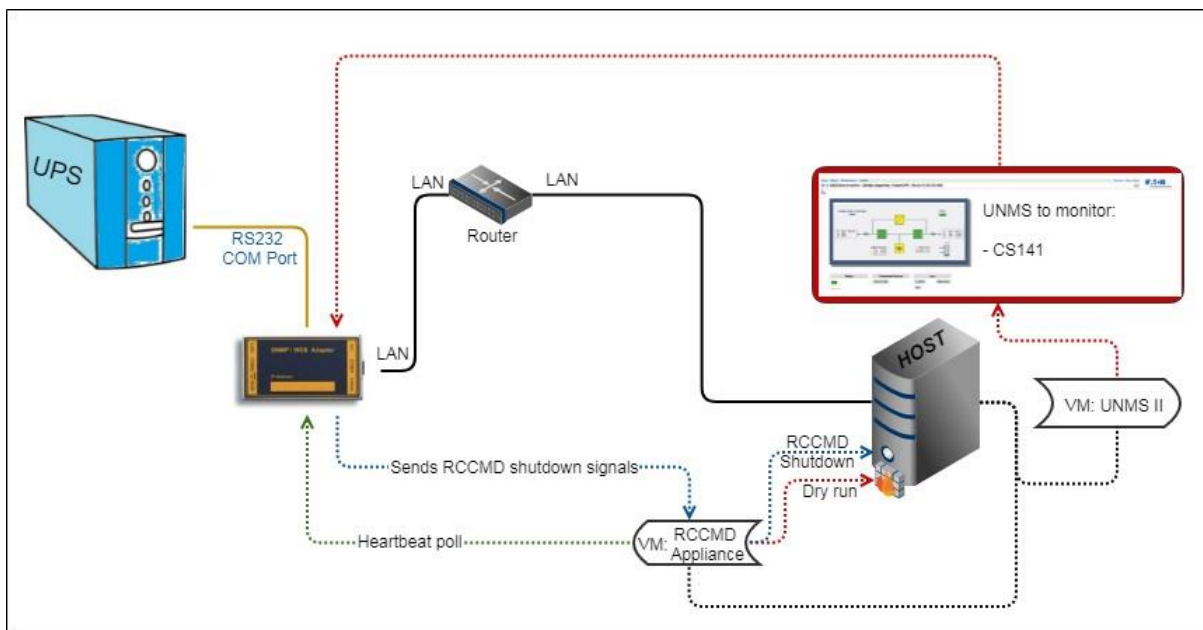
The Dry Run is a simulation mode, in which your RCCMD installations simulate the behavior, but do not physically execute.

This feature is useful when installing an RCCMD installation on a production server:

Accidental shutdown is prevented in this way. With Save and Execute, this feature is enabled, protecting your future configuration from accidental shutdown.

**Note**

Some configuration menus are locked during testing and cannot be adjusted "in between".

What a „Dry run“ does ...

Normally, a CS141 is the RCCMD server that sends a valid RCCMD command to an RCCMD client - the RCCMD software. The command and what to trigger with it depends on the final operating scenario. Due to the fact you can use the event handling from the CS141 for sending individual commands in order to start very delicate and complex scripts, it is possible to automate a server via scripts in many parts - you do not necessarily just have to shut down a server with RCCMD.

With VMware, the RCCMD appliance differs from normal client installation:

It is designed to ensure a structured shut down sequence for all hosts within a VMware environment-

To fulfill this task, RCCMD needs access data coming with system rights to allow a shutdown. The problem that RCCMD cannot differ between a real emergency situation and a user who press the test job - button at CS141. During testing, this is could be a problem. As soon as RCCMD will accept a valid signal, it will start the shutdown procedure - It is comparable with the quiet "OK" - console command of any normally shown „Are you sure " - Dialog inside an operating system.

Of course, you cannot simply shut down "all servers" during operation because you want to test your configuration - shutting down a real-time system with 100% availability is just for real emergency issues....

The dry run is a build-in self-running simulation mode

1. All configured hosts will be contacted
2. Credentials for the hosts will be tested
3. a protocol log will be written to log configuration issues as well as successful login tests.
4. The standard RCCMD shutdown signal is suppressed as long as simulation mode is active.

As long as dry run is active, no emergency shutdown is possible via any valid RCCMD server device.

Note:

If you change or adjust the standard scripts coming with a default installation or add new scripts, they will be executed consequently. The Dry Run only suppress its own standard scripted shutdown sequence - it does not check the changes you added manually.

This behavior contains advantages as well as disadvantages

1. Due to the fact your "sharp" scripts are executed mercilessly, the Dry Run test should take place beforehand!
2. By adding your own scripts that trigger harmless actions, you can check if your "sharp" scripts would work and all administrative shares on the target system are met.

Part 2: Advanced settings

If Maintenance Mode (vMotion) is selected



RCCMD will present two addition menu entries:

Maintenance Mode Timeout in Seconds



This value defines the time window that RCCMD grants the vCenter to move virtual machines to host that are not going down into maintenance mode.

Virtual machines that have not been migrated within this time window will be left for shut down by the ESXi host.

vCenter credentials

In order to use vMotion, RCCMD need valid vCenter credentials. Please note, an RCMD client can shut down many hotsts, but technically only maintain one vCenter. if you need to configure several different configuration types, it may be necessary to use 2 RCCMD appliances that work together.

Check values

Test the vCenter credentials. RCCMD will try to log into the vCenter and give a feedback including a reason why the login attempt failed.

Enter the vCenter Server credentials:

Host name or IP:	<input type="text" value="192.168.200.85"/>
User name:	<input type="text" value="administrator@vsphere.local"/>
Password:	<input type="password" value="*****"/>

Part 3: Selecting "Host are also vSAN nodes" at vSAN Safely decommission vSAN nodes

This setting enables several sub menus and a vSAN time out warning.



Keep an eye on this warning message!

A vSAN is a little bit tricky when running a shutdown routine and the vSAN has been terminated incorrectly. It is even possible that a wrong configured shutdown routine leads into data corruption or even total data loss.

vSAN shutdown options*No data evacuation*

This is the fastest way to ensure system shutdown. It shuts down the virtual machines, and then the vCenter synchronizes all the hosts that are inside the vSAN. There will be no data migration or virtual machines to be moved to other hosts.

Evacuate all data to other hosts

In principle, it is the same function that triggers vMotion. A vSAN can also be spanned across different sites, so you can also offload virtual machines to external hosts that are not in the vSAN cluster you are about to shut down. If you use vMotion, it will be executed first. Due to this fact it is possible that your vSAN host has no virtual machines that need a migration. But you may use it as "second try" to move machines away from your vSAN...

Ensure data accessibility

If larger vSAN systems provide enough capacities for redundancies, no data will be moved. Data migration will only be done for data without redundancy.

Note

With vSAN extensions, RCCMD introduces solution to allow you performing an emergency shut down of the entire vSAN system as fast as possible - virtual machines that have been previously migrated to another location via vMotion are not affected.

Due to the fact you want to stop and shut down the vSAN because there is an emergency, selecting "No data evacuation" is the best choice.

vSAN Resync timeout in Seconds

This setting is the basic time window RCCMD grants the vCenter synchronize the databases between the hosts before starting the next point in the shutdown sequence. This time window is a little bit tricky, because the resync time is a very relative value - in principle you can say it lasts as long as it takes ... the vCenter does not tell you an estimated resync time, you need to test it during a manual shut down. If your vCenter announces the job is done, you have the minimum time window for your emergency shutdown. Please calculate some extra time for this time window because the measured time during a manual shutdown is just a snapshot and not a general value.

Seconds to wait before setting Maintenance Mode for vSAN

Once the resync is completed, the vCenter is the last surviving virtual machine that needs to be shut down. With this setting, you define how long the vCenter has time to shut itself down before RCCMD starts the next step of the shutdown sequence.

Determine which VM is running the vCenter



Inside a vSAN, the vCenter is more:

The vCenter manages the complete data transfer within a vSAN and handles the complete post synchronization phase during a vSAN shut down. This means:

If the vCenter runs inside a vSAN or runs on a host that will be shut down to fast, the complete vSAN hung up. If the vCenter is located as a virtual machine within the vSAN, RCCMD needs to know the name of the virtual machine in order to exclude it from virtual machine shutdown.

Note:

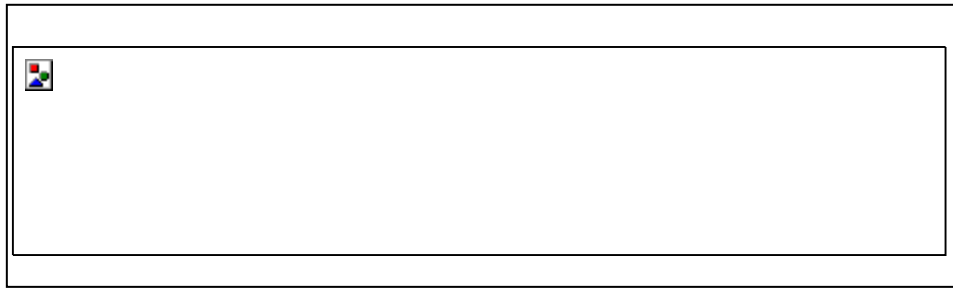
The vCenter that handles a vSAN is not always inside this cluster – it may be installed somewhere and handled separately. If the virtual machine with the vCenter is not inside the list of the hosts to be shut down, you do not need to enter it at this point. But you need to take an eye on it if when using different RCCMD appliances – Without it's vCenter, a vSAN cannot shut down as expected.

Advanced Settings



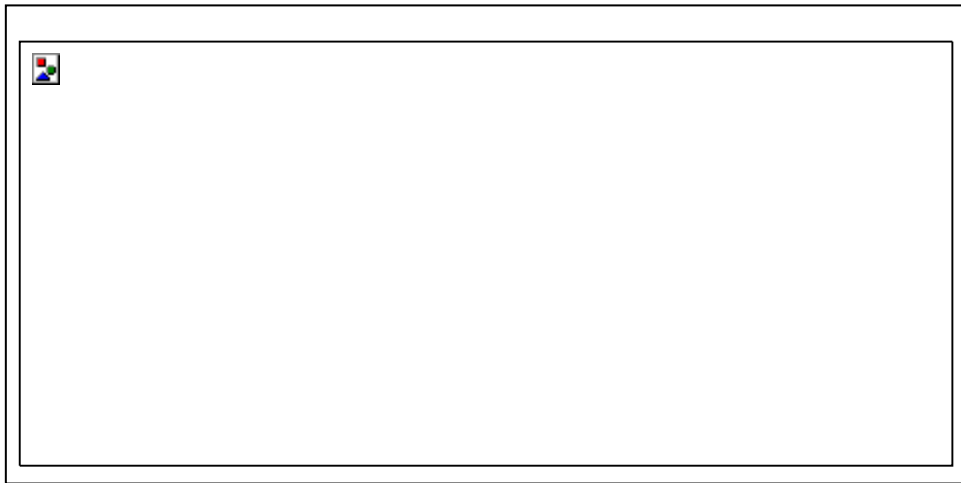
use Advanced Settings for additional settings to configure RCCMD. The menu is divided into three parts:

Event Logfile

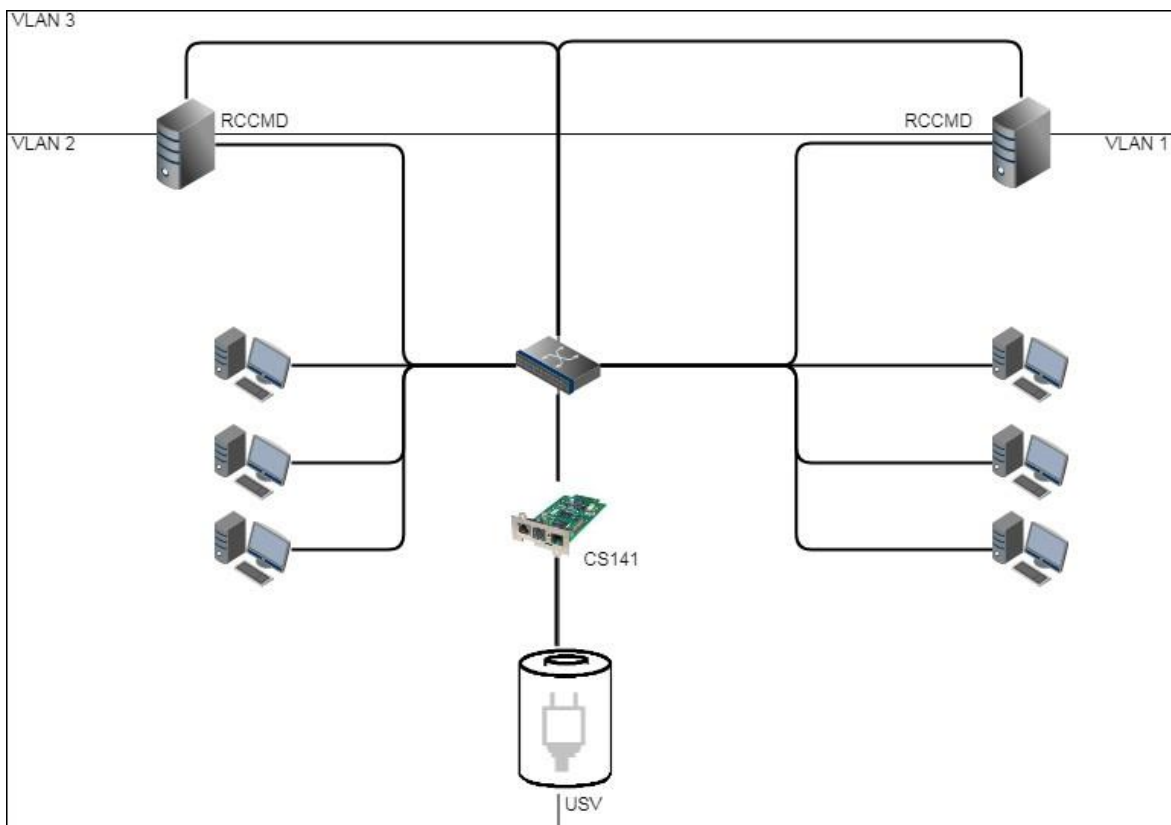


In general, any RCCMD Signal affecting the client will be logged. Due to the fact server systems may provide limited memory resources for log files, it may be necessary to limit the size of the log file to a maximum size to consume. In case the maximum file size is reached, the oldest entry is replaced by a new entry.

RCCMD Bindings

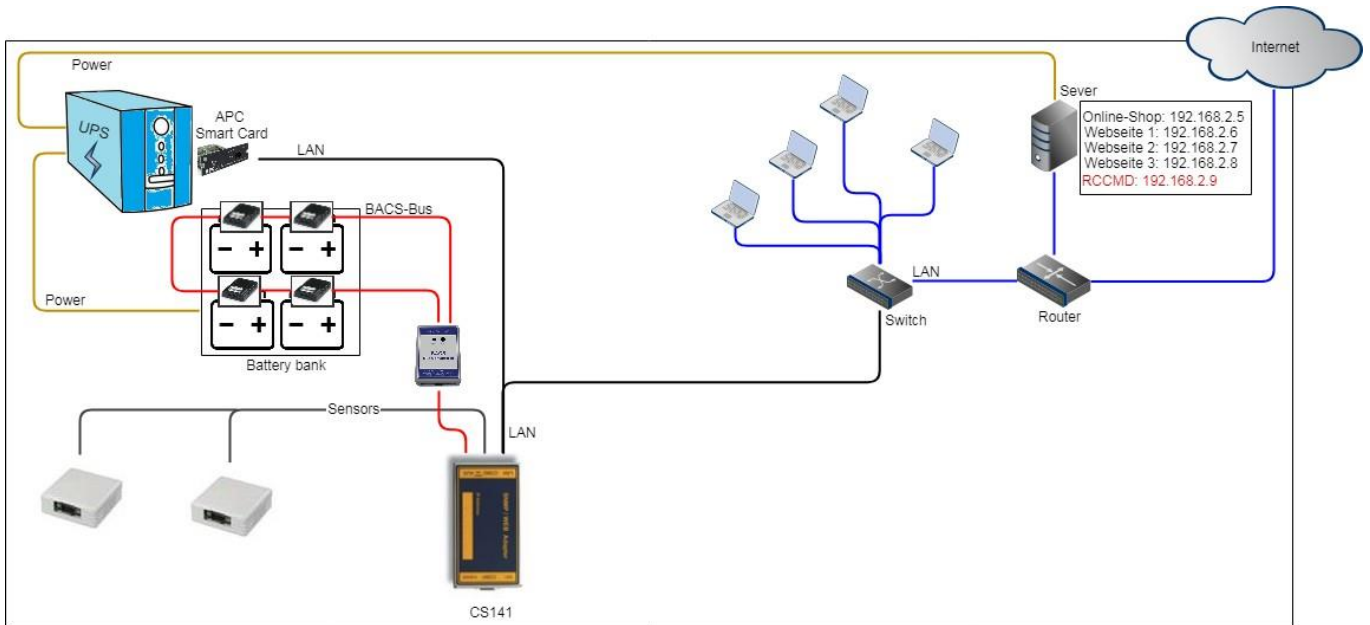


RCCMD Bindings is a sophisticated tool that helps you to limit traffic. Since this setting deeply affects your network setting, it should be used with caution. The bindings allow forcing RCCMD to listen on a specific network card. In case of multihoming is in use, the listener can be configured to a specific IP address within one network card. As an example, this will be used if there is a necessity to divide the network logically into a production network and an infrastructure network via VLAN:



In this example scenario, two or more network adapters can be installed. Binding RCCMD to one specific network card will prevent users to access the RCCMD client and accidentally shut down a server - this is only possible via devices that are located in VLAN 3 or have been properly enabled via a router.

Another scenario is the so-called multihoming:



It is not absolutely necessary for modern network devices that an IP address is firmly linked to one network interface. In fact, multiple IP addresses can be connected via a network interface - they share hardware, but otherwise form self-contained instances. As an example, this could be a web server that manages different websites with a unique IP address: the server is connected by a router that determines between incoming signals and signals provided by local network. Bindings will instruct RCCMD to listen for incoming RCCMD signals only at a specific IP address that is assigned to the local network only.

Note

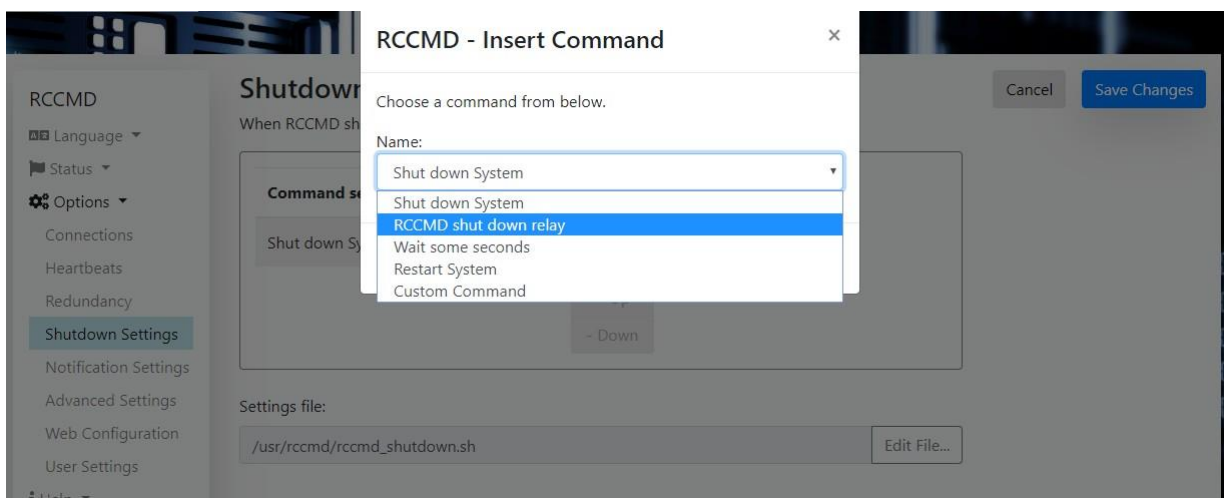
These configurations are used in special scenarios. Normally you can leave the setting 127.0.0.1 / local host, port 6003. In that case, RCCMD will listen on all available IP addresses for a valid incoming signal. Since you have defined the valid sender address at the menu Connections, RCCMD will notice the signal but deny execution and log this fact as an invalid RCCMD command.

Change RCCMD Target



The RCCMD appliance is more than just a small tool to handle just VMware hosts. On unchecking the checkbox and pressing Save changes, RCCMD changes to the local mode:

All VMware menus will be disabled and the Shutdown settings will switch to local options:



Due to the fact, RCCMD can not just receive, but also send RCCMD shutdown signals, it is possible to use an RCCMD appliance as a central RCCMD relay that runs with complete customized additional scripting.

When local mode is active, RCCMD provides the following command sequences:

Shut down system

RCCMD will shut down the server it runs on.

RCCMD shut down relay

With this option, RCCMD will forward a valid RCCMD shutdown to

- Single IP addresses
- An IP address range

With this option, it is possible to get advanced redundancy options - as an example, you may combine a CS141 and a second RCCMD client – if both advice a shutdown, the target RCCMD system will execute the command.

Wait some seconds

RCCMD will wait a customizable time window until the next command in the list will be executed.

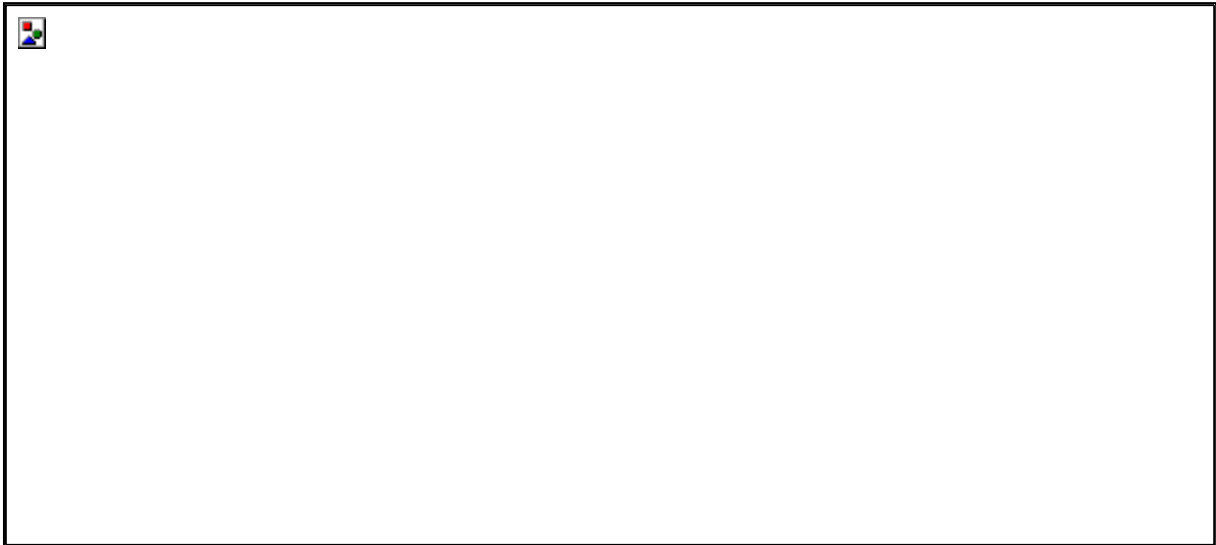
System restart

RCCMD will restart the complete RCCMD server that runs within a virtual machine

Custom command

Start programs, run kill-commands, run your own scripts, just enter the command and mandatory extensions and RCCMD will do the rest.

Web Configuration



Set the availability of the RCCMD web console.

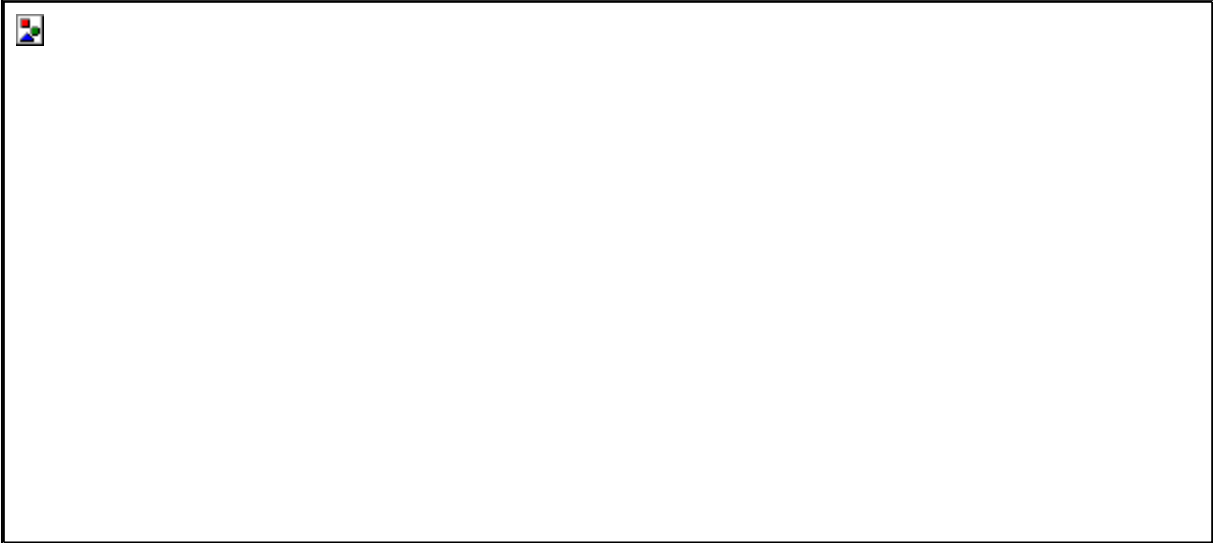
The default for web access is:

http: port 8080

https: port 8443

Please note changing the default values will cause the web console of RCCMD can only be reached via the ports you manually set.

User Settings



Customize the administrator password according to your ideas and company policies. Please note that this password also applies to the admin user on the console. The appendix contains instructions how to set up an emergency user for password recovery

Administrator User Name: `admin`

This user name is hard-coded and cannot be changed.

Current Administrator Password:

This is the currently assigned password.

New Administrator Password

Assign the new password.

Confirm New Password

Repeat the password you have assigned. Please note that Copy and Paste will repeat typing errors and may lock up your RCCMD client.

Note

Depending on the program version, there are two default passwords that can be assigned.

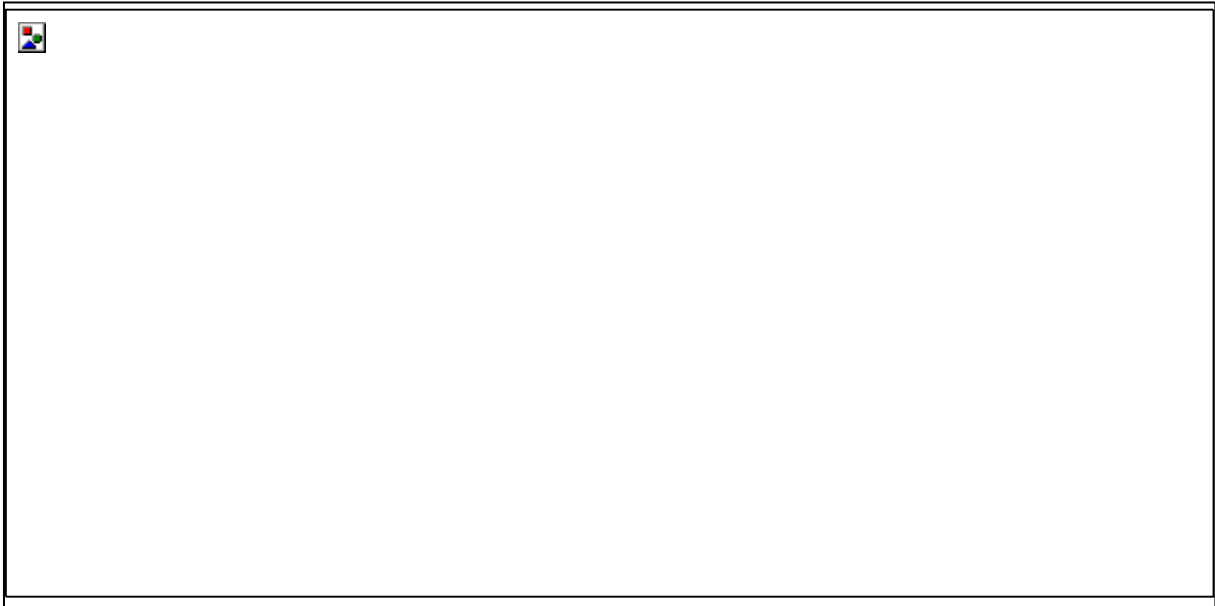
Program versions until 5/2018: cs121-snmp

Program versions from 5/2018: RCCMD

Due to the fact RCCMD comes with two years update authorization, it is possible that you need these two default passwords.

System tab: Help

If you do not know what to do...



Manual

You need help?

The manuals are available inside RCCMD – you do not need any additional network connection.

Due to the fact the manual is a pdf-file you may need additional software tools to open the according file.

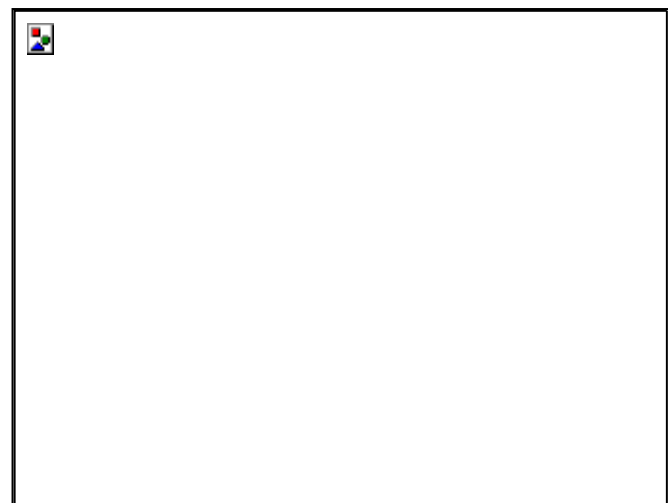


Info

Need additional information about your copy of RCCMD?

The info button will show

- Acknowledgements
- EULA
- Copyrights



RCCMD FAQ's*Setting up IP address data manually*

In some cases, a network design may not provide a DHCP server:

The carrier system starts, but without receiving a valid IP address RCCMD may use. Since the 100% availability of a DHCP server can never be given, it is advisable to assign a static IP address here. Search for the file interfaces – this file is responsible to manage dynamic or static IP address entries.

You need two commands to find required files:

Command: cd /etc/network

Command: ls

```
admin@rccmdAppliance:/etc/network$ ls
if-down.d if-post-down.d if-pre-up.d if-up.d interfaces interfaces.d
admin@rccmdAppliance:/etc/network$
```

The RCCMD appliance uses nano - a small and handsome editor to help viewing and editing files.

Command: nano interfaces

The editor opens and displays the contents of the file Interfaces:

```
# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
allow-hotplug ens33
iface ens33 inet dhcp
# iface ens33 inet static
#     address 192.168.200.223/24
#     gateway 192.168.200.1
#     # dns-* options are implemented by the resolvconf package, if installed
#     dns-nameservers 192.168.200.3 192.168.200.5 192.168.200.1
#     dns-search local
```

Configuring RCCMD network settings

Search for this crucial entry:

- ➔ `iface ens33 inet dhcp`
- ➔ `iface ens33 inet static`

Basically, these two configuration lines decide whether to use a static IP address or the appliance asks for a DHCP server.

```
Source /etc/network/interfaces.d/*

# The loopback network interface
Auto lo
Iface lo inet loopback
#The primary network interface
allow-hotplug ens33

#iface ens33 inet dhcp                <- use # to disable DHCP
iface ens33 inet static                <- Remove # to enable manual IP address settings
address 192.168.200.99                 <- Enter static IP-address
subnet 255.255.255.0                  <- Enter subnet mask
gateway 192.168.200.1                 <- Enter IP address of the gateway

# dns-* options are implemented by the resolvconf package, if installed

dns-namervers 192.168.200.3 192.168.200.5 168.168.200.1    <- Enter DNS Server Ip address data
# dns-search local
```

After reboot, the appliance should use and display a static IP address.

Note

If you choose to enter the IP address assigned by the DHCP server during startup as a static IP, ensure this IP address will be removed from the pool of dynamically assignable IP addresses. Alternatively, you can assign a fixed IP address via DHCP server and enter it statically in the appliance. By doing so, RCCMD will definitely be assigned an accessible IP address, which greatly increases resilience

Setting up an emergency user for RCCMD on VMware

2a. Setting up an emergency user

Note

You do not want it, but passwords can be lost - unfortunately always in company of big trouble:

For complex systems, a lost password can be very cumbersome and expensive, e.g. if complex scripts need to be completely rebuild from scratch. The emergency user is not an all-in-one Solution for these problems, but it may be very useful if something unexpected occurs. You can configure the emergency user at any time - it is no need to do it right before initial configuration of RCCMD.

You may skip this part in case of not using an emergency user or if you wish to configure it later.

It happens again and again that passwords are lost due to adverse circumstances:

- e.g. no proper documentation about the installed systems,
- systems and passwords have been forgotten
- systems are inherited from other companies

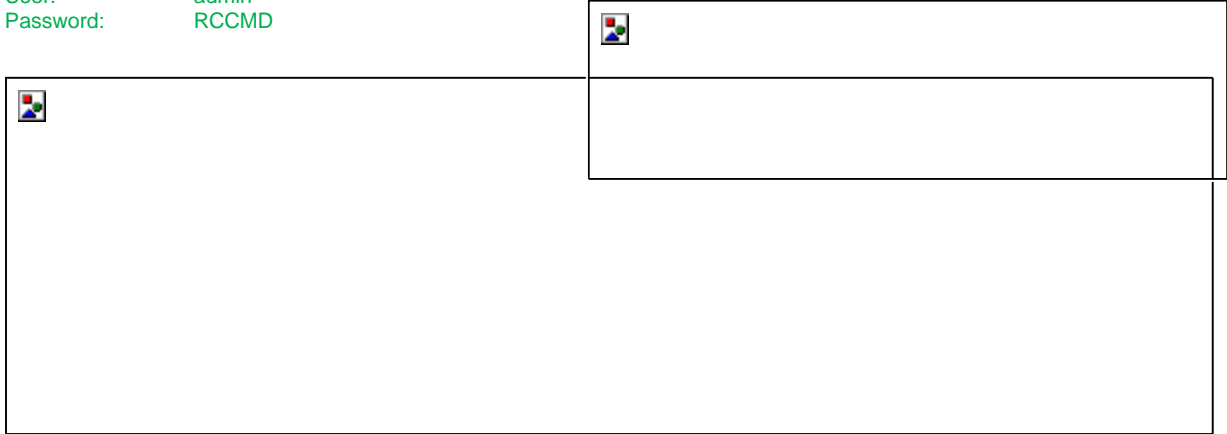
For safety reasons, RCCMD has no backdoors installed by default.

If you assign a new password to user admin, ensure it will be documented!

Otherwise you are damned to set up the complete RCCMD appliance again and reassemble all shutdown scripts. To prevent this incident, it is recommended to set up a backup user to ensure resetting passwords.

After installing the appliance, it is possible to access the console with a freeware tool like Putty:

User: admin
Password: RCCMD



Requesting root privileges

Command: sudo su

Note the user "admin" not yet has been granted the necessary rights to set up a corresponding emergency user. This command will enable the superuser for advanced rights

```
admin@rccmdAppliance:~$ sudo su
[sudo] password for admin:
root@rccmdAppliance:/home/admin#
```

Creating user and password

This step requires two commands

Command 1: useradd <Username>

This command will deploy a new user.

Command 2: passwd <Username>

This command sets up a valid password.

Adding to administrative user group

Command: usermod -G sudo -a Emergency

```
admin@rccmdAppliance:~$ sudo su
[sudo] password for admin:
root@rccmdAppliance:/home/admin# useradd Emergency
root@rccmdAppliance:/home/admin# passwd Emergency
Enter new UNIX password:
```

```
root@rccmdAppliance:/home/admin# usermod -G sudo -a Emergency
root@rccmdAppliance:/home/admin#
```

In order for the newly created user to be granted the necessary rights, he must be assigned to the appropriate user group

Logging off

Command: exit

Note: Enter exit twice:

The *first* exit will close up the SuperUser, the *second* exit will quit the connection to RCCMD and close the console.

```
root@rccmdAppliance:/home/admin# exit
exit
admin@rccmdAppliance:~$ exit
```

2b. Performing an emergency password reset

Start the session using the credentials of the emergency user.

Requesting extended system rights

Command: sudo su

```

Welcome to RCCMD-Appliance.
To configure RCCMD point your web browser to: [https://192.168.200.99]!
$ sudo su

We trust you have received the usual lecture from the local System
Administrator. It usually boils down to these three things:

#1) Respect the privacy of others.
#2) Think before you type.
#3) With great power comes great responsibility.

[sudo] password for Emergency:
root@rccmdAppliance:/#

```

The user Emergency has basically no authorization to administer the RCCMD appliance. Since this user is listed in the group of superusers, *sudo su* enables extend the system rights.

Navigating to required directory

Command: cd /usr/rccmd/webconfig/resources

This directory contains the configuration scripts you need to edit the password of the user admin.

```

root@rccmdAppliance:/# cd /usr/rccmd
root@rccmdAppliance:/usr/rccmd# cd webconfig/resources/
root@rccmdAppliance:/usr/rccmd/webconfig/resources#

```

Using a text editor to change passwords

Command: nano realm.properties

nano is a very handy and well laid-out editor for viewing and editing files and scripts within the RCCMD operating system. The file *realm.properties* itself contains the encrypted password for the web interface of RCCMD.

```

#RCCMD realm.properties
# username: password [,rolename ...]
admin: CRYPT:adg.Dq8TXmNZI, admin

```

Following changes have to be made:

<pre> #RCCMD realm.properties # username: password [,rolename ...] #admin: CRYPT:adg.Dq8TXmNZI, admin admin: Notfall, admin </pre>	<p>-> Use # to disable this line</p> <p>-> Add this line</p>
--	--

In this example, the user admin would now be assigned the password *-Notfall!*:

Saving settings.

Command: CTRL X

Save the file and exit the text editor. Be sure to overwrite the original file. Changing file name will not work.

Restarting RCCMD Web Interface

Command: /etc/init.d/rccmdConfig restart

```

root@rccmdAppliance:/usr/rccmd/webconfig/resources# /etc/init.d/rccmdConfig restart
stopping RCCMD-Configurator...
RCCMDConf has been stopped.
Starting RCCMD-Configurator...
RCCMDConf has been started.

```

This command will restart the web interface and set the new password.

Synchronizing passwords

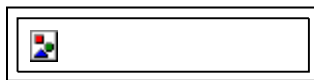
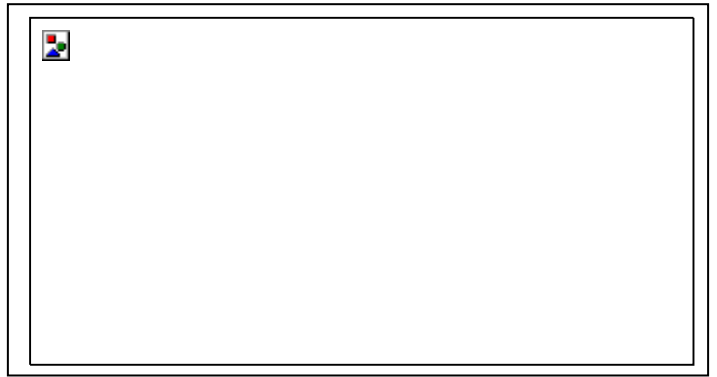
For the moment, the user admin uses two different passwords:

- The old password is valid inside the console of the RCCMD Appliance
- The new password is valid for the web interface of RCCMD

Furthermore, your password changes are not encrypted.

To synchronize and encrypt the credentials for user admin, open a web browser and enter the IP address of you RCCMD installation. After Login, navigate to User Settings and change password.

Press *Save changes* to synchronize and encrypt the password.



Copyright and licenses

The copyright authorization from Generex and other relevant software suppliers must be respected. Generex and their suppliers reserve the rights to the software components. In particular the following are prohibited:

- *copying and distribution,*
- *modifications and derivations,*
- *decompilation, reverse engineering,*

Components which fall under GNU General Public License and further Open Source licenses are integrated into the software. An overview of the integrated Open Source components and a copy of the current license can be obtained at www.generex.de/legal/sla.

Generex will provide the source code for all components of software licensed under the GNU General Public License and comparable Open Source licenses.

For source code requests, please email info@generex.de

FAQ**CS141 FAQ-Frequently asked questions***What does system error 500 / 503 mean?*

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

What does error 422 mean?

This error occurs when trying to adjust the configuration of certain values while using older firmware versions. Updating to the current firmware version shall fix it.

Was bedeutet Fehler 400 / 420/ 522?

This issue can occur if the firmware has been updated but the browser uses data cached from previous versions. Clearing browser cache should fix it. In rare cases the CS141 needs a cold reboot. Please note, a cold reboot of the CS141 will not affect the UPS.

Der USV status shows „Paused“.

When CS141 accesses the Alert History of the UPS, the normal connection must be temporarily stopped. By switching to another page inside CS141 menu and pressing F5 to restore the display status (if not done automatically) this should be fixed.

What does issue -1 mean?

This error occurs if no connection to CS141 is currently possible (CS141 reboots, network lost, etc.), but the user tries to access configuration screen. In this case the browser uses cached data to show the screen without the possibility to enter values. In case of a reboot just give the CS141 a little bit more time.

A little bit awkward, but I forgot my password...

This happens to everyone now and then. Take a look at the "Rescue system" chapter - this might help you. If not, contact support@generex.de and we want to find a way to help you.

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

Because the tooltips are related to the http service. Changing some values need to redirect the user after restarting the build-in http service.

The CON_R_AUX does not establish a connection!

This device is not supported by the CS141. You need to use the CON_R_AUX4.

I have entries in the log file called "UPSMAN started"

This entry is generated whenever there was a change in the event configuration: Because the changes are applied immediately, the "UPSMAN service" must be restarted - this will be protocolled.

When accessing the Alert History, I only get an error!

Maybe this function is not supported by the selected UPS. The fact the CS141 supports your UPS does not mean, your UPS supports all function available at the CS141 for this UPS. This is a little bit complicated to explain: sometimes the UPS should support a command, but ignores it consequently.

I get the error "Backend busy" when I try to log in!

Please wait a moment and try again with another browser. If the problem persists after 5 minutes, use the / reboot function. Refer the chapter If nothing works ...

Does the CS141 supports SNMP v1 queries?

Maybe ... yes or no ...

The CS141 has never or will officially support SNMP queries v1.0. On the other hand it does not mean that it can not if you wish to do that. The only issue that might prevent you using the CS141 the way you want: Due to the fact this is officially not supported, there will be no official bug fix if you have problems. Inofficially maybe our developers can do something if they know somethings not working as it should ...

I have questions that are not explained in the manual.

We always strive to improve our documentation. If you have something that is not or insufficiently explained, please send us a short message to support@generex.de - We are happy to help you as fast as possible.

Q: Why the GX_R_AUX need to be in it's own strain:

In principle, you can put the GX_R_AUX directly into a BACS bus, it would work too. However, in larger installations with many BACS modules in one string, this could be a problem:

Each BACS module has a galvanic isolation between the control and the communication module. The communication module is supplied with the necessary operating voltage by the BACS bus. However, the GX_R_AUX requires more power than the BACS modules, which could cause communication problems inside the complete string. The limit of installed modules before this occurs is fluent and depends heavily on where insed the string you placed the GX_R_AUX during installation. Therefore, this type of installation is only conditionally recommendable.

Q I habe 34 BACS modules and unfortunately 38 batteries... Can I just set up 34 batteries?

Well... in the end, yes, BACS will monitor and equalyize 34 batteries. The last 4 batteries will be just loaded. But this is not recommendable. It will lead into problems with the 4 batteries left:

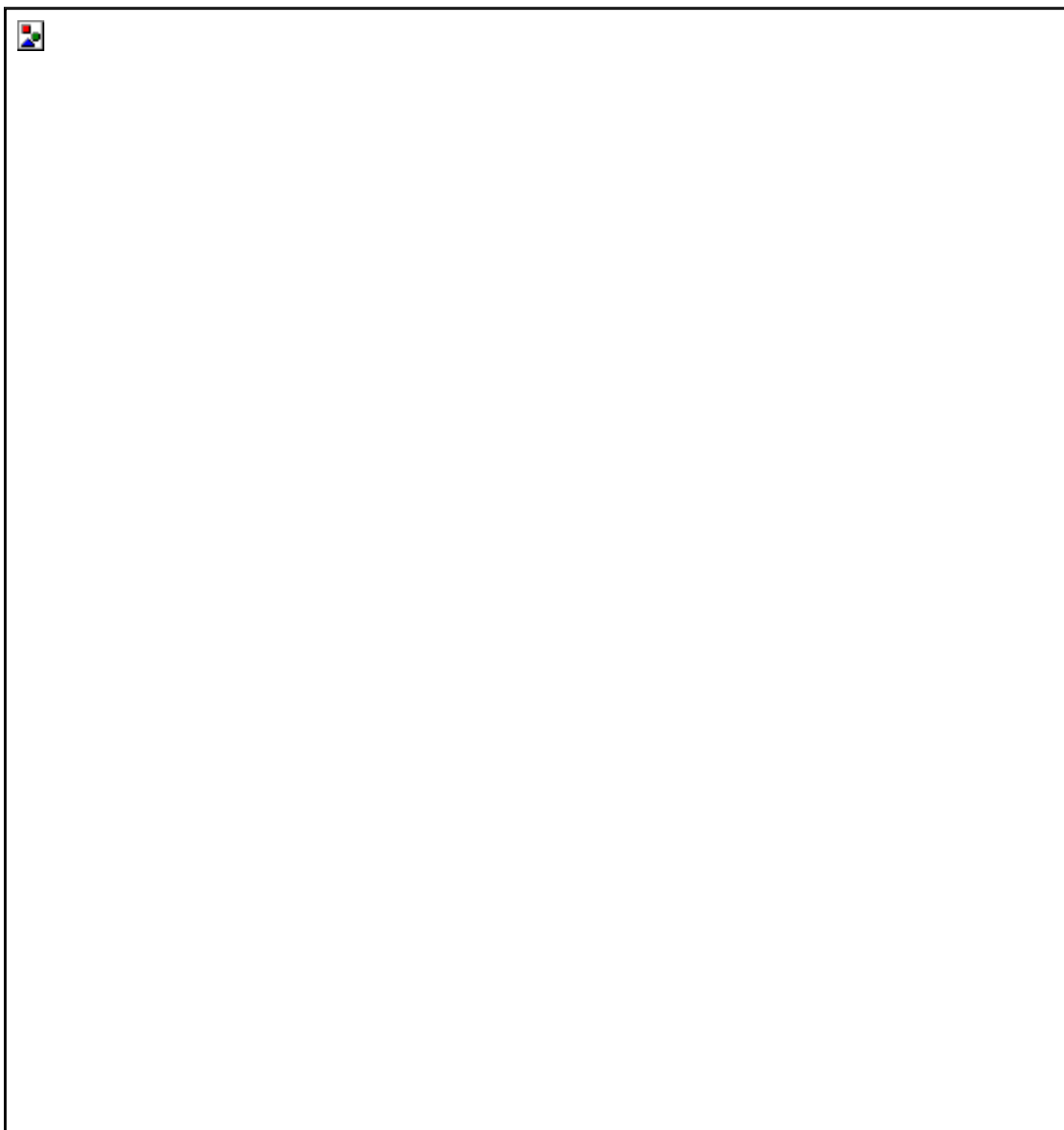
- No monitoring
- No battery management

The problem is normally not that you can add 4 modules later, the problem is, if BACS is running and working, you may forget to add the last 4 batteries.

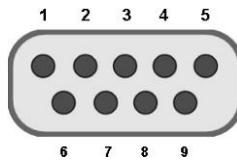
Appendix:

Hardware Layout CS141

1. Slide-Switch for network configuration
2. Network Interface
3. COM2 MINIDIN Connector for RS232
4. COM2 Phoenix Connector for RS485
5. Green and Red Status LED
6. AUX Interface
7. PoE Header
8. Debug Adapter
9. Rescue Jumper: Open = Normal Boot, Close = Rescue Boot
10. NAND Flash
11. CPU
12. RAM
13. USB Interface
14. COM1
15. Slot Interface
16. Power Supply
17. DIP Switch
18. Fuse



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	

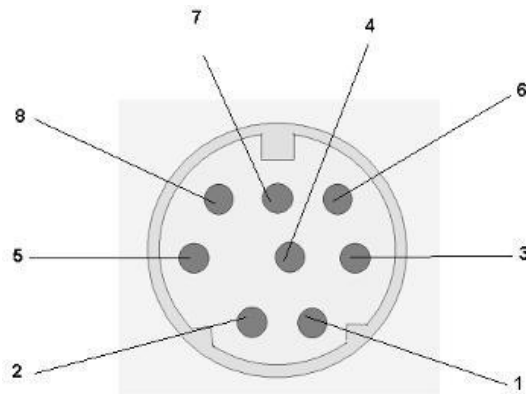


Slot version: Circuit board connection

Pin	Signal name	Level	Function
1	GND		Power Ground
2	8 – 34V DC		Power Input
3	COM1 TXD	V24	COM1 Transmit Data
4	COM1 RXD	V24	COM1 Receive Data
5	SW_GPIO_1 1) 2)	3,3V TTL	CS141DMINI: Functionality of DIP-Switch 1
6	SW_GPIO_2 1) 2)	3,3V TTL	CS141DMINI: Functionality of DIP-Switch 2
7	POW# Input 1)	3,3V TTL	Enable power supply (active low)
8	Bridged with Pin 10		
9	GND		Signal Ground
10	Bridged with Pin 8		
11	COM1 DTR 1)	V24	COM1 Data Transmit Ready
12	COM1 RI 1)	V24	COM1 Ring Indicator
13	COM3 RXD 1) 2)	5V TTL	COM3 Receive Data
14	COM3 TXD 1) 2)	5V TTL	COM3 Transmit Data
15	COM2 TXD 1) 2)	3,3V TTL	COM2 Transmit Data
16	COM2 RXD 1) 2)	3,3V TTL	COM2 Receive Data
17-26	-		n.c.

1) Connectable with solder bridge (MINI: resistor bridge)

2) Input with Pull-Up

Pin COM2 Mini-DIN 8 pol

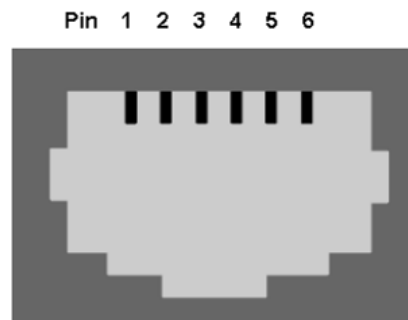
Mini DIN 8 socket RS-232:

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

RS-485 (optional):

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

AUX-Port (Hardware Revision 1.1 = from Serial numbers 0121-1203, 0122-00198, 0123-00564 onwards) RJ11 6-pol



Pin1: -> +3,3V
 Pin2: ->
 Pin3: ->
 Pin4: -> RxD (COM3 Input)
 Pin5: -> TxD (COM3 Output)
 Pin6: -> GND

Modbus addresses

OEM MODBUS Defaultadress (for all products/OEMS, not specified further down in this modbus manual)

Address	Type	Function	Name	Description	Length
97	U	3 / 4	OUTPUT_VOLT0	Output Voltage Phase 1 in V	1
98	U	3 / 4	OUTPUT_VOLT1	Output Voltage Phase 2 in V	1
99	U	3 / 4	OUTPUT_VOLT2	Output Voltage Phase 3 in V	1
100	U	3 / 4	OUTPOWER0	Outpower Phase 1 %	1
101	U	3 / 4	OUTPOWER1	Outpower Phase 2 %	1
102	U	3 / 4	OUTPOWER2	Outpower Phase 3 %	1
103	U	3 / 4	BATTCAP	Battery Capacity %	1
104	S	3 / 4	INVOLT0	Input Voltage Phase 1 V	1
105	S	3 / 4	INVOLT1	Input Voltage Phase 2 V	1
106	S	3 / 4	INVOLT2	Input Voltage Phase 3 V	1
107	S	3 / 4	TEMPDEG	Temperature C°	1
108	S	3 / 4	AUTONOMTIME	Autonomy Time minutes	1
109	U	3 / 4	STATUS (e. g. UPS normal = -4h, Powerfail = -12h, Battery test running = -68h, Bypass = -5h)	UPS Status (ASCII HEX) Please note UPSMAN status bytes table below	1
110	S	3 / 4	BATTVOLT	Battery Voltage V	1
111	U	3 / 4	INFREQ0	Input Frequency Hz Phase 1	1
112	U	3 / 4	INFREQ1	Input Frequency Hz Phase 2	1
113	U	3 / 4	INFREQ2	Input Frequency Hz Phase 3	1
114	U	3 / 4	CNT_PF	Powerfail Counter	1
115	U	3 / 4	Alarm Battery Bad	1 = active; 0 = not active	1
116	U	3 / 4	Alarm: On Battery	1 = active; 0 = not active	1
117	U	3 / 4	Alarm: Battery Low	1 = active; 0 = not active	1
118	U	3 / 4	Alarm: Battery Depleted	1 = active; 0 = not active	1
119	U	3 / 4	Alarm: Over temperature	1 = active; 0 = not active	1
120	U	3 / 4	Alarm: Input Bad	1 = active; 0 = not active	1
121	U	3 / 4	Alarm: Output Bad	1 = active; 0 = not active	1
122	U	3 / 4	Alarm: Output Overload	1 = active; 0 = not active	1
123	U	3 / 4	Alarm: On Bypass	1 = active; 0 = not active	1
124	U	3 / 4	Alarm: Bypass Bad	1 = active; 0 = not active	1
125	U	3 / 4	Alarm: Output Off as requested.	1 = active; 0 = not active	1
126	U	3 / 4	Alarm: UPS Off as requested.	1 = active; 0 = not active	1
127	U	3 / 4	Alarm: Charger Failed	1 = active; 0 = not active	1

128	U	3 / 4	Alarm: UPS Output Off	1 = active; 0 = not active	1
129	U	3 / 4	Alarm: UPS System Off	1 = active; 0 = not active	1
130	U	3 / 4	Alarm: Fan Failure	1 = active; 0 = not active	1
131	U	3 / 4	Alarm: fuse failure	1 = active; 0 = not active	1
132	U	3 / 4	Alarm: general fault	1 = active; 0 = not active	1
133	U	3 / 4	Alarm: diagnose test failed	1 = active; 0 = not active	1
134	U	3 / 4	Alarm: communication lost	1 = active; 0 = not active	1
135	U	3 / 4	Alarm: awaiting power	1 = active; 0 = not active	1
136	U	3 / 4	Alarm: shutdown pending	1 = active; 0 = not active	1
137	U	3 / 4	Alarm: shutdown imminent	1 = active; 0 = not active	1
138	U	3 / 4	Alarm: test in progress	1 = active; 0 = not active	1
139	U	3 / 4	AUX Port 1	1 = active (high), 0 = not active (low)	1
140	U	3 / 4	AUX Port 2	1 = active (high), 0 = not active (low)	1
141	U	3 / 4	AUX Port 3	1 = active (high), 0 = not active (low)	1
142	U	3 / 4	AUX Port 4	1 = active (high), 0 = not active (low)	1
143	U	3 / 4	Sensormanager/SMTCOM sensor 1	Analog value	1
144	U	3 / 4	Sensormanager/SMTHCOM sensor 2	Analog value	1
145	U	3 / 4	Sensormanager sensor 3	Analog value	1
146	U	3 / 4	Sensormanager sensor 4	Analog value	1
147	U	3 / 4	Sensormanager sensor 5	Analog value	1
148	U	3 / 4	Sensormanager sensor 6	Analog value	1
149	U	3 / 4	Sensormanager sensor 7	Analog value	1
150	U	3 / 4	Sensormanager sensor 8	Analog value	1

Section OEM: ABB/NEWAVE UPS Type Concept Power

Address	Type	Function	Name	Description	Length
100	U	3 / 4	OUTPOWER0	Outpower Phase 1 %	1
101	U	3 / 4	OUTPOWER1	Outpower Phase 2 %	1
102	U	3 / 4	OUTPOWER2	Outpower Phase 3 %	1
103	U	3 / 4	BATTCAP	Battery Capacity %	1
104	S	3 / 4	INVOLT0	Input Voltage Phase 1 V	1
105	S	3 / 4	INVOLT1	Input Voltage Phase 2 V	1
106	S	3 / 4	INVOLT2	Input Voltage Phase 3 V	1
107	S	3 / 4	TEMPDEG	Temperature C°	1
108	S	3 / 4	AUTONOMTIME	Autonomy Time minutes	1
109	U	3 / 4	STATUS (e. g. UPS normal = -4 , Powerfail = -12 , Battery test running = -68 , Bypass = -5)	UPS Status (ASCII HEX) Please note UPSMAN status bytes table below	1
110	S	3 / 4	BATTVOLT	Battery Voltage V	1
111	U	3 / 4	INFREQ0	Input Frequency Hz Phase 1	1
112	U	3 / 4	INFREQ1	Input Frequency Hz Phase 2	1
113	U	3 / 4	INFREQ2	Input Frequency Hz Phase 3	1
114	U	3 / 4	CNT_PF	Powerfail Counter	1
115	U	3 / 4	Alarm Battery Bad	1 = active; 0 = not active	1
116	U	3 / 4	Alarm: On Battery	1 = active; 0 = not active	1
117	U	3 / 4	Alarm: Battery Low	1 = active; 0 = not active	1
118	U	3 / 4	Alarm: Battery Depleted	1 = active; 0 = not active	1
119	U	3 / 4	Alarm: Over temperature	1 = active; 0 = not active	1
120	U	3 / 4	Alarm: Input Bad	1 = active; 0 = not active	1
121	U	3 / 4	Alarm: Output Bad	1 = active; 0 = not active	1
122	U	3 / 4	Alarm: Output Overload	1 = active; 0 = not active	1
123	U	3 / 4	Alarm: On Bypass	1 = active; 0 = not active	1
124	U	3 / 4	Alarm: Bypass Bad	1 = active; 0 = not active	1
125	U	3 / 4	Alarm: Output Off as requested.	1 = active; 0 = not active	1
126	U	3 / 4	Alarm: UPS Off as requested.	1 = active; 0 = not active	1
127	U	3 / 4	Alarm: Charger Failed	1 = active; 0 = not active	1
128	U	3 / 4	Alarm: UPS Output Off	1 = active; 0 = not active	1
129	U	3 / 4	Alarm: UPS System Off	1 = active; 0 = not active	1
130	U	3 / 4	Alarm: Fan Failure	1 = active; 0 = not active	1
131	U	3 / 4	Alarm: fuse failure	1 = active; 0 = not active	1
132	U	3 / 4	Alarm: general fault	1 = active; 0 = not active	1

Address	Type	Function	Name	Description	Length
133	U	3 / 4	Alarm: diagnose test failed	1 = active; 0 = not active	1
134	U	3 / 4	Alarm: communication lost	1 = active; 0 = not active	1
135	U	3 / 4	Alarm: awaiting power	1 = active; 0 = not active	1
136	U	3 / 4	Alarm: shutdown pending	1 = active; 0 = not active	1
137	U	3 / 4	Alarm: shutdown imminent	1 = active; 0 = not active	1
138	U	3 / 4	Alarm: test in progress	1 = active; 0 = not active	1
139	U	3 / 4	Manual Bypass Switch Closed	0 = open 1 = closed	1
140	U	3 / 4	OUTPUT_VOLT0	Outputvoltage Phase 1	1
141	U	3 / 4	OUTPUT_VOLT1	Outputvoltage Phase 2	1
142	U	3 / 4	OUTPUT_VOLT2	Outputvoltage Phase 3	1
143	U	3 / 4	OutputCurrent Phase A * 10	Output Current Phase 1 in Ampere devided by 10	1
144	U	3 / 4	OutputCurrent Phase B * 10	Output Current Phase 1 in Ampere devided by 10	1
145	U	3 / 4	OutputCurrent Phase C * 10	Output Current Phase 1 in Ampere devided by10	1
146	U	3 / 4	xid3017 Bits 0-15	Statusbit, for details please contact NEWAVE	1
147	U	3 / 4	xid3017 Bits 16-31	Statusbit, for details please contact ABB/NEWAVE	1
148	U	3 / 4	xid645 Bits 0-15	Alarmbit, for details please contact ABB/NEWAVE	1
149	U	3 / 4	xid645 Bits 16-31	Alarmbit, for details please contact ABB/NEWAVE	1
150	U	3 / 4	xid645 Bits 32-47	Alarmbit, for details please contact ABB/NEWAVE	1
151	U	3 / 4	xid645 Bits 48-63	Alarmbit, for details please contact ABB/NEWAVE	1
152	U	3 / 4	Sensormanager/SMTCOM sensor 1	Analog value	1
153	U	3 / 4	Sensormanager/SMTHCOM sensor 2	Analog value	1
154	U	3 / 4	Sensormanager sensor 3	Analog value	1
155	U	3 / 4	Sensormanager sensor 4	Analog value	1
156	U	3 / 4	Sensormanager sensor 5	Analog value	1
157	U	3 / 4	Sensormanager sensor 6	Analog value	1
158	U	3 / 4	Sensormanager sensor 7	Analog value	1
159	U	3 / 4	Sensormanager sensor 8	Analog value	1
160	U	3 / 4	TrueOutputPower Phase A in KW	True Output Power Current Phase 1 in Kilowatt	1
161	U	3 / 4	TrueOutputPower Phase A in KW	True Output Power Current Phase 1 in Kilowatt	1
162	U	3 / 4	TrueOutputPower Phase A in KW	True Output Power Current Phase 1 in	1

Address	Type	Function	Name	Description	Length
Kilowatt					
163	U	3 / 4	AUX Port 1	1 = active (high), 0 = not active (low)	1
164	U	3 / 4	AUX Port 2	1 = active (high), 0 = not active (low)	1
165	U	3 / 4	AUX Port 3	1 = active (high), 0 = not active (low)	1
166	U	3 / 4	AUX Port 4	1 = active (high), 0 = not active (low)	1
167	U	3 / 4	BATTERYCURRENT	Battery Current in Ampere	1
168	U	3 / 4	OUTFREQ0	Output Frequency Phase 1 in Hz	1
169	U	3 / 4	UPSIDMASK&0xFFFF	for details please contact NEWAVE	1
170	U	3 / 4	(UPSIDMASK&0xFFFF0000)>>16	for details please contact NEWAVE	1
171	U	3 / 4	AUXINPFREQ0	Auxiliary Input Frequency Phase 1	1
172	U	3 / 4	AUXINPFREQ1	Auxiliary Input Frequency Phase 2	1
173	U	3 / 4	AUXINPFREQ2	Auxiliary Input Frequency Phase 3	1
174	U	3 / 4	AUXINPVOLT0	Auxiliary Input Voltage Phase 1	1
175	U	3 / 4	AUXINPVOLT1	Auxiliary Input Voltage Phase 2	1
176	U	3 / 4	AUXINPVOLT2	Auxiliary Input Voltage Phase 3	1
177	U	3 / 4	BP_FREQ0	Bypass Frequency	1
178	U	3 / 4	BP_VOLT0	Bypass Voltage Phase 1	1
179	U	3 / 4	BP_VOLT1	Bypass Voltage Phase 1	1
180	U	3 / 4	BP_VOLT2	Bypass Voltage Phase 3	1
181	U	3 / 4	(RAWSTATEB&0x8)!=0x8	Statusbit, for details please contact ABB/NEWAVE	1

Section OEM: MASTERGUARD

Address	Type	Function	Name	Description	Length
97	U	3 / 4	OUTPUT_VOLT0	Output Voltage Phase 1 in V	1
98	U	3 / 4	OUTPUT_VOLT1	Output Voltage Phase 2 in V	1
99	U	3 / 4	OUTPUT_VOLT2	Output Voltage Phase 3 in V	1
100	U	3 / 4	OUTPOWER0	Outpower Phase 1 %	1
101	U	3 / 4	OUTPOWER1	Outpower Phase 2 %	1
102	U	3 / 4	OUTPOWER2	Outpower Phase 3 %	1
103	U	3 / 4	BATTCAP	Battery Capacity %	1
104	S	3 / 4	INVOLT0	Input Voltage Phase 1 V	1
105	S	3 / 4	INVOLT1	Input Voltage Phase 2 V	1
106	S	3 / 4	INVOLT2	Input Voltage Phase 3 V	1
107	S	3 / 4	TEMPDEG	Temperature C°	1
108	S	3 / 4	AUTONOMTIME	Autonomy Time minutes	1

109	U	3 / 4	STATUS (e. g. UPS normal = -4 , Powerfail = -12 , Battery test running = -68 , Bypass = -5)	UPS Status (ASCII HEX) Please note UPSMAN status bytes table below	1
110	S	3 / 4	BATTVOLT	Battery Voltage V	1
111	U	3 / 4	INFREQ0	Input Frequency Hz Phase 1	1
112	U	3 / 4	INFREQ1	Input Frequency Hz Phase 2	1
113	U	3 / 4	INFREQ2	Input Frequency Hz Phase 3	1
114	U	3 / 4	CNT_PF	Powerfail Counter	1
115	U	3 / 4	Alarm Battery Bad	1 = active; 0 = not active	1
116	U	3 / 4	Alarm: On Battery	1 = active; 0 = not active	1
117	U	3 / 4	Alarm: Battery Low	1 = active; 0 = not active	1
118	U	3 / 4	Alarm: Battery Depleted	1 = active; 0 = not active	1
119	U	3 / 4	Alarm: Over temperature	1 = active; 0 = not active	1
120	U	3 / 4	Alarm: Input Bad	1 = active; 0 = not active	1
121	U	3 / 4	Alarm: Output Bad	1 = active; 0 = not active	1
122	U	3 / 4	Alarm: Output Overload	1 = active; 0 = not active	1
123	U	3 / 4	Alarm: On Bypass	1 = active; 0 = not active	1
124	U	3 / 4	Alarm: Bypass Bad	1 = active; 0 = not active	1
125	U	3 / 4	Alarm: Output Off as requested.	1 = active; 0 = not active	1
126	U	3 / 4	Alarm: UPS Off as requested.	1 = active; 0 = not active	1
127	U	3 / 4	Alarm: Charger Failed	1 = active; 0 = not active	1
128	U	3 / 4	Alarm: UPS Output Off	1 = active; 0 = not active	1
129	U	3 / 4	Alarm: UPS System Off	1 = active; 0 = not active	1
130	U	3 / 4	Alarm: Fan Failure	1 = active; 0 = not active	1
131	U	3 / 4	Alarm: fuse failure	1 = active; 0 = not active	1
132	U	3 / 4	Alarm: general fault	1 = active; 0 = not active	1
133	U	3 / 4	Alarm: diagnose test failed	1 = active; 0 = not active	1
134	U	3 / 4	Alarm: communication lost	1 = active; 0 = not active	1
135	U	3 / 4	Alarm: awaiting power	1 = active; 0 = not active	1
136	U	3 / 4	Alarm: shutdown pending	1 = active; 0 = not active	1
137	U	3 / 4	Alarm: shutdown imminent	1 = active; 0 = not active	1
138	U	3 / 4	Alarm: test in progress	1 = active; 0 = not active	1
139	U	3 / 4	PXWARN		2
141	U	3 / 4	FAULT CODE 1		1
142	U	3 / 4	FAULT CODE 2		1
143	U	3 / 4	FAULT CODE 3		1
144	U	3 / 4	FAULT CODE 4		1
145	U	3 / 4	BADBATTBLOCK 1		1

146	U	3 / 4	BADBATTBLOCK 1	1
147	U	3 / 4	BADBATTBLOCK 1	1
148	U	3 / 4	BADBATTBLOCK 1	1
149	U	3 / 4	BADBATTBLOCK 1	1
150	U	3 / 4	BADBATTBLOCK 1	1

Section OEM: RITTAL PMC Extension

Address	Type	Function	Name	Description	Length
Digital Input Status(DI)					
0	bit	2	Bypass working	Status 0: Normal, Status 1: Alert	1
1	bit	2	Bypass Interruption	Status 0: Normal, Status 1: Alert	1
2	bit	2	Rectifier Failure	Status 0: Normal, Status 1: Alert	1
3	bit	2	Inverter Failure	Status 0: Normal, Status 1: Alert	1
4	bit	2	Over Temperature	Status 0: Normal, Status 1: Alert	1
5	bit	2	Over Load	Status 0: Normal, Status 1: Alert	1
6	bit	2	0	Status 0: Normal, Status 1: Alert	1
7	bit	2	Battery Voltage too Low	Status 0: Normal, Status 1: Alert	1
8	bit	2	Fuse broken	Status 0: Normal, Status 1: Alert	1
9	bit	2	Battery discharging	Status 0: Normal, Status 1: Alert	1
10	bit	2	0	Status 0: Floating charge, Status 1: Instant charging	1
11~30	bit	2	For future expansion		1
After 31	bit	2	Venders own definition		1
Analog Measurement point (AI)					
00	word	4	U in R phase input voltage	0.1 Volt	
01	word	4	U in S phase input voltage	0.1 Volt	
02	word	4	U in T phase input voltage	0.1 Volt	
03	word	4	I in R phase input current	0.1A	
04	word	4	I in S phase input current	0.1A	
05	word	4	I in T phase input current	0.1A	
06	word	4	F input frequency	0.1Hz	
07	word	4	U out R phase output voltage	0.1 Volt	
08	word	4	U out S phase output voltage	0.1 Volt	
09	word	4	U out T phase output voltage	0.1 Volt	
10	word	4	I out R phase output current	0.1A	
11	word	4	I out S phase output current	0.1A	
12	word	4	I out T phase output current	0.1A	
13	word	4	P out output power	0.1kVA	

14	word	4	P out output power	0.1kW
15	word	4	PF output power factor	0.01Cos
16	word	4	U Bypass, R phase voltage	0.1 Volt
17	word	4	U Bypass, S phase voltage	0.1 Volt
18	word	4	U Bypass, T phase voltage	0.1 Volt
19	word	4	F out output frequency	0.1Hz
20	word	4	U Bat battery voltage	0.1 Volt
21	word	4	I charch Bat battery charging/discharging	0.1A
22	word	4	Temp 1 battery temperature	0.1degC
23	word	4	Temp 2 battery temperature	0.1degC
24	word	4	Temp 3 battery temperature	0.1degC
25	word	4	Temp 4 battery temperature	0.1degC
26	word	4	Temp 5 UPS shelf temperature	0.1degC
Digital output (DO) (Function 1 to read data; 5 to control the function)				
0	bit	1 / 5	UPS Turn On	
1	bit	1 / 5	UPS Shut down	
2	bit	1 / 5	Alarm Reset	
3	bit	1 / 5	Battery Instant Charging	
4	bit	1 / 5	Battery Floating Charging	
5~10	bit		For future expansion	
After			Vender self-definition	

Address	Type	Function	Name	Description	Length
100	U	3 / 4	OUTPOWER0	True Output Power Current Phase 1 in Kilowatt	1
101	U	3 / 4	OUTPOWER1	True Output Power Current Phase 2 in Kilowatt	1
102	U	3 / 4	OUTPOWER2	True Output Power Current Phase 3 in Kilowatt	1
103	U	3 / 4	BATTCAP	Battery Capacity in %	1
104	U	3 / 4	INVOLT0	Input Voltage Phase 1	1
105	U	3 / 4	INVOLT1	Input Voltage Phase 2	1
106	U	3 / 4	INVOLT2	Input Voltage Phase 3	1
107	U	3 / 4	TEMPDEG	Temperature in Degree C°	1
108	U	3 / 4	AUTONOMTIME	Autonomy Time in Minutes	1
109	U	3 / 4	STATUS	UPS Status (ASCII HEX)	1
Please note UPSMAN status bytes table					

Address	Type	Function	Name	Description	Length
below					
110	U	3 / 4	BATTVOLT	Battery Voltage	1
111	U	3 / 4	INFREQ0	Input Frequency Phase 1 in Hz	1
112	U	3 / 4	INFREQ1	Input Frequency Phase 2 in Hz	1
113	U	3 / 4	INFREQ2	Input Frequency Phase 3 in Hz	1
114	U	3 / 4	CNT_PF	Powerfail Counter	1
115	U	3 / 4	SNMP Alarm	Alarmbit, for details please contact NEWAVE	1
116	U	3 / 4	SNMP Alarm	Alarmbit, for details please contact NEWAVE	1
117	U	3 / 4	SNMP Alarm	Alarmbit, for details please contact NEWAVE	1
118	U	3 / 4	SNMP Alarm	Alarmbit, for details please contact NEWAVE	1
119	U	3 / 4	SNMP Alarm	Alarmbit, for details please contact NEWAVE	1
120	U	3 / 4	SNMP Alarm	Alarmbit, for details please contact NEWAVE	1
121	U	3 / 4	SNMP Alarm	Alarmbit, for details please contact NEWAVE	1
122	U	3 / 4	SNMP Alarm	Alarmbit, for details please contact NEWAVE	1
123	U	3 / 4	SNMP Alarm	Alarmbit, for details please contact NEWAVE	1
124	U	3 / 4	SNMP Alarm	Alarmbit, for details please contact NEWAVE	1
125	U	3 / 4	SNMP Alarm	Alarmbit, for details please contact NEWAVE	1
126	U	3 / 4	SNMP Alarm	Alarmbit, for details please contact NEWAVE	1
127	U	3 / 4	SNMP Alarm	Alarmbit, for details please contact NEWAVE	1
128	U	3 / 4	SNMP Alarm	Alarmbit, for details please contact NEWAVE	1
129	U	3 / 4	SNMP Alarm	Alarmbit, for details please contact NEWAVE	1
130	U	3 / 4	SNMP Alarm	Alarmbit, for details please contact NEWAVE	1
131	U	3 / 4	SNMP Alarm	Alarmbit, for details please contact NEWAVE	1
132	U	3 / 4	SNMP Alarm	Alarmbit, for details please contact NEWAVE	1
133	U	3 / 4	SNMP Alarm	Alarmbit, for details please contact NEWAVE	1
134	U	3 / 4	SNMP Alarm	Alarmbit, for details please contact NEWAVE	1
135	U	3 / 4	SNMP Alarm	Alarmbit, for details please contact NEWAVE	1
136	U	3 / 4	SNMP Alarm	Alarmbit, for details please contact NEWAVE	1
137	U	3 / 4	SNMP Alarm	Alarmbit, for details please contact NEWAVE	1
138	U	3 / 4	SNMP Alarm	Alarmbit, for details please contact NEWAVE	1
139	U	3 / 4	Status Bit	Statusbit, for details please contact NEWAVE	1
140	U	3 / 4	OUTPUT_VOLT0	Output Voltage Phase 1	1
141	U	3 / 4	OUTPUT_VOLT1	Output Voltage Phase 2	1
142	U	3 / 4	OUTPUT_VOLT2	Output Voltage Phase 3	1
143	U	3 / 4	OUTPUT_CURR0	Output Current Phase 1 in KW	1
144	U	3 / 4	OUTPUT_CURR1	Output Current Phase 2 in KW	1
145	U	3 / 4	OUTPUT_CURR2	Output Current Phase 3 in KW	1

Address	Type	Function	Name	Description	Length
146	U	3 / 4	Status Bit	Statusbit, for details please contact NEWAVE	1
147	U	3 / 4	Status Bit	Statusbit, for details please contact NEWAVE	1
148	U	3 / 4	Status Bit	Statusbit, for details please contact NEWAVE	1
149	U	3 / 4	Status Bit	Statusbit, for details please contact NEWAVE	1
150	U	3 / 4	Status Bit	Statusbit, for details please contact NEWAVE	1
151	U	3 / 4	Status Bit	Statusbit, for details please contact NEWAVE	1
152	U	3 / 4	TEMP1	SensorManager/SM_T_H_COM Analog Value	1
153	U	3 / 4	TEMP2	SensorManager/SM_T_H_COM Analog Value	1
154	U	3 / 4	TEMP3	SensorManager Analog Value	1
155	U	3 / 4	TEMP4	SensorManager Analog Value	1
156	U	3 / 4	TEMP5	SensorManager Analog Value	1
157	U	3 / 4	TEMP6	SensorManager Analog Value	1
158	U	3 / 4	TEMP7	SensorManager Analog Value	1
159	U	3 / 4	TEMP8	SensorManager Analog Value	1
160	U	3 / 4	LOADKVA0	Load Phase 1 in KW	1
161	U	3 / 4	LOADKVA1	Load Phase 2 in KW	1
162	U	3 / 4	LOADKVA2	Load Phase 3 in KW	1

Section OEM: Netminder for all LT and MD types

Address	Type	Function	Name	Description	Length
100	U	3/4	INVOLT	Input Voltage	1
101	U	3/4	OUTPUTVOLT	Output Voltage	1
102	U	3/4	BATTVOLT	Battery Voltage	1
103	U	3/4	OUTPUTCURR	Output Current	1
104	U	3/4	LOADPERC	Load (%)	1
105	U	3/4	OUTPUTPOW	Output Power in W	1
106	U	3/4	KVA	KVA	1
107	U	3/4	FREQUENCY	Frequency	1
108	U	3/4	CS141UPSSTAT	CS141 UPS Status	1
109	U	3/4	Alarm: Battery Bad	1 = active; 0 = not active	1
110	U	3/4	Alarm: On Battery	1 = active; 0 = not active	1
111	U	3/4	Alarm: Battery Low	1 = active; 0 = not active	1
112	U	3/4	Alarm: Battery Depleted	1 = active; 0 = not active	1
113	U	3/4	Alarm: Overtemperature	1 = active; 0 = not active	1
114	U	3/4	Alarm: Input Bad	1 = active; 0 = not active	1

115	U	3/4	Alarm: Output Bad	1 = active; 0 = not active	1
116	U	3/4	Alarm: Output Overload	1 = active; 0 = not active	1
117	U	3/4	Alarm: On Bypass	1 = active; 0 = not active	1
118	U	3/4	Alarm: Bypass Bad	1 = active; 0 = not active	1
119	U	3/4	Alarm: Ouput Off As Requested	1 = active; 0 = not active	1
120	U	3/4	Alarm: UPS Off As Requested	1 = active; 0 = not active	1
121	U	3/4	Alarm: Charger Failed	1 = active; 0 = not active	1
122	U	3/4	Alarm: UPS Output Off	1 = active; 0 = not active	1
123	U	3/4	Alarm: UPS System Off	1 = active; 0 = not active	1
124	U	3/4	Alarm: Fan Failure	1 = active; 0 = not active	1
125	U	3/4	Alarm: Fuse Failure	1 = active; 0 = not active	1
126	U	3/4	Alarm: General Fault	1 = active; 0 = not active	1
127	U	3/4	Alarm: Diagnosis Test Failed	1 = active; 0 = not active	1
128	U	3/4	Alarm: Communication Lost	1 = active; 0 = not active	1
129	U	3/4	Alarm: Awaiting Power	1 = active; 0 = not active	1
130	U	3/4	Alarm: Shutdown Pending	1 = active; 0 = not active	1
131	U	3/4	Alarm: Shutdown Imminent	1 = active; 0 = not active	1
132	U	3/4	Alarm: Test In Progress	1 = active ; 0 = not active	1
133	U	3/4	AUX Port 1	1 = active (high) ; 0 = not active (low)	1
134	U	3/4	AUX Port 2	1 = active (high) ; 0 = not active (low)	1
135	U	3/4	AUX Port 3	1 = active (high) ; 0 = not active (low)	1
136	U	3/4	AUX Port 4	1 = active (high) ; 0 = not active (low)	1
137	U	3/4	SensorManager/SMTH_COM, Sensor 1	Analog Value	1
138	U	3/4	SensorManager/SMTH_COM, Sensor 2	Analog Value	1
139	U	3/4	SensorManager/Sensor 3	Analog Value	1
140	U	3/4	SensorManager/Sensor 4	Analog Value	1
141	U	3/4	SensorManager/Sensor 5	Analog Value	1
142	U	3/4	SensorManager/Sensor 6	Analog Value	1
143	U	3/4	SensorManager/Sensor 7	Analog Value	1
144	U	3/4	SensorManager/Sensor 8	Analog Value	1
145	U	3/4	Result of the last Battery Test	Value 3 = Battery Test passed, Value 4 = Battery Test failed	1

Section OEM: Netminder EON

Address	Type	Function	Name	Description	Length
11	U	3 / 4	Manufacturer	Manufacturer	1

27	U	3 / 4	Version	Version	1
43	U	3 / 4	Identification	Identification	1
75	U	3 / 4	MODEL	UPS Model	1
107	U	3 / 4	AUTONOMTIME	Autonomy time in minutes	1
108	U	3 / 4	BATTCAP	Battery capacity in percent	1
109	U	3 / 4	OUTFREQ0	Output Frequency	1
110	U	3 / 4	OUTPUTVOLT0	Output Voltage Phase 1	1
111	U	3 / 4	OUTPUTVOLT1	Output Voltage Phase 2	1
112	U	3 / 4	OUTPUTVOLT1	Output Voltage Phase 3	1
113	U	3 / 4	OUTPOWER0	Outpower Phase 1 in %	1
114	U	3 / 4	OUTPOWER1	Outpower Phase 2 in %	1
115	U	3 / 4	OUTPOWER2	Outpower Phase 3 in %	1
116	U	3 / 4	OUTPOWER0	Outpower Phase 1 in VA	1
117	U	3 / 4	OUTPOWER1	Outpower Phase 2 in VA	1
118	U	3 / 4	OUTPOWER2	Outpower Phase 3 in VA	1
119	U	3 / 4	INPUTFREQ0	Input Frequency Phase 1 in Hz	1
120	U	3 / 4	INPUTFREQ1	Input Frequency Phase 2 in Hz	1
121	U	3 / 4	INPUTFREQ2	Input Frequency Phase 3 in Hz	1
122	U	3 / 4	INPUTVOLT0	Input Voltage Phase 1 in V	1
123	U	3 / 4	INPUTVOLT1	Input Voltage Phase 2 in V	1
124	U	3 / 4	INPUTVOLT2	Input Voltage Phase 3 in V	1
125	U	3 / 4	INPUTCURR0	Input Current Phase 1 in A	1
126	U	3 / 4	INPUTCURR1	Input Current Phase 2 in A	1
127	U	3 / 4	INPUTCURR2	Input Current Phase 3 in A	1
128	U	3 / 4	INPUTPOW0	Input Power Phase 1 in W	1
129	U	3 / 4	INPUTPOW1	Input Power Phase 2 in W	1
130	U	3 / 4	INPUTPOW1	Input Power Phase 3 in W	1
131	U	3 / 4	BATTVOLT	Battery Voltage in V	1
132	U	3 / 4	BATTTEMPDEG	Battery Temperature in Degree Celsius	1
133	U	3 / 4	BATTSEC	Seconds on Battery	1
134	U	3 / 4	Battery Condition	Battery Condition	1
135	U	3 / 4	Amount of Input Phases	Amount of Input Phases	1
136	U	3 / 4	Amount of Output Phases	Amount of Output Phases	1
137	U	3 / 4	Results of Battery Test	1:Ok, 2: Active, 3: Canceled, 4: Failed, else: not started yet	1
138	U	3 / 4	Powerfail	Powerfail	1
139	U	3 / 4	System Shutdown	System Shutdown	1
140	U	3 / 4	UPSMAN started	UPSMAN started	1

141	U	3 / 4	UPS Connection lost	UPS connection lost	1
142	U	3 / 4	UPS Battery old	UPS Battery old	1
143	U	3 / 4	Load >80%	Load >80%	1
144	U	3 / 4	Load >90%	Load >90%	1
145	U	3 / 4	Overload	Overload	1
146	U	3 / 4	Overtemperature Condition	Overtemperature Condition	1
147	U	3 / 4	Bypass on	Bypass on	1
148	U	3 / 4	Battery low	Battery low	1
149	U	3 / 4	Batteries are weak	Batteries are weak	1
150	U	3 / 4	General Alarm Condition	General Alarm Condition	1
151	U	3 / 4	Input Bad Condition	Input Bad Condition	1
152	U	3 / 4	Output Bad Condition	Output Bad Condition	1
153	U	3 / 4	Bypass Not Available	Bypass Not Available	1
154	U	3 / 4	Low Battery Shutdown	Low Battery Shutdown	1
155	U	3 / 4	System off	System off	1
156	U	3 / 4	System Shutdown	System Shutdown	1
157	U	3 / 4	Charger Failure	Charger Failure	1
158	U	3 / 4	Manual Restart Required	Manual Restart Required	1
159	U	3 / 4	Output Circuit Breaker Open	Output Circuit Breaker Open	1
160	U	3 / 4	Remote Emergency Power off	Remote Emergency Power off	1
161	U	3 / 4	Shutdown imminent	Shutdown imminent	1

Section OEM: Netminder for all other types

Address	Type	Function	Name	Description	Length
100	U	3/4	INVOLT	Input Voltage (I1-n)	1
101	U	3/4	INVOLT	Input Voltage (I2-n)	1
102	U	3/4	INVOLT	Input Voltage (I1-I2)	1
103	U	3/4	OUTPUTVOLT	Output Voltage (I1-n)	1
104	U	3/4	OUTPUTVOLT	Output Voltage (I2-n)	1
105	U	3/4	OUTPUTVOLT	Output Voltage /(I1-I2)	1
106	U	3/4	OUTPUTCURR	Output Current (I1-n)	1
107	U	3/4	OUTPUTCURR	Output Current (I2-n)	1
108	U	3/4	OUTPUTWAT	Output Watts (I1-n)	1
109	U	3/4	OUTPUTWAT	Output Watts (I2-n)	1
110	U	3/4	OUTPUTWAT	Output Watts (I1-I2)	1
111	U	3/4	OUTPUTWATTOT	Output watts (total)	1
112	U	3/4	OUTPUTVA	Output VA (I1-n)	1

113	U	3/4	OUTPUTVA	Output VA (I2-n)	1
114	U	3/4	OUTPUTVA	Output VA (I1-I2)	1
115	U	3/4	OUTPUTVATOT	Output VA (total)	1
116	U	3/4	OUTPUTLOAD	Output Load (I1-n)	1
117	U	3/4	OUTPUTLOAD	Output Load (I2-n)	1
118	U	3/4	OUTPUTFREQ	Output Frequency	1
119	U	3/4	BATTVOLT	Battery Voltage	1
120	U	3/4	PERCBATT	Percentage Battery	1
121	U	3/4	DCCHARGECURR	DC Charging Current	1
122	U	3/4	CS141UPSSTAT	CS141 UPS Status	1
123	U	3/4	Alarm: Battery Bad	1 = active; 0 = not active	1
124	U	3/4	Alarm: On Battery	1 = active; 0 = not active	1
125	U	3/4	Alarm: Battery Low	1 = active; 0 = not active	1
126	U	3/4	Alarm: Battery Depleted	1 = active; 0 = not active	1
127	U	3/4	Alarm: Overtemperature	1 = active; 0 = not active	1
128	U	3/4	Alarm: Input Bad	1 = active; 0 = not active	1
129	U	3/4	Alarm: Output Bad	1 = active; 0 = not active	1
130	U	3/4	Alarm: Output Overload	1 = active; 0 = not active	1
131	U	3/4	Alarm: On Bypass	1 = active; 0 = not active	1
132	U	3/4	Alarm: Bypass Bad	1 = active; 0 = not active	1
133	U	3/4	Alarm: Ouput Off As Requested	1 = active; 0 = not active	1
134	U	3/4	Alarm: UPS Off As Requested	1 = active; 0 = not active	1
135	U	3/4	Alarm: Charger Failed	1 = active; 0 = not active	1
136	U	3/4	Alarm: UPS Output Off	1 = active; 0 = not active	1
137	U	3/4	Alarm: UPS System Off	1 = active; 0 = not active	1
138	U	3/4	Alarm: Fan Failure	1 = active; 0 = not active	1
139	U	3/4	Alarm: Fuse Failure	1 = active; 0 = not active	1
140	U	3/4	Alarm: General Fault	1 = active; 0 = not active	1
141	U	3/4	Alarm: Diagnosis Test Failed	1 = active; 0 = not active	1
142	U	3/4	Alarm: Communication Lost	1 = active; 0 = not active	1
143	U	3/4	Alarm: Awaiting Power	1 = active; 0 = not active	1
144	U	3/4	Alarm: Shutdown Pending	1 = active; 0 = not active	1
145	U	3/4	Alarm: Shutdown Imminent	1 = active; 0 = not active	1
146	U	3/4	Alarm: Test In Progress	1 = active; 0 = not active	1
147	U	3/4	AUX Port 1	1 = active (high) ; 0 = not active (low)	1
148	U	3/4	AUX Port 2	1 = active (high) ; 0 = not active (low)	1
149	U	3/4	AUX Port 3	1 = active (high) ; 0 = not active (low)	1
150	U	3/4	AUX Port 4	1 = active (high) ; 0 = not active (low)	1

151	U	3/4	Sensormngr 1 / SMT_COM,	Analog Value	1
152	U	3/4	Sensormngr 2 /SMTH_COM,	Analog Value	1
153	U	3/4	SensorManager/Sensor 3	Analog Value	1
154	U	3/4	SensorManager/Sensor 4	Analog Value	1
155	U	3/4	SensorManager/Sensor 5	Analog Value	1
156	U	3/4	SensorManager/Sensor 6	Analog Value	1
157	U	3/4	SensorManager/Sensor 7	Analog Value	1
158	U	3/4	SensorManager/Sensor 8	Analog Value	1
159	U	3/4	Result of the last Battery Test	Value 3 = Battery Test passd Value 4 = Battery Test failed	1

Section OEM : AEG Protect 3. M 2.0

Address	Type	Function	Name	Description	Length
100	U	3/4	(SNMPALARMS&0x6102)==0	Normal Operation	1
101	U	3/4	(SNMPALARMS&0x100)>>8	On Bypass	1
102	U	3/4	(SNMPALARMS&0x2)>>1	On Battery	1
103	U	3/4	(SNMPALARMS&0x4000)>>14	UPS System Off	1
104	U	3/4	(SNMPALARMS&0x20000)>>17	General Fault	1
105	U	3/4	(SNMPALARMS&0x80000)>>19	Communication Lost	1
106	U	3/4	(SNMPALARMS&0x20)>>5	Input Bad	1
107	U	3/4	(SNMPALARMS&0x1000)>>12	Charger Failed	1
108	U	3/4	(SNMPALARMS&0x1)	Battery Bad	1
109	U	3/4	(SNMPALARMS&0x40)>>6	Output Bad	1
110	U	3/4	(SNMPALARMS&0x200)>>9	Bypass Bad	1
111	U	3/4	(SNMPALARMS&0x4)>>2	Low Battery	1
				Depleted Battery	
112	U	3/4	(SNMPALARMS&0x8)>>3		1
113	U	3/4	(SNMPALARMS&0x10)>>4	Temperature Bad	1
114	U	3/4	(SNMPALARMS&0x80)>>7	Output Overload	1
115	U	3/4	(SNMPALARMS&0x8000)>>15	Fan Failure	1
116	U	3/4	(SNMPALARMS&0x2000)>>13	UPS Output Off	1
117	U	3/4	AUX1STATE	1 = active (high) ; 0 = not active (low)	1
118	U	3/4	AUX2STATE	1 = active (high) ; 0 = not active (low)	1
119	U	3/4	AUX3STATE	1 = active (high) ; 0 = not active (low)	1
120	U	3/4	AUX4STATE	1 = active (high) ; 0 = not active (low)	1
121	U	3/4	AMBTEMP		1
122	U	3/4	INFREQ0	Input Frequency Hz Phase 1	1
123	U	3/4	INVOLT0	Input Voltage Phase 1 V	1

124	U	3/4	INVOLT1	Input Voltage Phase 2 V	1
125	U	3/4	INVOLT1	Input Voltage Phase 3 V	1
126	U	3/4	INCURR0	Input Current Phase 1 in Ampere	1
127	U	3/4	INCURR1	Input Current Phase 2 in Ampere	1
128	U	3/4	INCURR2	Input Current Phase 3 in Ampere	1
129	U	3/4	EX_BYP_FREQ		1
130	U	3/4	EX_BYP_VOLT0		1
131	U	3/4	EX_BYP_VOLT1		1
132	U	3/4	EX_BYP_VOLT2		1
133	U	3/4	(EX_BATT_VOLTNEG+EX_BATT_VOLTPOS)*10.0		1
134	U	3/4	(EX_BATT_CURRNEG+EX_BATT_CURRPOS)*5.0		1
135	U	3/4	MIN(ftoi(BATTCAP),ftoi(EX_BATT_CAPNEG))		1
136	U	3/4	AUTONOMTIME	Autonomy Time Minutes	1
137	U	3/4	TEMPDEG	Temperature C°	1
138	U	3/4	OUTFREQ0	Output Frequency Hz	1
139	U	3/4	OUTPUT_VOLT0	Output Voltage Phase 1 V	1
140	U	3/4	OUTPUT_VOLT1	Output Voltage Phase 2 V	1
141	U	3/4	OUTPUT_VOLT2	Output Voltage Phase 3 V	1
142	U	3/4	OUTPOWER0	Outpower Phase 1 %	1
143	U	3/4	OUTPOWER1	Outpower Phase 2 %	1
144	U	3/4	OUTPOWER2	Outpower Phase 3 %	1
145	U	3/4	EX_OUT_CURR0		1
146	U	3/4	EX_OUT_CURR1		1
147	U	3/4	EX_OUT_CURR2		1
148	U	3/4	EX_OUT_WATT0		1
149	U	3/4	EX_OUT_WATT1		1
150	U	3/4	EX_OUT_WATT2		1

Section OEM: AEG Protect 3.31, 5.31, 8.31

Address	Type	Function	Name	Description	Length
100	U	3/4	(FKTSTATUS&0x4102)==0	Normal Operation	1
101	U	3/4	SNMPALARMS&0x100)>>8	On Bypass	1
102	U	3/4	(SNMPALARMS&0x2)>>1	On Battery	1
103	U	3/4	(SNMPALARMS&0x4000)>>14	UPS System Off	1
104	U	3/4	CNT_PF	Powerfail Counter	1
105	U	3/4	(SNMPALARMS&0x20000)>>17	General Fault	1
106	U	3/4	(SNMPALARMS&0x80000)>>19	Communication Lost	1
107	U	3/4	(SNMPALARMS&0x20)>>5	Input Bad	1
108	U	3/4	(SNMPALARMS&0x1000)>>12	Charger Failed	1
109	U	3/4	(SNMPALARMS&0x1)	Battery Bad	1
110	U	3/4	(SNMPALARMS&0x40)>>6	Output Bad	1
111	U	3/4	(SNMPALARMS&0x200)>>9	Bypass Bad	1
112	U	3/4	(SNMPALARMS&0x4)>>2	Low Battery	1
113	U	3/4	(SNMPALARMS&0x8)>>3	Depleted Battery	1
114	U	3/4	(SNMPALARMS&0x10)>>4	Temperature Bad	1
115	U	3/4	(SNMPALARMS&0x80)>>7	Output Overload	1
116	U	3/4	(SNMPALARMS&0x8000)>>15	Fan Failure	1
117	U	3/4	(SNMPALARMS&0x2000)>>13	UPS Output Off	1
118	U	3/4	AUX1STATE	State AUX Port 1 1 = active (high) ; 0 = not active (low)	1
119	U	3/4	AUX2STATE	State AUX Port 2 1 = active (high) ; 0 = not active (low)	1
120	U	3/4	AUX3STATE	State AUX Port 3 1 = active (high) ; 0 = not active (low)	1
121	U	3/4	AUX4STATE	State AUX Port 4 1 = active (high) ; 0 = not active (low)	1
122	U	3/4	INFREQ0*10.0	Input Frequency Hz Phase 1	1
123	U	3/4	INVOLT0	Input Voltage Phase 1 V	1
124	U	3/4	INVOLT1	Input Voltage Phase 2 V	1
125	U	3/4	INVOLT2	Input Voltage Phase 3 V	1
126	U	3/4	BP_FREQ0*10.0	Output Frequency [Hz]	1
127	U	3/4	BP_VOLT0	Bypass Voltage Phase 1 [V]	1
128	U	3/4	BATTVOLT*10.0	Battery Voltage [V] x 10	1
129	U	3/4	SOLABATTC*10.0	Battery Current [A] x 10	1
130	U	3/4	AUTONOMTIME	Autonomy Time in Minutes	1
131	U	3/4	BATTCAP	Battery Capacity	1

132	U	3/4	TEMPDEG*10.0	Temperature [°C] x 10	1
133	U	3/4	OUTFREQ0*10.0	Output Frequency [Hz] x 10	1
134	U	3/4	OUTPUT_VOLT0	Output Voltage Phase 1 [V]	1
135	U	3/4	OUTPOWER0	Outpower Phase 1 [%]	1
136	U	3/4	OUTPUT_CUR0	Output Current Phase 1 [A]	1
137	U	3/4	OUTPUT_POW0	Outpower Phase 1 [W]	1

Section OEM: AEG Protect 2.33, 3.33, 4.33, 5.33, 8.33, blue

Address	Type	Function	Name	Description	Length
100	U	3/4	(FKTSTATUS&0x4102)==0	Normal Operation	1
101	U	3/4	SNMPALARMS&0x100)>>8	On Bypass	1
102	U	3/4	(SNMPALARMS&0x2)>>1	On Battery	1
103	U	3/4	(SNMPALARMS&0x4000)>>14	UPS System Off	1
104	U	3/4	CNT_PF	Powerfail Counter	1
105	U	3/4	(SNMPALARMS&0x20000)>>17	General Fault	1
106	U	3/4	(SNMPALARMS&0x80000)>>19	Communication Lost	1
107	U	3/4	(SNMPALARMS&0x20)>>5	Input Bad	1
108	U	3/4	(SNMPALARMS&0x1000)>>12	Charger Failed	1
109	U	3/4	(SNMPALARMS&0x1)	Battery Bad	1
110	U	3/4	(SNMPALARMS&0x40)>>6	Output Bad	1
111	U	3/4	(SNMPALARMS&0x200)>>9	Bypass Bad	1
112	U	3/4	(SNMPALARMS&0x4)>>2	Low Battery	1
113	U	3/4	(SNMPALARMS&0x8)>>3	Depleted Battery	1
114	U	3/4	(SNMPALARMS&0x10)>>4	Temperature Bad	1
115	U	3/4	(SNMPALARMS&0x80)>>7	Output Overload	1
116	U	3/4	(SNMPALARMS&0x8000)>>15	Fan Failure	1
117	U	3/4	(SNMPALARMS&0x2000)>>13	UPS Output Off	1
118	U	3/4	AUX1STATE	State AUX Port 1 1 = active (high) ; 0 = not active (low)	1
119	U	3/4	AUX2STATE	State AUX Port 2 1 = active (high) ; 0 = not active (low)	1
120	U	3/4	AUX3STATE	State AUX Port 3 1 = active (high) ; 0 = not active (low)	1
121	U	3/4	AUX4STATE	State AUX Port 4 1 = active (high) ; 0 = not active (low)	1
122	U	3/4	INFREQ0*10.0	Input Frequency Hz Phase 1	1
123	U	3/4	INVOLT0	Input Voltage Phase 1 V	1
124	U	3/4	INVOLT1	Input Voltage Phase 2 V	1

125	U	3/4	INVOLT2	Input Voltage Phase 3 V	1
126	U	3/4	BP_FREQ0*10.0	Output Frequency [Hz]	1
127	U	3/4	BP_VOLT0	Bypass Voltage Phase 1 [V]	1
128	U	3/4	BP_VOLT1	Bypass Voltage Phase 2 [V]	1
129	U	3/4	BP_VOLT2	Bypass Voltage Phase 3 [V]	1
130	U	3/4	BATTVOLT*10.0	Battery Voltage [V] x 10	1
131	U	3/4	SOLABATTC*10.0	Battery Current [A] x 10	1
132	U	3/4	AUTONOMTIME	Autonomy Time in Minutes	1
133	U	3/4	BATTCAP	Battery Capacity	1
134	U	3/4	TEMPDEG*10.0	Temperature [°C] x 10	1
135	U	3/4	OUTFREQ0*10.0	Output Frequency [Hz] x 10	1
136	U	3/4	OUTPUT_VOLT0	Output Voltage Phase 1 [V]	1
137	U	3/4	OUTPOWER0	Outpower Phase 1 [%]	1
138	U	3/4	OUTPUT_CUR0	Output Current Phase 1 [A]	1
139	U	3/4	OUTPUT_POW0	Outpower Phase 1 [W]	1
140	U	3/4	OUTPUT_VOLT1	Output Voltage Phase 2 [V]	1
141	U	3/4	OUTPOWER1	Outpower Phase 2 [%]	1
142	U	3/4	OUTPUT_CUR1	Output Current Phase 2 [A]	1
143	U	3/4	OUTPUT_POW1	Outpower Phase 2 [W]	1
144	U	3/4	OUTPUT_VOLT2	Output Voltage Phase 3 [V]	1
145	U	3/4	OUTPOWER2	Outpower Phase 3 [%]	1
146	U	3/4	OUTPUT_CUR2	Output Current Phase 3 [A]	1
147	U	3/4	OUTPUT_POW2	Outpower Phase 3 [W]	1

Section OEM: POWERTRONIX

Adress	Name	MIZAR ALCOR	QUASAR	SUPERNOVAE
100	Outpower Phase 1 %	x	x	x
101	Outpower Phase 2 %	x	x	x
102	Outpower Phase 3 %	x	x	x
103	Battery Capacity %	x	x	x
104	Input Voltage Phase 1 V	x	x	x
105	Input Voltage Phase 2 V	x	x	x
106	Input Voltage Phase 3 V	x	x	x
107	Temperature °C	not supported	x	x
108	Autonomy Time minutes	x	x	x
109	UPS Status (ASCII Hex)	x	x	x
110	Battery Voltage V	x	x	x

111	Input Frequency Phase 1 Hz	not supported	x	not supported
112	Input Frequency Phase 2 Hz	not supported	x	not supported
113	Input Frequency Phase 3 Hz	not supported	x	not supported
114	Powerfail Counter	x	x	x
115	Alarm: Battery Bad	x	x	x
116	Alarm: On Battery	x	x	x
117	Alarm: Battery Low	not supported	not supported	x
118	Alarm: Battery Depleted	x	not supported	x
119	Alarm: Overtemperature	x	not supported	x
120	Alarm: Input Bad	x	x	x
121	Alarm: Output Bad	not supported	x	not supported
122	Alarm: Output Overload	x	x	x
123	Alarm: On Bypass	x	x	x
124	Alarm: Bypass Bad	x	x	x
125	Alarm: Output Off As Requested	x	x	x
126	Alarm: UPS Off As Requested	x	x	x
127	Alarm: Charger Failed		x	x
128	Alarm: UPS Output Off	x	x	x
129	Alarm: UPS Sytem Off	not supported	x	not supported
130	Alarm: Fan Failure	x	not supported	x
131	Alarm: Fuse Failure	not supported	not supported	not supported
132	Alarm: General Fault	x	x	x
133	Alarm: Diagnose Test Failed	not supported	not supported	not supported
134	Alarm: Communication Lost	x	x	x
135	Alarm: Awaiting Power	not supported	not supported	not supported
136	Alarm: Shutdown Pending	not supported	not supported	not supported
137	Alarm: Shutdown Imminent	not supported	not supported	not supported
138	Alarm: Test In Progress	x	not supported	not supported
139	AUX Port 1	x	x	x
140	AUX Port 2	x	x	x
141	AUX Port 3	x	x	x
142	AUX Port 4	x	x	x

Section OEM: Socomec UPS

Address	Type	Function	Name	Description	Length
97	U	3 / 4	OUTPUT_VOLT0	Output Voltage Phase 1 in V	1
98	U	3 / 4	OUTPUT_VOLT1	Output Voltage Phase 2 in V	1

Address	Type	Function	Name	Description	Length
99	U	3 / 4	OUTPUT_VOLT2	Output Voltage Phase 3 in V	1
100	U	3 / 4	OUTPOWER0	Outpower Phase 1 %	1
101	U	3 / 4	OUTPOWER1	Outpower Phase 2 %	1
102	U	3 / 4	OUTPOWER2	Outpower Phase 3 %	1
103	U	3 / 4	BATTCAP	Battery Capacity %	1
104	S	3 / 4	INVOLT0	Input Voltage Phase 1 V	1
105	S	3 / 4	INVOLT1	Input Voltage Phase 2 V	1
106	S	3 / 4	INVOLT2	Input Voltage Phase 3 V	1
107	S	3 / 4	TEMPDEG	Temperature C°	1
108	S	3 / 4	AUTONOMTIME	Autonomy Time minutes	1
109	U	3 / 4	STATUS	UPS Status (ASCII HEX) Please note UPSMAN status bytes table below (e. g. UPS normal = -4 , Powerfail = -12 , Battery test running = -68 , Bypass = -5)	1
110	S	3 / 4	BATTVOLT	Battery Voltage V	1
111	U	3 / 4	INFREQ0	Input Frequency Hz Phase 1	1
112	U	3 / 4	INFREQ1	Input Frequency Hz Phase 2	1
113	U	3 / 4	INFREQ2	Input Frequency Hz Phase 3	1
114	U	3 / 4	CNT_PF	Powerfail Counter	1
115	U	3 / 4	Alarm Battery Bad	1 = active; 0 = not active	1
116	U	3 / 4	Alarm: On Battery	1 = active; 0 = not active	1
117	U	3 / 4	Alarm: Battery Low	1 = active; 0 = not active	1
118	U	3 / 4	Alarm: Battery Depleted	1 = active; 0 = not active	1
119	U	3 / 4	Alarm: Over temperature	1 = active; 0 = not active	1
120	U	3 / 4	Alarm: Input Bad	1 = active; 0 = not active	1
121	U	3 / 4	Alarm: Output Bad	1 = active; 0 = not active	1
122	U	3 / 4	Alarm: Output Overload	1 = active; 0 = not active	1
123	U	3 / 4	Alarm: On Bypass	1 = active; 0 = not active	1
124	U	3 / 4	Alarm: Bypass Bad	1 = active; 0 = not active	1
125	U	3 / 4	Alarm: Output Off as requested.	1 = active; 0 = not active	1
126	U	3 / 4	Alarm: UPS Off as requested.	1 = active; 0 = not active	1
127	U	3 / 4	Alarm: Charger Failed	1 = active; 0 = not active	1
128	U	3 / 4	Alarm: UPS Output Off	1 = active; 0 = not active	1
129	U	3 / 4	Alarm: UPS System Off	1 = active; 0 = not active	1
130	U	3 / 4	Alarm: Fan Failure	1 = active; 0 = not active	1
131	U	3 / 4	Alarm: fuse failure	1 = active; 0 = not active	1
132	U	3 / 4	Alarm: general fault	1 = active; 0 = not active	1
133	U	3 / 4	Alarm: diagnose test failed	1 = active; 0 = not active	1

Address	Type	Function	Name	Description	Length
134	U	3 / 4	Alarm: communication lost	1 = active; 0 = not active	1
135	U	3 / 4	Alarm: awaiting power	1 = active; 0 = not active	1
136	U	3 / 4	Alarm: shutdown pending	1 = active; 0 = not active	1
137	U	3 / 4	Alarm: shutdown imminent	1 = active; 0 = not active	1
138	U	3 / 4	Alarm: test in progress	1 = active; 0 = not active	1
139	U	3 / 4	AUX Port 1	1 = active (high), 0 = not active (low)	1
140	U	3 / 4	AUX Port 2	1 = active (high), 0 = not active (low)	1
141	U	3 / 4	AUX Port 3	1 = active (high), 0 = not active (low)	1
142	U	3 / 4	AUX Port 4	1 = active (high), 0 = not active (low)	1
143	U	3 / 4	Sensormanager/SMTCOM sensor 1	Analog value	1
144	U	3 / 4	Sensormanager/SMTHCOM sensor 2	Analog value	1
145	U	3 / 4	Sensormanager sensor 3	Analog value	1
146	U	3 / 4	Sensormanager sensor 4	Analog value	1
147	U	3 / 4	Sensormanager sensor 5	Analog value	1
148	U	3 / 4	Sensormanager sensor 6	Analog value	1
149	U	3 / 4	Sensormanager sensor 7	Analog value	1
150	U	3 / 4	Sensormanager sensor 8	Analog value	1
151	U	3 / 4	INCURR0	Input Current Phase 1	1
152	U	3 / 4	INCURR1	Input Current Phase 2	1
153	U	3 / 4	INCURR2	Input Current Phase 3	1
154	U	3 / 4	OUTFREQ0	Output Frequency Phase 1	1
155	U	3 / 4	EX_OUT_CURR0	External Output Current Phase 1	1
156	U	3 / 4	EX_OUT_CURR1	External Output Current Phase 2	1
157	U	3 / 4	EX_OUT_CURR2	External Output Current Phase 3	1

Section MHD Modular / Multimatic Modular / AEG Protect 1. Modular, ENIGMA

Address	Type	Function	Name	Description	Length
100	U	3 / 4	OUTPOWER0	Outpower Phase 1 %	1
101	U	3 / 4	OUTPOWER1	Outpower Phase 2 %	1
102	U	3 / 4	OUTPOWER2	Outpower Phase 3 %	1
103	U	3 / 4	BATTCAP	Battery Capacity %	1
104	S	3 / 4	INVOLT0	Input Voltage Phase 1 V	1
105	S	3 / 4	INVOLT1	Input Voltage Phase 2 V	1
106	S	3 / 4	INVOLT2	Input Voltage Phase 3 V	1
107	S	3 / 4	TEMPDEG	Temperature C°	1
108	S	3 / 4	AUTONOMTIME	Autonomy Time minutes	1
109	U	3 / 4	STATUS (e. g. UPS normal = "4", Powerfail = "12", Battery test running = "68", Bypass = "5")	UPS Status (ASCII HEX), please note UPSMAN status bytes table below	1

Address	Type	Function	Name	Description	Length
110	U	3 / 4	BATTVOLT	Battery Voltage V	1
111	U	3 / 4	INFREQ0	Input Frequency Hz Phase 1	1
112	U	3 / 4	INFREQ1	Input Frequency Hz Phase 2	1
113	U	3 / 4	INFREQ2	Input Frequency Hz Phase 3	1
114	U	3 / 4	CNT_PF	Powerfail Counter	1
115	U	3 / 4	(SNMPALARMS&0x1)	Alarm Battery Bad	1
116	U	3 / 4	(SNMPALARMS&0x2)>>1	Alarm: On Battery	1
117	U	3 / 4	(SNMPALARMS&0x4)>>2	Alarm: Battery Low	1
118	U	3 / 4	(SNMPALARMS&0x8)>>3	Alarm: Battery Depleted	1
119	U	3 / 4	(SNMPALARMS&0x10)>>4	Alarm: Over temperature	1
120	U	3 / 4	(SNMPALARMS&0x20)>>5	Alarm: Input Bad	1
121	U	3 / 4	(SNMPALARMS&0x40)>>6	Alarm: Output Bad	1
122	U	3 / 4	(SNMPALARMS&0x80)>>7	Alarm: Output Overload	1
123	U	3 / 4	(SNMPALARMS&0x100)>>8	Alarm: On Bypass	1
124	U	3 / 4	(SNMPALARMS&0x200)>>9	Alarm: Bypass Bad	1
125	U	3 / 4	(SNMPALARMS&0x400)>>10	Alarm: Output Off as requested.	1
126	U	3 / 4	(SNMPALARMS&0x800)>>11	Alarm: UPS Off as requested.	1
127	U	3 / 4	(SNMPALARMS&0x1000)>>12	Alarm: Charger Failed	1
128	U	3 / 4	(SNMPALARMS&0x2000)>>13	Alarm: UPS Output Off	1
129	U	3 / 4	(SNMPALARMS&0x4000)>>14	Alarm: UPS System Off	1
130	U	3 / 4	(SNMPALARMS&0x8000)>>15	Alarm: Fan Failure	1
131	U	3 / 4	(SNMPALARMS&0x10000)>>1	Alarm: fuse failure	1
132	U	3 / 4	(SNMPALARMS&0x20000)>>1	Alarm: general fault	1
133	U	3 / 4	(SNMPALARMS&0x40000)>>1	Alarm: diagnose test failed	1
134	U	3 / 4	(SNMPALARMS&0x80000)>>1	Alarm: communication lost	1
135	U	3 / 4	(SNMPALARMS&0x100000)>>	Alarm: awaiting power	1
136	U	3 / 4	(SNMPALARMS&0x200000)>>	Alarm: shutdown pending	1
137	U	3 / 4	(SNMPALARMS&0x400000)>>	Alarm: shutdown imminent	1
138	U	3 / 4	(SNMPALARMS&0x800000)>>	Alarm: test in progress	1
139	U	3 / 4	AUX1STATE	AUX Port 1	1
140	U	3 / 4	AUX2STATE	AUX Port 2	1
141	U	3 / 4	AUX3STATE	AUX Port 3	1
142	U	3 / 4	AUX4STATE	AUX Port 4	1
143	U	3 / 4	TEMP1	Sensormanager/SMTCOM sensor 1	1
144	U	3 / 4	TEMP2	Sensormanager/SMTHCOM sensor 2	1
145	U	3 / 4	TEMP3	Sensormanager sensor 3	1
146	U	3 / 4	TEMP4	Sensormanager sensor 4	1
147	U	3 / 4	TEMP5	Sensormanager sensor 5	1
148	U	3 / 4	TEMP6	Sensormanager sensor 6	1
149	U	3 / 4	TEMP7	Sensormanager sensor 7	1
150	U	3 / 4	TEMP8	Sensormanager sensor 8	1
151	U	3 / 4	AEESerModulePresent(1)	Status data, for details contact Effekta	1
152	U	3 / 4	AEESerModulePresent(2)	Status data, for details contact Effekta	1
153	U	3 / 4	AEESerModulePresent(3)	Status data, for details contact Effekta	1
154	U	3 / 4	AEESerModulePresent(4)	Status data, for details contact Effekta	1
155	U	3 / 4	AEESerModulePresent(5)	Status data, for details contact Effekta	1
156	U	3 / 4	AEESerModulePresent(6)	Status data, for details contact Effekta	1
157	U	3 / 4	AEESerModuleError(1,1)	Status data, for details contact Effekta	1
158	U	3 / 4	AEESerModuleError(1,2)	Status data, for details contact Effekta	1
159	U	3 / 4	AEESerModuleError(1,3)	Status data, for details contact Effekta	1
160	U	3 / 4	AEESerModuleError(1,4)	Status data, for details contact Effekta	1

Address	Type	Function	Name	Description	Length
161	U	3 / 4	AEESerModuleError(2,1)	Status data, for details contact Effekta	1
162	U	3 / 4	AEESerModuleError(2,2)	Status data, for details contact Effekta	1
163	U	3 / 4	AEESerModuleError(2,3)	Status data, for details contact Effekta	1
164	U	3 / 4	AEESerModuleError(2,4)	Status data, for details contact Effekta	1
165	U	3 / 4	AEESerModuleError(3,1)	Status data, for details contact Effekta	1
166	U	3 / 4	AEESerModuleError(3,2)	Status data, for details contact Effekta	1
167	U	3 / 4	AEESerModuleError(3,3)	Status data, for details contact Effekta	1
168	U	3 / 4	AEESerModuleError(3,4)	Status data, for details contact Effekta	1
169	U	3 / 4	AEESerModuleError(4,1)	Status data, for details contact Effekta	1
170	U	3 / 4	AEESerModuleError(4,2)	Status data, for details contact Effekta	1
171	U	3 / 4	AEESerModuleError(4,3)	Status data, for details contact Effekta	1
172	U	3 / 4	AEESerModuleError(4,4)	Status data, for details contact Effekta	1
173	U	3 / 4	AEESerModuleError(5,1)	Status data, for details contact Effekta	1
174	U	3 / 4	AEESerModuleError(5,2)	Status data, for details contact Effekta	1
175	U	3 / 4	AEESerModuleError(5,3)	Status data, for details contact Effekta	1
176	U	3 / 4	AEESerModuleError(5,4)	Status data, for details contact Effekta	1
177	U	3 / 4	AEESerModuleError(6,1)	Status data, for details contact Effekta	1
178	U	3 / 4	AEESerModuleError(6,2)	Status data, for details contact Effekta	1
179	U	3 / 4	AEESerModuleError(6,3)	Status data, for details contact Effekta	1
180	U	3 / 4	AEESerModuleError(6,4)	Status data, for details contact Effekta	1
181	U	3 / 4	AEESerModuleWarning(1)	Status data, for details contact Effekta	1
182	U	3 / 4	AEESerModuleWarning(2)	Status data, for details contact Effekta	1
183	U	3 / 4	AEESerModuleWarning(3)	Status data, for details contact Effekta	1
184	U	3 / 4	AEESerModuleWarning(4)	Status data, for details contact Effekta	1
185	U	3 / 4	AEESerModuleWarning(5)	Status data, for details contact Effekta	1
186	U	3 / 4	AEESerModuleWarning(6)	Status data, for details contact Effekta	1
187	U	3 / 4	AEESerModuleState(1)	Status data, for details contact Effekta	1
188	U	3 / 4	AEESerModuleState(2)	Status data, for details contact Effekta	1
189	U	3 / 4	AEESerModuleState(3)	Status data, for details contact Effekta	1
190	U	3 / 4	AEESerModuleState(4)	Status data, for details contact Effekta	1
191	U	3 / 4	AEESerModuleState(5)	Status data, for details contact Effekta	1
192	U	3 / 4	AEESerModuleState(6)	Status data, for details contact Effekta	1
193	U	3 / 4	AEESerModuleVolt(1)	Status data, for details contact Effekta	1
194	U	3 / 4	AEESerModuleVolt(2)	Status data, for details contact Effekta	1
195	U	3 / 4	AEESerModuleVolt(3)	Status data, for details contact Effekta	1
196	U	3 / 4	AEESerModuleVolt(4)	Status data, for details contact Effekta	1
197	U	3 / 4	AEESerModuleVolt(5)	Status data, for details contact Effekta	1
198	U	3 / 4	AEESerModuleVolt(6)	Status data, for details contact Effekta	1
199	U	3 / 4	AEESerModuleCurr(1)	Status data, for details contact Effekta	1
200	U	3 / 4	AEESerModuleCurr(2)	Status data, for details contact Effekta	1
201	U	3 / 4	AEESerModuleCurr(3)	Status data, for details contact Effekta	1
202	U	3 / 4	AEESerModuleCurr(4)	Status data, for details contact Effekta	1
203	U	3 / 4	AEESerModuleCurr(5)	Status data, for details contact Effekta	1
204	U	3 / 4	AEESerModuleCurr(6)	Status data, for details contact Effekta	1
205	U	3 / 4	seconbat	Time on Battery [sec.]	1
206	U	3 / 4	OUTPUT_VOLT0	Output Voltage [V]	1
207	U	3 / 4	E_OUTPOWER*10.0	Enigma total output power [KW]	1
208	U	3 / 4	E_OUTCPOWER*10.0	Enigma total output compl. power [KVA]	1

Address	Type	Function	Name	Description	Length
1	U	3 / 4	Manufacturer	Manufacturer	1
17	U	3 / 4	Version	Version	1
33	U	3 / 4	Identification	Identification	1
65	U	3 / 4	Model	Model	1
97	U	3 / 4	AUTONOMTIME	Autonomy time in minutes	1
98	U	3 / 4	BATTCAP	Battery capacity in percent	1
99	U	3 / 4	OUTPUT	Output Source 0 Mains, 1 Battery, 2 Bypass	1
100	U	3 / 4	OUTFREQ0	Output Frequency	1
101	U	3 / 4	SOLAWROV0	Outputvoltage Phase 1 in V	1
102	U	3 / 4	SOLAWROV1	Outputvoltage Phase 2 in V	1
103	U	3 / 4	SOLAWROV2	Outputvoltage Phase 3 in V	1
104	U	3 / 4	SOLAWROC0	Output Current Phase 1 in A	1
105	U	3 / 4	SOLAWROC1	Output Current Phase 2 in A	1
106	U	3 / 4	SOLAWROC2	Output Current Phase 3 in A	1
107	U	3 / 4	OUTPOWER0	Outpower Phase 1 %	1
108	U	3 / 4	OUTPOWER1	Outpower Phase 2 %	1
109	U	3 / 4	OUTPOWER2	Outpower Phase 3 %	1
110	U	3 / 4	SOLSETEMPBAD	Temperature bad	1
111	U	3 / 4	SOLSEINPUTBAD	Input bad	1
112	U	3 / 4	SOLSEOVERLOAD	Overload	1
113	U	3 / 4	SOLSEBYPASSFAULT	Bypass fault	1
114	U	3 / 4	SOLSECHARGERFAULT	Charger fault	1
115	U	3 / 4	SOLSEGENERALFAULT	General fault	1
116	U	3 / 4	SOLSESDPENDING	Shutdown pending	1
117	U	3 / 4	SOLSETESTRESULT	Test result	1
118	U	3 / 4	(SNMPALARMS&0x80000)>>19	Communication Lost Alarm	1
119	U	3 / 4	INFREQ0	Input Frequency Phase 1 in Hz	1
120	U	3 / 4	INFREQ1	Input Frequency Phase 2 in Hz	1
121	U	3 / 4	INFREQ2	Input Frequency Phase 3 in Hz	1
122	U	3 / 4	INVOLT0	Input Voltage Phase 1 in V	1
123	U	3 / 4	INVOLT1	Input Voltage Phase 2 in V	1
124	U	3 / 4	INVOLT2	Input Voltage Phase 3 in V	1
125	U	3 / 4	INCURR0	Input Current Phase 1 in A	1
126	U	3 / 4	INCURR1	Input Current Phase 2 in A	1
127	U	3 / 4	INCURR2	Input Current Phase 3 in A	1
128	U	3 / 4	EX_BYP_VOLT0	Bypass Voltage Phase 1 in V	1

129	U	3 / 4	EX_BYP_VOLT1	Bypass Voltage Phase 2 in V	1
130	U	3 / 4	EX_BYP_VOLT2	Bypass Voltage Phase 3 in V	1
131	U	3 / 4	EX_BYP_CURR0	Bypass Current Phase 1 in A	1
132	U	3 / 4	EX_BYP_CURR1	Bypass Current Phase 2 in A	1
133	U	3 / 4	EX_BYP_CURR2	Bypass Current Phase 3 in A	1
134	U	3 / 4	EX_BYP_WATT0	Bypass Power Phase 1 [W]	1
135	U	3 / 4	EX_BYP_WATT1	Bypass Power Phase 2 [W]	1
136	U	3 / 4	EX_BYP_WATT2	Bypass Power Phase 3 [W]	1
137	U	3 / 4	EX_BYP_FREQ0	Bypass Frequency [Hz]	1
138	U	3 / 4	EX_INP_WATT0	Input Power Phase 1 [W]	1
139	U	3 / 4	EX_INP_WATT1	Input Power Phase 2 [W]	1
140	U	3 / 4	EX_INP_WATT2	Input Power Phase 3 [W]	1
141	U	3 / 4	BATTVOLT	Battery Voltage [V]	1
142	U	3 / 4	TEMPDEG	Temperature [°C]	1
143	U	3 / 4	EX_BATT_SECONBATT	Time on Battery [sec.]	1
144	U	3 / 4	EX_BATT_CURRPOS	positive battery current [A]	1
145	U	3 / 4	BATTCONDITION	Flags for battery condition	1
146	U	3 / 4	INPHASES	amount of Phases at Input	1
147	U	3 / 4	OUTPHASES	amount of Phases at Output	1
148	U	3 / 4	SOLABATTC	Battery Current [A]	1

Section Inform UPS / Pyramid DSP/Online DSP

Address	Type	Function	Name	Description	Length
100	U	3 / 4	OUTPOWER0	Outpower Phase 1 %	1
101	U	3 / 4	OUTPOWER1	Outpower Phase 2 %	1
102	U	3 / 4	OUTPOWER2	Outpower Phase 3 %	1
103	U	3 / 4	BATTCAP	Battery Capacity %	1
104	S	3 / 4	INVOLT0	Input Voltage Phase 1 V	1
105	S	3 / 4	INVOLT1	Input Voltage Phase 2 V	1
106	S	3 / 4	INVOLT2	Input Voltage Phase 3 V	1
107	S	3 / 4	TEMPDEG	Temperature C°	1
108	S	3 / 4	AUTONOMTIME	Autonomy Time minutes	1
109	U	3 / 4	STATUS (e. g. UPS normal = -4 , Powerfail = -12 , Battery test running = -68 , Bypass = -5)	UPS Status (ASCII HEX) Please note UPSMAN status bytes table below	1
110	S	3 / 4	BATTVOLT	Battery Voltage V	1
111	U	3 / 4	INFREQ0	Input Frequency Hz Phase 1	1

112	U	3 / 4	INFREQ1	Input Frequency Hz Phase 2	1
113	U	3 / 4	INFREQ2	Input Frequency Hz Phase 3	1
114	U	3 / 4	CNT_PF	Powerfail Counter	1
115	U	3 / 4	Alarm Battery Bad	1 = active; 0 = not active	1
116	U	3 / 4	Alarm: On Battery	1 = active; 0 = not active	1
117	U	3 / 4	Alarm: Battery Low	1 = active; 0 = not active	1
118	U	3 / 4	Alarm: Battery Depleted	1 = active; 0 = not active	1
119	U	3 / 4	Alarm: Over temperature	1 = active; 0 = not active	1
120	U	3 / 4	Alarm: Input Bad	1 = active; 0 = not active	1
121	U	3 / 4	Alarm: Output Bad	1 = active; 0 = not active	1
122	U	3 / 4	Alarm: Output Overload	1 = active; 0 = not active	1
123	U	3 / 4	Alarm: On Bypass	1 = active; 0 = not active	1
124	U	3 / 4	Alarm: Bypass Bad	1 = active; 0 = not active	1
125	U	3 / 4	Alarm: Output Off as requested.	1 = active; 0 = not active	1
126	U	3 / 4	Alarm: UPS Off as requested.	1 = active; 0 = not active	1
127	U	3 / 4	Alarm: Charger Failed	1 = active; 0 = not active	1
128	U	3 / 4	Alarm: UPS Output Off	1 = active; 0 = not active	1
129	U	3 / 4	Alarm: UPS System Off	1 = active; 0 = not active	1
130	U	3 / 4	Alarm: Fan Failure	1 = active; 0 = not active	1
131	U	3 / 4	Alarm: fuse failure	1 = active; 0 = not active	1
132	U	3 / 4	Alarm: general fault	1 = active; 0 = not active	1
133	U	3 / 4	Alarm: diagnose test failed	1 = active; 0 = not active	1
134	U	3 / 4	Alarm: communication lost	1 = active; 0 = not active	1
135	U	3 / 4	Alarm: awaiting power	1 = active; 0 = not active	1
136	U	3 / 4	Alarm: shutdown pending	1 = active; 0 = not active	1
137	U	3 / 4	Alarm: shutdown imminent	1 = active; 0 = not active	1
138	U	3 / 4	Alarm: test in progress	1 = active; 0 = not active	1
139	U	3 / 4	AUX Port 1	1 = active (high), 0 = not active (low)	1
140	U	3 / 4	AUX Port 2	1 = active (high), 0 = not active (low)	1
141	U	3 / 4	AUX Port 3	1 = active (high), 0 = not active (low)	1
142	U	3 / 4	AUX Port 4	1 = active (high), 0 = not active (low)	1
143	U	3 / 4	Sensormanager/SMTCOM sensor 1	Analog value	1
144	U	3 / 4	Sensormanager/SMTHCOM sensor 2	Analog value	1
145	U	3 / 4	Sensormanager sensor 3	Analog value	1
146	U	3 / 4	Sensormanager sensor 4	Analog value	1
147	U	3 / 4	Sensormanager sensor 5	Analog value	1
148	U	3 / 4	Sensormanager sensor 6	Analog value	1

149	U	3 / 4	Sensormanager sensor 7	Analog value	1
150	U	3 / 4	Sensormanager sensor 8	Analog value	1
151	U	3 / 4	OUTPUT_VOLT0	Outputvoltage Phase 1	1
152	U	3 / 4	OUTPUT_VOLT1	Outputvoltage Phase 2	1
153	U	3 / 4	OUTPUT_VOLT2	Outputvoltage Phase 3	1
154	U	3 / 4	OUTPUT_CURRENT0	Output Current Phase 1 in Ampere *10	1
155	U	3 / 4	OUTPUT_CURRENT1	Output Current Phase 2 in Ampere *10	1
156	U	3 / 4	OUTPUT_CURRENT2	Output Current Phase 3 in Ampere *10	1

Section Transfer Switches (All Transfer Switch vendors, except PILLER, STS TUMEL)

Address	Type	Function	Name	Description	Length
1	U	3 / 4	Sources Asynchronous	Warning, input current difference, switching might not be possible	1
2	U	3 / 4	Static Switch A Failure	Alarm, switching failure	1
3	U	3 / 4	Static Switch B Failure	Alarm, switching failure	1
4	U	3 / 4	On Static Switch A	Supplied from input A	1
5	U	3 / 4	On Static Switch B	Supplied from input B	1
6	U	3 / 4	On Manual Bypass A	Supplied via bypass from input A	1
7	U	3 / 4	On Manual Bypass A	Supplied via bypass from input B	1
8	U	3 / 4	Source A Failure	Alarm, input A failure, problem with voltage	1
9	U	3 / 4	Source B Failure	Alarm, input B failure, problem with voltage	1
10	U	3 / 4	General Fault	General alarm	1
11	U	3 / 4	Redundancy Lost	Redundancy lost,	1
12	U	3 / 4	Output Overload	To much load	1
13	U	3 / 4	Output Failure	Output failure	1

Section STS TUMEL Transfer Switch

Address	Type	Function	Name	Description	Length
100	U	3 / 4	INPVOLT_NET_10	Input Voltage	1
101	U	3 / 4	INPVOLT_NET_11	Input Voltage	1
102	U	3 / 4	INPVOLT_NET_12	Input Voltage	1
103	U	3 / 4	INFREQ_NET_1	Input Frequency	1
104	U	3 / 4	INPVOLT_NET_20	Input Voltage	1
105	U	3 / 4	INPVOLT_NET_21	Input Voltage	1
106	U	3 / 4	INPVOLT_NET_22	Input Voltage	1
107	U	3 / 4	INFREQ_NET_2	Input Frequency	1

108	U	3 / 4	STS_SYNCANGLE		1
109	U	3 / 4	STS_SYNDIFF		1
110	U	3 / 4	STS_S1BALANCE		1
111	U	3 / 4	STS_S2BALANCE		1
112	U	3 / 4	TEMPDEG	Temperature in degrees C°	1
113	U	3 / 4	OUTPUT_VOLT0	Output Voltage Phase 1	1
114	U	3 / 4	OUTPUT_VOLT1	Output Voltage Phase 2	1
115	U	3 / 4	OUTPUT_VOLT1	Output Voltage Phase 3	1
116	U	3 / 4	EX_OUT_CURR0		1
117	U	3 / 4	EX_OUT_CURR1		1
118	U	3 / 4	EX_OUT_CURR2		1
119	U	3 / 4	OUTPOWER0	Output Power Phase 1	1
120	U	3 / 4	OUTPOWER1	Output Power Phase 2	1
121	U	3 / 4	OUTPOWER2	Output Power Phase 3	1

Section OEM TRIMOD

Address	Type	Function	Name	Description	Length
100	U	3 / 4	OUTPOWER0	Outpower Phase 1 %	1
101	U	3 / 4	OUTPOWER1	Outpower Phase 2 %	1
102	U	3 / 4	OUTPOWER2	Outpower Phase 3 %	1
103	U	3 / 4	BATTCAP	Battery capacity in percent	1
104	U	3 / 4	INVOLT0	Input Voltage Phase 1 in V	1
105	U	3 / 4	INVOLT1	Input Voltage Phase 2 in V	1
106	U	3 / 4	INVOLT2	Input Voltage Phase 3 in V	1
107	U	3 / 4	TEMPDEG	Temperature C°	1
108	U	3 / 4	AUTONOMTIME	Autonomy Time minutes	1
109	U	3 / 4	STATUS	GENEREX UPS status	1
110	U	3 / 4	BATTVOLT	Battery Voltage V	1
111	U	3 / 4	INFREQ0	Input Frequency Hz Phase 1	1
112	U	3 / 4	INFREQ1	Input Frequency Hz Phase 2	1
113	U	3 / 4	INFREQ2	Input Frequency Hz Phase 3	1
114	U	3 / 4	CNT_PF	Powerfail Counter	1
115	U	3 / 4	(SNMPALARMS&0x1)	Alarmbit,contact legrand / Meta	1
116	U	3 / 4	(SNMPALARMS&0x2)>>1	Alarmbit,contact legrand / Meta	1
117	U	3 / 4	(SNMPALARMS&0x4)>>2	Alarmbit,contact legrand / Meta	1
118	U	3 / 4	(SNMPALARMS&0x8)>>3	Alarmbit,contact legrand / Meta	1
119	U	3 / 4	(SNMPALARMS&0x10)>>4	Alarmbit,contact legrand / Meta	1

120	U	3 / 4	(stoi(TRIMOD_STATUS)&0x8)	Alarmbit,contact legrand / Meta	1
121	U	3 / 4	(CBSER2ALARM&0x40)>>6	Alarmbit,contact legrand / Meta	1
122	U	3 / 4	(SNMPALARMS&0x80)>>7	Alarmbit,contact legrand / Meta	1
123	U	3 / 4	(SNMPALARMS&0x100)>>8	Alarmbit,contact legrand / Meta	1
124	U	3 / 4	(stoi(TRIMOD_STATUS)&0x8)	Alarmbit,contact legrand / Meta	1
125	U	3 / 4	(SNMPALARMS&0x2000)>>13	Alarmbit,contact legrand / Meta	1
126	U	3 / 4	(SNMPALARMS&0x4000)>>14	Alarmbit,contact legrand / Meta	1
127	U	3 / 4	(SNMPALARMS&0x1000)>>12	Alarmbit,contact legrand / Meta	1
128	U	3 / 4	(SNMPALARMS&0x2000)>>13	Alarmbit,contact legrand / Meta	1
129	U	3 / 4	(SNMPALARMS&0x4000)>>14	Alarmbit,contact legrand / Meta	1
130	U	3 / 4	(SNMPALARMS&0x8000)>>15	Alarmbit,contact legrand / Meta	1
131	U	3 / 4	(SNMPALARMS&0x10000)>>16	Alarmbit,contact legrand / Meta	1
132	U	3 / 4	(SNMPALARMS&0x20000)>>17	Alarmbit,contact legrand / Meta	1
133	U	3 / 4	(stoi(CP_TESTRESULT)==2)	Alarmbit,contact legrand / Meta	1
134	U	3 / 4	(SNMPALARMS&0x80000)>>19	Alarmbit,contact legrand / Meta	1
135	U	3 / 4	(SNMPALARMS&0x100000)>>20	Alarmbit,contact legrand / Meta	1
136	U	3 / 4	(CBSER2ALARM&0x200000)>>2	Alarmbit,contact legrand / Meta	1
137	U	3 / 4	(CBSER2ALARM&0x400000)>>2	Alarmbit,contact legrand / Meta	1
138	U	3 / 4	(SNMPALARMS&0x800000)>>23	Alarmbit,contact legrand / Meta	1
139	U	3 / 4	(stoi(TRIMOD_STATUS)&0x10)	Alarmbit,contact legrand / Meta	1
140	U	3 / 4	OUTPUT_VOLT0	Outputvoltage Phase 1	1
141	U	3 / 4	OUTPUT_VOLT1	Outputvoltage Phase 2	1
142	U	3 / 4	OUTPUT_VOLT2	Outputvoltage Phase 3	1
143	U	3 / 4	TRIMOD_OUTCURR0*10.0	Output Current 1	1
144	U	3 / 4	TRIMOD_OUTCURR1*10.0	Output Current 2	1
145	U	3 / 4	TRIMOD_OUTCURR2*10.0	Output Current 3	1
152	U	3 / 4	TEMP1	Sensorman. sensor 1 / SMTCOM	1
153	U	3 / 4	TEMP2	Sensorman. sensor 2 / SMTHCOM	1
154	U	3 / 4	TEMP3	Sensormanager sensor 3	1
155	U	3 / 4	TEMP4	Sensormanager sensor 4	1
156	U	3 / 4	TEMP5	Sensormanager sensor 5	1
157	U	3 / 4	TEMP6	Sensormanager sensor 6	1
158	U	3 / 4	TEMP7	Sensormanager sensor 7	1
159	U	3 / 4	TEMP8	Sensormanager sensor 8	1
160	U	3 / 4	TRIMOD_OUTACTPWR0/1000.0	Output Phase 1	1
161	U	3 / 4	TRIMOD_OUTACTPWR1/1000.0	Output Phase 2	1
162	U	3 / 4	TRIMOD_OUTACTPWR2/1000.0	Output Phase 3	1
163	U	3 / 4	AUX1STATE	AUX Port 1	1

164	U	3 / 4	AUX2STATE	AUX Port 2	1
165	U	3 / 4	AUX3STATE	AUX Port 3	1
166	U	3 / 4	AUX4STATE	AUX Port 4	1

Section: EverExceed Inverter

Address	Type	Function	Name	Description	Length
100	U	3 / 4	TEMPDEG	Temperature in Degrees	1
101	U	3 / 4	INFREQ0	Line frequency	1
102	U	3 / 4	INVOLT0	Line voltage	1
103	U	3 / 4	OUTFREQ0	Frequency	1
104	U	3 / 4	OUTPUT_VOLT0	Output voltage	1
105	U	3 / 4	EX_OUT_VA0	Output power	1
106	U	3 / 4	STATUS	GENEREX UPS status (see below)	1
107	U	3 / 4	EX_EXTSTATUS	Alarm information	1
108	U	3 / 4	STATUS&1	Bypass mode, 1 = on, 0 = off	1
109	U	3 / 4	(STATUS&0x02)>>2	Output active, 1 = on, 0 = off	1
110	U	3 / 4	(STATUS&0x100)>>8	Overload, 1 = on, 0 = off	1
111	U	3 / 4	(STATUS&0x2000)>>13	General alarm, 1 = on, 0 = off	1

UPS Status EverExceed	Hex-Value	Dec-Value	Description
UPS_SB_BYPASS_MODE	0x0001	1	Bypass mode
UPS_SB_OUTPUT_ACT	0x0004	4	Output active
UPS_SB_OUTPUT_HIGH	0x0100	256	Overload
UPS_SB_UPS_FAILED	0x2000	8192	General alarm

Other OEM's : See OEM MODBUS Defaultadress 100 – 146 above

UPSMAN Status Bytes - Standard Device Status Bits

UPS Status	Hex-Value	Dec-Value	Description
UPS_SB_BYPASS_MODE	0x0001	1	power piped thru
UPS_SB_SHUTDOWN	0x0002	2	shutdown ups
UPS_SB_OUTPUT_ACT	0x0004	4	inverter on = UPS OK
UPS_SB_BACKUP_MODE	0x0008	8	battery power
UPS_SB_BATTERY_LOW	0x0010	16	low battery err

UPS_SB_OVER_TEMP	0x0020	32	over temp err
UPS_SB_TEST_ACT	0x0040	64	test in progress
UPS_SB_INPUT_HIGH	0x0080	128	over power err
UPS_SB_OUTPUT_HIGH	0x0100	256	over load err
UPS_SB_INVERTER_FAILURE	0x0200	512	Inverter error
UPS_SB_BATTERY_BAD	0x0400	1024	Battery error
UPS_SB_ECO_MODE	0x0800	2048	eco - bypass
UPS_SB_INVERTER_WARN	0x1000	4096	eco - bypass
UPS_SB_UPS_FAILED	0x2000	8192	prser flag
UPS_SB_COMM_LOST	0x4000	16384	for snmp
UPS_SB_DVG_ALARM	0x8000	32768	SiteManager/SiteMonitor

Example (decimal):

STATUS= „5|| means UPS_SB_OUTPUT_ACT (4) + UPS_SB_BYPASS_MODE (1) are active ! = UPS on Bypass!

STATUS= „12|| means UPS_SB_OUTPUT_ACT (4) + UPS_SB_BACKUP_MODE (8) are active ! = UPS Powerfail!

STATUS= „22|| means UPS_SB_OUTPUT_ACT (4) + UPS_SB_BACKUP_MODE (8) + UPS_SB_BATTERY_LOW (10) are active ! = UPS Powerfail and Battery low!

STATUS= „4|| means UPS_SB_OUTPUT_ACT (4) + no other alarms = UPS OK

BACS MODBUS Parameter

Standard BACS – Address Description

Note: the max. number of BACS Modules requestable through MODBUS is 330.

Note: —Type U/SI: this defines whether the answer has an algebraic sign (math. +/-) or not. U means —

Address	Type	Function	Name	Description	Length	
Note:						
"Type U/S": this defines whether the answer has an algebraic sign (math. +/-) or not. U means "unsigned". S means "signed", this answer may be positive or negative.						
1000	U	3 / 4	BACS_Alarm	BACS Alarm Flags (see alarm flag definition below) *4	1	
1001	U	3 / 4	BACS_ALARM	BACS Alarm Flags (see alarm flag definition below) *5	1	
1002	U	3 / 4	BACS_ALARM	BACS Alarm Flags (see alarm flag definition below) *6	1	
1003	U	3 / 4	BACS_NUMSTRINGS	Number of BACS Strings	1	
1004	U	3/4	BACS_NUMMODULES	Total number of BACS modules	1	
<i>This address range describes current and voltage of each single string as configured</i>						
1010	S	3 / 4	STRING_01_CUR	String 1 current in Ampere [A]	1	
1011	S	3 / 4	BACS_StrSumVolt	String 1 Overall BACS string voltage	1	
1012	S	3 / 4	BACS_StrAvgVolt	String 1 Average BACS string voltage	1	
1013	S	3 / 4	BACS_Str_CurrAC	String 1 BACS string current	1	
1014			<RESERVED>	Do not use		
1015	S	3 / 4	STRING_02_CUR	String 2 current in Ampere [A]	1	
1016	S	3 / 4	BACS_StrSumVolt	String 2 Overall BACS string voltage	1	
1017	S	3 / 4	BACS_StrAvgVolt	String 2 Average BACS string voltage	1	
1018	S	3 / 4	BACS_Str_CurrAC	String 2 BACS string current	1	
1019			<RESERVED>	Do not use		
1020	S	3 / 4	STRING_03_CUR	String 3 current in Ampere [A]	1	
1021	S	3 / 4	BACS_StrSumVolt	String 3 Overall BACS string voltage	1	
1022	S	3 / 4	BACS_StrAvgVolt	String3 Average BACS string voltage	1	
1023	S	3 / 4	BACS_Str_CurrAC	String 3 BACS string current	1	
1024			<RESERVED>	Do not use		
[...]	[...]	[...]	<i>[...Continue modbus string count until address ...]</i>			[...]
1055	S	3 / 4	STRING_10_CUR	String 10 current in Ampere [A]	1	
1056	S	3 / 4	BACS_StrSumVolt	String 10 Overall BACS string voltage	1	
1057	S	3 / 4	BACS_StrAvgVolt	String 10 Average BACS string voltage	1	
1058	S	3 / 4	BACS_Str_CurrAC	String 10 BACS string current	1	
1059			<RESERVED>	Do not use		

<i>This address range describes the BACS module modbus address range for module 1-330: Each module section contains 5 measuring values. There is no reserved address between the modules!</i>						
1060	S	3 / 4	MODULE_001_TEMP	Module 1 Temperature in Celsius [°C] (see Temfjasdfashfklashf) *1	1	
1061	S	3 / 4	MODULE_001_VOLT	Module 1 Voltage in Volt [V] *2	1	
1062	S	3 / 4	MODULE_001_IMPC	Module 1 Impedance in milliOhm [mΩ] *3	1	
1063	U	3 / 4	MODULE_001_ALARM	Module 1 Alarm flags *6	1	
1064	S	3 7 4	Module_001_ModBypVoltPc	Module 1 Exuqlizing / Balancing in %	1	
1065	S	3 / 4	MODULE_002_TEMP	Module 2 Temperature in Celsius [°C] (see Temfjasdfashfklashf) *1	1	
1066	S	3 / 4	MODULE_002_VOLT	Module 2 Voltage in Volt [V] *2	1	
1067	S	3 / 4	MODULE_002_IMPC	Module 2 Impedance in milliOhm [mΩ] *3	1	
1068	U	3 / 4	MODULE_002_ALARM	Module 2 Alarm flags *6	1	
1069	S	3 7 4	Module_002_ModBypVoltPc	Module 2 Exuqlizing / Balancing in %	1	
1070	S	3 / 4	MODULE_003_TEMP	Module 3 Temperature in Celsius [°C] (see Temfjasdfashfklashf) *1	1	
1071	S	3 / 4	MODULE_003_VOLT	Module 3 Voltage in Volt [V] *2	1	
1072	S	3 / 4	MODULE_003_IMPC	Module 3 Impedance in milliOhm [mΩ] *3	1	
1073	U	3 / 4	MODULE_003_ALARM	Module 3 Alarm flags *6	1	
1074	S	3 7 4	Module_003_ModBypVoltPc	Module 3 Exuqlizing / Balancing in %	1	
[...]	[...]	[...]	[...Continue modbus BACS module count until address ...]			[...]
2705	S	3 / 4	MODULE_330_TEMP	Module 330 Temperature in Celsius [°C] (see Temfjasdfashfklashf) *1	1	
2706	S	3 / 4	MODULE_330_VOLT	Module 330 Voltage in Volt [V] *2	1	
2707	S	3 / 4	MODULE_330_IMPC	Module 330 Impedance in milliOhm [mΩ] *3	1	
2708	U	3 / 4	MODULE_330_ALARM	Module 330 Alarm flags *6	1	
2709	S	3 / 4	Module_330_ModBypVoltPc	Module 330 <DESCRIPTION>	1	
<i>The following address range describes single string current and voltage for BACS strings 11-16</i>						
2710	S	3 / 4	STRING_11_CUR	String 11 current in Ampere [A]	1	

2711			<RESERVED>	Reserved, do not use		
2712			<RESERVED>	Reserved, do not use		
2713	S	3 / 4	String_11_AC	String 11 voltage	1	
2714			<RESERVED>	Reserved, do not use		
2715	S	3 / 4	STRING_12_CUR	String 12 current in Ampere [A]	1	
2716			<RESERVED>	Reserved, do not use		
2717			<RESERVED>	Reserved, do not use		
2718	S		String_12_AC	String 12 voltage	1	
2719			<RESERVED>	Reserved, do not use		
...	<i>[...Continue modbus BACS String count until address ...]</i>			...
2735	S	3 / 4	STRING_16_CUR	String 16 current in Ampere [A]	1	
2736			<RESERVED>	Reserved, do not use		
2737			<RESERVED>	Reserved, do not use		
2738	S		String_12_AC	String 12 voltage	1	
2739			<RESERVED>	Reserved, do not use		
<i>This address range describes the BACS module modbus address range for module 331-512: Each module section contains 5 measuring values. There is no reserved address between the modules!</i>						
2740	S	3 / 4	MODULE_331_TEMP	Module 331 Temperature in Celsius [°C] (see Temfjasdfashfklashf) *1	1	
2741	S	3 / 4	MODULE_331_VOLT	Module 331 Voltage in Volt [V] *2	1	
2742	S	3 / 4	MODULE_331_IMPC	Module 331 Impedance in milliOhm [mΩ] *3	1	
2743	U	3 / 4	MODULE_331_ALARM	Module 331 Alarm flags *6	1	
2744	S	3 / 4	Module_331_ModBypVoltPc	Module 331 Exuqlizing / Balancing in %	1	
2745	S	3 / 4	MODULE_332_TEMP	Module 332 Temperature in Celsius [°C] (see Temfjasdfashfklashf) *1	1	
2746	S	3 / 4	MODULE_332_VOLT	Module 332 Voltage in Volt [V] *2	1	
2747	S	3 / 4	MODULE_332_IMPC	Module 332 Impedance in milliOhm [mΩ] *3	1	
2748	U	3 / 4	MODULE_332_ALARM	Module 332 Alarm flags *6	1	
2749	S	3 / 4	Module_332_ModBypVoltPc	Module 332 Exuqlizing / Balancing in %	1	

...	[...Continue modbus BACS module count until address ...]		...
3645	S	3 / 4	MODULE_512_TEMP	Module 512 Temperature in Celsius [°C] (see Temfjasdfashfklashf) *1	1
3646	S	3 / 4	MODULE_512_VOLT	Module 512 Voltage in Volt [V] *2	1
3647	S	3 / 4	MODULE_512_IMPC	Module 512 Impedance in milliOhm [mΩ] *3	1
3648	U	3 / 4	MODULE_512_ALARM	Module 512 Alarm flags *6	1
3649	S	3 / 4	Module_512_ModBypVoltPc	Module 512 Exuqlizing / Balancing in %	1

Note: A value of -1 or -9999 means: This value is currently —Not availablell (-N/All).

***1 - Temperature value definition:**

Temperature T in °C $T = \frac{X-78}{2}$ e.g. $T = \frac{128-78}{2} = 25$

0xXX → 0 bis 255

0x7F 127 => 24,5°C

0x80 128 => 25°C

0x81 129 => 25,5°C

***2 - Voltage value definition:**

Voltage U in V Wert / 1000

e.g. **Voltage U in V** = 12825 / 1000 = 12,825 V

***3 - Impedance value definition:**

Impedance Z in mΩ Wert / 100

e.g. **Impedance Z in mΩ** = 4372 / 1000 = 43,72 mΩ

***4 – Address 1000 MODBUS/SNMP** (hexadecimal) (decimal)

BACS_STATE_NONE	0x0000	0
BACS_STATE_RUNNING	0x0001	1
BACS_STATE_CONNECTED	0x0002	2
BACS_STATE_MODULE_LOST	0x0004	4
BACS_STATE_DISCHARGING	0x0008	8
BACS_STATE_CHARGING	0x0010	16
BACS_STATE_DISCHARGING_STOPPED	0x0020	32
BACS_STATE_FLOAT_CHARGING	0x0040	64
BACS_STATE_EQUALISATION	0x0080	128
BACS_STATE_SYSTEM_FAILURE	0x0100	256
BACS_STATE_VOLTAGE_OUTOFRANGE	0x0200	512
BACS_STATE_TEMPERATURE_OUTOFRANGE	0x0400	1024
BACS_STATE_RESISTOR-OUTOFRANGE	0x0800	2048
BACS_STATE_MODULE-ADDRESSING	0x1000	4096
BACS_STATE_MODULE-SEARCHING	0x2000	8192
BACS_STATE_MODULE-INITIALIZING	0x4000	16384
BACS_STATE_MODULE-POLLING	0x8000	32768

***5 – Address 1001 MODBUS/SNMP** (hexadecimal) (decimal)

BACS_STATE-GENERAL-ALARM	0x0001	1
BACS_STATE-VOLTAGE-DIFF-HIGH	0x0002	2
BACS_STATE-BATTERY-BREAKER-OPEN	0x0004	4
BACS_STATE_THERMAL_RUNAWAY	0x0008	8

***6 – Address 1002 Alarm Flags MODBUS/SNMP** (hexadecimal) (decimal)

BACS_ALARM_NONE	0x0000	0
BACS_ALARM_GENERAL_ALARM	0x0001	1
BACS_ALARM_COMMUNICATION_LOST	0x0002	2
CS_ALARM_VOLTAGE_HIGH	0x0004	4

BACS_ALARM_VOLTAGE_LOW	0x0008	8
BACS_ALARM_TEMPERATURE_HIGH	0x0010	16
BACS_ALARM_TEMPERATURE_LOW	0x0020	32
BACS_ALARM_RESISTOR_HIGH	0x0040	64
BACS_ALARM_RESISTOR_LOW	0x0080	128
BACS_ALARM_EQUALISATION_ERR	0x0100	256
BACS_ALARM_VOLTAGE_WARN_HIGH	0x0200	512
BACS_ALARM_VOLTAGE_WARN_LOW	0x0400	1024
BACS_ALARM_TEMPERATURE_WARN_HIGH	0x0800	2048
BACS_ALARM_TEMPERATURE_WARN_LOW	0x1000	4096
BACS_ALARM_RESISTOR_WARN_HIGH	0x2000	8192
BACS_ALARM_RESISTOR_WARN_LOW	0x4000	16384
BACS_ALARM_MODREV_INCOMPATIBLE	0x8000	32768

Copyright and licenses

The copyright authorization from Generex and other relevant software suppliers must be respected.

Generex and their suppliers reserve the rights to the software components.

In particular the following are prohibited:

- *copying and distribution,*
- *modifications and derivations,*
- *decompilation, reverse engineering,*

Components which fall under GNU General Public License and further Open Source licenses are integrated into the software. An overview of the integrated Open Source components and a copy of the current license can be obtained at www.generex.de/legal/sla.

Generex will provide the source code for all components of software licensed under the GNU General Public License and comparable Open Source licenses.

For source code requests, please email info@generex.de.