RCCMD – Multiple Server Shutdown Software

User manual

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.

Revision	History	Date
-001	First Release	10/2008
-012	Added: RCCMD on Citrix XEN Server	12/2008
-013	RCCMD with SSL	12/2008
-014	Update: UNIX multiple sender configuration	01/2009
-015	Added: Alternative SSL configuration	02/2009
-016	Added: Syntax for switching outputs	03/2009
-017	Added: RCCMD Client as relay station	03/2009
-018	Update: Installation of RCCMD	06/2009
-019	Update: RCCMD InstallAnywhere Installation	07/2009
-020	Added: Silent Installation Windows	08/2009
-021	Added: Grafical RCCMD relay configuration	08/2009
-022	Added: Combined RCCMD Silent Installation and Configuration	10/2009
-023	Added: RCCMD auf ESXi 4.0.x	10/2009
-024	Added: Silent Installation UNIX	11/2009
-025	Added: Console Installation UNIX	11/2009
-026	Added: Know How Pool	11/2009
-027	Added: Automatic Reset of the Redundancy Alarm	01/2010
-028	Added: Grafical RCCMD relay configuration UNIX/MAC	03/2010
-029	Added: Configuration on Windows 2008 Server Core x64	07/2010
-030	Added: RCCMD FAQ	08/2010
-031	Added: RCCMD on ESXi 4.1 with vMA 4.1	11/2010
-032	Added: RCCMD Tray Description	06/2011
-033	Added: Raritan Dominion PDU Configuration	09/2011
-034	Added: RCCMD on ESXi 5	10/2011
-035	Added: RCCMD WebInterface	04/2012
-036	Added: RCCMD with VMware vCenter	08/2012
-037	Added: RCCMD Email Settings	08/2013
-038	Added: RCCMD Installation with vCenter	08/2014
-039	Updated: New RCCMD WebInterface Design	09/2014
-040	Added: RCCMD on ESXi 6, vCenter 6, vMA 6	05/2015
-041	Cleaned up RCCMD and VMWare Section	06/2016

Inhalt

1 Introduction

RCCMD is a network client software, which enables receiving shutdowns or messages from UPS status senders like UPSMAN UPS Software, CS121/CS141 SNMP Adapters or any other kind of RCCMD capable network-cards and/or software of other licensed partners. RCCMD is the most successful multiple server shutdown and messaging tool in the entire UPS world.

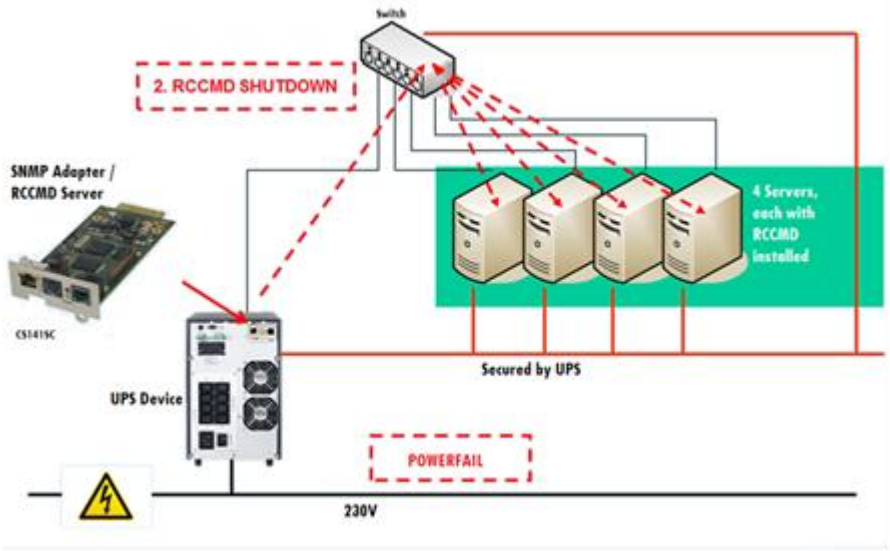


Fig. 1: Schema RCCMD

RCCMD is designed to execute a command on a remote system in a TCP/IP network. RCCMD works like the Remote Shell (RSH) known in the Unix environment. Inside the UPS-Management Software RCCMD is used to shutdown sev¬eral servers that are all powered by a single UPS. For this job, one of these computers is configured as UPS-master server.

2 Operation of RCCMD

RCCMD Client acts as a listener and will only trigger configured jobs when configured to do so. RCCMD has to be installed on every single client you want to shutdown in case of a certain event (eg. power fail). Note that you need a license for every client. Using the same license key in your environment will stop the RCCMD service on the affected clients. RCCMD comes with a webinterface you can access with every browser. This interface is password protected. After logging in, you can adjust the settings and behaviour of the client, examine the log files and start / stop the service. You can access the webinterface by entering the IP address of your client on port 8443.

2.1 Network Shutdown with RCCMD

The program RCCMD is designed to execute a command on a remote system in a TCP/IP network. RCCMD works like the Remote Shell (RSH) known in the Unix environment. Inside the UPS-Management Software RCCMD is used to shutdown sev-eral servers that are all powered by a single UPS. For this job, one of these computers is configured as UPS-master server.

Install the UPS-Management Software UPSMAN on your UPS server and connect it to the UPS. Alternatively, a SNMP adapter CS-111 or CS-121 can be used for this as well. The other servers are only connected to the UPS power supply, no RS-232 connection is necessary. On these remote systems, install RCCMD (copy the modules) and create a shutdown routine for every system. This shutdown routine may be a batch file, shell script or ncf-file, that contains the down and other commands for this system. After that, add RCCMD to the shutdown job or to the EVENT configuration of the computer running as UPS master server.

So now you have a computer in your server network supervising the UPS. The other servers execute RCCMD and wait for the RCCMD signal of the UPS server. If a power failure forces the master computer to shutdown the server-network, the shutdown-job of the UPS-server will start RCCMD. RCCMD now sends the RCCMD-signal to all computers in its list. The comput¬ers receive this signal and the installed RCCMD will execute the programmed command.

Please note that it is required to install RCCMD in two different operating ways:

1. **As a sending process on the UPS-server (RCCMD –s) (send)**
2. **As a receiving process (background-process) on the receiving computers (RCCMD –l) (listen)**

In contrast to the RSH, RCCMD does not include the command that is to be executed in the sending process, but instead deposits the command with the receiving process. This provides a security advantage in comparison to the RSH. Furthermore the receiving process may check, which computer sends the RCCMD-signal and determines whether to accept it or not.

Attention : If a name resolution is achieved via DNS, please always use the IP-address (and not the computer name) for a network shutdown with RCCMD. In case the DNS is not available, the network shutdown will not work, if this method is not used.

2.1.1 RCCMD Version 2 or higher

The extended Version of RCCMD is also able to execute commands on remote computers, execute the shutdown batch in the same TCP/IP port 6003, execute an e-mail batch, enable log file entries etc. The RCCMD 2 sender (UPSMAN or CS121/CS141 SNMP adapter) sends the corresponding RCCMD signal and the RCCMD 2 client starts the corresponding batch file, which lead to the execution of the net send message.

The initial command will always come from the UPSMAN or CS121/CS141 where as the execution will always be on the RCCMD client side.

Example: The CS121/CS141 should send a net send (network message) to a Windows NT network. The CS121/CS141 can be programmed so that during the event “Powerfail” a “RCCMD message” will be send. The text of the message is configurable by the user.

Upon on receiving the message by the RCCMD 2 client, the client is starting a batch file and sends the net send message. Sender of the message will be the client and initiator is the UPSMAN or CS121/CS141.

This way it is possible to send messages, e-mail etc. in the different networks and operating systems, initiated by an UPS alarm.

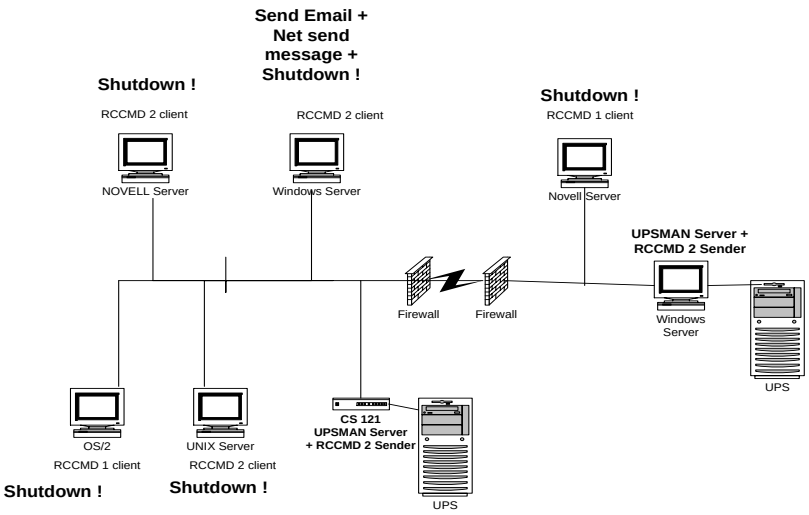


Fig. 2: RCCMD and UPSMAN in a network environment

3 Installation / Configuration of RCCMD for Windows

Note: The RCCMD Installer is using our delivered Java Runtime Environment version, which is used for the installation or rather uninstallation only. In addition the RCCMD Web Configurator is using a Java web-server (jetty). You can deactivate the RCCMD service RCCMDWebIf into the services administration and RCCMD is running without Java!

3.1 Installation of RCCMD

Prior of the start, please make sure that you have full administrator rights in order to complete the installation.

Put the CD into the CD-ROM drive of your computer or download the software into a specific directory.

Please execute the installation program installRCCMD.exe in order to copy the files to your system.

Menu **„Introduction“:**
In the next menue you can see the progress column where the next steps are visible.

Click the “**Next**” button to continue.

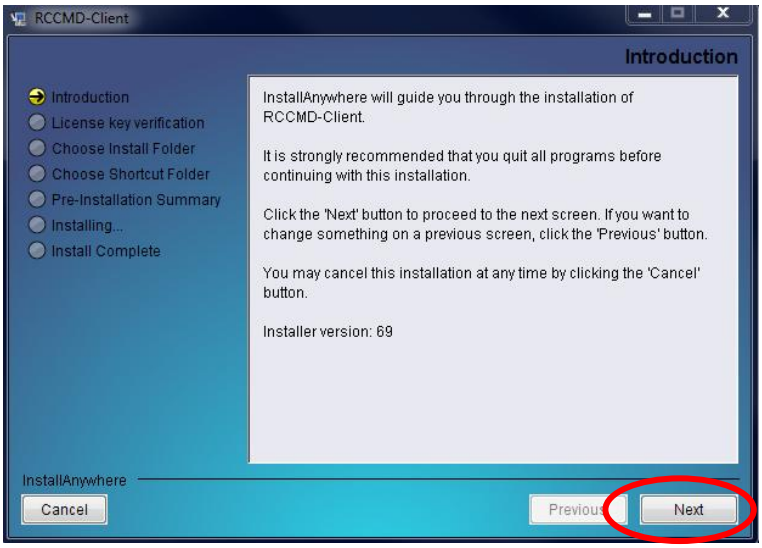


Fig. 3: Introduction

Please enter your **license key** an choose your corresponding Windows OS from the list. The used license determines, which module can be installed.

You need a special license key for your RCCMD software. You can identify the key with the “RX3” in the first part of the license key. Most of the times you need to order the key separately.

Click the “**Next**” button to continue.

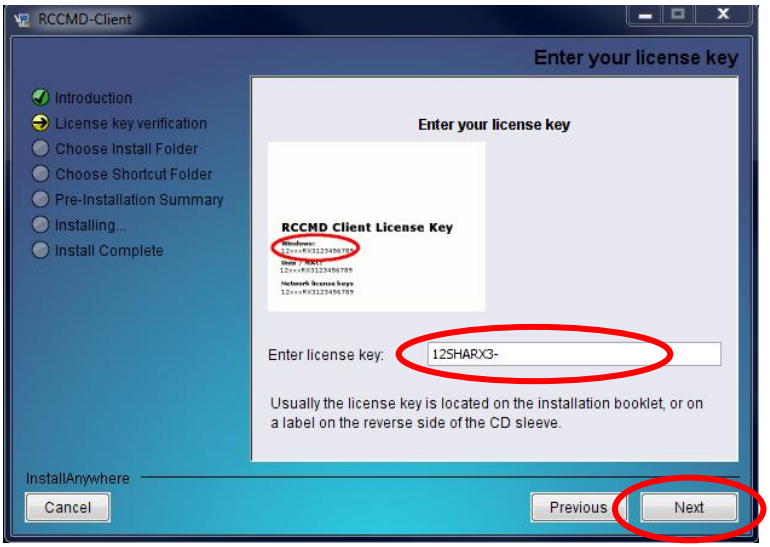


Fig. 4: License Key Entry

Attention: If you enter a wrong license number at this stage, the RCCMD client software will be set to a 30 day trial version. Please contact your UPS dealer for the full, correct license if it was not with the original CD-ROM.

Menu **„License Agreement“:**
Read and confirm the **license agreement**.

Click the “**Next**” button to continue.

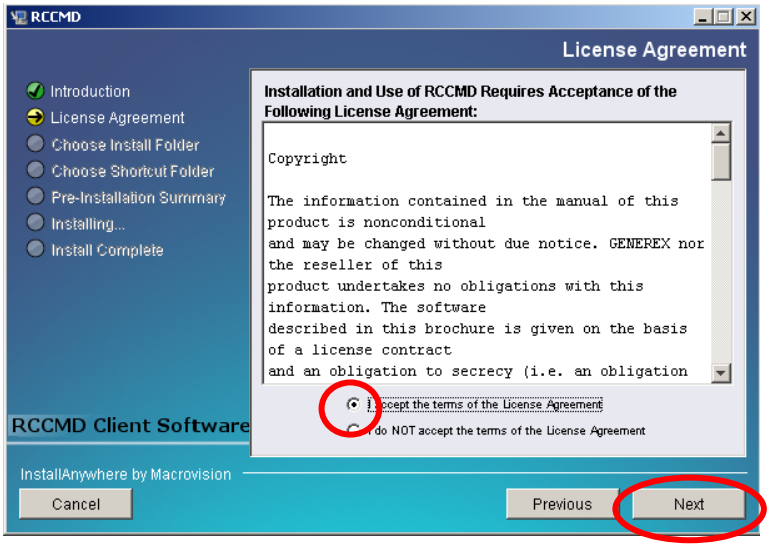


Fig. 5: License Agreement

Menu „ **Choose Install Folder**“:
Select the **features** you want to install.

Click the “**Next**” button to continue.

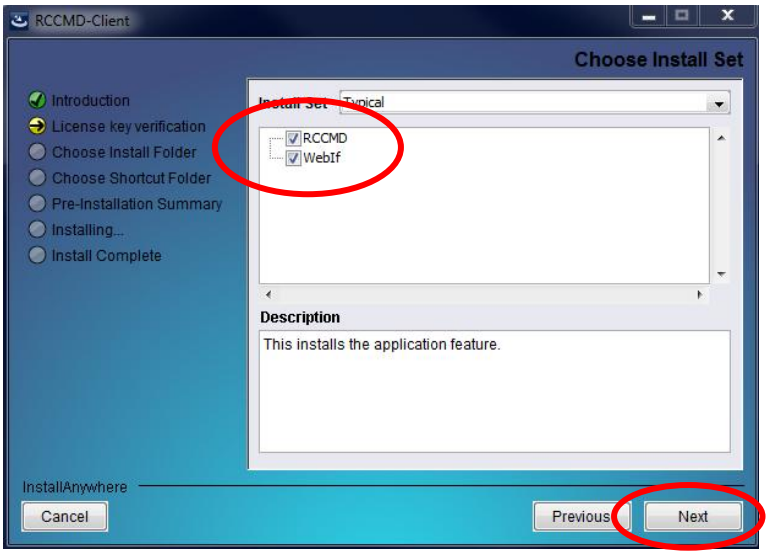


Fig. 6: Choose Install Set

In the next window enter the path where you want to install the software. Default is the subdirectory “RCCMD” into the program files folder onto the hard disk “C:”.

Click the “**Next**” button to continue.

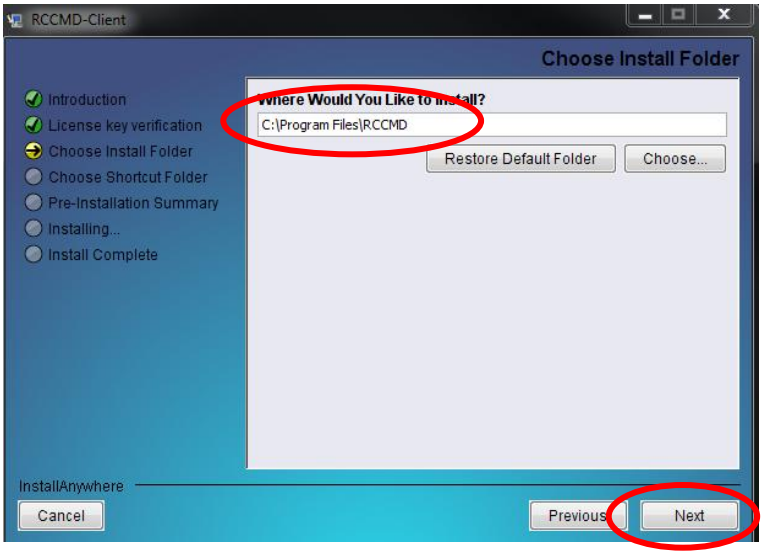


Fig. 7: Install Folder Selection

Attention: If you want to execute a program or a batch file with RCCMD, it is required that this program or batch file is located into the RCCMD installation folder \RCCMD (Not into “Program files\RCCMD like default) or a search path is set on the folder.

It will be signalized Into the next window, that **firewall exceptions** will be created for the RCCMD.exe (6003, 5769 TCP), the RCCMDTray.exe (971 TCP) and the RCCMD WebIf (8080 TCP).

Click the "**Next**" button to continue.

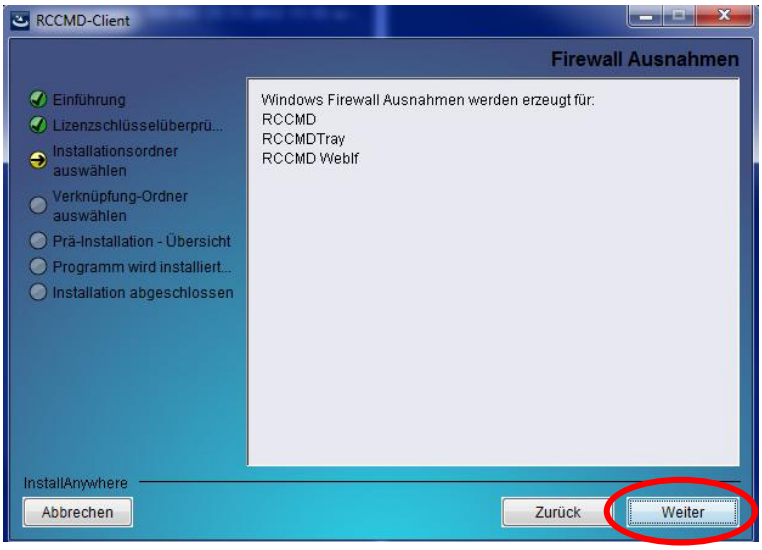


Fig. 8: Firewall Exceptions

The RCCMD tray provides the appearance of the RCCMD message box as pop-up into the foreground. If you do not want to receive messages from the RCCMD, please close the RCCMD tray via the context menu. To disable the RCCMD tray permanently, you can disable it into the RCCMD configuration.

The **RCCMD tray** appears into the taskbar.

The red point means, that the RCCMD service is not started or rather a problem has occured (powerfailure, communication lost). Green means, that the UPS status is okay.

Fig. 9: RCCMD Tray

Menu „**Choose Shortcut Folder**":
In next menu you can choose to create a new **program group** (default) or to choose icons elsewhere or not at all.

Click the "**Next**" button to continue.

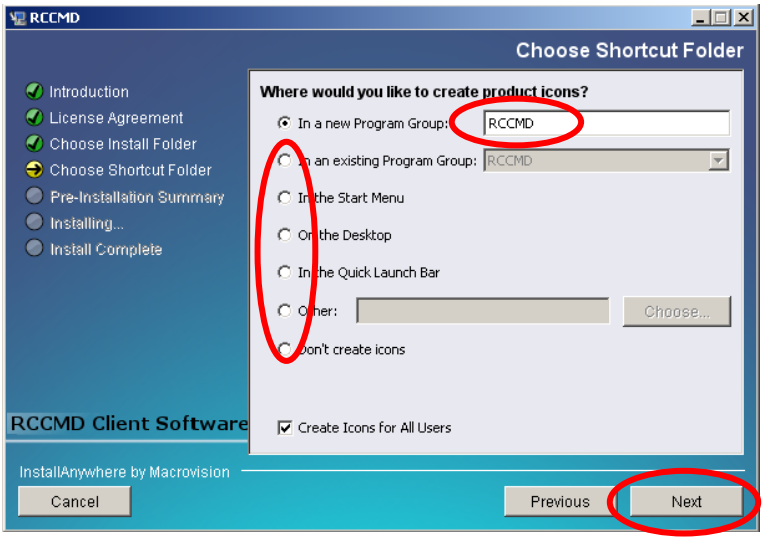


Fig. 10: Shortcut Folder Selection

Menu „**Pre-Installation Summary**“:
Please check your **selection**!

Click the “**Install**” button to beginn the installation.

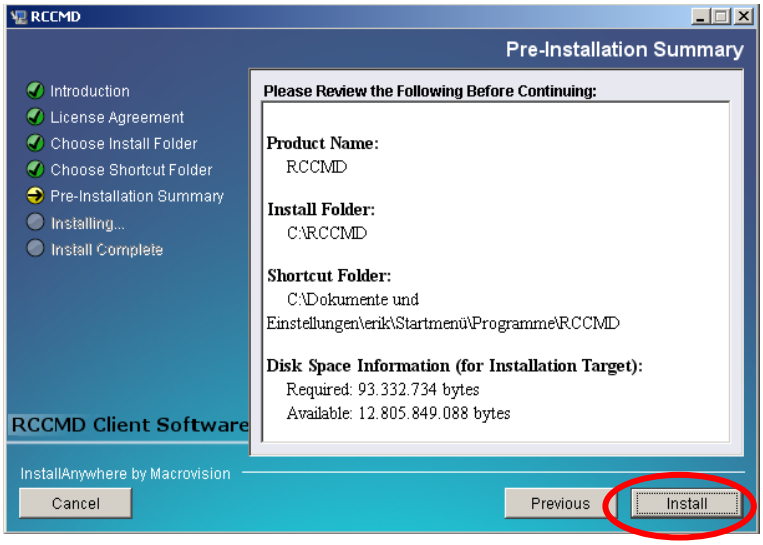


Fig. 11: Summary

Menu „**Installing…**“:
Select these default values for **port** and **protocol** for RCCMD WebIf or select new ones.

Click the “**Next**” button to continue.

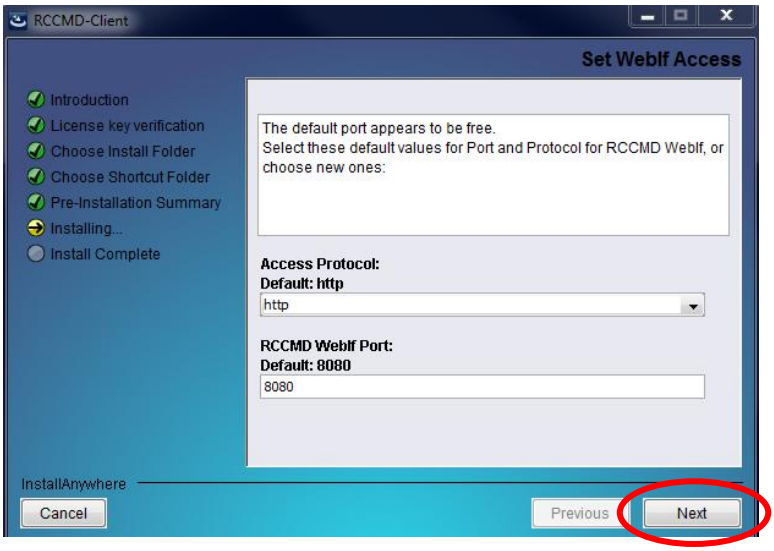


Fig. 12: Set WebIf Access

It is possible to use an own password for the RCCMD Web interface. Otherwise, the system uses the standard password „cs121-snmp“.

Click the “**Next**” button to continue.

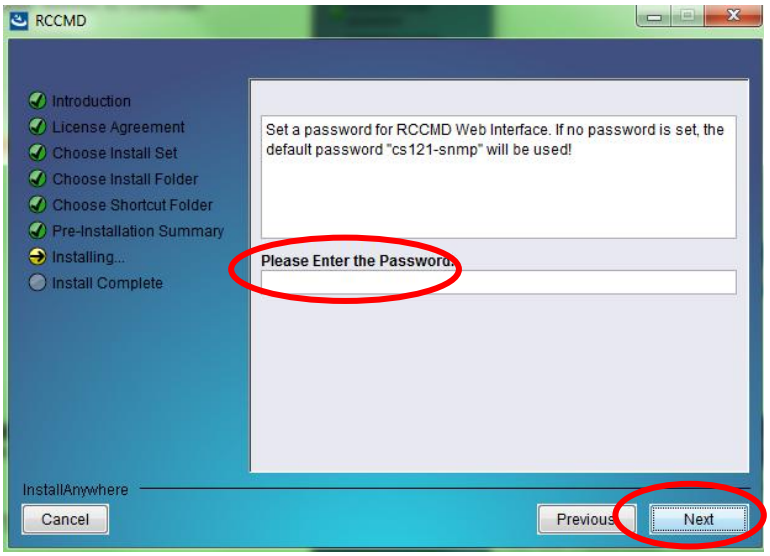


Fig. 13: Password entry

In the next you can create an own password hint!

Click the “**Next**” button to continue.

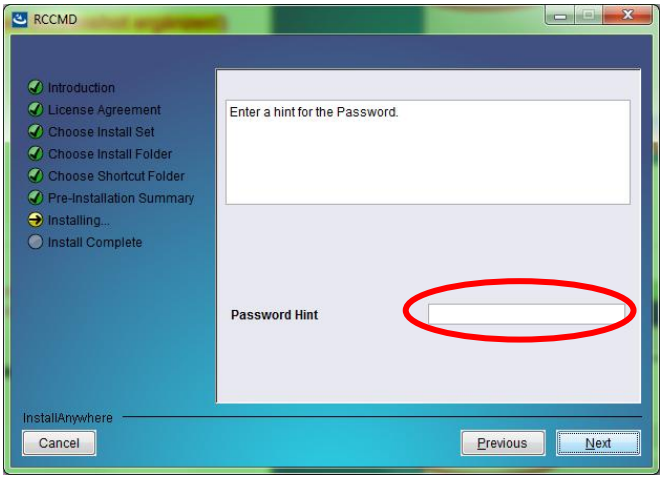


Fig. 14: Password hint entry

Menu „**Install Complete**“:
RCCMD has been installed successful.

Click the “**Done**” button to finish the installation.

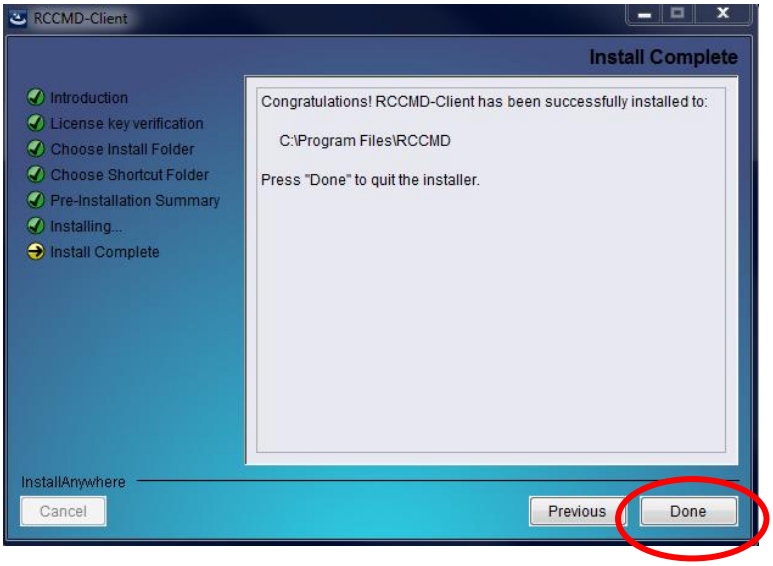


Fig. 15: Install Complete

3.1.1 Silent Installation of the RCCMD Installation

The RCCMD Software provides a silent installation, but it is required to enter some settings into the “Installer.Properties” file. This file is located into the CD folder \Rccmd\Windows\12.

Usage:
#
To record a new response file start the installer from command line
with parameter '-r'.
Use the new Values for the provided Variables from this file.
#
To perform a silent install, start the installer on the commandline.
The installer also needs the parameters '-f <path/to/resonsefile>'.
Choose Install Folder

Uncomment this variable to set a new default Folder into which the program will be installed.

```
## The example represents the default, that will be used, if no folder is provided.
## According to the example backslash characters ('\') need to be escaped by a backslash.
## Spaces in the path also require a backslash as an escape character.
## USER_INSTALL_DIR=C:\\RCCMD
# Choose Link Location
# --------------------
## You can tell the installer in which folder the shortcuts should be installed.
## The absolute path must be given.
## options are: "Do Not Install" if you do not want any shortcuts,
##  or a path to the folder in which the shortcuts should be created.
## Here are two examples:
## USER_SHORTCUTS=Do Not Install
## USER_SHORTCUTS=C:\\Dokumente und Einstellungen\\<Windows User>\\Startmenü\\Programme\\UPS
## Choose Feature List
## -------------------
## If you want to install a subset of features from this installer,
##  make a list of all the features you want to be installed.
## The List must be entered in the CHOSEN_INSTALL_FEATURE_LIST variable.
## Options for the list are: RCCMD, WebIf
## CHOSEN_INSTALL_FEATURE_LIST=RCCMD,WebIf
## Choose OEM
## ----------
## Enter your OEM number here.
## OEM=0
## Choose locatization
## -------------------
## If you want to install a different language than English
## you will want to provide the valid country code here
## This is only important for silent installations.
## Valid codes are: zh_cn, de, en, fr, el, it, ja, ko, pt, ru, es, tr
## INST_LANG=de

## Choose License Key
## ------------------
## For silent installation your License Key must
## be provided here.
## GXLICENSEKEY=yournumber
## Choose Installer User Interface
## -------------------------------
## For installation in console modus, pass the parameter: "-i console" to
## the installer.
## If you want to use the installer in silent mode with no user interaction,
## you can set this variable to "silent".
## Default is "gui".
## INSTALLER_UI=silent
#INSTALLER_UI=gui
## WebIf Settings
## --------------
```

Here you can override default settings for access to the RCCMD WebIf.
These settings are ignored, if the variable CHOSEN_INSTALL_FEATURE_LIST
is set and does not contain the WebIf feature.
In interactive install modes (gui, console) the installer will check, whether
the chosen port is free to be used.
Valid values are: 1-65535
WEBIF_PORT=8080
Valid protocols are: http, https
WEBIF_PROTOCOL=http

Fig. 16: Content of the “installer.properties”

It is required to remove the hash mark prior of the variable INSTALLER_UI=silent. In addition the setting of the license key is required behind the variable GXLICENSEKEY=.

If you don’t want to install RCCMD not in the default directory `C:\Program Files\RCCMD`, please note that backslashes and blankets need another backslash, for example:

```
USER_INSTALL_DIR=C:\\program\ files\\RCCMD
```

The language can be set with the variable INST_LANG=en, so all tooltips are in your desired language when configuring RCCMD.

3.1.2 RCCMD Silent Installation and Takeover of own Configuration

After you have finished the edition of the “installer.properties” file, it is possible to create an own RCCMD configuration and to “silent” install.Thereto it is required to execute the RCCMD configuration manually once. Then export this configuration out of the registry into a file as follows:

- Click the right mouse button on “Parameters” into the directory HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\rccmd, select “Export” and save the file with the name “rccmd.reg” as “WIN95/NT4 Registration File”.
- Store the file “rccmd.reg” into the directory, where the RCCMD-Installer packet is located.
- Open the file “rccmd.reg” with an editor and delete the complete line, which contains the license key.
- Create a new Windows batch-file (*.bat) with an editor, e. g. with the name “InstalAndConfigRCCMD.bat”, which should look like as follows:
-

```
@echo off
cls
echo *** Installation of RCCMD, please wait... ***
installRCCMD.exe
echo *** Importing RCCMD configuration file ***
regedit.exe -s rccmd.reg
echo Ready
```

Fig. 17: Windows-Batch-Datei

Now you can start a combined RCCMD silent installation and configuration via executing of your Windows batch-file “InstallAndConfigRCCMD.bat”.

Click “**Install**” to continue.

3.2 Console Installation of RCCMD Installation

This console installation works interactive and will ask for user input, defined in the installation script file “installer.properties” (see above).

Note: This concerns the installation only. The configuration will be performed via editor into the „rccmd.cfg“ file.

For the activation of the console installation, it is required to remove the hash mark prior of the variable INSTALLER_UI= and to enter console. This is the interactive RCCMD installation onto the console. Execute the “**installRCCMD.exe**” file.

By the configuration you can change the language, to receive the right Tooltips! Please use the variable INST_LANG=de .

3.2.1 Example of a Console Installation

Adjust the file “installer.properties” accordingly like described above or execute the following command:

```
installRCCMD.exe –i console
```

Select the desired **language** and note the introduction.

Confirm with ENTER

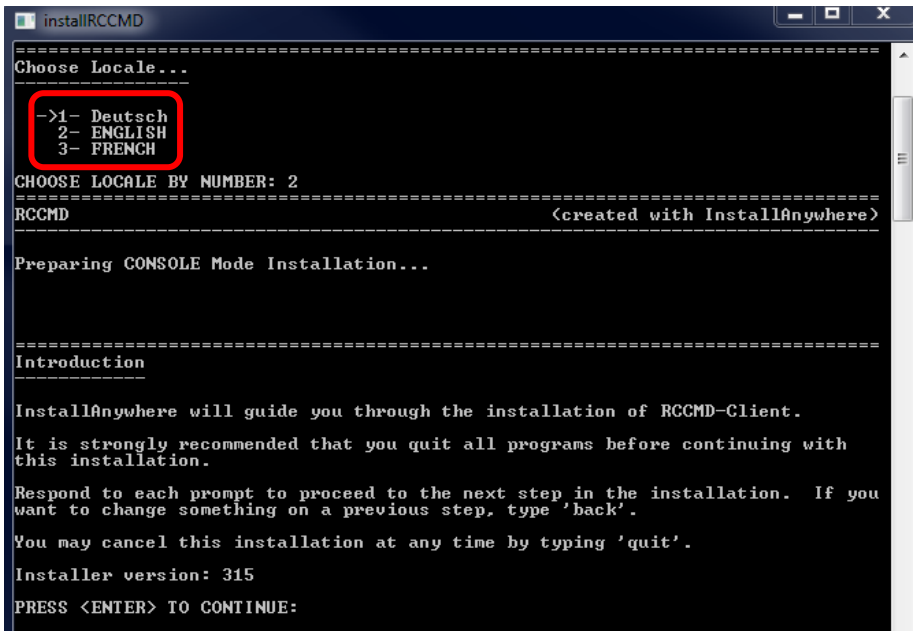


Fig. 18: RCCMD Console Installation – Language Selection, Introduction

Enter your **license key** and note **the license agreement**.

Confirm with „ENTER“

```
================================================================================
Enter your license key
----------------------

Enter your license key
Usually the license key is located on the installation booklet, or on a label
on the reverse side of the CD sleeve.
Enter license key: 12SHARX3-23456789
Test version - Only meant for testing purposes, key only valid for 30 days.
Would you like to enter a different license key? (Yes/No): No


================================================================================
License Agreement
-----------------

Installation and Use of RCCMD Requires Acceptance of the Following License
Agreement:


Copyright

The information contained in the manual of this product is nonconditional
and may be changed without due notice. GENEREX nor the reseller of this
product undertakes no obligations with this information. The software
described in this brochure is given on the basis of a license contract
and an obligation to secrecy (i.e. an obligation not to further publicise
the software material). The purchaser may make a single copy of the software
material for backup purposes. No parts of this manual may be transfered to
third persons, either electronically or mechanically, or by photocopies
or similar means, without the express written permisson of the GENEREX
or the royalty holder.

The UPSMAN management software includes for every serialnumber the licence for
using the UPS service at one server with one UPS. The
UPSMON/JAVAMON/Webinterface
is freeware and may be copied and used from an unlimited numbers of connected
workstations.

The RCCMD client software requires a separate license key for every
installation.
Unless a RCCMD enterprise license is available, the user must NOT install

PRESS <ENTER> TO CONTINUE:
```

Fig. 19: RCCMD Console Installation – License Key, License Agreement

Select the desired **product features**, enter an **install folder** and note the **firewall exceptions**.

Confirm with „ENTER“

```
================================================================================
Choose Install Set
------------------




================================================================================
Choose Product Features
-----------------------

ENTER A COMMA_SEPARATED LIST OF NUMBERS REPRESENTING THE FEATURES YOU WOULD
LIKE TO SELECT, OR DESELECT. TO VIEW A FEATURE'S DESCRIPTION, ENTER
'?<NUMBER>'.  PRESS <RETURN> WHEN YOU ARE DONE:

  1- [X] RCCMD
  2- [X] WebIf

Please choose the Features to be installed by this installer.:


================================================================================
Choose Install Folder
---------------------

Where would you like to install?

  Default Install Folder: C:\Program Files\RCCMD

ENTER AN ABSOLUTE PATH, OR PRESS <ENTER> TO ACCEPT THE DEFAULT
      :



================================================================================
Firewall Exceptions
-------------------

Firewall Exceptions will be added for:
RCCMD
RCCMDTray
RCCMDWebIf

PRESS <ENTER> TO CONTINUE:
```

Fig. 20: RCCMD Console Installation – Produkt Auswahl, Pfad, Firewall Ausnahmen

Select a **link location** and note the **pre-installation summary**.

Confirm with „ENTER“

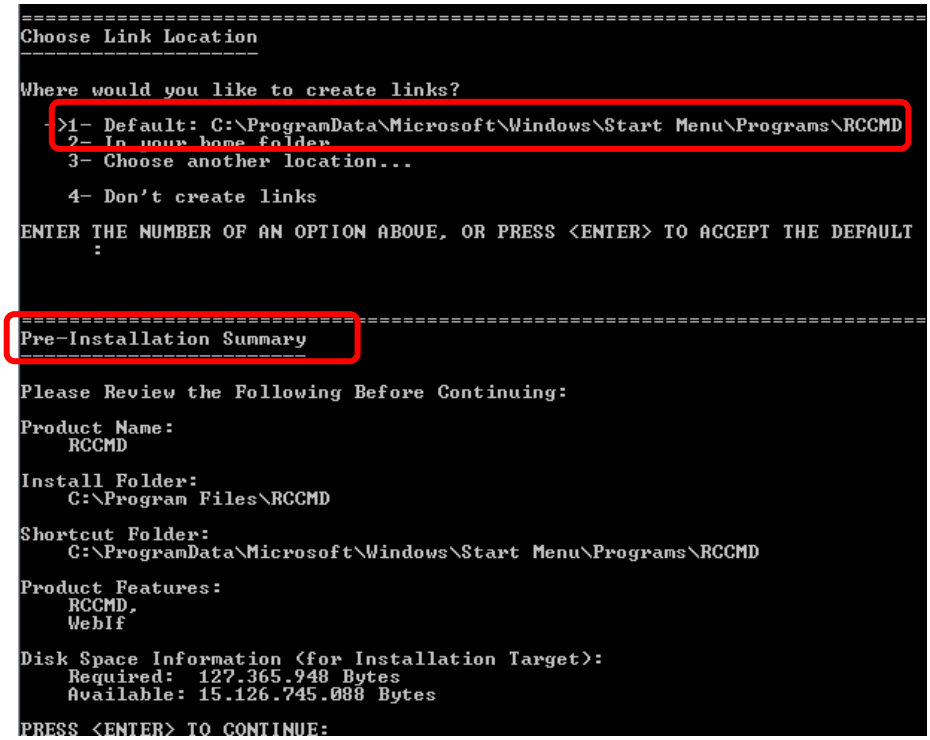


Fig. 21: RCCMD Console Installation – Link Location, Pre-Installation Summary

Set the WebIf **port** and the **protocol** and RCCMD has been installed successful.

Press „ENTER“ to exit the Installation.

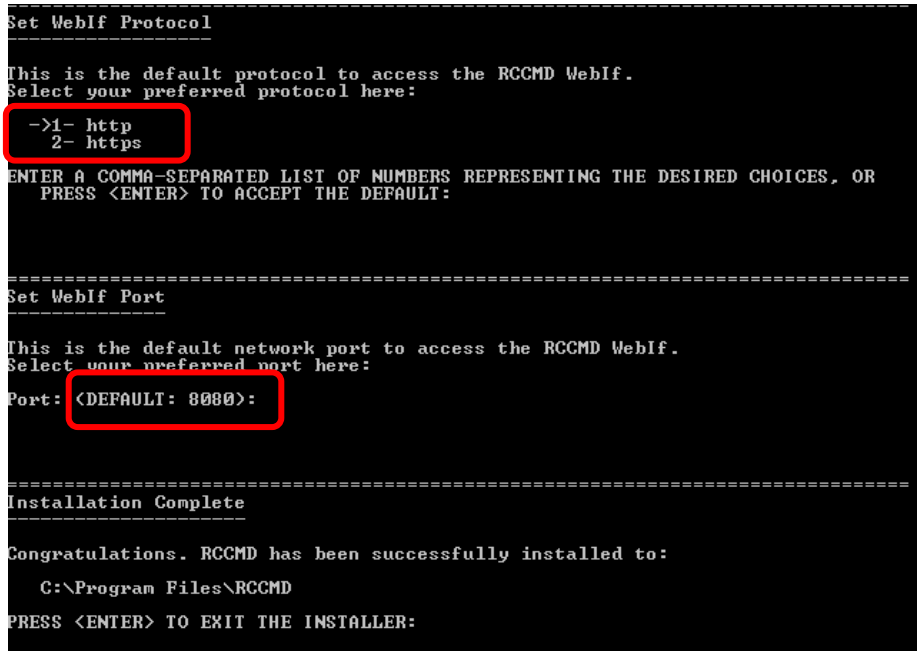


Fig. 22: RCCMD Console Installation – Set WebIf Protocol, Port

3.3 RCCMD WebInterface (from version 4.0.1.9)

RCCMD provides its own web-interface from version 4.0.1.9 or higher. Therefore it is possible to configure and control RCCMD remotely. After the successful installation, your default web-browser of your OS starts automatically.

Attention: Use the access data User: "admin" Password: "cs121-snmp"

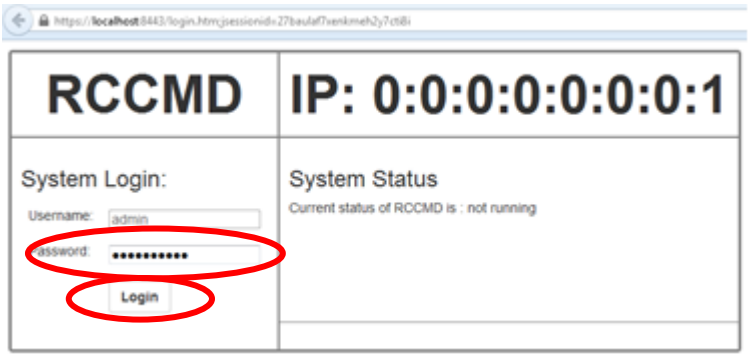


Fig. 23: RCCMD Configurator

Click the "Login" button.

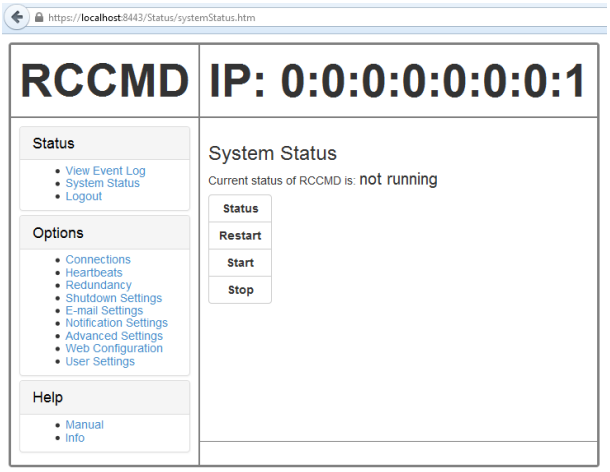


Fig. 24: RCCMD Configurator

Menu **„Connections":**
You can enter the **IP addresses** of the allowed RCCMD senders (CS121/141/UPSMAN) into the **"Connections"** menu. Click the "**Insert Sender**" button to enter the IP address of the 1st ender. Click the "**Remove Sender**" button, if you want to remove the already entered IP address. Click the "**Edit Sender**" button, if you want to edit the entered IP address.

Attention: If you do not enter an address, then every server has the permission to send a shutdown command.

You can define under **"Protocol"**, if RCCMD should use SSL certificates. Enable the "**Reject expired SSL certificates**", if you want to reject connections with expired certificates. Please take a look into chapter 3.9 for further information about RCCMD **with SSL.**

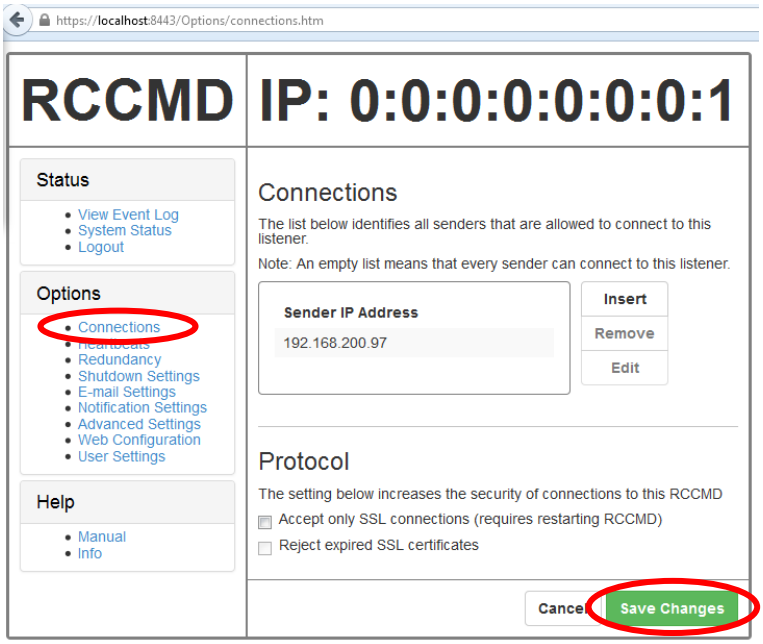


Fig. 25: RCCMD WebInterface Configurator – Connections

Click the "**Save Changes**" button prior of the leaving of this site to save your changes.

Menu **„Heartbeats“:**

You can enable the “UPSMAN Alive Check” feature into the menu “Heartbeats”. This check is a signal, that will be send to the CS121/CS141/UPSMAN via port 5769, if the UPSMAN service still got UPS data. If not, the script file “alive.bat” will be executed, which will trigger an accordant pop-up message.

The feature “**by the use of CS121/UPSMAN Traps**” provides UPSMAN/RCCMD/UNMS messages, which will display the UPS status as message. If enabled, this feature will trigger a message, if the UPS status of the UPSMAN/RCCMD servers has changed.

The feature “**by polling CS121/UPSMAN every x seconds**” provides the pure signal polling without receiving UPS data or rather messages.

The polling rate (default 1800 seconds) defines the polling of the UPSMAN service, connection retries (default 100) means after 100 unsuccessful connection tries an alarm will be triggered.

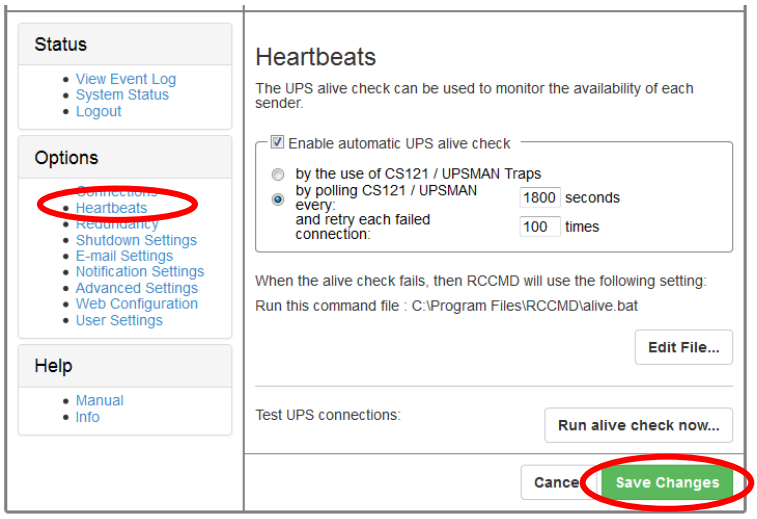


Fig. 26: RCCMD WebInterface Configurator – Heartbeats

Die You can test the UPS connection, if you click the “**Run alive check now…**” button (the port 5769 will be tested).

Click the “**Save Changes**” button prior of the leaving of this site to save your changes.

Menu „**Redundancy**“:

You can enable the redundancy management feature into the menu **“Redundancy”**. The **redundancy level** defines the number of redundant senders in the redundancy group. This means, that level 1+ senders must have sent a shutdown signal before this RCCMD starts its shutdown sequence.

When redundancy suppresses a shutdown, then RCCMD will trigger the “suppressed.bat”. You can edit this file, if you click the “**Edit file…”** button.

Please note, that it is required to configure a reset of the redundancy alarm on the sender (CS121/CS141/UPSMAN). You can use the function „**Send RCCMD cancel shutdown**“, to discard a previously sent shutdown automatically. If a shutdown was suppressed, because of the existing redundancy at this point of time, but the problem was solved at the UPS intermediate, you can reset the shutdown with the function „Send RCCMD cancel shutdown“. The client, which received the shutdown, will be encouraged to reset it.

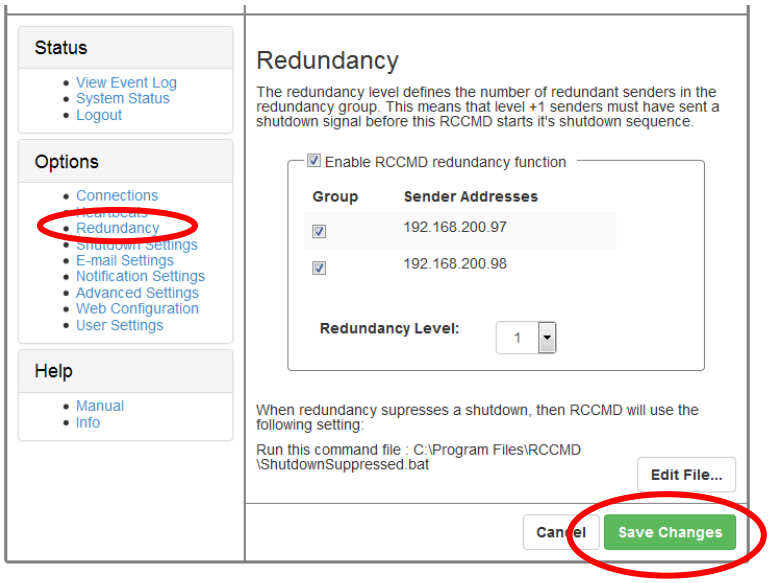


Fig. 27: RCCMD WebInterface Configurator – Redundancy

Please take a look into chapter 3.4 or rather 3.4.1 for further information about RCCMD with redundancy.

Click the “**Save Changes**” button prior of the leaving of this site to save your changes.

Menu **„Shutdown Settings“:**
You can change or rather extend the shutdown sequence into the “Shutdown Settings” menu.

If you want to execute a powershell script, you can edit or add desired scripts here. If you want to edit the shutdown.bat, mark “Shut down System”, click the “Edit Command” button and the “Save Changes” button. Please note to restart RCCMD.

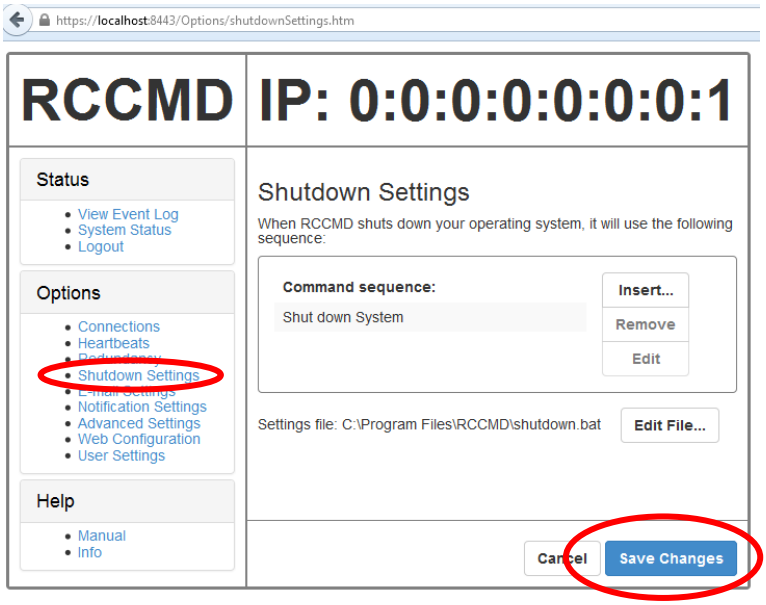


Fig. 28: RCCMD WebInterface Configurator – Shutdown Setting

The shutdown.bat will be executed by default:

rem created by setup

@echo off

set path=%path%;C:\Program Files\RCCMD

ExitWin.exe shutdown force

@cls

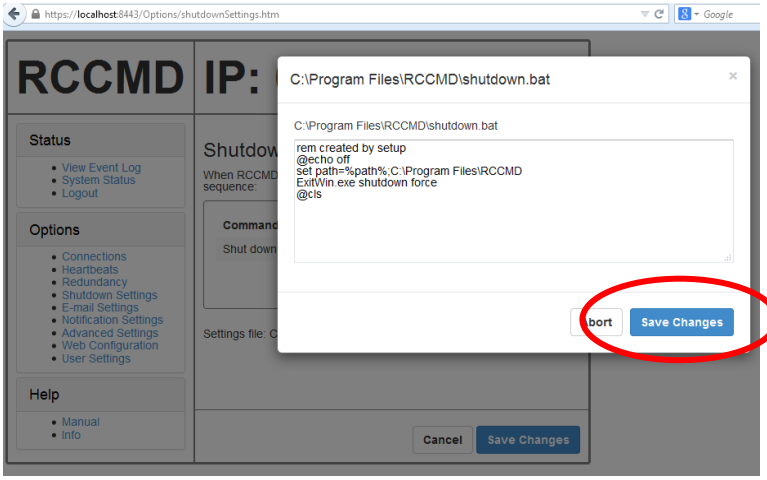


Fig. 29: RCCMD WebInterface Configurator – Shutdown Settings – Edit File

The following commands are available for the shutdown sequence configuration:

Attention: The shutdown sequence will be executed from top to down. The “Shutdown Windows” command should be at the bottom, because after the execution of the shutdown, no other commands will be executed.

Shut down System:	Ends your session and shuts down Windows, so that you can safely turn off the power.
Log Off from System:	Ends your session, leaving the workstation on full power.
Power off System:	Ends your session, shuts down Windows and turns off the power.
Restart System:	Ends your session, shuts down Windows and restarts Windows.
Hibernate System:	Hibernates your session, the content of the RAM will be written on hard disk.
Suspend System:	Suspends your session, the content of the RAM will NOT be written on hard disk.
Quit Lotus Notes:	Closes Lotus Notes prior of the shutdown of Windows. Please configure a “Wait” delay after this command.
Quit Siemens SIMATIC:	Closes WIN CC Database prior of the shutdown of Windows. Please configure a “Wait” delay after this command.
Quit Windows Applications:	Closes all applications prior of the shutdown of Windows.
Wait some seconds:	Waits a duration in seconds until the next command will be executed.
RCCMD shut down relay:	Relays RCCMD shutdown command to another workstation. Enter the IP address or the hostname of the remote station you want to shutdown.

Click the “**Save Changes**” button prior of the leaving of this site to save your changes.

Menu “**E-mail Settings**”:
You can define the email settings of the sender in the menu “E-mail Settings”. In addition you can enable the **encryption** or rather enter another **SMTP port**.

Click “**Save Changes**” prior leaving this site to save your changes.

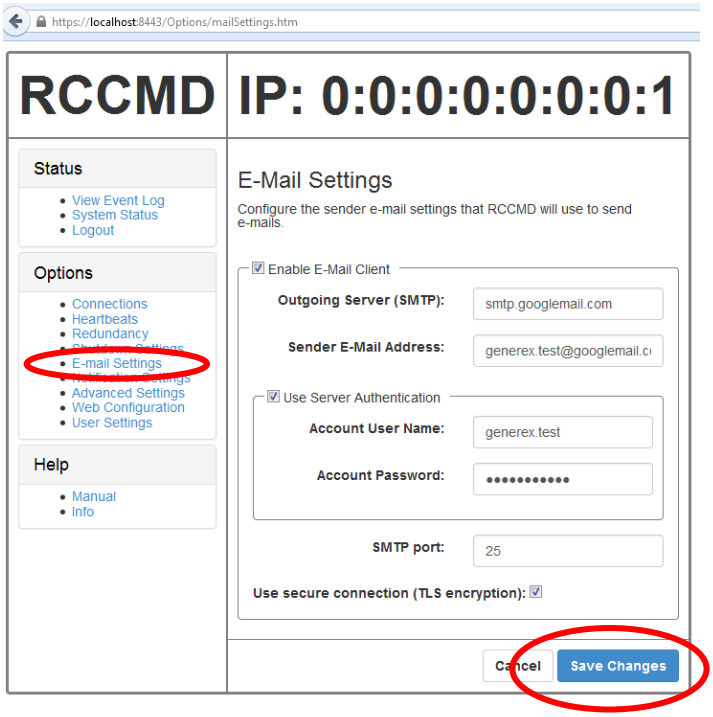


Fig. 30: RCCMD WebInterface Configurator – E-mail Settings

Menu „**Notification Settings**“:
You can change or rather extend the default **bat files for E-Mail**, Message and Execute, if you click the “Edit File…” button.

Click the “**Save Changes**” button prior of the leaving of this site to save your changes.

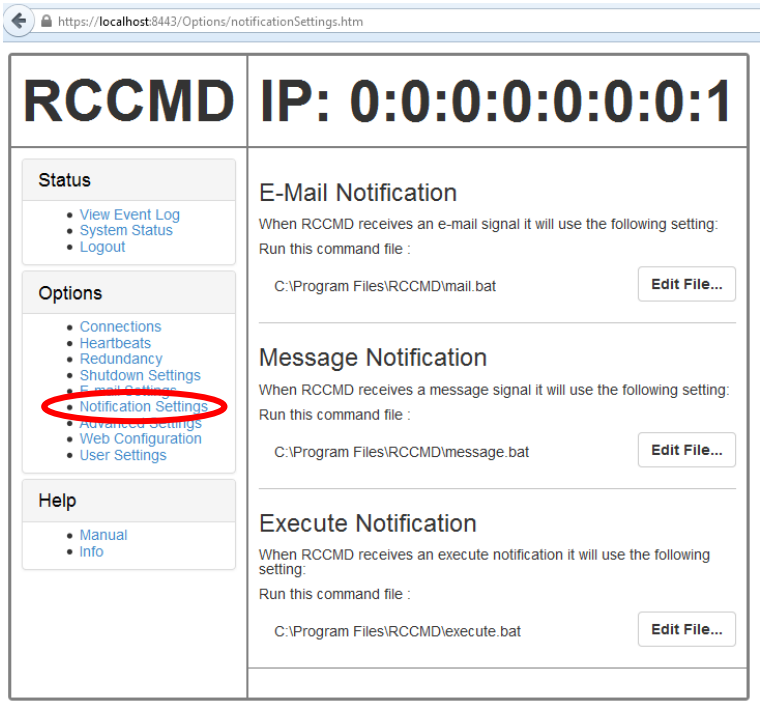


Fig. 31: RCCMD WebInterface Configurator – Notification Settings

Menu „**Advanced Settings**“:
You can define the **maximum size of the event logfile** into the menu “Advanced Settings”, where the overwriting of older entries will start, the **RCCMD bindings** for the IP address, the RCCMD listener TCP port and the RCCMD Tray Message Port, which will be used for the RCCMD messages.

In addition you can enable the “**Start Jobs as interactive user**” feature, that means, if disabled, that RCCMD will execute jobs only, if somebody is logged in on the system and the RCCMD Tray is active!

Attention: The shutdown job would not be executed too, if nobody is logged in! If this feature is enabled, assure that somebody is logged in at anytime!

Click the “**Save Changes**” button prior of the leaving of this site to save your changes.

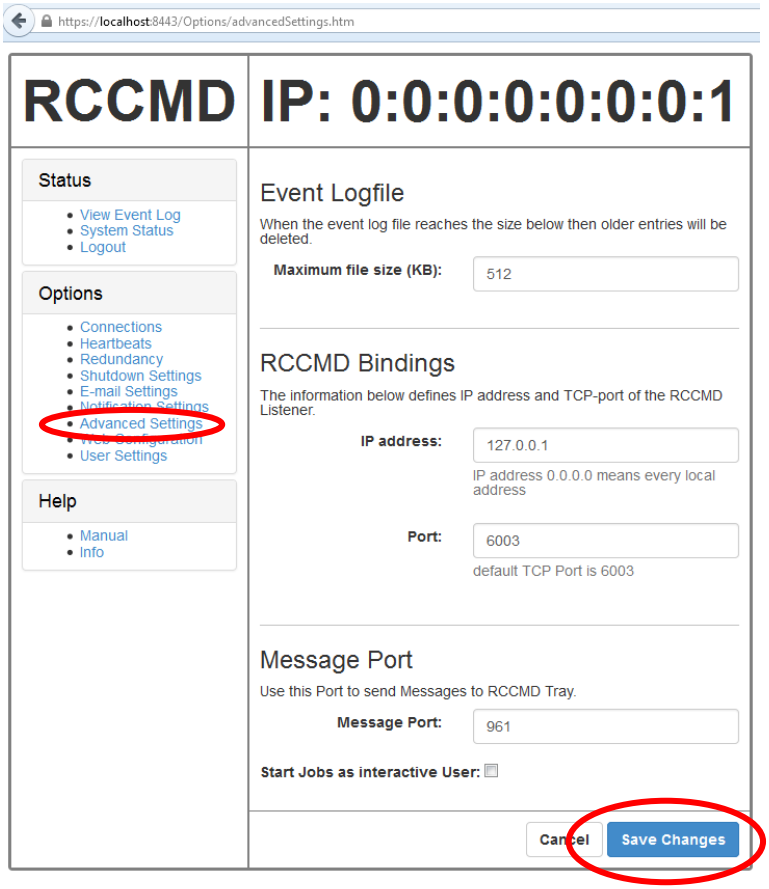


Fig. 32: RCCMD WebInterface Configurator – Advanced Settings

Menu „**Web Configuration**“:
You can change the default password for the user “admin” into the menu “Web Configuration”. In addition you can disable the **HTTPS protocol**, if you just want to use the HTTP protocol.

The RCCMD version 4.0.2.1 or higher provides the feature of changing the default ports for HTTP and HTTPS.

Click the “**Save Changes**” button prior of the leaving of this site to save your changes.

Afterwards you have to restart the RCCMD service!

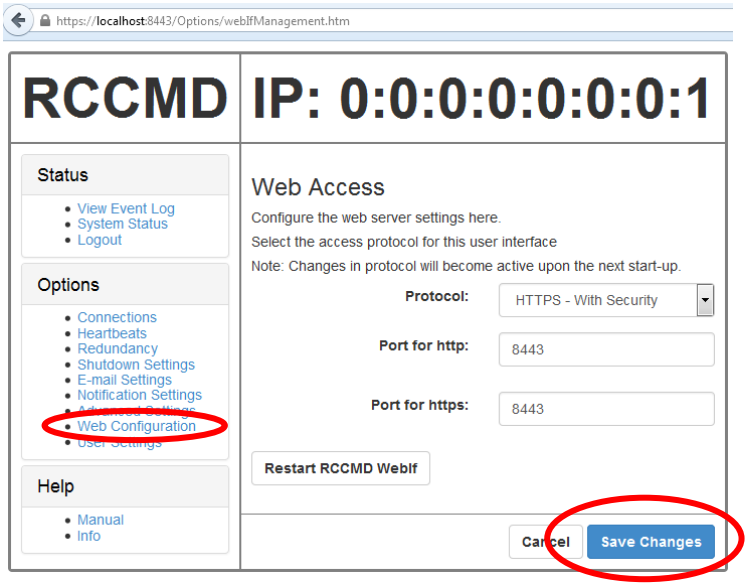


Fig. 33: RCCMD WebInterface Configurator – Web Configuration

User Settings menu
Here you can change the default password for admin.

Afterwards you have to restart the RCCMD service!

Click the “Save Changes” button prior of the leaving of this site to save your changes.

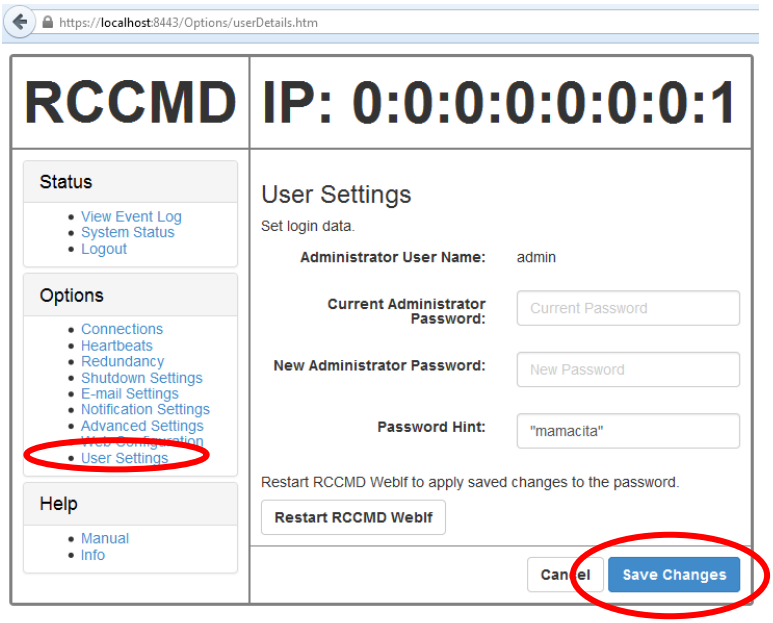


Fig. 34: RCCMD WebInterface Configurator – User Settings

Menu „**Status, View Event Log**“:
You can see the **logging of the events** into the menu “Status, Event Log”.

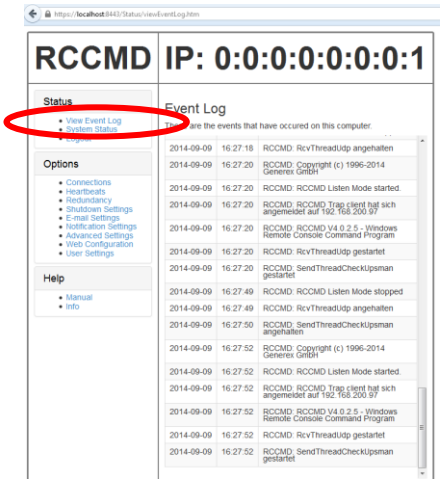


Fig. 35: RCCMD WebInterface Configurator – View Event Log

Menu „**System Status“:**
You can check the current status of RCCMD into the menu “Status, System Status”, update the status and restart or rather stop/start the RCCMD service.

„Logout“
You can logout here when you finished configuration.

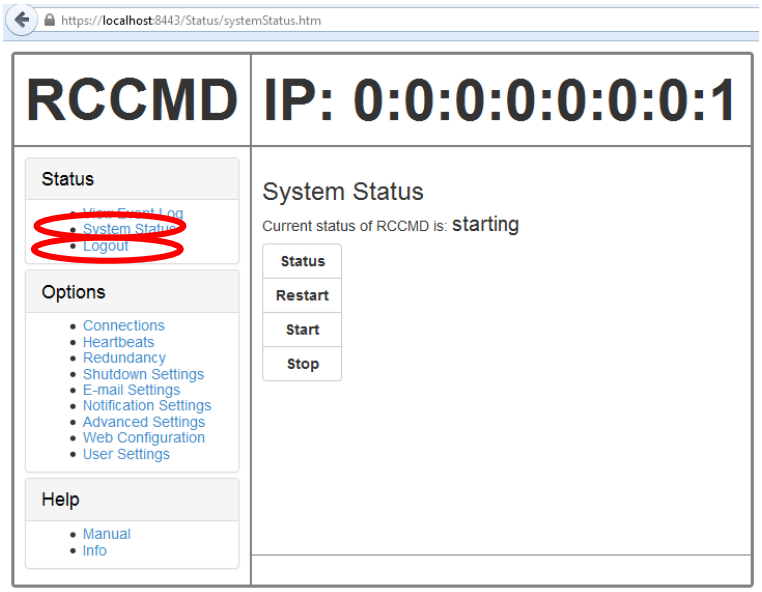


Fig. 36: RCCMD WebInterface Configurator – System Status

Menu „**Help**“:
You can open the **RCCMD user manual** into the menu “Help” ad you can follow the link to www.generex.de.

With „Info“ you can view the installer version.

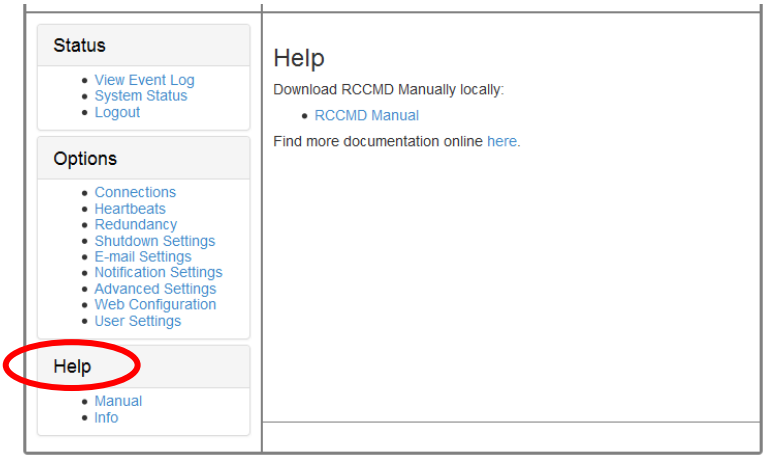


Fig. 37: RCCMD WebInterface Configurator – Help

3.3.1 RCCMD WebInterface Remote Access

RCCMD provides its own web-interface from version 4.0.1.9 or higher. Therefore it is possible to configure and control RCCMD remotely. Please note, that the firewall port 8443 TCP is enabled. Enter the following into a web-browser, to connect to a workstation, where RCCMD is running:

https://IP address of the RCCMD client: 8443

Nun besteht die Möglichkeit, die Konfiguration bzw. Steuerung aus der Ferne auszuführen.

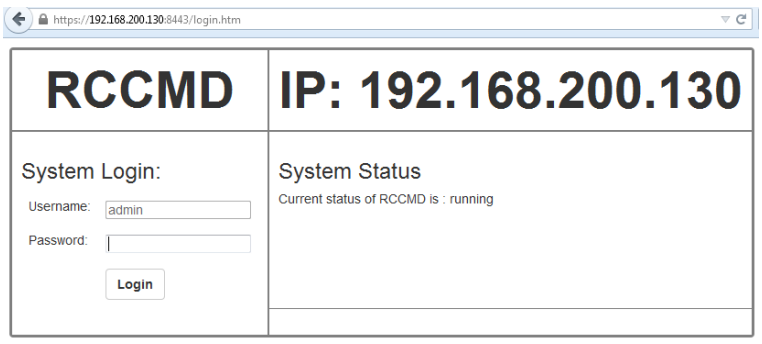


Fig. 38: RCCMD WebInterface Configurator – Remote Access

3.4 RCCMD Client as Relay Station

In order to reach a bigger number of RCCMD receivers, one RCCMD client needs to be operated as relay station. The receiver will be configured so that it will receive a RCCMD signal and this signal will be used to start a batch file, which then starts even more RCCMD sender signals. This workstation is then sender and receiver at the same time and is therefore an important link in the UPS monitoring chain. Generally the usage of a RCCMD client as a relay station makes the management of several 100 RCCMD clients far easier than configuring this via the Web-interface of the CS121/CS141. Additionally, all Web-browser event configurations have a certain limitation so that it is required to use the relay function, if the number of jobs exceed 50 per event at the CS121 HW 131, at older CS121 adapters even earlier.

See the following script, which lets the RCCMD-client act as relay station:

```
rem created by setup
@echo off
set path=%path%;C:\Program Files\RCCMD
# RELAY RCCMD
# This batch will send RCCMD shutdowns to the IP addresses listed below
# At the end of the batch this computer will initiate the local shutdown
start rccmd -s -a 192.168.200.2
start rccmd -s -a 192.168.200.3
start rccmd -s -a 192.168.200.4
start rccmd -s -a 192.168.200.5
start rccmd -s -a 192.168.200.6
start rccmd -s -a 192.168.200.7
# to be continued
#
# local shutdown
ExitWin.exe shutdown force
@cls
```

Fig. 39: Example: Batch File RCCMD act as Relay Station

“start” is a Windows batch command to start the program call in several instances. This allows to execute programs simoultanously and speeds up the shutdown process. Please note that “start” is not supported in all Windows versions and it should be tested before using.

3.5 Automatic Reset of the Redundancy Alarm

You can use the function „**Send RCCMD cancel shutdown**“, to discard a previously sent shutdown automatically. If a shutdown was suppressed, because of the existing redundancy at this point of time, but the problem was solved at the UPS intermediate, you can reset the shutdown with the function „**Send RCCMD cancel shutdown**“. The client, which received the shutdown, will be encouraged to reset it.

This command can be set individually into your CS121/CS141, UPSMAN or BACS WEBMANAGER Events/Alarms configuration, but makes sense only, if the event, which will send the command, is true, if the UPS is back in normal condition. For this the events „**POWER RESTORED**“, „**BATTERY LOW OFF**“, „**UPSMAN STARTED**“ and „**GENERAL ALARM OFF**“ are suitable, if they are provided from your UPS into the CS121/CS141. The job „Send RCCMD cancel shutdown“ would be set into these all-clear events, so that e. g. at restart of the UPS, the event „UPSMAN STARTED“ would reset the accordant RCCMD client automatically.

Alternative: Should the job „**Send RCCMD cancel shutdown**“ not be present into your CS121/CS141, UPSMAN or BACS WEBMANAGER, you can use the job „**Send RCCMD shutdown to remote client**“ or rather „**Send RCCMD execute to remote client**“ alternatively.

The parameter „**WAKEUP**“ got the same function like the „Send RCCMD cancel shutdown“ and resets the redundancy alarm of a RCCMD Client into initial state. For this the events „**POWER RESTORED**“, „**BATTERY LOW OFF**“, „**UPSMAN STARTED**“ and „**GENERAL ALARM OFF**“ are suitable too, to configure the function „**Send RCCMD command to remote client“** with the „**WAKEUP**“ command.

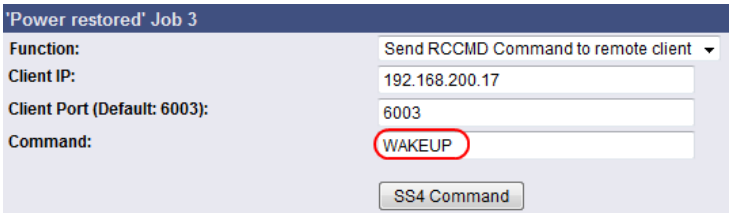


Fig. 40: CS121/CS141 Configuration “WAKEUP” Command

Menu „**CS121/CS141“**:
Click into the CS121/CS141 menu “**Events/Alarms**” onto “**Power restored**” and add a new job. Select the function “**Send RCCMD command to remote client**”, set the accordant **IP address** of the RCCMD client and enter the command “**WAKEUP**”.

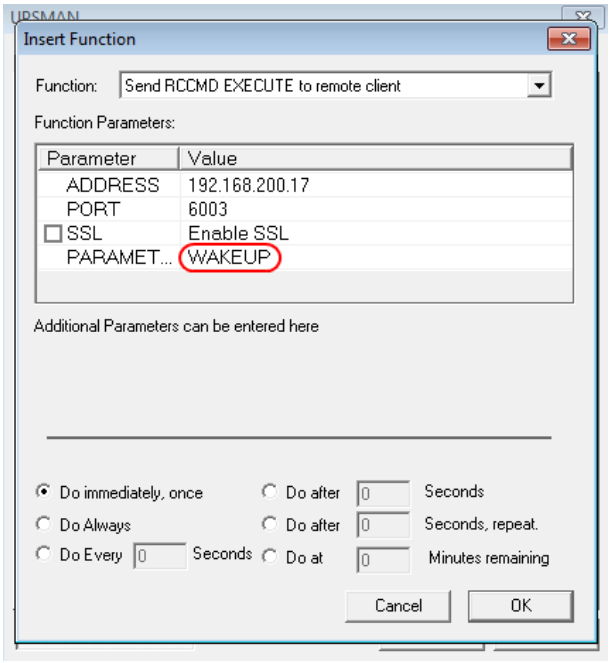


Fig. 41: CS121/CS141 Configuration “WAKEUP” Command

Configuration **„UPSMAN“**
Click into the UPSMAN configuration the buttons “**Advanced Users**”, “**Events**”, “**Power restored**” and “Insert”. Add the function “**Send RCCMD execute to remote client**”, set the accordant **IP address** of the RCCMD client and enter the command “**WAKEUP**”.

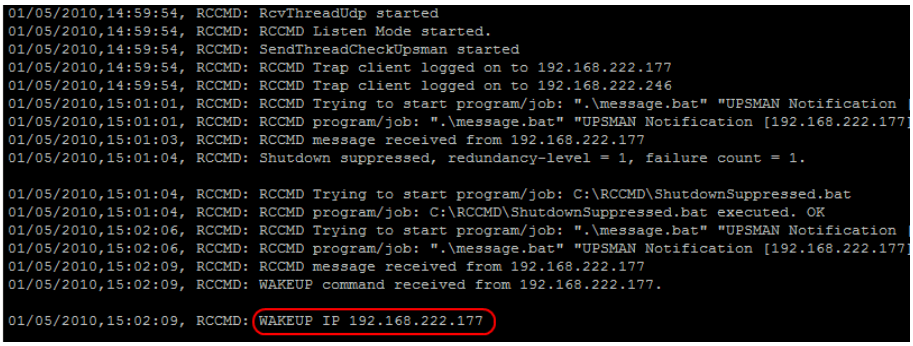


Fig. 42: „WAKEUP“ Befehl im RCCMD Log

Advise: The restart of the RCCMD service is a third opportunity to reset the redundancy alarm.

3.6 RCCMD with SSL for Windows

The Secure Sockets Layer (SSL) protocol is a cryptographic protocol that provides security and data integrity for communications over TCP/IP networks. By sending a RCCMD message it will be encrypted (also with own certificates) and only executed if the codes with the client match and the time stamp is not to far apart.

Configuration menu **„SNMP Adapter“:**
Use your Web-browser to navigate to the address of your UPS Web-Manager. Click the “**Network & Security**” configuration button and enable the **SSL** network feature.

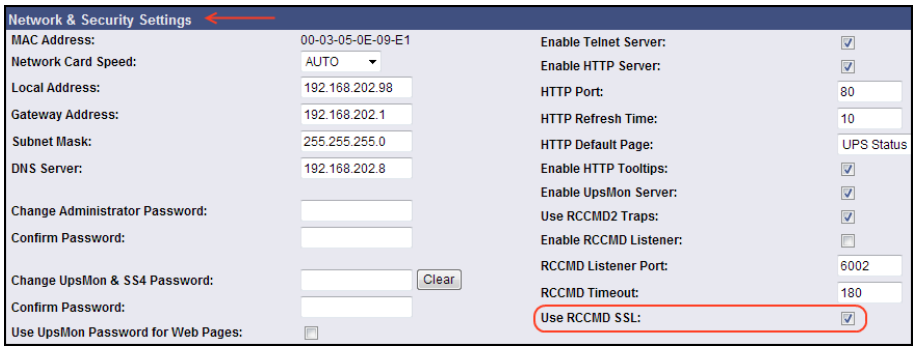


Fig. 43: RCCMD SSL Settings

Menu „**Timeserver**“:
The SSL network feature requires correct time settings, so it is required to configure a timeserver. Click the „**Timeserver**“ configuration button and enter the address of at least one timeserver.

Click the „**Apply**“ button.

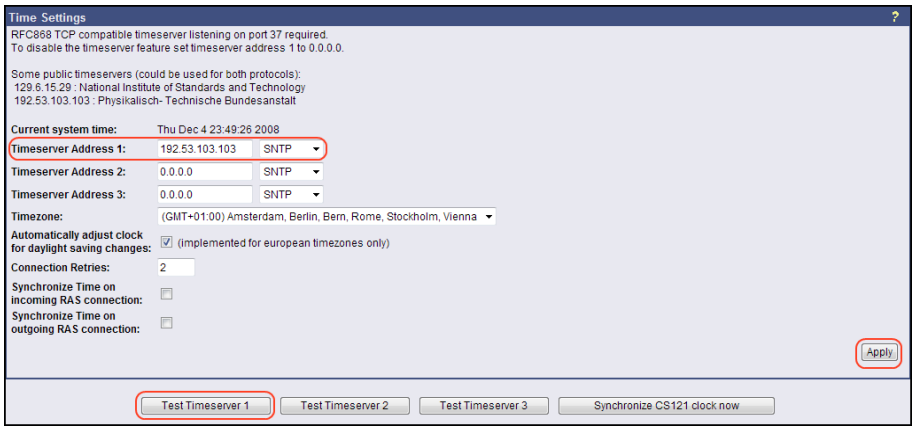


Fig. 44: Timeserver Konfiguration

Menu **„Save Configuration“:**
Click the „Save Configuration“ button and the „**Save, Exit & Reboot**“ button to confirm your settings.

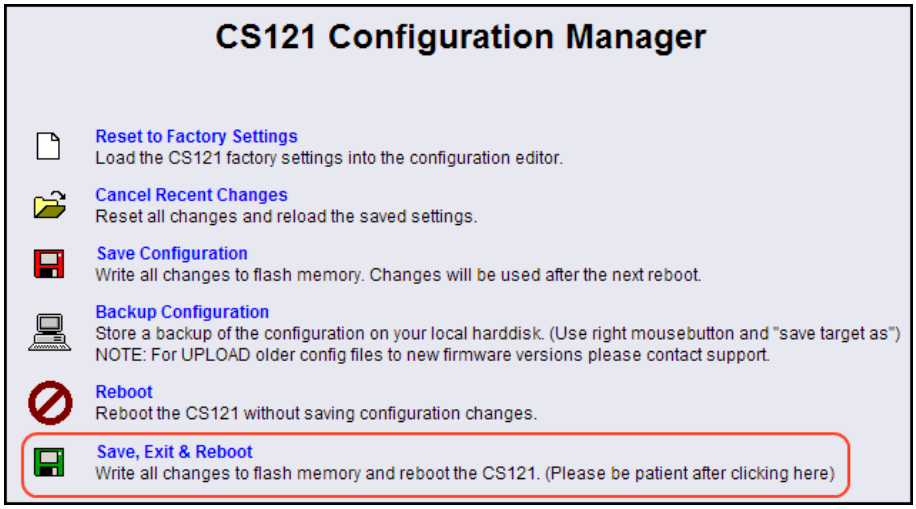


Fig. 45: Settings Confirmation

Menu „**RCCMD Web Configurator**“:
Start the RCCMD Web Configurator again and enable the **SSL network feature**.

If you want to accept expired certificates, please enable the function “**Reject expired SSL certificates**”.

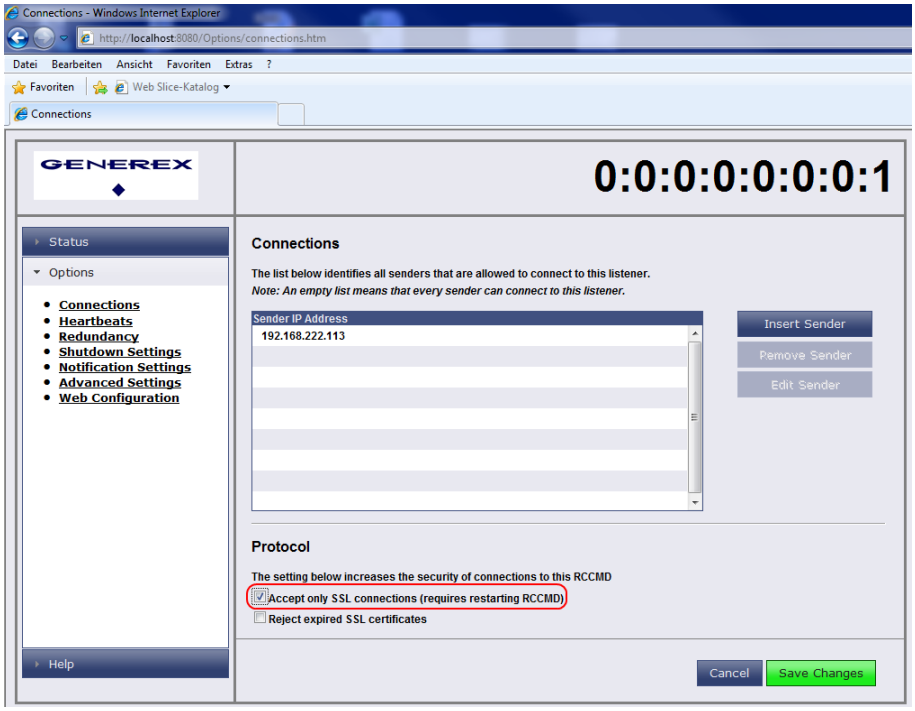


Fig. 46: RCCMD Web Configurator - SSL Konfiguration

3.6.1 RCCMD with own SSL certificates

In this chapter we will describe, how to use an own SSL certificate with RCCMD, e. g. OpenSSL (http://www.openssl.org/related/binaries.html):

Be your own CA

Using OpenSSL it is quite simple to become your own CA. Just run:

```
CA.pl -newca
```

Done! Just ensure, that you select a useful CN (common name)!

Create your RCCMD certificate

You need to create your certificate for RCCMD now. As it will use it for verification, it should contain the same useful common name (CN), that you selected for the CA. The private key must not be encrypted to let the RCCMD Client (service) start without trouble. Therefore we use the “–nodes” option and the “-newreq” command:

```
CA.pl -newreq -nodes
```

Sign with your CA:

```
CA.pl -sign
```

Now create an empty file named “rccmd.pem“ and copy the cert information of newcert.pem (rccmd certificate), newkey.pem (private key) and cacert.pem (CA) into it. Please note, that the exact copying is required to use it without trouble!

Use your own RCCMD certificate

Do the following steps at the RCCMD Client and every sender (e. g. UPS Web Manager):

- Backup the existing “rccmd.pem”
- Replace the existing “rccmd.pem” with your own
- Restart the RCCMD Client
- Restart the RCCMD Sender!

3.7 Settings of the Authorization of the RCCMD Service

This function is used for the commitment of the user authorization of the UPSMAN service, which exceeds the system shutdown, e.g. execution of batch files, script files etc.

RCCMD Properties Menu „**General**“:
Open the menu of the properties window for the RCCMD service (via control panel, administration and services).

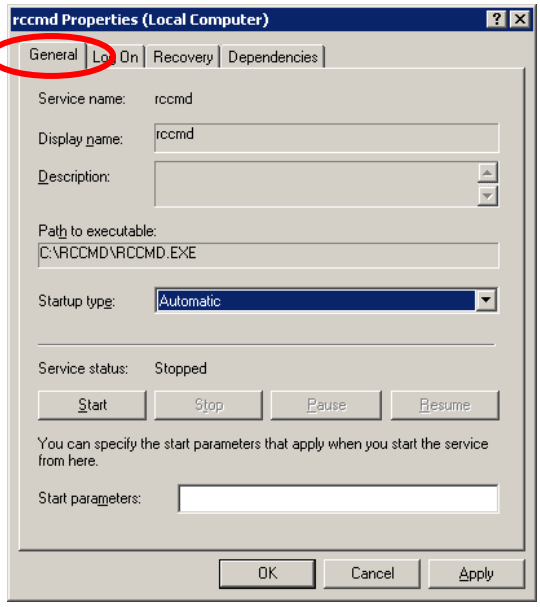


Fig. 47: RCCMD Properties Window

RCCMD Properties Menu „**Log On**“:
Click the “Log On” button on the upper left side.

Disable the “**Local System account**”.

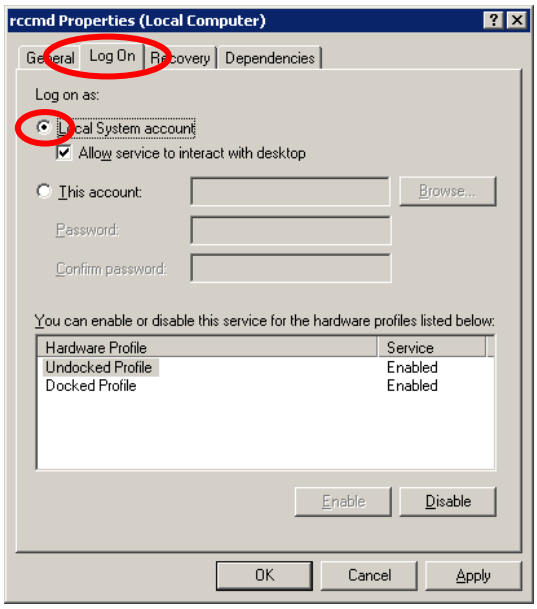


Fig. 48: RCCMD Properties Log On Window

Check the “**This account**” ring and **delete the passwords** and click the “**Browse…**” button.

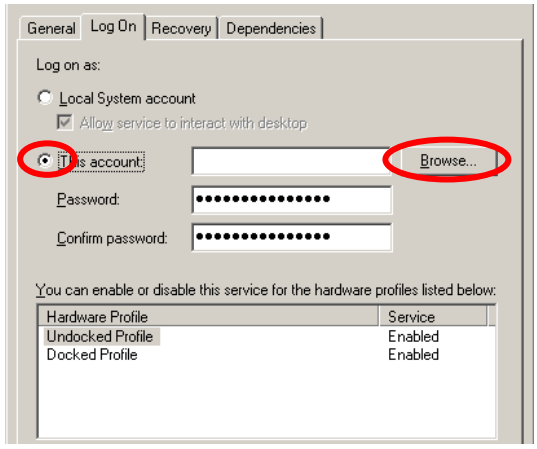


Fig. 49: RCCMD Properties Password Confirmation

A new window opens.
Click the **"(examples)"** button to select the object name.

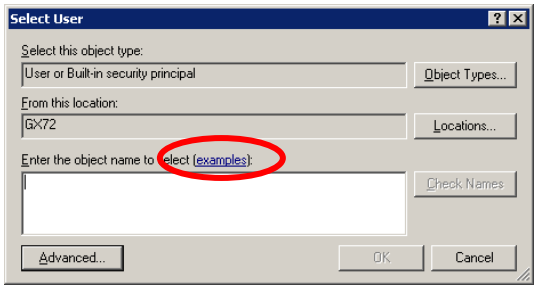


Fig. 50: Select User Window

Choose the object name.

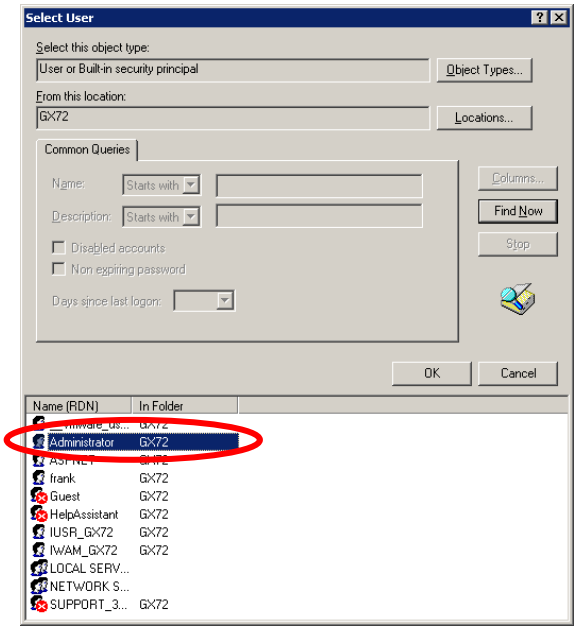


Fig. 51: Selection of the Object Name

Click the "**OK**" button.

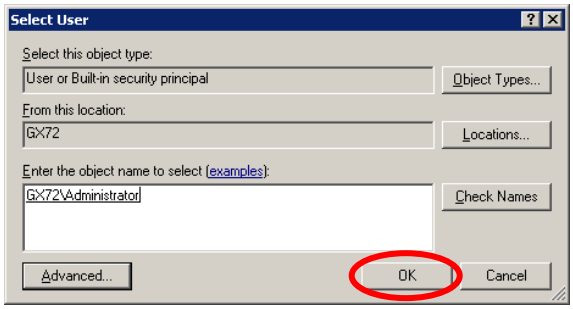


Fig. 52: Administrator Selection

Enter the **new password** twice.

Click the „**OK**“ button.

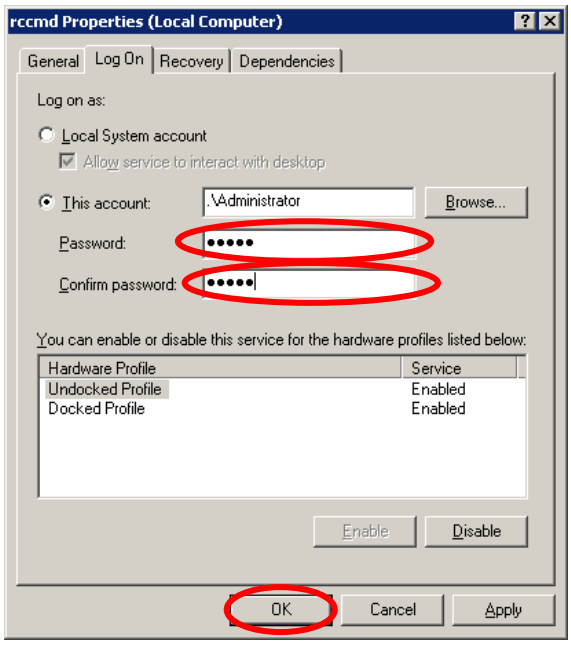


Fig. 53: Administrator Password Confirmation

A new window opens. Confirm the account with the „**OK**“ button.

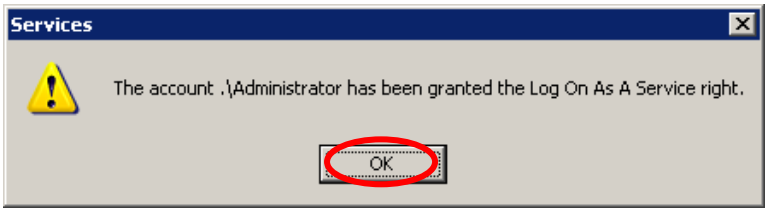


Fig. 54: Service Right Info Window

3.8 Testing of the Shutdown.Bat Files

We recommend to test the edited shutdown.bat file. The shutdown program **EXITWIN.EXE** is predefined. Just enter **RCCMD -?** in the **RCCMD directory** for syntax help for this shutdown tool. You may use also your own shutdown tool or any other which we provide with this software.

Attention: If your configuration works fine in the DEBUG mode, does not necessaryly mean that it works also with the RCCMD as NT service. Please ensure that the RCCMD as service has been started in a user account with administrative rights, otherwise it may happen that only non-restrictive programs may be executed (like notepad.exe) but no Shutdown. (This will result in the NT error message ”Adjust Token Privileges failed”.) If a program has in fact started or not can be seen in Taskmanager window (ALT+CTRL+DEL), because a service does not a started program in the current user session due to non-interactive transaction with the desktop.

The full command syntax for the NT consol for RCCMD in <Listen mode>:

rccmd [–debug] -l [-a IP adress] [–h hostname] [-p port] "command"

The command can be either a program or a path for another batchfile on this workstation. The command file should be given with full path. The -p port option can be included if you want to start RCCMD more than once at a single workstation to proceed different commands for different events. The default port number is 6003, use any other availabe port number for different RCCMD commands.

RCCMD in the send mode:

rccmd [–debug] -s [-a IP adress] [-h hostname] [-p port]

This command is regularly used in the batchfile of the sender (shutdown.bat) and sends a "ping" to the computers IP adress or hostname. If this ”ping” has been answered, the next command RCCMD –s may be executed, etc.

When you have finished the edition of the bat files, click the “**Restart RCCMD**” button into the “System Status” menu.

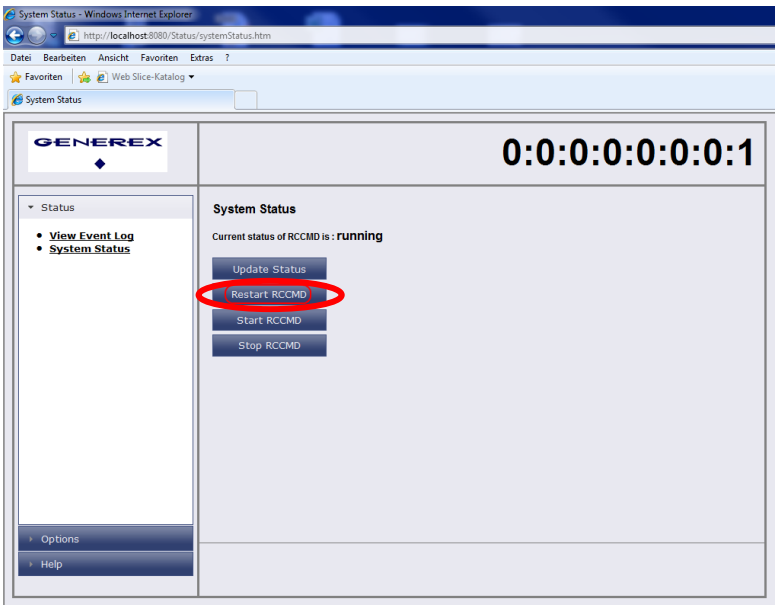


Fig. 55: System Status – Restart RCCMD

RCCMD is now running as Service with automatic startup. To configure the automatic start of RCCMD use administrative rights and control panel, service to change the settings.

IMPORTANT: RCCMD as service with local desktop interactions is permitted to execute local shutdowns – for this action no user rights – except administrative rights – are required. But for any user specific actions, e. g. starting a net send message or any other command – the RCCMD may need extra rights! These rights have to configured in the Control panel, services.

Sending of a message to all RCCMD clients

To send a message to all RCCMD clients, please use the following syntax:

rccmd –se “MSG_TEXT ups_says_hello_world” –a 192.9.200.255

The RCCMD client, which should receive this message, need to get the entry of the ip-address of the RCCMD sender or rather the list should be empty. The CS121/CS141 is not able to send UDP broadcasts, so you have to enter the above mentioned syntax into the RCCMD client. The client will operate as relay station and will forward the message. It is no problem to send the message from a Windows-, UNIX- or MAC OS RCCMD sender.

3.9 Testing the RCCMD connection

Finally test your configuration if all RCCMDs are present and working. For this you may use the RCCMD in the Debug mode Syntax (RCCMD –debug –s/l –a), so that you have screen output. ”PING” every remote computer with the command ”ping [hostname] [IP address]”. If the PING works fine, you can now start to test the RCCMD connection with the debug mode. If everything works fine, you will see that a connection is established and closed again. This means that the remote RCCMD received your signal and will execute the shutdown script on the remote side.

Attention! This test will execute the shutdown script! If you want to avoid the shutdown, please remove the shutdowncommand from the RCCMD client Shutdown.Bat/SH file!

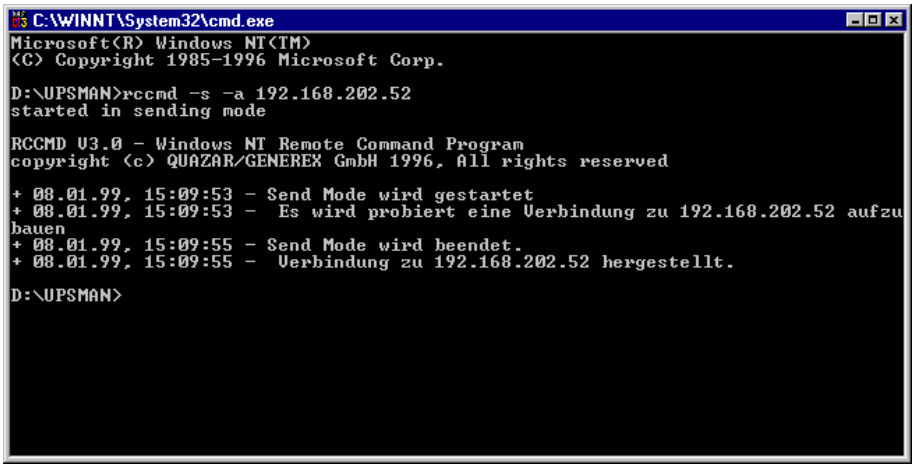


Fig. 56: RCCMD Console Test

3.9.1 Testing the RCCMD 2 connection

In order to see under RCCMD 2 if the UPSMAN processes on the remote client are still active, the following syntax can be entered via command line:

rccmd –sc –ac <IP address>

If the UPSMAN is active, the message “**UPSMAN <IP address> alive**”. There is no message if the UPSMAN is inactive.

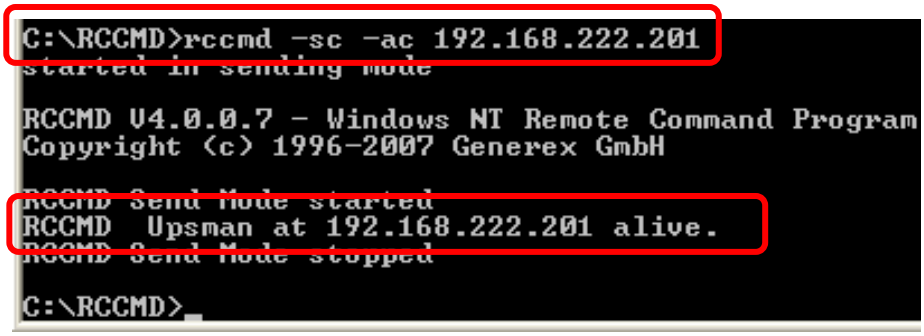


Fig. 57: RCCMD Alive Check via Command Line

Use this command to get help:

C:\Program Files\RCCMD>rccmd -?

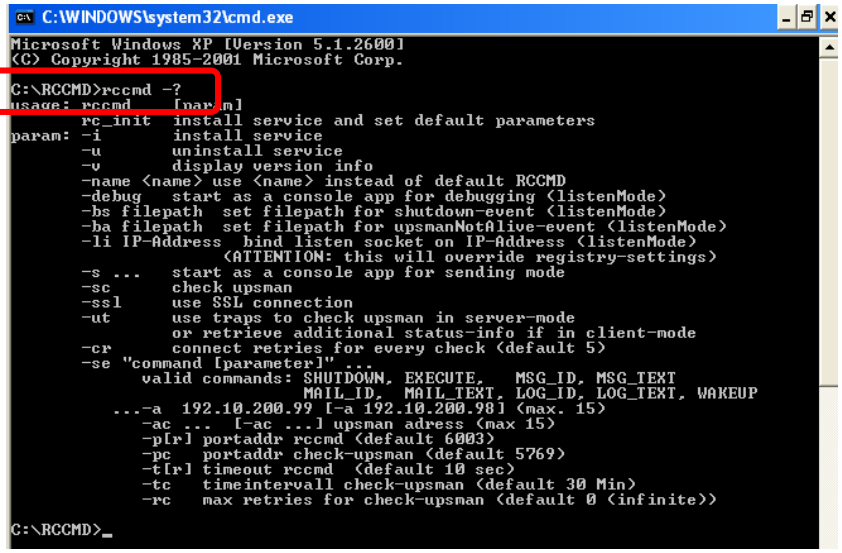


Fig. 58: RCCMD Console -?

3.10 RCCMD on Windows 95/98

RCCMD for Windows 95/98 functions similar to RCCMD on Windows NT. The only difference is the program name, which changes to **RCCMD95.EXE**. Please also refer to the RCCMD Windows section of this manual. Note that both OS are NOT supported anymore.

Attention: For Windows 95/98 users we do recommend the installation of the TCP/IP protocol first and then run the configuration program making use of the RCCMD WIZARD.

Attention: In case Winpop.exe is used on Windows 95/98, RCCMD can not be started on port 6003 otherwise the computer will hang-up. Please change the sender and receiver call up accordingly.

Experienced users may use the registry editor and enter all changes manually. Unexperiecend users should use the RCCMD wizard.

Registry settings: Please check the following: In order to start the RCCMD process in ”Listen” mode, the RCCMD parameter have to be entered in the registration database. Please enter:

regedit.exe rccmd95.reg or simply start rc_init.bat

The parameters are now located under the registration-key:

HKEY_LOCAL_MACHINE\CurrentControlSet\Services\RCCMD95\Parameters

Start *regedit.exe* again if you want to reconfigure RCCMD.

Parameters:

Port: Special TCP-Port that receives the RCCMD signal.

***Addr1... 10*: TCP/IP address of the computer that accepts the RCCMD-signal.**

***ExecutePrg*: Command that is to be executed when receiv¬ing the RCCMD-signal.**

To start RCCMD execute the command:

rccmd95

Or start the program using the Windows 95/98-launch bar.

To start RCCMD in sending-mode (send) enter the following line in your shut¬down-job:

RCCMD95 -s -a <address> [-p 6003]

For <address> enter the TCP-address of the machine to which you want to send the RCCMD-signal.

Optional parameters:

-p <port> = TCP-Port on which the RCCMD-signal will be send

The option –a can be used several times, if a shutdown on more remote computers in the network should be executed.

Do not use the CD License key more than once. (Copyright regulations page 1). If more RCCMD modules need to be installed for the shutdown, additional CD license key must be purchased. Additional license keys are available from your UPS dealer, whereas the CD can be used again for the actual installation.

3.11 RCCMD for Windows NT/2000/XP/2003/2008

The RCCMD (remote console command) is a program that allows the execution of programs on remote computers. This tool is part of all UPSMAN supported operating systems with the exception of Windows 3.x.. With this tool it is possible to connect different operating systems. Is the UPS-Management Software installed on a Windows NT/2000/XP computer and should a remote shutdown be executed on a computer with a different operating system in a heterogeneous network, the RCCMD tool is necessary.

Attention: For first time users we do recommend the use of the RCCMD Wizard, which makes the configuration easier. Please start the RCCMD Wizard from your program group.

Attention: Please do not use the wizard and manual settings at the same time.

Now the RCCMD has been installed and configured to execute C:\ups\shutdown.bat.

3.12 RCCMD for Windows 2008 Server Core x64

The configuration of the RCCMD Software on Windows 2008 Server Core x64 got one specific. It is required to start the RCCMD configuration out of the default folder C:\RCCMD with the following command:

```
C:\RCCMD>RCCNF_NT.EXE
```

Please take a look into the chapter for the installation procedure and into the chapter for the configuration of RCCMD.

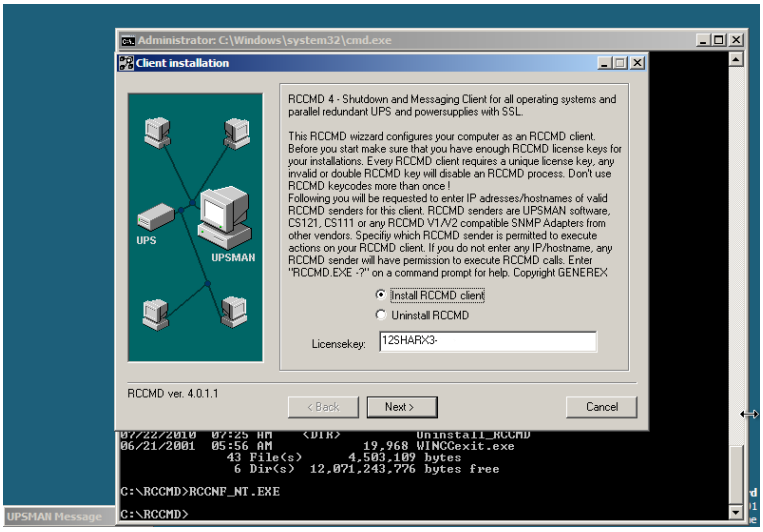


Fig. 59: RCCMD Configuration

3.13 Older RCCMD Configuration

Attention: In the following we are describing the RCCMD configuration of the Windows tool “Rccnf_nt.exe”, which was delivered until 04/2012. All functions are equal to the newer RCCMD WebInterface version, which is delivered since 05/2012. The detailed functions of RCCMD are user interface independent and will be described for the older RCCMD version.

RCCMD Configuration „**Introduction“:**
Make sure that „**Install RCCMD client**“ is marked.

Click the „**Next**“ button.

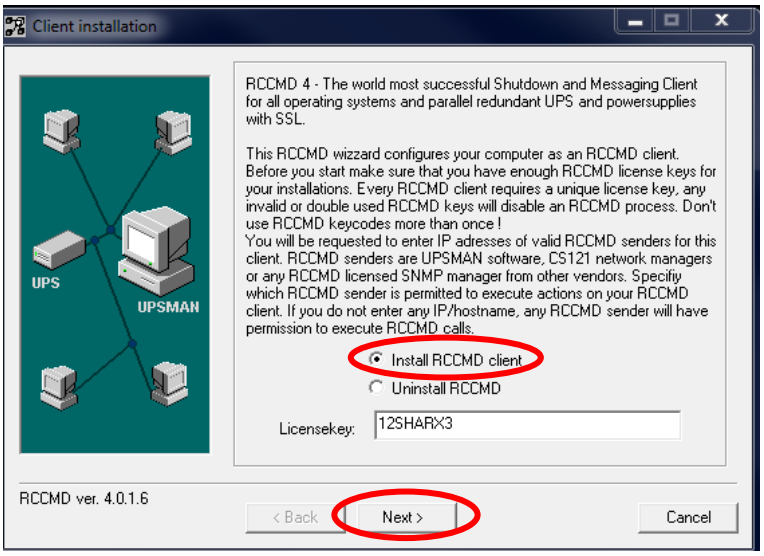


Fig. 60: Client Installation

RCCMD Configuration “**IP address”:**
To enter an authorized IP-Adress of a sender click on **„Add Address“.**

Add the IP address of the RCCMD server, which is allowed to send a shutdown to this client.

Click the „**OK**“ button.

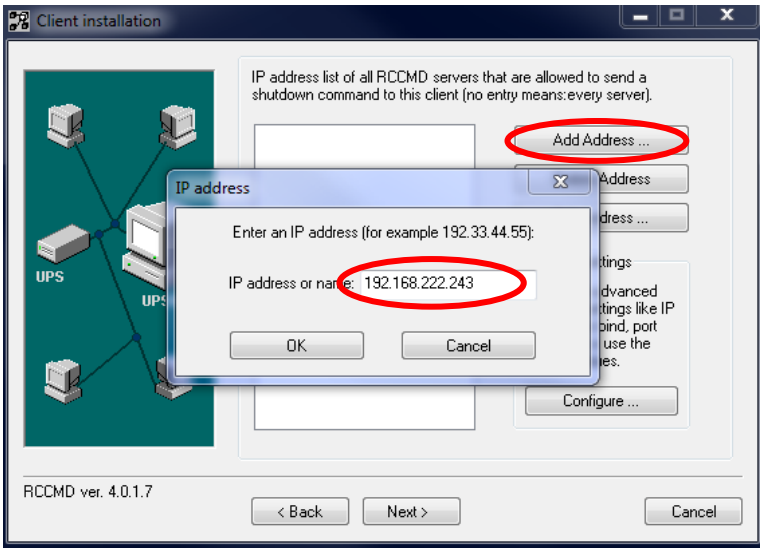


Fig. 61: Add IP-Address Window

Attention: If you do not enter an address, then every server has the permission to send a shutdown command. If more than one CS121/CS141 or rather UPSMAN is existent, thus a redundancy situation, you need to enter more than one address as authorized sender.

RCCMD Configuration

“Advanced network settings”:

If you want to use the secure connection (**SSL**), click the “**Configure…**” button and check the “SSL” box and you can change the **port** for the messages..

Click on the „OK“ button and then next.

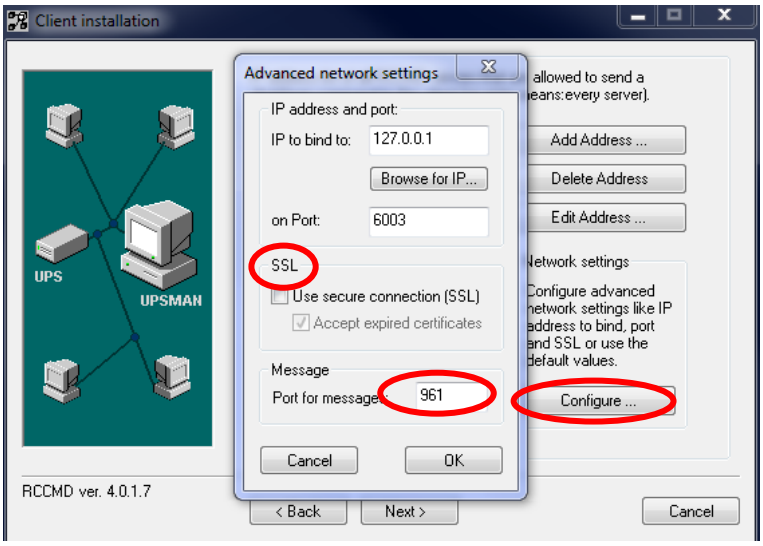


Fig. 62: Advanced Network Settings

RCCMD Configuration

“**UPSMAN alive checking”:**

If you want to use the **UPSMAN alive checking** (recommended), check the “Enable connection check” box. Alive check is a signal, send out to the UPSMAN or CS121/CS141 on port 5769 to check if the UPSMAN has still UPS data – or not. If this fails, the scriptfile alive.bat will be executed which causes a messagbox coming up. The polling rate (default 30 min.) defines the polling of the UPSMAN service, connect retries (default 5) means after 5 unsuccessful connection tries an alarm will be triggered.

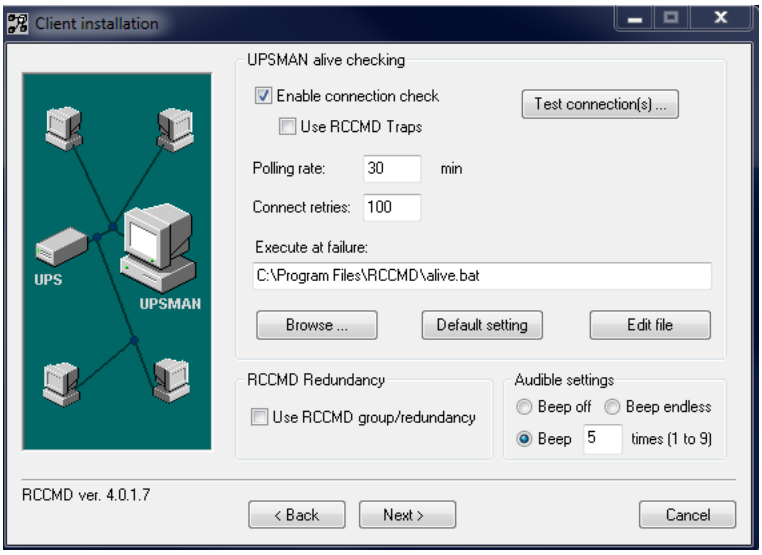


Fig. 63: UPSMAN Alive Checking / Redundancy Window

RCCMD Configuration “**Use RCCMD Traps”:**

The function “**Use RCCMD Traps**” enables UPSMAN/RCCMD/UNMS traps, which show the UPS status as a trap message. If activated it will display a local message when the UPS status of the UPSMAN/RCCMD server changes.

RCCMD Configuration
“Test connections…”:
If you click the “**Test connection(s)…**” button, the UPSMAN alive checking of the entered IP addresses will start (port 5769 will be tested).

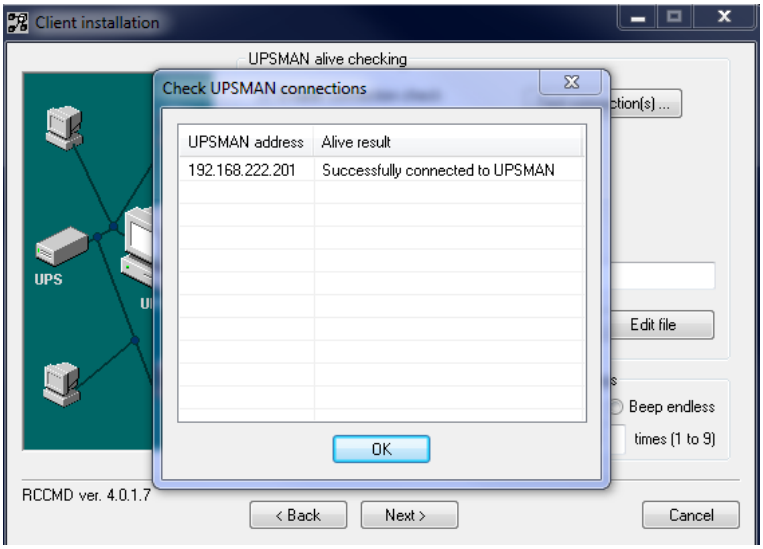


Fig. 64: Check UPSMAN Connection Windows

RCCMD Configuration “**Browser…”:**
If you click the „**Browse...**“ button, you will get a selection of the default batch files.

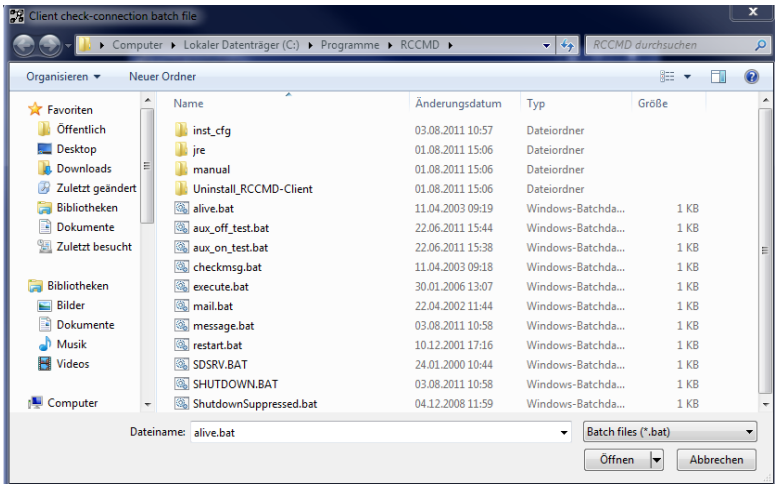


Fig. 65: Client Check Connection Batch File Window

RCCMD Configuration “**Default setting”:**
If you click the „**Default setting**“ button, you will get back to the default batchfile (alive.bat).

At the failure of the UPSMAN alive checking, you can define an executing file or edit the default file “alive.bat”: (file contents as follows):

@echo off

rem * "messagetext" %1 == ip-address, %2 == date, %3 == time *** "title" -c counter for beeps**

start /b msg.exe "Check Upsman %1 failed (%2, %3)" "ATTENTION RCCMD:" -c:1

RCCMD Configuration “**Audible Settings”:**
You can define the “**Audible Settings**” as follows:

- **Beep off**
- **Beep endless**
- **Beep amount (1 to 9)**

RCCMD Configuration “**Edit file”:**
Logfile configuration

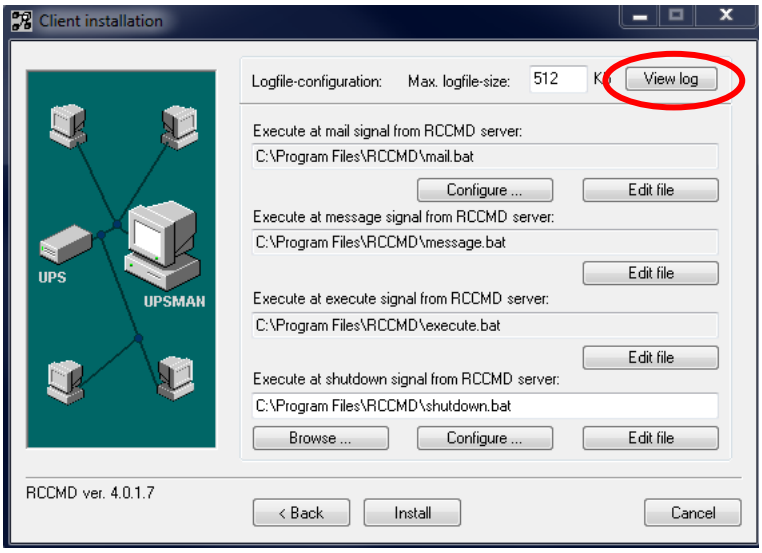


Fig. 66: Configure / Edit Bat Files

When you click the button „View log“, you can configure the log file size and edit the executing bat files in this installation window.

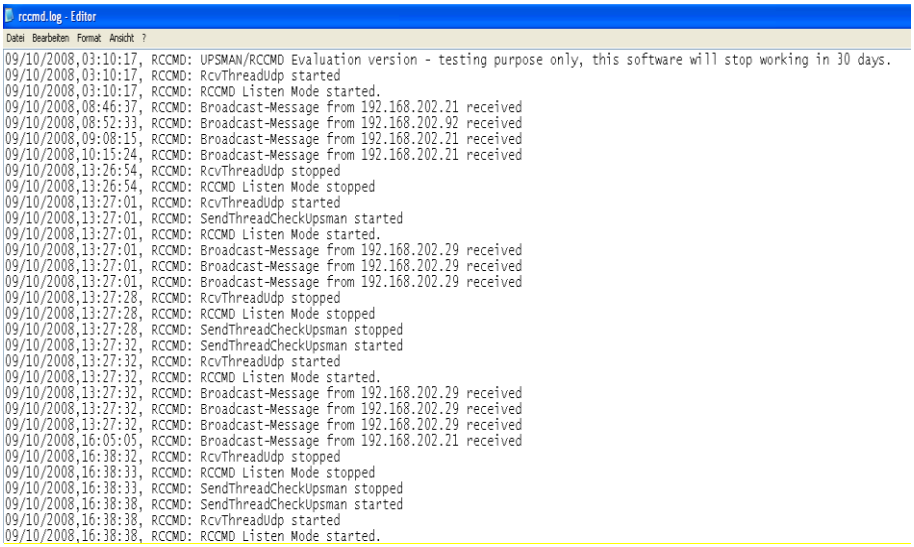


Fig. 67: RCCMD Log File

RCCMD Configuration “**Email settings”:**
If you want to send **emails** via RCCMD, click the “**Configure…**” button.

Enter the accordant **parameter**.

Click the „**OK**“ button.

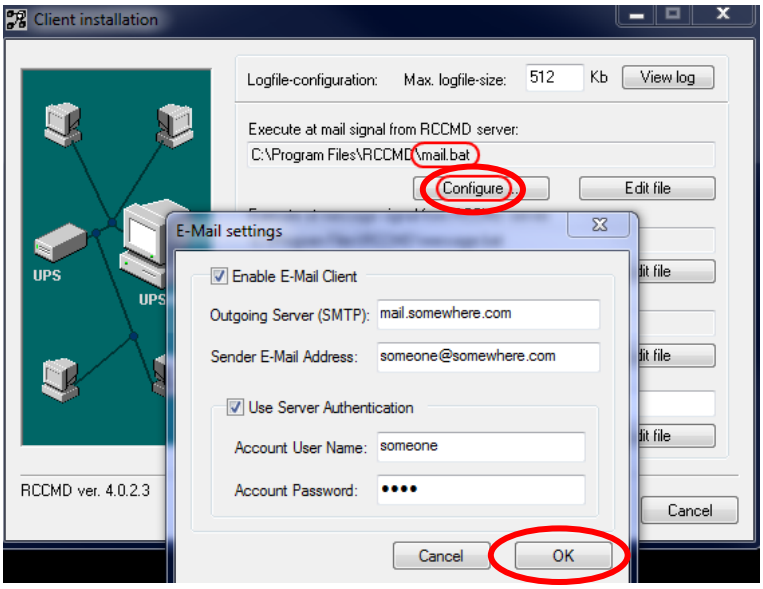


Fig. 68: RCCMD Email Settings

Use the following RCCMD command:

mail „receiver address“ text

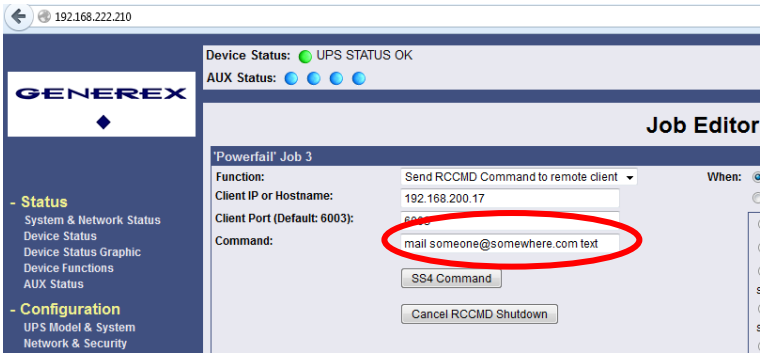


Fig. 69: CS121/CS141 Email Command

If you want to change the shutdown sequence, click the “**Configure…**” button..

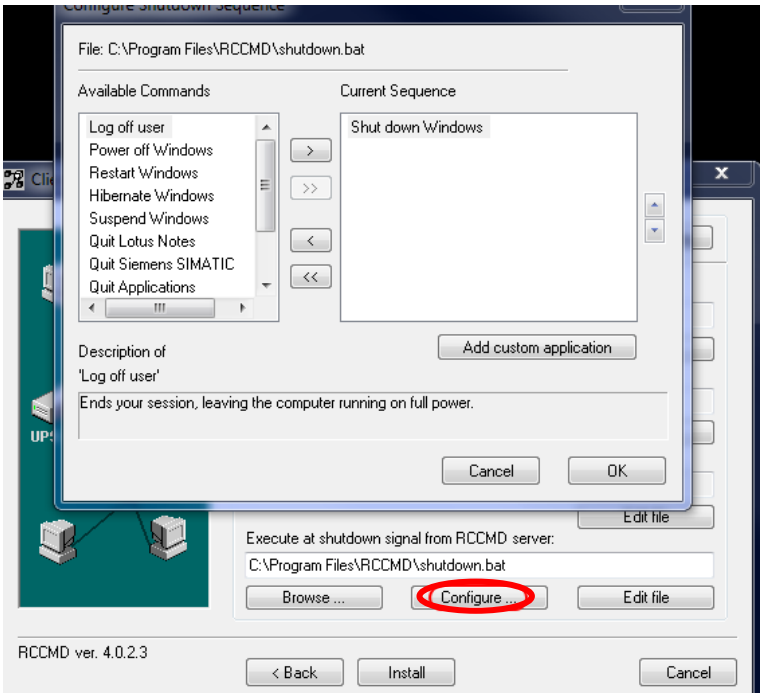


Fig. 70: RCCMD Shutdown Sequenz Configuration

3.13.1 RCCMD Client as Relay Station

In order to reach a bigger number of RCCMD receivers, one RCCMD client needs to be operated as relay station. The receiver will be configured so that it will receive a RCCMD signal and this signal will be used to start a batch file, which then starts even more RCCMD sender signals. This workstation is then sender and receiver at the same time and is therefore an important link in the UPS monitoring chain. Generally the usage of a RCCMD client as a relay station makes the management of several 100 RCCMD clients far easier than configuring this via the Web-interface of the CS121/CS141. Additionally, all Web-browser event configurations have a certain limitation so that it is required to use the relay function, if the number of jobs exceed 50 per event at the CS121 HW 13.

See the following script, which lets the RCCMD-client act as relay station:

```
rem created by setup
@echo off
set path=%path%;C:\Program Files\RCCMD
# RELAY RCCMD
# This batch will send RCCMD shutdowns to the IP addresses listed below
# At the end of the batch this computer will initiate the local shutdown
start rccmd -s -a 192.168.200.2
start rccmd -s -a 192.168.200.3
start rccmd -s -a 192.168.200.4
start rccmd -s -a 192.168.200.5
start rccmd -s -a 192.168.200.6
start rccmd -s -a 192.168.200.7
# to be continued
#
# local shutdown
ExitWin.exe shutdown force
@cls
```

Fig. 71: Example: Batch File RCCMD act as Relay Station

"**start**" is a Windows batch command to start the program call in several instances. This allows to execute programs simoultanously and speeds up the shutdown process. Please note that "start" is not supported in all Windows versions and it should be tested before using.

The RCCMD Version 4.0.1.0 or higher provides a grafical configuration of the RCCMD relay function.

Click the "**Configure…**" button..

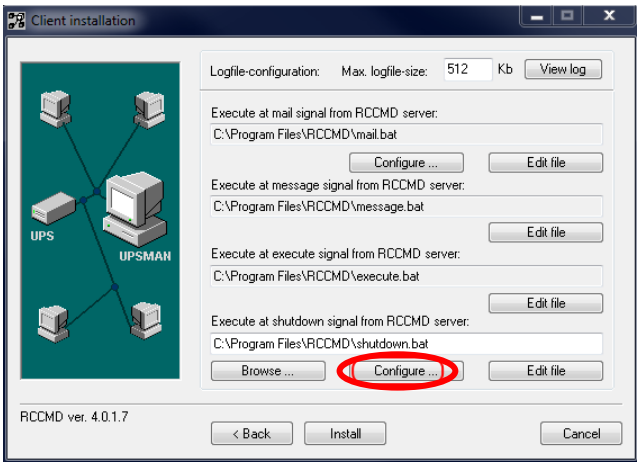


Fig. 72: RCCMD Client Shutdown Configuration

Tag the "**RCCMD shutdown relay**" into the "**Available Commands**" window and click the "**>**" button, to add this function into the "Current Sequence".

Click the „**OK**" button.

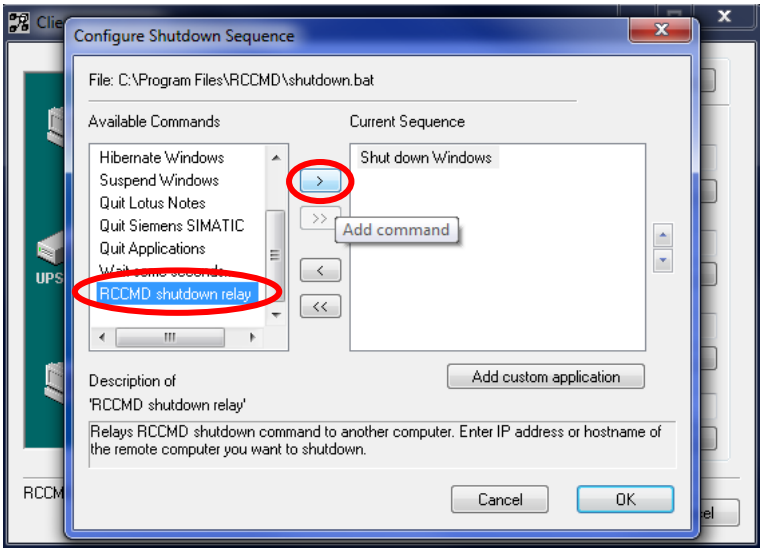


Fig. 73: RCCMD Shutdown Relay

The following panel will appear, in which you can enter the desired **IP address range**.

Additionally you can enable the SSL function.

Click the „OK“ button.

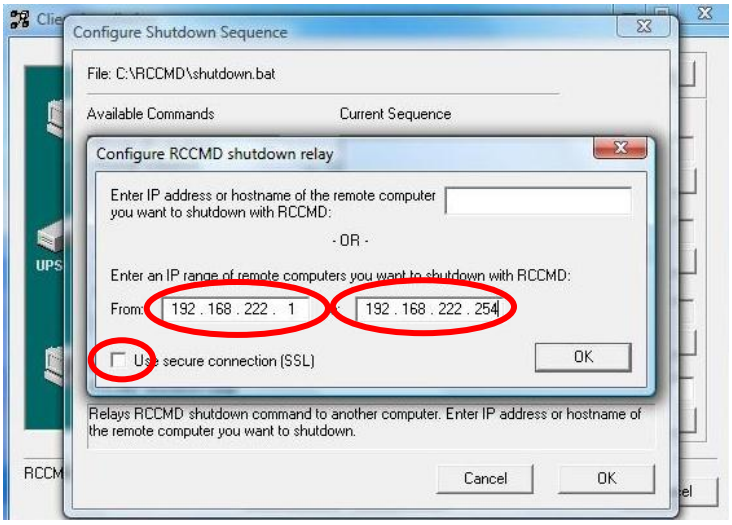


Fig. 74: RCCMD Configuration IP Address Range

If you want to **remove** single **IP addresses**, mark the line with its desired **IP address** and click the “**<**” button.

Click the „OK“ button

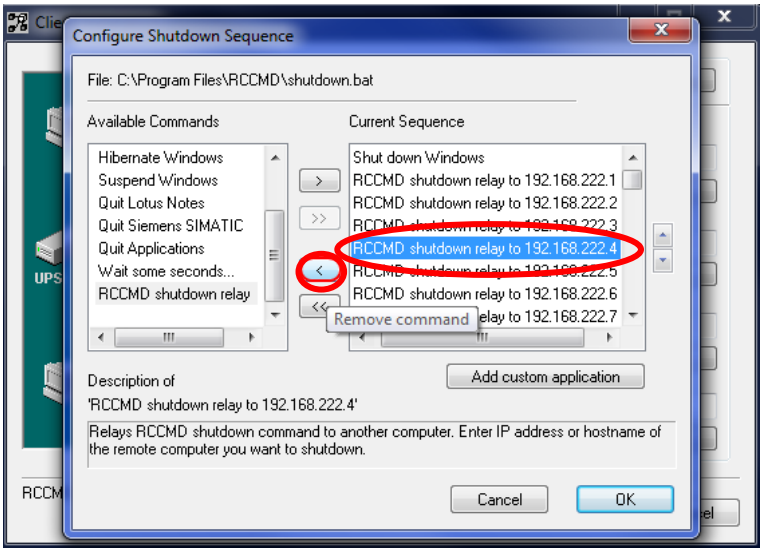


Fig. 75: RCCMD Shutdown Relay Removal

The result of this graphical configuration of an RCCMD relay is found in the shutdown scriptfile “**shutdown.bat**”.

```
@ECHO off
REM --- Created by RCCMD configuration ---
SET path=%path%;C:\Program Files\RCCMD
rccmd.exe -s -a 192.168.200.10
rccmd.exe -s -a 192.168.200.11
rccmd.exe -s -a 192.168.200.12
rccmd.exe -s -a 192.168.200.13
rccmd.exe -s -a 192.168.200.14
rccmd.exe -s -a 192.168.200.15
rccmd.exe -s -a 192.168.200.16
rccmd.exe -s -a 192.168.200.17
rccmd.exe -s -a 192.168.200.18
rccmd.exe -s -a 192.168.200.19
rccmd.exe -s -a 192.168.200.20
ExitWin.exe shutdown force
@CLS
```

Fig. 76: RCCMD Shutdown Relay in the „Shutdwown.bat“

In difference to the above mentioned manual entries of an rccmd shutdown sequence, the graphical tool does not use the command “start” as parameter and therefore the shutdown is taken serially – which means one-after-the-other. Every IP address which does not respond to such an RCCMD call may take up to 10seconds (default) until the timeout is reached and the next command is executed.

4 RCCMD on UNIX (with graphical interface)

The RCCMD (remote console command) is a program that allows the execution of programs on remote computers. This tool is part of all UPSMAN supported operating systems as well as all GENEREX CS121/CS141 SNMP Manager, BACS Webmanager or RCCMD licensed SNMP Manager of other manufacturers (Rittal CMC, General Electric SNMP, Chloride Masterguard). With this tool it is possible to connect different operating systems. E.g. is the UPS-Management Software installed on a Unix computer and should a remote shutdown be executed on a computer with a different operating system in heterogene network, the RCCMD tool is necessary.

The RCCMD tool is based on the TCP/IP protocol. During the installation, the TCP/IP protocol should be installed in the first place.

The RCCMD tool works in two different modes. In the so called ”Listen” mode, the program (as UNIX daemon in a background process) waits for a command from the ”Send” mode of the RCCMD modul.

Note: The RCCMD Installer is using our delivered Java Runtime Environment version, which is used for the installation or rather uninstallation only. In addition the RCCMD Web Configurator is using a Java web-server (jetty). You can delete the RCCMD Web Configurator out of the autostart (etc/init.t/rccmdConfig) or rename the symlink /usr/rccmd/runRccmdConfig. Then RCCMD is running without Java!

Attention: If you got an OS without grafical interface, please take a look into the FAQs, how to mount a USB stick.

4.1 RCCMD installation on UNIX OS

Menu „**Introduction**“:
It is required to install RCCMD as user root out of a rootshell or a graphical terminal. Extract the file **rccmd.tar**, copy it to a temporary folder and start the program “**installRCCMD.bin”**. The following graphical installation will start.

Click the „**Next**“ button.

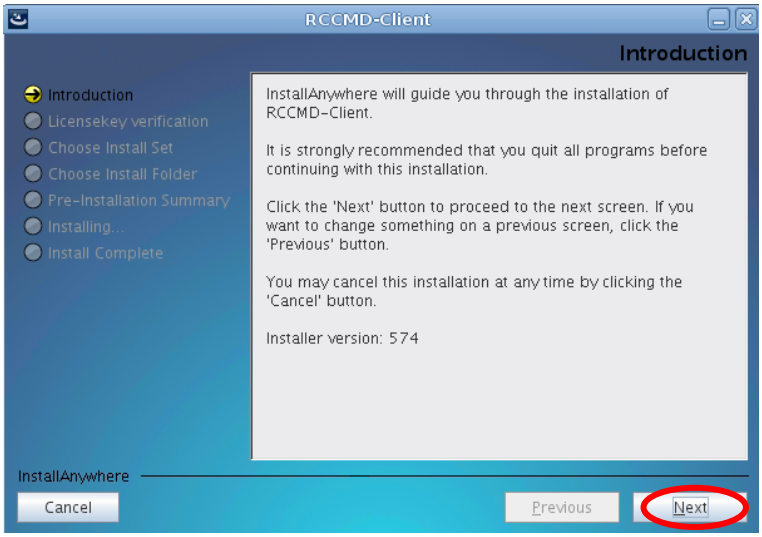


Fig. 77: Installation – Introduction

Enter your **license key**.

Click the „**Next**“ button.

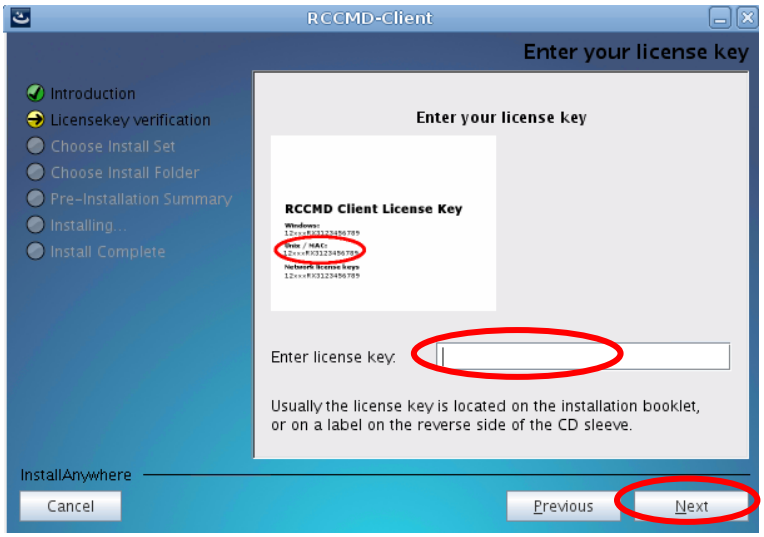


Fig. 78: Installation – License Key

Menu „**Choose Install Set**“:
Choose the desired **features**.

Click the „**Next**“ button.

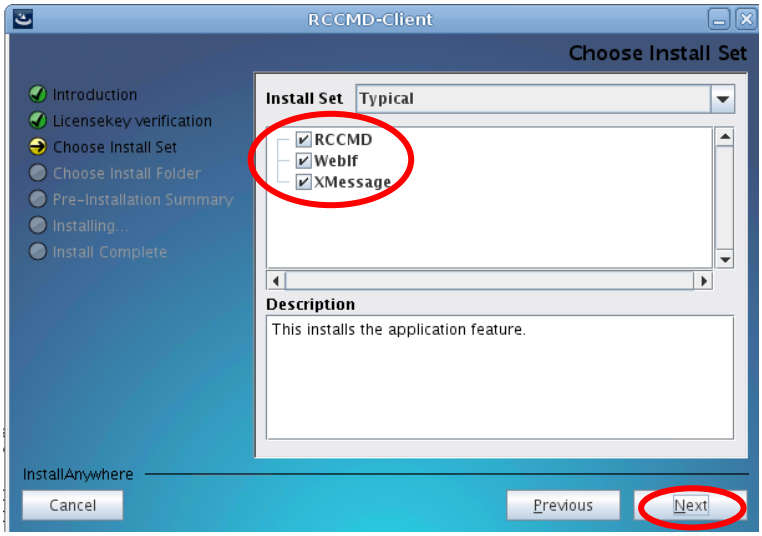


Fig. 79: Installation – Choose Install Set

Menu „**Choose Install Folder**“:
Choose your desired **installation path**.

Click the „**Next**“ button.

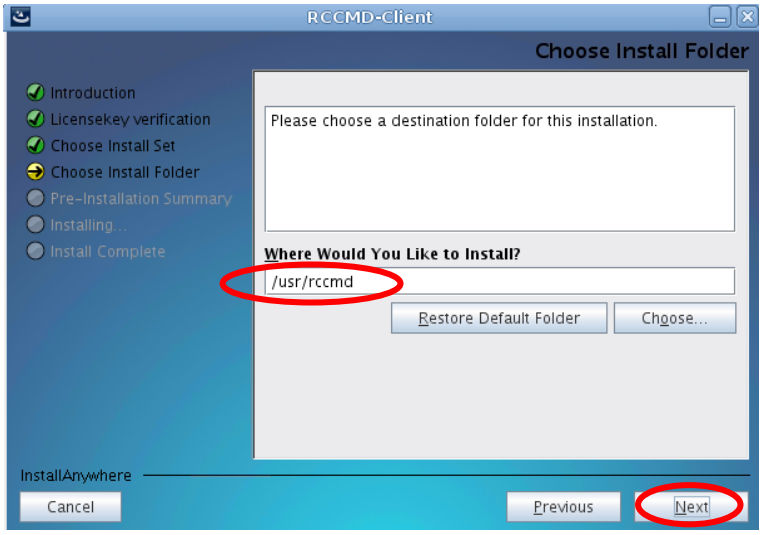


Fig. 80: Installation – Choose Install Folder

Choose the additinal **output options**.

Click the „**Next**“ button.

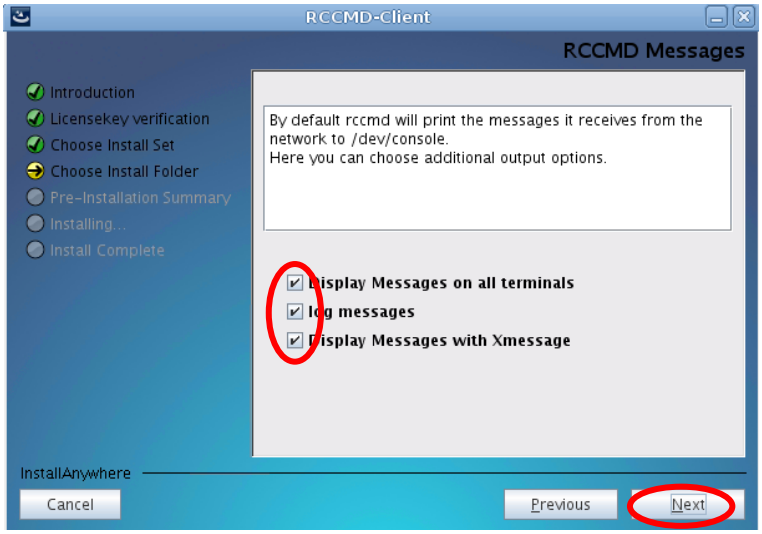


Fig. 81: Installation – RCCMD Messages

Menu „**Pre-Installation Summary**“:
In the next menu you see an **overview** of your installation and you may now press “Install” to begin.

Click on „**Install**“ button to start the installation.

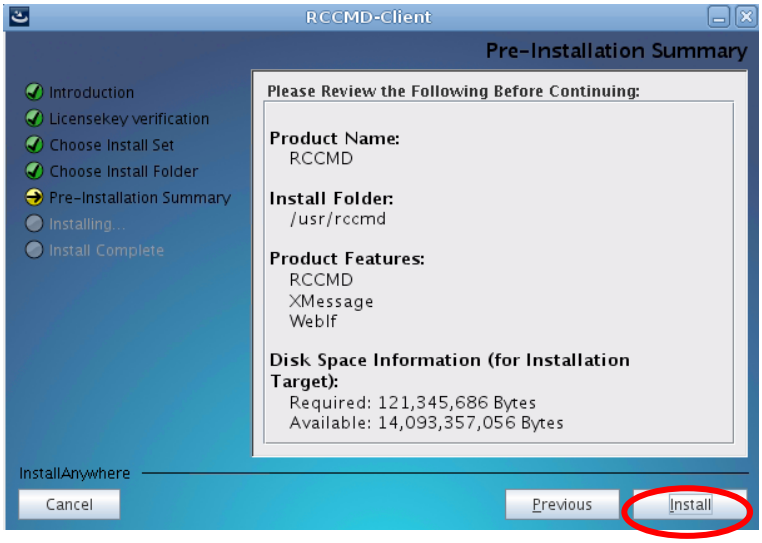


Fig. 82: Installation – Pre-Installation Summary

Menü „**Installing**“:
Select these **default values** for the RCCMD WebIf port and protocol or select new ones.

Click the „**Next**“ button.

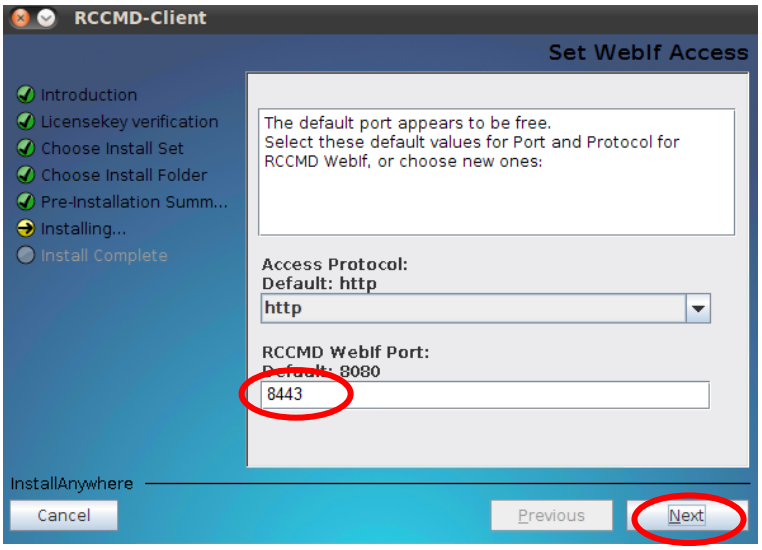


Fig. 83: Installation – Set WebIf Port

Please note the required **firewall exceptions**.

Click the „**Next**“ button.

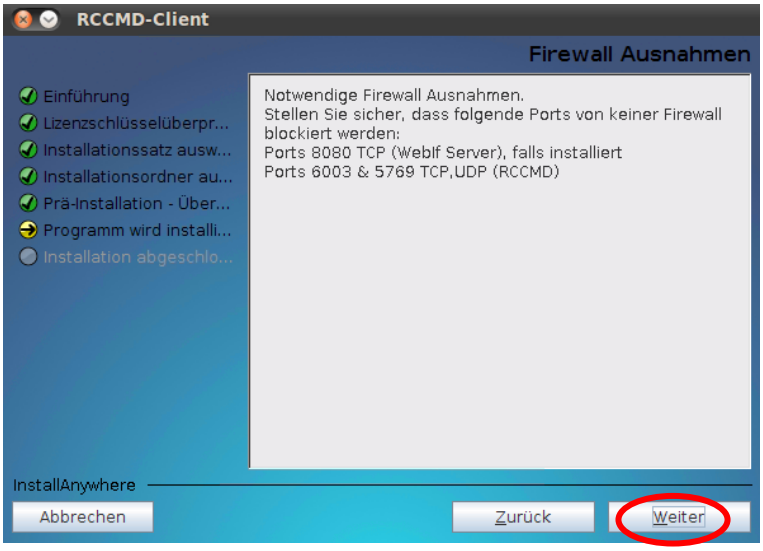


Fig. 84: Installation – Firewall Exceptions

Here you can change the default password.

Click the „**Next**“ button.

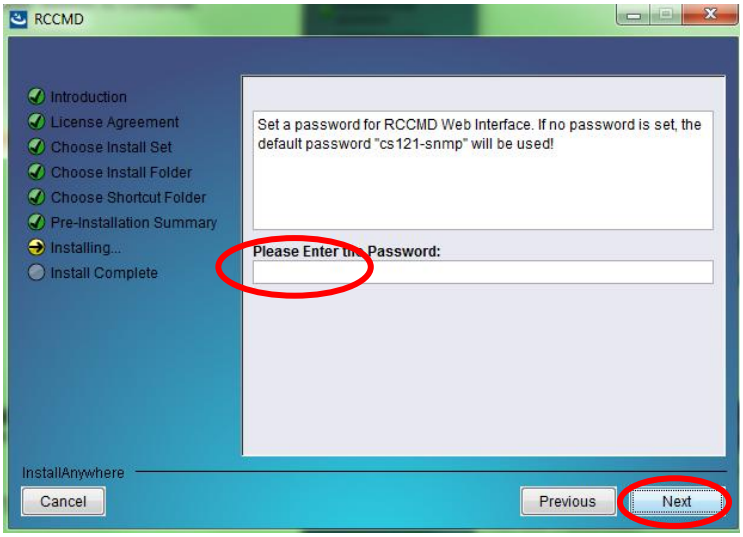


Fig. 85: Installation – Enter password

Here you can set a password hint.

Click the „**Next**“ button.

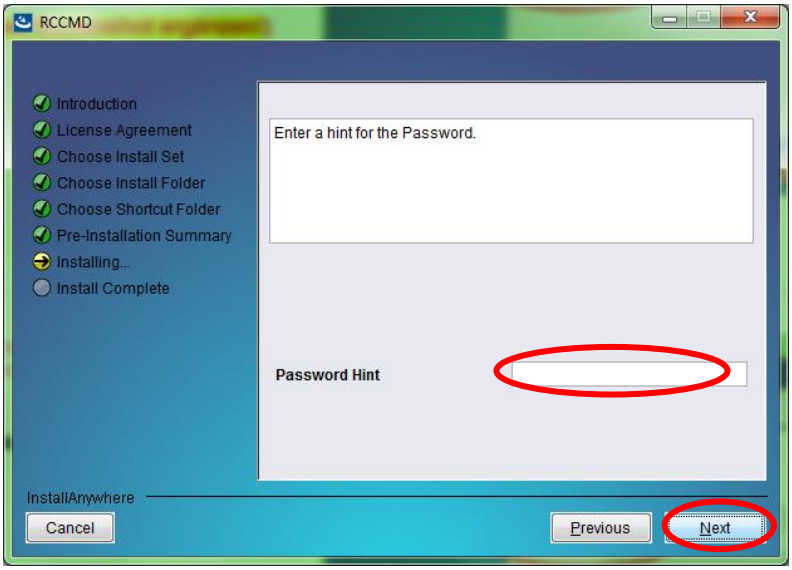


Fig. 86: Installation – Passworthinweis-Eingabe

A reminder appears that you have to configure RCCMD afterwards.

Click the „**Next**“ button.

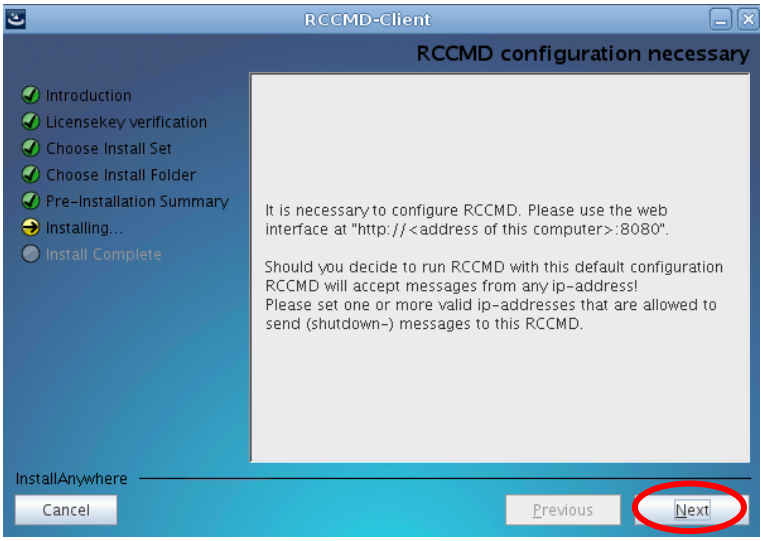


Fig. 87: Installation – Configuration Advice

Choose **RCCMD start**.

Click the „**Next**“ button.

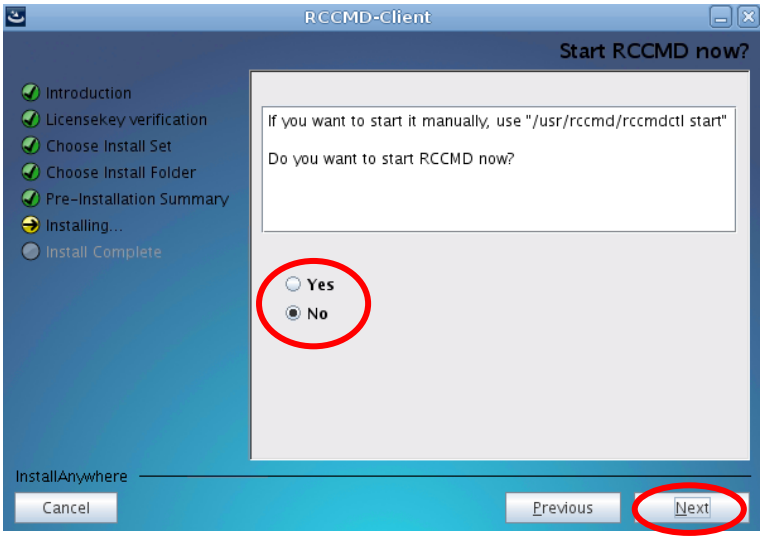


Fig. 88: Installation – Start RCCMD now?

So, RCCMD has been installed successful. Click „**Done**“to finish the installation.

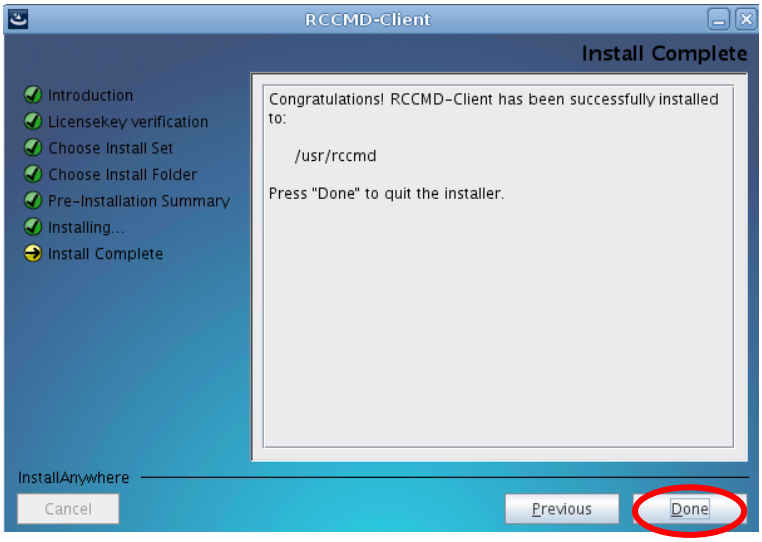


Fig. 89: Installation – Install Complete

4.2 Silent Installation of RCCMD Installation of UNIX OS

A “Silent Installation” is an automated installation procedure, where the user inputs are received from a response file. This allows the user to install a software product without user input or graphical interface.

The RCCMD Software provides a silent installation, but it is required to enter some settings into the “installer.properties” file. This file is located into the CD folder \Rccmd\Linux\12.

```
## This file provides Values to alter the behaviour of the installer.
## You can preset Values for some internal Variables.
## For the installer to find and use this file it is necessary to either rename
##  this file or pass a parameter to the installer when calling it.
## If this file is called 'installer.properties' or has the same name as the
##  installer, e.g. 'install_RCCMD.properties' then the installer should
##  automatically use this file.
## To call the installer with a parameter providing a properties file, the
##  installer need the parameter '-f' in this case the command line call looks
##  somewhat like this: "install_RCCMD.exe -f silent-installer.properties".
## To set the installer User Interface without providing the variable in the
##  properties file, the parameter '-i' can be used.

##  E.g. "install_RCCMD.exe -i silent"
##  The interface options are "silent,gui,console" the gui option is default.
## Choose Feature List
## --------------------
## If you want to install a subset of features from this installer,
##  make a list of all the features you want to be installed.
## The List must be entered in the CHOSEN_INSTALL_FEATURE_LIST variable.
## Options for the list are: RCCMD, WebIf,XMessage
## CHOSEN_INSTALL_FEATURE_LIST=RCCMD,WebIf,XMessage
## This will set the User Interface of the installer
## For installation in console modus, pass the parameter: "-i console" to
## the installer.
#INSTALLER_UI=silent
## This presets the Licensekey. This value is necessary for a silent
##  installation, because there is no other way to pass this information to
##  the installer.
#GXLICENSEKEY=
## The Dialogbutton variable contains the answer to the pop-up question whether
##  the RCCMD should be started at system boot.
##  The value '0' (default) resembles the answer 'Yes' the value '1' corresponds
##  to 'no'.
# CONSOLE_START_RCCMD_NOW=0
## This variable decides whether RCCMD is started after installer ends. Use with care!
## RCCMD should be configured before it is started!
```

```
## '0' resembles the answer 'Yes' the value '1' (default) corresponds
##  to 'no'.
#CONSOLE_START_RCCMD_NOW=1
## Select the language for the installed version of RCCMD by setting the
##  INST_LANG variable to the desired country-code
##  (e.g.: el,en,es,de,fr,he,it,ja,ko,pt,ru,tr,zh_cn).
#INST_LANG=en
## Select the destination where the program should be installed
#USER_INSTALL_DIR=/usr/rccmd
## If the target System is a vSphere Management Assistant (vMA)
##  please provide the name or IP for the ESXi host.
#ESXI_HOST=127.0.0.1
## WebIf Settings
## --------------
## Here you can override default settings for access to the RCCMD WebIf.
## These settings are ignored, if the variable CHOSEN_INSTALL_FEATURE_LIST
## is set and does not contain the WebIf feature.
## In interactive install modes (gui, console) the installer will check, whether
## the chosen port is free to be used.
## Valid values are: 1-65535
## WEBIF_PORT=8080
## Valid protocols are: http, https
## WEBIF_PROTOCOL=http
```

Fig. 90: Content of the “installer.properties”

It is required to remove the hash mark prior of the variable INSTALLER_UI=silent. In addition the setting of the license key is required behind the variable GXLICENSEKEY=. Execute the “installRCCMD.bin” file as root.

Further installation options are: INSTALLER_UI=console for a non-grafical user input console or: INSTALLER_UI=gui to use the graphical installation (default).

4.3 Console Installation of RCCMD Installation of UNIX OS

A console installation is required, if your target operating system does not have a grafical interface for the execution of the “installRCCMD.bin”. This console installation works interactive and will ask for user input, defined in the installation script file “installer.properties”.

Note: This concerns the installation only. The configuration will be performed via editor into the „rccmd.cfg“ file.

For the activation of the console installation, it is required to remove the hash mark prior of the variable INSTALLER_UI= and to enter console. This is the interactive RCCMD installation onto the console. Execute as root the “installRCCMD.bin” file.

By the configuration you can change the language, to receive the right Tooltips! Please use the variable INST_LANG=de .

4.3.1 Example of a Console Installation

Adjust the file “installer.properties” accordingly like described above or execute the following command:

./installRCCMD.bin –i console

Select the desired **language** and note the **introduction**.

Confirm with „ENTER“.

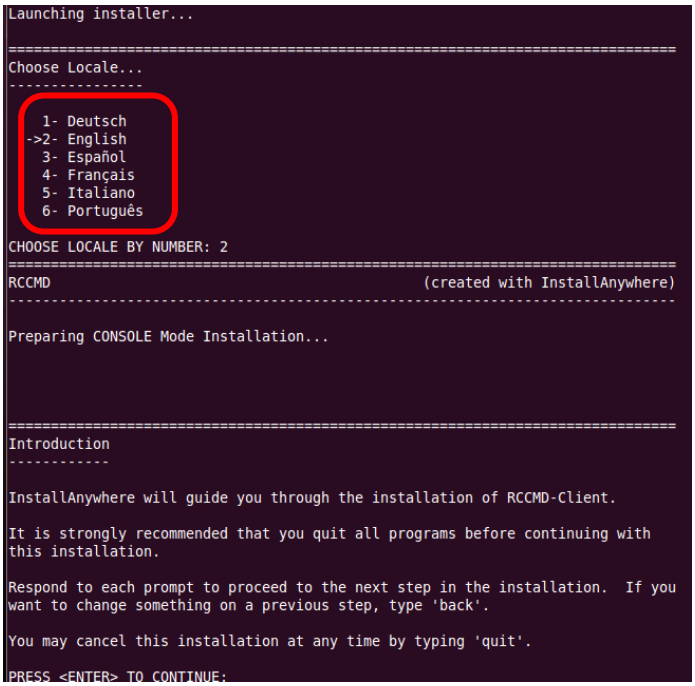


Fig. 91: Console Installation – Language Selection, Introduction

It continues with the **OS** and **platform** detection, the **RCCMD license key** and the **license contract**.

Confirm with „ENTER“.

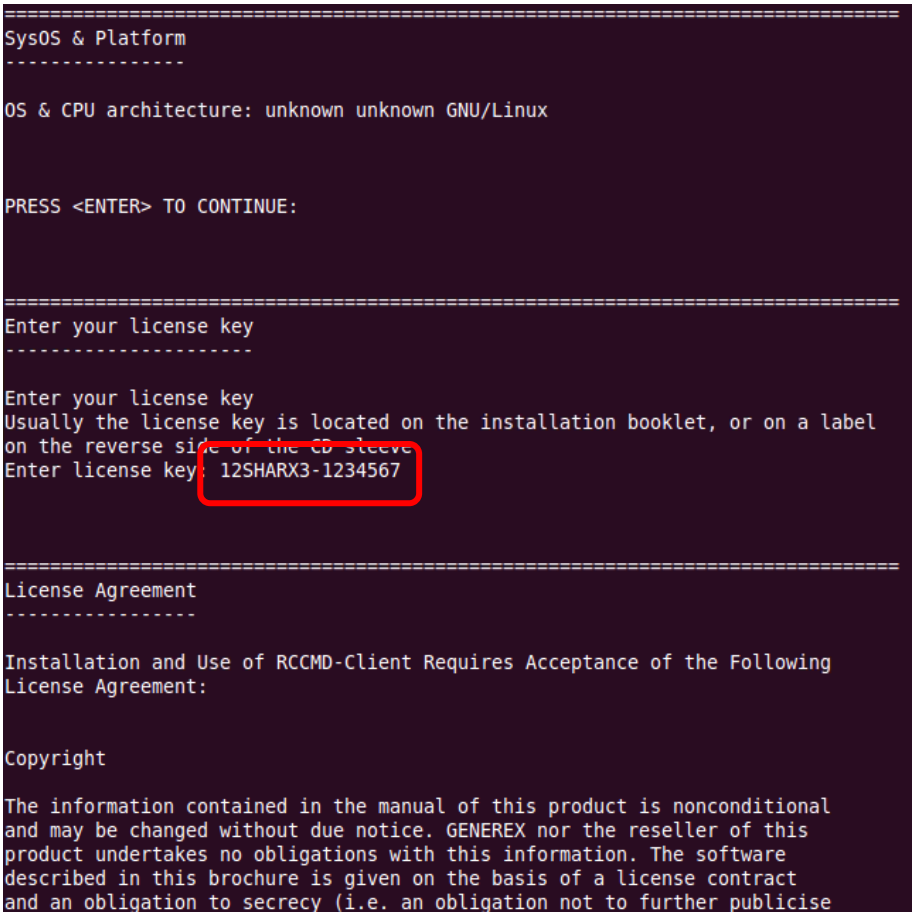


Fig. 92: Console Installation – OS Detection, License Agreement

Select the **features**, you want to install or press the “Enter” key, if you want to use them all.

Confirm with „ENTER“.

```
================================================================================
Choose Product Features
-----------------------

ENTER A COMMA_SEPARATED LIST OF NUMBERS REPRESENTING THE FEATURES YOU WOULD
LIKE TO SELECT, OR DESELECT. TO VIEW A FEATURE'S DESCRIPTION, ENTER
'?<NUMBER>'.  PRESS <RETURN> WHEN YOU ARE DONE:

    1- [X] RCCMD
    2- [X] WebIf
    3- [X] XMessage

Please choose the Features to be installed by this installer.:



================================================================================
Pre-Installation Summary
------------------------

Please Review the Following Before Continuing:

Product Name:
    RCCMD

Install Folder:
    /usr/rccmd

Product Features:
    RCCMD,
    WebIf,
    XMessage

Disk Space Information (for Installation Target):
    Required:  116,423,910 Bytes
    Available: 3,049,369,600 Bytes

PRESS <ENTER> TO CONTINUE:
```

Fig. 93: Console Installation – Features Selection

It continues with the selection of the RCCMD **automatic start**, WebIf protocol and port.

Confirm with „ENTER“.

```
Run RCCMD at System Boot?
-------------------------

Should the RCCMD be automatically started when the System boots?

  ->1- OK
    2- NO

ENTER THE NUMBER OF THE DESIRED CHOICE, OR PRESS <ENTER> TO ACCEPT THE
   DEFAULT:
```

Fig. 94: Console Installation – Autostart

Choose the protocol for the web interface.

Confirm with „ENTER“.

```
================================================================================
Set WebIf Protocol
------------------

This is the default protocol to access the RCCMD WebIf.
Select your preferred protocol here:

  ->1- http
    2- https

ENTER A COMMA-SEPARATED LIST OF NUMBERS REPRESENTING THE DESIRED CHOICES, OR
   PRESS <ENTER> TO ACCEPT THE DEFAULT:




================================================================================
Set WebIf Port
--------------

This is the default network port to acces the RCCMD WebIf.
Select your preferred port here:

Port: (DEFAULT: 8080):
```

Fig. 95: Console Installation – WebIf Selection

Please note, that it is required to **configure** the RCCMD Software and the required **firewall exceptions**.

Confirm with „ENTER“.

```
================================================================================
RCCMD configuration necessary
-----------------------------

It is necessary to configure RCCMD. Please use the web interface at
"http://<address of this computer>:8080".

Should you decide to run RCCMD with this default configuration RCCMD will
accept messages from any ip-address!
Please set one or more valid ip-addresses that are allowed to send (shutdown-)
messages to this RCCMD.

PRESS <ENTER> TO CONTINUE:



================================================================================
Required Firewall Exceptions
----------------------------

Required Firewall Exceptions.
Make sure following Ports are not blocked by any firewall:
Ports 8080 tcp (WebIf Server), if installed
Ports 6003 & 5769 tcp,udp (RCCMD)

PRESS <ENTER> TO CONTINUE:
```

Fig. 96: Console Installation – RCCMD Configuration required, Firewall Exceptions

Do you want to **run** RCCMD **now** ?

By pressing „**Enter**“you exit the installation.

```
================================================================================
RCCMD jetzt starten?
--------------------

Es wird empfohlen RCCMD im WebIf zu konfigurieren und von dort zu starten.
Zum manuellen Starten verwenden Sie: "/usr/rccmd/rccmdctl start" oder das
Webinterface.

Soll RCCMD jetzt gestartet werden?

  ->1- OK
    2- Abbrechen

GEBEN SIE DIE NUMMER DER GEWÜNSCHTEN KOMPONENTE AN, ODER DRÜCKEN SIE DIE
   EINGABETASTE, UM DIE STANDARDEINSTELLUNGEN ZU ÜBERNEHMEN:



================================================================================
Installation abgeschlossen
--------------------------

Herzlichen Glückwunsch. RCCMD-Client wurde erfolgreich im folgenden Verzeichnis
installiert:

     /usr/rccmd

DRÜCKEN SIE DIE EINGABETASTE, UM DEN INSTALLER ZU BEENDEN:
```

Fig. 97: Console Installation – RCCMD Start, Installation Complete

4.4 RCCMD WebInterface (from Version 4.2.0.0)

RCCMD provides its own web-interface from version 4.2.0.0 or higher. Therefore it is possible to configure and control RCCMD remotely. After the successful installation, your default web-browser of your OS starts automatically.

Enter your password and click on Login.

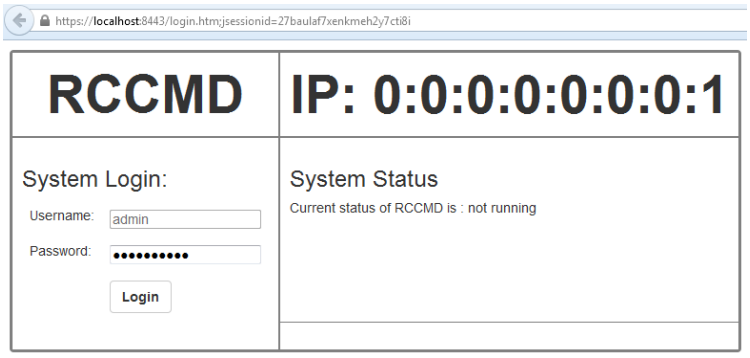


Fig. 98: RCCMD WebInterface

Menu **„Connections“:**
You can enter the **IP addresses** of the allowed RCCMD senders (CS121/CS141/UPSMAN) into the “Connections” menu. Click the “**Insert**” button to enter the IP address of the 1st ender. Click the “**Remove**” button, if you want to remove the already entered IP address. Click the “**Edit**” button, if you want to edit the entered IP address.

Attention: If you do not enter an address, then every server has the permission to send a shutdown command.

You can define under “**Protocol**”, if RCCMD should use **SSL certificates**. Enable the “**Reject expired SSL certificates**”, if you want to reject connections with expired certificates. Please take a look into chapter 6.6.1 for further information about RCCMD with SSL.

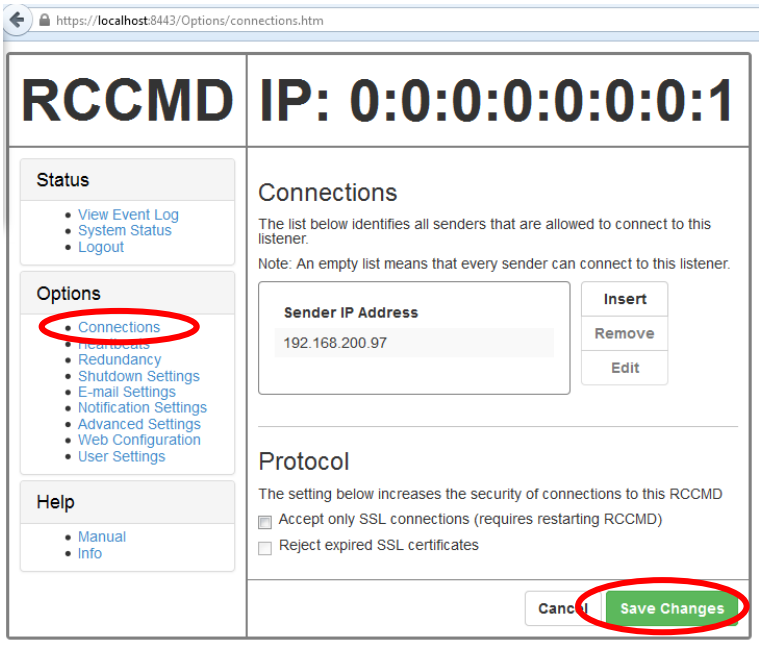


Fig. 99: RCCMD WebInterface – Connections

Click “**Save Changes**” before leaving this site to save your changes!

Menu **„Heartbeats“:**

You can enable the “**UPSMAN Alive Check**” feature into the menu “Heartbeats”. This check is a signal, that will be send to the CS121/CS141/UPSMAN via port 5769, if the UPSMAN service still got UPS data. If not, the script file “alive.bat” will be executed, which will trigger an accordant pop-up message.

The feature “**by the use of CS121/UPSMAN Traps**” provides UPSMAN/RCCMD/UNMS messages, which will display the UPS status as message. If enabled, this feature will trigger a message, if the UPS status of the UPSMAN/RCCMD servers has changed.

The feature “**by polling CS121/UPSMAN every x seconds**” provides the pure signal polling without receiving UPS data or rather messages.

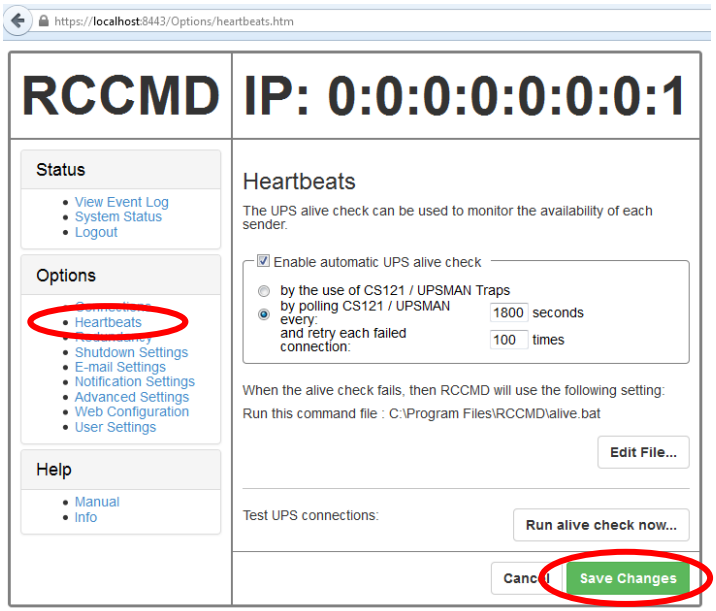


Fig. 100: RCCMD WebInterface – Heartbeats

The polling rate (default 1800 seconds) defines the polling of the UPSMAN service, connection retries (default 100) means after 100 unsuccessful connection tries an alarm will be triggered.

You can test the UPS connection, if you click the “**Run alive check now…**” button (the port 5769 will be tested).

Click the “**Save Changes**” button prior of the leaving of this site to save your changes.

Menu **„Redundancy“**:

You can enable the **redundancy management feature** into the menu “Redundancy”. The **redundancy level** defines the number of redundant senders in the redundancy group. This means, that level 1+ senders must have sent a shutdown signal before this RCCMD starts its shutdown sequence.

When redundancy suppresses a shutdown, then RCCMD will trigger the “suppressed.bat”. You can edit this file, if you click the “**Edit file…**” button.

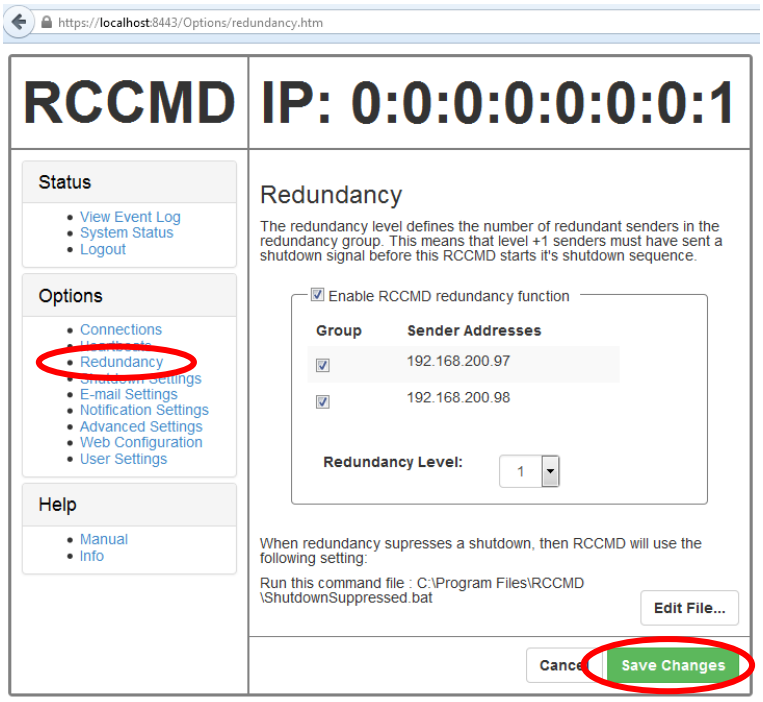


Fig. 101: RCCMD WebInterface – Redundancy

Please note, that it is required to configure a reset of the redundancy alarm on the sender (CS121/CS141/UPSMAN). You can use the function „**Send RCCMD cancel shutdown**“, to discard a previously sent shutdown automatically. If a shutdown was suppressed, because of the existing redundancy at this point of time, but the problem was solved at the UPS intermediate, you can reset the shutdown with the function „**Send RCCMD cancel shutdown**“. The client, which received the shutdown, will be encouraged to reset it.

Please take a look into chapter for further information about **RCCMD with redundancy**.

Click the “**Save Changes**” button prior of the leaving of this site to save your changes.

.

Menu **„Shutdown Settings“:**
You can change or rather extend the shutdown sequence into the “Shutdown Settings” menu.

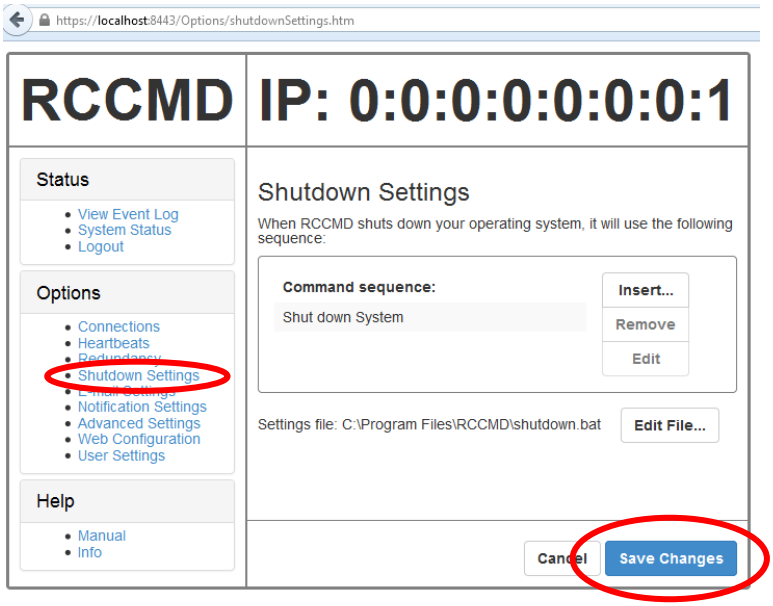


Fig. 102: RCCMD WebInterface – Shutdown Settings

Click the “**Save Changes**” button prior of the leaving of this site to save your changes.

Menu „**Notification Settings**“:
You can change or rather extend the **default bat files** for E-Mail, Message and Execute, if you click the “Edit File…” button.

Click the “**Save Changes**” button prior of the leaving of this site to save your changes.

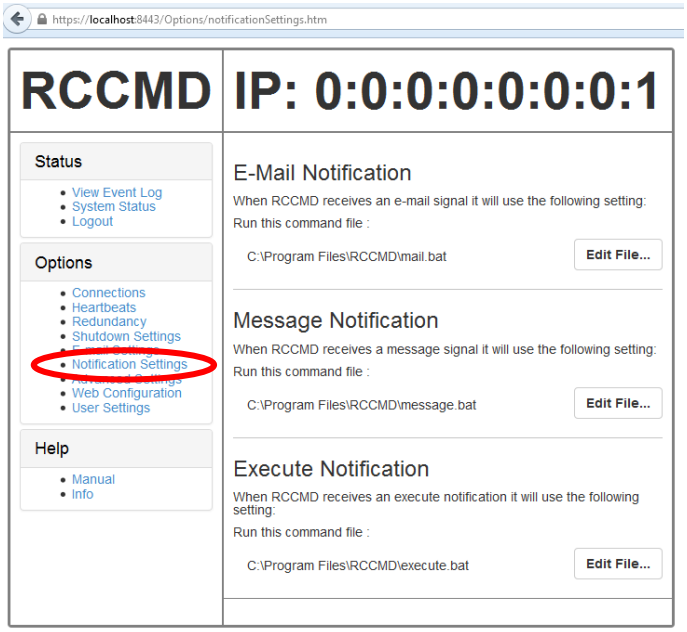


Fig. 103: RCCMD WebInterface – Notification Settings

Menu „**Advanced Settings**“:
You can define the **maximum size of the event logfile** into the menu “Advanced Settings”, where the overwriting of older entries will start, the **RCCMD bindings for the IP address**, the RCCMD listener **TCP port** and the RCCMD **Tray Message Port**, which will be used for the RCCMD messages.

Click the “**Save Changes**” button prior of the leaving of this site to save your changes.

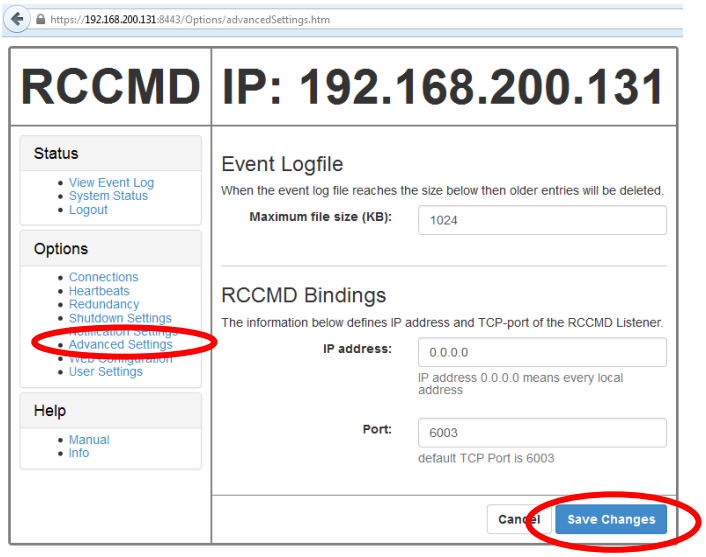


Fig. 104: RCCMD WebInterface – Advanced Setting

Menu „**Web Configuration**“:
You can change the default password for the user “admin” into the menu “Web Configuration”. In addition you can disable the **HTTPS protocol**, if you just want to use the HTTP protocol. The RCCMD version 4.2.3.0 or higher provides the feature of changing the **default ports** for HTTP and HTTPS..

Click the “Save Changes” button prior of the leaving of this site to save your changes.

Afterwards you have to restart the RCCMD service!

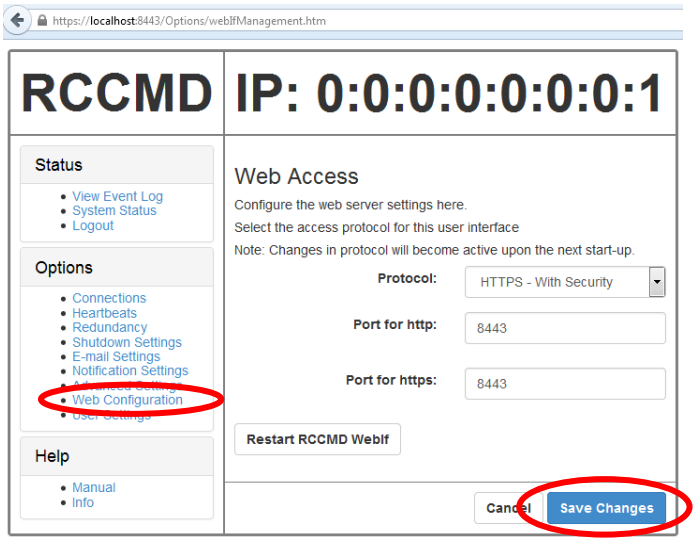


Fig. 105: RCCMD WebInterface – Web Access

„User Settings“ menu:
Here you can change the default password for „admin“.

Afterwards you have to restart the RCCMD service!

Click the “Save Changes” button prior of the leaving of this site to save your changes.

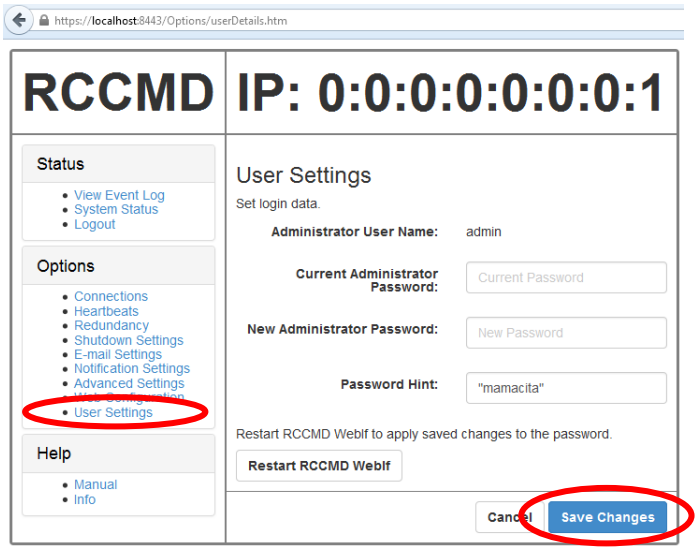


Fig. 106: RCCMD WebInterface – User Settings

Menu **„Status, View Event Log“**:
You can see the **logging of the events** into the menu “View Event Log”.

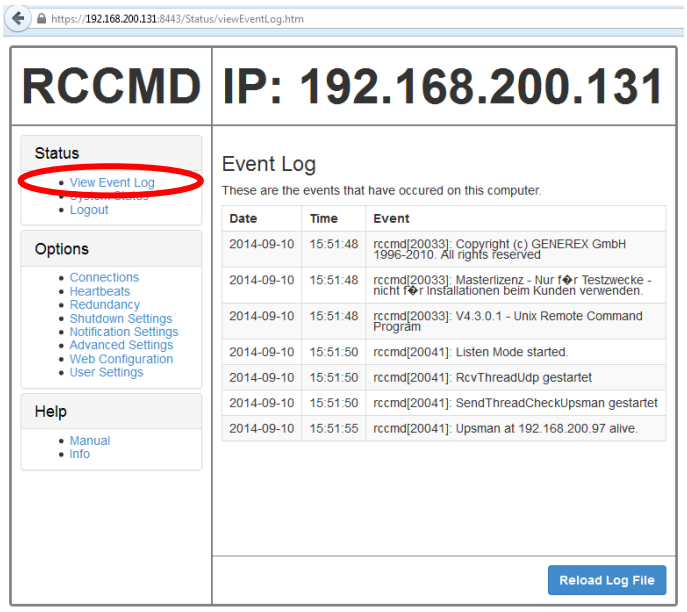


Fig. 107: RCCMD WebInterface – Event Log

Menu **„Status, System Status“:**
You can check the current **status** of RCCMD into the menu “Status, System Status”, **update** the status and restart or rather stop/start the RCCMD service.

„ Logout“:
Here you can logout when you have finished the configuration.

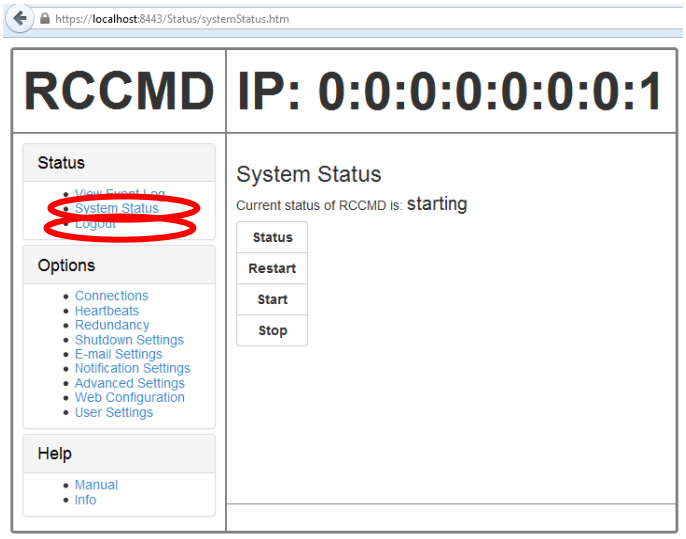


Fig. 108: RCCMD WebInterface – System Status

Menu „**Help**“:
You can open the RCCMD user manual into the menu “Help” ad you can follow the link to www.generex.de.

Click on Info to view the installer version.

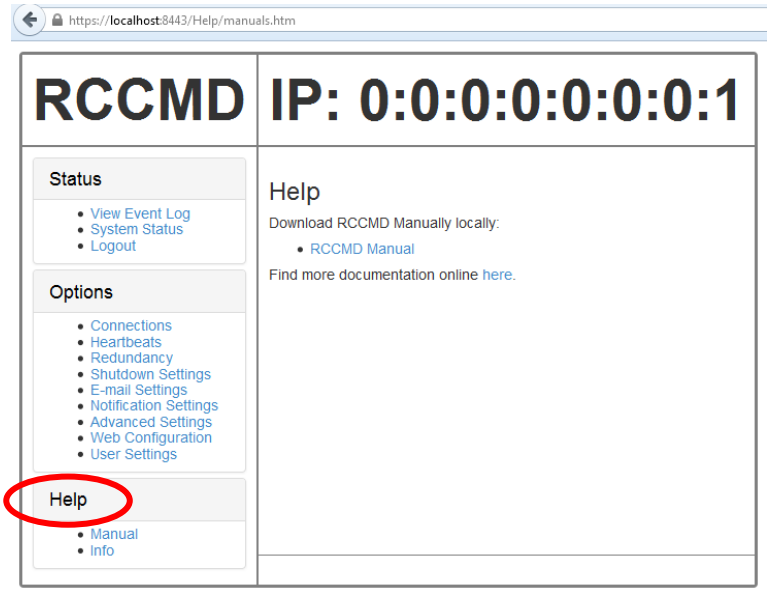


Fig. 109: RCCMD WebInterface – Help

4.5 RCCMD WebInterface Remote Access

RCCMD provides its own web-interface from version 4.2.0.0 or higher. Therefore it is possible to configure and control RCCMD remotely. Please note, that the firewall port 8443 TCP is enabled. Enter the following into a web-browser, to connect to a workstation, where RCCMD is running:

https://IP address of the RCCMD client: 8443

Now you can configure RCCMD remotely.

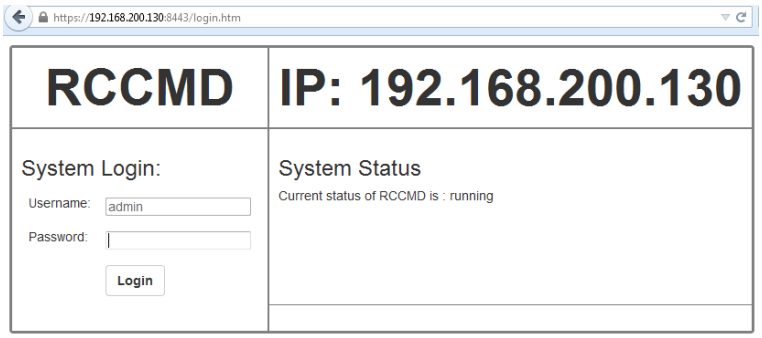


Fig. 110: RCCMD WebInterface – RemoteAccess

4.6 Automatic Reset of the Redundancy Alarm

You can use the function „**Send RCCMD cancel shutdown**“, to discard a previously sent shutdown automatically. If a shutdown was suppressed, because of the existing redundancy at this point of time, but the problem was solved at the UPS intermediate, you can reset the shutdown with the function „**Send RCCMD cancel shutdown**“. The client, which received the shutdown, will be encouraged to reset it.

This command can be set individually into your CS121/CS141, UPSMAN or BACS WEBMANAGER Events/Alarms configuration, but makes sense only, if the event, which will send the command, is true, if the UPS is back in normal condition. For this the events „**POWER RESTORED**“, „**BATTERY LOW OFF**“, „**UPSMAN STARTED**“ and „**GENERAL ALARM OFF**“ are suitable, if they are provided from your UPS into the CS121/CS141. The job „**Send RCCMD cancel shutdown**“ would be set into these all-clear events, so that e. g. at restart of the UPS, the event „**UPSMAN STARTED**“ would reset the accordant RCCMD client automatically.

Alternative: Should the job „**Send RCCMD cancel shutdown“** not be present into your CS121/CS141, UPSMAN or BACS WEBMANAGER, you can use the job „**Send RCCMD shutdown to remote client**“ or rather „**Send RCCMD execute to remote client**“ alternatively.

The parameter „**WAKEUP**“ got the same function like the „Send RCCMD cancel shutdown“ and resets the redundancy alarm of a RCCMD Client into initial state. For this the events „**POWER RESTORED**“, „**BATTERY LOW OFF**“, „**UPSMAN STARTED**“ and „**GENERAL ALARM OFF**“ are suitable too, to configure the function „**Send RCCMD command to remote client**“ with the „**WAKEUP**“ command.

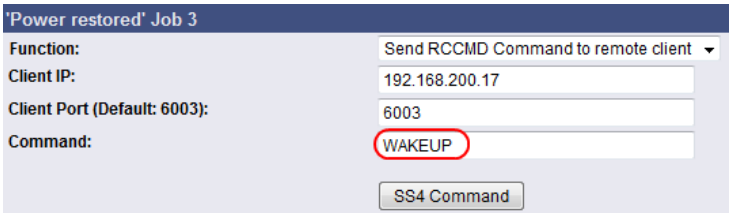


Fig. 111: CS121/CS141 Configuration „WAKEUP“ Command

Menu „**CS121/CS141“**:
Click into the CS121/CS141 menu “**Events/Alarms**” onto “Power restored” and add a new job. Select the function “**Send RCCMD command to remote client**”, set the accordant **IP address** of the RCCMD client and enter the command “**WAKEUP**”.

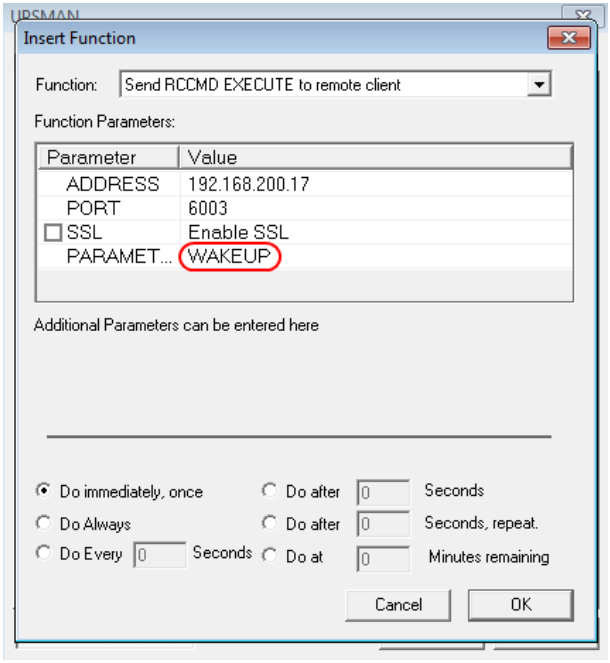


Fig. 112: UPSMAN Configuration „WAKEUP“ Command

Configuration **„UPSMAN“:**
Click into the UPSMAN configuration the buttons “**Advanced Users**”, “**Events**”, “**Power restored**” and “**Insert**”. Add the function “**Send RCCMD execute to remote client**”, set the accordant **IP address** of the RCCMD client and enter the command “**WAKEUP**”.

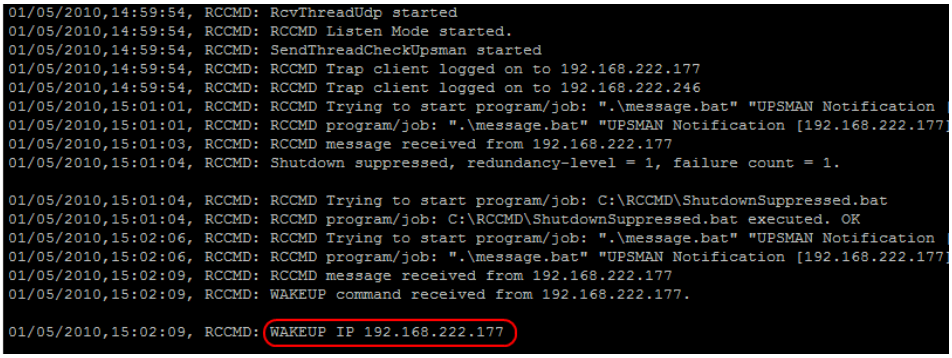


Fig. 113: „WAKEUP“ Befehl im RCCMD Log

4.7 RCCMD with SSL for UNIX

The *Secure Sockets Layer* (SSL) protocol is a cryptographic protocol that provides security and data integrity for communications over TCP/IP networks..

Configuration menu **„SNMP Adapter“:**
Use your Web-browser to navigate to the address of your UPS Web-Manager. Click the “**Network & Security**” configuration button and enable the SSL network feature “**Use RCCMD SSL**”.

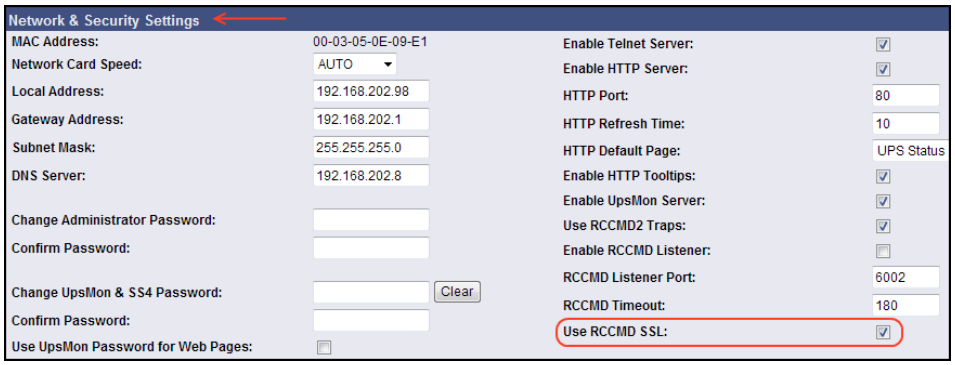


Fig. 114: RCCMD SSL Settings

Menu **„Timeserver“**:
The SSL network feature requires correct time settings, so it is required to configure a timeserver. Click the „Timeserver“ configuration button and enter the **IP address** of at least one timeserver.

Click the „**Apply**“ button.

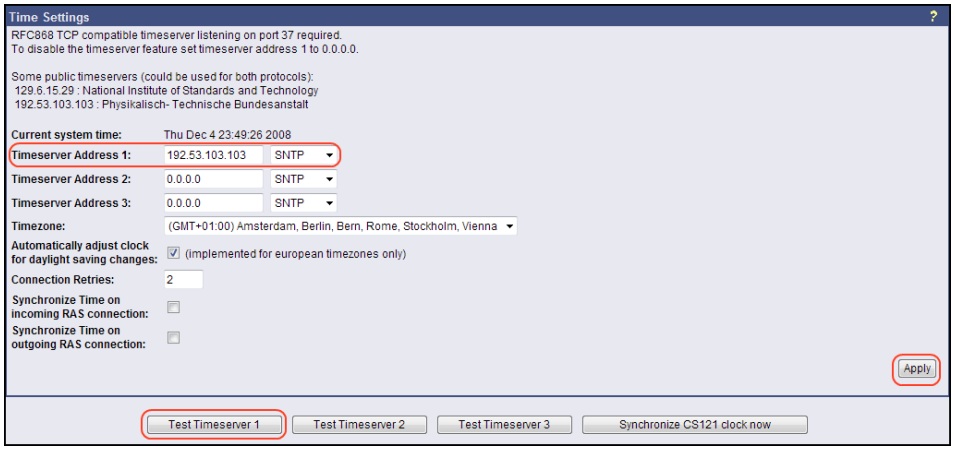


Fig. 115: Timeserver Settings

Menu **„Save Configuration“**:
Click the „Save Configuration“ button and the „**Save, Exit & Reboot**“ button to confirm your settings.

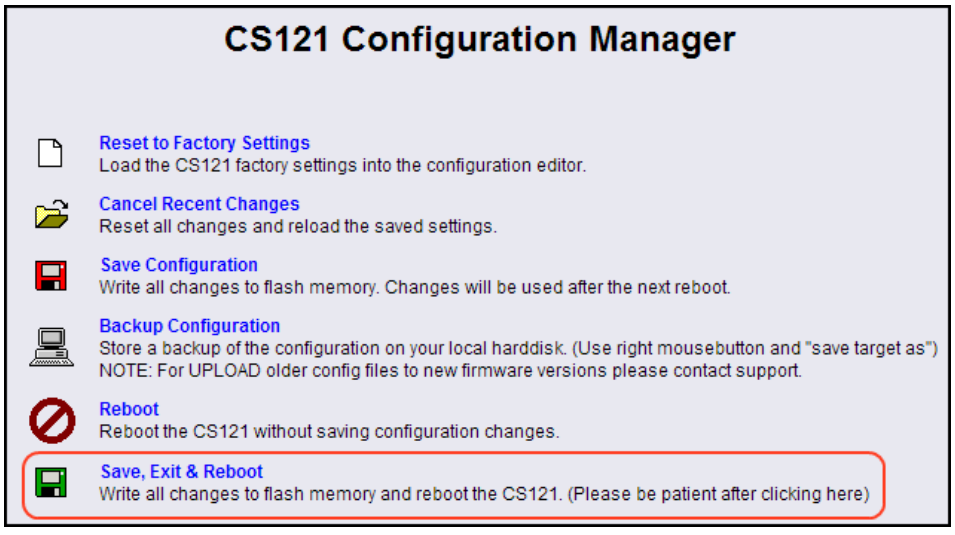


Fig. 116: Settings Confirmation

Menu **„RCCMD Web Configurator“**:
Start the RCCMD Web Configurator again and enable the **SSL network feature**.

If you want to accept expired certificates, please enable the accordant function “**Reject expired SSL certificates**”.

Restart RCCMD with the „Restart RCCMD“ Button in the System Status.

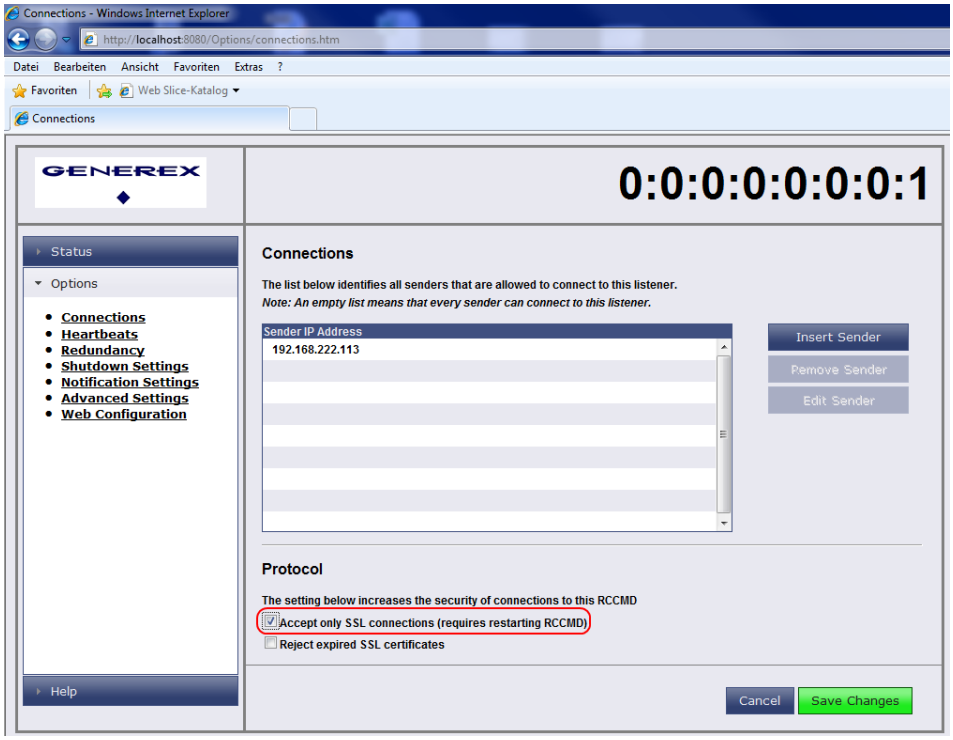


Fig. 117: SSL Configuration

4.7.1 RCCMD with own SSL certificates

In this chapter we will describe, how to use an own SSL certificate with RCCMD, e. g. OpenSSL (http://www.openssl.org):

Be your own certificate authority (CA)

Using OpenSSL it is quite simple to become your own CA. Just run:

```
CA.pl –newca
```

Done! Just ensure, that you select a useful CN (common name)!

Create your RCCMD certificate

You need to create your certificate for RCCMD now. As it will use it for verification, it should contain the same useful common name (CN), that you selected for the CA. The private key must not be encrypted to let the RCCMD Client (service) start without trouble. Therefore we use the “–nodes” option and the “-newreq” command:

```
CA.pl –newreq –nodes
```

Sign with your CA:

```
CA.pl –sign
```

Now create an empty filed named “rccmd.pem“ and copy the cert information of “newcert.pem” (rccmd certificate), “newkey.pem” (private key) and “cacert.pem” (CA) into it. Please note, that the exact copying is required to use it without trouble!

Use your own RCCMD certificate

Do the following steps at the RCCMD Client and every sender (e. g. UPS Web Manager):

- Backup the existing “rccmd.pem”
- Replace the existing “rccmd.pem” with your own
- Restart the RCCMD Client
- Restart the RCCMD Sender

4.8 Alternative RCCMD Configuration with Editor

It is required to perform the configuration via editor, if you do not have a graphical interface. The configuration file is the “rccmd.cfg” and is located into the “/usr/rccmd” folder (default). The file contains the description of the single configuration parameters. Please take a look into the following example of the “rccmd.cfg” file and change the settings to your installation:

```
########################################
# RCCMD Configuration
########################################
# Bind on Interface
# Defines on which interface we listen for incoming commands
# Default: 0.0.0.0 (All possible interfaces on this host)
ListenAddress=0.0.0.0
# Listen on Port
# Defines on which interface port we listen for incoming commands.
# Default: 6003
ListenPort=6003
# Enable UDP
# Defines if we should listen for rccmd (UDP) broadcasts
# Default: true
ListenUDP=true
# Access Control List
# A list of valid sender addresses, only its members can connect to us.
# Seperate IP addresses with a space, e.g.: "192.168.0.1 192.168.0.2".
# Default: <empty> (Everyone is allowed to connect to us)
AllowedAddresses=
# Alive Check
# Enable Alive Check
# Defines if we should perform UPSMan alive checking.
# Default: false
AliveEnabled=false
# Alive Check Rate
# Defines the interval of UPSMan alive checking, in seconds.
# Default: 1800
AliveInterval=1800
# Alive Retry Rate
# Defines the number of UPSMan alive checking retries, in case of problems.
# Default: 0
AliveRetries=5
# Alive Check Group Members List
# A list of UPS device addresses that should be checked periodically.
# Seperate IP addresses with a space, e.g.: "192.168.0.1 192.168.0.2".
# Default: <empty> (No alive checking)
AliveAddresses=
# Alive Program
```

```
# Full path to script that is executed when an alive check fails.
# Default: rccmd_notalive.sh
AliveProg=
# Redundancy Mode
# Enable Redundancy
# Defines if we should operate in redundancy mode.
# Requires an enabled <Alive Check> configuration.
# Default: false
RedundancyEnabled=false
# Redundancy Group Members List
# A list of redundancy group member addresses, must be also in <AliveAddresses>.
# Seperate IP addresses with a space, e.g.: "192.168.0.1 192.168.0.2".
# Default: <empty> (No redundancy available)
RedundancyAddresses=
# Redundancy Level
# Defines how many of the <RedundancyAddresses> are redundant.
# Shutdown is executed when the number of shutdown requests exceeds this number.
# Default: 0 (No redundancy available)
RedundancyLevel=0
# Enable Redundancy Script
# Defines if we should NOT execute a script when redundancy suppresses a shutdown.
# Default: false.
RedundancyBatchSuppress=false
# Redundancy Script
# Full path to script that is executed when redundancy suppresses a shutdown.
# Default: ShutdownSuppressed.sh
RedundancyBatchFile=
```

If no entries are changed in this default rccmd.cfg file, all incoming RCCMD commands will be executed from any sender and use the default shutdown scriptfile “rccmd_shutdown.sh”.

4.9 Older RCCMD Configuration on UNIX OS

Menu „**Addresses**“:
Add the **IP address** of the RCCMD server, which is allowed to send a shutdown to this client.

Attention: If you do not enter an address, then every server has the permission to send a shutdown command. If more than one CS121/CS141 or UPSMAN is existent, thus a redundancy situation, you need to enter more than one address as authorized sender.

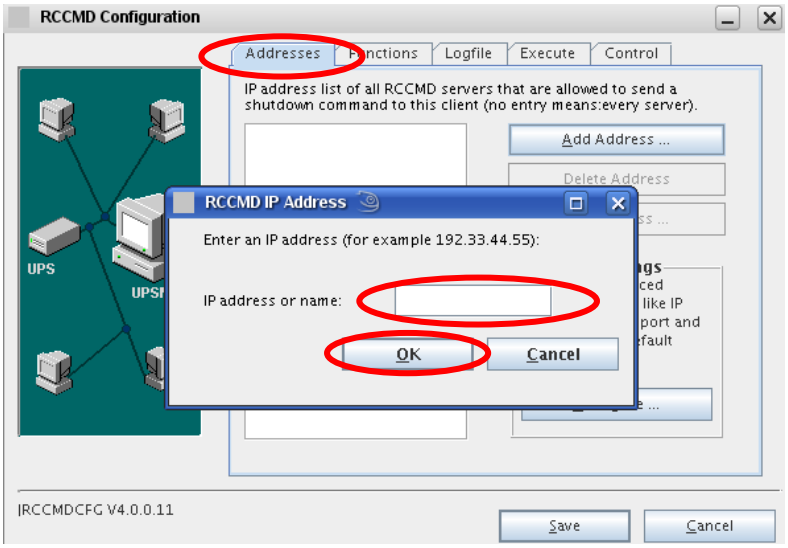


Fig. 118: Configuration – RCCMD Sender IP Address

Click the „**OK**“ button“.

Menu „**Functions**“:
If you want to use the “UPSMAN alive checking” (recommended), check the “**Enable connection check**” box. Alive check is a signal, send out to the UPSMAN or CS121/CS141 on port 5769 to check if the UPSMAN has still UPS data – or not. If this fails, the scriptfile rccmd_execute.sh will be executed which causes a messagbox coming up. The polling rate (default 30 min.) defines the polling of the UPSMAN service, connect retries (default 5) means after 5 unsuccessful connection tries an alarm will be triggered.

The function “**Use RCCMD Traps**” enables UPSMAN/RCCMD/UNMS traps, which show the UPS status as a trap message. If activated it will display a local message when the UPS status of the UPSMAN/RCCMD server changes.

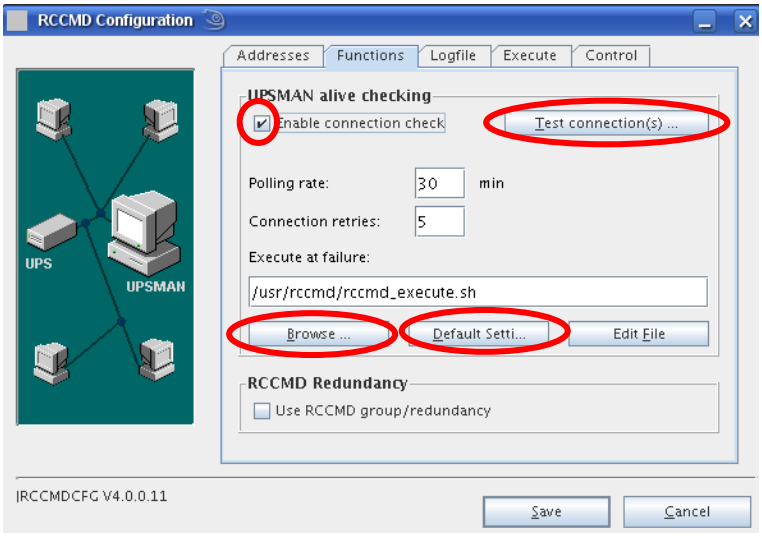


Fig. 119: Configuration – Functions

If you click the “**Test connection(s)…**” button, the UPSMAN alive checking of the entered IP addresses will start (port 5769 will be tested).

If you click the „**Browse...**“ button, you will get a selection of the default sh-files.

By clicking „**Default Setting**“ you will attain the „rccmd_execute.sh“.

By encounting an error with UPSMAN Alive Check you can configure an executable file or edit the default file.

At UPS installation RCCMD offers **redundancy management functionality** as follows:

Every UPS must be equipped with a CS121/CS141 or UPSMAN software computer. When ticking the box "**Use RCCMD group/redundancy**" – you are guided to a menue where you can choose which CS121/CS141/UPSMAN are supplying this RCCMD client. E.g. if 4 CS121/CS141/UPSMAN are installed into 4 UPS – than each may send a shutdown signal to this RCCMD client.

Click the „**Save**" button".

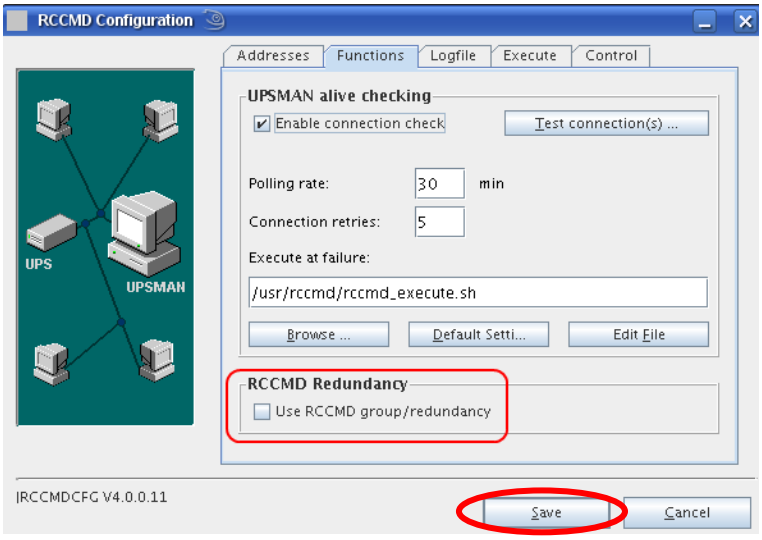


Fig. 120: Configuration – RCCMD Redundancy

The redundancy level defines how many shutdown signals are required to execute the shutdown.bat file. As long as this number is not exceeded, the RCCMD client will react on such a shutdown signal only with a messagebox "Execute command when redundancy suppresses a shutdown" box. This will show a message to inform the user that there has been a shutdown signal from one of the UPS in the group, but since all other UPS are still reading OK – or did not yet send any shutdown, the shutdown is suppressed. 3 shutdown signals would create messages in the above example (redundancy level 3) only, just the 4th signal would initiate the shutdown.

Menu „**Logfile**":
You can configure the **log file** size and edit the executing sh-files.

Click the „**Save**" button".

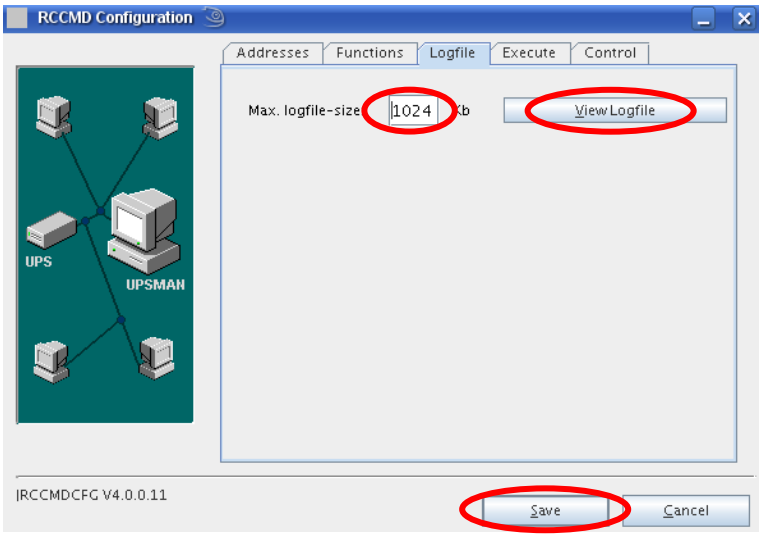


Fig. 121: Configuration – RCCMD Log File

Menu „**Execute**":
If you click the „**Configure...**" button, you will be able to enter the **mail settings** and to use the mail function of RCCMD.

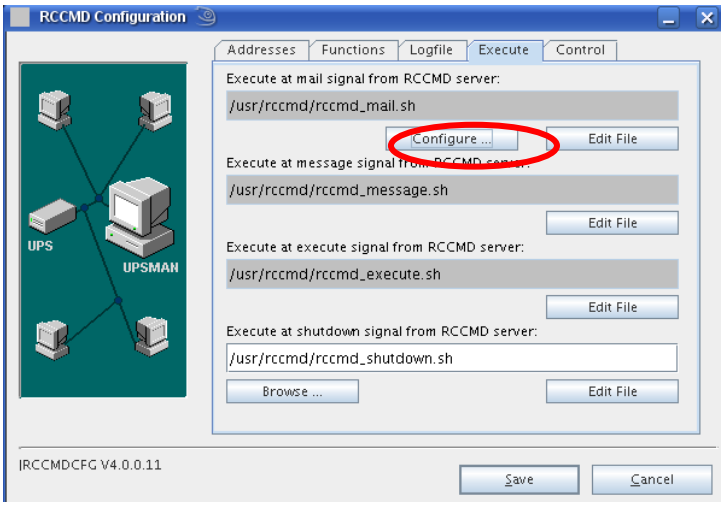


Fig. 122: Configuration – RCCMD Execute

Click the **“Save**” button.

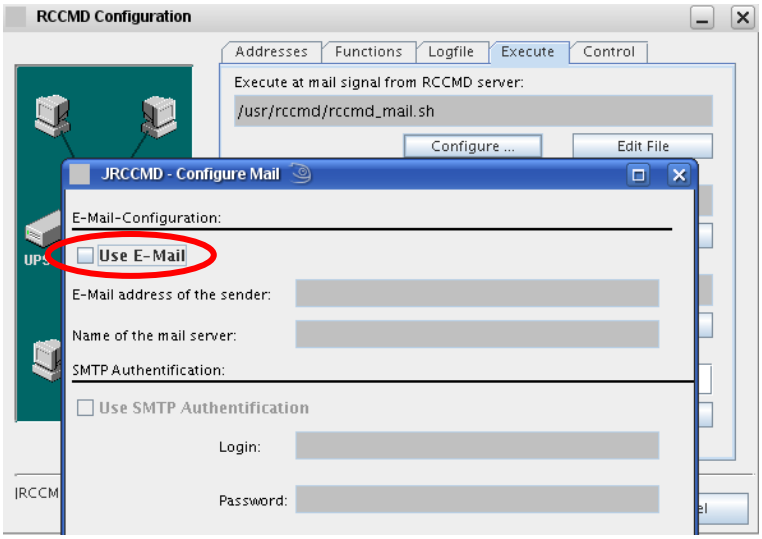


Fig. 123: Konfiguration – RCCMD Configure Email

The RCCMD version 4.0.2.0 provides a grafical configuration of the **shutdown sequence**.

Click the „**Configure**“ button to enter the shutdown sequence settings.

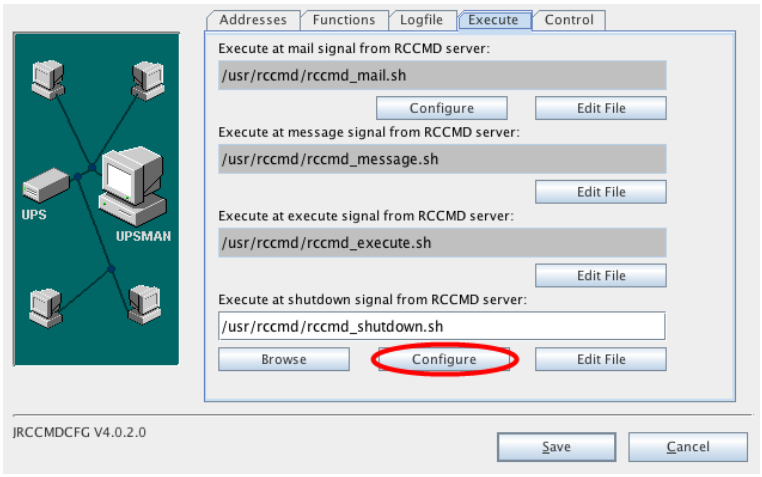


Fig. 124: Configuration – RCCMD Shutdown.sh

The following commands are available:

RCCMD shutdown relay: Relays RCCMD shutdown command to another workstation. Enter the IP address or the hostname of the remote station you want to shutdown.

Wait seconds...: Waits a duration in seconds until the next command will be executed.

Restart System: Ends your session, shuts down the system and restarts it.

Shutdown System: Ends your session and shuts down the system, so that you can safely turn off the power.

Click the „**Save**“ button“.

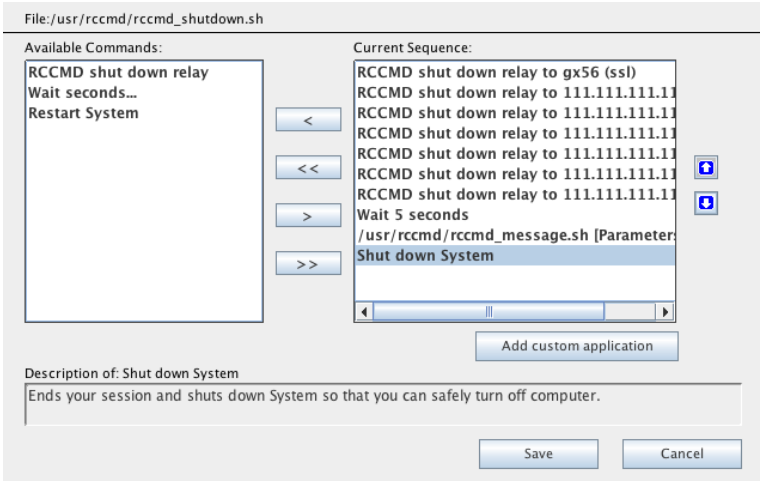


Fig. 125: Konfiguration – RCCMD Shutdown Sequenz

Menu „**Control**“:
Click „**Control**“ to get to the following functions::

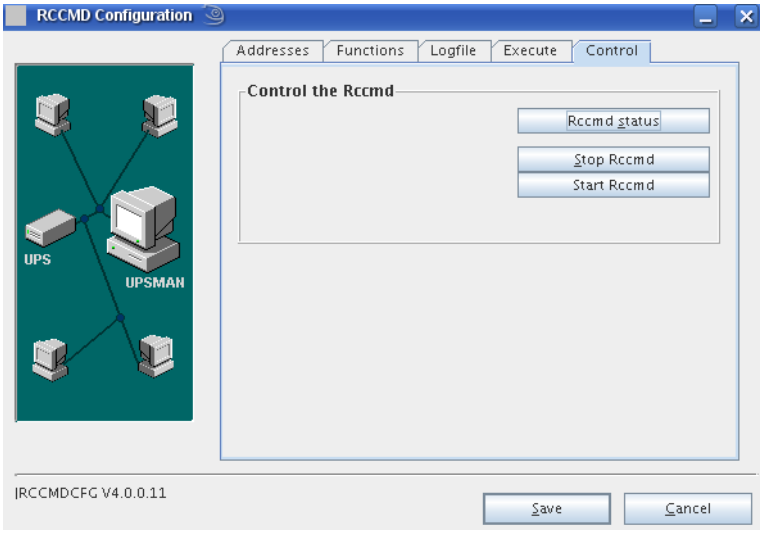


Fig. 126: Configuration – RCCMD Control

4.9.1 RCCMD Client as Relay Station

If you need to reach a bigger amount of receivers, it is required to define the CS121/CS141 as relay station. The receiver must be defined, if receiving a RCCMD signal, that it will start a script, which will send further RCCMD signals. The workstation is receiver and sender at the same time and thus an important connection in the UPS monitoring. The usage of a RCCMD client as relay station makes the monitoring of more than hundred RCCMD clients as easier as the configuration of the CS121/CS141 via web-browser. Furthermore the web-browser event configuration got a limit, so that it is required to use the relay function, if the amount of jobs is more than 50 per event at the CS121/CS141.

The following steps are required for the configuration of the relay function:

- Open the file “rccmd_shutdown.sh” with an editor.
- Add prior of the shutdown of the workstation (“shutdown –h now”) the relay calls, e. g. the call of the included “send_shutdown.sh”.
- Add the desired IP addresses or rather the DNS names:

```
./send_shutdown.sh -a 10.10.10.10 -a 10.10.10.11 -a 10.10.10.12
```

- Save the settings of the “rccmd_shutdown.sh”.

The RCCMD version 4.0.2.0 provides a grafical configuration of the shutdown sequence.

Click on „**Configure**“to open the Shutdown sequency.

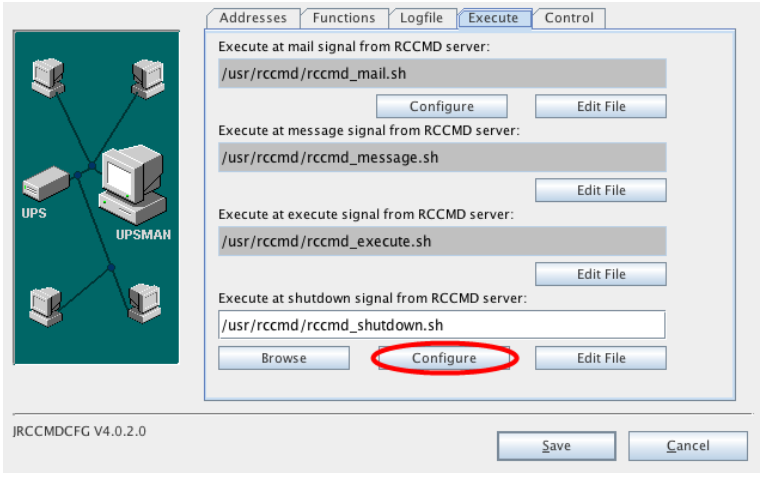


Fig. 127: Configuration – RCCMD Shutdown.sh

Tag the “**RCCMD shutdown relay**” into the “Available Commands” window and click the “**>**” button, to **add** this function into the “Current Sequence”..

If you want to **remove** single IP addresses, mark the line with its desired IP address and click the “**<**” button.

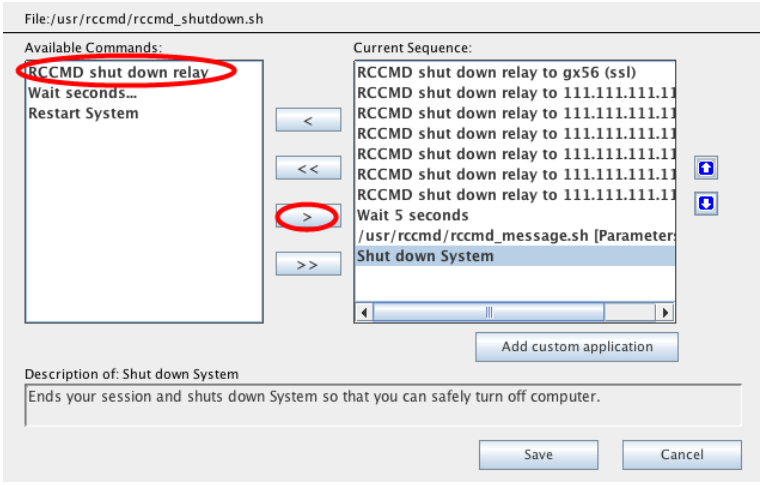


Fig. 128: Configuration – RCCMD Shutdown Sequenz

The following panel will appear, in which you can enter the desired **IP address** range or **hostname**.

Additionally you can enable the **SSL** function.

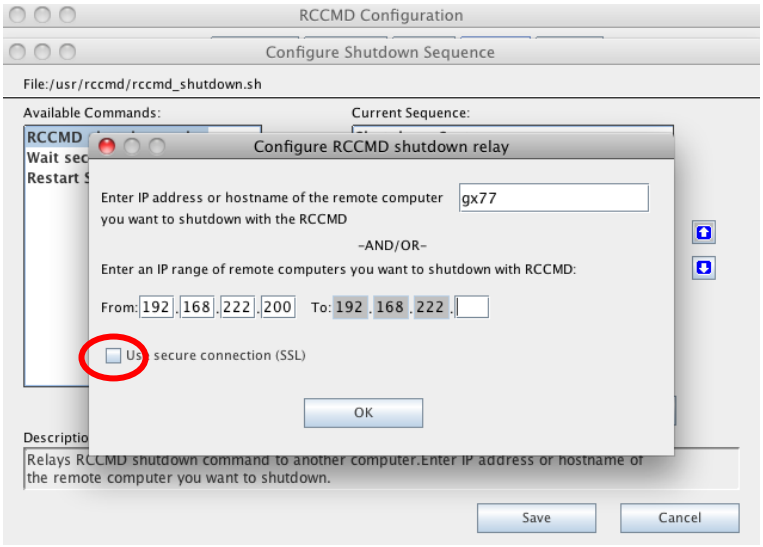


Fig. 129: Konfiguration – RCCMD Relay Konfiguration IP-Adressen-Bereich

4.10 UNIX RCCMD Configuration with CURSES Library

Note: The contents of 'rccmd.cfg' are vital to system security. It should be writeable only for the System User 'root'.

Rccmd V2 running in 'Listen' mode may be configured using a configuration file. By default rccmd will look for a file named 'rccmd.cfg' in its startup directory (usually '/usr/ups'). This file may be generated using rccmd_conf. Rccmd_conf is a small curses-based utility which runs on the console or a terminal or a terminal-emulation under the X Window System (e.g. xterm).

Note: This section does not apply to rccmd V1 for Unix, in addition it only applies to rccmd running in 'Listen' mode. This tool “rccmd_conf” is not supported by newer operating systems. If you try to start on not supported OS, you will receive an error message about missing “curses” library.

Run rccmd_conf:

$ su -

Password:

cd /usr/ups

./rccmd_conf

Bedienungshinweis:

To switch between menu entries press [**Tabulator**] or use Arrow keys **[↑] [↓]**

To confirm an entry, press **[Enter]**

To go back to default settings choose **[Default]**

To save entries choose **[Ok] / [Save]**

To leave a menu entry, choose **[Exit] / [Cancel]**

If 'rccmd.cfg' does not exist (e.g. if you run rccmd_conf for the first time) the following notice will be displayed:

Select the „**Create**“ button.

Press „**Enter**“.

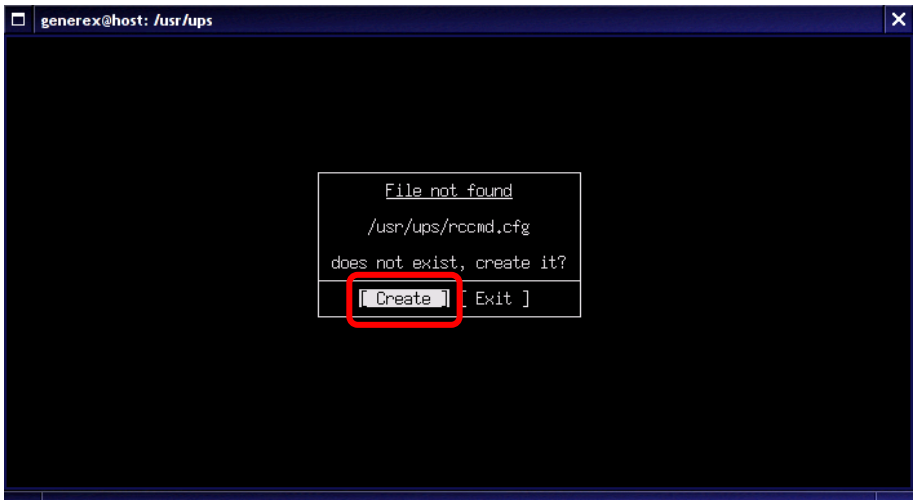


Fig. 130: Making the Configuration File

If you created 'rccmd.cfg' or if the file existed already rccmd_conf will switch to its main configuration menu.

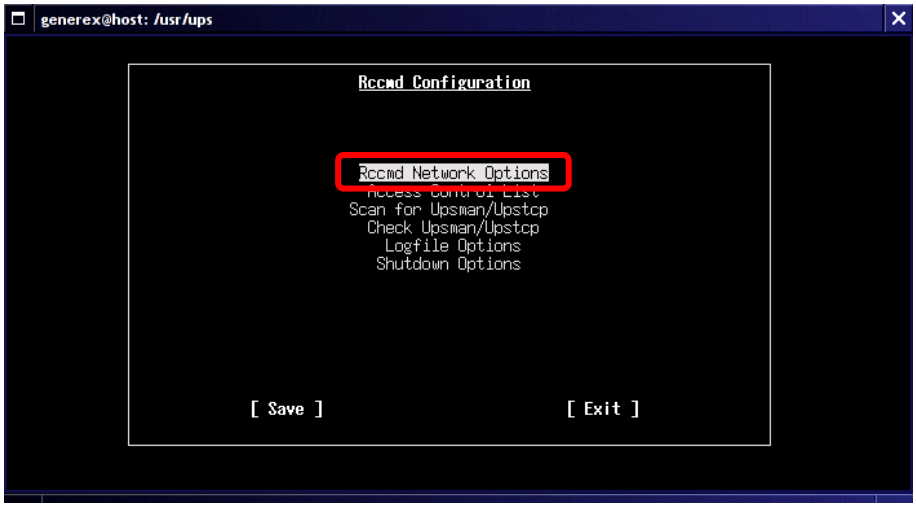


Fig. 131: RCCMD Configuration Menu UNIX

It is not necessary to work from top to the bottom, you may configure the menu items in any order. In fact it is not necessary to configure anything at all, if you just select [save] 'rccmd.cfg' will be written with default values sufficient to run rccmd. To use all features of rccmd and/or improve security it is however strongly suggested to customize 'rccmd.cfg'.

Configuration**"RCCMD Network Options"**
In this screen you may configure network related options of the rccmd listener.

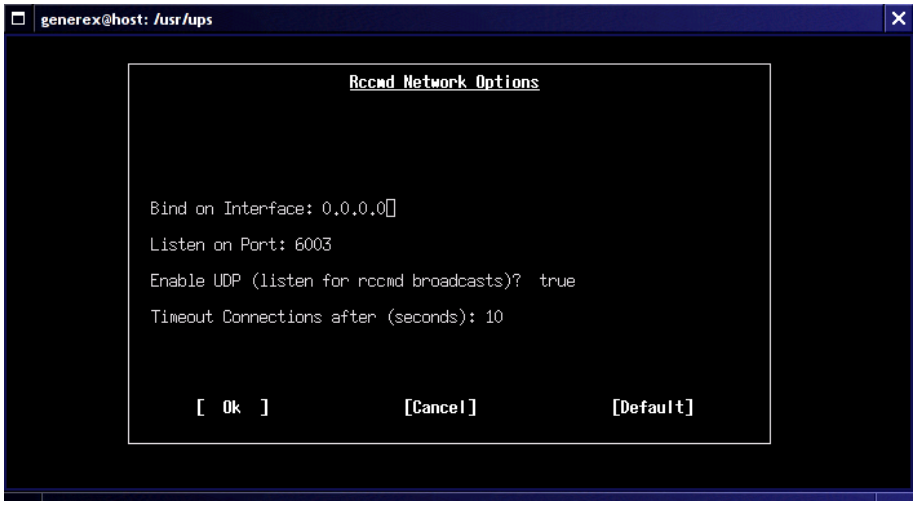


Fig. 132: RCCMD UNIX Network Options

Bind on Interface: This option tells rccmd on which network interface it binds its main tcp listen socket. You may enter any valid IP address your host can be reached.

The default value for this option is 0.0.0.0, this is a working value, it means 'listen on all possible interfaces of this host'. If your host has a dial up connection to the internet you may want to change the default, to ensure rccmd will not be connected from the internet. In this case you will enter the primary IP address of the host rccmd listener is running on.

Example:
Your company runs a private network in the 192.168.1.0/24 address range. The host rccmd listener is running on is assigned the IP 192.168.1.9. You may enter 192.168.1.9 for "Bind on Interface", to ensure only host from the private network can connect to rccmd.

Listen on Port: This is the port rccmd will listen to. Allowed values range from 1 to 65535 (inclusive). The default is 6003. If you change the port of the rccmd listener you will also have to switch the port of the rccmd sender in order to enable a connection. It is normally not necessary to change this setting.

Enable UDP: If this opion is enabled rccmd will open an UDP Listen Socket in addition to the TCP Socket. This allows the rccmd listener to receive rccmd broadcasts. Possible values are 'true' and 'false'. The default is "true".

Timeout: Timeout for TCP connections. The default is 10 seconds. It is normally not necessary to change this setting.

Configuration
"Access Control List"
"Access Control List" contains a list of **valid sender addresses**. A valid sender address is the IP address of an rccmd sender that is allowed to connect to the rccmd listener. Initially the list is empty.

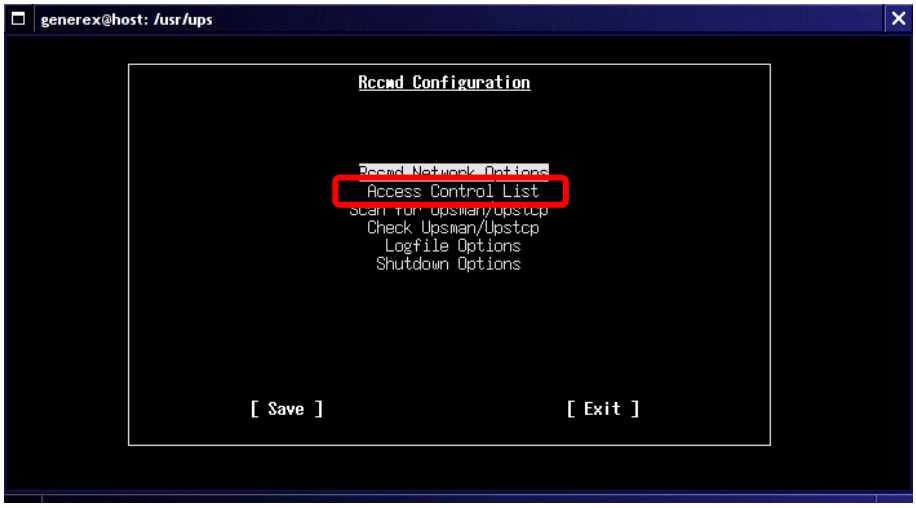


Fig. 133: Selection Access Control List

Note: An empty Access Control List means everyone is allowed to connect.

To **add an IP address** hit the [Tab] key until the **[Add]** button is highlighted, then press **[Enter].**

Fig. 134: RCCMD UNIX Add Sender

Enter **the IP address** of the host you want to be able to connect, then press **[Enter]**.

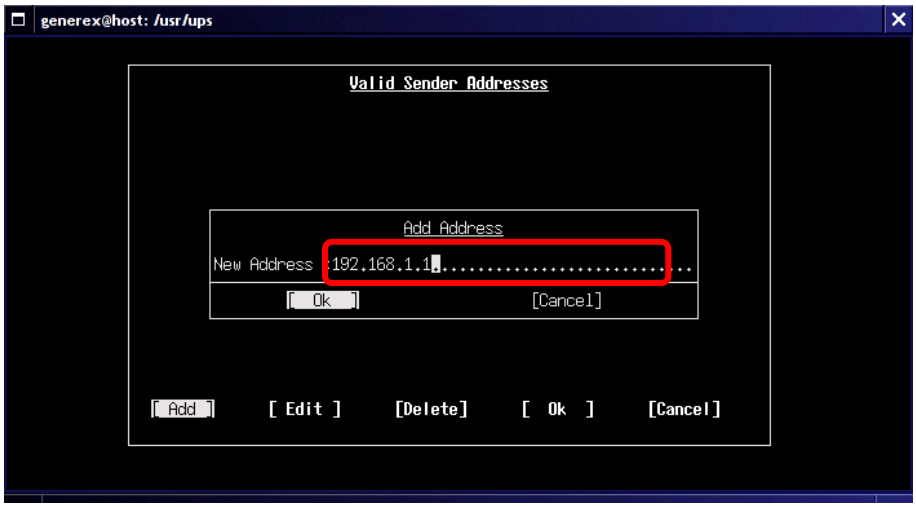


Fig. 135: RCCMD UNIX Sender Example

To edit an **entry in the list select** it by hitting the [↑] and [↓] keys until the entry is highlighted, then hit the [Tab] key until the **[Edit]** button is highlighted, then press **[Enter]**.

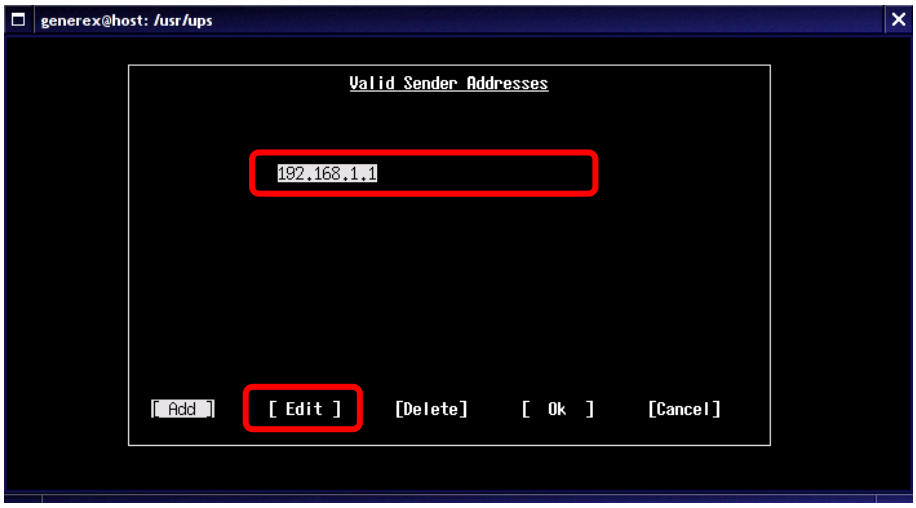


Fig. 136: RCCMD UNIX Sender Overview

Edit the Address in the "**Edit Address**" Window. To keep your changes select the [**Ok**] button with the [Tab] key and press [**Enter**] otherwise select [Cancel].

To **delete** an entry in the list select it by hitting the [↑] and [↓] keys until the entry is highlighted, then hit the [Tab] key until the **[Delete]** button is highlighted, then press **[Enter].**

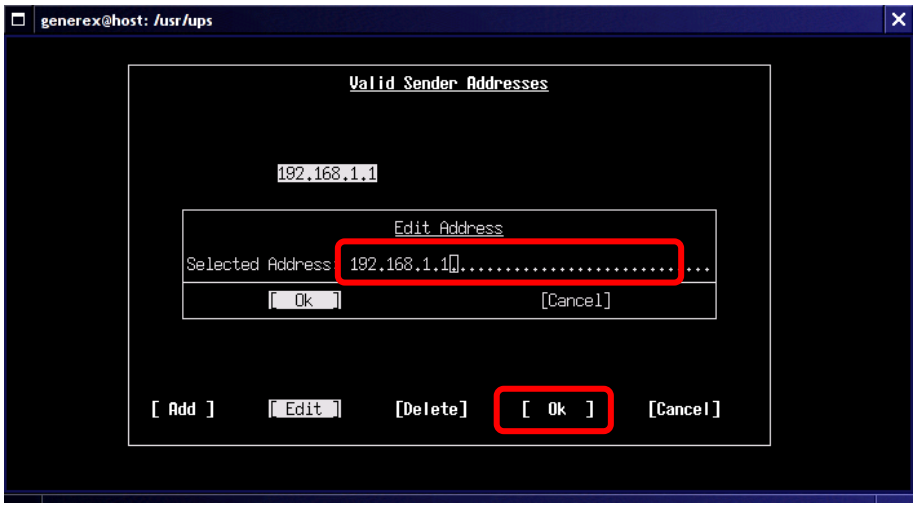


Fig. 137: RCCMD UNIX Sender Editing

Confirm to **delete the entry** by selecting **[Ok]** with the [Tab] key and pressing **[Enter],** otherwise select [Cancel].

To **leave the screen** select either [Ok] or [Cancel] with the [Tab] key and press [Enter]. [Ok] means accept the list as displayed on the screen, [Cancel] means discard all changes made to the list.

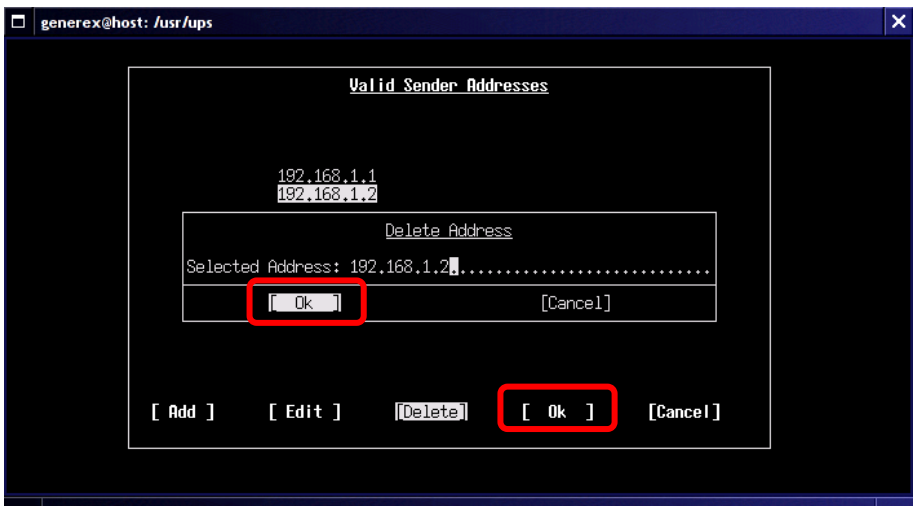


Fig. 138: RCCMD UNIX Delete Sender

Scan for UPSMAN/UPSTCP:
This screen allows you to **scan your network for Upsman/Upstcp servers**. You may want to add the detected IP addresses to the “Access Control List”.

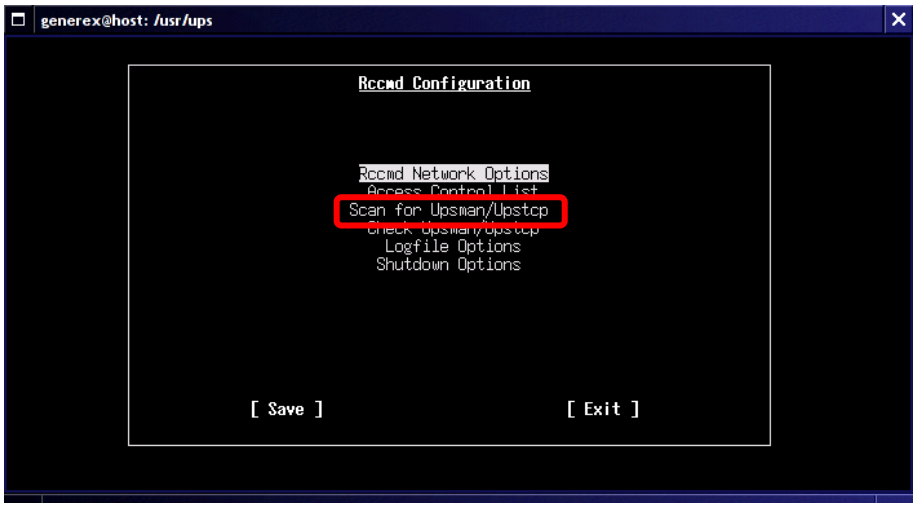


Fig. 139: Configuration – Scan for UPSMAN/Upstcp

Note: The options on this screen do not directly affect rccmd. However, the results of a network scan may be transferred to the “Access Control List”.

Menu **„Scan Options“: lowest/highest IP:**
On startup rccmd_conf tries to determine the hosts primary IP address. From this address a corresponding Class C network range is derived. These are the default boundaries for the network scan. If you want to scan another network or adjust the range, move to the desired entry (lowest and/or highest IP) using the [Tab] key and change the address as appropriate.

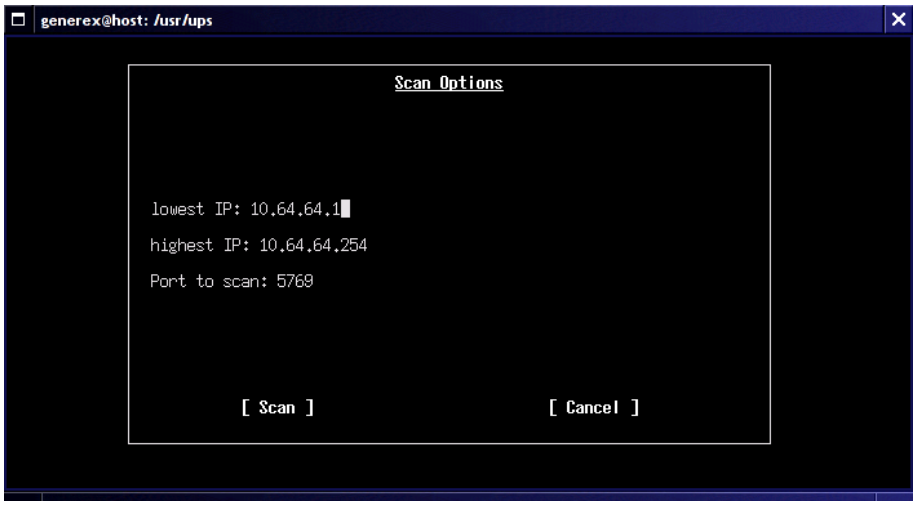


Fig. 140: RCCMD UNIX Sender Scan

Port to scan:
The port the scanner will try to connect to. The default is 5769, which is the default port of the Upsman/Upstcp server. If you have Upsman/Upstcp running on a different port you may want to switch this option accordingly.

To **start the scan select** [Scan] using the [Tab] key and press [Enter], otherwise select [Cancel].

Configuration **“Check Upsman/Upstcp”:**
The Rccmd listener has the ability to check periodically if the Upsman/Upstcp servers configured in “Access Control List” are alive.

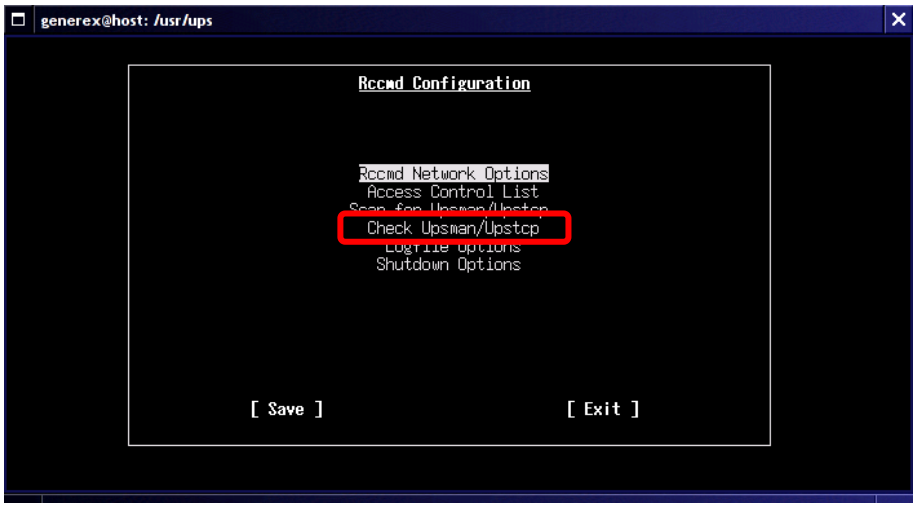


Fig. 141: Configuration Check Upsman/Upstcp

Note: The “Check Upsman/Upstcp” feature is only available if there are any addresses configured in the “Access Control List”.

If there are one or more entries in “Access Control List” the screen “Check Upsman Options” pops up.

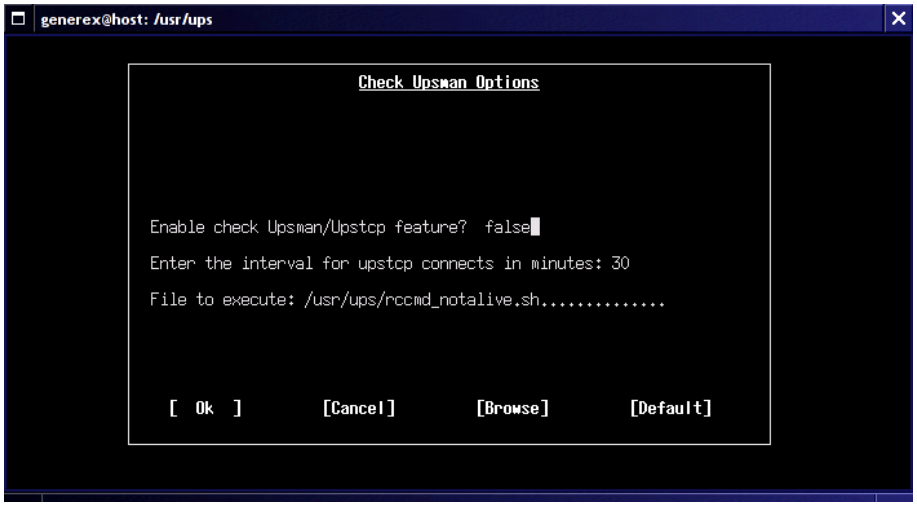


Fig. 142: RCCMD UNIX Check Upsman

Enable check Upsman/Upstcp feature: Possible values are “true” and “false”, “false” is the default. To change the value use the [↑] and [↓] keys.

Enter the interval for upstcp connects in minutes: Interval to connect Upsman/Upstcp servers in minutes. Default is 30 minutes. To change overwrite the value in the options field.

File to execute: This file will be executed if rccmd is not able to connect one (or more) of the configured Upsman/Upstcp servers, asuming that either the host is down or the Upsman/Upstcp process is not running. Default is '/usr/ups/rccmd_notalive.sh'. You may change this value by overwriting the string in the options-field or by selecting a file in the file-browser. To invoke the file-browser hit the [Tab] key until the [Browse] button is highlighted, then press [Enter].

Configuration
“Logfile Options”:

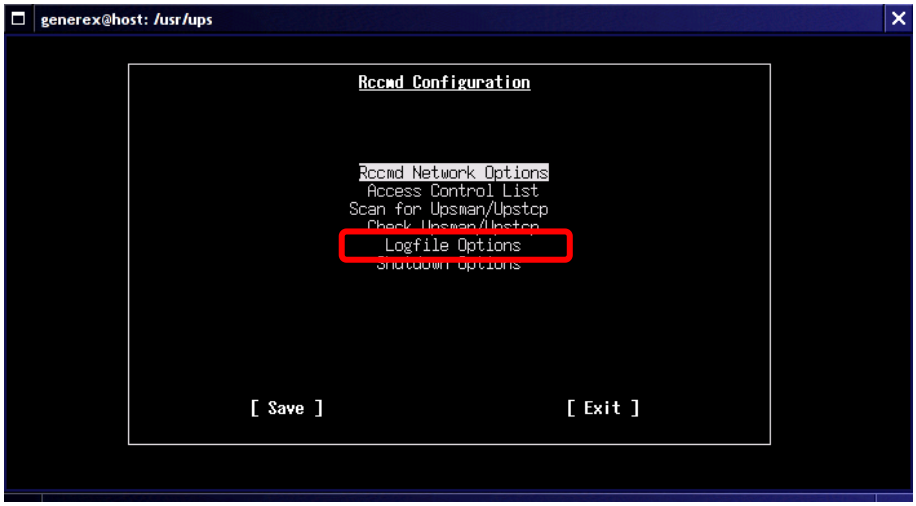


Fig. 143: Configuration Logfile Options

The rccmd listener is able to write and maintain a **logfile**. It will log events such as startup and shutdown of the program, accepted and denied network connections and executed commands. Some **parameters** may be configured on this screen.:

Fig. 144: RCCMD UNIX Log File Optionen

Enable logging to file: Possible values are “true” and “false”, “true” is the default. To change the value use the [↑] and [↓] keys.

Select maximum size of log file: The log file will not gain larger than this size. If the size of the log file would exceed this limit rccmd will automatically shrink it by 10% before it continues write to the log. The file will be shrinked from the start, so older entries will be removed first. The default size is 1024 Kb. To change the value use the [↑] and [↓] keys. The special value '0' means the file will not be shrinked.

Log file name: This option specifies the name and location of the logfile. The default is “/usr/ups/rccmd.log”. You may change this value by overwriting the string in the options-field or by selecting a file in the file-browser. To invoke the file-browser hit the [Tab] key until the [Browse] button is highlighted, then press [Enter].

Configuration
“Shutdown Options”:

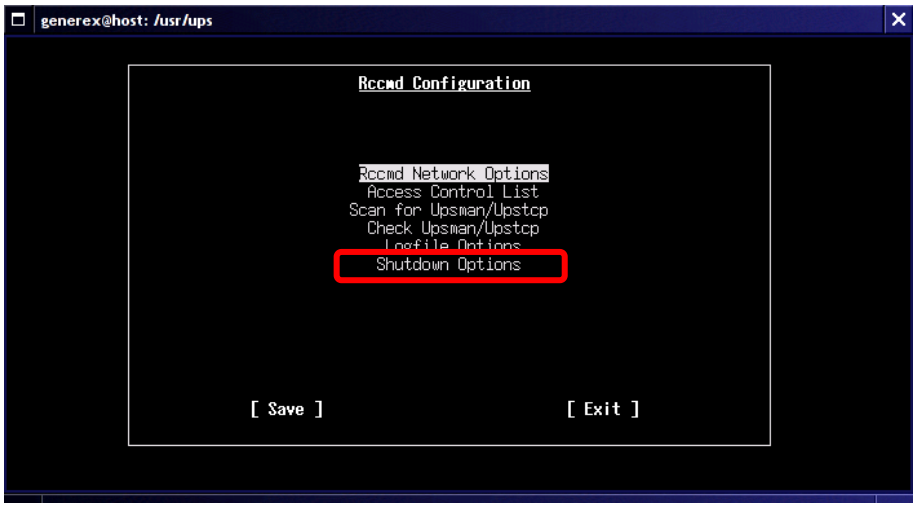


Fig. 145: Configuration Shutdown Options

This file will be executed if rccmd receives the “SHUTDOWN” command from the network.

Default ist “/usr/ups/rccmd_shutdown.sh”

Fig. 146: RCCMD UNIX Shutdown Optionen

Exit rccmd_conf:
In the main configuration menu “Rccmd Configuration” select either [Save] or [Exit] by hitting the [Tab] key until the desired button is highlighted and press [Enter]. [Save] means 'rccmd.cfg' will be written according to the actual values of the configuration screens, [Exit] will just exit the program, leaving 'rccmd.cfg' untouched.

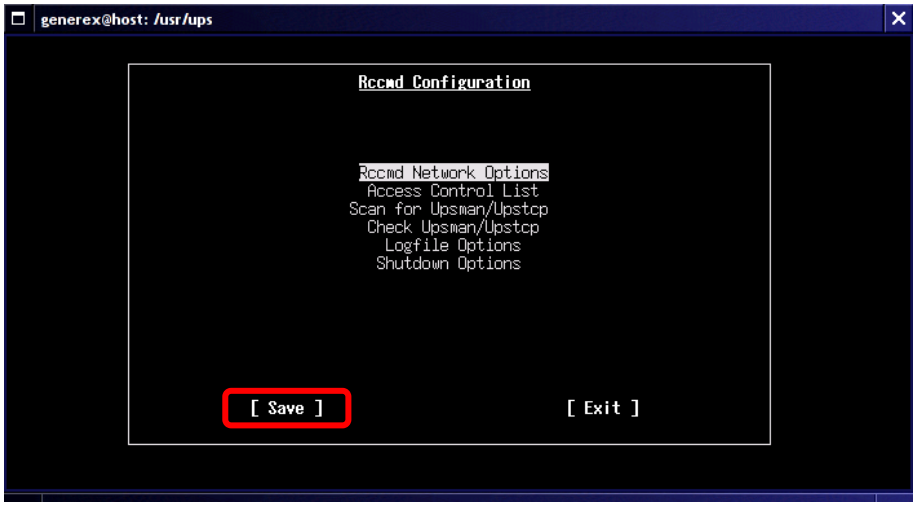


Fig. 147: Exit rccmd_conf

The File Browser:

Some of the screens above use a small build-in file browser like this:

The [↑] and [↓] keys may be used to move the list up and down. Pressing the [Enter] key will select the highlighted entry. If the selected entry is a directory the browser wil move into this directory and list its contents.

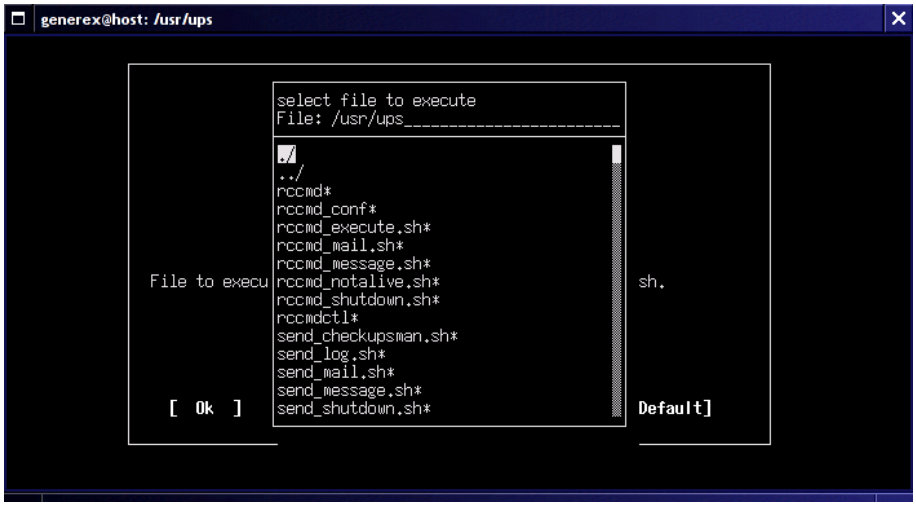


Fig. 148: RCCMD UNIX File Browsing

As usual the double dot '..' means the parent directory. File types are indicated similar to the output of 'ls -F'. This means a '*' is appended for executables, '/' for directories, '@' for symbolic links and '=' for sockets.

UNIX RCCMD multiple sender configuration :

In case the user wants to utilise more than one sender address the rccmd.sh has to be modified like this:

```
#! /bin/sh

# You may specify a sender IP to accept signals from,
# default is everyone.
SENDER="-a 10.55.52.82 -a 10.55.52.83 -a 10.55.52.84"

# You may change the port to listen on,
# default is 6003.
PORT=

# You must define a command to be executed upon
# receiving signal.
SCRIPT=/usr/ups/doshutdown.sh

# test -z $SENDER || SENDER="-a $SENDER"
test -z $PORT || PORT="-p $PORT"
# to start:
./rccmd -l $SENDER $PORT $SCRIPT
```

UNIX RCCMD multiple sender configuration (V3 and higher):

How to start several RCCMD sessions via different ports on UNIX?

Every RCCMD session needs an own TCP port, e. g..:

```
./rccmd -l -p 6003
./rccmd -l -p 6004
./rccmd -l -p 6005
```

Import into RC files:

Set an accordant amount of starting scripts and invoke them trough the old ones.:

1) Create new starting scripts:
   copy 3 times the old script and rename them:

```
cp rccmdctl.sh rccmdctl-1.sh
cp rccmdctl.sh rccmdctl-2.sh
cp rccmdctl.sh rccmdctl-3.sh
```

2) Adjust the new scripts:
   through the variable “RCCMDPORT”:

```
...
   RCCMDPORT=6003
...
```

3) Adjust the old script, because it starts the new one, replace the start- and stop sector
   in the folder „rccmdctl“:

```
 start)
     /usr/ups/rccmdctl-1.sh start
     /usr/ups/rccmdctl-2.sh start
     /usr/ups/rccmdctl-3.sh start
   ;;

   stop)
     /usr/ups/rccmdctl-1.sh stop
     /usr/ups/rccmdctl-2.sh stop
     /usr/ups/rccmdctl-3.sh stop
   ;;
```

Attention: Do not edit the scripts with a Windows editor, because the different word wrap of Windows/Unix would destroy them!

5 RCCMD on VMware

5.1 Requirements

a) The ESXi host:

You need an ESXi host, version 4 or higher (version 6 is recommended). You have to install this software on your machine to run virtual machines. This manual does not describe ESXi itself, you can download the latest version and documentation about ESXi on vmware.com. Note that you need a valid license to access the downloads at vmware.com; otherwise you can download only trial versions. You will need the login credentials of the ESXi host (username and password for “root” user.

b) V-Sphere Management Assistant (vMA)

You can download the latest versions (version 5.5 or higher recommended) from vmware.com after you logged in and provided a valid license on the vmware.com webpage. The vMA is required to install RCCMD on your ESXi. It provides a terminal interface for IP address configuration and controlling your ESXi. Without the vMA, it is not possible to install RCCMD.

Please note: If you use ESXi 6.5, you don’t use the vSphere client anymore and use a browser plugin instead. Open the IP of your ESXi, followed by ***/ui/#/login***. This is the only change between the versions, other configuration is similar to vSphere client.

c) V-Sphere Client

The client is required to connect to your ESXi host. Available on vmware.com after logging in and providing a valid license. When connected to your ESXi you can configure and manage the ESXi host and also add, remove shut down, (re)start and manage virtual machines. The V-Sphere Client is required to install the vMA and to configure the shutdown of the virtual machines running on this ESXi host.

d) RCCMD for ESXi

The RCCMD client is the shutdown software developed by Generex. Once installed, it listens to the other Generex products to receive and handle commands and messages. Download the latest version from the Generex website. Note that you have to enter a valid serial number to download the files.

e) sFTP client

You need a sFTP client (eg. Filezilla) for transferring the RCCMD files to your vMA virtual hard disk.

f) Terminal client

You need a terminal client (eg. Putty) to connect to the vMA and start the script installation of RCCMD. (RCCMD has a graphical interface, but through Terminal Client the RCCMD configuration file rccmd.cfg may edited manually).

5.2 Setup and Configuration of vMA

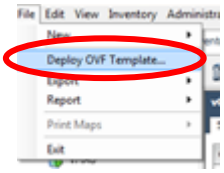
Install the V-Sphere client. You have to set a folder for the installation of the V-Sphere client and proceed.

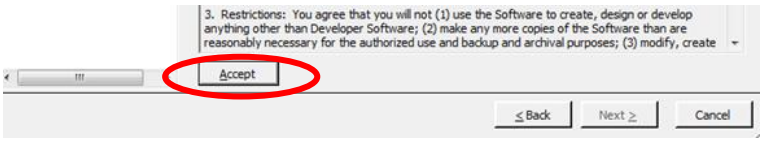
Now, login on vmware.com and download the latest vMA archive.

Note that you need a valid license to gain access to the required download section. After downloading, unzip the archive.

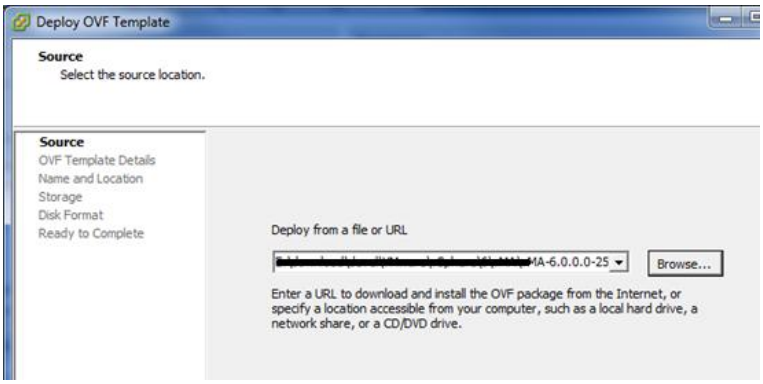
Start the V-Sphere client and enter the IP address of your ESXi host. Enter the correct credentials and login onto your ESXi. (Username and Password for root user)

Menu „**File**“
Now, click on File -> **Deploy OVF template** and browse to the **extracted vMA archive**. Choose the .**ovf-file**. You will see a list of preconfigured parameters and the amount of disk storage used for the installation. If you proceed, you have to **accept** the **license agreement**.

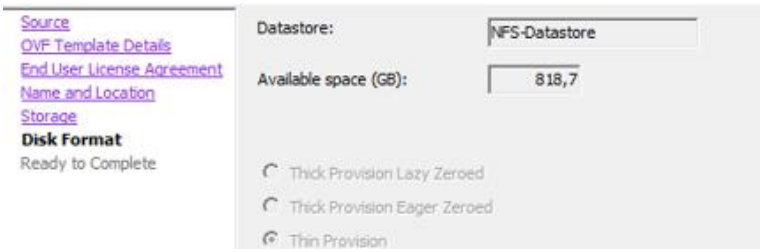




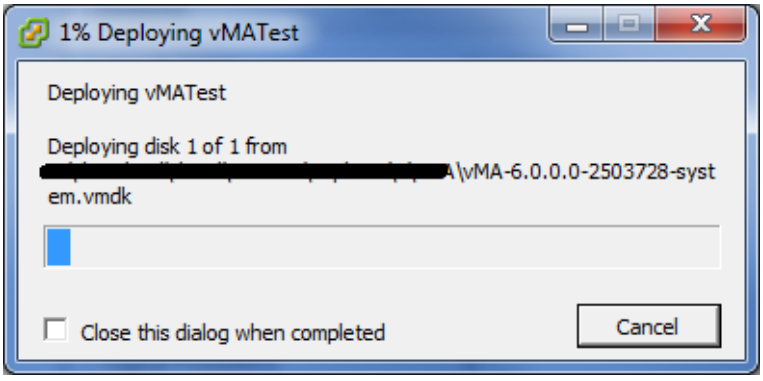
Set a **name for the vMA** where RCCMD will be running – the default name is *vSphere Management Assistant (vMA).* We recommend to take a shorter description, eg. **vMA_RCCMD**.

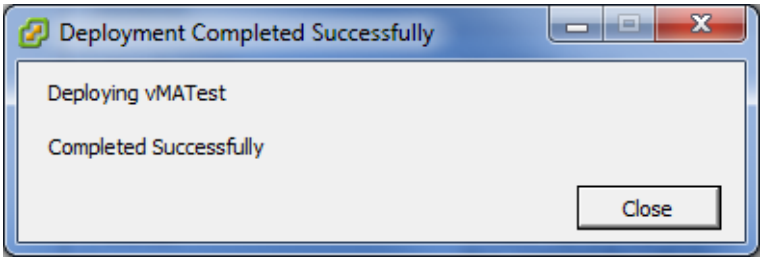


After you choose a **hard disk format**, the progress will start. Note that it depends on the datastore you choose if you can change the given format.

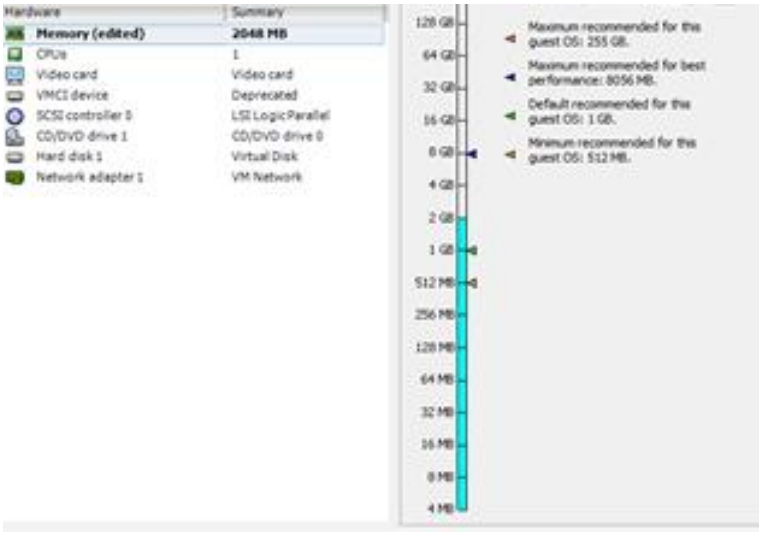


This will take a few minutes.

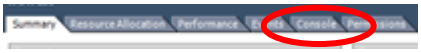




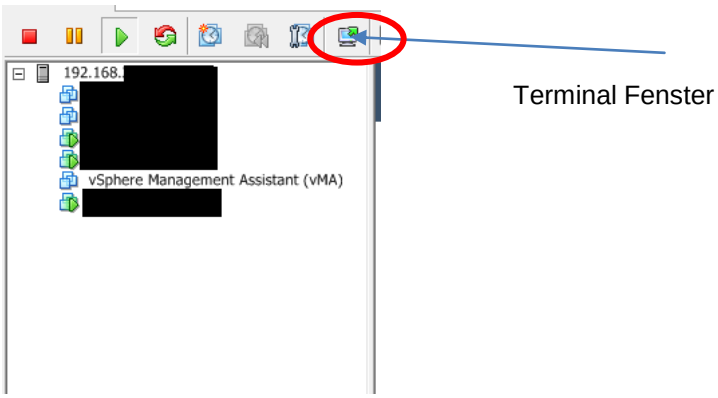
After the progress is finished, you will notice a new virtual machine. Open the **settings**. The preconfigured RAM is only for small installations, we recommend at least **2 GB**.



Run the virtual machine and open the **console.**



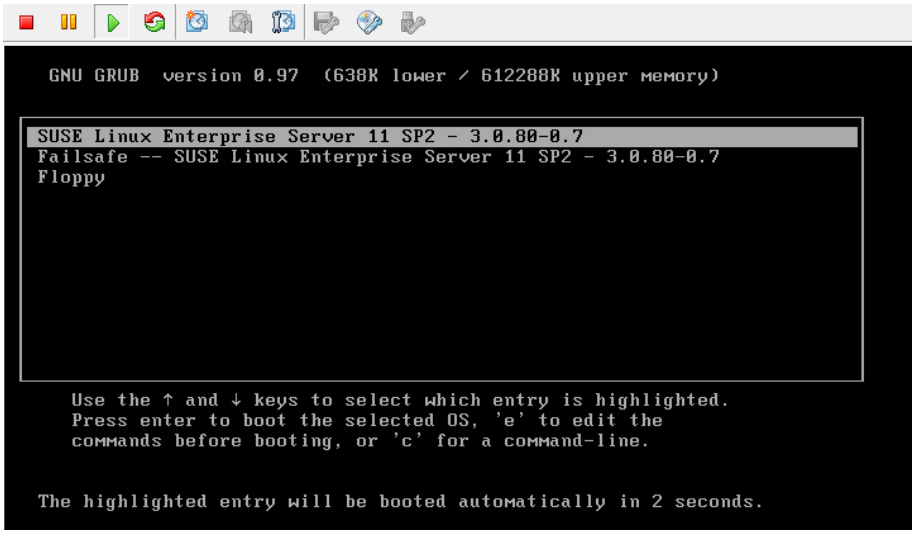
or alternatively the **terminal**, but **NOT** both.



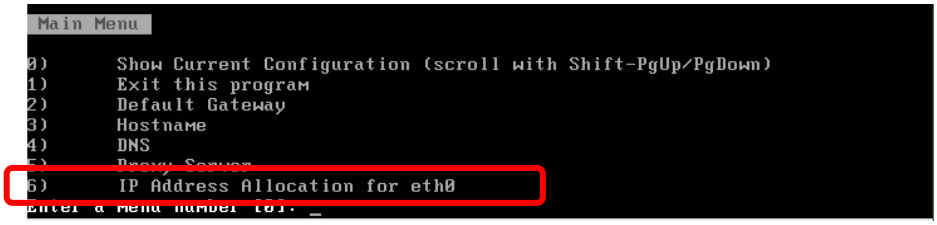
The virtual machine will start within ~5 seconds the correct OS. Here you have two options for restoring a broken vMA or booting from a floppy.

Afterwards, you will see a menu.

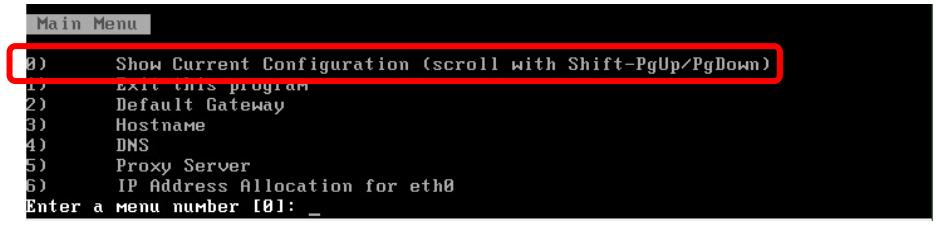
For RCCMD it is necessary to set an **IP address** and a **password** for the vi-admin account. The vi-admin has root access in this virtual machine.



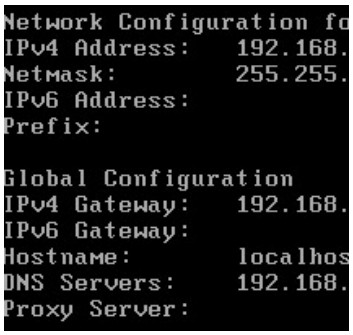
Type in **6** and press enter. You may choose to set an **IPv6 address** and, after that, an **IPv4 address**.
We recommend to use an IPv4 address. You may also choose to get an IP by DHCP.



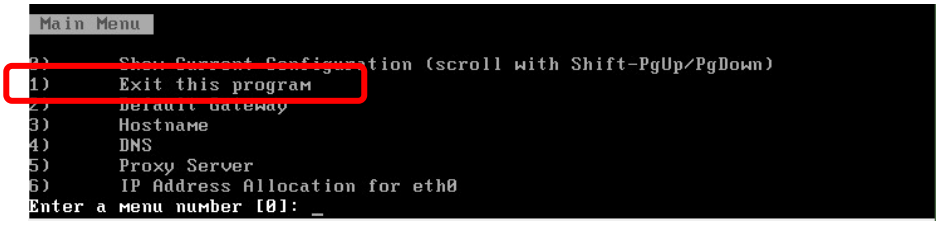
After you have made your selection, you will see the menu again. Press **0** and enter to see your configuration.



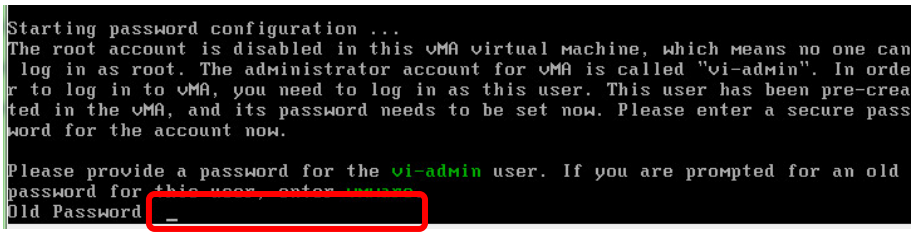
Write down your configuration.



Press **1** to exit this menu. You will be prompted to set a password for vi-admin. In case you did not enter a password before, the default password for the vi-admin is **vmware**.



You now have to enter a **new password**.

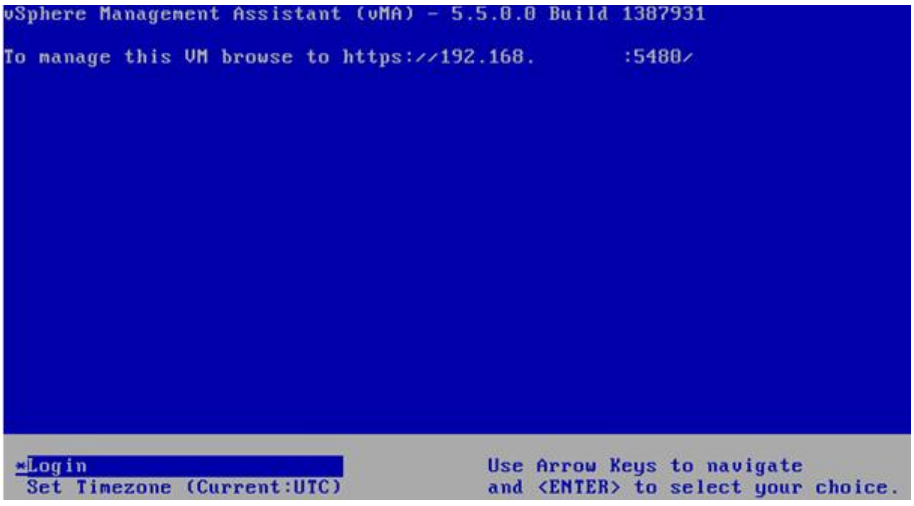


Note: The vMA is using an US keyboard and requires certain password conditions.
Note that this password must contain:

- at least 8 characters
- 1 small letter
- 1 capital letter
- 1 digit
- 1 special character

Also, passwords containing the same letters to often will be rejected.
Working example:
G0ld!G0ld!

After that, the vMA will progress the configuration until you see the login window, your IP address and the port. If you enter this IP address and port in your browser, you have access to the web GUI of the vMA.



The configuration of the vMA is now completed. You may close the vMA terminal. (if you have used this option)

For the next step, you need a sFTP client and a terminal program.

Note: You cannot use the v-Sphere client to install or copy the RCCMD files.

5.3 Preparing RCCMD installation

Go to the Generex website and download the latest version of RCCMD for ESXi. You will be asked for a valid license before you can download the archive.

This RCCMD Client License comes with every CS121/CS141 or RCCMD client which you purchase through your UPS vendor. You cannot use a trial version.

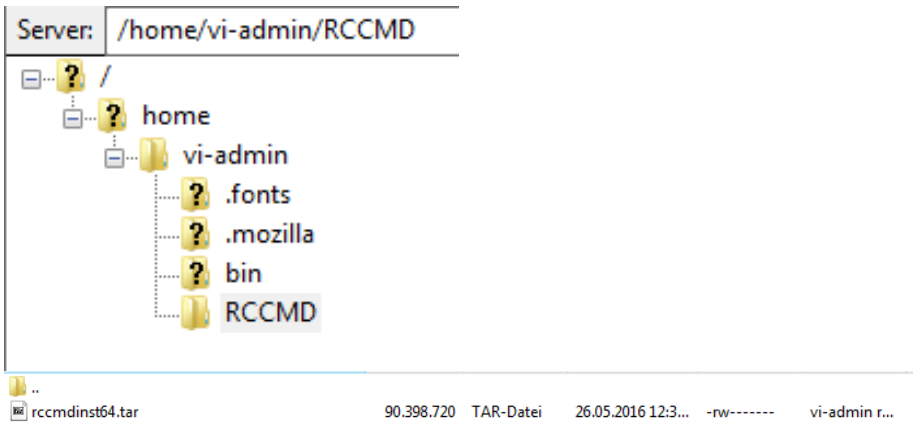
After you have finished your download, open your sFTP client to transfer the downloaded RCCMD file rccmdinst64.tar

Connect to the vMA IP address. Use your vi-admin credentials and connect on port 22 (SFTP).

You will see the content of the vi-admin account. Create a **folder** and **copy** the downloaded **RCCMD.tar.gz** archive to this folder.

.

After transferring the data, you may **close** the **sFTP-client** and **open your terminal program**.

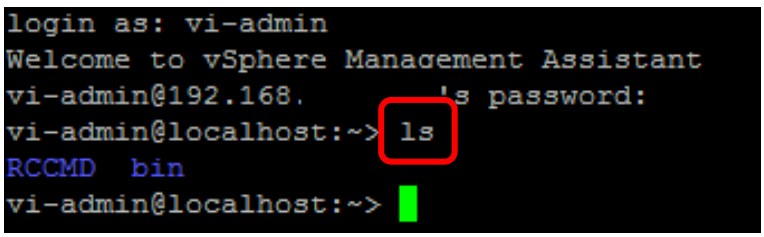


5.4 Installation of RCCMD

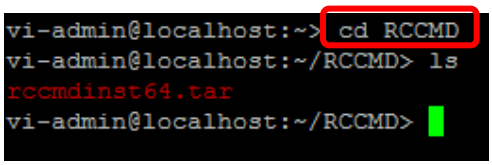
Connect your terminal program via SSH to the vMA “RCCMD”.

Login using the same credentials you have used in your sFTP client.

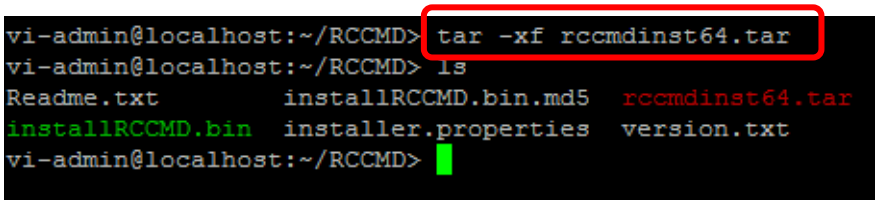
In this case, we created a folder named RCCMD in the vi-admin account. If you type in ***ls*****,** you can see the content of a folder, in this case the home folder of the vi-admin account.



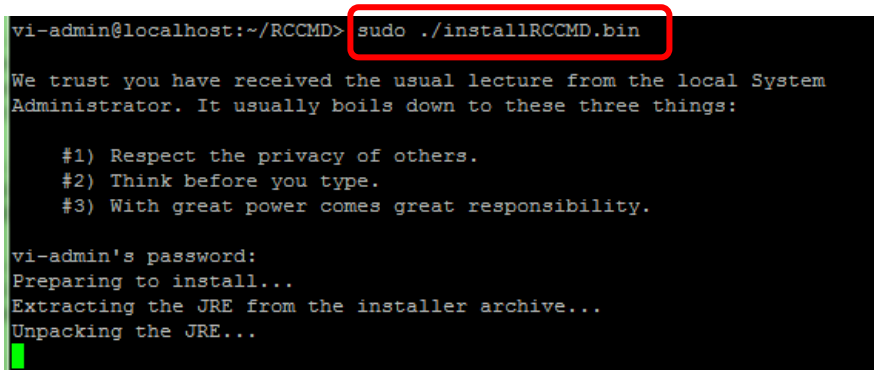
The purple displayed names are folders. Use the **cd ..** command to navigate to a higher level in the folder hierarchy.To open a folder enter ***cd xxx***, in this case ***cd RCCMD***. Note that all inputs in the terminal are case sensitive.



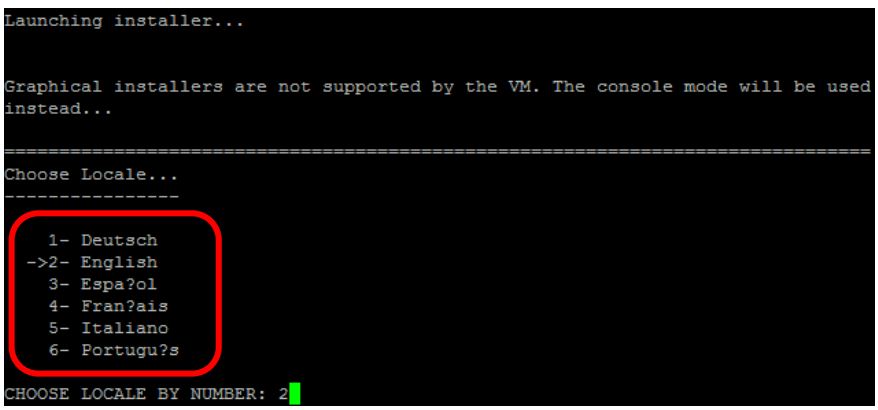
The red displayed names are archives. Unzip the file with the following parameters:
tar –xf rccmdinst64.tar
Now, the archive is unzipped with the correct values.



To start the installation, type in ***sudo ./installRCCMD.bin***

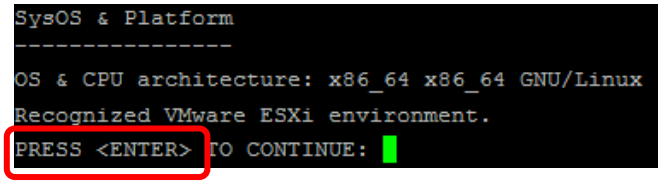


You will be asked for the **vi-admin's password** again.
After that, the **progress will start**. You will now be asked for your **language**. **Enter** the number and press enter.
Note that the terminal may not display the correct characters if they are not basic characters. This depends on the terminal software you are using.



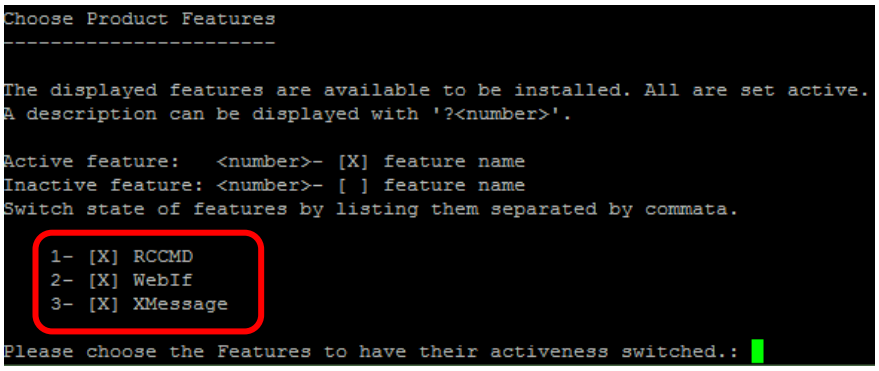
Now, the installation begins. Whenever you have the option to make a choice, you may type ***quit*** to cancel the installation.

You will see the version number of the installer. Press **enter**.
The installer will **check** if you use the correct environment and the correct installer.



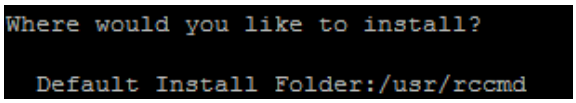
Now you will be asked for your license key again. Note that you have to enter a serial which is not active in your network. Otherwise, the service will not start.
Now you see the license agreement. If you agree, confirm with ***y*** and press enter.

In the next step you have the options to enable or disable the **features** you want to install. We recommend to install **all** features. If you have made your choice or if you don't want to change any values, press **enter**.



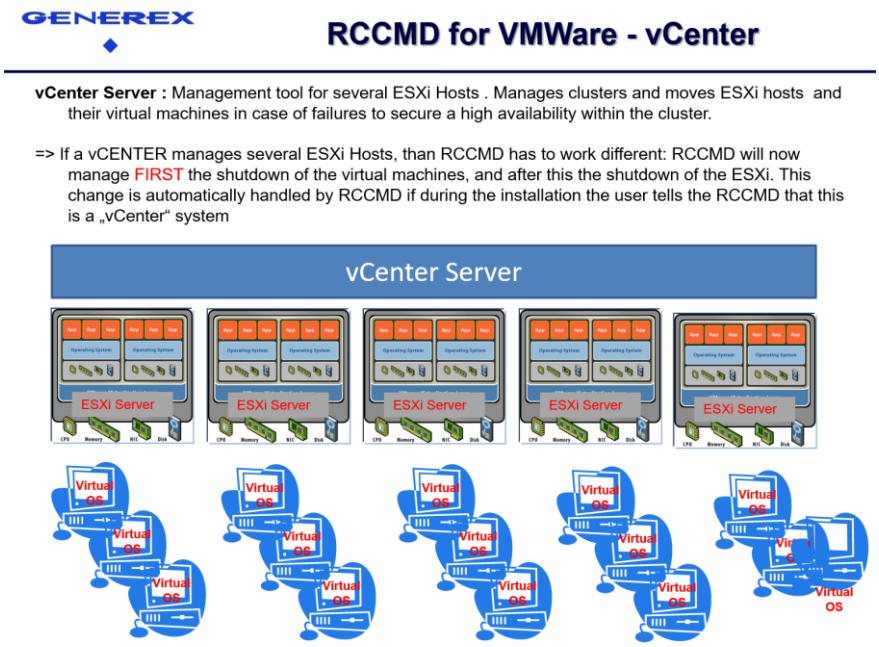
You will be asked if you want to switch the **installation path**. We recommend strongly to keep the default settings.
NOTE: If you do not want to use the RCCMD a web interface, it is still possible to set minimal parameters to run RCCMD.

Press **Enter** if you don't want to change the folder.



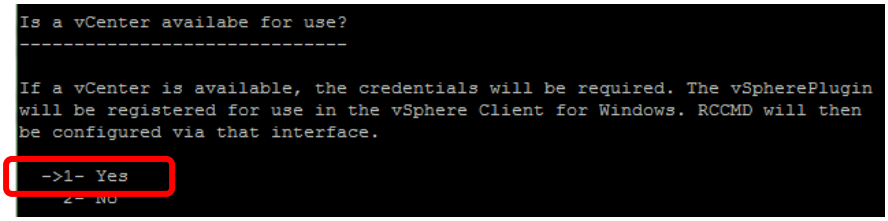
In the next step you will be asked if you use the **V-Center** for your ESXi.

VCenter Server provides centralized management and operation, resource provisioning and performance evaluation of virtual machines residing on a distributed virtual data center. VMware VCenter Server is designed primarily for VSphere, VMware's platform for building virtualized cloud infrastructures. VMware VCenter Server was previously known as VMware VirtualCenter.

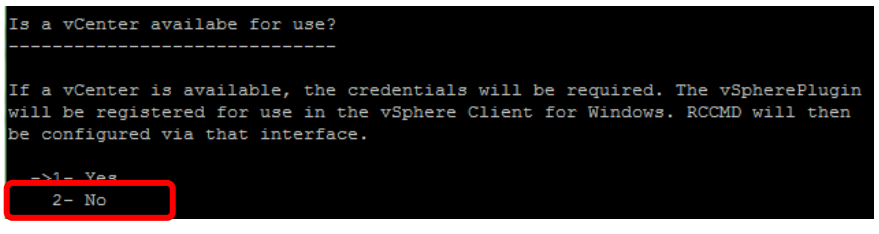


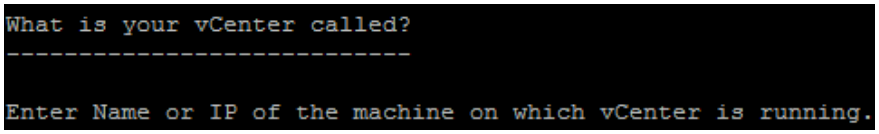
Make your **selection** and press enter.

If you have set the option to **yes (1),** you will be asked for the machine where vCenter is running, followed by **username** and **password**.

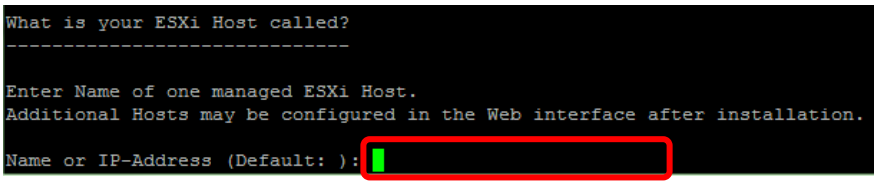


If you have set the option to **no (2)** , the installer will ask for the **host name or IP of your ESXi**.



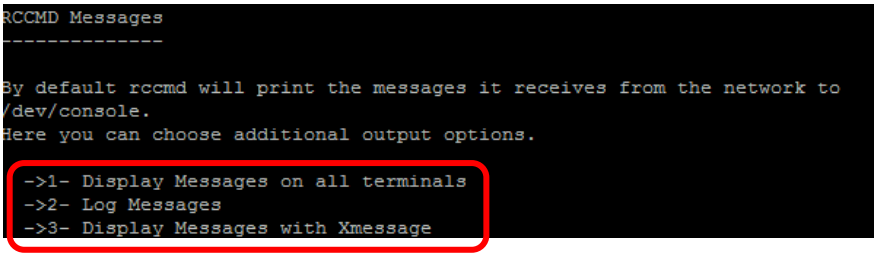


Enter the **host name** or **IP of your ESXi**. You will be asked for a user with administration privileges (Default root) and the password. Do **not** enter the vMA credentials (vi-admin).



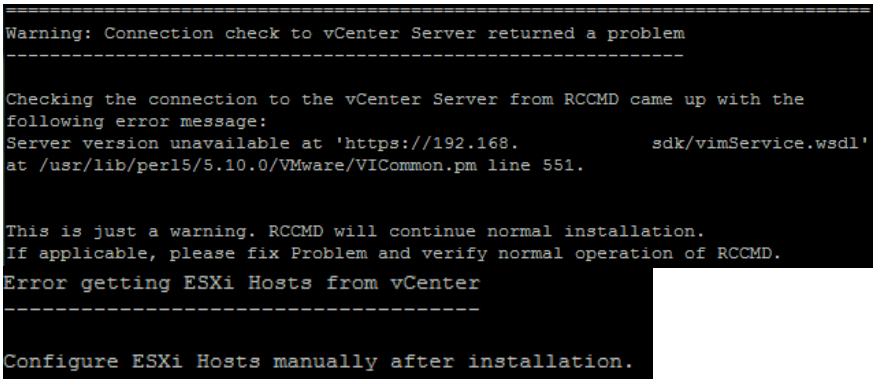
Afterwards, you will be asked for a **shutdown duration**. This is the duration the ESXi needs to shutdown ALL actually running virtual machines. Note: You can later change these values in the web GUI of RCCMD.
Now, the installer asks for the **vMA name**. You entered this name earlier.
Default name: vSphere Management Assistant (vMA), we used in our example RCCMD_vMA.

In the next step, you will be asked how RCCMD will display the received **messages**. Make your choice and press enter. We recommend to use the default settings (all enabled).



Finally, the **summary of your choices appears**. If you press **enter** now, the installation will start.

Note: If you are using the vCenter and entered wrong credentials in this script earlier, you will get a few **warnings**. You can ignore them for now; the configuration can be changed later.

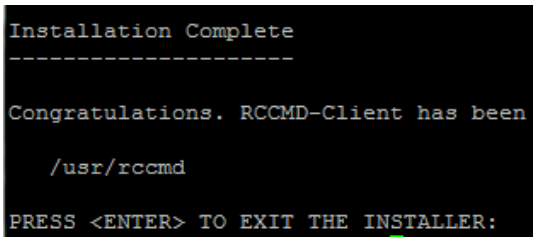


During the installation you will be asked if you want to access RCCMD with **http** or **https** (default).
Make your **selection** and press **enter**. You can now change the default https port 8443.
Remember if you change the port you have to set the same port to open your RCCMD web interface!

You will now be asked for a **password** (default: cs121-snmp) and a password hint.
The installer shows your **IP** and **port for configuration**.
Choose if you want to **start** the **service** now (1) or later (2).

Note: With the default configuration, every IP could send a shutdown command!

Finally, the installer shows the message that the **installation was successful** and the folder you have installed RCCMD in.

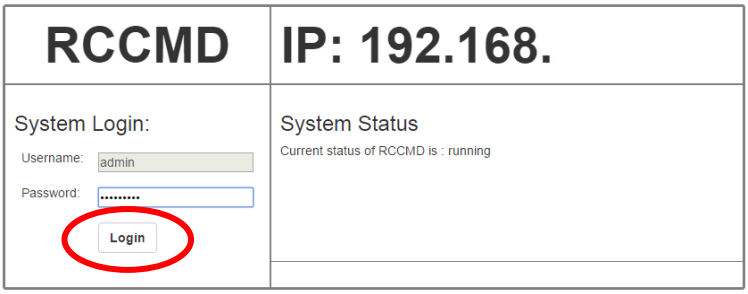


The installation of RCCMD is finished. You can close your terminal software and open your web browser.

5.5 Configuration of RCCMD

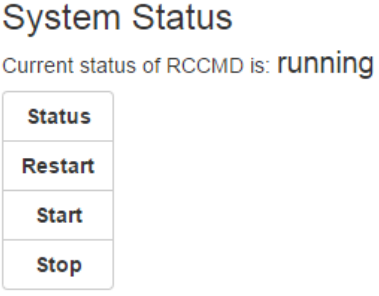
After installation is finished, open the **IP:Port** in your browser.
Example: https://192.168.100.200:8443

You should see the login now. **Log in** with your configured credentials (Default: admin and **cs121-snmp**).

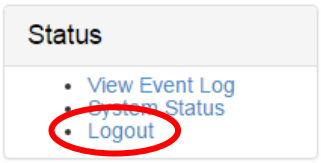


Menu „**Event Log**“:
In the Event Log, you can see all notifications and alerts.

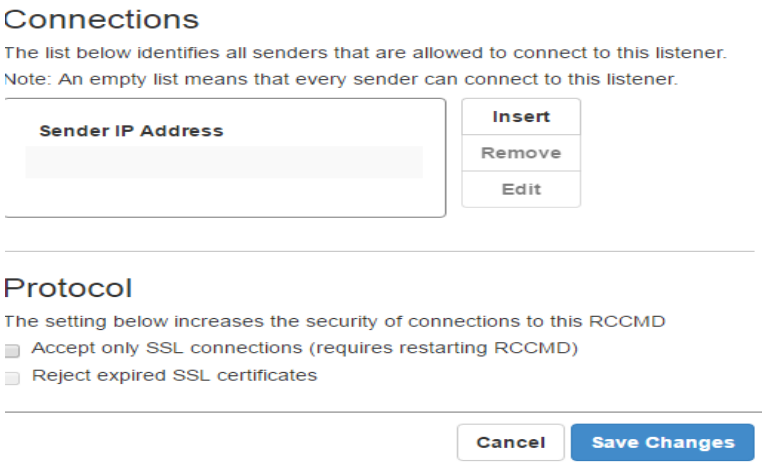
Menu „ **System Status**“:
At the system status, you can start, stop and restart the RCCMD service. Also, you can click on status for a refresh.



If you click on **Logout** you are immediately logged out from RCCMD.



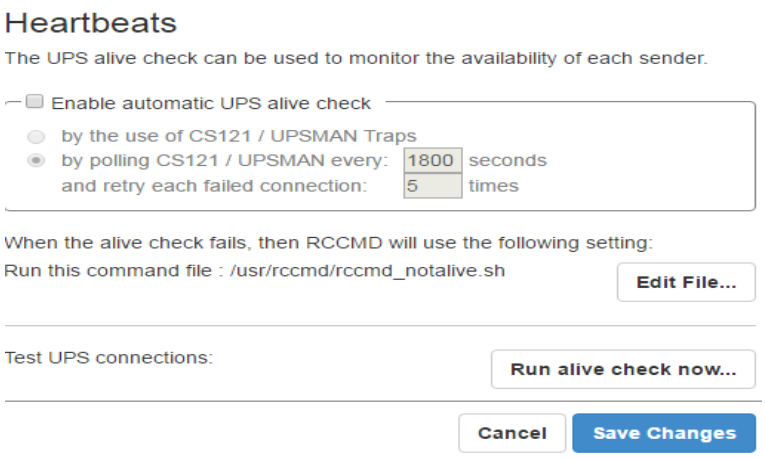
Menu „**Connections**“:
Connections will allow you to set specific **IPs** which are allowed to send you notifications and shutdown commands. **If you do not enter any addresses, every IP could send a notification or shutdown command.** You can insert, edit and delete any IP. You may also set the options for accepting only **SSL** connections and rejecting expired **SSL** certificates.



Menu „**Heartbeats**“:
The heartbeat menu offers several settings for an **alive check**. If you use the UPSMAN alive check, a signal is sent to determine if the UPSMAN still provides data values. In case of no returned data, the configured script (Default: /usr/rccmd/rccmd_notalive.sh) will be executed which shows a popup message.
The entry *by the use CS121/CS141/UPSMAN Traps* enables UPSMAN/RCCMD/UNMS to display local messages if the status of UPSMAN/RCCMD changes. If you choose the other option (Polling every x seconds) you decide to request only signal data without getting UPS data values or messages.

The **polling rate** determines the interval of requesting status. If you have set 100 times, RCCMD will send an alert in case of 100 failed connections.

If you click on ***Run alive check now*** the UPSMAN alive checking will be started (on port 5769).

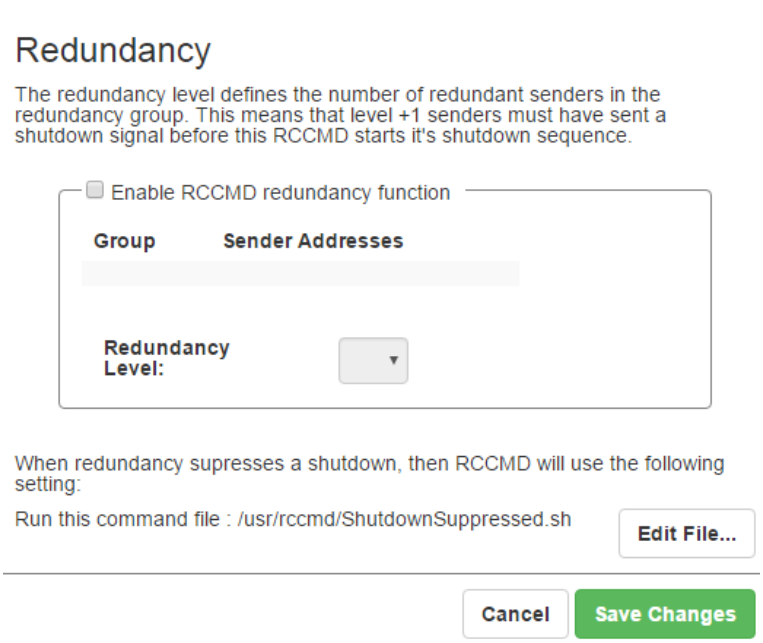


Menu „**Redundancy**“:

The redundancy menu allows **configuring certain levels** before the ESXi will start the shutdown progress. This is only possible if you use two or more UPS devices.

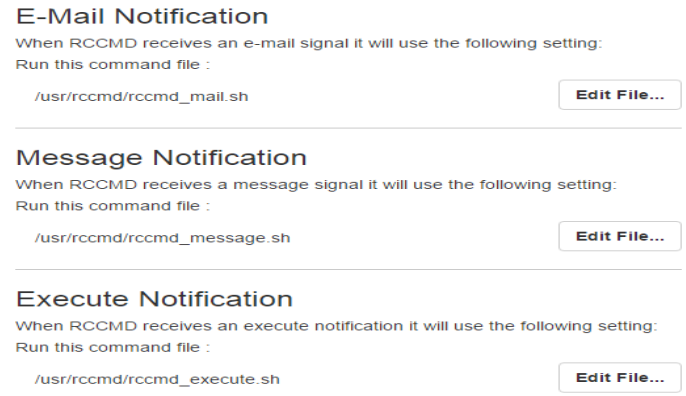
At first, you have to enter at least two connections in the connections menu. Then, you can activate the redundancy function. For each connection entry after the first, you can raise the level by one. If a sender triggers a shutdown command with the ESXi as a target, the level decreases by one. If the level drops below zero, the shutdown progress initiates.

You may also edit the redundancy script manually, which is configured in ShutdownSuppressed.sh.

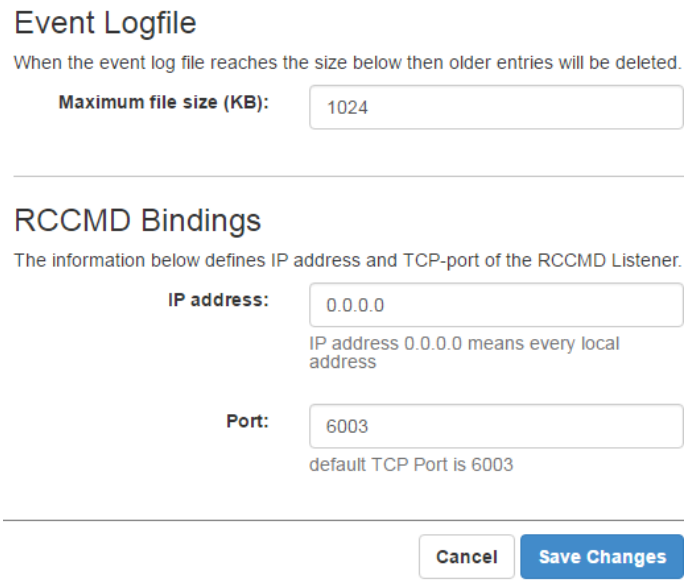


Menu „**Notification**“:

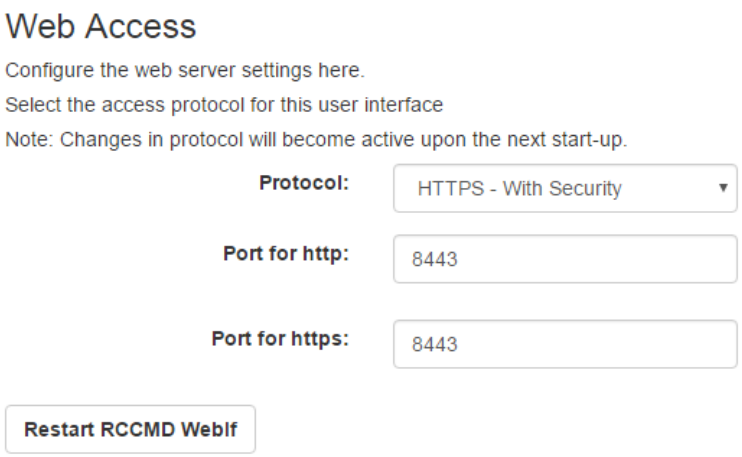
In the notification menu, you may change the **scripts** and therefore the behavior of RCCMD in case of receiving email notifications, messages and execution commands.



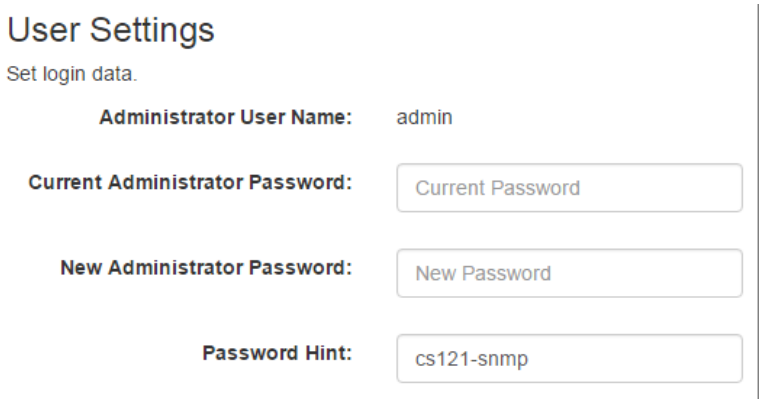
The advanced options handle the **size of the logfile** (Default is 1 Mbyte, which should be changed to a higher value). Also, you can set a single RCCMD listener when entering an IP address and port. Default is here the setting for each local address gaining access.



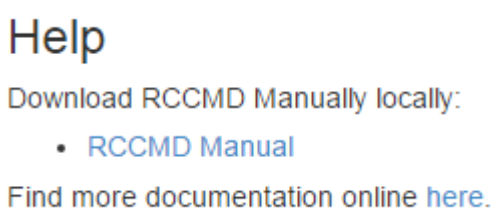
Menu „**Web Access**“:
In the web configuration menu, you just set the settings for this web **GUI.** We recommend to use https and the default port (8443). You can also restart the Web interface here.



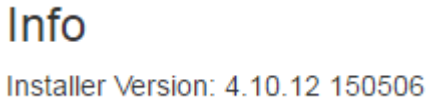
Menu „**User Settings**“:
The user settings menu is for changing the default password and the password hint. Just enter the new values and save the changes.



If you click on “**manual”,** you will find a link to the RCCMD manual and also a link to the Generex website.



The “**Info**” button shows the installer version.
This one is required in case of support cases.



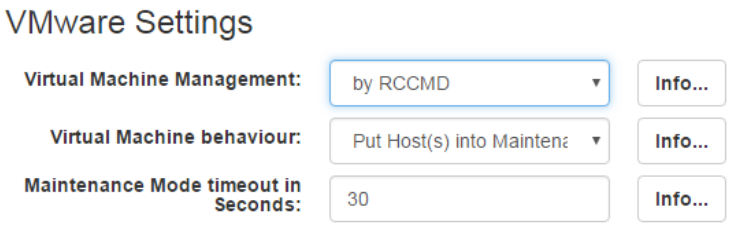
5.6 Configuration of VMWare and RCCMD

RCCMD distinguishes between two possible configurations.
To ensure the correct behavior in the event of an emergency, you need to clarify which hardware and software components are in use.

1) ESXi with V-Center

RCCMD will shutdown all VMs at once. For a safe shutdown, install VMWare Tools on each virtual machine. If you want a solution where you can set a different time for each machine, you have to purchase a license for each virtual machine and install RCCMD directly on this machine.
RCCMD will shutdown the Virtual machines without considering any kind of order. Additionally, you have to create a job for each single virtual machine in the configuration of your sender. The ESXi ignores the settings you made with vSphere when using a vCenter.

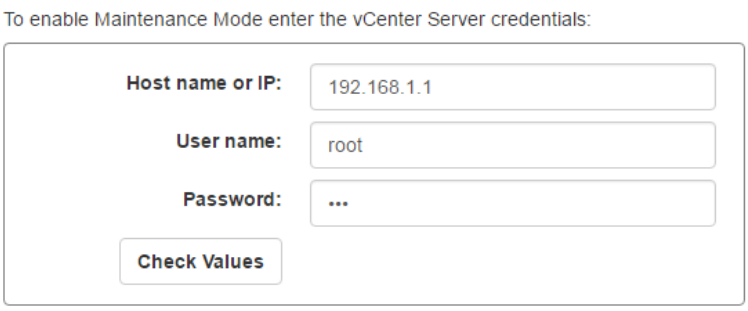
Menu „**VMware Settings**“:
You may choose here at the machine management if the **shutdown** should be initiated by RCCMD or ESXi. If you use V-Center, you have to choose RCCMD. Otherwise, all changes you made in your ESXi configuration will be ignored and nothing happens. The V-Center handles the shutdown and migration of your virtual machines. The “**maintenance mode”** is also usable if you want to delay certain hosts to shutdown. Put Host(s) into Maintenance Mode” can attempt to send a host into maintenance mode, thereby triggering vMotion for the virtual machines. Select this option only, if DRS (Distributed Resources Scheduler) is configured to be in fully automated mode and vMotion has been successfully tested for every virtual machine! If maintenance mode fails, then the remaing hosts will proceed with the “Shutdown Virtual Machines Behaviour”. To calculate how much backup time remain, when initiating this RCCMD command, the values for the longest “Shutdown Duration” of the hosts and maintenance mode timeout must be added.
Enter the period of time after which to abort trying to reach Maintenance Mode. If Maintenance Mode is not reached after this time, then the remaining hosts will proceed with the „Shutdown Virtual Machines“ behaviour. This is the last resort to shutdown the hosts and virtual machines gracefully.



The “**behavior”** signalizes your ESXi what to do in case of a shutdown. If you use more than one ESXi and you use VMotion, you may put the machines into maintenance mode. All machines are transferred and the original ESXi will be shut down. If you choose Shutdown virtual machines, all machines are handled equally and will shut down.

The “**maintenance mode timeout”** is simply the duration how long RCCMD should try to get the machines into maintenance. If the timeout expires, the machines will shut down instead.

If you use the V-Center you can edit and check the **credentials** here.

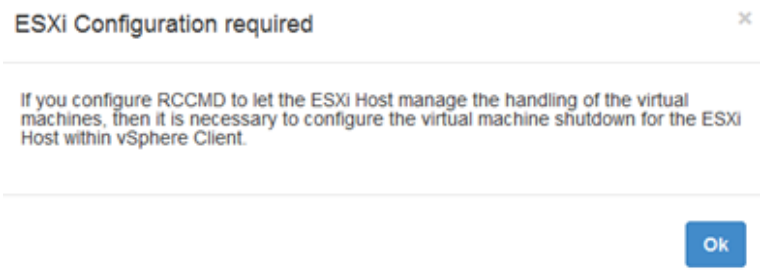


RCCMD will communicate directly with the ESXi. Only if you have a V-Center with V-Motion RCCMD will communicate with the V-Center.

2) ESXi without V-Center

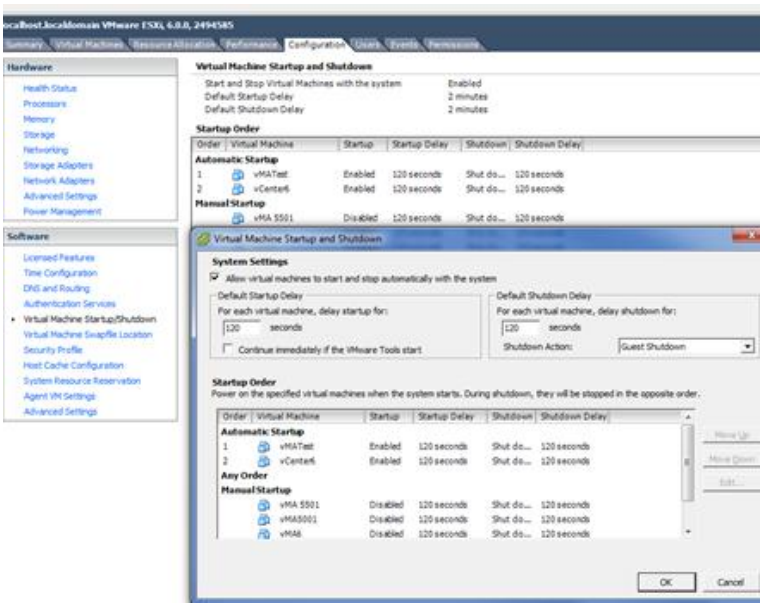
An ESXi without a V-Center will handle the shutdown order itself.

If you get this message, it is necessary to **configure the shutdows in your V-Sphere** client.

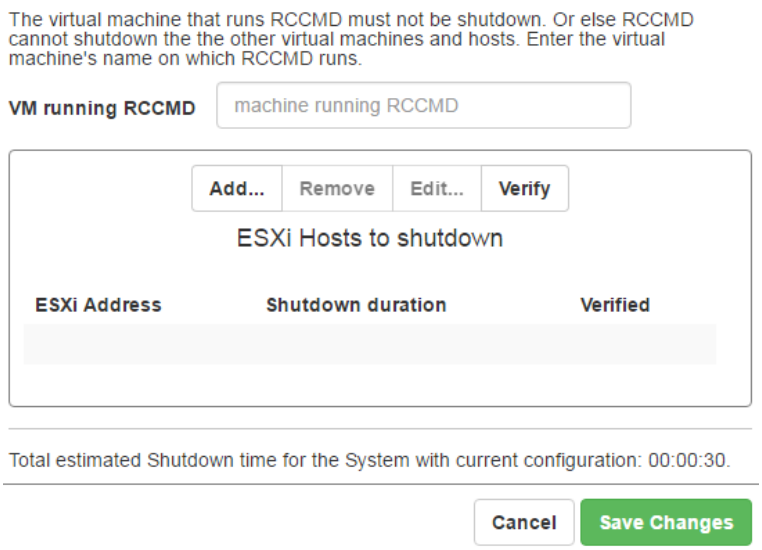


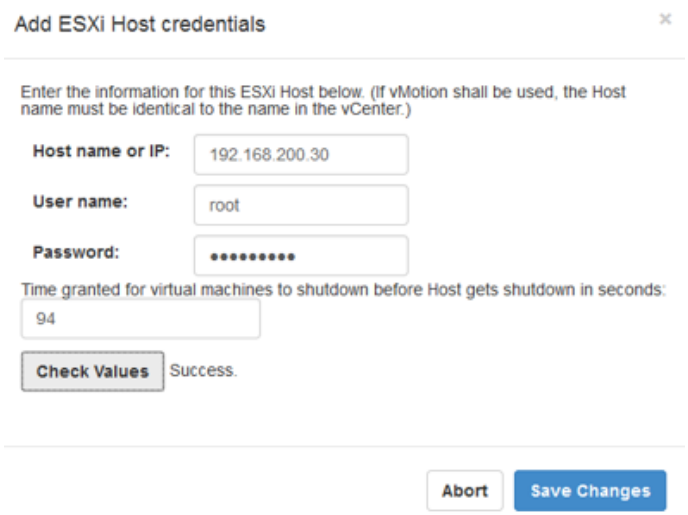
As you can see, it is possible for a single ESXi to set a **specific order in which the machines are shut down**.

In the last menu, you may configure additional ESXi to shutdown.



If you click on “**Add”**, a popup appears where you have to enter the required values for a shutdown. All ESXi are handled equally.





Remember:
RCCMD will not work if no shutdown signal or execution command is sent. An additional device (such as CS121 or CS141) and/ or software (Like UPSMAN or UNMS) is required and must be configured correctly.

For more information, use the documentation from our website (www.generex.de)

5.7 Alternative RCCMD Configuration via Editor

You can edit the „rccmd.cfg“ file (default /usr/rccmd) as follows:

```
########################################
# RCCMD Configuration (v3-default)
########################################

#
# Bind on Interface
# Defines on which interface we listen for incoming commands
# Default: 0.0.0.0 (All possible interfaces on this host)
ListenAddress=0.0.0.0
#
# Listen on Port
# Defines on which interface port we listen for incoming commands.
# Default: 6003
ListenPort=6003
#
# Enable UDP
# Defines if we should listen for rccmd (UDP) broadcasts
# Default: true
ListenUDP=true
#
# Access Control List
# A list of valid sender addresses, only its members can connect to us.
# Seperate IP addresses with a space, e.g.: "192.168.0.1 192.168.0.2".
# Default: <empty> (Everyone is allowed to connect to us)
AllowedAddresses=
########################################
# Alive Check
#
# Enable Alive Check
# Defines if we should perform UPSMan alive checking.
# Default: false
AliveEnabled=false
#
# Alive Check Rate
# Defines the interval of UPSMan alive checking, in seconds.
# Default: 1800
AliveInterval=1800
#
# Alive Retry Rate
# Defines the number of UPSMan alive checking retries, in case of problems.
# Default: 0
AliveRetries=5
#
# Alive Check Group Members List
# A list of UPS device addresses that should be checked periodically.
# Seperate IP addresses with a space, e.g.: "192.168.0.1 192.168.0.2".
# Default: <empty> (No alive checking)
AliveAddresses=
#
# Alive Program
# Full path to script that is executed when an alive check fails.
# Default: rccmd_notalive.sh
AliveProg=/usr/rccmd/rccmd_notalive.sh
########################################
# Redundancy Mode
#
# Enable Redundancy
# Defines if we should operate in redundancy mode.
# Requires an enabled <Alive Check> configuration.
# Default: false
RedundancyEnabled=false
#
# Redundancy Group Members List
```

```
# A list of redundancy group member addresses, must be also in <AliveAddresses>.
# Seperate IP addresses with a space, e.g.: "192.168.0.1 192.168.0.2".
# Default: <empty> (No redundancy available)
RedundancyAddresses=
#
# Redundancy Level
# Defines how many of the <RedundancyAddresses> are redundant.
# Shutdown is executed when the number of shutdown requests exceeds this number.
# Default: 0 (No redundancy available)
RedundancyLevel=0
# Enable Redundancy Script
# Defines if we should NOT execute a script when redundancy suppresses a shutdown.
# Default: false.
RedundancyBatchSuppress=false
# Redundancy Script
# Full path to script that is executed when redundancy suppresses a shutdown.
# Default: ShutdownSuppressed.sh
RedundancyBatchFile=/usr/rccmd/ShutdownSuppressed.sh
# SSL encryption
# enables SSL encrypted messages RCCMD
SSL=false
# Rejection/Acceptance of expired Certificates
# disables SSL communication that try to use expired certificates
SSLRejectExpiredCert=false
ExecProg=/usr/rccmd/rccmd_execute.sh
########################################
vCenter=true
shutdownHosts=192.168.200.34|91
hostshutdownactive=true
ups_vm_name=vMA5.1
Key=secret
Language=english
vMotion=true
vCenterAddress=192.168.200.65
vMotionTimeout=92
```

6 RCCMD on Citrix XEN Server

The RCCMD Software for Citrix XEN Server is a Linux based TCP client for receiving shutdown calls from UPSMAN software (any vendor), CS121/CS141 (any vendor) or other RCCMD licensed applications like SNMP adapters etc. from other vendors.

RCCMD for XEN Server runs on GNU Linux 2.6.18 or higher, which is the basis of the 2008 XEN Serverplatform.

For installing RCCMD please refer to the user manual of RCCMD for UNIX, following we describe some special aspects which are only applicable to XEN Server.

Installation:

Since the XEN Server does not offer any graphical interface, the download of RCCMD client for XEN Server from the GENEREX Website or other sites is not easy – unless you have extra tools installed like commandline browsers like Wget.

Additionally, by default, there is no FTP server active on XEN Server, so a transfer of a downloaded RCCMD package is also blocked. For this reason we recommend to use a local interface on your XEN Server like CD ROM Driver or, USB stick..

- Download RCCMD for XEN Server from the GENEREX Website – using your original RCCMD licensekey (not older than 2 years !) and extract the TAR file. Copy the files on a CD-R and insert this CD now into your XEN Server CD drive. Alternativly use UPSMAN CD ROM Version 5.48 or higher.
- Enter: "`mount /dev/cdrom /media`"
  Since it's a CD ROM in your driver, the system will respond
  "`mount: block device /dev/cdrom is write protected, mounting read-only`"
- Change to the CD ROM by : "`cd /media`" – by "ls" you can see the files on the CD, change now to the folder UNIX (UPSMAN CD ROM) or "**generex**" until you find the installationprogramm "**install**".
- Start now the installation by entering : "`./install`" and follow the instructions on the screen – from here the installation is identical to any other RCCMD installation for UNIX.
- After the installation is finished, a new process will be running on your XEN Server : "`:/rccmd -l`" which means the system is ready now.
- **ATTENTION:** XEN Server has per default a firewall active, which does not allow to send from remote RCCMD signals. To open this firewall you have to edit the file "`iptables`" (/etc/sysconfig #).

Firewall Configuration:
Add all ports on the basis of the following lines

`/etc/sysconfig/iptables`

before the last REJECT rule. The ports are 6003, 5769 and 8443.

Fig. 149: Firewall Configuration

Restart the **iptables** using:

`/etc/init.d/iptables restart`

RCCMD is now listening and will start the file "shutdown.sh" on your XEN Server when any CS121/CS141 or UPSMAN transmit a RCCMD shutdown call. This file shutdown.sh makes an "init 0" shutdown on your XEN Server, edit this file, if you want to use a different shutdown procedure.

Advise: We recommend to install RCCMD on the virtual guest systems too and to shut them down PRIOR of the shutdown of the physical host. Therefore the secure shutdown of the guest systems is assured and avoids the lost of their data.

7 RCCMD on MAC OS 10.X

Note: The RCCMD Installer is using our delivered Java Runtime Environment version, which is used for the installation or rather uninstallation only. In addition the RCCMD Web Configurator is using a Java web-server (jetty). If you want to use RCCMD without Java, delete the entry /System/Library/StartupItems/RccmdWebIf (till MAC OS 10.5) or (since MAC OS 10.5)
/Library/LaunchDaemons/de.generex.rccmdWebif.plist

Menu **„Introduction“:**
In the next menue you can see the progress column where the next steps are visible.

Click the “**Next**” button to continue.

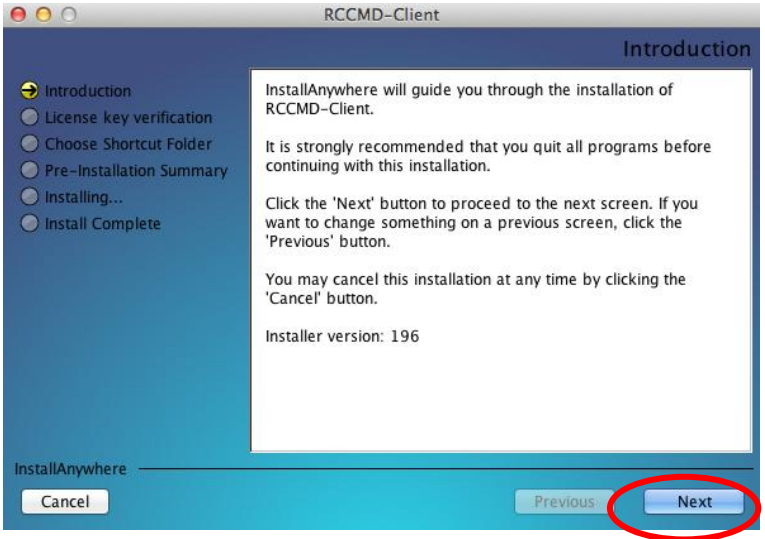


Fig. 150: RCCMD Installation

You need a special **license key** for your RCCMD software. You can identify the key with the “RX3” in the first part of the license key. Most of the times you need to order the key separately.

Click the “**Next**” button to continue.

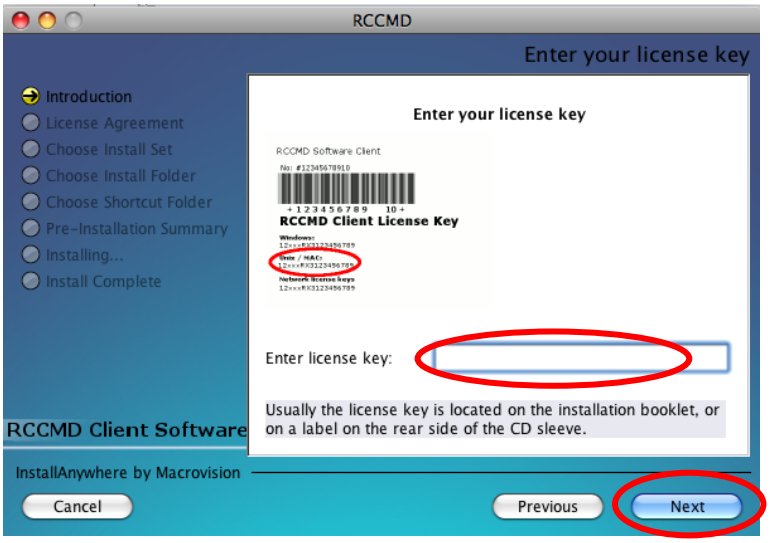


Fig. 151: RCCMD Lizenz Key Enter

Choose an alias **folder**.

Click the “**Next**” button to continue.

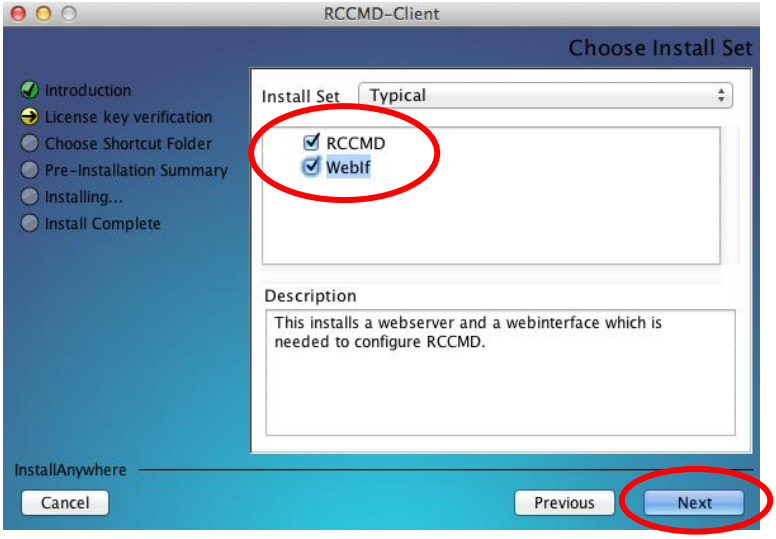


Fig. 152: RCCMD Chosse Install Set

Choose your preferred option.

Click the “**Next**” button to continue.

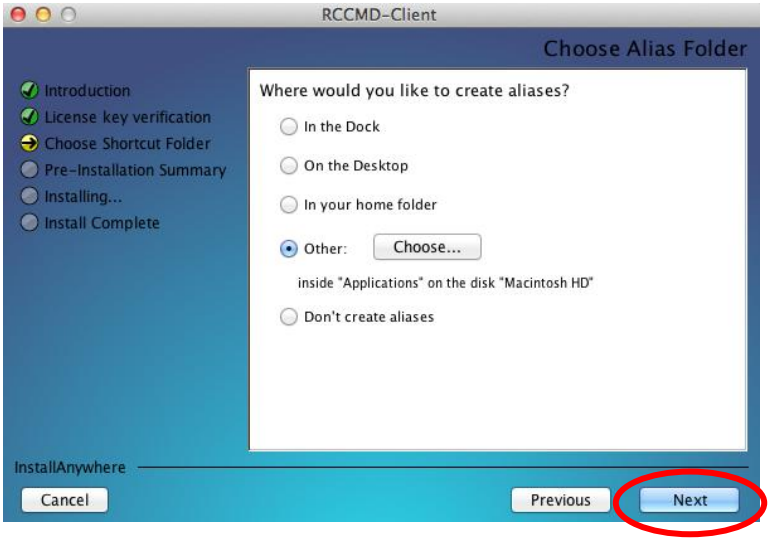


Fig. 153: RCCMD Choose Alias Folder

Select the additional **output options**.

Click the “**Next**” button to continue.

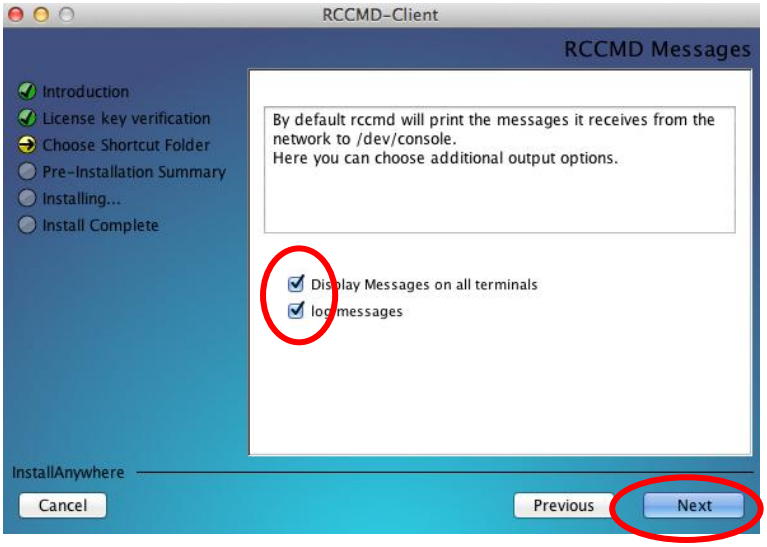


Fig. 154: RCCMD Nachrichten

It continues the **pre-installation summary**.

Click „**Install**“ to complete the installation.

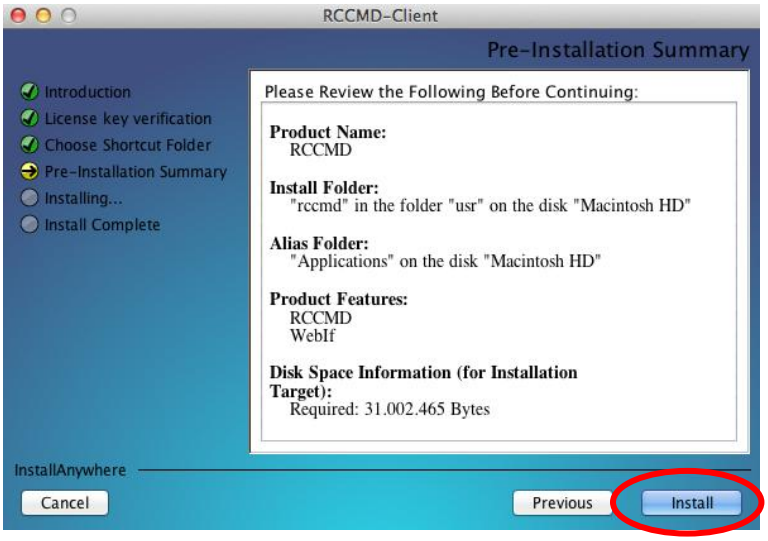


Fig. 155: Pre-Installation Summary

Select these **default values** for the port and protocol of the web-interface or select new ones.

Click the “**Next**” button to continue.

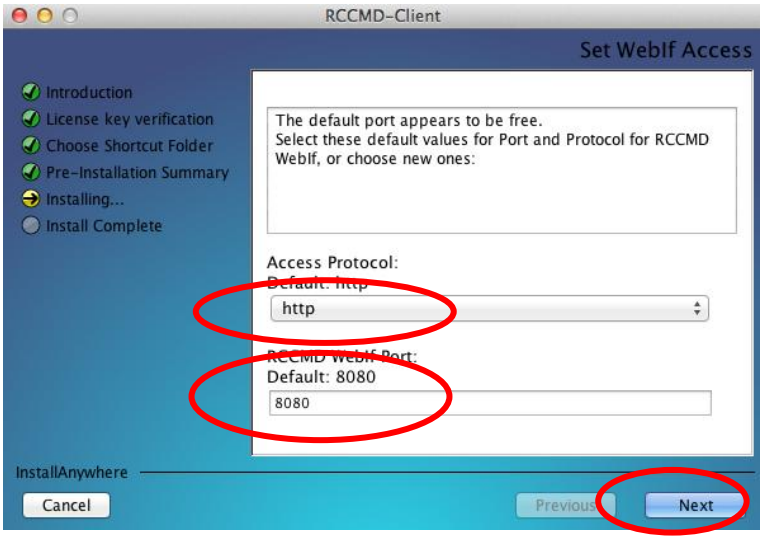


Fig. 156: WebIf Zugriff einstellen

It is possible to create an own password for the RCCMD Web interface. Otherwise, the system uses the standard password „cs121-snmp“.

Click the “**Next**” button to continue.

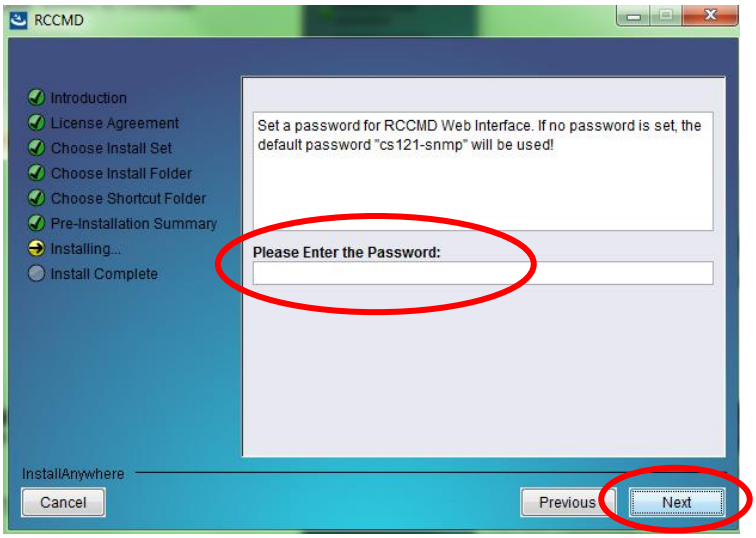


Fig. 157: Kennworteingabe

In the next menu it is possible to create an own password hint.

Click the “**Next**” button to continue.

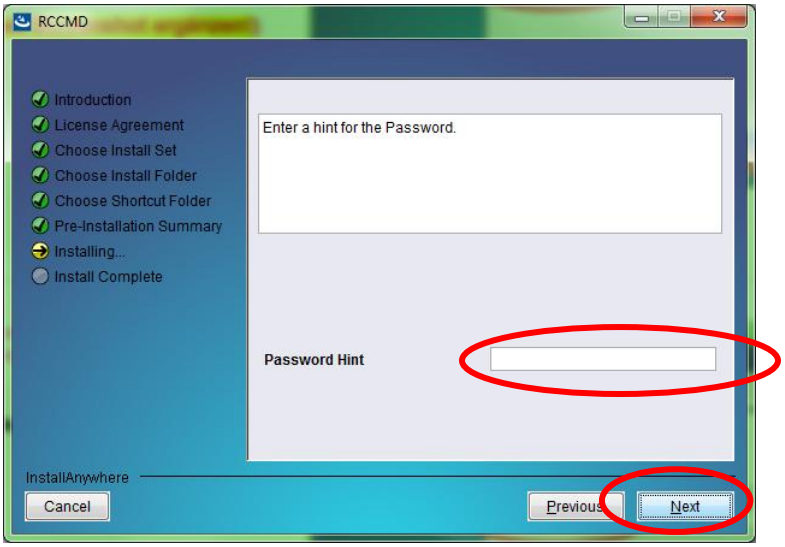


Fig. 158: Passworthinweis-Eingabe

Please read the text below.

Click the “**Next**” button to continue.

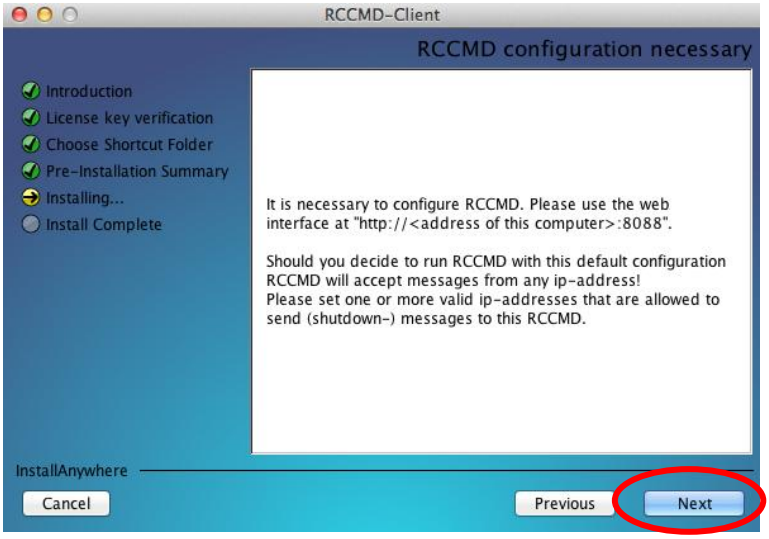


Fig. 159: RCCMD Configuration required

Menu „**Install Complete**“:
RCCMD has been installed successful.

Click the “**Done**” button to finish the installation.

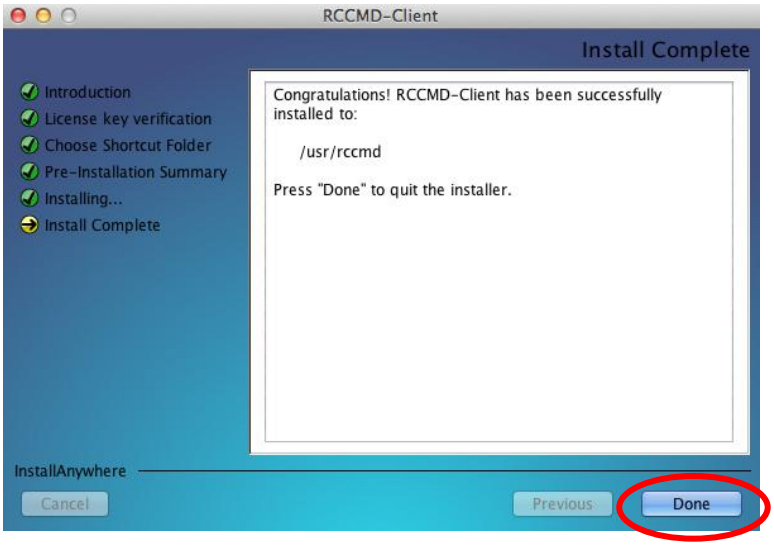


Fig. 160: RCCMD Install Complete

7.1 RCCMD WebInterface (from Version 4.2.0.0)

RCCMD provides its own web-interface from version 4.2.0.0 or higher. Therefore it is possible to configure and control RCCMD remotely. After the successful installation, your default web-browser of your OS starts automatically.

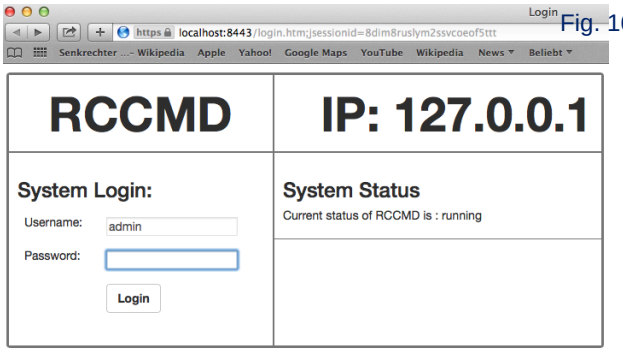


Fig. 161: RCCMD WebInterface

Menu **„Connections“:**

You can enter the **IP addresses** of the allowed RCCMD senders (CS121/CS141/UPSMAN) into the “Connections” menu. Click the “**Insert**” button to enter the IP address of the 1st ender. Click the “**Remove**” button, if you want to remove the already entered IP address. Click the “**Edit**” button, if you want to edit the entered IP address.

You can define under “**Protocol**”, if RCCMD should use **SSL certificates**. Enable the “**Reject expired SSL certificates**”, if you want to reject connections with expired certificates.

Click the “**Save Changes**” button prior of the leaving of this site to save your changes.

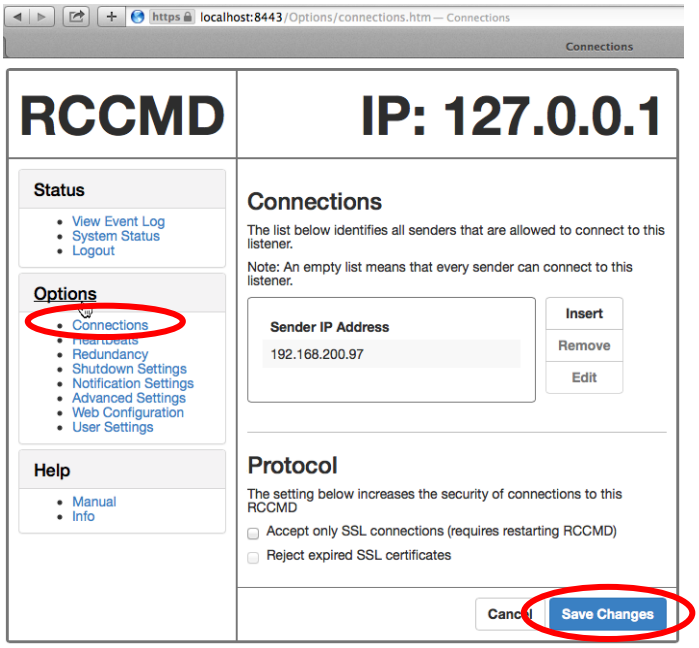


Fig. 162: RCCMD WebInterface – Connections

Attention: If you do not enter an address, then every server has the permission to send a shutdown command.

“Heartbeats”. This check is a signal, that will be send to the CS121/CS141/UPSMAN via port 5769, if the UPSMAN service still got UPS data. If not, the script file “alive.bat” will be executed, which will trigger an accordant pop-up message.

The feature “**by the use of CS121/UPSMAN Traps**” provides UPSMAN/RCCMD/UNMS messages, which will display the UPS status as message. If enabled, this feature will trigger a message, if the UPS status of the UPSMAN/RCCMD servers has changed.

Menu **“Heartbeats”:**

You can enable the “**UPSMAN Alive Check**” feature into the menu

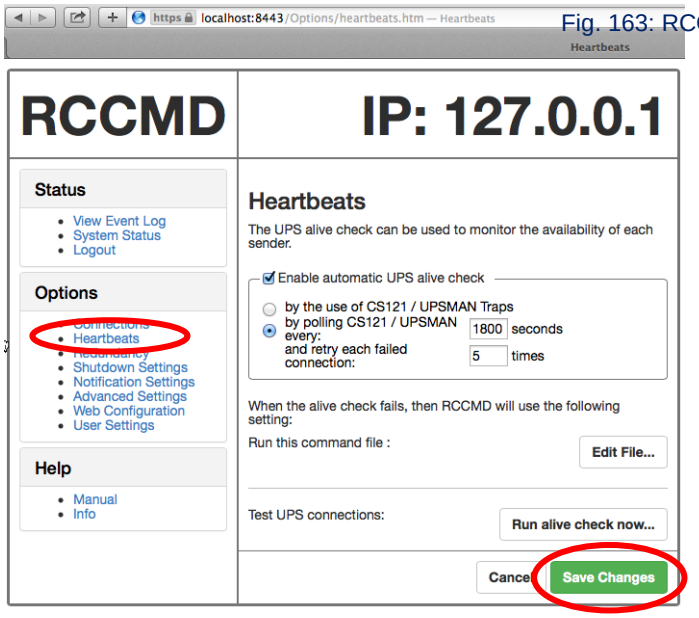


Fig. 163: RCCMD WebInterface – Heartbeats

The feature "**by polling CS121/UPSMAN every x seconds**" provides the pure signal polling without receiving UPS data or rather messages.

The polling rate (default 1800 seconds) defines the polling of the UPSMAN service, connection retries (default 100) means after 100 unsuccessful connection tries an alarm will be triggered.

You can test the UPS connection, if you click the "**Run alive check now…"** button (the port 5769 will be tested).

Click the "**Save Changes**" button prior of the leaving of this site to save your changes.

Menu „**Redundancy**":

You can enable the **redundancy management feature** into the menu "Redundancy". The **redundancy level** defines the number of redundant senders in the redundancy group. This means, that level 1+ senders must have sent a shutdown signal before this RCCMD starts its shutdown sequence.

When redundancy suppresses a shutdown, then RCCMD will trigger the "suppressed.bat". You can edit this file, if you click the "**Edit file…"** button.

Please note, that it is required to configure a reset of the redundancy alarm on the sender (CS121/CS141/UPSMAN).

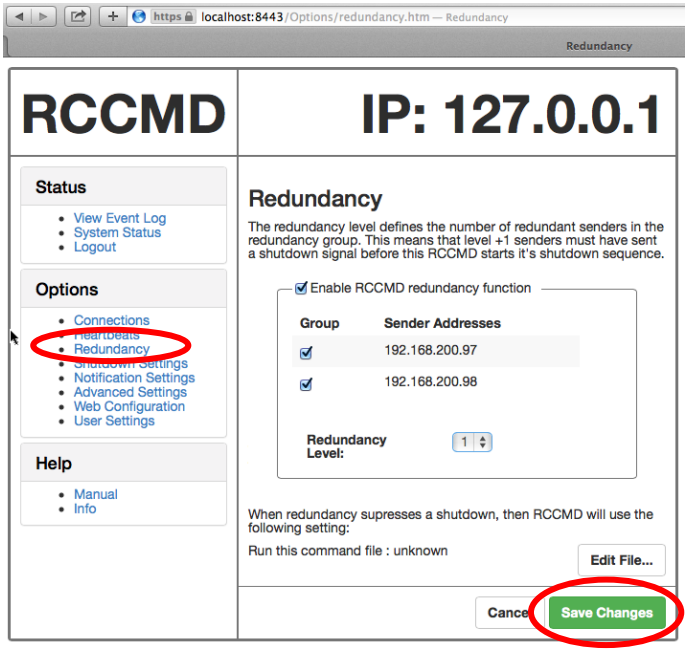


Fig. 164: RCCMD WebInterface – Redundancy

You can use the function „**Send RCCMD cancel shutdown**", to discard a previously sent shutdown automatically. If a shutdown was suppressed, because of the existing redundancy at this point of time, but the problem was solved at the UPS intermediate, you can reset the shutdown with the function „**Send RCCMD cancel shutdown**". The client, which received the shutdown, will be encouraged to reset it.

Click the "**Save Changes**" button prior of the leaving of this site to save your changes.

Menu **„Shutdown Settings“:**

You can change or rather extend the shutdown sequence.

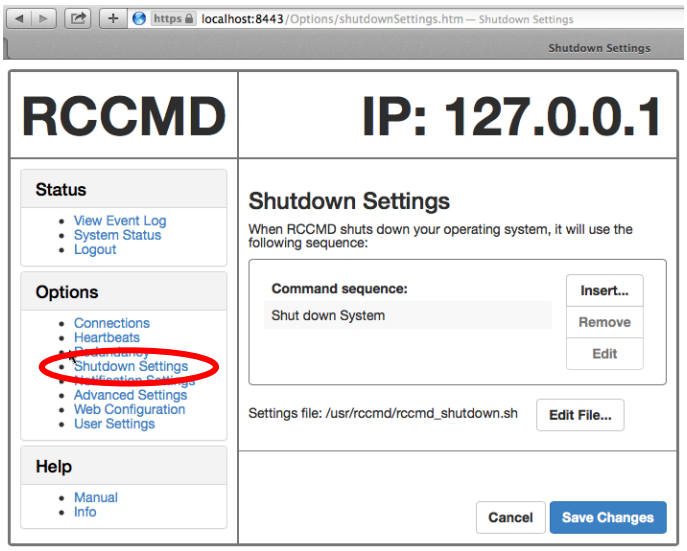


Fig. 165: RCCMD WebInterface – Shutdown Settings

Menu „**Notification Settings**“:

You can change or rather extend the default **bat files** for E-Mail, Message and Execute, if you click the “Edit File…” button.

Click the “**Save Changes**” button prior of the leaving of this site to save your changes.

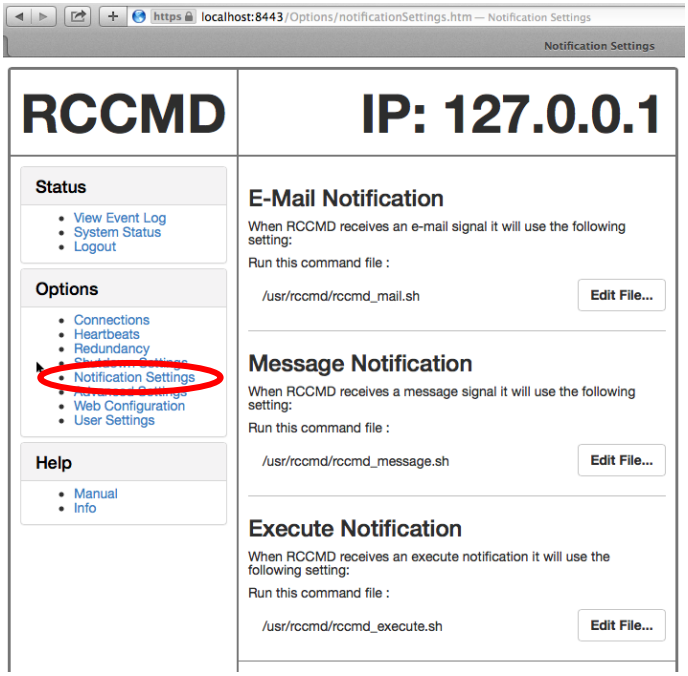


Fig. 166: RCCMD WebInterface – Notification Settings

Menu „**Advanced Settings**“:

You can define the **maximum size of the event logfile** into the menu “Advanced Settings”, where the overwriting of older

entries will start, the **RCCMD bindings** for the IP address, the RCCMD listener TCP port and the RCCMD Tray Message Port, which will be used for the RCCMD messages.

Click the "**Save Changes**" button prior of the leaving of this site to save your changes.

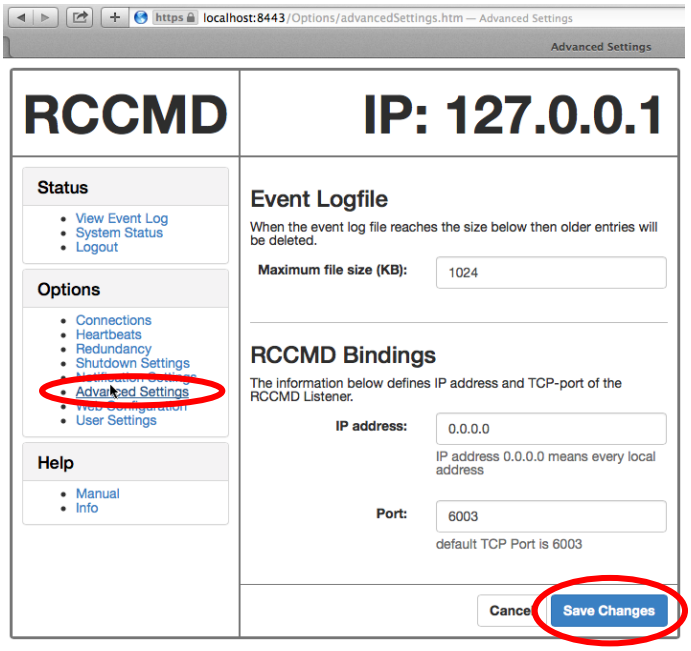


Fig. 167: RCCMD WebInterface – Advanced Settings

Menu „**Web Configuration**":
You can change the default password for the user "admin" into the menu "Web Configuration". In addition you can disable the **HTTPS protocol**, if you just want to use the HTTP protocol. The RCCMD version 4.2.3.0 or higher provides the feature of changing the default ports for HTTP and HTTPS.

Click the "**Save Changes**" button prior of the leaving of this site to save your changes.

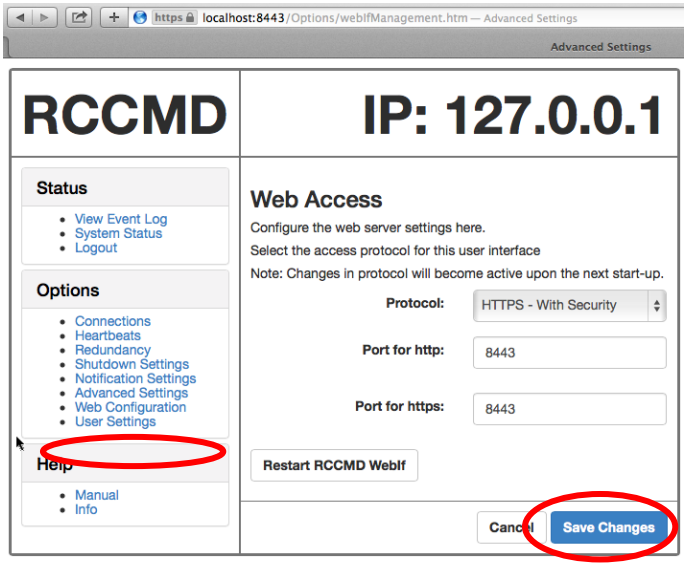


Fig. 168: RCCMD WebInterface – Web Access

User Settings menu
Here you can change the default password for admin.

Afterwards you have to restart the RCCMD service!

Click the "Save Changes" button prior of the leaving of this site to save your changes.

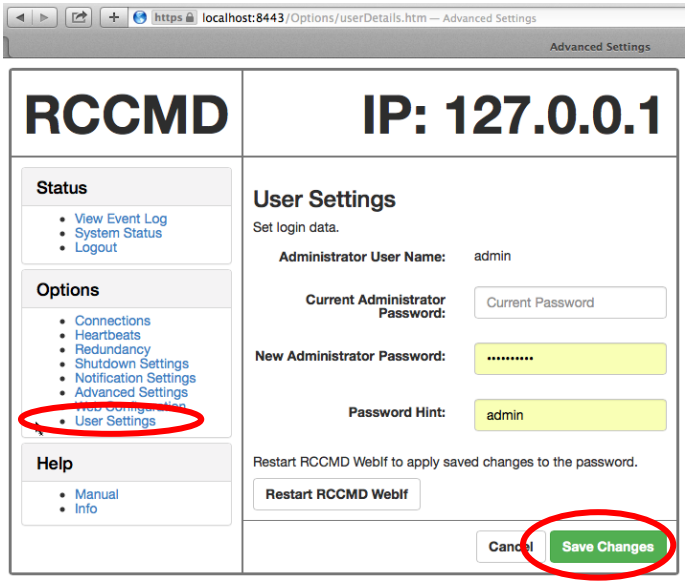


Fig. 169: RCCMD WebInterface – User Settings

Click „Logout“ when RCCMD configuration is finished.

Menu „**Status, View Event Log**“:
You can see the **logging of the events** into the menu “Status, Event Log”.

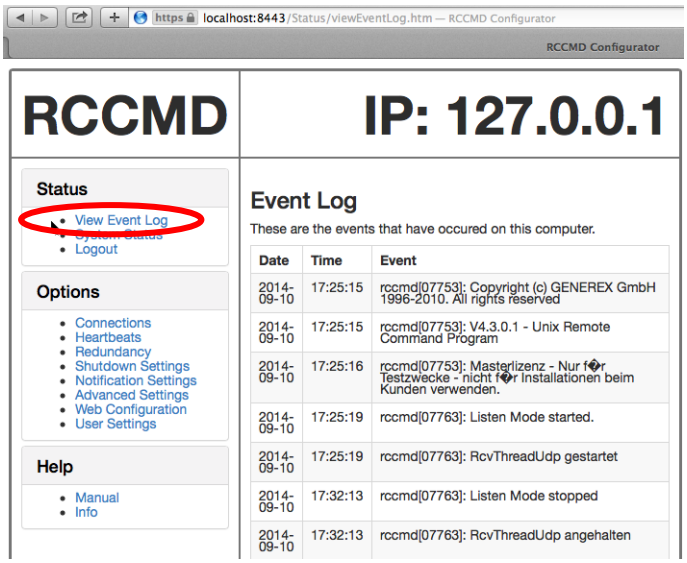


Fig. 170: RCCMD WebInterface – Event Log

Menu **„Status, System Status“:**
You can check the current **status of RCCMD** into the menu “Status, System Status”, **update** the status and **restart** or rather **stop/start** the RCCMD service.

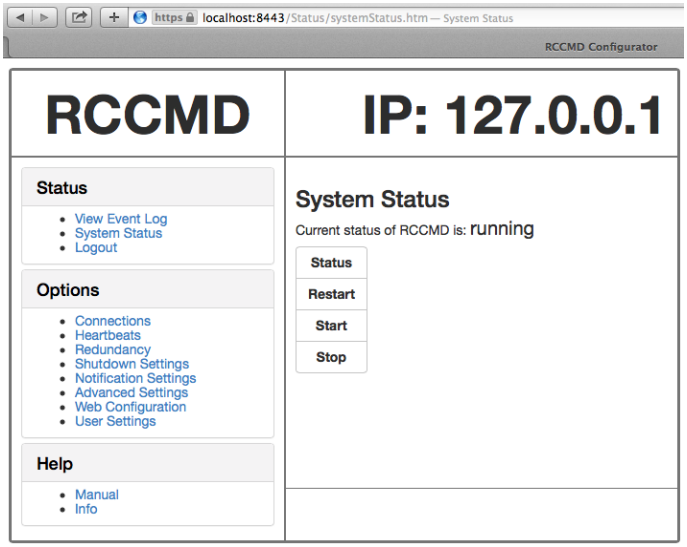


Fig. 171: RCCMD WebInterface – System Status

Menu „**Help**“:
You can open the RCCMD **user manual** into the menu “Help” ad you can follow the link to www.generex.den .

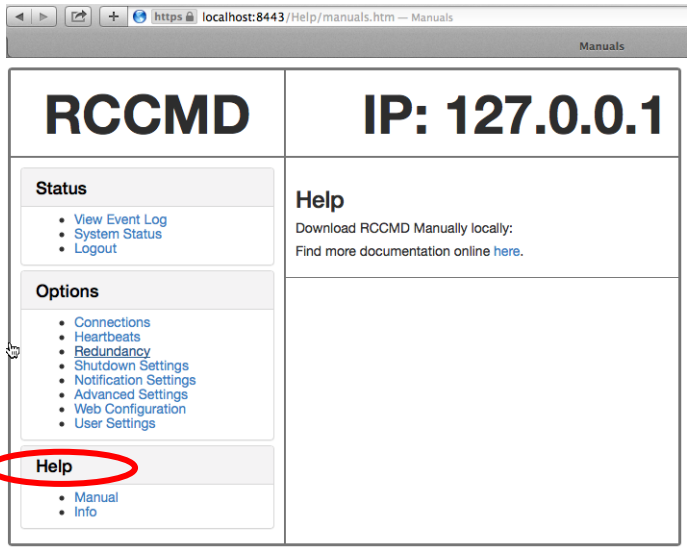


Fig. 172: RCCMD WebInterface – Help

7.2 RCCMD WebInterface Remote Access

RCCMD provides its own web-interface from version 4.2.0.0 or higher. Therefore it is possible to configure and control RCCMD remotely. Please note, that the firewall port 8443 TCP is enabled. Enter the following into a web-browser, to connect to a workstation, where RCCMD is running:

https://IP address of the RCCMD client: 8443

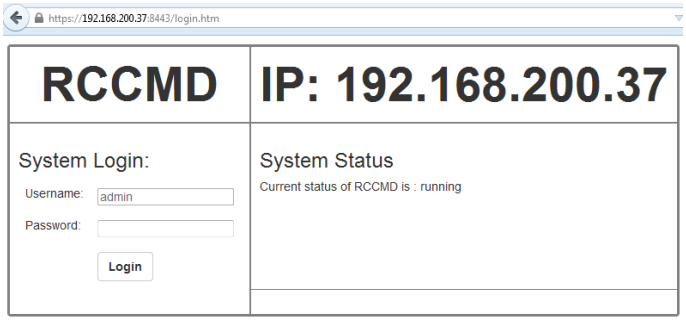


Fig. 173: RCCMD WebInterface – Remote Access

Now you can access the configuratior by remote.

7.3 Old RCCMD Configuration on MAC OSX

Menu „**Addresses**“:
Add the **IP address** of the RCCMD server, which is allowed to send a shutdown to this client..

Attention: If you do not enter an address, then every server has the permission to send a shutdown command. If more than one CS121/CS141 or UPSMAN is existent, thus a redundancy situation, you need to enter more than one address as authorized sender.

Click the “**OK**” button to continue.

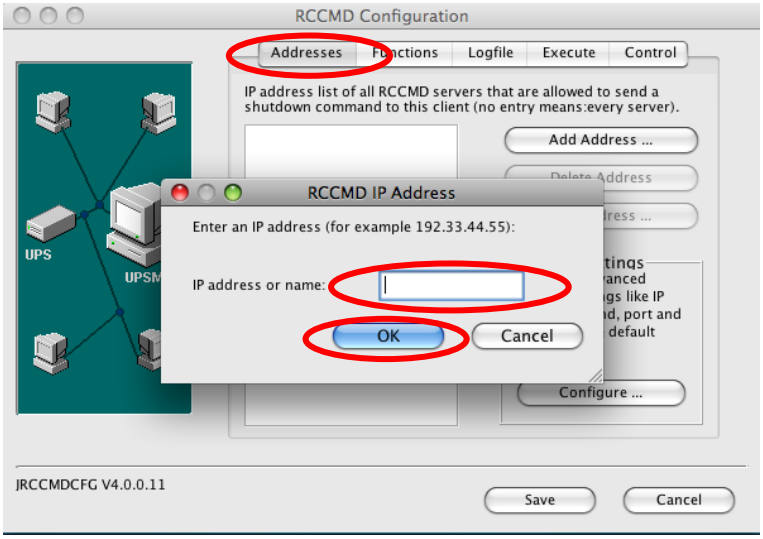


Fig. 174: RCCMD Address Window

Menu „**Functions**“:

If you want to use the UPSMAN alive checking (recommended), check the “**Enable connection check**” box. Alive check is a signal, send out to the UPSMAN or CS121/CS141 on port 5769 to check if the UPSMAN has still UPS data – or not. If this fails, the scriptfile alive.bat will be executed which causes a messagbox coming up. The polling rate (default 30 min.) defines the polling of the UPSMAN service, connect retries (default 5) means after 5 unsuccessful connection tries an alarm will be triggered.

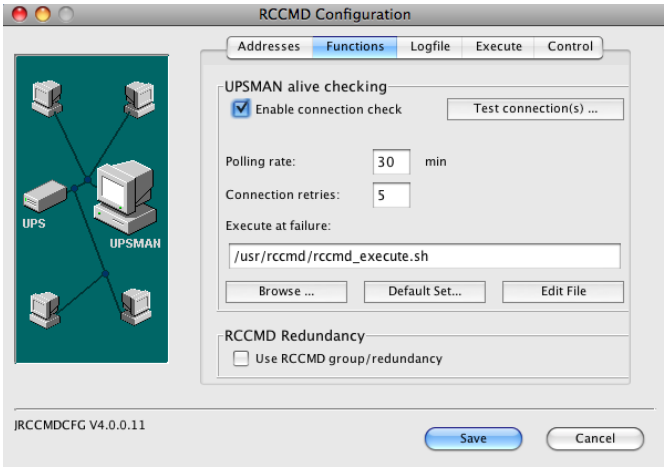


Fig. 175: RCCMD Configuration Window „Functions“

“**Use RCCMD Traps**” enables UPSMAN/RCCMD/UNMS notifications which show the UPS status. If activated, these function will show local messages on status changes.

If you click the “**Test connection(s)…”** button, the UPSMAN alive checking of the entered IP addresses will start (port 5769 will be tested).

If you click the „**Browse...**“ button, you will get a selection of the default batch files.

If you click the „**Default setting**“ button, you will get back to the default batchfile (alive.bat).

At the failure of the UPSMAN alive checking, you can define an executing file or edit the default file “alive.bat”.

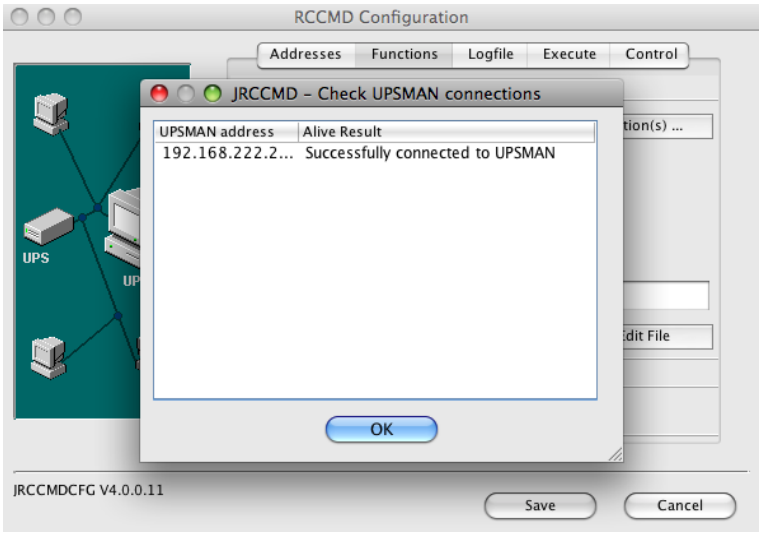


Fig. 176: RCCMD Check UPSMAN Connections

At UPS installation RCCMD offers a redundancy management functionality as follows:

Every UPS must be equipped with a CS121/CS141 or UPSMAN software computer. When ticking the box “**Use RCCMD group/redundancy**” – you are guided to a menue where you can choose which CS121/CS141/UPSMAN are supplying this RCCMD client. E. g. if 4 CS121/CS141/UPSMAN are installed into 4 UPS – than each may send a shutdown signal to this RCCMD client.

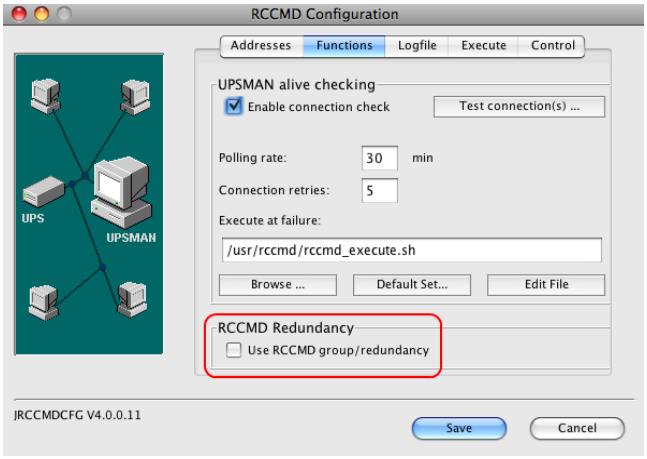


Fig. 177: RCCMD Redundancy

Menu „**Logfile**“:
You can configure the **log file size** and edit the executing bat files in this installation window.

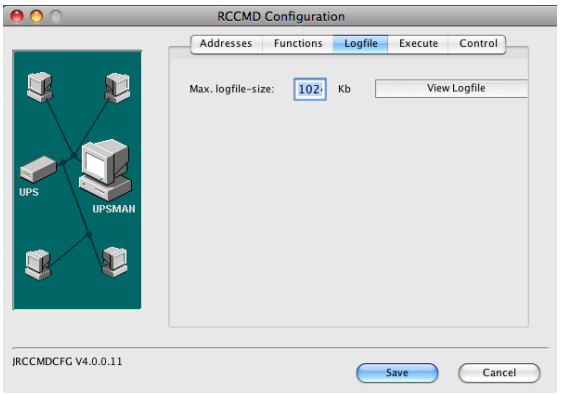


Fig. 178: RCCMD Configuration Window „Logfile“

Menu „**Execute**“:
If you click the „Configure...“ button, you will be able to enter the mail settings and to use the mail function of RCCMD.

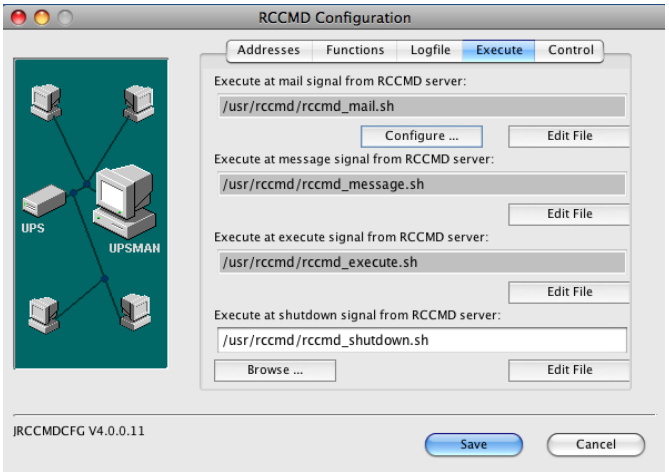


Fig. 179: RCCMD Configuration Window „Execute“

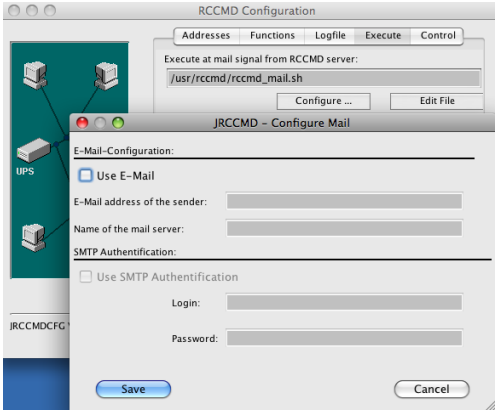


Fig. 180: RCCMD Email-Configuration

The RCCMD version 4.0.2.0 provides a **grafical configuration** of the **shutdown sequence**.

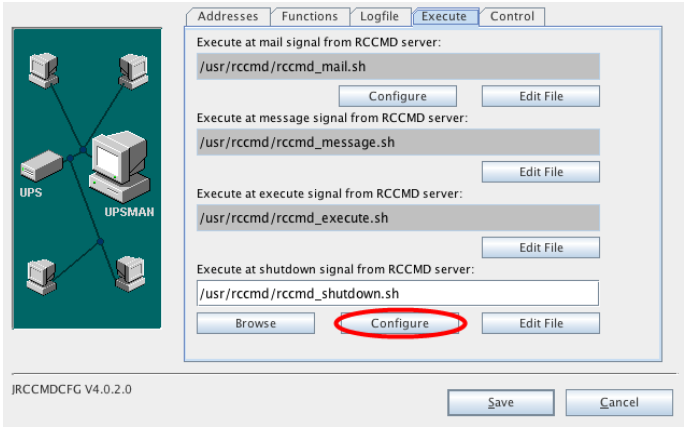


Fig. 181: Configuration – RCCMD Shutdown.sh

Click the „**Configure**“ button to enter the shutdown sequence settings.

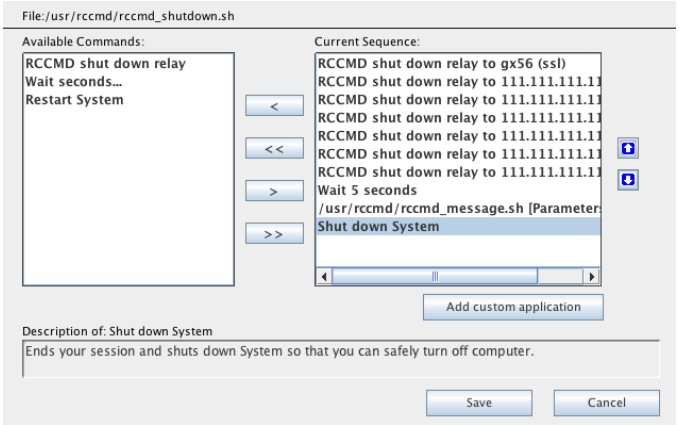


Fig. 182: Configuration – RCCMD Shutdown Sequenz

The following commands are available:

RCCMD shutdown relay: Relays RCCMD shutdown command to another workstation. Enter the IP address or the hostname of the remote station you want to shutdown.

Wait seconds...: Waits a duration in seconds until the next command will be executed.

Restart System: Ends your session, shuts down the system and restarts it.

Shutdown System: Ends your session and shuts down the system, so that you can safely turn off the power.

Click the „**Control**“ button to get into the folowing screen:

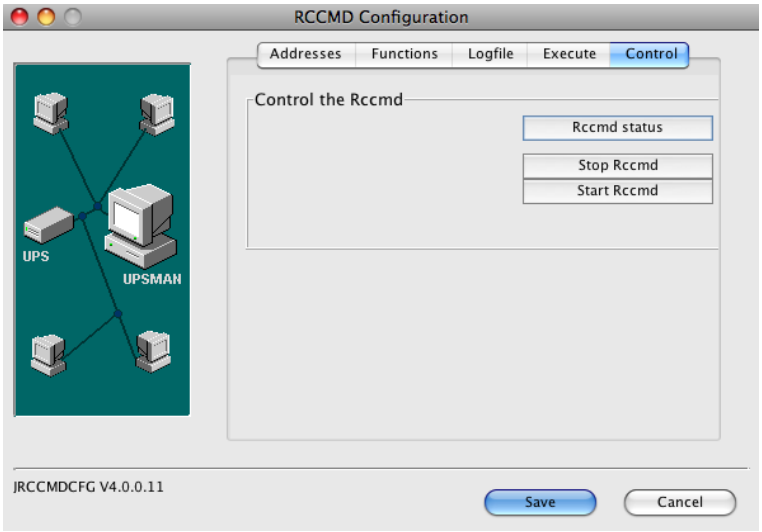


Fig. 183: RCCMD Control

8 RCCMD on NovellNetWare

Download the RCCMD netwar5.zip file. Extract it to any folder of your Windows or Novell server. Create a directory “UPS” on the Netware SYS Volume (e.g. F:\UPS). Copy the extracted file to this folder. Execute the following:

```
load rccmd.nlm –l –a load down.ncf
```

The following text is presented when entering RCCMD with the help parameter “?” inside a NovellNetWare console:

```
Possible parameters:

 -l
     listen. waits for a command from RCCMD sender

 -s
     sends a ping to a listening program

 -se <command> <param>
     sends a command to a listening program

 -p  <port>
     Portadress (Defaultadress = 6003)

 -a  <ipaddress>
     Address in IP Format. Ex. -a 192.10.20.30 (max. 10)

 -t  <timeout>
     Time in Seconds (Defaulttimeout = MAX_TIMEOUT)

 -?
     this help

Supported Commands (for use with -se argument):

 SHUTDOWN
          This will call the configured shutdown-batchfile (default:
shutdown.bat)

 EXECUTE
          This will call the execute.bat file

 MSG_TEXT
          This will call the message.bat file                          <text,
unrestricted word count>

 MSG_ID <ID>
          This will call the message.bat file                          <message
parameters, seperated by blanks>

 LOG_TEXT
          This will write to configured log-file (default: rccmd.log) <text,
unrestricted word count>

 LOG_ID <ID>
          This will write to configured log-file (default: rccmd.log) <message
parameters, seperated by blanks>
```

```
Examples:

 load rccmd.nlm -s -a 192.10.200.52 -a 192.10.200.53
 load rccmd.nlm -s -a 192.10.200.52 -a 192.10.200.53 -t 10
 load rccmd.nlm -se "SHUTDOWN" -a 192.10.200.52

 load rccmd.nlm -se "EXECUTE" -a 192.10.200.52
 load rccmd.nlm -se "MSG_TEXT this is a message" -a 192.10.200.52
 load rccmd.nlm -l
 load rccmd.nlm -l -a 192.10.200.53 -a 192.10.200.52
 load rccmd.nlm -l -a 192.10.200.52

If you have added a search path i.e.: "search add sys:rccmd",
otherwise you have to use the absolute path.

 load sys:rccmd\rccmd.nlm -l
```

To start RCCMD in receiving-mode (listen) enter the following line:

load <path> RCCMD -l [-a 192.200.100.10] [-p 6003] load <path> shutcmd.nlm –f

Optional parameters:

-a <address> TCP/IP address of the master computer(s), which sends the RCCMD-signal.

-p <port> (optional) TCP-Port address, on which the master computer is sending

To start RCCMD in sending-mode (send) enter the following line in your shut¬down-job:

load RCCMD -s -a <address> [-p 6003]

For <address> enter the TCP-address of the machine to which you want to send the RCCMD-signal. (Workstations in "listening" mode, with an active RCCMD with parameter -l)

Optional parameters:

-p <port> TCP-Port, which the RCCMD-signal is using.

The option -a can be used multiple times, if a shutdown on remote network servers should be initiated.

Example: (Example path <path> = sys:\ups\upsman\rccmd.nlm)

load <path> RCCMD.NLM –s –a 192.168.210.3 -a 192.168.210.4 -a 192.168.210.10

...etc.until ”end of line”

unload RCCMD

load <path> RCCMD.NLM –s –a 192.168.210.8...etc.

unload RCCMD

Do not use the CD License key more than once. If more RCCMD modules need to be installed for the shutdown, additional CD license keys must be purchased. Additional license keys are available from your UPS dealer, whereas the CD can be used again for the actual installation.

rccmd.nlm

Modul for the multiserver shutdown in IP-networks.

The rccmd.nlm contains different command line parameters, which are either for the ”send” or ”listen” modul of the RCCMD modul.

rccmd -? Help

rccmd -s Sending off a ”ping” signal to a waiting program

rccmd -lWaiting for a ”ping” signal. A command can be executed after the reception of the ”ping” signal.

rccmd –p Setting the port address (default = 6003).

rccmd –a Address in IP format e.g. 192.168.202.1

rccmd –t Time in seconds until a connection will be established. (default timeout = 10)

Example:

load sys:ups\rccmd.nlm -s -a 192.168.202.1 [-a 192.168.202.1]

load sys:ups\rccmd.nlm -s -a 192.168.202.1 -t 10

load sys:ups\rccmd.nlm -l -a 192.168.202.1 shutcmd.nlm [/para]

rccmdipx.nlm

This is a modul for just IPX networks. This modul sends a shutdown command (or any other console command) directly to every IPX server name. Please start RCCMDIPX on all Novell consols. The modul needs to be loaded on both servers.

This modul has to loaded on both servers first

(1. Rename RCCMDIPX to RCCMS.NLM 2. Load RCCMD The following syntax is valid:

rccmd <server name> <console command>

Whereas <server name> is a valid server in a network enviroment and <console command> a valid NetWare command is.

Example:

1. load sys:ups\rccmdipx (or load RCCMD if RCCMDIPX.NLM is renamed to RCCMD.NLM)

2. rccmd gnw1 forcedown

or 1. load sys:ups\rccmdipx

2. rccmd gnw1 sys:ups\down.ncf

Instead of the down command for older clib.nlm files, the forcedown command maybe used.

Multiple-start RCCMD on Novell

The multiple start RCCMD on Novell is relatively easy to manage. Several RCCMD clients may be started with the following command line:

load rccmd.nlm -l -a load down.ncf

whereas the syntax goes as follows:

LOADING RCCMD.NLM -L(LISTENER) -A(IP adress of UPSMAN/CS121/CS141/RCCMD SENDER) COMMAND (COMMAND TO BE EXECUTED)

Example:

LOAD RCCMD.NLM -L -A 192.168.10.2 LOAD DOWN.NCF

In this scenario the “down.ncf“ file is executed, which leads to an immediate shutdown of the client computer, if the RCCMD call from the RCCMD server (sender) is received. Other . ncf or .nlm (executables) files may be executed too.

A group of 8 .ncf example files can be found in the UPSMAN installation directory. Please note that these example files ma have to be adjusted by user/administrator according to the configuration of the system.

9 RCCMD on DEC VMS

The UPS-Management-Software CD contains the RCCMD software. The VMS RCCMD installation can be done by following the UNIX installation instructions in this manual, all of the steps are the same.

Note: The VMS license is not part of the standard CD; It is to be ordered separately. It is not permitted to use the VMS version and its RCCMD modules without registered license.

Prior of the installation you should verify that port 6003 is not in use. Check this with the command « netstat –an ». Ensure that there is no other process running or start the RCCMD module at another port address with the option –p for sending and receiving. Ensure too, that you will use this port for every command in the network. Please follow the instructions of the next chapter carefully. For further help you may use the user manual and the troubleshooting pages or contact your UPS software dealer.

Important: The Alpha-Version is linked to OpenVMS 7.1. For OpenVMS 6.x use the Version 6.x in the following CD directory (ex. DKA200:[VMS.ALPHA.6X]).

Installation procedure:

- Connect the workstation to the network.
- Login into the VMS System using SYSTEM login.
- Mount the CD-ROM device (if DKA200 is the device name of the CD-ROM):

$ MOUNT/OVERRIDE=IDENT DKA200: UPS UPS:

This is a system specific command. Use the VMS help pages for your system or ask the system operator, if you do not know, how to mount your input device.

- Start the VMS install procedure by: @SYS$UPDATE:VMSINSTAL
- or: @SYS$UPDATE:VMSINSTAL <device>
- e. g.: @SYS$UPDATE:VMSINSTAL RCCMD DKA200: [VMS.ALPHA]

VMSINSTAL is an interactive script, so just follow the installation instructions on the screen (all instructions are aditionally listed in the following subjects 5-11).

- Answer YES at the prompt: "* *Are you satisfied with the backup of your system disk [YES*]"
- Answer the prompt: "* *Where will the distribution volumes be mounted*:" with your correct input device name e. g.:

CDROM: *dka500: [VMS]* (your CDROM device and path [VMS], the device may be different on your system).

- Answer the prompt*:"* *Enter installation options you wish to use [none]:"* by pressing RETURN
- At the prompt*:"Please mount the first volume of the set on MKA300:." "* *Are you ready?"* please insert your tape (or disk or CDROM) and answer *"yes"*
- Enter the license key of your RCCMD version
- Enter the complete path of the target directory, e. g.: *dka100: [ups]*
- Answer the question *"Would you like to start the RCCMD module automatically on your system".*
- Exit the VMSINSTALL procedure by RETURN at the "*Product:" prompt and change to your target UPS directory (e. g.: set default dka100: [ups])
- Now install the RCCMD software in sending mode on your RCCMD server workstation. Your server workstation is the computer, which is connected to the UPS via the RS232 port.

DEC ALPHA CD Problems: If the CD could not be mounted or if you have problems to start the VMSINSTAL script on the DEC ALPHA hardware, please follow the instructions below:

- Copy the archive VMSA.ZIP (ALPHA directory) into a temporary directory on your system. COPY RCCMD.ZIP DKA100:[TEMP]

If you have not installed the ZIP utilities on your workstation already, you have to assign a system value: UNZIP==$DKA200:[VMS.ALPHA]UNZIP.EXE, where DKA200: is your CDROM device.

- Unpack your VMS UPS archive:

SET DEF DKA100:[TEMP] UNZIP RCCMD.ZIP

- Start the VMS installation routine: @SYS$UPDATE:VMSINSTAL RCCMD DKA100:[TEMP]

Configuration procedure:

After the installation there are 3 command files:

- RCCMDSTART.COM: RCCMD startup command file should be called in the VMS startup file
- RCCMD.COM: Command file to start RCCMD program itself, this should be configured to your requirements
- RCCMD_SHUTDOWN.COM: sample command file which could be called by RCCMD to shutdown VMS

Configure the RCCMD.COM command file by calling the RCCMD program with the following command: “rccmd –l” optional you can use “rccmd –l –a<IP address of the sender> -p <port (standard 6003)>”. After that you can start the RCCMD by caklling the command file RCCMDSTART.COM with “@rccmdstart”.

Check the process by calling “show system”. There should be a process with the name RCCMD.

The automatic startof the RCCMD should be initiated from the VMS startup file. You may use the enclosed script rccmdstart.com. Add a line to your startup file (prior to the exit command):

$ @your_disk:[your_path]rccmdstart.com (e. g.: $ @dka100:[ups]rccmdstart.com)

The UPS software will be started automatically after the next reboot.

10 RCCMD AS400-Client

RCCMD for AS 400 an iSeries is not described in this manual, but has identical functions as any other RCCMD. RCCMD for AS 400 comes with a separate user manual with the product.

Download AS400 RCCMD Manual

11 RCCMD FAQ

In this chapter we will give you some solutions of well known problems.

FAQ – Frequently Asked Questions

Problem : The execution of « sudo sh rccmd_shutdown.sh » on ESXi 4 with vMA 4.1 fails with the following error message or similar :

“Compilation failed in require at /usr/lib/perl5/site_perl/5.8.8/VMware/VIFPLib.pm line 10. BEGIN failed”

“compilation aborted at /usr/lib/perl5/site_perl/5.8.8/VMware/VIFPLib.pm line 10. Compilation failed in require at /usr/rccmd/upsVIShutdown.pl line 12.”

“Can't load '/usr/lib/perl5/site_perl/5.8.8/libvmatargetlib_perl.so' for module vmatargetlib_perl: libtypes.so: cannot open shared object file: No such file or directory at /usr/lib64/perl5/5.8.8/x86_64-linux-thread-multi/DynaLoader.pm line 230.”

“BEGIN failed--compilation aborted at /usr/rccmd/upsVIShutdown.pl line 12. at /usr/lib/perl5/site_perl/5.8.8/VMware/VmaTargetLib.pm line 10”

Reason: The procedure of the authentication is completely different from vMA 4.0 to vMA 4.1. The integration of RCCMD is not possible unless you use a newer version of RCCMD or to use vMA 4.0 instead.

Solution : Use the vMA 4.0. A new setup for integration of the vMA 4.1 will be released after November 2010.

Problem : You get the following error, after the execution of the upsVIShutdown.pl

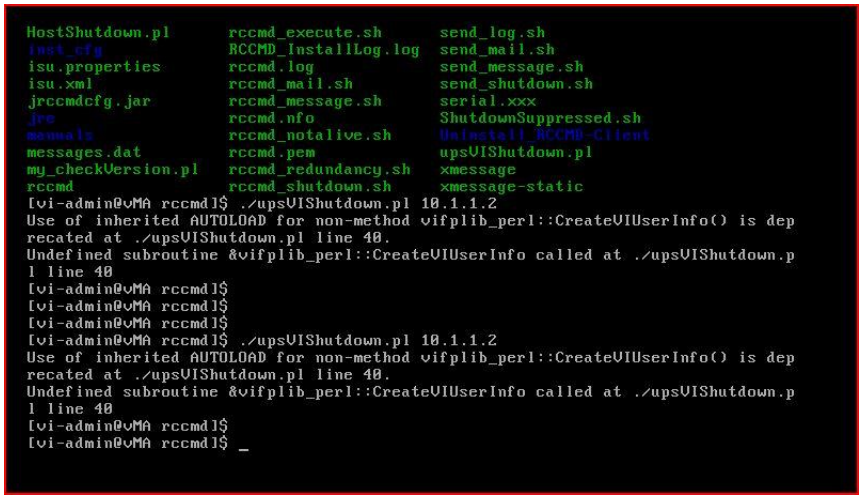


Fig. 184: Error after execution of upsVIShutdown.pl

Solution: You do not use the latest RCCMD version. Please download the current RCCMD version from our website www.generex.de .

Problem: Shutdown of NetApp storages

Solution: Typically all low-cost NAS systems export their NFS shares in the "asnyc" mode. This is an extremly fast write process, which secures, that no data is lost if the power suddenly fails. As long as the user has not changed the default NFS protocol write mode from "async" to "sync", than there is no risk to lose data.

Anyhow an UPS should be connected to any NAS to avoid, that network computers will not be shut downed but rather will die down. For this case, we recommend to connect an UPS to the NAS and we think it makes sense to connect an UPS to a NAS system.

Otherwise it is enough, if the computers will be shut downed via RCCMD, if a powerfail occurs. If the computers are down, there are no open data anymore, that can be lost. You could switch off any NAS as soon as the network computers are down.

Specific feature: QNAP/NETAPP systems are using the “sync” mode and are therefore faster and more sensitive accordingly, but these devices possess an own battery, to assure a secure shutdown at any time. This internal battery clears the cache and parks the recording head, if no data have to be stored. So, you will not lose data, if the network computers are down.

We do not think, that an additional cable connection between the UPS and the NAS is required, if it is assured, that the computers are down.

Problem: Error messages at “UPSMAN Alive Check” on Windows Server 2008

Solution: The firewall port 5769 has to be enabled for all profiles (domain, home, public)!

Problem: Mount of USB stick via command line.

Solution: Change into the directory /dev. Execute ls. There you will see the connected devices. Note the devices like sda, sda1… Connect your USB stick. Execute ls again into /dev. Now you should see more entries under sda. My stick got the entry sdc1.

Enter the following : mount /dev/sdc1 /mnt

Use this command on **FreeBSD OS** : mount_msdosfs /dev/da0s1 /mnt/usb

Execute ls –lisa

Now you should the folders of your stick. Change into the accordant directory : cd /mnt/name of the folder, which contains the installation data.

Extract the the rccmdinst.tar file : tar –xvf rccmdinst.tar

Execute the binary file : ./installRCCMD.bin

Problem: The RCCMD Software does not execute RCCMD shutdowns and you can determine the following error message into the file “rccmd.log” (default folder C\Program Files\RCCMD):

11/23/2011,12:56:55, RCCMD: ERR: WaitForOkay - Read failed with error <0>

Solution: Update your RCCMD Software!

Problem: You got the following error into the CS121/CS141 alarm log:
12/06/2011,16:30:56, RCCMD could not connect. (RccmdConn01) Reason: Host prohibited

Solution: The server denied an incoming TCP connection. Check your firewall configuration.

Problem: Enable firewall ports manually

Solution: You can check, if the required ports were opened, with the following command:

```
sudo iptables -L
```

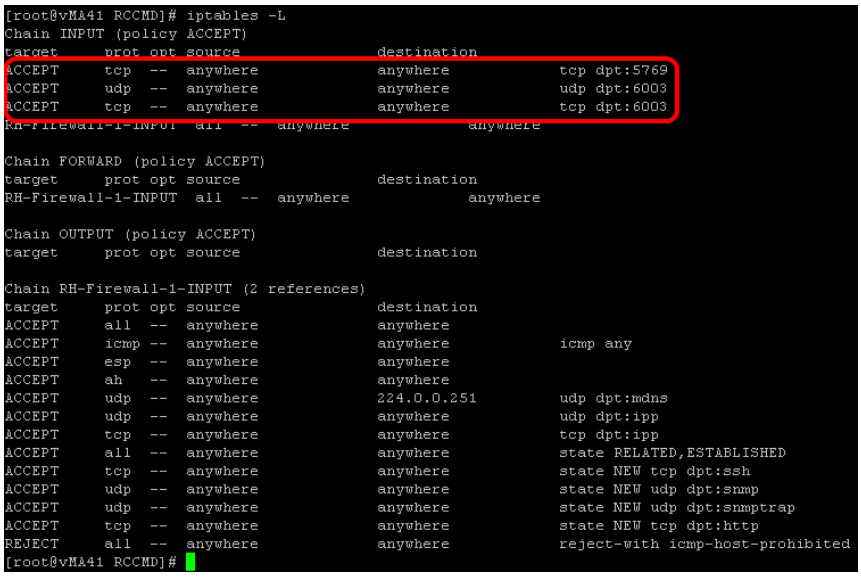


Fig. 185: Listing of the IP tables, see the “ACCEPT” at the TCP and UDP ports 6003, TCP port 5769

Sollte das Installscript die Ports nicht öffnen können, so ist dies auch manuell möglich:

Enable Firewall Port 6003 UDP/TCP manually

You can enable the firewall port 6003 UDP/TCP as follows :

```
/usr/sbin/esxcfg-firewall

esxcfg-firewall -o 6003,tcp,in,"RCCMD receive 6003"
esxcfg-firewall -o 6003,udp,in,"RCCMD receive udp 6003"
esxcfg-firewall -o 6003,tcp,out,"RCCMD transmit 6003"
esxcfg-firewall -o 6003,udp,out,"RCCMD transmit udp 6003"

oder

/usr/sbin/iptables oder /sbin/iptables

iptables -I INPUT -p tcp --dport 6003 -j ACCEPT
iptables -I OUTPUT -p tcp --sport 6003 -j ACCEPT
iptables -I INPUT -p udp --dport 6003 -j ACCEPT
iptables -I OUTPUT -p udp --sport 6003 -j ACCEPT
```

Save your settings as follows:

```
service iptable save
```

Problem: RCCMD error message on VMware ESXi server:

04/25/2012,14:40:24, rccmd[08066]: message received from 192.168.2.67

04/25/2012,14:40:24, rccmd[08066]: Trying to start program/job: /usr/rccmd/rccmd_shutdown.sh

04/25/2012,14:40:24, rccmd[08066]: error: /usr/rccmd/rccmd_shutdown.sh program/**job start failed**

The error message “job start failed” appears, if the user got no rights for the execution of the rccmd_shutdown.sh.

Solution 1: Arrange the “X” right on the rccmd_shutdown.sh as follows:

```
CHMOD +x rccmd_shutdown.sh
```

Solution 2: If the accordant rights are at present, the user did enter the wrong login data for the physical ESXi server. You can adjust these data into the file “esxi_creds” in the folder /usr/rccmd.

Problem: You get a message during the installation „Perhaps host is not a vCenter or ESX server“

Solution: Turn off the Lockdown Mode:
https://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=1008077

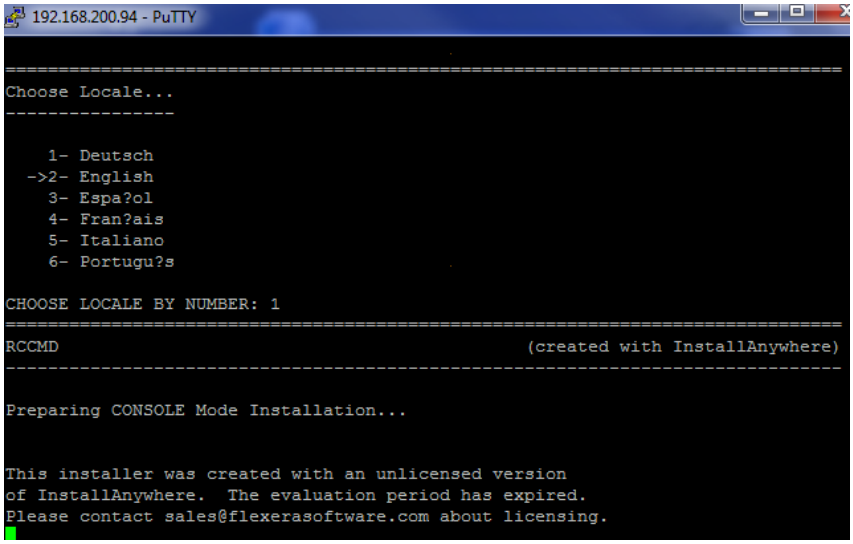


Fig. 186: Error Message „Unlicensed Version“

Problem: You get the following message after the start of the installation on a vMA on an ESXi server.

Solution: It is required, that the OS contains a TMP folder (/tmp) to execute a successful RCCMD installation.

Appendix

A OpenSSL

"This product includes software developed by the OpenSSL Project for use

in the OpenSSL Toolkit (http://www.openssl.org/).

B Syntax for the switching of the outputs

Set the RCCMD client at port 6002 to “on”, define the CS121/CS141 AUX ports as outputs and restart the CS121/CS141. Install the RCCMD Windows Wizard and open a DOS box. The following is a syntax example with the IP address 192.168.202.165:

```
C:\Program Files\RCCMD\

rccmd -se "EXECUTE |AUX|1|1" -a 192.168.202.165 -p 6002
```

ATTENTION! The blank after the “Execute” is important!

Common syntax for the switching of AUX ports:

```
|AUX|1|0  Port1, set to low
|AUX|1|1  Port1, set to high
|AUX|2|0  Port2, set to low
|AUX|2|1  Port2, set to high
|AUX|3|0  Port3, set to low
|AUX|3|1  Port3, set to high
|AUX|4|0  Port4, set to low
|AUX|4|1  Port4, set to high
```

Syntax for the switching of the outputs of the SiteManager:

```
C:\Program Files\RCCMD\rccmd -s -a 192.168.222.238 -p 6002 -se "EXECUTE
|UPSCMD|20000|1,1"
```

ATTENTION! The blank after the “Execute” is important!

```
|UPSCMD|20000|1,0  output 1 to low
|UPSCMD|20000|1,1  output 1 to high
|UPSCMD|20000|2,0  output 2 to low
|UPSCMD|20000|2,1  output 2 to high
|UPSCMD|20000|3,0  output 3 to low
|UPSCMD|20000|3,1  output 3 to high
|UPSCMD|20000|4,0  output 4 to low
|UPSCMD|20000|4,1  output 4 to high
|UPSCMD|20000|5,0  output 5 to low
|UPSCMD|20000|5,1  output 5 to high
|UPSCMD|20000|6,0  output 6 to low
|UPSCMD|20000|6,1  output 6 to high
|UPSCMD|20000|7,0  output 7 to low
|UPSCMD|20000|7,1  output 7 to high
|UPSCMD|20000|8,0  output 8 to low
|UPSCMD|20000|8,1  output 8 to high
```

C Know How Pool

SuSE 8.1 or older Linux versions

If you are using a SuSE 8.1 or an older Linux version, it is required to select the OS „XEN-Server“ during the interactive RCCMD installation!

D RARITAN Dominion PDU Configuration

In the following, we will describe, how a RARITAN PDU Type Dominion can be controlled through any RCCMD client or any CS121/CS141 or any other RCCMD compatible device :

1. Install a RCCMD client on a Windows OS and copy/create a file, like the following, into the RCCMD directory (default C:\Program Files\RCCMD) and use a SNMPwalk tool from an open source with the mandatory distribution txt-file « Copying.txt ». This file is included for legal reasons (Open Source).

```
@echo off
set PX_OID=1.3.6.1.4.1.13742.4.1.2.2.1.3.

if x%1==x goto paramerror
if x%2==x goto paramerror
if x%3==x goto paramerror
if x%4==x goto paramerror

snmpset -v 2c -c %2 %1 %PX_OID%%3 i %4
goto end

:paramerror
echo.
echo missing parameter!
echo.
echo Usage: pxout.bat ip community port value
echo ip:        address of the PX device
echo community: SNMP community string
echo port:      1-12
echo value:     0 or 1

:end
```

Fig. 187: „pxout.bat“

The command is called « pxout.bat » and expect 4 parameters :

- IP address or hostname of the Raritan device
- SNMP community string (the one for write access)
- Outlet number (1 to 12)
- 0 = off, 1 = on
-

2. The batch file “pxout.bat” accepts now several parameters from incoming RCCMD executes and translates these into SNMP set commands for the Raritan.

The “pxout.bat” accepts the following command syntax:

“pxout.bat <IP address> <community> <Outlet> <on/off>”

- **IP address**: This is the IP address of the Raritan
- **Community**: This is the community string for “write access”, configured at the Raritan or SNMP set commands, default is “public”.
- **Outlet**: This is the number of the Raritan Outlet 1 to 12, which you want to switch.
- **On/Off**: This is the signal you want to transmit, where “0” is off and “1” is on.
- Example: “pxout.bat 192.168.200.11 public 0” This example will switch the Raritan with the IP address 192.168.200.11, the outlet 4 to off!

If this works manually from your Windows RCCMD computer, than you can go ahead with step 3.

3. Now you have to select the desired CS121/CS141 event and add a RCCMD command, which will be send to the Windows computer, where RCCMD is running and the “pxout.bat” file is located.

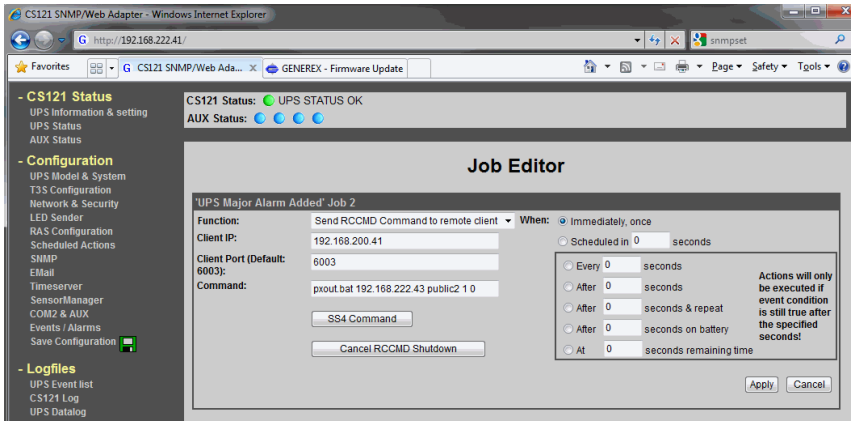


Fig. 188: CS121/CS141 Configuration for such a relay command

The target of the RCCMD command is the Windows computer with RCCMD and the „pxout.bat“ with the IP address 192.168.200.41. If the event „UPS Major Alarm Added“ will occur, this Job will execute the command „pxout.bat 192.168.222.43 public2 1 0“ to switch off the socket number 1 at the Raritan with the IP address 192.168.222.43 immediately.

Tip: You should stop RCCMD running in the background on this Windows computer, so you will better see, whats going on. Stop the RCCMD service, than open a command line into the RCCMD folder and start „rccmd.exe –debug“. Now the software will run in the foreground and you can watch the communication.

4. The Raritan with firmware 1.4.1 is unfortunetaley buggy. Here the workaround:

The default community strings for the Raritan are identically set for „read“ and „write“ to „public“, but this configuration is invalid! It must be different!

Solution: Stop the SNMP Agent at the Raritan, change the community for „write“ to any other than „public“ and restart it!

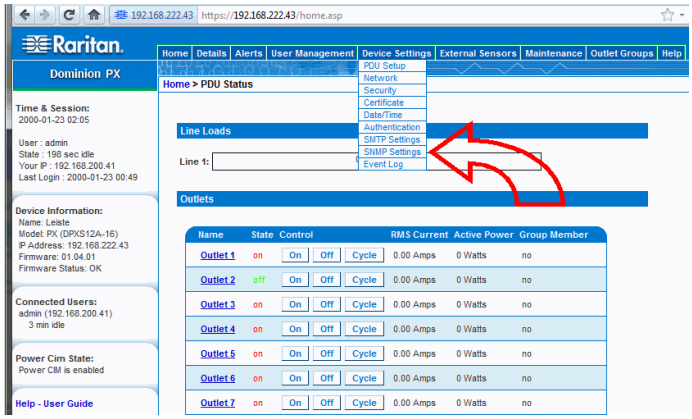


Fig. 189: Raritan Device Settings

The default Raritan user is „admin“, password is „nimda“.

Attention! This does not work with MS Internet Explorer! Use any other web-browser, e. g. Mozilla Firefox.

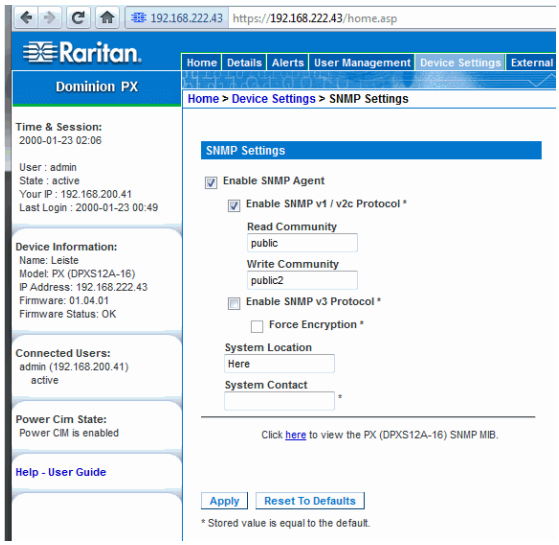


Fig. 190: Raritan SNMP Settings

Click on „Stop“, change the configuration on „Write Community“, e. g. to „public2“ and restart.

E Figures