RCCMD – Multiple Server Shutdown Software

Manual

Content:

7. RCCMD Screens explained in Detail

This chapter explains in detail all screens and how to use them in order to configure RCCMD. Please note that any script examples are generally carried out for standard installations on windows-based operating systems and may have to be adapted to fit to your operating system and configuration.

7.1: Windows / Linux /MAC - The RCCMD client configuration interface in detail

This chapter will explain all regular client configuration screens as seen when using any Linux, Windows (Desktop, Server, Hyper-V, Core, etc.), MAC/OS or Unix-based version.

7.2: The RCCMD Appliance for VMware configuration interface in detail

All Appliance menus explained in detail as seen in any VMware environment. Note, at "Advanced Options" is a special feature called "Change RCCMD target". With this feature, it is possible to switch as needed between VMWARE Mode and Client Mode.

7.3 Appendix

Among other things, this chapter is dedicated to special functions of RCCMD that do not find a place in the standard application and deserve or need some explanation.

8. License agreement, Disclaimer, Copyrights and other stuff

This chapter shows important information no one reads normally …

General functions of the RCCMD Client
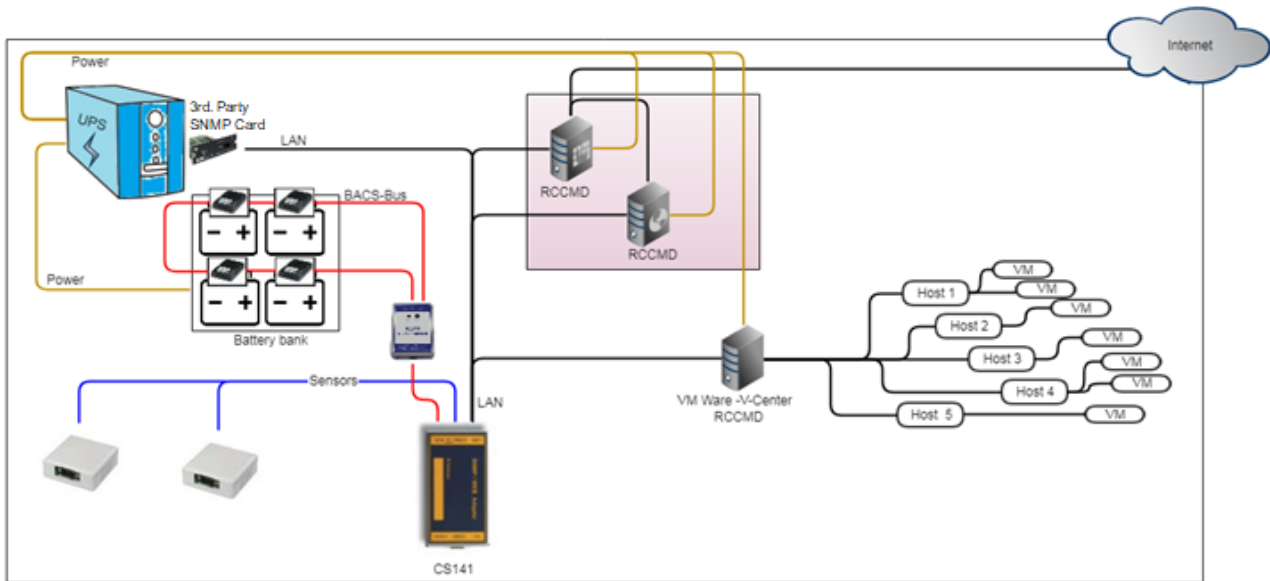
RCCMD is designed to individually shut down your systems in an emergency. In this case, a shutdown command is sent to the clients by an RCCMD server - usually a UPSMan or CS141 - and implemented accordingly by the client.

The following ports must be open on your network:

Port 8080	The local RCCMD web interface is accessed via this port
Port 8443	The RCCMD web interface is called up via https
Port 6003	The RCCMD communication port for managing control signals

The RCCMD client requires a fixed IP address

This IP address must be communicated to the RCCMD server so that a clear command can be sent. If the IP address changes dynamically or if there is no DHCP server in emergency situations, RCCMD can also be addressed directly in this way.

Generally supported operating systems

We provide UPSMAN installers for multiple platforms.

📄 Supported Operating Systems

♀ Acknowledgements

With few exceptions, RCCMD supports almost every operating system available on the market based on Unix / Linux, Windows and numerous versions of MAC/OS and is available as a special version for AS400. A precise list of all supported operating systems can be found in the download area when selecting the respective installer. If your operating system or derivative is not listed, please contact our technical support at support@generex.de - Our technical support will be happy to answer all your questions.

Minimum system requirements for the VMware RCCMD Appliance

VMware 6.5 - 8.X – based systems

The appliance, which is officially available for download, requires *VMware version 6.7 or higher*. Older versions are not supported by the official download. A download link is free of charge available at www.generex.de.

On request available: Legacy versions of the appliance for older VMware systems available

For VMware 6.x users…

There is a special legacy version of the appliance for these systems, which is specially tailored to the needs of operation from VMware 6.5. The appliance also supports the VMware vSAN function introduced with 6.7. Installation and configuration can be carried out as described below (there may be slight deviations in the menu control compared with the latest RCCMD).

VMware 5.x / 6.0 and older…

These older systems use VMware's Virtual Media Assistant, which is exclusively available in the VMware download area. After rolling out the VMA, a special RCCMD version for VMware can be uploaded and installed via ftp.

If there is need to use an older version of RCCMD, just refer to our technical support at support@generex.de.

RCCMD – for VMware 6.5 - 8.X

Some typical installation Problems:

During testing, everything worked very well, but now …

Check the license of your ESXi host. If you have used an evaluation key for the ESXi host when setting it up, you may have configured some commercial functions. If you then imported the free key, strange error messages suddenly appear or the host no longer shuts down.

Also check whether you have entered the correct key in the RCCMD. Basically, the RCCMD appliance is equipped with an evaluation key that can be changed at any time via the web interface. When the evaluation period has expired, RCCMD will stop the service. If you enter an incorrect or invalid key, the evaluation phase is automatically activated.

Sometimes one RCCMD runs, then the other, …

This always happens if you have accidentally entered RCCMD keys several times. In this case, when the network starts, the first RCCMD that starts with an affected key will claim it for itself. Subsequent RCCMD clients, however, will stop again with a corresponding log entry "License fraud <IP address>.

Typical network problems, e.g., …

vLAN is in use:
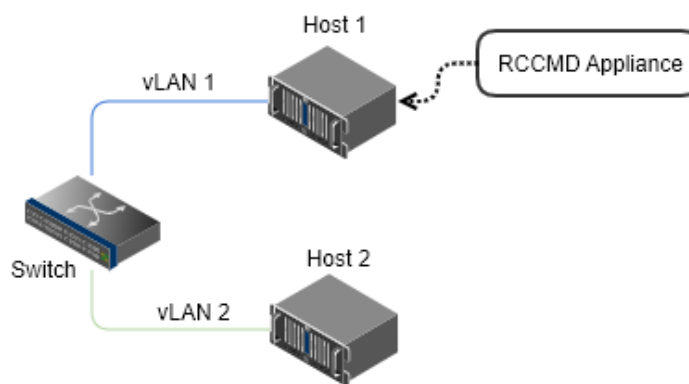
Even if both hosts are on the same switch, because the ports are separated via vLAN, they must be seen as two separate networks.

Port separation and/or missing routing:
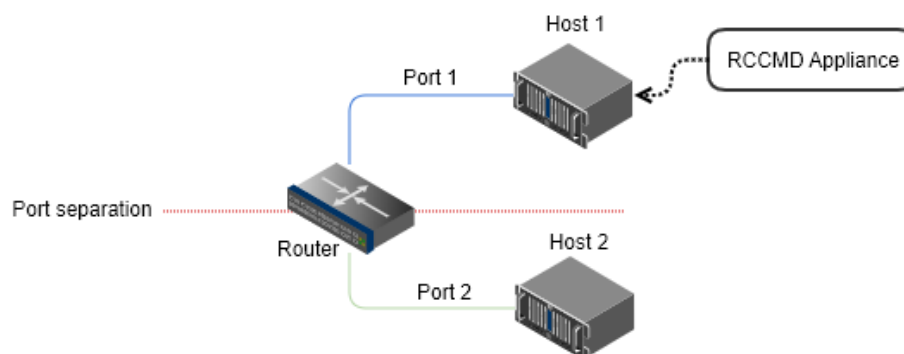
This configuration is quite common when servers are in different network segments and e.g., an uplink line to a neutral third network segment with internet connection exists. The router requires special routing entries in order to be able to mediate between the networks. Among other things, you can also set here that the RCCMD appliance can only reach the hosts.

Firewall settings and intrusion detection
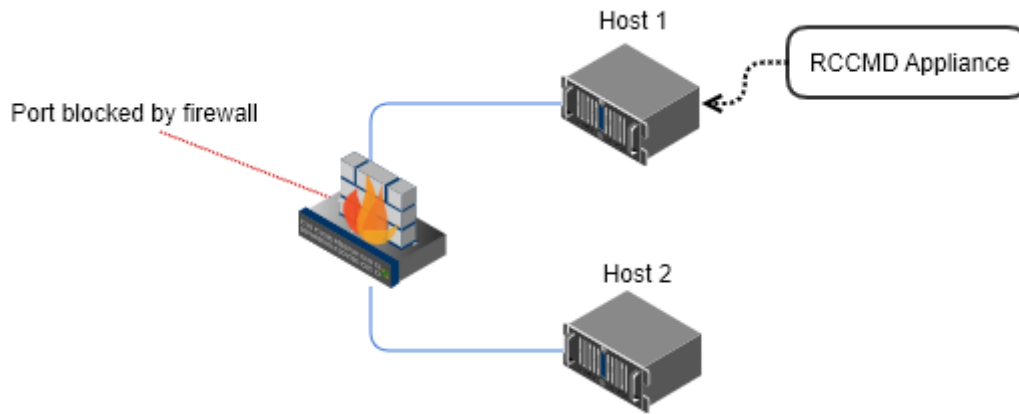
A firewall or intelligent intrusion detection thinks that RCCMD has no internal port release and rejects communication. As a consequence, RCCMD cannot reach host 2. Very large networks also use a multi-level or modular firewall concept. Check whether the firewall settings have to be adjusted. Smaller systems, on the other hand, can get these problems if e.g., a local firewall and an additional Internet security software package is in use simultaneously.

Deploying the RCCMD Appliance:

Open your VMware ESXi – Host and login as root:

After successfully logging in create a new VM - For ESXi 6.5 you will find the corresponding tab in the upper bar:

Then select the following option:

Deploy a virtual machine from an OVF or OVA file:

Click next to proceed to the next configuration dialogue:

Give your new RCCMD machine a unique name:

Enter a name for the virtual machine.

RCCMD Easy Install ✕

Virtual machine names can contain up to 80 characters and they must be unique within each ESXi instance.

Place the OVA file into the necessary ESXi host window using drag and drop ...

✕ 🖥 RCCMD-Appliance33.ova
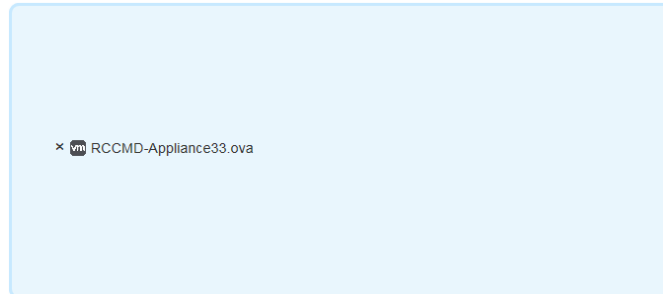
… and click Next:

| Back | Next | Finish | Cancel |

The OVA file is preconfigured, there is no need to do any additional settings:

The following datastores are accessible from the destination resource that you selected. Select the destination datastore for the virtual machine configuration files and all of the virtual disks.

Name	Capacity	Free	Type	Thin pro...	Access
datastore1	458.25 GB	402.17 GB	VMFS5	Supported	Single

1 items

Due to this fact, just click on next:

| Back | Next | Finish | Cancel |

The RCCMD client will be managed by an according RCCMD server device. Therefore, this server device must be able to reach your RCCMD client over local network structures.
In general, you can accept the preconfigured settings.

Network mappings	bridged	VM Network ▼
Disk provisioning	⦿ Thin ○ Thick	

The same works for provisioning of the hard disk space. The RCCMD OVF file is preconfigured for best use unless your hardware platform differs from standard installation routines.

Once you have made the settings as you like, click *Next* to go to the next step:

| Back | Next | Finish | Cancel |

This is the final step:
Please review all settings before clicking Finish:

Product	RCCMD-Appliance
VM Name	RCCMD Easy Install
Disks	RCCMD-Appliance33-disk1.vmdk
Datastore	datastore1
Provisioning type	Thin
Network mappings	bridged: VM Network
Guest OS Name	Unknown

Obey the special notification carefully to prevent damaging RCCMD during installation routine is running.

⚠ Do not refresh your browser while this VM is being deployed.
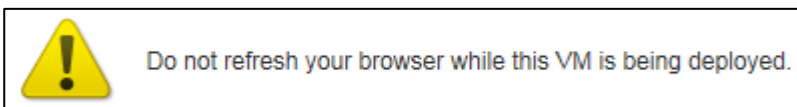
VMWare responds sensitive to browser updates during installation process. If the browser will be refreshed before installation is finished, the process will be aborted, rendering the virtual machine unusable.

Click finish to start the installation process:

Back   Next   Finish   Cancel

The automatic installation

Results and completed shows the current installation state and proper success.

Task	Target	Initiator	Queued	Started	Result	Completed ▼
Destroy	RCCMD_Easy_Install	root	05/15/2018 13:32:17	05/15/2018 13:32:17	✓ Completed successfully	05/15/2018 13:32:17
Shutdown Guest	RCCMD_Easy_Install	root	05/15/2018 13:31:53	05/15/2018 13:31:53	✓ Completed successfully	05/15/2018 13:31:53
Upload disk - RCCMD-Appliance33-dis...	RCCMD Easy Install	root	05/15/2018 12:37:10	05/15/2018 12:37:10	Running... 61 %	
Import VApp	Resources	root	05/15/2018 13:43:10	05/15/2018 13:43:10	Running... 56 %	

Obey the Daleks:
The administrator will wait for the installation to complete before updating this browser window.

Note:

[browser tab bar: Zertifikatfehler | localhost.generex.local – VMw... | localhost.generex.local – V... ✕]

Use tabbed browsing to keep working. VMware will automatically detect the current session. By doing so, administrators will be allowed to continue working on the system while waiting for a finished RCCMD installation.

The Installation progresses

On the left side you want to find a tool called navigator. The navigator displays an overview of all virtual machines installed on the system.
This installation example is called

Navigator

▼ 🗔 Host
   Manage
   Monitor
▸ 🖳 Virtual Machines   13
▸ 🖴 Storage   1
▸ 🌐 Networking   2

9
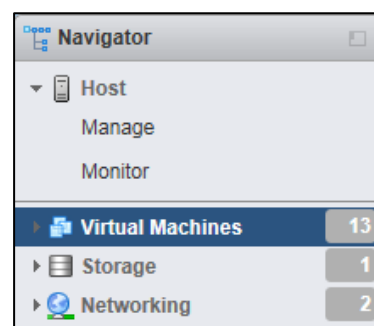
Search for virtual machine including the RCCMD appliance.
Clicking on it will open advanced system information about the virtual machine.

Ensure the virtual machine is running. Take a look at the list of all virtual machines and search for the RCCMD Appliance

 The virtual machine is running

 The virtual machine is off
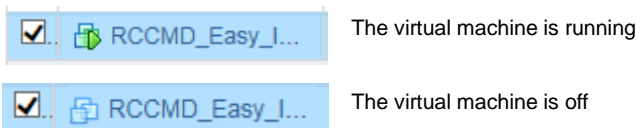
Click on the virtual machine you have installed for more detailed information.
By pressing the console screenshot, the web console for the virtual machine will be opened:
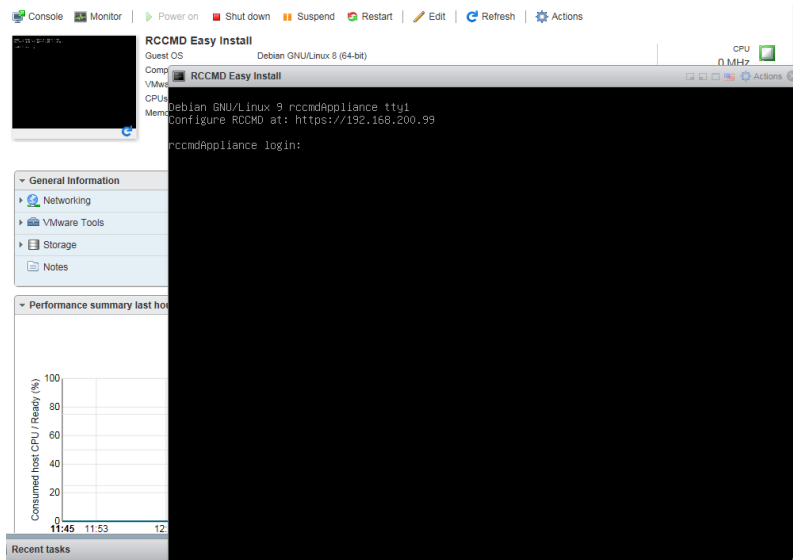
As a default, the appliance will ask for a valid IP address. If your network provides a DHCP server,
RCCMD will automatically display the current IP address.

If there is no valid IP address by DHCP, it is necessary to manually assign an IP address. in the appendix, you will find information
about the procedure

10

Post installation console login

You can log on to the RCCMD appliance directly from the web console:

User: admin

Password: RCCMD

Gaining root privileges

The VMware Appliance is based on a Linux Debian 9 - The root privileges allow the manual re-installation of official packages as well as advanced configuration of the network interfaces.

```
admin@rccmdAppliance:~$ sudo su
[sudo] password for admin:
root@rccmdAppliance:/home/admin#
```

command: sudo su

by default settings, admin has not been granted system privileges to make changes - you need to assign increased system privileges by using the Linux command sudo su.

The installation of the RCCMD appliance is now complete. For further configuration, refer the web interface. A configuration guide for assigning an IP address manually can be found in the appendix to this manual.

Installing RCCMD with a vCenter

At VCenter context menu, start the RCCMD installation routine by choosing *Deploy OVF Template ...:*
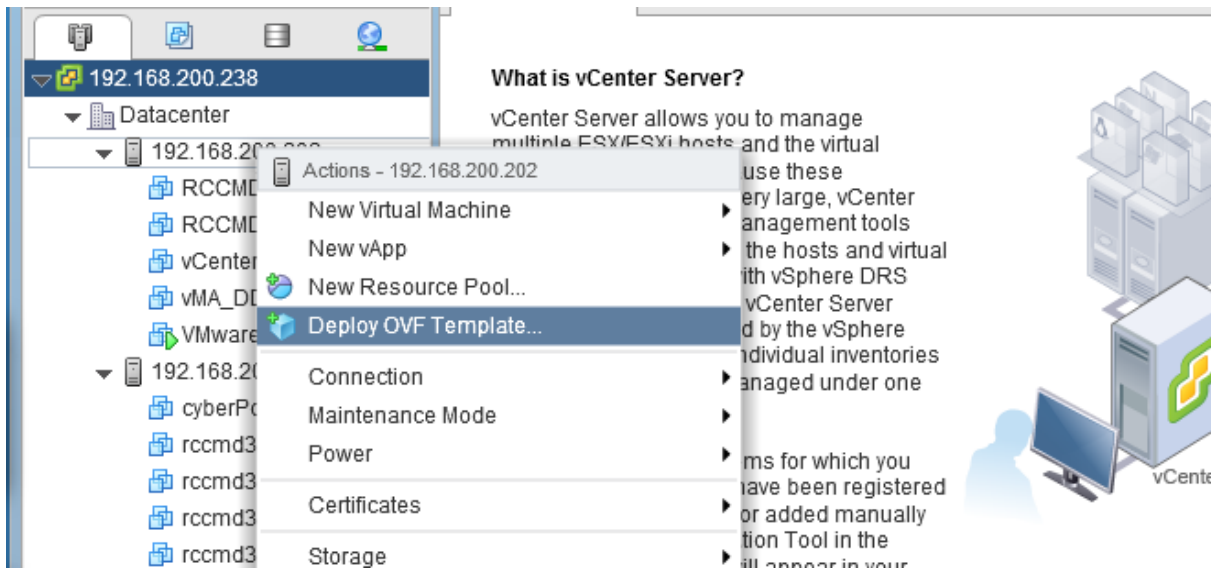
First, select the necessary file. vCenter provides two options:

URL:

If the OVF file is provided by web resources, specify the appropriate path.

Local File

If you have saved the OVF file as a local file, select the file directly.
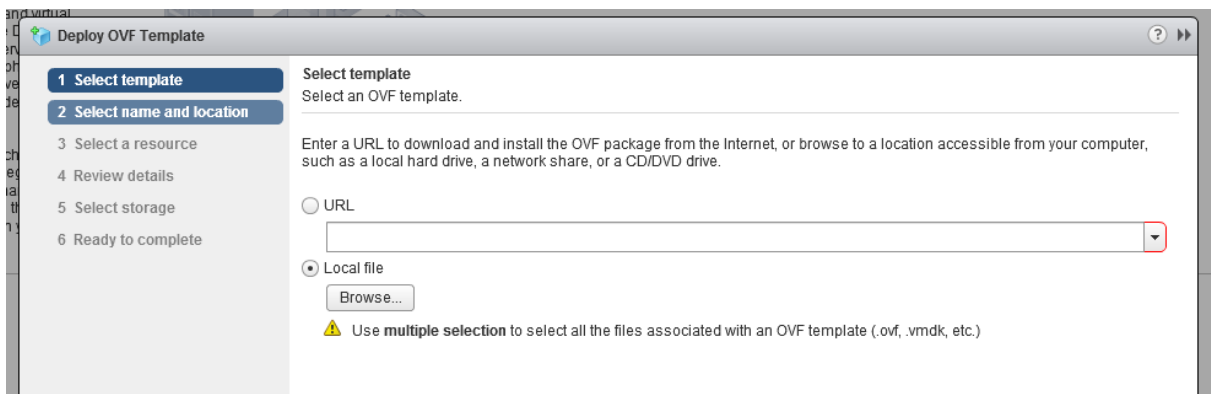
In this example installation, the local file will be used to install the RCCMD Appliance:

After selecting the local file, press Next to proceed to the next installation step:
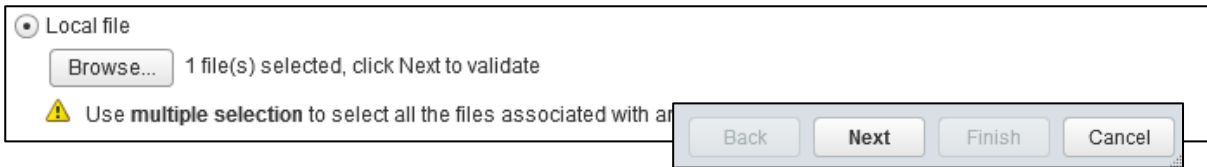
The next step asks you to name the virtual machine VM a uniquely. This name is needed in the later configuration steps of RCCMD. Click Next to proceed to next configuration step.
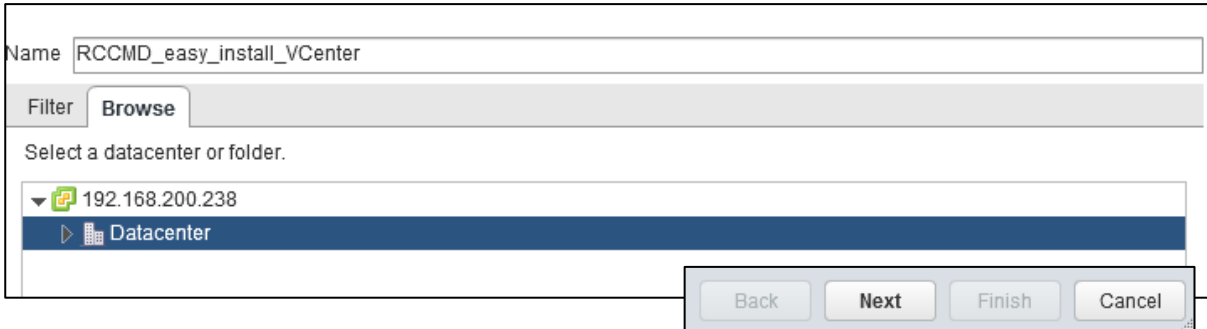
vCenter needs to know the destination host to set up and install the virtual machine
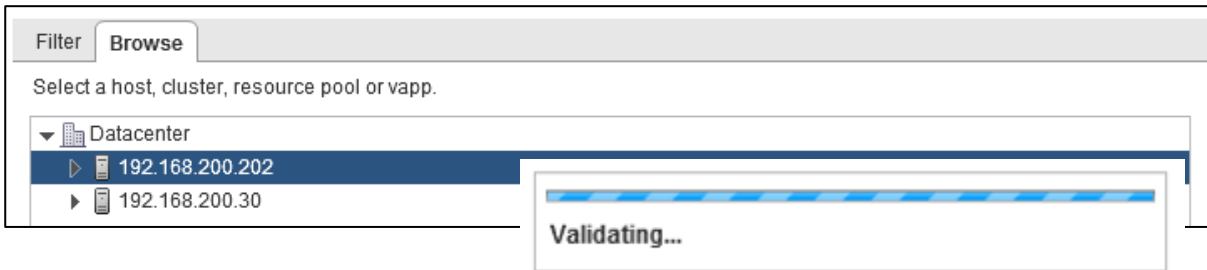
vCenter will provide a general overview of the settings according to the virtual machine. Press Next to continue.
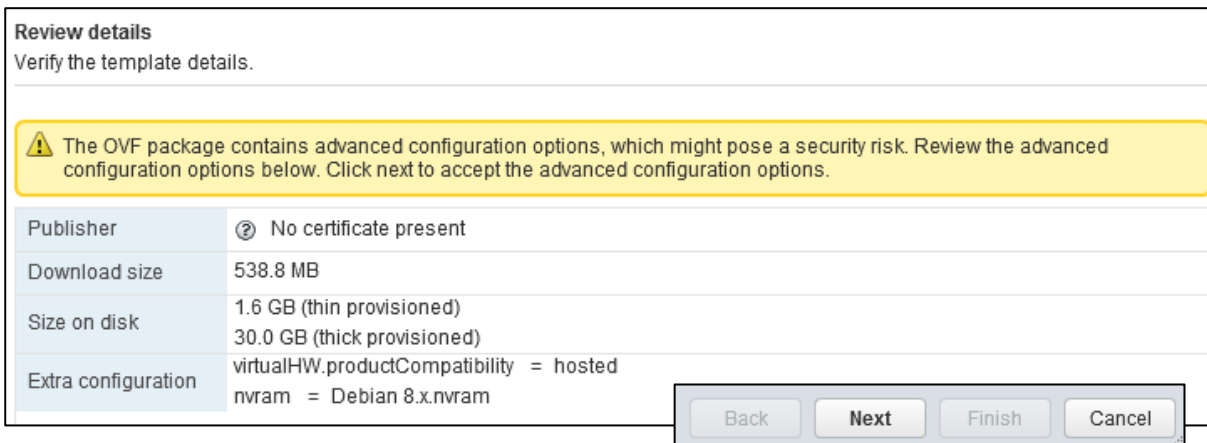
Please note that there is no way but confirming the copyright terms...

Please press Accept before proceeding the installation - the Next button will not work unless this has been happened.

12
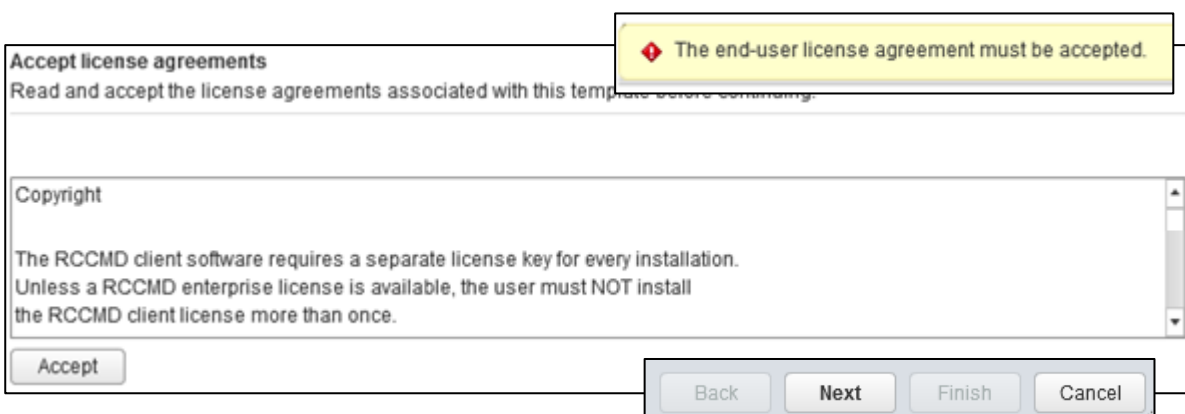
Disk usage may vary depending on the configuration of your system:
Please refer to local system administrators to get the correct setting. If you are unsure, select Thin provision and as VM storage policy none.
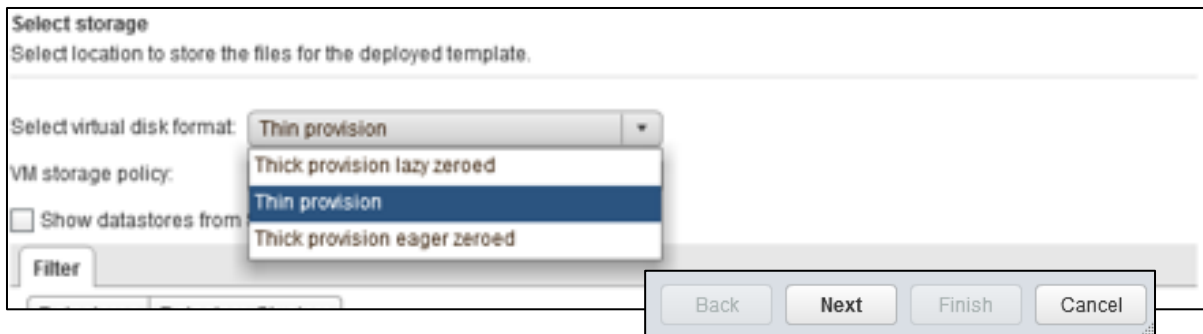
The appliance needs access to the network. Again, please refer your local system administrator...If you are unsure, first select VM Network in bridged mode. In this installation example, we use VM Network to correctly connect the VM to the network.
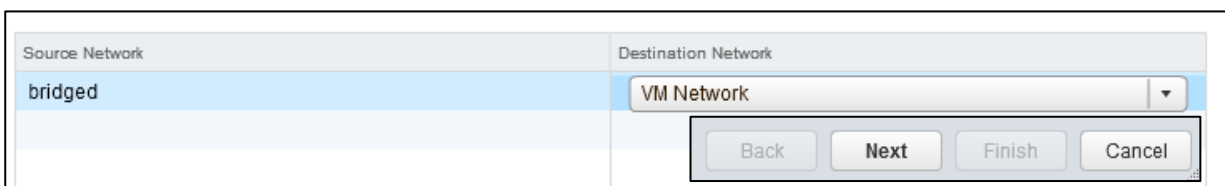
Take some time to review your settings: you will be shown an overview of your configuration. If the settings are to your liking, proceed by clicking *Finish*. This button will quit the configuration dialog and triggers the RCCMD appliance automatic installation routine.
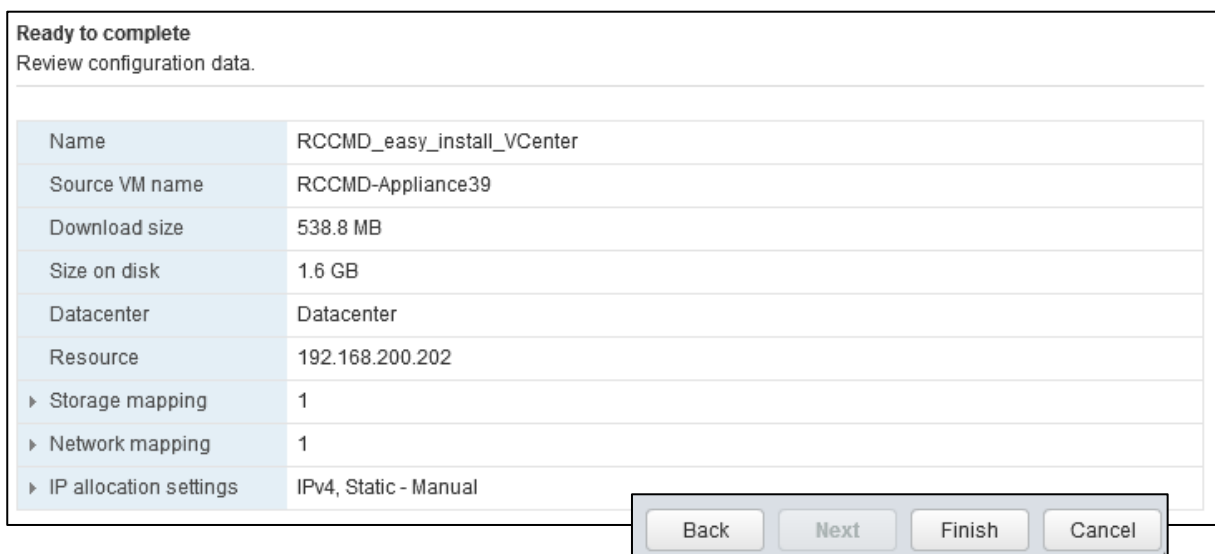
How to observe the installation progress

Under Recent Tasks, you can track the current installation progress:
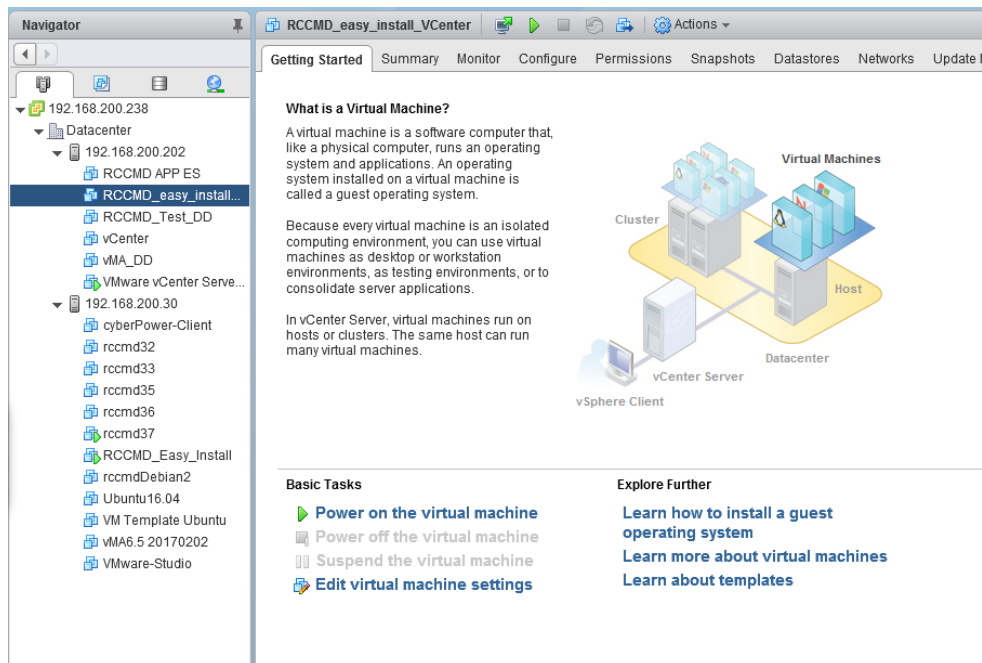
Task Name	Target	Status		Initiator	Queued For	Start Time	1 ▼	Completion Time	Server
Deploy OVF template	RCCMD_easy_inst...	10 %	⊗	VCENTER6.7.GENE...	3 ms	5/31/2018 10:22:19 ...			192.168.200.238
Import OVF package	192.168.200.202	10 %	⊗	Administrator	140 ms	5/31/2018 10:12:11 ...			192.168.200.238

Please wait until the complete installation process is done and the status is set to *Completed*:

Target	Status
RCCMD_easy_inst...	✔ Completed
192.168.200.202	✔ Completed

Starting the VM and console access using vCenter

At navigator, search for the corresponding virtual machine and power it up.

Console login after installation

After the VM boots successfully, you can access the console directly from the vCenter console menu:

14

As a default, the appliance will ask for a valid IP address. If your network provides a DHCP server, RCCMD will automatically display the current IP address.


```
Debian GNU/Linux 9 rccmdAppliance tty1
Configure RCCMD at: https://192.168.200.203
```

If there is no valid IP address by DHCP, it is necessary to manually assign an IP address. in the appendix, you will find information about the procedure

Post installation console login

You can log on to the RCCMD appliance directly from the web console:

User: admin

Password: RCCMD

Gaining root privileges

The VMware Appliance is based on a Linux Debian 9 - The root privileges allow the manual re-installation of official packages as well as advanced configuration of the network interfaces.


```
admin@rccmdAppliance:~$ sudo su
[sudo] password for admin:
root@rccmdAppliance:/home/admin#
```

command: sudo su

by default settings, admin has not been granted system privileges to make changes - you need to assign increased system privileges by using the Linux command sudo su.

The installation of the RCCMD appliance is now complete. For further configuration, refer the web interface. A configuration guide for assigning an IP address manually can be found in the appendix to this manual.

RCCMD quick configuration guide

This chapter explains the essential settings that are required for the operation of RCCMD if you operate one or more hosts.
A prerequisite for this configuration section is that the appliance has been successfully deployed.

Web Login: RCCMD

To access configuration screen of RCCMD, open a web browser and proceed to the IP address of you RCCMD installation:

https://<IP address of the RCCMD appliance >

Use the default credentials to log in:

User: admin
Password: RCCMD

Before starting any configuration, RCCMD displays the current terms of use. Accepting them is required for using RCCMD software.

End User License Agreement

Accept

15

You may read the end user conditions and then click on the Accept button. The configuration dialog will proceed after accepting the end user license agreement

Next, RCCMD will prompt you to enter a valid license key:

Please note that the key used by RCCMD installation will work with these conditions:

1. One Key – one RCCMD installation

You can use any number of RCCMD clients in your system. In general, the prerequisite is that only one unique key will be used for one RCCMD client. If a key will be accidently assigned twice, the RCCMD client that launches first will claim the license. The following RCCMD clients starting up will recognize a claimed license and will show an according log entry:

2018-05-30 09:17:51 rccmd [00490]: Licence fraud from IP address 192.168.200.144 detected. Functionality will deteriorate.

In case of using a key valid for a certain number of installations, only the according number of RCCMD installations will be activated with this appropriate key.

Please note, the demonstration key itself is a unique basic key that will be used for any installation:
You cannot use more than one RCCMD trial versions in one network.

2. If there is no valid key present, RCCMD will run in trial version mode

If you do not have the key or want to test the product, do not enter a key.
By doing so, RCCMD will assume that you will use an initially a full-featured trial installation and uses a build-in 30-day evaluation key.
RCCMD provides a configuration dialog for changing the key at any time.
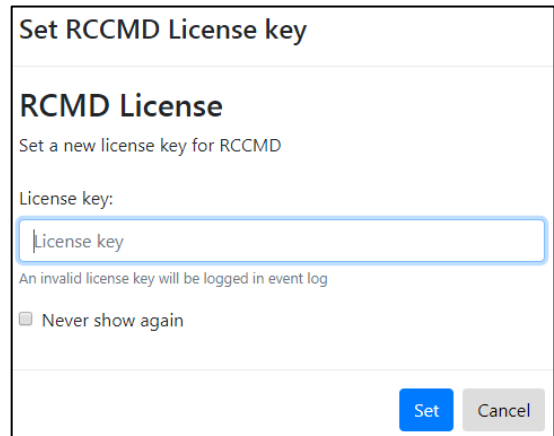
Note
RCCMD offers you within theWeb console on a dialogue to change the key:

Open Advanced Settings and click Update License Key
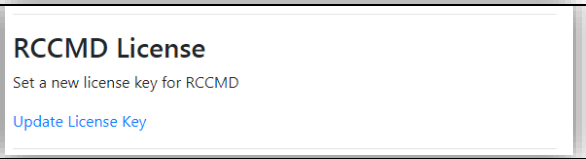
Note: Please restart after essential configuration work

During the configuration of RCCMD a custom restart of the service is necessary:

Whenever a change has been made to the configuration, it is required to restart the RCCMD service. Otherwise, the data is saved but not transferred to the active configuration.

If you activate Do not ask again, RCCMD will not inform you about the fact a restart is required.
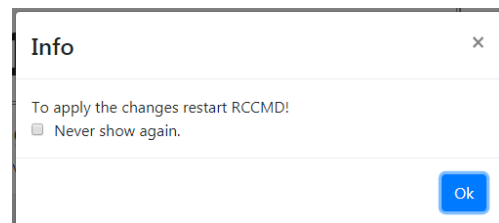
Securing the RCCMD appliance

Menu: Open Options click on Connections

Protection against accidental server shutdown

Currently, each RCCMD transmitter can trigger a shutdown that cannot be taken back. The RCCMD client therefore offers you to limit these commands to specific stations.

Under Options, click on *Connections* to open the corresponding dialog. With *Insert* you can add a new IP address:

Enter the IP address expressly entitled to RCCMD shutdown command.

Note: An empty list means that every sender can connect to this listener.

Sender IP Address

Insert

Remove

RCCMD - Insert | Edit Sender   ×

Enter the Name or IP-address of the incoming RCCMD Sender below.

IPv6 is not supported.

Incoming RCCMD Sender:

Close   Save changes

Activating RCCMD encryption

If your network requires to use an SSL encryption, RCCMD can be advised use SSL encryption.

Protocol

The setting below increases the security of connections to this RCCMD

☐ Accept only SSL connections (requires restarting RCCMD)

☐ Reject expired SSL certificates

To force SSL encryption, enable Accept only SSL connections. In case of up-to-date certificates only, RCCMD can be forced to reject outdated certificates.

With Save Changes, the IP address settings will be insert into the corresponding configuration script.

Cancel   **Save Changes**

Checking current RCCMD system state

Menu: Status

Click System Status and press Restart.

The Current status of RCCMD is used to detect the now active operating state.

The following status messages indicates the current RCCMD operating state:

not running   RCCMD is offline

running   RCCMD is online

System Status

Current status of RCCMD is: running

▶ Start   ■ Stop   ↻ Restart
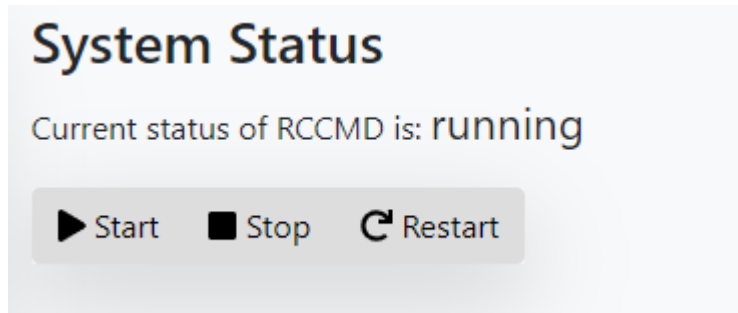
RCCMD running status at the login screen

RCCMD

System Status : running

Version: 4.19.12 190604

English ▾

System Login:

Username: admin

Password:

Login

Passing the shutdown control to RCCMD when using a single host

Menu: VMware Settings

Go to VMware Settings:
If you have not yet made any settings, RCCMD will inform you that RCCMD needs additional information:

ESXi Configuration required   ✕

If you configure RCCMD to let the ESXi Host manage the handling of the virtual machines, then it is necessary to configure the virtual machine shutdown for the ESXi Host within vSphere Client.

Ok
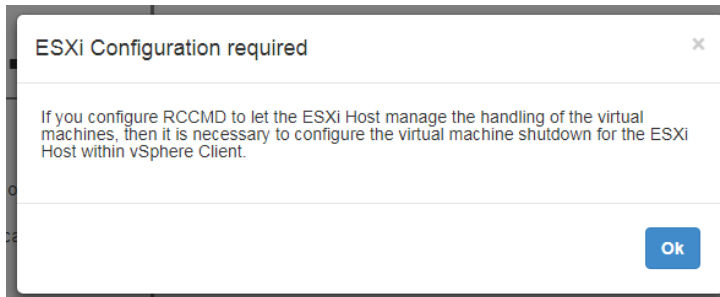
Although RCCMD is installed as a virtual machine and is already ready for use, it cannot yet fulfil its actual function since the necessary access authorizations have not yet been stored. Confirm this message with OK to open the VMware settings:

When using a single host is, virtual machines

Virtual Machine Management: by RCCMD ▾   Info...

Virtual Machine behaviour: Shutdown Virtual Machi ▾   Info...
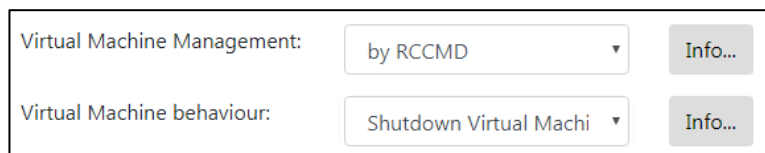
can be powered off before the ESXi host itself shuts down.

> **Note**
>
> The regular shutdown routine requires the virtual machines to be shut down and the host itself to be shut down. In this case, the shutdown duration merely defines the time window that the virtual machines have to shut down immediately after the RCCMD shutdown signal is received. The Maintenance Mode timeout defines the time window that RCCMD grants vMotion before the regular shutdown routine of the hosts takes effect. The maintenance mode in the shutdown behaviour can therefore also be used to trigger a shut down for different hosts including a time delay.

For Virtual Machine Management, select *by RCCMD*. As Virtual Machine Behaviour *Shutdown Virtual Machines*.

To prevent RCCMD from shutting itself down, the VMware host must know what the machine running the RCCMD Client itself is:

☐ 🔳 RCCMD_TEST_GUNNAR	✅ Normal	1,84 GB
☐ 🔳 RCCMD_Easy_Install	✅ Normal	3,95 GB

… RCCMD at the ESXi …

The virtual machine that runs RCCMD must not be shutdown. Or else RCCMD cannot shutdown the other virtual machines and hosts. Enter the virtual machine's name on which RCCMD runs.

VM running RCCMD   RCCMD_Easy_Install

… the current RCCMD client

RCCMD requires the following information:

HOST / IP name
Normally, we recommend using the IP address of the ESXi Host here. You can, however, also enter the host name itself.

User
A user with the appropriate system privileges to shut down the VMware environment accordingly.

Note: It is recommended to use the user "root" or a user with explicit root rights to grant the shutdown of virtual machines.

Password
The password assigned to the user that allows RCCMD to authenticate itself as authorized.

Add ESXi Host credentials ✕

Enter the information for this ESXi Host below. (If vMotion shall be used, the Host name must be identical to the name in the vCenter.)
Do not put credentials for vCenter here!

Host name or IP: 192.168.200.30

User name: RCCMD

Password: ••••••••

Time granted for virtual machines to shutdown before Host gets shutdown in seconds:
Seconds

Check Values   ⟳ checking ESXi Host credentials...

Abort   **Save Changes**

The next step will determine how much time RCCMD should allow the virtual machines to quit before the ESXi host powers down:

Shutdown delay: Seconds

Time virtual machines are granted to shut down. Default: 90

Virtual machines take different amounts of time to shut down and shut down properly. The exact time, how long a machine needs, is very individual and depends strongly on the task and the promised hardware. To prevent data loss or damage to the virtual machine, the host can be instructed to give the machines a proper time window to shut themselves down before shutting down itself.

Shutdown delay indicates the time in seconds that the host waits before being turned off.

The Default setting is 90 seconds - virtual machines taking more will be turned off due to the fact the ESXi host powers down.

You can check the access data with Check Values:

If the test was successful, press Save Changes to exit the configuration dialog.

Click on Verify to confirm the entered ESXi data as verified server.

You will notice that at the bottom right the Save Changes has changed colour:

You will notice that at the bottom right the Save Changes has changed colour:

You have made a change that requires RCCMD to be restarted to permanently save the inputs and apply them to the active configuration. This process is indicated by the green button.

Handing over the shutdown control to RCCMD using a vCenter
Menu: VMware Settings

The vCenter differs with its operating modes from a standalone host. While the Standalone Host works on its own and shuts down virtual machines as needed, vCenter provides the so-called vMotion: The HA - High Availability - of vMotion allows virtual machines to be moved from one host to another before the host is intentionally powered down.

Please note:

Before you can use the RCCMD appliance with vMotion, the Distributed Resources Scheduler DRS must be configured to use the fully automatic mode.

Note
Before using RCCMD in conjunction with vMotion, ensure to verify that each virtual machine running on the host has been tested working with the maintenance mode. If maintenance mode fails, non-migrated virtual machines will be switched off when the host is powering down.

Open VMware Settings:

If you have not yet made any settings, RCCMD will inform you that RCCMD needs additional information:

Although RCCMD is installed as a virtual machine and is already ready for use, it cannot yet fulfil its actual function since the necessary access authorizations have not yet been stored. Confirm this message with OK to open the VMware settings:
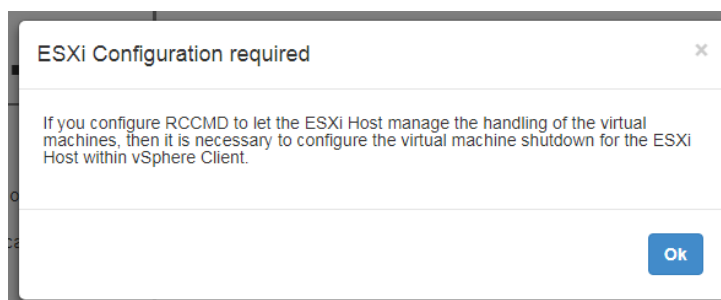
While using a vCenter, virtual machines can migrate to another host before the original host powers down. The virtual machines them self will continue working seamlessly. Please note the different access data:

Under Virtual Machine Behaviour, select Maintenance Mode (vMotion).
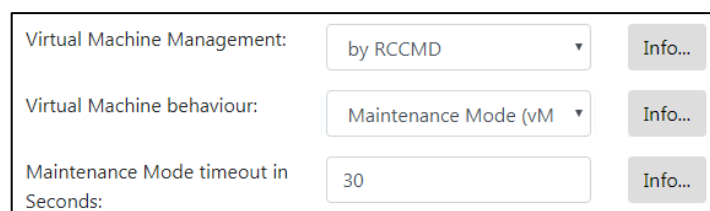
The Maintenance Mode time out in Seconds defines the time vCenter is given to move a virtual machine to another host. The behaviour of vMotion is configured within the high availability (HA) within the vCenter. As soon as time is up, the standard shutdown procedure will be initiated:

remaining virtual machines will shut down due to the fact the host powers down.

Unlike the standalone host, RCCMD requires user data with the corresponding authorizations of the vCenter:

Use Check Values validate the credentials of the vCenter - Check values will display whether the vCenter is reached and the access data has been entered correctly:

If RCCMD cannot reach the vCenter correctly, it will show a corresponding error message.

To prevent RCCMD from shutting itself down, the VMware host must know what the machine running the RCCMD Client itself is:

… RCCMD at the ESXi …

The virtual machine that runs RCCMD must not be shutdown. Or else RCCMD cannot shutdown the other virtual machines and hosts. Enter the virtual machine's name on which RCCMD runs.

VM running RCCMD RCCMD_Easy_Install

… the current RCCMD client

RCCMD requires the following information:

HOST / IP name
Normally, we recommend using the IP address of the RCCMD host here. You can, however, also enter the host name itself.

User
A user with the appropriate system privileges to shut down the VMware environment accordingly.

Password
The password assigned to the user that allows RCCMD to authenticate itself as authorized.

The next step will determine how much time RCCMD should allow the virtual machines to quit before the ESXi host powers down:
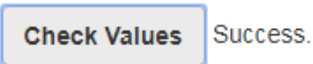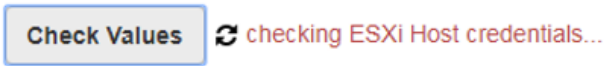

21

Virtual machines take different amounts of time to shut down and shut down properly.

The exact time, how long a machine needs, is very individual and depends strongly on the task and the promised hardware. To prevent data loss or damage to the virtual machine, the host can be instructed to give the machines a proper time window to shut themselves down before shutting down itself.

Shutdown delay indicates the time in seconds that the host waits before being turned off.

The Default setting is 90 seconds - virtual machines taking more will be turned off due to the fact the ESXi host powers down.

You can check the access data with Check Values:

| Check Values | ⟳ checking ESXi Host credentials... |
| Check Values | Success. |

If the test was successful, press Save Changes to exit the configuration dialog.

Click on Verify to confirm the entered ESXi data as verified server.

| Add... | Remove | Edit... | **Verify** |

You will notice that at the bottom right the Save Changes has changed colour:

| Cancel | **Save Changes** |

You will notice that at the bottom right the Save Changes has changed colour:

You have made a change that requires RCCMD to be restarted to permanently save the inputs and apply them to the active configuration. This process is indicated by the green button.

Advanced Shutdown: Cluster Shutdown with dependencies

Menu 1: VMware Settings
Menu 2: VMware Shutdown Management

Independent to a standard shutdown via the VMware Settings, RCCMD offers the option of not only organizing virtual machines into shutdown groups, but also establishing a direct dependency between individual virtual machines in advance. RCCMD proceeds as follows:

Sequence 1: Custom Shutdown Group

The Custom Shutdown Group defines a first group of virtual machines for the initial shut down. Virtual machines can be added or changed in position relative to each other by using drag and drop. A placed virtual machine placed will be permanently removed from the list of ESXi hosts and displayed exclusively under the „Custom Shutdown Group".

➔ In case of a shutdown, RCCMD will exclusively contact all known servers as configured at „VMware Settings" to search for this virtual machine name.
➔ If the virtual machine cannot be found, configured time windows are meticulously tracked, but the virtual machine state is no longer taken into account.

#	Virtual Machine	Trigger	Duration (s)	Delay (s)	State	Remove
1	🔒RCCMD-Test_nr03_12_12_24		13	10	⏻	🗑
2	🔒RCCMD 250210 new	after previous ⌄	10	10	⏻	🗑
3	🔒dry_run	after previous ⌄	10	10	⏻	🗑
4	🔒GH_RCCMD_NEW_FUNCTION	after previous ⌄	10	10	⍰	🗑
5	🔒Kirby-Webdevel	after previous ⌄	10	10	⏻	🗑

Trigger, Duration (s) und Delay (s)

Virtual machines stored in the Custom Group can be shut down individually in relation to each other. Since the settings are not tied to the respective states of virtual machine, RCCMD run the shutdown with the specified order as conifgured, even if the virtual machine requires less or more time for the individual shutdown process.

Trigger: „after previous"*	Defines that the individual delay (s) is started restrictively after the duration (s) of the previous machine has expired
Trigger: with previous"*	Definiert, dass der individuelle Delay (s) zeitgleich mit der Duration (s) der vorangehenden Maschine startet.
Duration (s)	Defines that the individual delay (s) starts at the same time as the duration (s) of the previous machine.
Delay (s)	Defines a time delay when the shutdown is sent to the respective virtual machine. The time delay has an effect relative to the trigger.
State	Shows the current operating state of the found virtual machine. Only active virtual machines can be shut down. The operating state is for information only and does not affect the shutdown procedure.
Remove	Removes the virtual machine from the list and adds it back to the known ESXi host. The virtual machine is then automatically shut down using Shutdown Sequence 3: Default Group.
*) The Duration (s) represents an administrator-defined value a virtual machine has been granted before RCCMD consideres the shut down is done and jumps to the next step: If an administrator knows that an upstream management server with all routines needs around 300 seconds to shut down, but closes the network connections within 100 seconds, a downstream backup or database server does not necessarily have to wait for the full duration (s) of 300 seconds of the management server. In this case, an administrator may deside touse the triggers to define whether the individual delay (s) of a virtual machine starts at the same time as the shutdown of the previous machine, or explicitly only after it has expired.	

Sequence 2: General Shutdown Group

This static shutdown group is started as soon as the delay (s) of the last entry of the custom group (sequence 1) has expired. All virtual machine names that are listed in the General shutdown group will be shut down at the same time without an individual shutdown timing: the default value of 90 seconds is applied for all virtual machines before the next shutdown group is called.

Sequence 3: Default Shutdown Group - No Cathegory / General Shutdown Group

Each host configured at "VMware Settings" is queried in real time during the shutdown procedure for currently available VMs:

A virtual machine found that is not managed by a static shutdown group is dynamically recorded and shut down accordingly - including the virtual machines that were newly rolled out after configuring RCCMD or migrated to one of the hosts defined under VMware Settings at a later point in time.

➔   This group is a dynamic system group and cannot be configured.

Sequence 4: Host based Shutdown Group

This is the last group to be shut down. The essential infrastructure servers such as DHCP, DNS, RADIUS, mail services, virtual telephone systems and the appliance are stored here. In this case, the shutdown does not take place via the VMWare Shutdown Management, but is transferred to the VMware Settings with the shutdown duration for hosts, which shuts down the virtual machines stored here and then the physical hosts.

Quick configuration, extended shutdown scenario:

Step 1: Hosts Definition

In this configuration step, define the ESXi hosts that should be shut down by RCCMD. Add all hosts and confirm the access data and verify the communication.

Step 2: Virtual Machine Dependency Setup

In this configuration step, define the interdependencies and assign shutdown groups.

Open the "VMware Shutdown Management" menu:

	Add... Remove Edit... Verify	
	ESXi Hosts to shutdown	
ESXi Address	**Shutdown duration**	**Verify**
192.168.200.202	90 Seconds	success
192.168.200.156	90 Seconds	success
192.168.200.107	90 Seconds	success

All ESXi hosts specified under VMware Settings, including the virtual machines located on them, are displayed together with their respective operating status:

	This virtual machine is OFF – System is secured in case of an ESXi host shutdown.
	This virtual maschine is paused, or hybernating for the moment.
	This virtuelle Maschine is ON and therefore harmed in case of a power failure.
	The virtual machine is added to a static shutdown group, but RCCMD cannot find it (moved to other hosts or deleted by administrators). RCCMD will use the timing settings and configured triggers to jump to the next virtual machine in list.
	Guest System: This Icon represents a virtual machine with a custom content or function.
	A virtual machine with this icon ist he vCenter oft he according cluster.
	The RCCMD Appliance: RCCMD knows his own virtual machine name. The RCCMD Appliance is in general excluded from any configurable shutdown procedure.
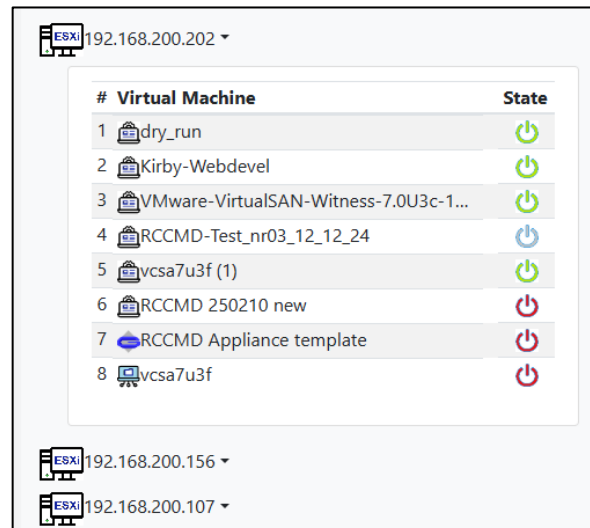
Note: Exception for vCenter and RCCMD Appliance

All virtual machines are treated equally - except the virtual machine RCCMD is running on as well as the vCenter, which can also appear as a virtual machine within an ESXi cluster. Depending on the configuration, RCCMD will handle both virtual machines separately to grant a structured shutdown management.

Enabling shutdown control when using a vSAN

Before starting, please read the following configuration notes carefully to prevent shutdown issues caused by a wrong configuration of RCCMD.

- **RCCMD can handle vSAN VMware environments.**

    Due to the fact, a vSAN is very complex and the operating conditions of a vSAN differs when compared with a single host or a standard cluster, there are some pre-conditions that must met before RCCMD can shut down a vSAN:

- **The RCCMD client that handles the vSAN cannot be installed inside a vSAN**

    Due to the fact, each host of a vSAN must be set to in maintenance mode before the can be switched off. As long as one virtual machine is running, it is not possible to switch off the hosts.

- **The vCenter that handles the vSAN is always the first virtual machine and the last virtual machine.**

    The vCenter is the control unit of a vSAN. It is allowed to install the vCenter inside the vSAN as well as running it on a single host that is not part of the cluster. The essential function of the vCenter is managing the data synchronization inside a vSAN after all other virtual machines are down. You need to ensure that the vCenter can complete this operation.

- **If you run a Witness-Server as a virtual machine inside a vSAN**

    The Witness Server has a special task If two hosts do not match which host holds the most recent data, they ask the witness server. The witness server acts like a complete host but cannot maintain virtual machines.

    Due to this fact, the witness server can also be virtualized in the vSAN and still acts as a stand-alone host. In that case, you need to differ between the Witness server's IP address and the host's virtual machine where the witness server's virtual machine is located.

- **The witness server is shut down regularly within the vSAN cluster.**

The host that maintains the virtual machine that contains a witness server, needs a second RCCMD client for enabling the maintenance mode after the witness server is switched off. Technically, an RCCMD client can only handle the vSAN or the host it runs on:
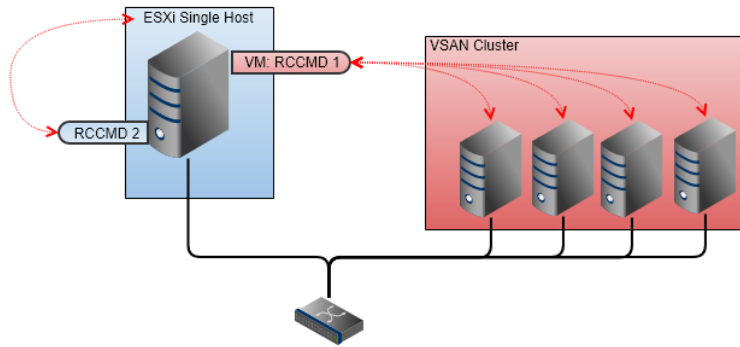
Therefore, if you have single hosts AND a VSAN cluster, you will need at least 2 RCCMD clients: RCCMD 1 manages the shutdown of the VSAN cluster and RCCMD 2 manages the shutdown of the single host. The shutdown routine is then divided into 2 different commands for the CS141:

> o Shutdown the VSAN cluster

> o Shutdown of the single host

Since the two RCCMD clients run side by side:

When choosing the correct time window for shutdown tasks, ensure the VSAN has turned off all hosts completely before turning off the last remaining single host - otherwise the RCCMD client that manages the shutdown of the VSAN may not be able to complete the shutdown routine because the second RCCMD client performs a local virtual machine shutdown.

Note

Appliance vs Appliance - What is the Virtual Machine and what is "the RCCMD client"

Basically, the two appliances do not differ from each other: Both are virtual machines. However, because you use two appliances, the name of the virtual machine they run themselves on, will differ. Entering the name of the virtual machine will prevent that an RCCMD client will shut down itself first. So, if you tell RCCMD 2 the name of his own virtual machine, it will consider that RCCMD 1 is just another "guest VM" and will shut down it. When using a vSAN, the shutdown commands of the CS141 will harmonize the shutdown behaviour of both appliances.

✓ **Ensure required time windows due to the changed shutdown sequences in case of a vSAN:**

The target when using a vSAN is to combine maximize resource availability with data redundancy. The system is therefore not well suited to carry out a fast shutdown without strict procedures. Since a system-wide complete shutdown is rather an exception, it is difficult to estimate how much time the VCenter within a vSAN will need to take all hosts into maintenance mode.

In principle, vSAN proceeds a shutdown in three steps

The time-critical part is the post-synchronization phase, as this phase is difficult to estimate:

Maintenance mode can only be reached after the synchronization of the data in between all hosts has been completed. This process is dynamic and changes depending on available hardware, the number of virtual machines, and the amount and type of data contained within the virtual machines that ultimately need to be synchronized between all hosts.

What makes matters worse is that this process takes place within the vSAN - at some point, the hosts are in maintenance mode, which means that the process is complete.

This is offset by the maximum operating time of the UPS

RCCMD needs clear time windows to be specified for the shutdown, which, in addition to the calculated times for a shutdown, must also be based on the operating time of the UPS - RCCMD therefore needs a reserved time window to carry out the shutdown, it should grant enough time to

Shutdown all all active virtual machines

During this shutdown phase, al virtual machines will be shut down.

Post Synchronization phase

At this system state, all hosts synchronize their current datasets.

Switching into maintenance mode

All virtual machines are shut down and the datasets are up to date. The hosts announced to reach the maintenance mode for switching off

- o   allow the IT to be shut down in a timely manner,
- o   provide a time buffer if the post-synchronization phase changes
- o   carry out shutdown procedure within the safety range of the UPS's running time
- o   ensure there is enough time for the host outside the cluster to shut dow

Take DRS within the vSAN cluster in sight

Contrary to popular belief, DRS and vCenter are independent system services that simply communicate with each other. It's even possible to set up an HA cluster without DRS, although this doesn't necessarily make sense, since the HA cluster itself actually implies DRS.

In contrast to an HA cluster, DRS is an essential component in a vSAN because this service can detect unused storage resources in the background and bundle them for a virtual machine. This intelligent, real-time resource management allows the operation of more virtual machines than in a normal cluster:

Virtual machines that now assume this distributed state are particularly vulnerable to a host-based cluster shutdown because vCenter and DRS only implement the cluster shutdown cleanly together if explicitly instructed to do so by an administrator via vCenter.

Although VMware recommends a cluster shutdown procedure via maintenance mode, if the hosts are put into maintenance mode too quickly, the DRS service may not be able to immediately determine the necessary resources for an internal migration of VM data and will attempt again after a sort of waiting loop. Virtual machines whose allocated disk space is withdrawn in this case because the hardware is no longer available are acutely affected by the outage. Whether and to what extent the operating system and data are damaged depends heavily on the memory state and the operating system's use.

The new RCCMD Shutdown Management with its customized shutdown procedure can not only shut down sensitive systems in a manner that is dependent on one another but also save valuable system resources once the general shutdown takes effect.

Important:

An overview of the time window the UPS can provide is mandatory for an orderly shutdown. This will determine not only the specific schedule but also the latest time slot to start the system shutdown:

Shutting down a vSAN is a very system-critical process due to its technical nature. A vSAN reacts sensitively if it is not shut down properly.
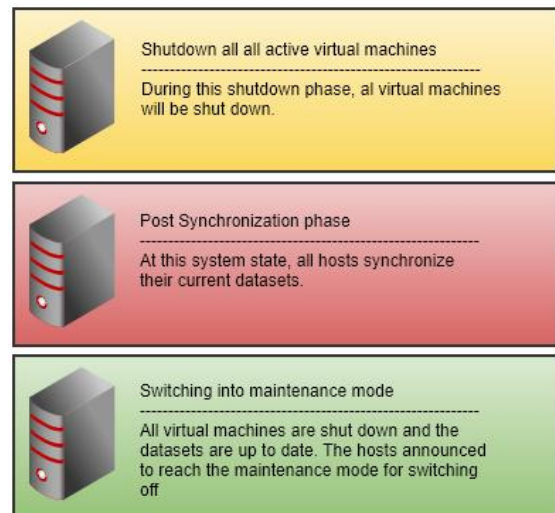
Preparing RCCMD for the vSAN

At VMware settings, enable "Hosts are also vSAN nodes"

Virtual Machine Management:	by RCCMD ▾	Info...
Virtual Machine behaviour:	Shutdown Virtual Machines ▾	Info...
Safely decomission vSAN nodes:	No vSAN in use ▾	Info...
	No vSAN in use	
	Hosts are also vSAN nodes	

To manage the shutdown routine, ensure that the RCCMD appliance must be located outside the VSAN cluster.

Once you have activated the vSAN mode, you will get additional menus:

vSAN Timeouts
Ensure all operations complete within their timeouts! Integrity of vSAN Objects will break if any timeout interrupts a running operation.

Mode for decommissioning vSAN nodes:	No data evacuation ▾	Info...
vSAN Resync timeout in Seconds:	200	Info...
Seconds to wait before setting Maintenance Mode for vSAN:	100	Info...

<u>Mode for decommissioning vSAN nodes</u>

Leave the decommissioning mode on No data evacuation - this mode is the fastest method to shut down a vSAN cluster:
The virtual machines are shut down in a structured way and then all data will be synchronized on all affected hosts.

<u>Definition of the vSAN Resync timeout</u>

Unlike the default procedure, the vCenter becomes active after the virtual machine shut down and start synchronizing all records within the cluster.

This post synchronization phase defines the critical phase of the shutdown procedure:

All datasets from the virtual machines must be in sync with mirrored data stored on other hosts.
As long as this synchronous system state is not reached, the Maintenance mode cannot be taken by any host.

Note:

This process is very dynamic and depends on the type of data that needs to be synchronized. You may have created several new virtual machines and the synchronization time will only change marginally. However, it can also happen that you create a virtual machine and thus radically increase the post-sync time. In other scenarios, the data within the virtual machine may grow organically cause by the usage, which in turn affects the time required:

This value cannot be determined once during the first installation as a fixed value, it must be regularly checked for up-to-datedness and adjusted if necessary.

The vCenter takes all the time needed for this process. Unfortunately, this relative amount of time is in direct contrast to a clearly defined time window that can be provided by the UPS during an emergency power operation. You need to calculate a sufficiently large time window to give the vCenter a time reserve in case of the calculated period is insufficient.

<u>Defining maintenance mode for the vCenter.</u>

This setting defines how much time the vCenter has to shut itself down after synchronizing data. If the vCenter runs as a virtual machine within the vSAN, this point in time becomes interesting: After this time window, the hosts are put into maintenance mode and the vCenter is switched off by its host.

Enter data for the vSAN managing vCenter

Enter the vCenter Server credentials:

Host name or IP:

192.168.200.85

User name:

administrator@vsphere.local

Password:

•••••••••••

Check Values

Since RCCMD must coordinate with the vCenter over the entire process, the access data for the vCenter, which manages the vSAN, is mandatory.

At this configuration dialog, do not enter credentials for individual host.

Define the vSAN managing RCCMD client:

RCCMD has the task of shutting down all virtual machines and turning off the hosts at the end. Since within a vCenter not only a vSAN but further hosts can be mapped, RCCMD can shut them down, too. There are two exceptions that need more attention:

Information about the virtual machine running RCCMD

The virtual machine that runs RCCMD must not be shutdown. Or else RCCMD cannot shutdown the other virtual machines and hosts. Enter the virtual machine's name on which RCCMD runs.

VM running RCCMD:

hayabusa

Although RCCMD itself cannot run in the vSAN that should be shut down, the vCenter that manages the vSAN may include additional hosts in its list. The RCCMD appliance is a virtual machine that must comply with the control commands of the host on which it is running itself - if the host advices a shutdown, the appliance will do it. To prevent RCCMD from inadvertently giving itself a shutdown command, enter the name of the virtual machine you chose for RCCMD. When entered, the virtual machine that holds this name will be excluded from the shutdown process.

Define the virtual machine that contains the vSAN managing vCenter

The virtual machine that runs vCenter must not be shutdown. Or else vSAN Hosts cannot be decommissioned properly. Enter the virtual machine's name on which vCenter server runs. If vCenter Server is not shut down by RCCMD, or is not running on a virtual machine, then ignore this field.

VM running vCenter:

vcsa67 (2)

Within the vSAN system, the vCenter performs special administrative tasks, but is also a virtual machine. During the shutdown, RCCMD first gets an overview of active virtual machines and then shuts them down, migrates them, etc. With this setting, RCCMD will know which of the virtual machines is the vCenter and will shut down it exclusively as the last machine in the vSAN shutdown procedure.

Definition of the vSAN ESXi host nodes

Define the hosts to be shut down by RCCMD. The virtual machines can be moved to other hosts via the vCenter. To shut down a host, RCCMD requires the following information:

HOST / IP name

We recommend using the IP address of the host at this point to avoid addressing problems when parts of the IT infrastructure are down.

Due to the fact RCCMD supports host names, you may enter a host name, too.

User

A user with the appropriate system rights to shut down the VM Ware environment accordingly. Keep in mind to use a local l host administrator with root rights to grant the shutdown command permission!

Password

The password assigned to the user that allows RCCMD to authenticate itself as authorized.

Add ESXi Host credentials ×

Enter the information for this ESXi Host below. (If vMotion shall be used, the Host name must be identical to the name in the vCenter.)
Do not put credentials for vCenter here!

Host name or IP: 192.168.200.30

User name: RCCMD

Password: ••••••••

Time granted for virtual machines to shutdown before Host gets shutdown in seconds:

Seconds

Check Values ⟳ checking ESXi Host credentials...

Abort   Save Changes

28

Shutdown delay

The next step is to determine how much time RCCMD should allow the virtual machines to shut down before the before the ESXi host will quit all operation and switches off:

Shutdown delay:	Seconds
	Time virtual machines are granted to shut down. Default: 90

The vSAN has a special feature compared to other operating modes:

The shutdown duration typically defines the time window that a host grant the operating systems within virtual machines before the virtual machine is simply powered off. Thereby it does not matter if a vCenter has previously tried to migrate machines or not.

When this command is issued to the hosts running in a vSAN, there are no more virtual machines that need to be powered off:

- All hosts must be in maintenance mode

- A host can only be in maintenance if all virtual machines are moved or switched off.

For the hosts in vSAN, this means that the shutdown time of virtual machines can be set to 1 second:

The shutdown routine on a vSAN has already brought all hosts into maintenance mode. Consequently, no time window is required to grant operating systems within a virtual machine for a shut down.

Add...	Remove	Edit...	Verify

ESXi Hosts to shutdown

ESXi Address	Shutdown duration	Verified
192.168.200.107	1 Seconds	
192.168.200.124	1 Seconds	
192.168.200.156	1 Seconds	

Special role: The witness server

Small vSAN systems lack the necessary resources to be able to independently adjust all data stocks.

To prevent problems with data synchronization in minimalist vSAN systems, a witness server is used:

This witness server acts as a stand-alone host in vSAN, but is not responsible for hosting and managing virtual machines - as soon as hosts are unable to agree with the timeliness of their datasets, the witness server decides which host has to synchronize the data.

The witness server can be both, a real physical machine with its own hardware as well as an acting like physical host but running within a virtual machine. The vSAN knots cannot see the difference between the different setup strategies of a witness server. But this difference affects the RCCMD configuration:

If running a real witness server as a standalone machine:

In this case, assign the witness server and any hosts that you want to shut down. The hosts will go into maintenance mode accordingly:

- Shut down virtual machines

- The vCenter will perform the resynch

- The hosts switch into maintenance mode

- The hardware can be switched off.
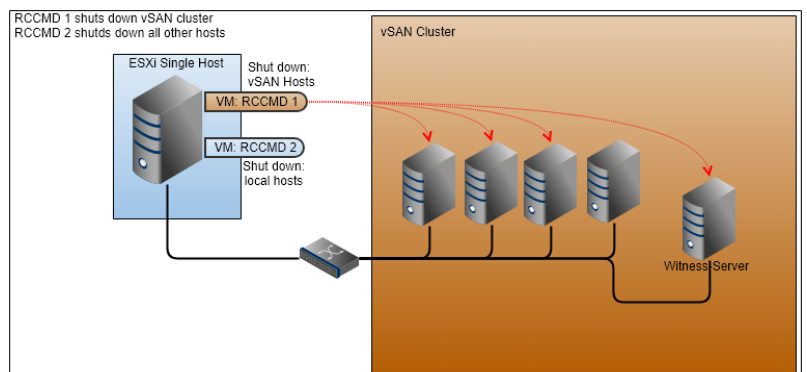
When using a virtual machine to run a witness server

If you run the witness server as a virtual machine in the vSAN, you must differ between the host on which the witness server is stored and the witness server as a stand-alone host. Since the witness server acts like a host within the vSAN, it is perceived and treated accordingly - The installation type does not matter:

While the host that maintains the virtual machine of the witness internally perceives only one virtual machine running "some kind of system", it accepts the witness server as a standalone host and network node on the network. If the wrong IP address has now been specified, the host responsible for the virtual machine will respond correctly:

- The host will stop running the virtual machine

- The host changes to Maintenance Mode

However, since the (albeit virtualized) witness server represents a full-fledged host and network node, it must consequently be treated as a real host and put into maintenance mode before being turned off. Formally, you need two RCCMD appliances to shut down a vSAN. If you use a virtualized witness server, you can use the second RCCMD to regularly switch off the host that manages the virtual witness server.
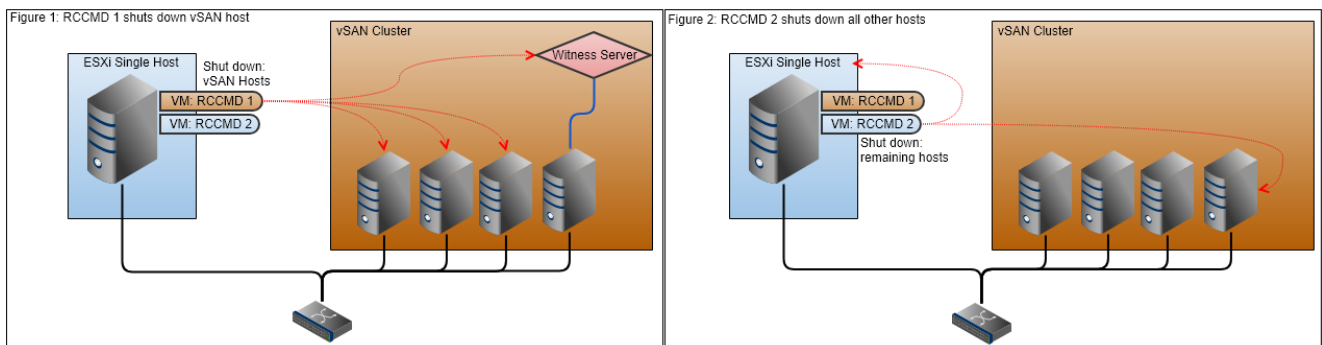
Tutorial: If the shutdown on a vSAN has to be aborted once...

A normal ESXi cluster with vCenter differs from a vSAN:

While a normal cluster with individual hosts can ultimately shut down and switch off its virtual machines on its own if maintenance mode is not possible, a vSAN can only be switched off if absolutely no virtual machines except the vCenter are running on the vSAN. The second major difference is, that the RCCMD client that manages the vSAN cannot logically run within the vSAN cluster- it must control it from outside. The third point is that vSAN requires a run-on time after all virtual machines have been shut down, during which all inventory data is synchronized; only then may the hosts be switched off safely.

Due to these differences, there are logical sections between in between aborting the shutdown sequence is quite possible. This tutorial shows one way in which an automated shutdown could be aborted. Please note, this is not the intended way how to use RCCMD and you will do it at your own risk...

In this example, the framework conditions are fulfilled that allow operation without a Witness server:
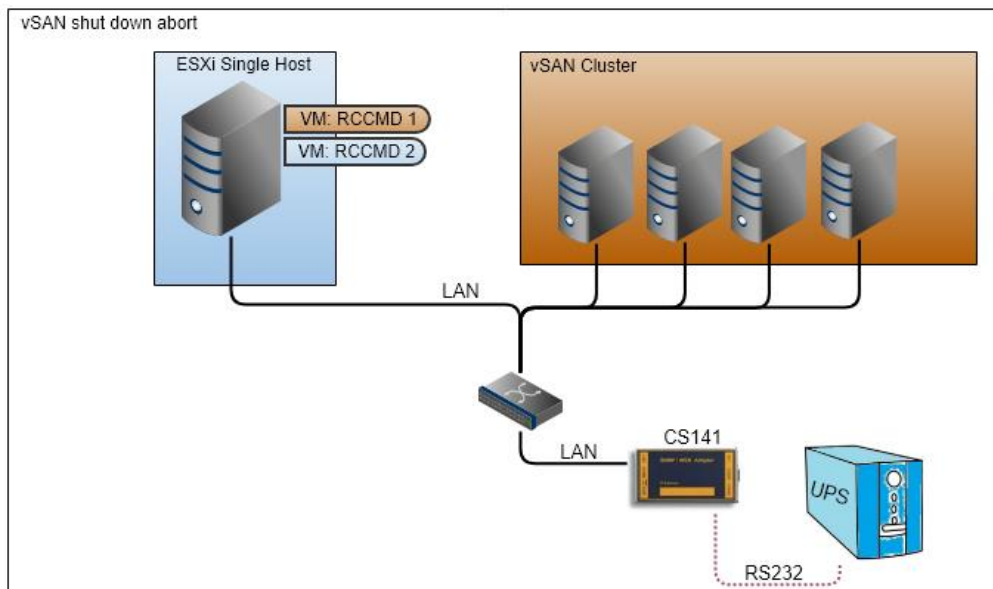
Problem:

As soon as there is a power failure, RCCMD 1 becomes active and starts the shutdown process in time. Measurements have shown that the entire shutdown will take something around 38 minutes. Since the UPS can cover up to 45 minutes, the shutdown must therefore be initiated after 5 minutes at the latest, otherwise the system cannot be shut down correctly. With a time window of 20 minutes, it now results that the main power supply returns and a further shutdown is no longer necessary.

Since the RCCMD appliance, by definition of the software purpose, cannot revert or stop the shutdown sequence, RCCMD 1 will also perform this to the end and shut down the vSAN cleanly. The CS141 cannot send a "clear all pending commands" - signal to RCCMD 1.

Make a decision of principle

Since the UPS was running for 20 minutes, another mains failure is likely to have fatal consequences, consideration should be given to whether a shutdown and a wait until the minimum 40-minute hold-off time or an abort of the shutdown is an option. The commands given are identical at this point, but the event changes. In this example, an abort of the shutdown was chosen. Like the shutdown, the termination is initiated via the CS141, only with the event "Power Restored".

It is important always to keep in mind: The shutdown itself is already an emergency measure - thinking about a forced termination of the emergency measure is legitimate, but always associated with additional risks.

Interrupt the shutdown sequence

When the Power restored event occurs, a shutdown signal is applied to RCCMD 2 - which is supposed to shut down the last single host - which includes the immediate shutdown of all virtual machines. RCCMD 1, as a virtual machine, will adhere to this default and shut down and power off accordingly - forgetting that there are still official control commands pending that affect the vSAN.

The vCenter will process the last commands and then wait for further instructions accordingly. Since the control commands are bound to time windows that have been stored in RCCMD 1, it is possible to quickly find out in this way what has already been done.

1. vMotion is active and tries to move the virtual machines by default.
2. vSAN - shutdown is active and the virtual machines are shut down or moved.
3. The post-synchronization phase is running.

This method will end the current running phase and if no new command is received afterwards, the vSAN will stand in this system state and wait for further orders

Structured Restart: Reactivate RCCMD Protection

Send the WOL signal to the ESXi Single Host - it will power up via the WOL signal and accordingly the RCCMD appliances also start and move to their start position. The RCCMD protection is now up.

Starting the depowered hosts

Now, send a WOL signal to each single host - it does not matter whether this host has already been switched off or not: If the host is running, the WOL signal falls into a void and is ignored at its destination.

Start the Virtual Machines (VM''s)

Depending on the systen configuration, virtual machines that have been switched off you may decide to switch them on via a WOL signal. To do this, send a WOL signal to the MAC address of the respective virtual machine.

Note

Keep in mind that WOL signals are sent to the MAC address, the CS141 must be in the same network segment or the signal must be routed through accordingly.

Since you can freely define the timing, it is even possible to specify a special order in which virtual machines start up. This allows you to have the basic network start up automatically.

What else is importan when aborting a vSAN shutdown:

Do not just restart the RCCMD client via web interface

RCCMD has a protection mechanism that executes a valid shutdown even if someone stops the RCCMD service via the web interface after the shutdown has been triggered. The system is nevertheless shut down cleanly and switched off. That's why you need to shut down the managing RCCMD client – just click "restart" with the web interface will not interrupt.

A *SAN may change the time window and there may require to adapt the timing parameters regularly:*

Depending on the current data situation and the expansion stage of the vSAN, this shutdown can be very protracted and the procedure must be started accordingly early. If the main power supply or an emergency generator becomes available during this time, this does not change the shutdown routine - RCCMD follows an instruction and organises the implementation..

And, of course, if a shutdown in progress must be stopped…

This process cannot be automated completely in the end, because RCCMD coordinates the instructions and their time windows, but does not receive any feedback from the vCenter about logical sections. As a result, an administrator must consider whether to let the shutdown run to the end and restart the system or to provoke an abort within a shutdown routine:

Both have their respective advantages and disadvantages.

To stop the shutdown process and set the associated scripts back to 0, stop the appliance virtual machine on the host. Once this happens, no more commands are transmitted to the hosts and the system stops the shutdown process after the last command has been successfully transmitted. You may save time, but a clear restart may also be the better way for some server operations.

IMPORTANT:

For a shutdown abort, ensure that the virtual machine is shut down with the appliance, even if you set RCCMD to "Stop" in the web interface and the service has been stopped according to the web interface:

The shutdown sequence will still be executed

How long is the estimated shutdown time?

Basic shutdown time

After entering all the data, an estimate time will be shown RCCMD may be need for a full shutdown.

You can see the estimated shutdown time below the ESXi host settings.

Total estimated Shutdown time for the System with current configuration: 00:05:54.

Please note that this value is a guideline calculated by entered data.

This value is intended to help you to find the optimized trigger time to run an emergency shutdown routine if a power failure occurs.

Note:

Each UPS can only grant a pre-defined time window emergency power. When the batteries are depleted, the UPS will shut down itself to avoid damaging the batteries. In general, it will not help if you just play with the numbers within RCCMD until the estimated shut down time matches the data sheet of the UPS:

Furthermore, these values are just a snapshot of your system based on the data you entered! Please check regularly whether the entered values meet the real shut down condition in case of an emergency.

Keep in mind that between two shutdown tests the shutdown conditions may change. When calculating and adapting the average shutdown time, we recommend to take some extra time than the minimum time requires.

The configuration of RCCMD is now complete and RCCMD will be able to shut down your system in an emergency. Please note that RCCMD does not become active automatically - it needs a valid RCCMD shutdown command. The transmitter is usually an SNMP card or a software tool that can handle RCCMD shutdown signals.

On the following pages all configuration menus are explained in detail in the order of appearance.

Tutorial: Setting up a manual IP address

Sometimes, no DHCP server is available. In this case, the carrier system starts, but without a valid IP address that RCCMD can use. Since the 100% availability of a DHCP server can never be granted, it is recommendable to assign a static IP address for the RCCMD appliance.

The required configuration file can be found within this directory:

/etc/network

To switch the appliance to a static IP address, the file "interfaces" must be edited:

With nano, the appliance comes with a powerful and user-friendly text editor. To start editing, type the following command:

sudo nano /etc/network/interfaces

By doing so, the editor starts with required root rights for saving and presents the network configuration file:

Search for this entry:

➔   Iface ens33 inet dhcp

This entry decides whether the appliance has been assigned the IP address via DHCP or statically.

Edit the following settings to adapt the network configuration to fit to your local network environment::

Source /etc/network/interfaces.d/*

The loopback network interface
Auto Io
Iface Io inet loopback
#The primary network interface
Alllow-hotplug ens33
#Iface ens33 inet dhcp   <- Use # to disable this line
iface ens33 inet static   <- Remove # to enable this line
Address 192.168.200.223/24   <- Assign an IP-address and a subnet mask
Gateway 192.168.200.1   <- Define the local network gateway
dns-* options are implemented by the resolvconf package, if installed

dns-namservers 192.168.200.3 192.168.200.5 168.168.200.1   <- Define your local DNS-Server.
dns-search local

Save and restart the appliance. After reboot, the manual IP address should be active.

Note

It is possible to assign the IP address assigned by the DHCP server on first start as a static IP, but, on the other hand, it is also required to ensure that the DHCP server excludes the IP address from the general address pool.

Tutorial: Setting up an emergency user for the appliance.

> **Note**
>
> You don't want it, but passwords can get lost. Within complex systems, this can be very inconvenient and expensive issue, if a VM has to be completely relaunched and newly configured. The effort depends strongly on the complexity of the RCCMD configuration. If you decide to set up an emergency backup user, this should therefore be done before you start with the actual configuration work.

It happens again and again that passwords are lost due to adverse circumstances, e.g., because there is no proper documentation on the installed systems, passwords are forgotten because they are so rarely used, IT systems are inherited from other companies, etc.

by default settings, RCCMD does not provide any backdoors to recover lost passwords.

If you assign a different password to the standard console user admin and this password is lost, you basically have to set up the RCCMD client again. This could become a very complex problem in some cases, for example, if there are special scripts are stored that have to be recreated.

To prevent this uncomfortable situation, it is recommendable to set up a backup user with administrative access rights.

After installation work for the appliance is done, access the console with a freeware tool like Putty is provided.:

User: admin

Password: RCCMD

Getting root

Command: sudo su

Note that after logging in, you have not yet been granted the necessary rights to set up a corresponding emergency user. To set up such a user extended system rights are required.

Setting up user and password

Command 1: useradd <username>

With this command the user account is generated.

Command 2: passwd <username>

Assign a new password tot he according user.

Assign a user group

Command: usermod – G sudo -a Emergency

To grant the new user administrative rights, the user must be added to the according user group

Logging out

Command: exit

You need to enter exit two times. The first exit will end the superuser, the second exit will quit the session.

Performing an emergency user password reset

Start a session with the emergency user account. With the command sudo su, root rights are granted.

```
Welcome to RCCMD-Appliance.
To configure RCCMD point your web browser to: [https://192.168.200.99]!
$ sudo su

We trust you have received the usual lecture from the local System
Administrator. It usually boils down to these three things:

    #1) Respect the privacy of others.
    #2) Think before you type.
    #3) With great power comes great responsibility.

[sudo] password for Emergency:
root@rccmdAppliance:/#
```

Please note:

Your emergency user does not have the system rights to maintain the web console. Its only purpose is to reset the password for the user „admin ".

However, navigate to the director „resources ":

Command: cd /usr/rccmd/webconfig/resources

The configuration scripts required for the password query are located in this directory.

```
root@rccmdAppliance:/# cd /usr/rccmd
root@rccmdAppliance:/usr/rccmd# cd webconfig/resources/
root@rccmdAppliance:/usr/rccmd/webconfig/resources#
```

Opening the text editor to change the password

Command: nano realm.properties

With this command, the editor nano opens the according configuration file. Within this file, it is possible to reset the password for the user "admin" that will be used for the web based front end of RCCMD.

```
#RCCMD realm.properties
# username: password [,rolename ...]
admin: CRYPT:adg.Dq8TXmNZI, admin
```

Edit the file as followed:

#RCCMD realm.properties
username: password [,rolename ...]
#admin: CRYPT:adg.Dq8TXmNZI, admin   -> Type # to disable this line
admin: Notfall, admin   -> Add this line below

In this example, the user admin will use the Password „Notfall".

```
#RCCMD realm.properties
# username: password [,rolename ...]
#admin: CRYPT:adg.Dq8TXmNZI, admin
admin: Notfall, admin
```

Save the file and quit the text editor. Make sure that the original file name is overwritten and that your changes are not saved with a different file name.

Reloading the RCCMD configuration

Command: /etc/init.d/rccmdConfig restart
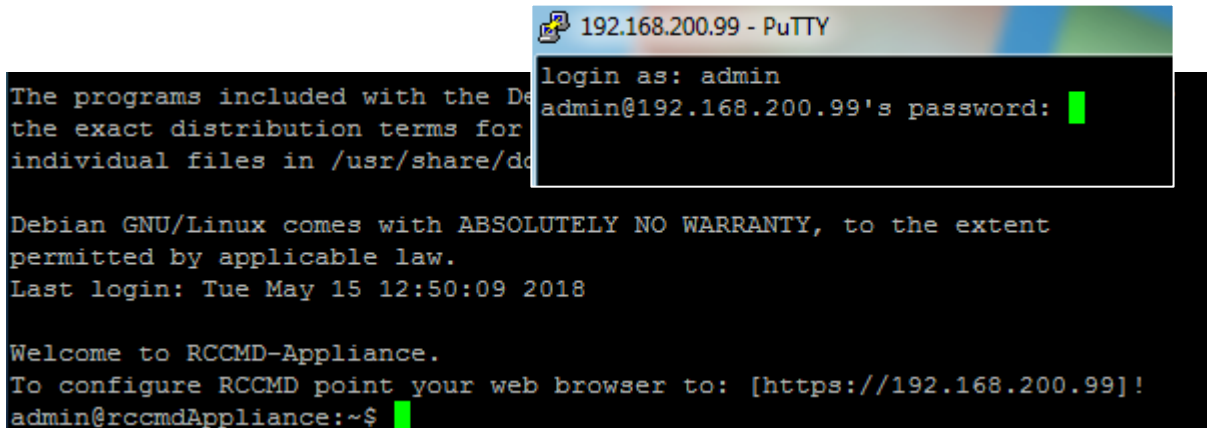
```
root@rccmdAppliance:/usr/rccmd/webconfig/resources# /etc/init.d/rccmdConfig restart
stopping RCCMD-Configurator...
RCCMDConf has been stopped.
Starting RCCMD-Configurator...
RCCMDConf has been started.
```

This command activates the password you have just assigned. Alternatively, restart the appliance. Now, open the web interface of your RCCMD installation and log in with the new password. From there, navigate to the user settings and set a new password.

Tutorial: Login via external tools

After installation, the RCCMD appliance allows direct access via a corresponding tool as soon as a valid and reachable IP address is available via both, static IP settings or assigned by DHCP. After rolling out the appliance, the console is directly reachable with a freeware tool like Putty:

User: admin

Password: RCCMD

Tutorial: Adding a keyboard layout

Since there are many world languages and corresponding keyboard layouts, you may want to use another keyboard layouts than default settings provide. If you want to make special settings within the console, it is therefore much more comfortable to switch the keyboard layout into your preferred language setup

To do this, first log in with the user admin and the current RCCMD password and obtain the system rights of a super user. In this example, the default password RCCMD is set:

Step 1: RCCMD console login

User: admin
Password: RCCMD

Step 2: Some installation work

Command: sudo su
Password: RCCMD

To proof your command, ensure that in front of *admin* the word *root@ … is visible...*

Now, install the appropriate tool that allows you to configure the keyboard layouts:
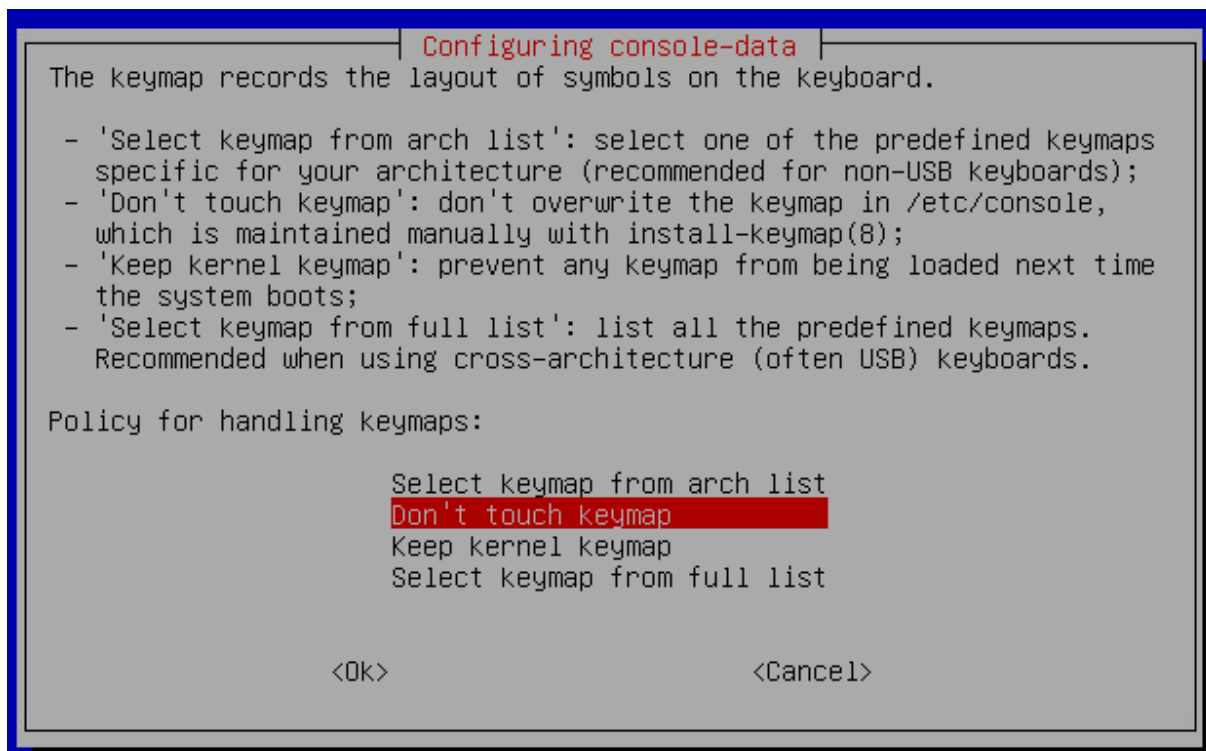
Command: apt-get install console-data

```
root@rccmdAppliance:/home/admin# apt-get install console-data
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  console-common
Suggested packages:
  unicode-data
The following NEW packages will be installed:
  console-common console-data
0 upgraded, 2 newly installed, 0 to remove and 1 not upgraded.
Need to get 0 B/1,270 kB of archives.
After this operation, 2,996 kB of additional disk space will be used.
Do you want to continue? [Y/n] _
```

Confirm the installation progress.

Step 3 The configuration dialog

After installation the configuration dialog should start automatically:

```
┌──────────────────┤ Configuring console-data ├──────────────────┐
│ The keymap records the layout of symbols on the keyboard.       │
│                                                                 │
│  - 'Select keymap from arch list': select one of the predefined keymaps
│    specific for your architecture (recommended for non-USB keyboards);
│  - 'Don't touch keymap': don't overwrite the keymap in /etc/console,
│    which is maintained manually with install-keymap(8);
│  - 'Keep kernel keymap': prevent any keymap from being loaded next time
│    the system boots;
│  - 'Select keymap from full list': list all the predefined keymaps.
│    Recommended when using cross-architecture (often USB) keyboards.
│                                                                 │
│ Policy for handling keymaps:                                    │
│                                                                 │
│                   Select keymap from arch list                  │
│                   Don't touch keymap                            │
│                   Keep kernel keymap                            │
│                   Select keymap from full list                  │
│                                                                 │
│                                                                 │
│          <Ok>                           <Cancel>                │
│                                                                 │
└─────────────────────────────────────────────────────────────────┘
```

Choose „Select keymap from full list" and confirm with ENTER.

Then select the keyboard you want to use from the list of available keyboard layouts and confirm your selection by pressing Enter.

```
     pc / qwertz / German / Apple USB / latin1 - no dead keys
     pc / qwertz / German / Standard / Programmer
     pc / qwertz / German / Standard / latin1
     pc / qwertz / German / Standard / latin1 - no dead keys
     pc / qwertz / Hungarian / Standard / Standard
     pc / qwertz / Polish / Standard / Standard
     pc / qwertz / Serbian / Standard / Standard
```

The configuration tool will install and activate the new keyboard setup.

Changing the keyboard layout

Since the tool is now installed and active, it is not possible to run the installation command again. Instead of the install command, you need to use this:

Command: dpkg-reconfigure console-data

```
To configure RCCMD point your web browser to: [https://192.168.200.124]!
admin@rccmdAppliance:~$ sudo su
[sudo] password for admin:
root@rccmdAppliance:/home/admin# dpkg-reconfigure console-data
```

This will restart the keyboard selection menu – you may now use another keyboard setup.

Note:

The command sudo su grants administrative rights until exiting with the command "exit". Alternatively, you can of course enter sudo [command] directly, but then you have to enter the password again each time. Do not forget to quit the superuser mode.

Tutorial: Installing RCCMD on a public ESXi Host

This installation instruction describes how to use RCCMD on a public domain ESXi Host.
Please notice that the installation on a public domain host is officially not supported by Generex (the warning in the RCCMD web configurator will never disappear).

There are several possibilities here - which instructions apply to you depends on two factors:

1. Which ESXi version is being used
2. Which RCCMD version is in use

Using RCCMD with VMware 5.x

For version 5.x, a (long since deprecated) Media Assistant was offered by VMware itself, on which an RCCMD for VMware was installed. The following steps must therefore be taken for the use of a free host with version 5.x:

1. Activate SSH in vSphere client:

In the ESXi Host configuration go to -> Software/Security profile -> Services->
Properties-> SSH and choose the option "Start and shutdown with the Host". Start the service and confirm with a click on OK.
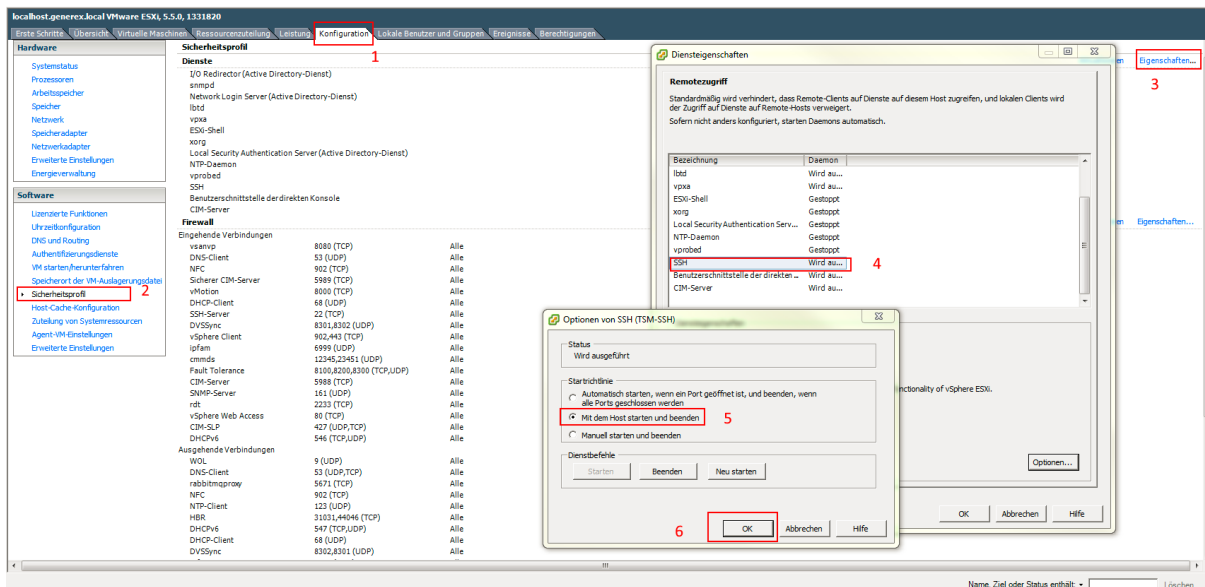
2. Activate automatic boot and shutdown of virtual machines in vSphere Client:

In the ESXi Host configuration, go to -> Start/shutdown VM -> Properties and set the mark for "Enable automatic boot and shutdown of VM"
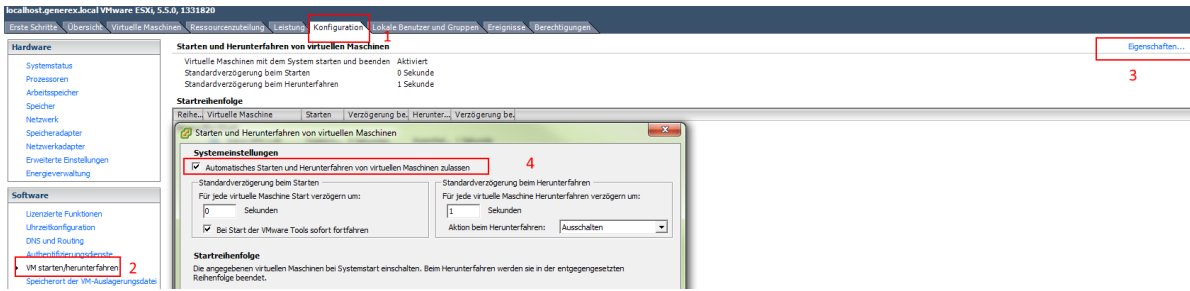
3. Make sure that all VM have installed the VMS VMware tools

4. Connect via SSH with the vMA, and copy the content of the file /root/.ssh/id_rsa.pub

5. Connect via SSH with the ESXi Host directly and paste the content of id_rsa.pub into the file /etc/ssh/keys-root/authorized_keys.

Make sure that the access authority for the file authorized_key is set to 600!

Command for this action is: "chmod /root/.ssh/id_rsa.pub 600"

6. Connect from the vMA via SSH onto the ESXi Host. On first startup you will be asked to add the host key to the known hosts.

7. Check the configuration. If you connect via SSH from vMA to ESXi host, you shouldn't get a password request.
If a password is requested, make sure that both files are 100% identical. If not, repeat the steps 4-7.

8. Activate the FREE_ESXI_SHUTDOWN script in the rccmd_shutdown.sh.

Comment the line ${ESXI_HOST_SHUTDOWN} with #, and remove in the line #${FREE_ESXI_SHUTDOWN} the comment at the beginning of the line.

Now you can test RCCMD.

RCCMD with VMware 6.7 onwards

The configuration is slightly different for version 6.7, as the VMA was deprecated with ESXi v. 6.5. Since version 6.5, RCCMD has been delivered with its own appliance, which contains a pre-installed and pre-configured RCCMD installation. The configuration path required depends on the age of the appliance being used.

For RCCMD Appliance *up to version 4.54.12 231129*, the configuration will be carried out as followed:

Note: This example decribes how to enable SSH-support for ethe ESXi 6.7 onwards free hist with the basic user admin. Ince RCCMD itself runs with the user "ROOT", you may run into the problem that it works the user admin, but not with the RCCMD command itself.

To avoid confusion, it is recommended to set up the user admin AND the user root. By doing so, it will work with the user root and athe user admin. To enable the root (or super user) for the entire procedure, type the command "sudo su".

<u>Activating the SSH console at the ESXi host</u>
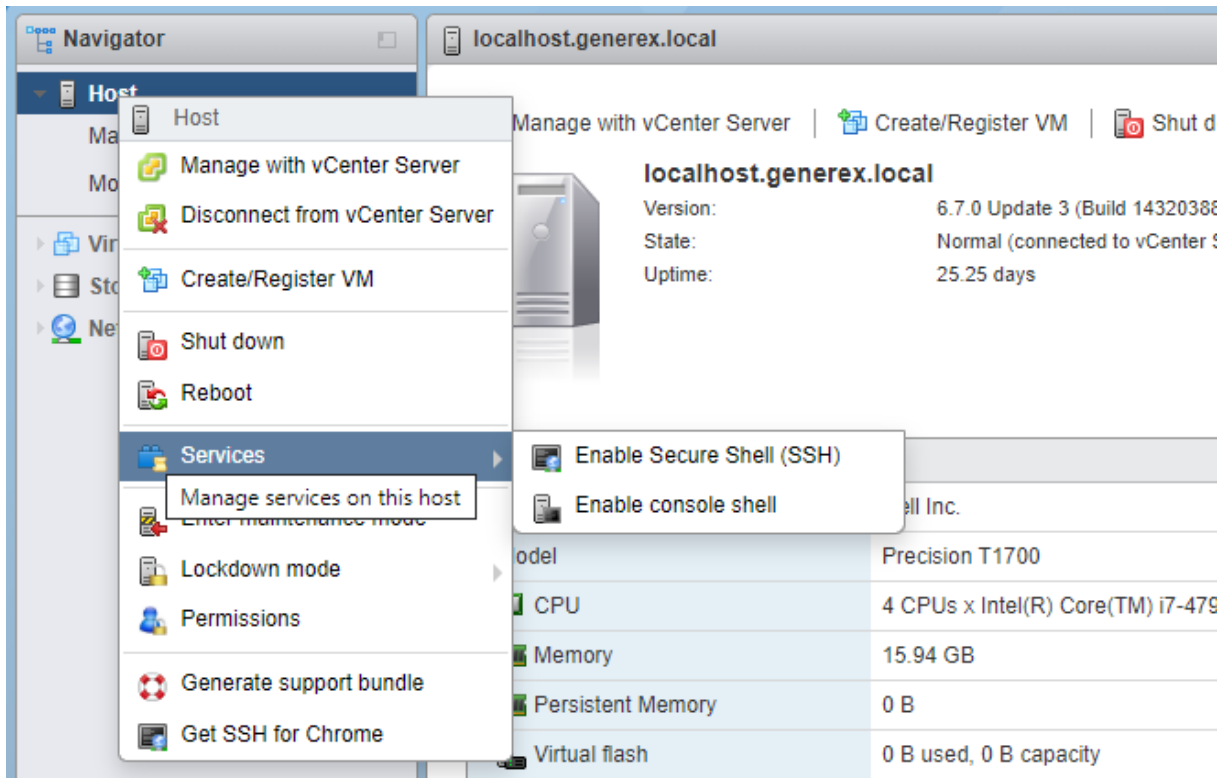
At the navigator on the left side, right-click the its according host. Under Services, click "Enable Secure Shell (SSH)". Repeat this procedure with "Enable console shell". After this, click on Manage and open the tab "Services":
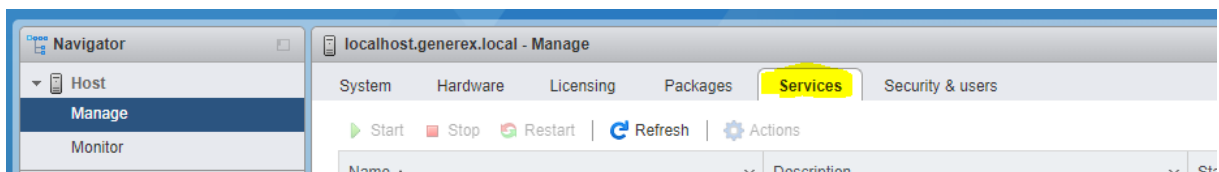
Search for TSM and TSM-SSH and ensure the system state is "Running".

In the next step, right-click on TSM to open the context menu. Under Policy, change the start condition to "Start and Stop with host". Otherwise, the service will not start when the ESXi host comes back after a power fail.

| TSM | ESXi Shell | ▶ Running |
| TSM-SSH | SSH | ▶ Running |

TSM		ESXi Shell		Running
TSM		SSH		Running
Restart		Syslog Server		Running
Start		vSphere High Availability Agent		Stopped
Stop		VMware vCenter Agent		Running
		X.Org Server		Stopped
Policy	►	Start and stop with firewall ports		
Policy options for this service		✓ Start and stop with host		
		Start and stop manually		
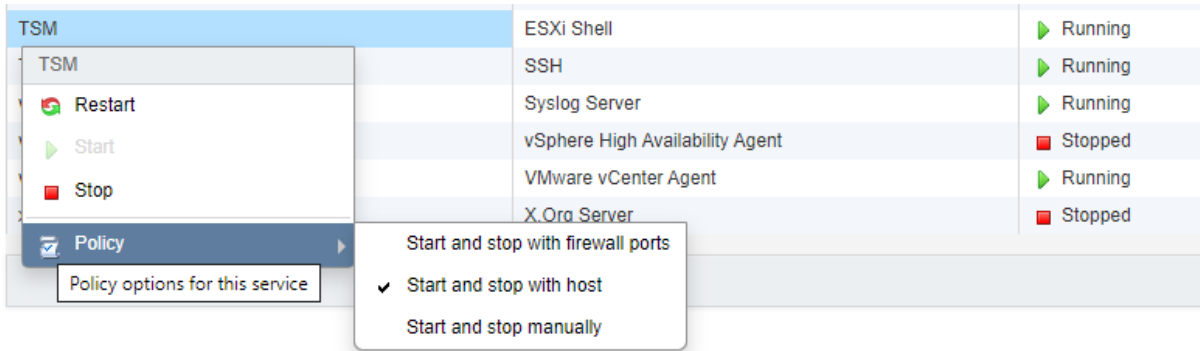
Repeat it with TSM-SSH service:

TSM-SSH		SSH		Running
TSM-SSH		Syslog Server		Running
Restart		vSphere High Availability Agent		Stopped
Start		VMware vCenter Agent		Running
Stop		X.Org Server		Stopped
Policy	►	Start and stop with firewall ports		
Policy options for this service		✓ Start and stop with host		
		Start and stop manually		

How to connect the RCCMD Appliance via SSH with the ESXi host

the following configuration steps cannot be done by the web interface, you need to use the console of the RCCMD appliance. You may use an appropriate tool such as the freeware program putty and log in directly on the console of RCCMD.

As an alternative, you can use the console feature of the host to open the RCCMD console.

```
Debian GNU/Linux 9 rccmdAppliance tty1
Configure RCCMD at: https://192.168.81.138

Hint: Num Lock on

rccmdAppliance login: admin
Password:
Last login: Mon Oct 14 14:14:59 CEST 2019 on tty1
Linux rccmdAppliance 4.9.0-8-amd64 #1 SMP Debian 4.9.130-2 (2018-10-27) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.

Welcome to RCCMD-Appliance.
To configure RCCMD point your web browser to: [https://192.168.81.138]!
admin@rccmdAppliance:~$
```
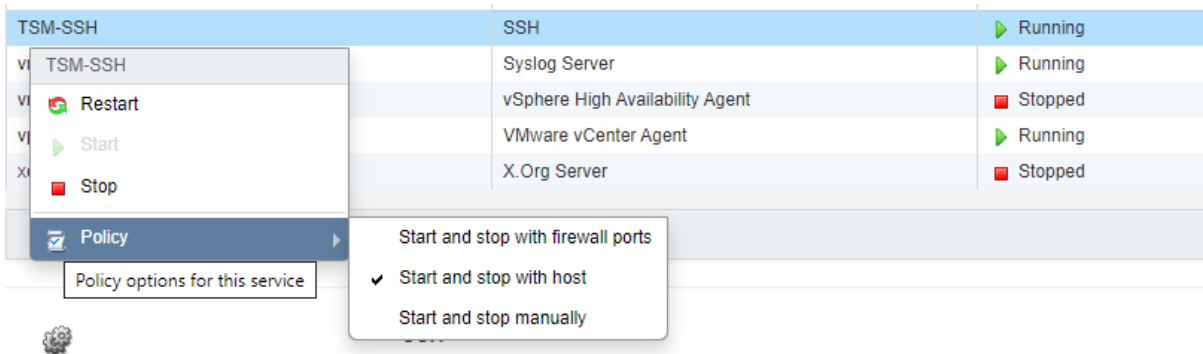
The RCCMD Appliance uses this default settings:

User: admin
Password: RCCMD

First you need to create a valid pair of SSH keys. The public key needs to be transferred to the ESXi host to authenticate the RCCMD Appliance.

Command: ssh-keygen

```
admin@rccmdAppliance:~$ ssh-keygen
```

Follow the configuration dialog:

a. Please define the file location:

```
Generating public/private rsa key pair.
Enter file in which to save the key (/home/admin/.ssh/id_rsa):
```

Keep the original settings, just press enter.

If you repeat this configuration step, an old key already exists. In this case, ssh-keygen will ask to overwrite the existing key:

```
/home/admin/.ssh/id_rsa already exists.
Overwrite (y/n)? y
```

To erase the existing key, just press "y"

b. Advanced password security

When dealing with high security standards, additional passwords to protect key data from unauthorized access, is mandatory. If you do not need additional password security to encrypt files, press enter without setting up additional passwords. For setting up a key, additional passwords are optional, not mandatory.

```
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
```

c. Finishing configuration work

```
Your identification has been saved in /home/admin/.ssh/id_rsa.
Your public key has been saved in /home/admin/.ssh/id_rsa.pub.
The key fingerprint is:
SHA256:rubVkhjMLzlXQAds8z708PagHW6UQsacuv9iYpdfdN8 admin@rccmdAppliance
The key's randomart image is:
+---[RSA 2048]----+
|        .o..     |
|        .+.      |
|        ..= .    |
|      o   .X     |
|       + S*.+ .. .|
|        *.++ O. .o|
|        = B..X +. E|
|        .*+.* +.. |
|        oo. =.=o  |
+----[SHA256]-----+
```

ssh-keygen tells you when it finished the key creation.

Transferring the public key part to the ESXi Host, Part 1

Now it is time to transfer the public key to the public ESXi host to allow the RCCMD appliance to send a shutdown command via SSH without additional passwords.

Command: ssh-copy-id root@<Ip address of your ESXi host>

```
admin@rccmdAppliance:~$ ssh-copy-id -f root@192.168.200.107
/usr/bin/ssh-copy-id: INFO: Source of key(s) to be installed: "/home/admin/.ssh/id_rsa.pub"
Password:
```

You need to enter he root password of your ESXi host. ESXi hosts.

Due to the fact the host is not authenticated, the appliance warns you it could be a faked server and asks if the connection should still be made:

```
/usr/bin/ssh-copy-id: INFO: Source of key(s) to be installed: "/home/admin/.ssh/id_rsa.pub"
The authenticity of host '192.168.200.107 (192.168.200.107)' can't be established.
RSA key fingerprint is SHA256:rbII6HjWaSPUcYUVfdiYttQurCL/1cjb2Ioveb/336c.
Are you sure you want to continue connecting (yes/no)? yes
/usr/bin/ssh-copy-id: INFO: attempting to log in with the new key(s), to filter out any that are alr
eady installed
/usr/bin/ssh-copy-id: INFO: 1 key(s) remain to be installed -- if you are prompted now it is to inst
all the new keys
Password:
```

Please answer this security question with "yes" (do not just enter y) to confirm the security warning.

When finished, the RCCMD appliance will show the success of the key transfer:

```
Number of key(s) added: 1

Now try logging into the machine, with:   "ssh 'root@192.168.200.107'"
and check to make sure that only the key(s) you wanted were added.

admin@rccmdAppliance:~$ _
```

Transferring the public key part to the ESXi Host, Part 2

Although the file was transferred correctly to the default directory, SSH without password will not work:
You need to correct a VMware-specific difference at the default directories:

Command: ssh root@<IP address of your ESXi host>

```
admin@rccmdAppliance:~$ ssh root@192.168.200.107
Password:
```

You need the ESXi root password to log in:

```
The time and date of this login have been sent to the system logs.

WARNING:
   All commands run on the ESXi shell are logged and may be included in
   support bundles. Do not provide passwords directly on the command line.
   Most tools can prompt for secrets or accept them from standard input.

VMware offers supported, powerful system administration tools.  Please
see www.vmware.com/go/sysadmintools for details.

The ESXi Shell can be disabled by an administrative user. See the
vSphere Security documentation for more information.
[root@localhost:~]
```

Please note: The first time you may be asked by the RCCMD appliance to add the ESXi host to the known hosts list.
If everything has worked properly so far, you are now connected via SSH with the ESXi server local console.

Now move on to the default directory .ssh where the ssh-copy-id command has placed the public key file:

Command 1: cd /.ssh
Command 2: ls

If everything is all right, you will now see the public key file "authorized keys"

```
[root@localhost:~] cd /.ssh
[root@localhost:/.ssh] ls
authorized_keys
[root@localhost:/.ssh] _
```

The contents of this file must now be appended to the "real" authorized keys file of the ESXi host without deleting other valid keys:

Command: cat authorized_keys >> /etc/ssh/keys-root/authorized_keys

```
[root@localhost:/.ssh] cat authorized_keys >> /etc/ssh/keys-root/authorized_keys
```

Please note that you will not get a confirmation message, the console will only report if something went wrong (missing file, etc.)
After you appended the public key, quit the SSH console and log off.

Command: exit, exit, exit,

```
[root@localhost:/.ssh] exit_
```

Testing your public key settings


```
Debian GNU/Linux 9 rccmdAppliance tty1
Configure RCCMD at: https://192.168.81.138

rccmdAppliance login: _
```

To validate that the public key works as expected, just log into the ESXi host again via SSH. If the certificate has been installed correctly, this can be done without a password query.

Log into the console of the RCCMD-Appliance:

User: admin
Password: RCCMD

Opening an SSH connection the authorized keys ESXi host:

Command: ssh root@<IP address of the host >

If everything is prepared correctly, you will see the following screens:

Local RCCMD Appliance login screen:

```
rccmdAppliance login: admin
Password:
Last login: Tue Oct 15 09:47:29 CEST 2019 on tty1
Linux rccmdAppliance 4.9.0-8-amd64 #1 SMP Debian 4.9.130-2 (2018-10-27) x86_64
```

SSH-Command to your ESXi host:

```
To configure RCCMD point your web browser to: [https://192.168.8
admin@rccmdAppliance:~$ ssh root@192.168.200.107
The time and date of this login have been sent to the system log
```

Welcome screen of the ESXi host:

```
The ESXi Shell can be disabled by an administrative user. See the
vSphere Security documentation for more information.
[root@localhost:~]
```

Reconfigure RCCMD to manage the public ESXi server

RCCMD need to know that it is a public server (or community edition) and the shutdown is an SSH command - you need to adapt the shutdown script for ESXi hosts.

Log into the console of the RCCMD appliance and move on to the according directory:

Command 1: cd /opt/rccmd/remoteHostScripts/
Command 2: ls

```
admin@rccmdAppliance:/$ cd /opt/rccmd/remoteHostScripts/
admin@rccmdAppliance:/opt/rccmd/remoteHostScripts$ ls
bash_tools.sh                              pltmp.pl
cache_host_dns_names.sh                    rccmd_shutdown.sh
checkESXipwd.pl                            registerGXPlugin.sh
checkESXiVersion.pl                        registerPlugin.pl
get_ESXi_Hosts_from_vCenter.pl             shutdown_ESXI.pl
getESXiVersionNumber.pl                    shutdown_ESXI.sh
is_ESXI_in_maintenancemode.pl              shutdown_freeESXi.sh
listESXiLicenses.pl                        shutdown_Vms.pl
maintenancemode_ESXi_direct.pl             verify_hosts.pl
maintenancemode_vcenter.pl                 vsanHostMaintenanceMode.pl
noBlockSendOneHostIntoMaintenanceMode.pl
admin@rccmdAppliance:/opt/rccmd/remoteHostScripts$ _
```

Keep in mind that local installations may differ: Older versions of RCCMD use the directory /usr/rccmd, whereas later versions use /opt/rccmd as directory.

However, you need to adapt the script rccmd_shutdown_sh in both cases. The RCCMD appliance provides the user-friendly editor nano to help doing this configuration work.

Since this script is system-relevant, this configuration can only be carried out as the so-called "SuperUser":

Command: sudo nano rccmd_shutdown_sh

```
admin@rccmdAppliance:/opt/rccmd/remoteHostScripts$ sudo nano rccmd_shutdown.sh
[sudo] password for admin: _
```

Edit the script as followed:

```
 GNU nano 5.4                        rccmd_shutdown.sh
#!/bin/sh

# rccmd_shutdown.sh - This script is called by rccmd after receiving
# the "SHUTDOWN" command from the network.
RCCMD_DIR=/opt/rccmd
SCRIPT_DIR=${RCCMD_DIR}/remoteHostScripts
ESXI_HOST_SHUTDOWN=${SCRIPT_DIR}/shutdown_ESXI.sh
FREE_ESXI_SHUTDOWN=${SCRIPT_DIR}/shutdown_freeESXi.sh

${ESXI_HOST_SHUTDOWN} "$@"              <---  Add # to disable this line
# IMPORTANT: Read instructions contained in shutdown_freeESXi.sh before use!
#${FREE_ESXI_SHUTDOWN} "$@"             <---  Remove # to enable this line

exit $?
```

Press CTRL + X to exit the editor and do not forget to save:

```
Save modified buffer?  (Answering "No" will DISCARD changes.)
 Y Yes
 N No                ^C Cancel
```

Now you can test RCCMD.

RCCMD Appliance Version 4.54.12 231129 onwards: Configuration for Free Hosts

With the version 4.45.12 231129 and later, some basic configuration steps are obsolete. Due to this fact, the complete configuration process is less complex:

Enable the SSH -Console on your ESXi Host.
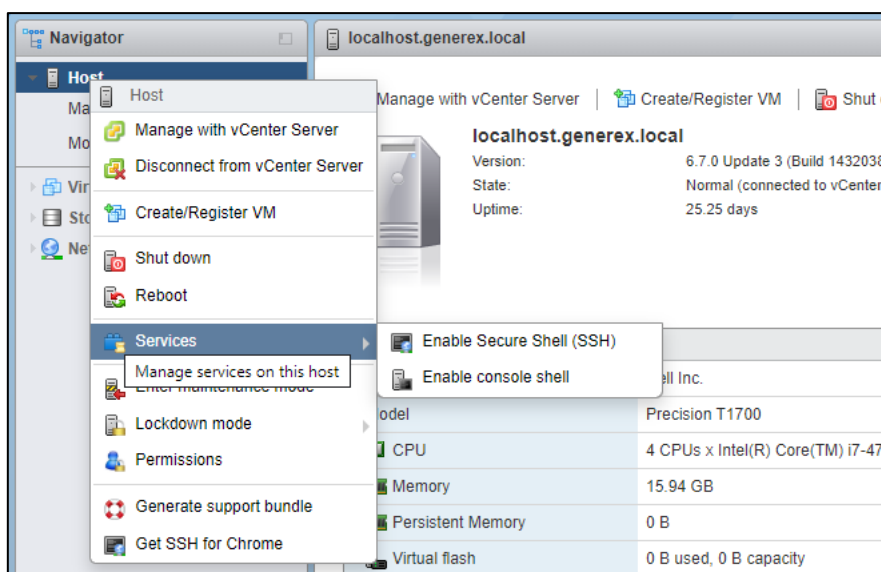
To do this, right-click on the host in the navigator and go to "Enable Secure Shell (SSH)" under Services. If it works, VMware will react with a corresponding message that you should turn the shell off if you do not need it.

Ensure, this is not just a temporary, but a permanent setting:
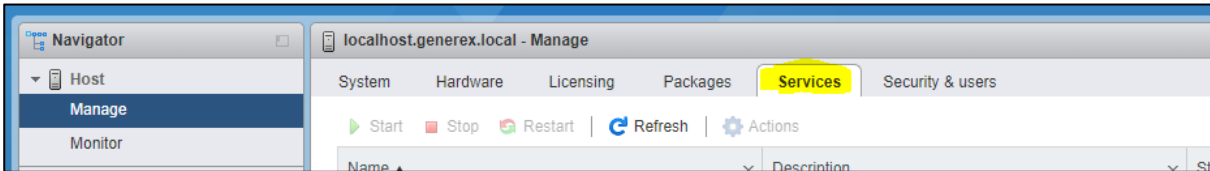
At the Navigator, click on Manage - Open the tab „services". Search for these two entries:

The default setting fort these services is a manual start / stop. As a consequence, the host will not restart this service automatically.
Click with the right mouse button on the TSM service and select from the context menu „Policy"
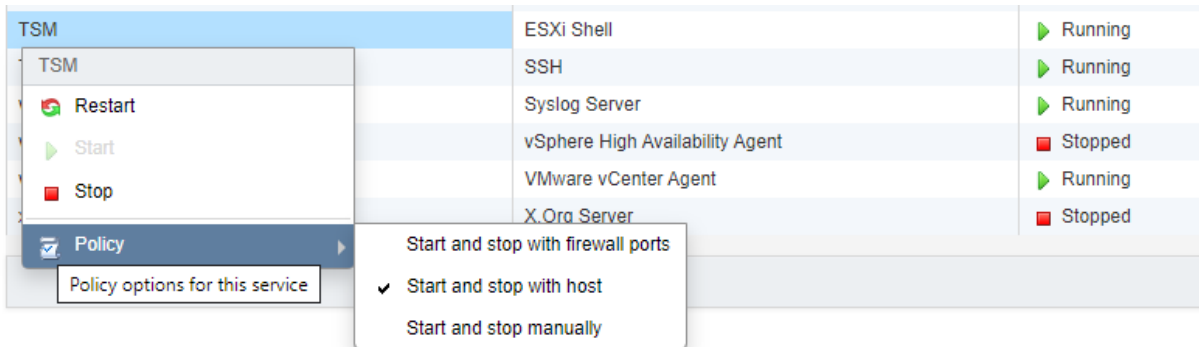
Change the setup to „Start and stop with host". Repeat this setup for the service TSM-SSH:
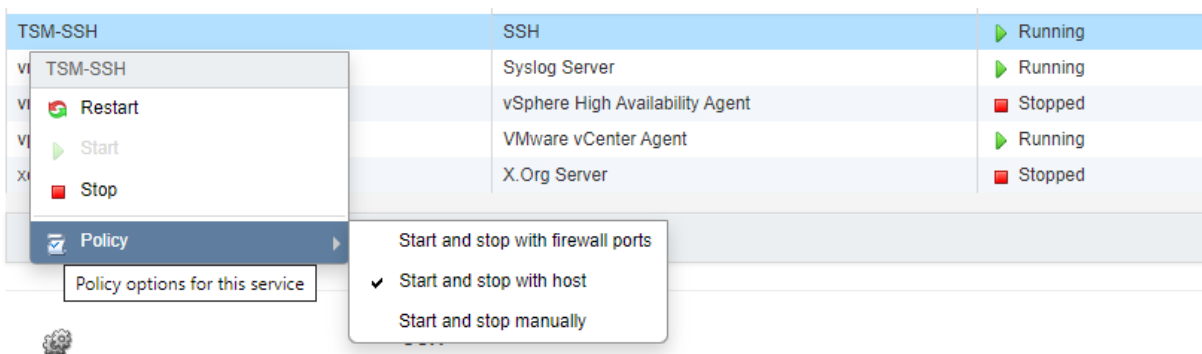
Connect the appliance with the host

You cannot perform this step via the web interface. You need to switch to the console of the RCCMD Appliance. To do this, use an appropriate tool such as the freeware program PuTTY and log in directly to the console of RCCMD.

As an alternative, you may also use the VMware integrated console to carry out this configuration step.

For this tutorial, the default credentials are configured:

User: admin
Password: RCCMD

Enable ESXi Free / Public Host configuration

In the last step, you only need to tell RCCMD that it is a public server (or a Community Edition). To do this, you must adapt the special shutdown script manually.

Log in to the console of the RCCMD appliance with the user "admin" and change to the script directory with the following command and display the content:

Command 1: cd /opt/rccmd/remoteHostScripts/
Command 2: ls

```
admin@rccmdAppliance:~$ cd /opt/rccmd/remoteHostScripts/
admin@rccmdAppliance:/opt/rccmd/remoteHostScripts$ ls
bash_tools.sh                          pltmp.pl
cache_host_dns_names.sh                rccmd_shutdown.sh
checkESXipwd.pl                        registerGXPlugin.sh
checkESXiVersion.pl                    registerPlugin.pl
get_ESXi_Hosts_from_vCenter.pl         shutdown_ESXI.pl
getESXiVersionNumber.pl                shutdown_ESXI.sh
is_ESXI_in_maintenancemode.pl          shutdown_freeESXi.sh
listESXiLicenses.pl                    shutdown_Vms.pl
maintenancemode_ESXi_direct.pl         verify_hosts.pl
maintenancemode_vcenter.pl             vsanHostMaintenanceMode.pl
noBlockSendOneHostIntoMaintenanceMode.pl
admin@rccmdAppliance:/opt/rccmd/remoteHostScripts$
```

The script that you need to edit is called rccmd_shutdown.sh. The RCCMD appliance offers you the user-friendly editor nano, which is already pre-installed. As this script is system-relevant, you can only edit this file as a super user:

Commnand: sudo nano rccmd_shutdown_sh

```
admin@rccmdAppliance:/opt/rccmd/remoteHostScripts$ sudo nano rccmd_shutdown.sh
[sudo] password for admin:
```

Configure the script as follows:

```
 GNU nano 7.2                          rccmd_shutdown.sh *
#!/bin/sh

# rccmd_shutdown.sh - This script is called by rccmd after receiving
# the "SHUTDOWN" command from the network.


# IMPORTANT: Read instructions contained in shutdownFreeESXi.pl before
#setting FREE_ESXI_SHUTDOWN=true!                          Replace "false":
FREE_ESXI_SHUTDOWN=false  <----                            Write "true" instead

RCCMDDIR=/opt/rccmd
RCCMDSHUTDOWNNAME="RCCMDConfig.jar"


RCCMDSHUTDOWN_PROG=$RCCMDDIR/webconfig/$RCCMDSHUTDOWNNAME


RCCMDCONFIG_PROPERTIES=$RCCMDDIR/webconfig/resources/rccmdConfig_lin.properties

JAVADIR=/opt/rccmd/jre/java-linux/bin
```

1. Search for FREE_ESXI_SHUTDOWN=**false**
2. Set it to true: FREE_ESXI_SHUTDOWN=**true**

Type CTRL + X to quit the editor.
Click Y to confirm saving your changes:

```
Save modified buffer?  (Answering "No" will DISCARD changes.)
 Y Yes
 N No              ^C Cancel
```

Please ensure not changing the filename.

RCCMD is ready to run with an RCCMD free host.

Tutorial: BACKUP / UPDATE / RESTORE

A – Procedure up to Version 4.54.12 231129:

An update of RCCMD within the existing appliance is not possible - for an update, a new appliance must be rolled out as as described above.

Backup & Restore

Important for older RCCMD installations:

If you come from an older RCCMD installation and switch to the latest version, please note that the main folders may differ: If there is no /op/rccmd/ (later versions of RCCMD) - directory, the files can be found at /usr/rccmd (older versions of RCCMD).

During the work, make sure that you have obtained the necessary administrative release in advance with the command **sudo su**.

1. Create your backup file
2. Roll out the new Appliance
3. Importing a backup file

Step 1: Copying files as backup:

a. Change to the directory /opt/rccmd
   Save this file:

   o Die Datei „rccmd.cfg"

b. Change to the directory /opt/rccmd/webconfig/resources
   Save these files:

   o rccmdConfig_eclipse.properties
   o ream.properties

c. Save your custom skripts.

Step 2 Continue with installation workn

Roll out the new appliance as described.

Step 3: Restoring the configuration:

The import of the backup is carried out in a similar way to the backup:

a. Copy your own scripts to the according directories. If necessary, overwrite old files.

b. Change to the directory /opt/rccmd

   o Place your saved rccmd.cfg and overwrite the existing file

c. Change to the directory /opt/rccmd/webconfig/resources
   Place the following files from your backup here and overwrite any existing files:

   o rccmdConfig_eclipse.properties
   o realm.properties

d. To activate the data backup, restart RCCMD.
   Check the settings and functions.

B – Procedure from Version 4.54.12 231129 onwards:

Important: former program version backups are not compatible! With program version 4.54.X.231129, an initial RCCMD configuration is mandatory.

Using the web interface for a BACKUP / RESTORE:

    1.   Create a Backup
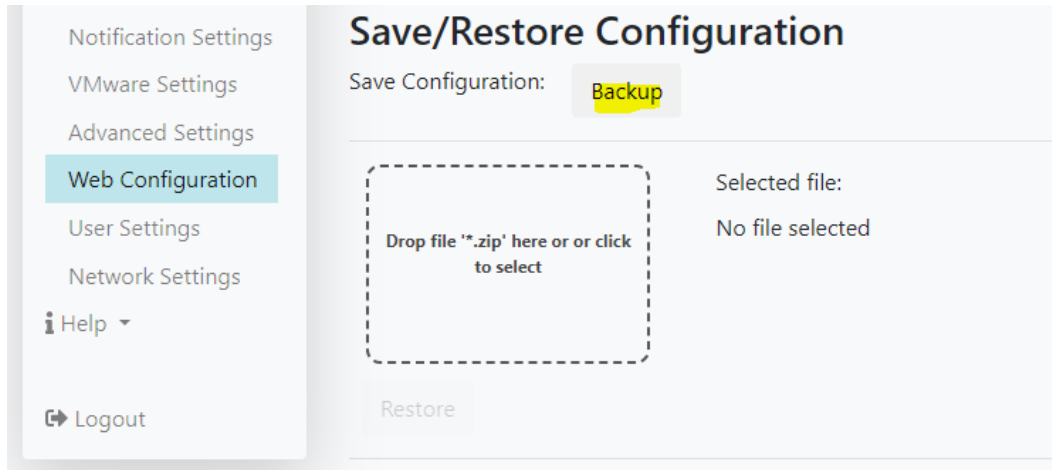
        Open Options> Web Configuration, search for „Save/Restore Configuration" and click on the button „Backup". The RCCMD configuration file will be downloaded as a packed file.

        Remember the IP address of the Appliance.

        After noting the IP address, shut down the existing appliance and turn it off. It is not necessary to delete the virtual machine immediately.

    2.   Roll out a new Appliance.

        Important: To access the web interface, the appliance requires a valid IP address. If this was not assigned during the rollout process or there is no DHCP server available, you must assign the IP address manually using the console.

    3.   Restore the Backup.

        Place the backup file as downloaded in the given box and click Restore.

    4.   Test your Settings.

        Please note that for some features the backup has been tailored to a specific IP address. For example, if you received the IP address via a DHCP server, it may have changed. As a result, a CS141 sends a signal to the "old" IP address, which would render the RCCMD shutdown ineffective.
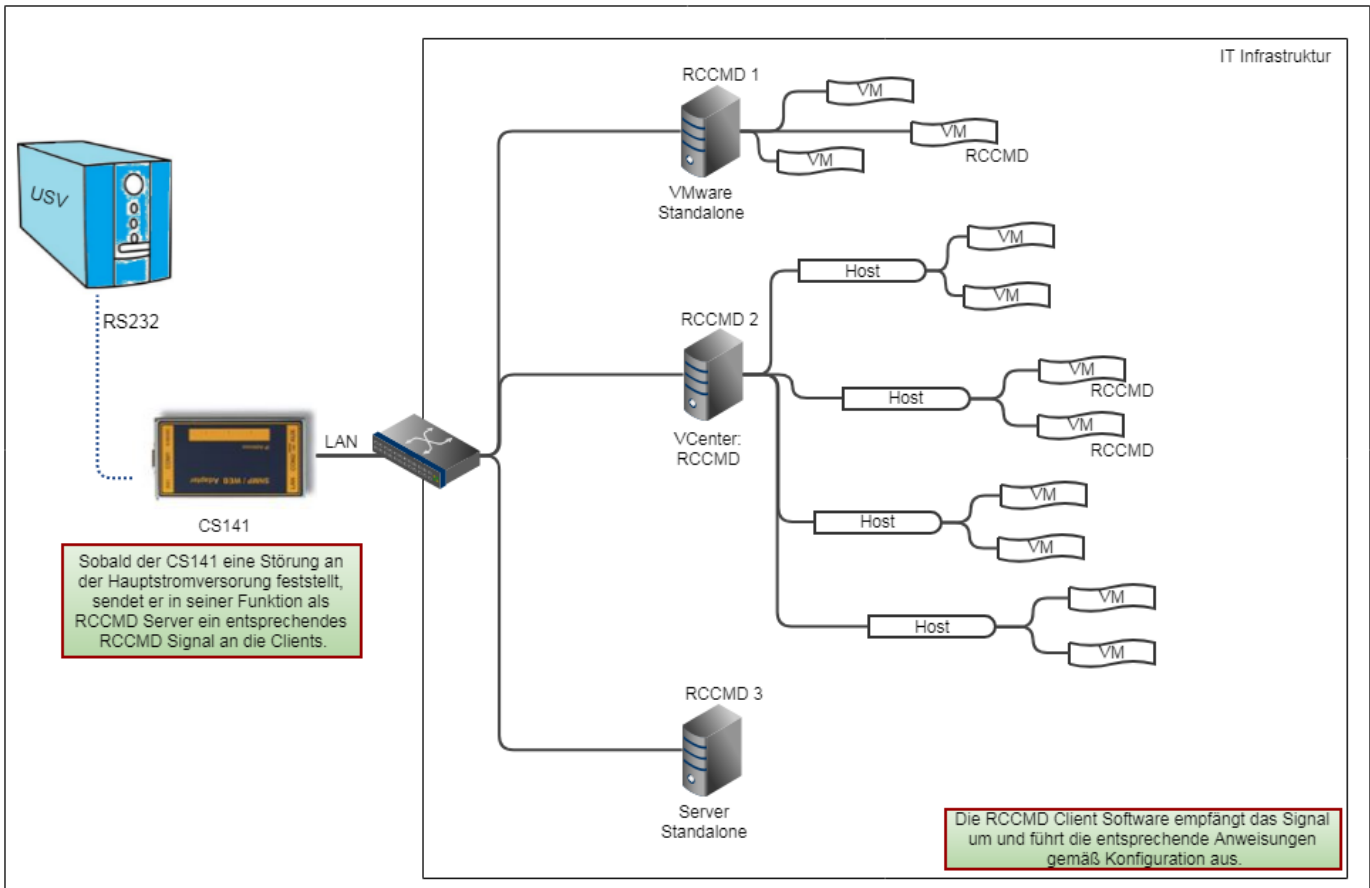
Installation – RCCMD for Microsoft Windows

Installation guide for Windows operating systems

Differences to VMware

How the principles of functionality differ from RCCMD for VMware:

In its function as a valid RCCMD server, the CS141 usually sends control signals to a client, which implements the corresponding commands depending on the configuration. There are two basic possibilities:

1. Both, signal and sending device are valid.
2. The signal itself is correct and valid, but the sending devices is not listed.

The difference between VMware, Hyper-V and a single server becomes more apparent when looking in detail:

With VMware, different virtual machines normally run on one physical host. When the RCCMD appliance is in use, RCCMD does not communicate with the virtual machines, but only with the physical host itself. Both, the number of virtual machines and hosts are irrelevant:

As soon as the IP address is known, the RCCMD appliance can communicate with the according host. Due to this fact, the RCCMD appliance can be configured to contact as many hosts as wanted - independent to its own host. If you can roll out an OVA file, you will be able to run the appliance. Furthermore, the virtual machines are not touched by the RCCMD appliance. In this context, shutting down or moving is a matter between the host and, if applicable, the vCenter.

Windows based operating systems and HYPER-V differ:

You have a Windows operating system on which you can run virtual machines with Hyper-V. When the Windows operating system is shut down, Hyper-V takes over the coordination of moving and shutting down individual virtual machines. Since RCCMD is not a virtual machine, but a running program, you move at the level of the local administrator as known from a standalone system:

machines. When the Windows operating system is shut down, Hyper-V takes over the coordination of moving and shutting down individual virtual machines. Since RCCMD is not a virtual machine, but a running program, you move at the level of the local administrator as known from a standalone system:

It is possible to run jobs and trigger local scripts to automate everything on the server itself. With a Hyper-V cluster, RCCMD shut down the local Windows Computer, and Hyper-V will take care of the whereabouts of the virtual machines. This eliminates some menus that are important for VMware and replaces them with other menu items that are only possible with standalone servers. As a consequence, you need for each single server an RCCMD client.

Installation: Windows with GUI

First, unpack the file completely (do not confuse it with the preview of Windows) and change to the unpacked directory. To start the installation, run rccmdinstaller.exe:
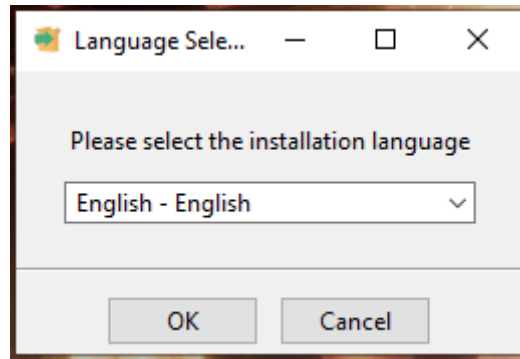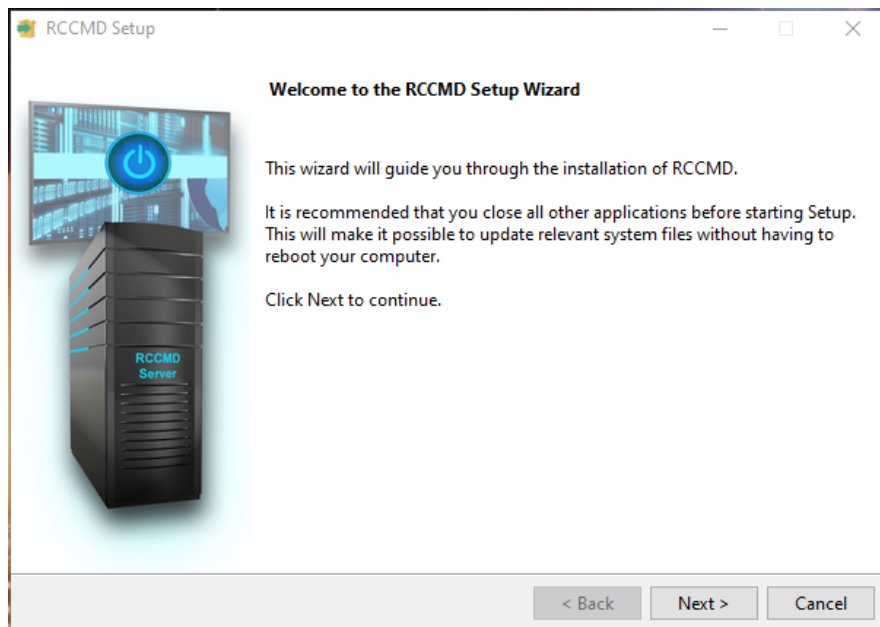

First select the language in which you want to carry out the installation. Please note that this language selection has no influence on the RCCMD client itself - you can adjust it later when configuring RCCMD.

After choosing your preferred installation language, click on OK to start the installation.

The installation dialogs

The installation dialog is straight and guides you through the complete installation process. When ready to begin, click „Next "

Note
The installation is divided into two parts. During the first part, RCCMD asks you to enter parameter. When the installation is aborted, the installation dialog quits and withdraw your choices. Part two is the installation itself – On your mark, RCCMD will start the installation as configured.

**Step 1: Copyrights, terms of usage
and license information**

In this step, you may read our boring warranty conditions, copyrights and terms of use or, alternatively, simply accept them without reading... . If you do not agree, the installation process is terminated without any changes to your system. Remember these iconic words: Resistance is futile.

✓ ***Accept the agreements and click „Next "***
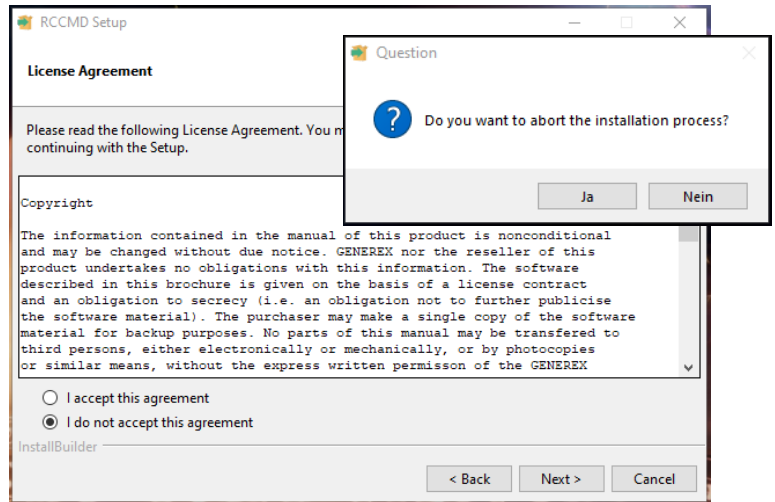
Step 2: Enter the license key

The RCCMD license key is either enclosed with your CS141 or you have received an email with a valid key from your local dealer. Enter the license key and click on "Next" - The installer automatically checks the validity and informs in case of an issue.

If you do not have a license key at hand, leave the field empty and click directly on "Next", RCCMD will automatically use an internal 30-day evaluation key.
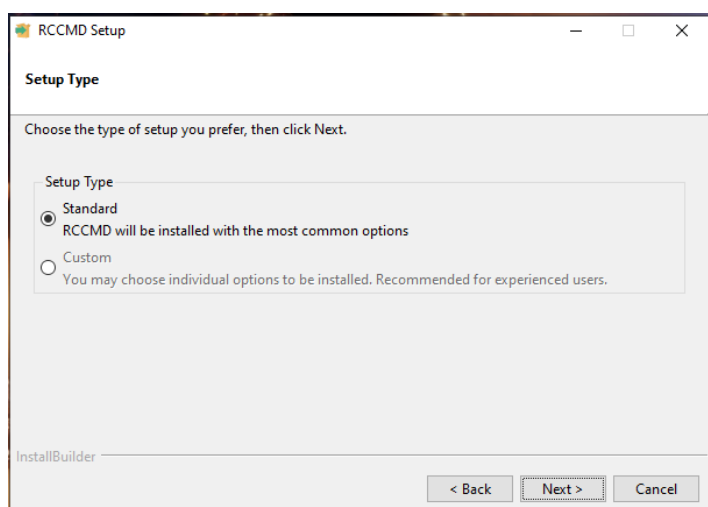
When finished, click "Next. "
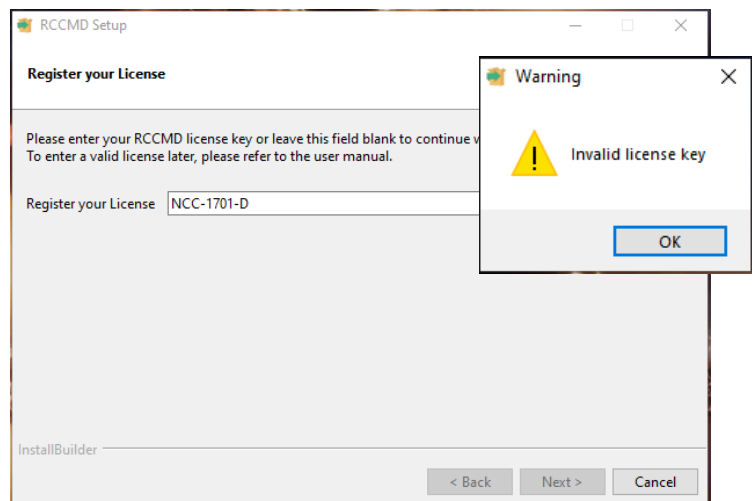
Step 3: Choose your setup type.

The standard installation uses default installation paths and a comes with a recommended installation for modules and ports.

The Custom Installation is aimed at experienced users and system integrators who want to adapt general RCCMD functions like installation path or port settings to the target system during installation.

When finished, click "Next".

### Step 4 – If Standard installation is selected

Installation summary

The setup dialog presents an overview of the installation work to be carried out. If all settings are OK, press „Next" to start the installation.

To review and change settings, press "Back" and select "Custom".

Press "Cancel" to exit the installation dialogue, no changes will be made to your system

Click „Back "to change your settings

Click „Next ", to start the installation process
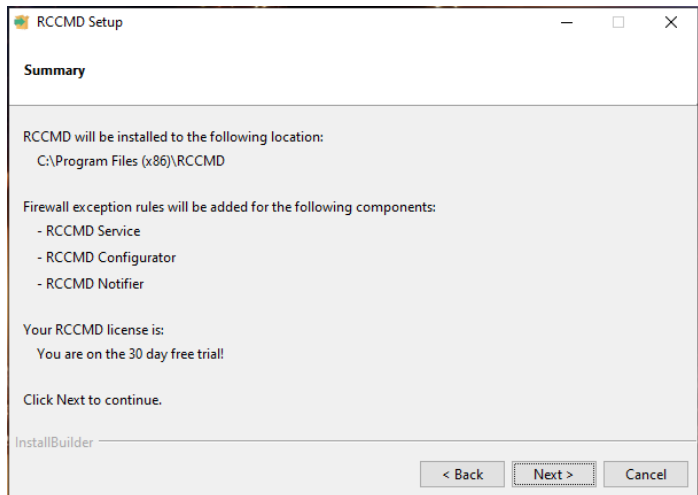
Proceed to Step 5 – Finalizing your installation

Step 3a – Custom installation

Define the installation path

The installation path determines where RCCMD can be found after installation. Usually, RCCMD uses the standard path for programs within Windows operating systems.

In case of custom program paths, the configuration dialogue provides to specify the new path directly. Please note: If configured, changing the installation path may run into problems with system right management

For the graphical file manager, click on the folder symbol next to the input field.

When finished, click „Next "to proceed
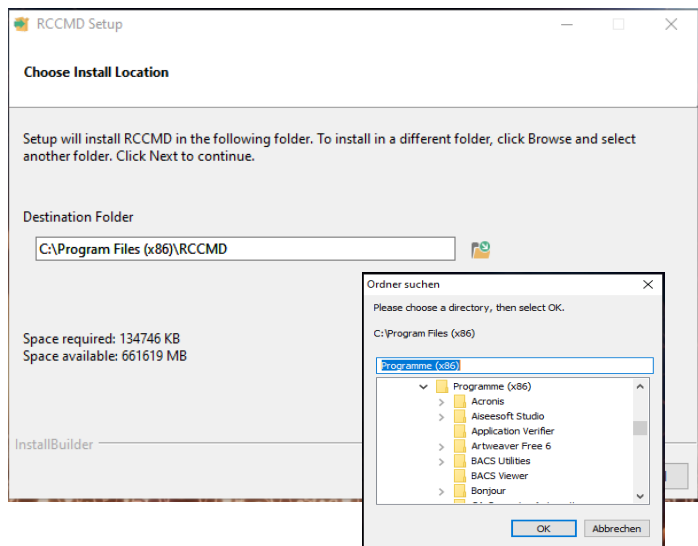
Step 3b – Custom installation

Program icons

The program icons are quick starters with which functions of RCCMD can be reached directly from the desktop.

If an administrator connects to the corresponding computer remotely at a later time, he may comfortably configure RCCMD locally with the quick-start icons.

If you do not want to have program icons, just uncheck.

Please make your choice and click „Next "
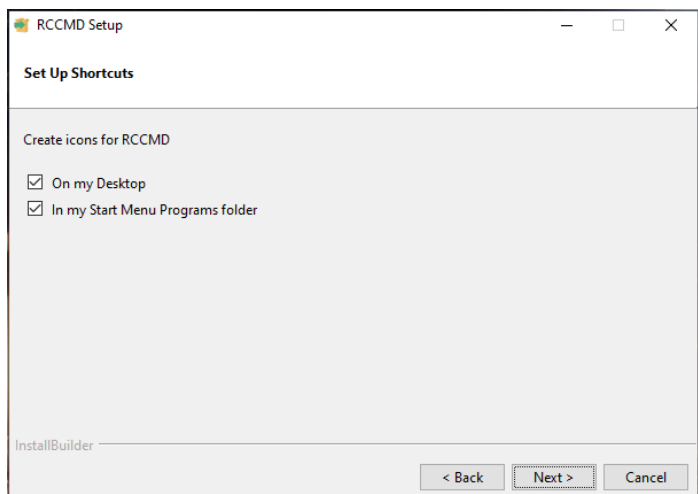
Step 3c – Custom installation

Select system modules

RCCMD consists of several modules that depend on each other.

RCCMD service: The central background process that manages your emergency shutdown. This module is mandatory for operation.

RCCMD Configurator: This module is the web-based configuration dialogue for RCCMD. The RCCMD service may work without the configurator, but since it will harm the configuration work, we recommend to install it.

RCCMD Notifier: The notifier allows a popup with RCCMD messages. Furthermore, RCCMD background processes can be executed interactively with the current user. This module can be very helpful when using your own scripts.

Select your modules and click „Next"

Step 3d – Custom installation

HTTP / HTTPS and Web Console Password

By default, RCCMD uses HTTPS for its web interface. An integrated certificate is available for this purpose. With this setting, define whether HTTP or HTTPS is to be used as standard.

TCP/Port: RCCMD does not respond to every port on requests to the web interface. The default port is 8443. If you want to use a different port, please specify.

Password: Set the password for the RCCMD web interface log in. If you want to set the password later, leave the field as it is. RCCMD will then use the standard password "RCCMD".

**After configuration, click „Next "**

Step 3e – Custom installation

Configuration Overview

The Summary shows your installation configuration. If some changes are needed, select "Back" until you reach the according configuration step.

„Next "will start the final installation process.

Cancel closes the installation dialogue and discards the parameters you have set without performing any changes to the operating system. On Restart, you need to enter all parameters again.

The configuration work is done, click „Next "to start the installation.
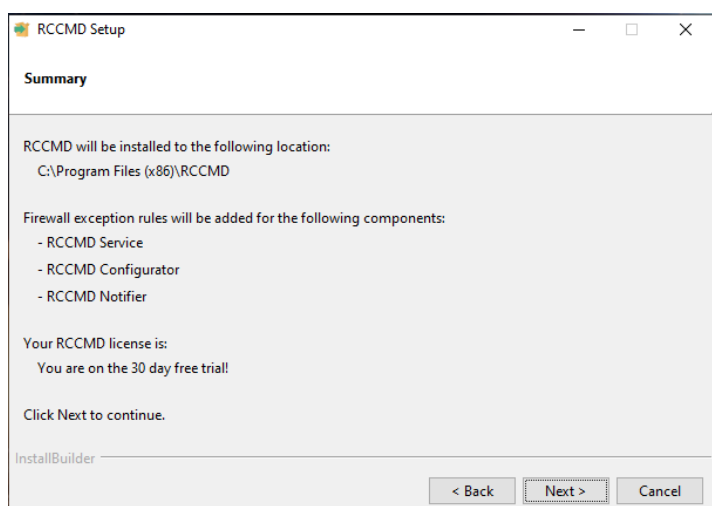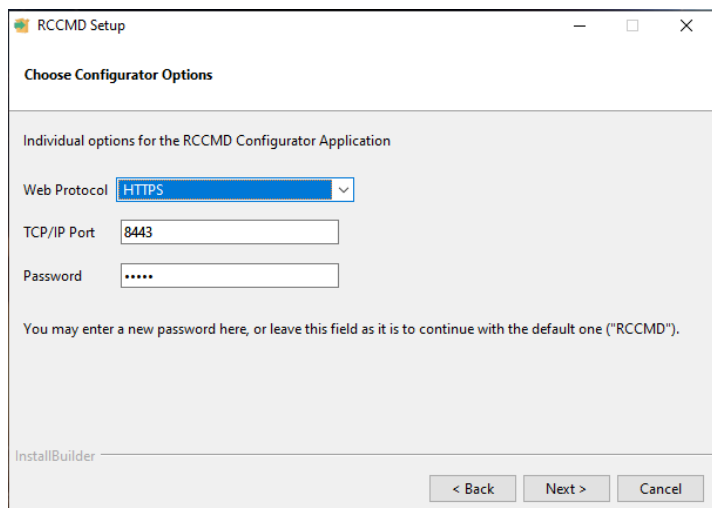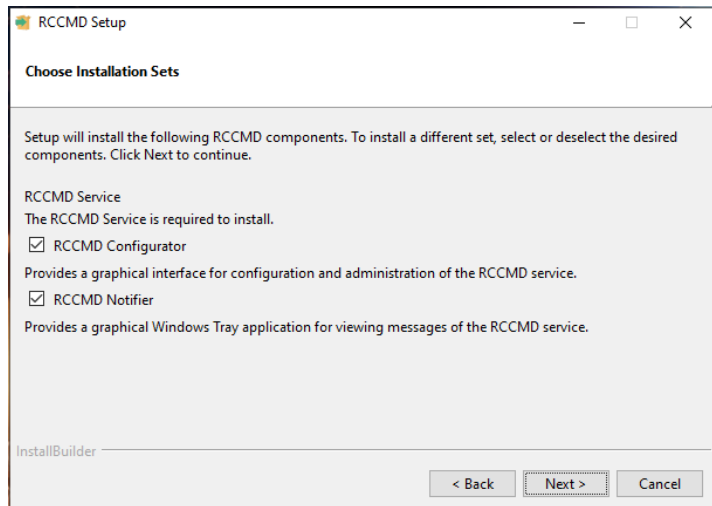
Step 5 – Finalizing your installation
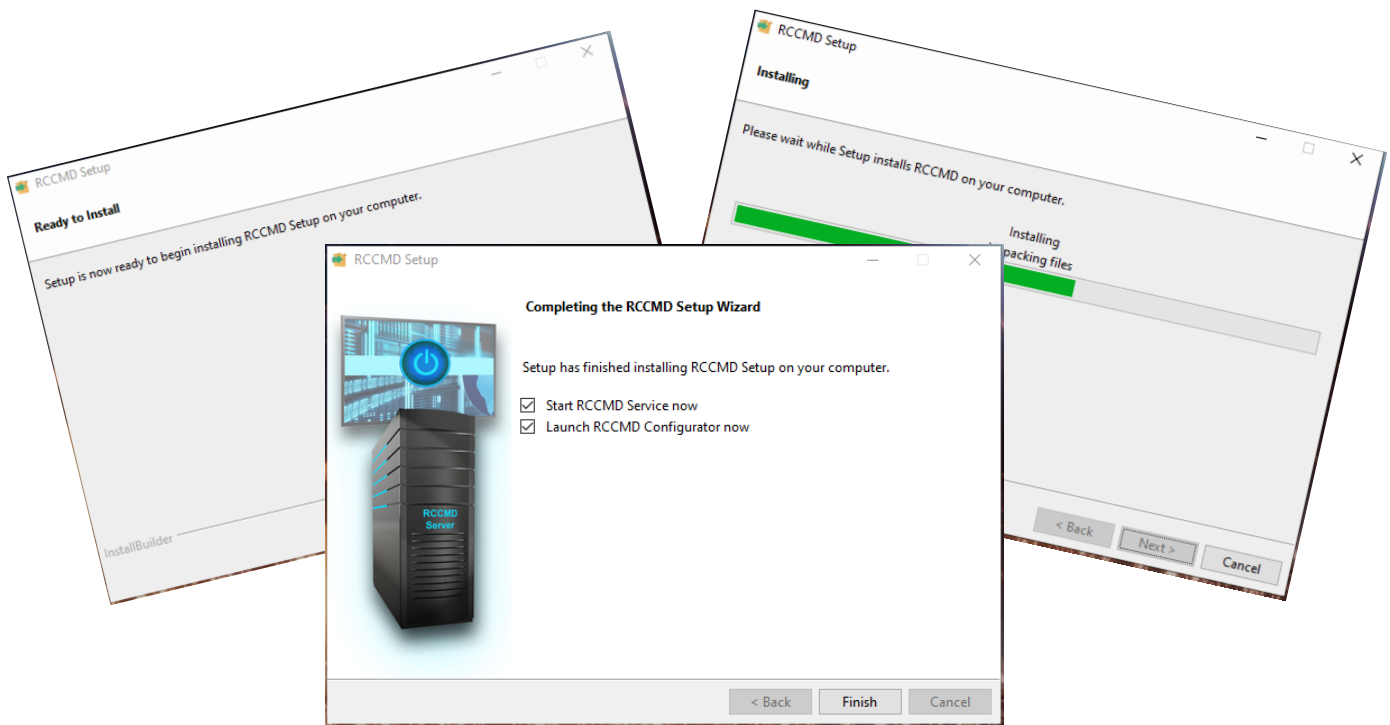
RCCMD automatically installs and configures all selected components. Afterwards configuration work can be done via the web interface by entering the IP address of the computer:

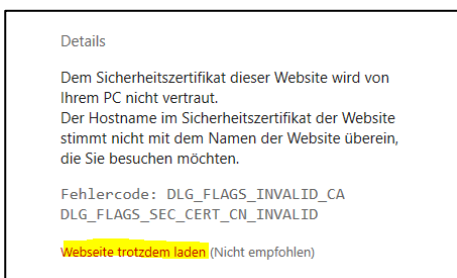How to access the interface via web browser:

- https://127.0.0.1:8443 ,
- https://[IP-address of the target computer]:8443,
- https://localhost:8443

Password: RCCMD or your selected password.

The graphical installation of RCCMD is now completed. Please continue with the configuration of RCCMD via the web menu.

Note:

On first visit you may encounter a "certificate error":

The reason for this behaviour depends on the nature of a certificate: The certificate itself is valid, but RCCMD was of course installed on a server for whose hardware the SSL certificate cannot logically be signed. The web browser notices this and consequently indicates that there might be a faked server.

With Edge, click on "Details", with Crome on "Advanced Options" to get to the RCCMD login page.

The graphical installation is done, please proceed to the Quick Configuration Guide

RCCMD Quick Configuration: Windows, Linux and MAC OS

Installation via console

```
C:\Users\gunnar\Downloads\rccmdcd\rccmdcd>rccmdinstaller.exe
```

```
Select your preferred installation language
[1] English - English
[2] German - Deutsch
Please choose an option [1] : 2
```
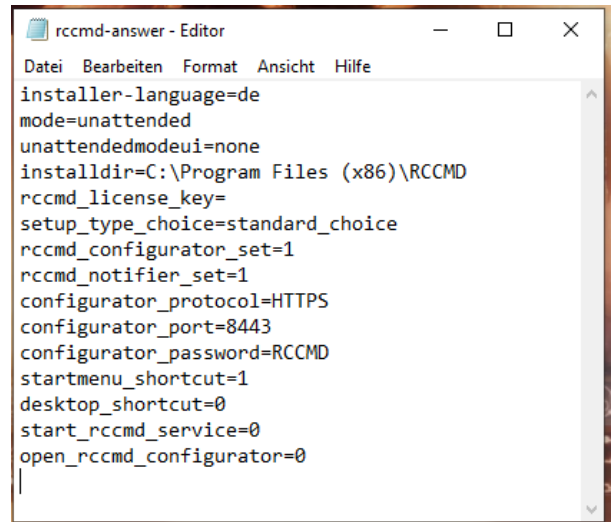
Core servers or operating systems via console access do not offer a GUI - The RCCMD installer automatically and offers an alternative text mode for the configuration menus. The setup program will guide you through the installation process in exactly the same way as with the graphical installation.

Silent Install with an options file

The „Silent Install" is a special mode in which all parameters required for the installation are stored in a central response file.

How to create a Silent Install file

Open a text editor and save the file e.g., as rccmd-answer.txt. The structure of the file is without special characters or special format symbols.

```
rccmd-answer - Editor
Datei  Bearbeiten  Format  Ansicht  Hilfe
installer-language=de
mode=unattended
unattendedmodeui=none
installdir=C:\Program Files (x86)\RCCMD
rccmd_license_key=
setup_type_choice=standard_choice
rccmd_configurator_set=1
rccmd_notifier_set=1
configurator_protocol=HTTPS
configurator_port=8443
configurator_password=RCCMD
startmenu_shortcut=1
desktop_shortcut=0
start_rccmd_service=0
open_rccmd_configurator=0
```

For a complete silent install, we recommend the following settings

installer-language=de/en	Define the installer language
mode=unattended	Set the installation mode to silent install.
unattendedmodeui=none	Deny interactive questions
installdir=C:\Program Files (x86)\RCCMD	Select the installation path
rccmd_license_key=	The RCCMD key for this installation. If you do not have a key for the moment, leave the field empty. RCCMD will then be installed with an evaluation key.
setup_type_choice=standard_choice	Choose "Standard" for the module setup
rccmd_configurator_set=1	Install the configuration interface*
rccmd_notifier_set=1	Installs the messeging service for RCCMD*
configurator_protocol=HTTPS	Define the standard access protocol
configurator_port=8443	Choose the access port for RCCMD
configurator_password=RCCMD	Enter the default password for the web interface
startmenu_shortcut=1	Do you need a start menu short cut?*
desktop_shortcut=0	Do you need desktop short cuts? *
start_rccmd_service=0	Shall the RCCMD service start directly after installation without configuration? *
open_rccmd_configurator=0	Shall the web configurator start directly after installation? * If your operating system does not provide a GUI, you may dismiss this step*

* 1 = YES / 0= NO

➔ **Command to start the silent installation: rccmdinstaller.exe --option file rccmd-answer.txt**

The installation will be done as a background process. After installation, visit the web interface to configure the RCCMD client.

How to access the interface via web browser:

- https://127.0.0.1:8443 ,
- https://[IP-address of the target computer]:8443,
- https://localhost:8443

Password: RCCMD or your selected password.

Der Schnellstart von RCCMD endet an dieser Stelle. Weiterführende Informationen und was man sonst noch Konfigurieren kann, können Sie weiter unten im Handbuch entnehmen – die Screens werden dort im Detail noch einmal erklärt.

Installation - RCCMD for Linux

Installation guide for Linux based operating systems
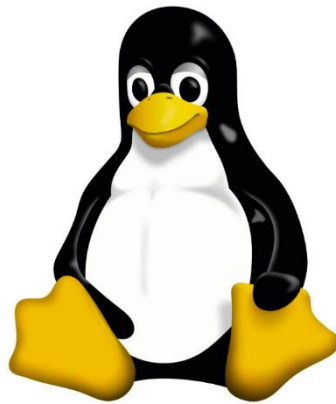
Installation under Linux with GUI

In this case, we have chosen a Linux Mint "Ulaya 64 Bit" with the Cinnamon GUI. Please note that other distributions, derivatives and GUIs may differ. Please refer to the according user's manual or your operating system.

Download and unpacking the software

After downloading your copy of RCCMD, you need to unpack the file before installation is possible.

Please ensure that the files are and it is not just a preview of the packed files. The installation will not work with packed files.
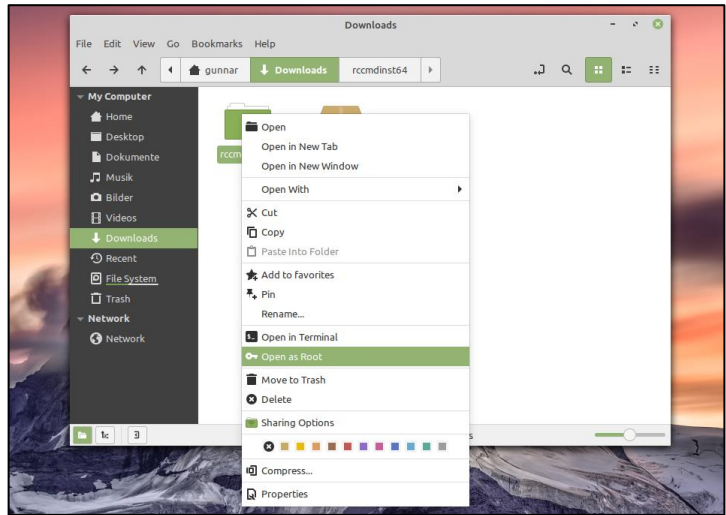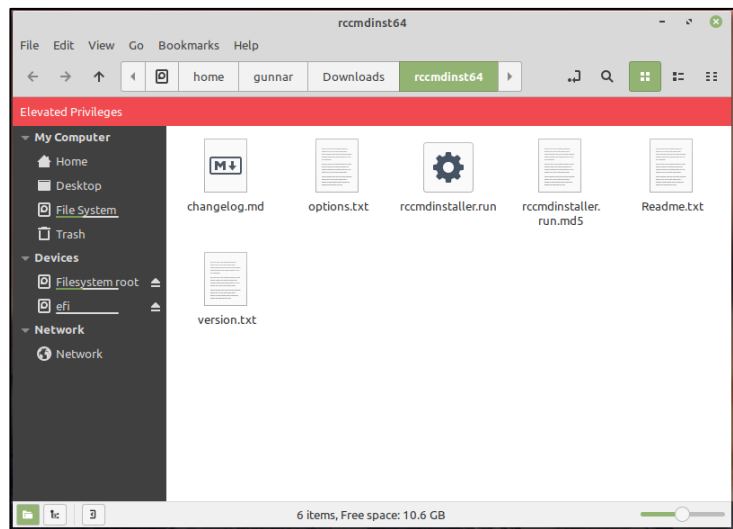

Installing RCCMD

For the installation, elevated system rights are necessary. To get elevated system rights, open the unpacked folder as system administrator.
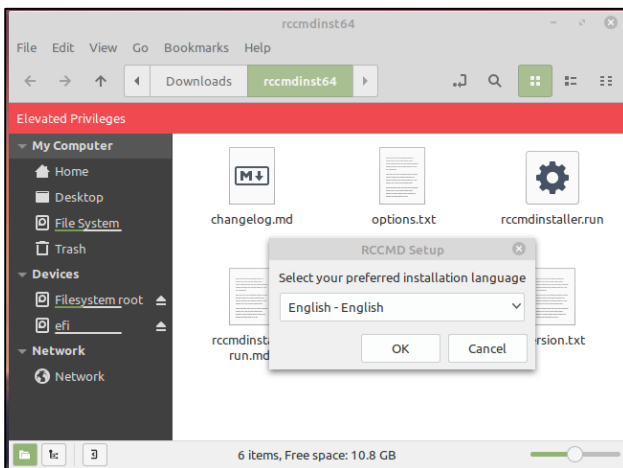
Once opened the directory correctly, there is a note that you are working within the directory with elevated rights.

With a double-click on installer.run, the installation process will start.

The installation screen overview:

Run the file „rccmdinstaller.run "with a double-click.

Select language…   … Click "Forward"

The license agreement:

We know that nobody really reads a licence agreement, but we have nevertheless included it here. In order to use the RCCMD software, it is necessary to confirm the licence agreement. Due to this fact, we recommend to read it carefully before accepting…

If you do not agree, the installer will exit and no changes will be made to your operating system.t.
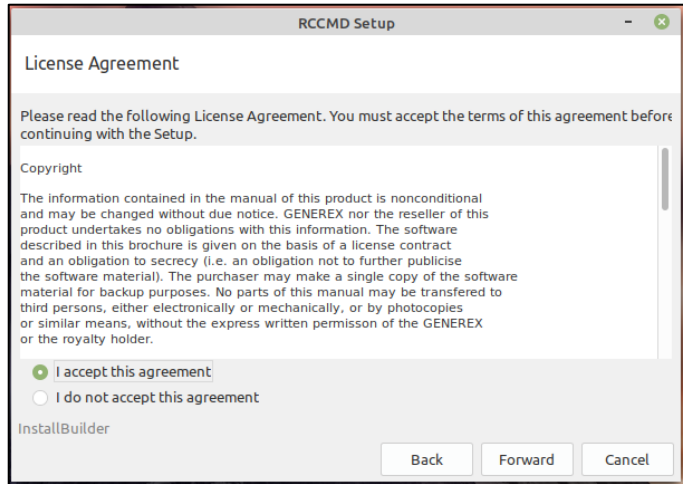

The License Key

Please enter the licence key you bought with your copy of RCCMD. If you do not have a key to hand, leave the field blank - RCCMD will then automatically use a 31-day evaluation key, after which the client will deactivate itself until a valid licence is entered. The operating system is not affected by this. Please note that you can use as many RCCMD clients in your network as you like, but each licence key can only be used once.

As soon as a client is started with the key, the following client will terminate its service with the message "Licence Fraud".

Only the so-called Corporate Key is valid for a certain number of clients and can therefore be entered several times. For more information about the corporate key, please contact your local dealer. If you want to reuse a key, simply uninstall the corresponding RCCMD installation that is no longer needed.

Note: You can change the licence key at any time via the Advanced Settings in the RCCMD configuration menu.
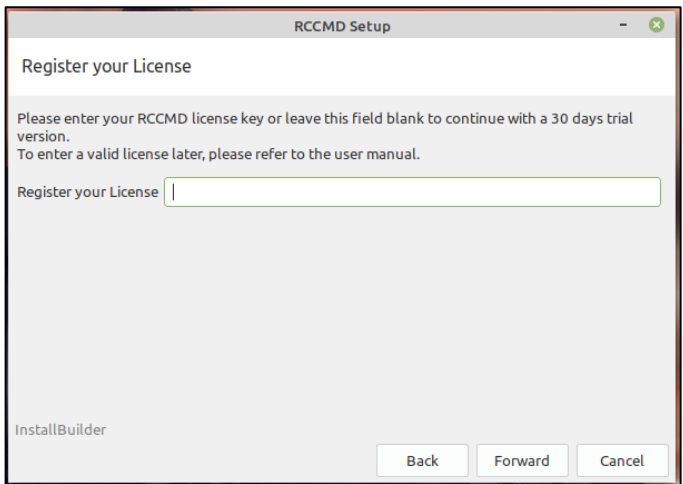
Setup Types
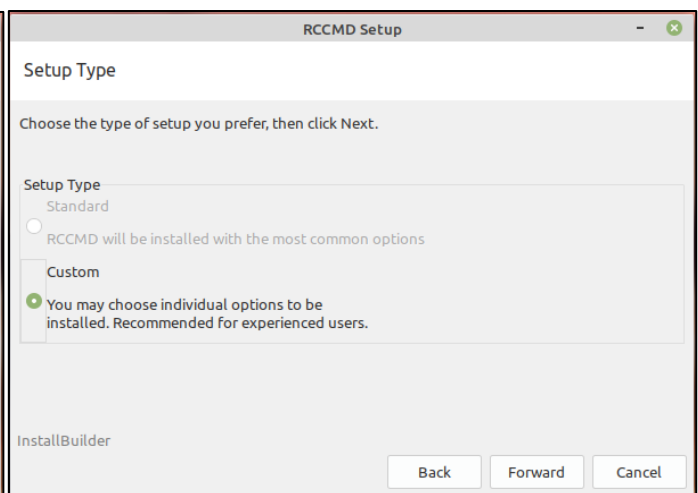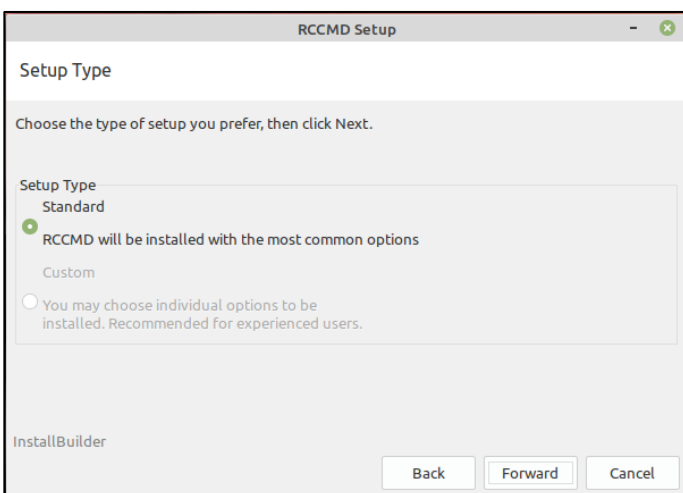
Choose the installation type. There are two basic ways to carry out the installation.:

Standard installation

The standard installation will be carried out with a default configuration that holds all recommended basic settings for your RCCMD software.
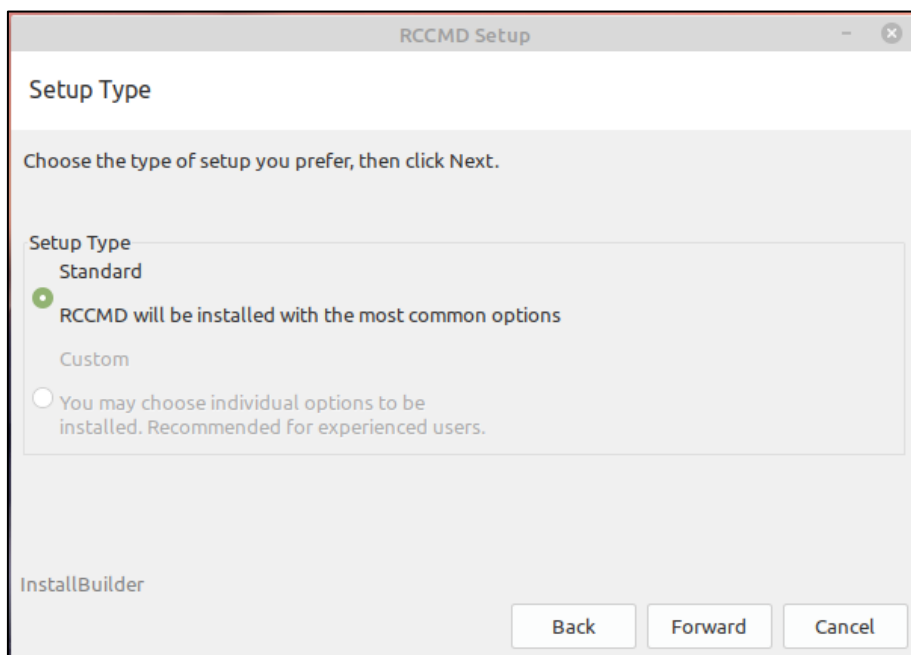
For post-installation configuration, the following settings are pre-defined:

https://127.0.0.1:8443	The Local Host: The RCCMD web configurator will serve your access attempt.
https:// [IP address of the computers]:8443	The web interface can also be opened by any computer that is within the same network segment or reachable network
Default password:	RCCMD

Custom installation

this installation type offers an installation dialogue to adjust the installation more precisely. Please note that the changed parameters may require additional administrative adjustments in the operating system. This type of installation is therefore only recommended for experienced users

RCCMD offers options as followed:

Destination Folder

The default installation will be carried out at /opt/rccmd.

If needed, please adapt the destination path.

 For a graphical file browser, click thin icon.

Adapt the modules

The RCCMD service is mandatory for the operation of RCCMD, therefore it cannot be selected or deselected.

The RCCMD Configurator provides a web interface through which all necessary settings can be done after the installation. The web interface can be reached under the following addresses:
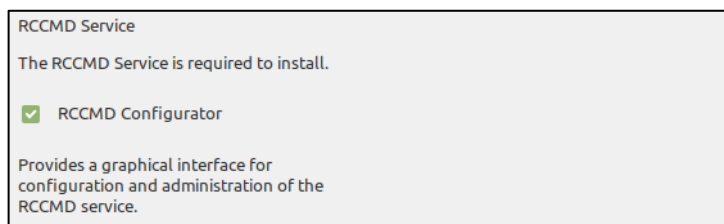
https://127.0.0.1:8443	The Local Host: The RCCMD web configurator will serve your access attempt.
https:// [IP address of the computers]:8443	The web interface can also be opened by any computer that is within the same network segment or reachable network

RCCMD Messaging Outputs

By default, all messages that RCCMD receives and wants to pass on will be directed to the console.

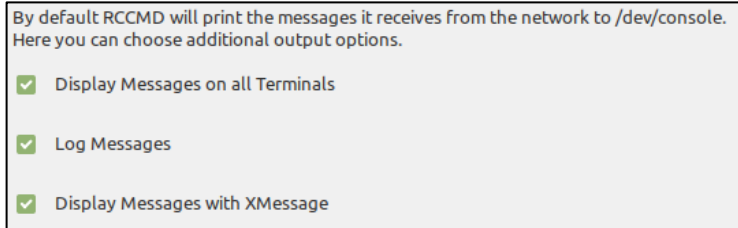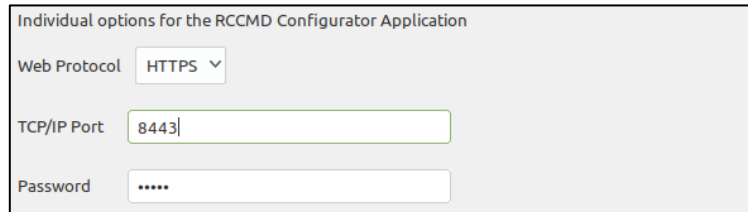With these settings, an additional alarm behaviour can be configured:

1. Display on all terminals: The message is displayed on all open terminals.
2. Log messages: The messages are logged
3. Display messages with XMessage:
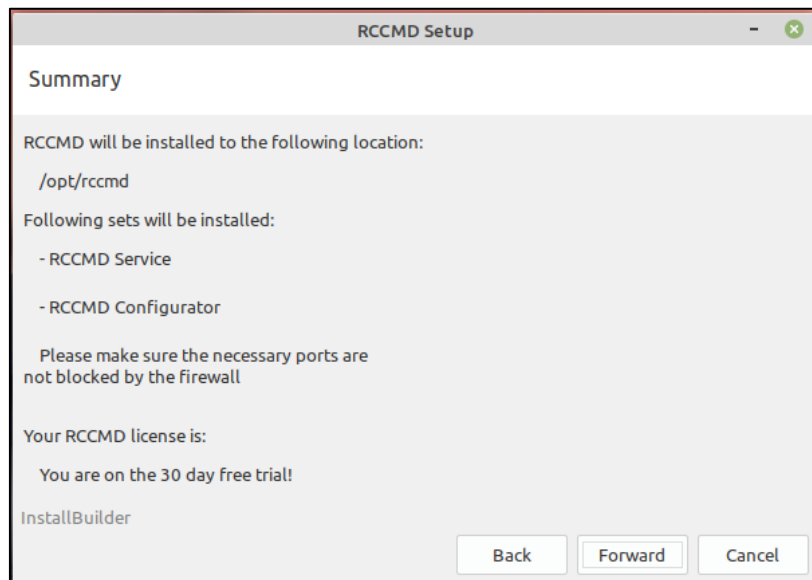   In case of a GUI, a popup-window appears to show RCCMD messages.

By default RCCMD will print the messages it receives from the network to /dev/console. Here you can choose additional output options.

☑ Display Messages on all Terminals

☑ Log Messages

☑ Display Messages with XMessage

Configure the Web Interface of RCCMD

By default, the web interface of RCCMD is addressed with https and TCP/Port 8443. Edit the settings accordingly to adapt the RCCMD to fit to your network infrastructure. The default password is generally RCCMD. You can adapt it to your needs at a later time via the web interface.

Individual options for the RCCMD Configurator Application

Web Protocol [HTTPS ⌄]

TCP/IP Port [8443]

Password [•••••]

Installation Summary

RCCMD Setup – ⊗

Summary

RCCMD will be installed to the following location:

/opt/rccmd

Following sets will be installed:

- RCCMD Service

- RCCMD Configurator

  Please make sure the necessary ports are not blocked by the firewall

Your RCCMD license is:

You are on the 30 day free trial!

InstallBuilder

[Back] [Forward] [Cancel]
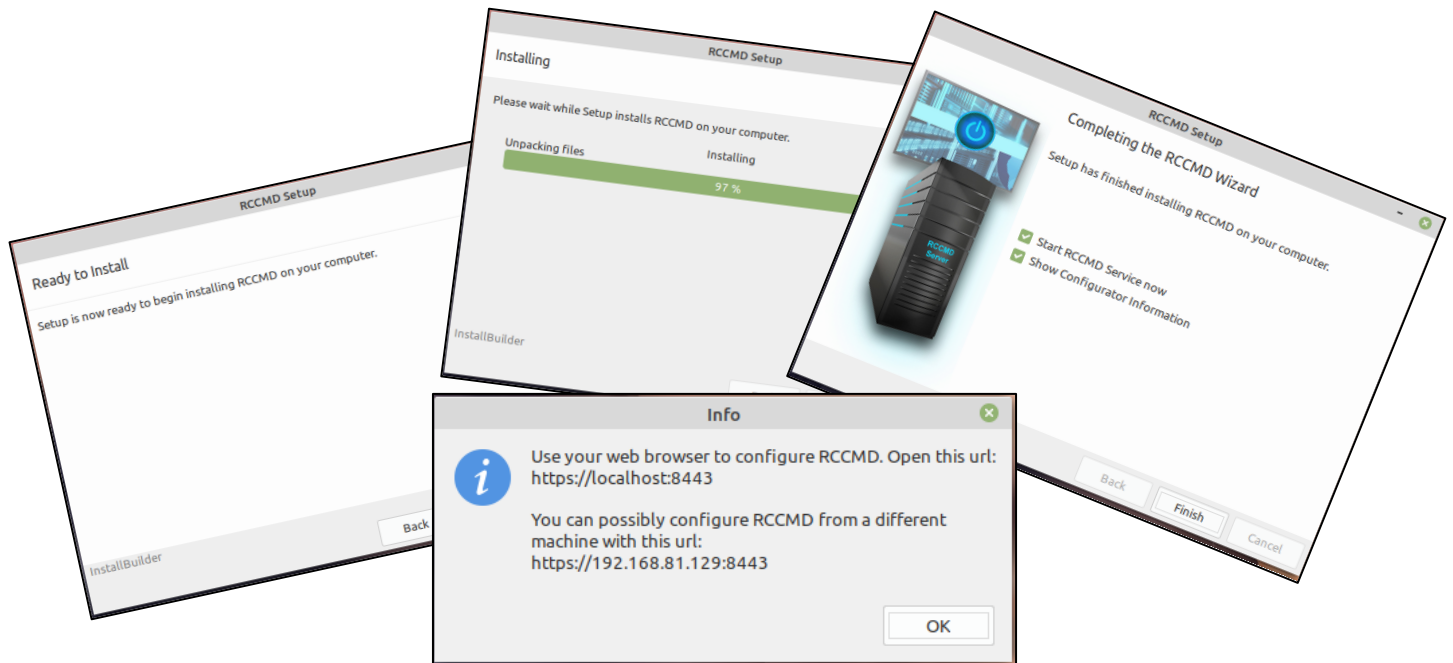
Depending on whether you have selected the standard installation or the manual installation, you can once again clearly display your selection here. Up to this point, RCCCMD has not yet carried out any installation work.

Linux: Finalizing the installation

RCCMD automatically installs and configures all necessary components. Afterwards, you can access the web interface by entering the IP address of the computer:

How to access the web interface:

- https://127.0.0.1:8443,
- https:// [IP address of the computer]:8443,
- https://localhost:8443

Password: RCCMD or your selected password.

The graphical installation of RCCMD is now completed. Please continue with the configuration of RCCMD via the web menu.

Console installation

Basically, the console installation needs the same configuration steps as with the graphical installer.

The following installation example shows the installation on a Linux Mint 20.1 "Ulyssa". Please note that the exact installation commands may differ with your Linux version.

After logon and downloading RCCMD, change to the according download directory and first unpack the file rccmd64.tar.

```
Linux Mint 20.1 Ulyssa linuxmint-64Bit tty2

linuxmint-64Bit login: gunnar
Password:
Last login: Thu Apr 22 12:25:18 CEST 2021 on tty2
gunnar@linuxmint-64Bit:~$ cd Downloads
gunnar@linuxmint-64Bit:~/Downloads$ dir
rccmdinst64   rccmdinst64.tar
gunnar@linuxmint-64Bit:~/Downloads$
```

Then change to the newly created directory with the unpacked installation files.

Expand system rights

Since system-relevant changes must be done during installation that are reserved for a system administrator, expanded system rights are required:

Command: sudo su

With the command sudo su necessary increased system rights can be obtained until revoking with the command "exit". As a result, this is recognizable by the fact that the username is preceded by "root@".

```
Linux Mint 20.1 Ulyssa linuxmint-64Bit tty2

linuxmint-64Bit login: gunnar
Password:
Last login: Thu Apr 22 12:25:18 CEST 2021 on tty2
gunnar@linuxmint-64Bit:~$ cd Downloads
gunnar@linuxmint-64Bit:~/Downloads$ dir
rccmdinst64   rccmdinst64.tar
gunnar@linuxmint-64Bit:~/Downloads$ cd rccmdinst64
gunnar@linuxmint-64Bit:~/Downloads/rccmdinst64$ sudo su
[sudo] Passwort für gunnar:
root@linuxmint-64Bit:/home/gunnar/Downloads/rccmdinst64#
```

This completes the preparatory work and you can start the installation dialogue.

The installation dialogues

In this mode, the installer offers an interactive setup that guides you comfortably through the installation process. The setup is called up via ./rccmdinstaller.run.

Command: ./rccmdinstaller.run

```
root@linuxmint-64Bit:/home/gunnar/Downloads/rccmdinst64# ./rccmdinstaller.run
RCCMD Setup
```

Language selection

The language selection defines the language the installer should use. You can select another language later within RCCMD. Select your preferred installation language.

```
Select your preferred installation language
[1] English - English
[2] German - Deutsch
Please choose an option [1] : 1
```

Copyrights, terms of use and license

```
--------------------------------------------------------------------
This wizard will guide you through the installation of RCCMD.

It is recommended that you close all other applications before starting Setup.
This will make it possible to update relevant system files without having to
reboot your computer.

Click Next to continue.

--------------------------------------------------------------------
Please read the following License Agreement. You must accept the terms of this
agreement before continuing with the Setup.

Press [Enter] to continue:
```

While we do not believe that anyone has ever enough time to read this licence agreement, in order to use the RCCMD software it is necessary to accept the terms of use and license agreements. So, contrary to the recommendation to read carefully, press the enter key until you can accept the terms of use document directly.:

```
function of our software. No warranty to correct functions of the software with
the operating systems, loss of data or interruption of work processes, other
UPS problems or to other errors that may occur out of this combination.

Press [Enter] to continue:

 [y/n]: y_
```

If you do not agree, the installer will exit and no changes will be made to your operating system and the installation dialogue will close.

If you agree, press „y "and confirm with ENTER your decision.

The text-based installer:

Part1: The key

Enter the license key of your RCCMD software here. You can obtain the license key for a fee from your UPS provider. If you have purchased a CS141 Web manager with your UPS, a license is already included.

If you do not have the key at hand, leave this field empty, RCCMD will automatically use an evaluation key. You can change the key later in the configuration menu of RCCMD and thus activate your copy permanently.

```
--------------------------------------------------------------------
Please enter your RCCMD license key or leave this field blank to continue with a
30 days trial version.
To enter a valid license later, please refer to the user manual.

Register your License []:
```

Part 2: The Setup-Type

The setup type defines how many changes can be done during installation.

```
Setup Type

[1] RCCMD will be installed with the most common options: Standard
[2] You may choose individual options to be installed. Recommended for experienced users.: Custom
Please choose an option [1] :
```

In general, there are two different setup styles:

1. Recommended settings
    RCCMD selects the required components for you in order to grant error-free configuration and operation

2. Custom installation
    In this installation mode, you can decide which program parts of RCCMD are to be installed. Please note that the individual modules are coordinated with each other. If you do not install some modules, it may result in RCCMD not functioning properly. This mode is only recommended for experienced users.

If Option 1 is selected:

The setup tool selects the recommended default setting for you and prepares the installation for you:

```
Your RCCMD license is:

    You are on the 30 day free trial!

-----------------------------------------------------------------
Setup is now ready to begin installing RCCMD on your computer.

Do you want to continue? [Y/n]: _
```

You will get a small overview about the modules. access, method and the installation path. On your mark, the installation of RCCMD is starts. With "Cancel", at this point, the installation is withdrawn and the setup program quits.

Option 2: Custom installation

Adapt the installation to fit to your infrastructure:

Destination Folder:

```
Destination Folder

  [/opt/rccmd]: _
```

As a standard, RCCMD uses /opt/rccmd for the program data. If necessary, adapt the destination folder to your file system.

RCCMD Service and Configurator

```
RCCMD Service

The RCCMD Service is required to install.



RCCMD Configurator [Y/n]:
```

The RCCMD service is mandatory – this service manages your shutdown procedure

The RCCMD Configurator is the configuration interface for the RCCMD service. Unless you do exactly know what, you want to do, we recommend installing this module.

RCCMD Messages

```
-----------------------------------------------------------------
RCCMD Messages

By default RCCMD will print the messages it receives from the network to
/dev/console.
Here you can choose additional output options.



Display Messages on all Terminals [Y/n]:
```

RCCMD is capable to receive and display both, automatically generated status messages and custom configured text messages on system events within your UPS or BACS from all units of the CS121 and CS141 product family. With this setting you can define where the received messages are displayed accordingly.

Log RCCMD messages

```
Log Messages [Y/n]: _
```

All units of the CS121 and CS141 product family automatically create an event log with a time stamp for the system events. Therefore, it is normally not necessary to record all incoming messages. If you want to record the incoming messages, activate this function.

XMessage for RCCMD

```
Display Messages with XMessage [Y/n]:
```

If a graphical user interface is in use, RCCMD can display the messages as pop-up windows.

Web protocol, port selection and password

```
Web Protocol

[1] HTTPS: HTTPS
[2] HTTP: HTTP
Please choose an option [1] : 1

TCP/IP Port [8443]: 8443

Password [********] :_
```

The web interface can be accessed via http as well as https, whereby RCCMD activates HTTPS by default. You can adapt this setting to your requirements later via the configurator. For the correct setting, contact the local administrator.

TCP / IP Port

The port specification defines on which port the web interface can be reached. As a default setting, RCCMD uses port 8443 for its interface. Please refer to the local administrator to get the correct setting – the port must be available and may have to be enabled within firewall-solutions and port settings.

Password

Define the login password of RCCMD. This password will be used later when logging in to the web interface. If you want to assign the password later during configuration work, leave the field empty and confirm with ENTER. By doing so, the default password "RCCMD" is automatically active.

Installation summary and start installation

```
Setup is now ready to begin installing RCCMD on your computer.

Do you want to continue? [Y/n]:
```

Up to this point, no changes have been made to your system. If you cancel the installation, your entries will be discarded and you will revert to the standard installation.

Completing the installation:

```
------------------------------------------------------------------
Please wait while Setup installs RCCMD on your computer.

 Installing
 0% _____ 50% _____ 100%
 ##################################
------------------------------------------------------------------
Setup has finished installing RCCMD on your computer.

Start RCCMD Service now [Y/n]:
```

The configuration work is done - RCCMD automatically carries out the installation

---

Note:

By default, RCCMD is preconfigured to manage the shutdown of the operating system in case of receiving a valid RCCMD shutdown signal. However, since you have not yet defined the conditions a shutdown signal is to be sent or authorized a specific sender, "just activating "could lead to unpleasant surprises, e.g., if team members test the shutdown management at the same time.
Before you start the service within a productive environment (and thus "arm" the shutdown), we recommend a quick configuration via the convenient web interface.

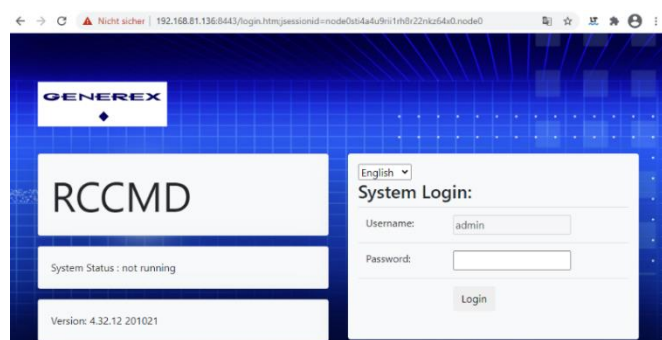The installation is finished, you may proceed with the configuration work.

How to access the web interface:

- http(s)://127.0.0.1:8443,
- http(s):// [IP address of the computer]:8443,
- http(s)://localhost:8443

Password: RCCMD or your own configured password.

For the quick configuration via the web interface refer to the chapter:

RCCMD Quick Configuration: Windows, Linux and MAC OS

Maintenance, Backup, Update, Restore and Uninstallation

Note:

The following instruction deals with uninstallation under Linux MINT (!) coming with a standard installation under /opt/rccmd/ - Depending on the distribution and your specifications during installation, installation paths, procedures and required parameters may differ from these instructions. Please Keep in mind that older versions of RCCMD used as installation path /usr/rccmd.

In this case, you will find the exact commands in the help section of the Linux distribution you are using.

Creating a backup file

Please keep in mind: Depending on the user that is currently logged in; you may need to increase the current system rights with the command *sudo su.* Before installing a new (updated) version of RCCMD, cleanly uninstall the old RCCMD version. Depending on the configuration, a data backup as a preparatory measure can save a lot of work. To create a data backup, some configuration work is necessary:

4. Create a backup that holds files
5. Uninstalling the existing RCCMD client
6. Installing the new /updated RCCMD client
7. Implement the backup files.

Step 1: Create a backup file:

d. Open the directory /opt/rccmd
Save a copy of this file:

o The file „rccmd.cfg"

e. Switch to the directory /opt/rccmd/webconfig/resources
Save a copy of these files:

o rccmdConfig_eclipse.properties
o ream.properties

f. Save all custom scripts and folders you want to hold.

Step 2/3: Do the installation work

Uninstall the existing RCCMD software and then install the new RCCMD software.

Step 4: Import the backup files:

The import of the backup is carried out in a similar way as the backup:

e. Copy all custom scripts back to the original folders.

f. Switch to the directory /opt/rccmd

o Place your saved "rccmd.cfg" here and, if necessary, overwrite the existing file

g. Move on to the directory /opt/rccmd/webconfig/resources
Place the following files from your backup here and, if necessary, overwrite any existing files:

o rccmdConfig_eclipse.properties
o realm.properties

h. To reload your active RCCMD settings, restart RCCMD.
i. Check settings and functions.

Uninstalling RCCMD for Linux

The following instructions deal with the uninstallation of RCCMD for linux under Linux MINT (!) that was carried out with a standard installation at /opt/rccmd/ - Depending on the distributions and linux modules as well as user defined specifications during the installation, installation paths, procedures and required parameters may differ from these instructions. if in doubt, please contact the vendor of your linux operating system or refer to our technical support at support@generex.de:

Simple method for a linux with an active GUI

Option 1: Use the installer

When installing RCCMD for the first time, this feature is not noticeable because there is no installed version of RCCMD yet.

When updating to a higher program version, however, the old RCCMD version must first be uninstalled. For this purpose, the installer provides the corresponding caller routine.

To do this, open the RCCMD installation package as system administrator and start the file "rccmdinstaller.run" with a double click.

The installer automatically recognizes that RCCMD is already installed and offers to uninstall it automatically. Confirm the uninstallation with "Yes" and confirm that you want to uninstall all modules.
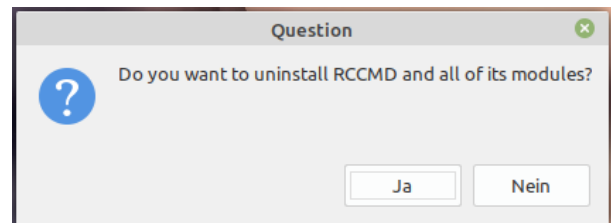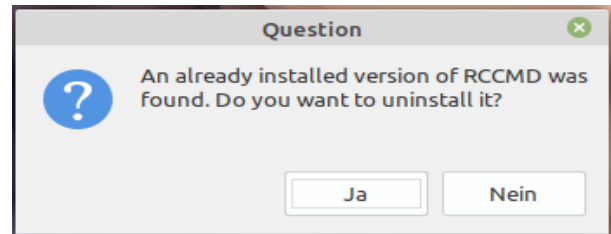
The uninstallation will be carried out automatically:
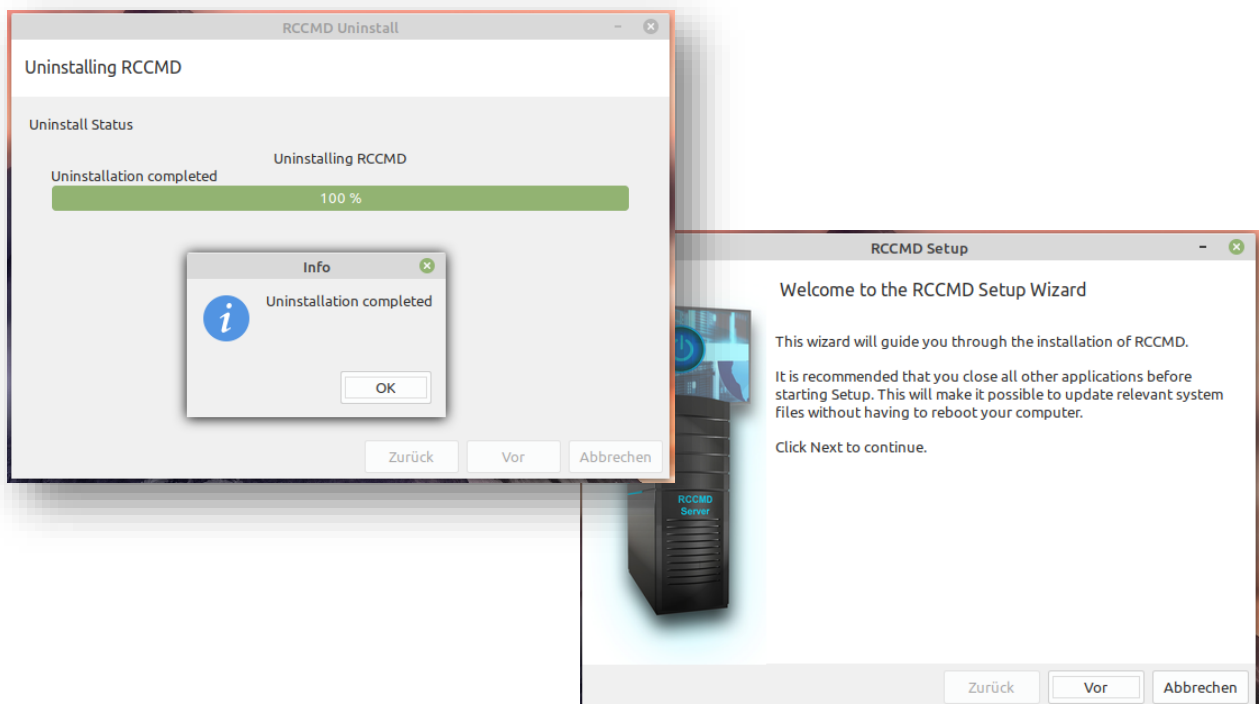
After the uninstallation is done, just click "Abort" to Cancel the installation dialog of RCCMD.

Note:
Uninstalling via the package and app management is specific to the respective Linux distribution and also depends on the personal taste of the system administrator. For more information about how to uninstall a program via the system settings, please refer to the in user manual of the according linux distribution.

Uninstalling RCCMD via console

RCCMD also comes with its own uninstallation program that you can call directly from the installation directory.

To do this, first open a terminal window. To access the installation directory /opt/rccmd, you first need increased system rights:

To do this, first open a terminal window. But to access the installation directory /opt/rccmd, you first need increased system rights:

Command: sudo su

```
gunnar@gunnar-virtual-machine:~$ sudo su
[sudo] Passwort für gunnar:
root@gunnar-virtual-machine:/home/gunnar#
```

You can recognise success by the fact that "root@" appears in front of your user name.

Starting the uninstallation

Now switch to the installation path of RCCMD to start the uninstallation:

Command 1: cd /opt/rccmd

Command 2: dir

Command 3: Uninstall_RCCMD/uninstall

First, change to the installation directory of RCCMD with the command "cd /opt/rccmd" and make sure with the command "dir" that you are in the correct directory and that the file Uninstall_RCCMD is present.

```
root@gunnar-virtual-machine: /opt/rccmd
Datei  Bearbeiten  Ansicht  Suchen  Terminal  Hilfe

gunnar@gunnar-virtual-machine:~$ sudo su
[sudo] Passwort für gunnar:
root@gunnar-virtual-machine:/home/gunnar# cd /opt/rccmd
root@gunnar-virtual-machine:/opt/rccmd# dir
changelog.md          rccmd_install_log.log   send_log.sh
inst_cfg              rccmd.log               send_mail.sh
jrccmdcfg.jar         rccmd_mail.sh           send_message.sh
jre                   rccmd_message.sh        send_shutdown.sh
manuals               rccmd.nfo               serial.xxx
messages.dat          rccmd_notalive.sh       ShutdownSuppressed.sh
rccmd                 rccmd.pem               Uninstall_RCCMD
rccmd.cfg             rccmd_shutdown.sh       version.txt
rccmd.cfg~            readme.txt              webconfig
rccmdctl              runRccmdConfig
rccmd_execute.sh  send_checkupsman.sh
root@gunnar-virtual-machine:/opt/rccmd# Uninstall_RCCMD/uninstall
```

Question

Do you want to uninstall RCCMD and all of its modules?

Ja   Nein

As soon as you enter Uninstall_RCCMD/uninstall and confirm with Enter, the dialogue for the uninstallation starts, which will guide you through the procedure:

Uninstalling of no GUI is present

The direct installation can also be triggered from the installation directory of RCCMD directly. By default, this is located under /opt/rccmd. To get there, however, you need extended system rights after logging in:

Command: sudo su

```
Linux Mint 20.1 Ulyssa gunnar-virtual-machine tty2

gunnar-virtual-machine login: gunnar
Password:
Last login: Fri Jul 30 13:53:29 CEST 2021 on tty2
gunnar@gunnar-virtual-machine:~$ sudo su
[sudo] Passwort für gunnar:
root@gunnar-virtual-machine:/home/gunnar#
```

Initiate uninstall

Switch into the installation path of RCCMD:

Command 1: cd /opt/rccmd

Command 2: dir

Command 3: Uninstall_RCCMD/uninstall

```
root@gunnar-virtual-machine:/home/gunnar# cd /opt/rccmd
root@gunnar-virtual-machine:/opt/rccmd# dir
changelog.md    rccmd.cfg           rccmd_message.sh    send_checkupsman.sh   Uninstall_RCCMD
inst_cfg        rccmd.cfg~          rccmd.nfo           send_log.sh           version.txt
jrccmdcfg.jar   rccmdctl            rccmd_notalive.sh   send_mail.sh          webconfig
jre             rccmd_execute.sh    rccmd.pem           send_message.sh
manuals         rccmd_install_log.log rccmd_shutdown.sh send_shutdown.sh
messages.dat    rccmd.log           readme.txt          serial.xxx
rccmd           rccmd_mail.sh       runRccmdConfig      ShutdownSuppressed.sh
root@gunnar-virtual-machine:/opt/rccmd# Uninstall_RCCMD/uninstall
Möchten Sie RCCMD und alle verbundenen Module löschen? [Y/n]: _
```

First, change to the installation directory of RCCMD with the command "cd /opt/rccmd" and make sure with the command "dir" that you are in the correct directory and that the file Uninstall_RCCMD is present. As soon as you enter Uninstall_RCCMD/uninstall and confirm with Enter, the dialogue for the uninstallation starts, which will guide you through the procedure:

```
Möchten Sie RCCMD und alle verbundenen Module löschen? [Y/n]: y

------------------------------------------------------------------------
Deinstallations Status

 Deinstallieren von RCCMD
 0% _____ 50% _____ 100%
 #######################################

Information: Deinstallation erfolgreich
Drücken Sie [Enter] um fortzufahren:_
```

The uninstallation is done, press Enter to return to your console.

Installation - RCCMD for MAC OS

MAC OS Installation guide
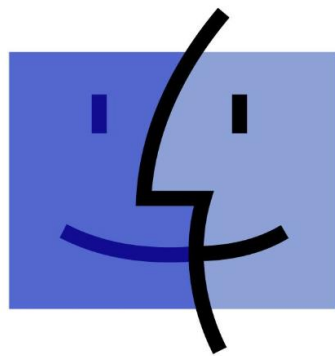
Installation with the Install Builder r\2020-04-07\MacOSX

Releasing the file for installation

Apple differs between installable software and original certified software. Due to this fact, an application for MAC OS that ultimately does not come from the Apple Store itself, may simply be rejected the first installation attempt. Instead of installing as wanted, MAC OS offers to drop this piece of software into Recycle Bin:
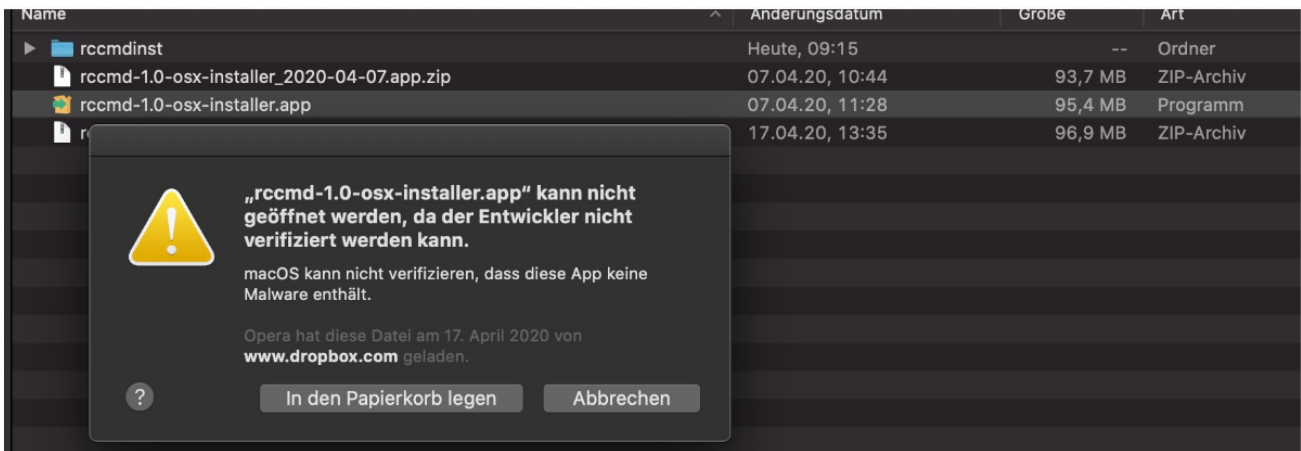
To continue the installation, click on the lock symbol under Settings/Security. Now click on the "Cancel" button of the warning message. MAC OS will offer you the option "Open anyway":
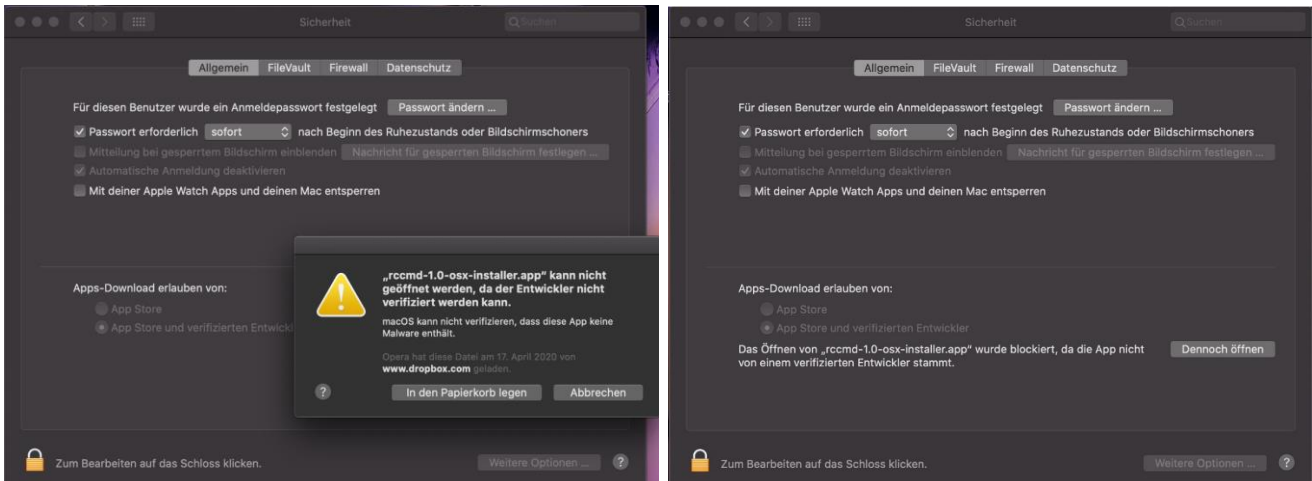
This shall trigger a warning message with the „Open "– button:

Approving a file for the installation

 If someone wants to install something on an Apple PC, extended system rights are sometimes necessary or the installation cannot be carried out.

Apple's installation manager needs to hand over the entire installation process to the 3rd party software. To confirm this step, the installation manager asks for the corresponding password.

RCCMD installation dialogue

The installer is multilingual, you may choose the default language (English) or a language that is more familiar with you.

Due to the fact that the language of the installer has nothing to do with the language of RCCMD itself, feel free to choose your language - it is possible to adapt the language later on.

For this Installation guide, we choose the default language "English".

When ready, click on OK

The RCCMD Welcome Screen

After selecting your preferred language, RCCMD needs some information for the installation process:

In general, the installer asks for some basic data that are necessary for the initial setup configuration. Before you continue, please ensure a valid key is available and at hand. RCCMD will ask for it. at any time up to the start, it is possible to abort the installation by clicking "Cancel"; Unless to the final click, no changes will be made to your operating system.

Click NEXT
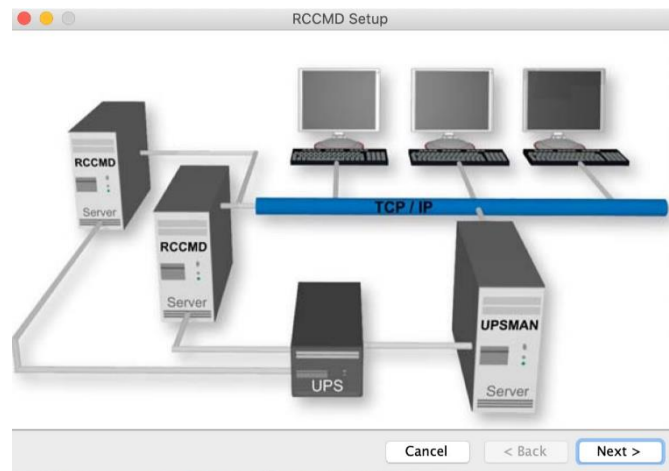
Copyrights, licence agreements, and other stuff to read

We would like to briefly explain what you are allowed to do, what you are not allowed to do, how the software has to be used, etc - Information that can be read within estimated 0.8 seconds before clicking "I accept the agreement".

By the way, we recommend to read it carefully and if you click on "I do not accept the agreement", the installation will be aborted because you have not agreed, previously saved data will be removed again and the installation dialogue will be closed.

After selecting „I accept the agreement "click NEXT
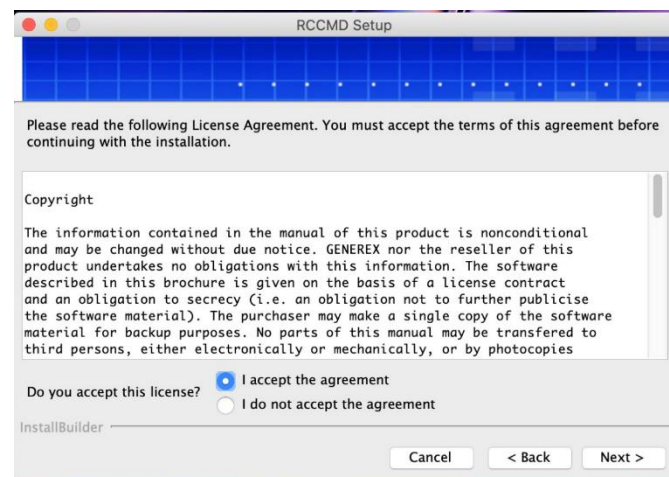
 Select installation directory

The installer selects a typical Apple installation directory and recommends it for installation.

If the installation directory does not fit to your system, adjust the location according to your wishes and ideas.

After selecting an installation path, click „NEXT "
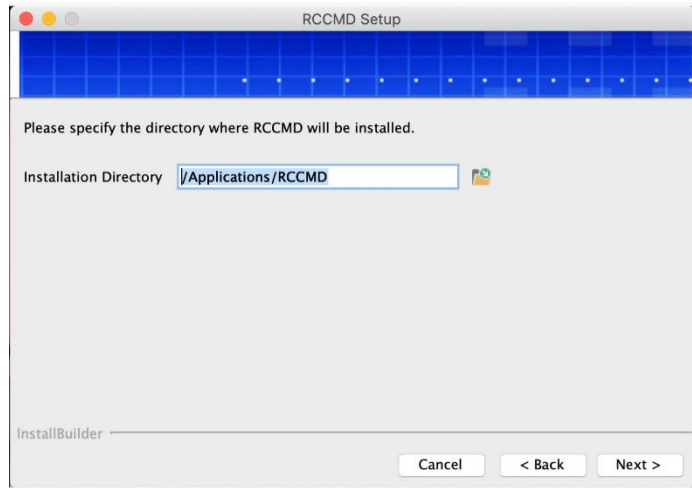
The licence key:

Enter your licence key - this was given to you by your dealer with the UPS documentation, is included in the documentation of your CS141 / SITEMANAGER or SITEMONITOR or was brought to you via e-mail.

If you do not have a licence key at hand, simply enter "DEMO" at this point. RCCMD will use an internal evaluation key and start the test phase. You can change the licence key at any time via the web interface.

By doing so, RCCMD will be unlocked to the full version on restart.

After entering the licence key (or „nothing "), click „NEXT ".
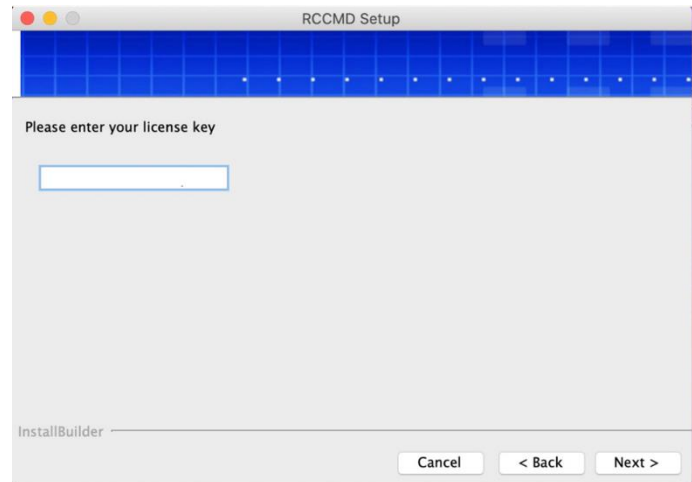
Optional modules:

The WebIf installs the user interface you need for convenient and mandatory configuration.

If the WebIf is not selected, please select it so that it is installed.

Why is this optionally when I need it?

It's simple: other software versions may use modules that are really not important. In this case, you need it.

Click „NEXT "to continue
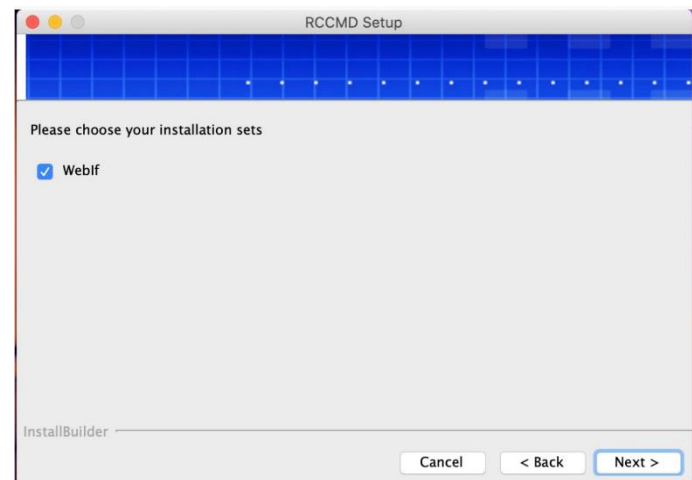
http(s) and port setting

RCCMD is configured via a modern web interface.

To provide access to the web interface, RCCMD needs to know whether you want to use http/https or on which port internally the interface should be accessible. The default port for RCCMD is port 8443, but you can select any port that fits your network and is not occupied. RCCMD is configured via a modern web interface.

In order to access the web interface, RCCMD needs to know whether you want to use http/https and on which port internally the interface should be accessible. The default port for RCCMD is port 8443, but you can select any port that suits your network and is available:
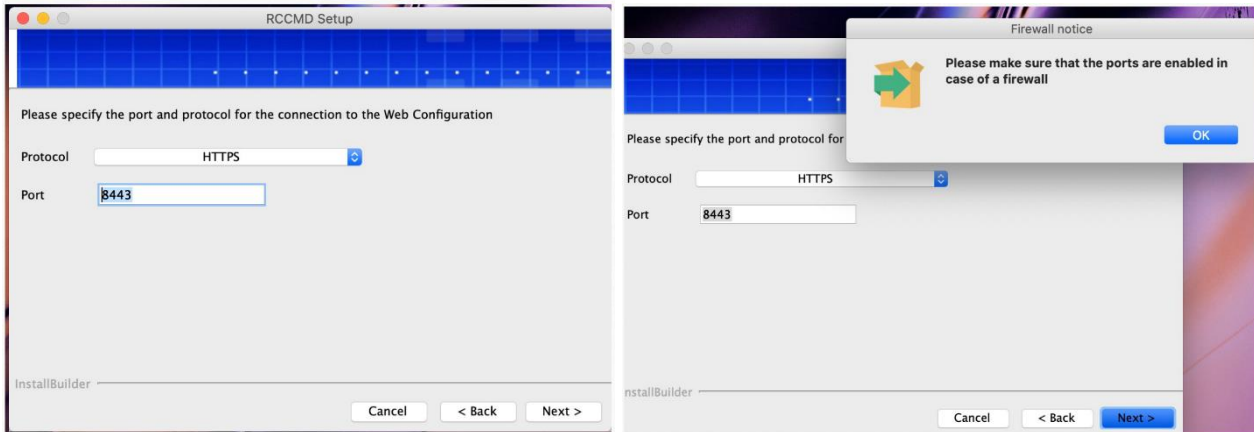
Please note:

RCCMD comes with its own certificate, but it was not created on the MAC OS. A modern web browser will of course notice this and complain that although there is a valid certificate, it cannot be guaranteed that the website is also what it claims to be. Since this is a local installation, you may can ignore this notice accordingly.

Click „NEXT "

Summary and start installation

In the next step, RCCMD shows you your selection, i.e., the installation directory, the available disk space and the estimated disk space required for the installation. With "Back" you can go back to the individual configuration steps and with "Cancel" you can cancel and discard the installation.
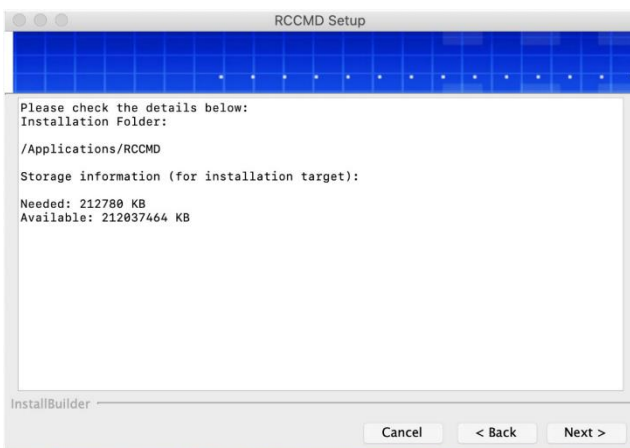
Click "NEXT" to confirm your choices.   Click "NEXT "to start the installation.
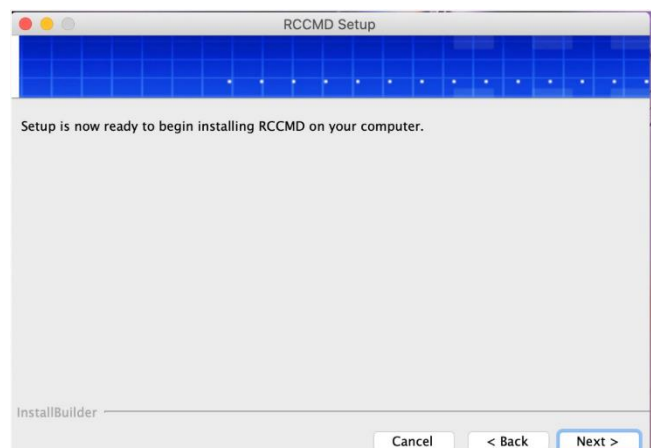
Installation progress and firewall

The installer shows you an overview of the installation process.

RCCMD will ask you whether the firewall should be configured automatically so that you can access the web interface afterwards. With this question, the installation is completed and RCCMD is ready for use.
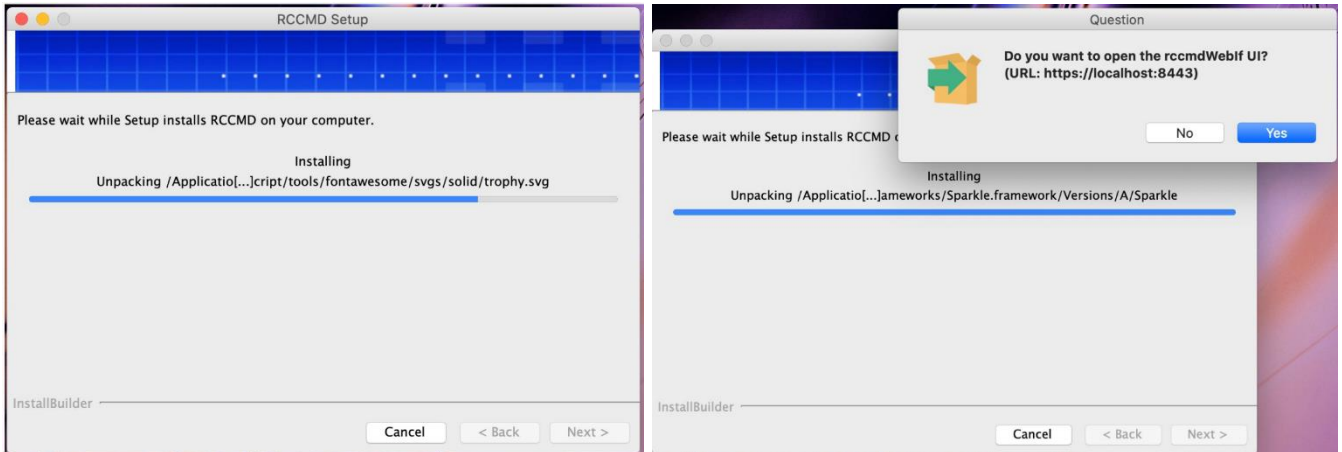
Confirm the firewall question with a click on „YES"

First start of the web configurator

The Safari web browser will inevitably detect that RCCMD is using a supposedly invalid certificate. This is not quite correct:

The certificate is valid, but it was not issued on this computer. Thus, the computer cannot authenticate itself as credible to itself. However, since you are on your own computer and are sitting in front of the machine via the WebIF or via the URL https://localhost:8443, you can ignore this notice and confirm the certificate permanently.
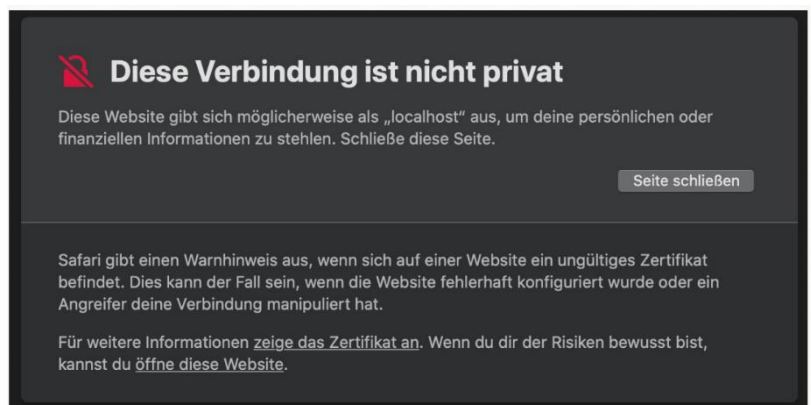
Quick configuration

The installation of RCCMD on a MAC OS is completed. Now proceed with the chapter for quick configuration of RCCMD via the web interface.
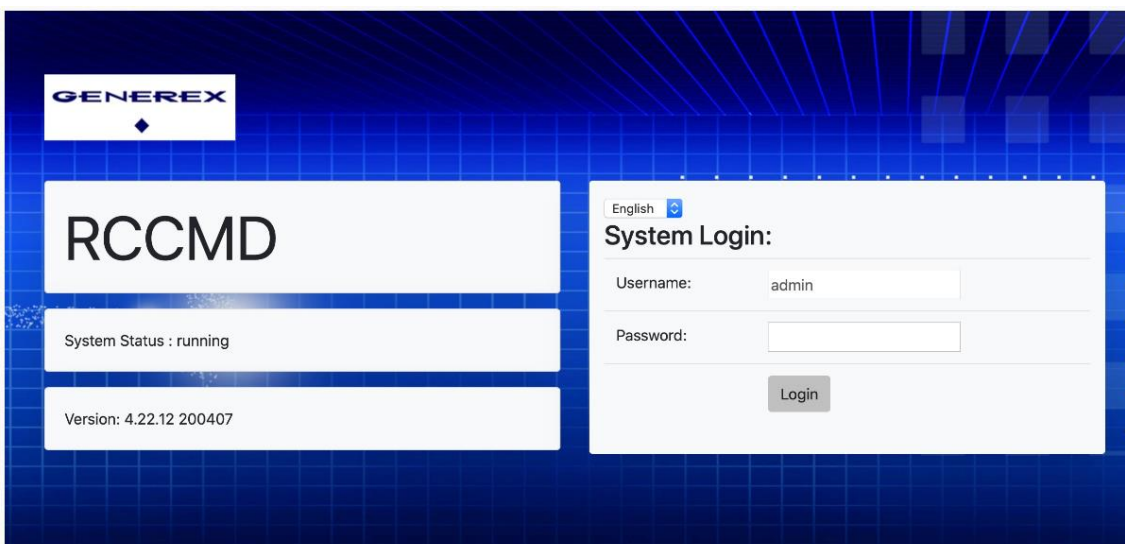
RCCMD Quick Setup: Windows, Linux and MAC OS

Quick Configuration Guide – The most important settings
For Windows, Linux und Mac OS

Login and quick configuration

This chapter is about getting started quickly and securing your RCCMD installation.

How to access the web-based interface:

- https://127.0.0.1:8443 ,
- https:// [IP-Adresse des Computers]:8443,
- https://localhost:8443

Password: RCCMD or your password
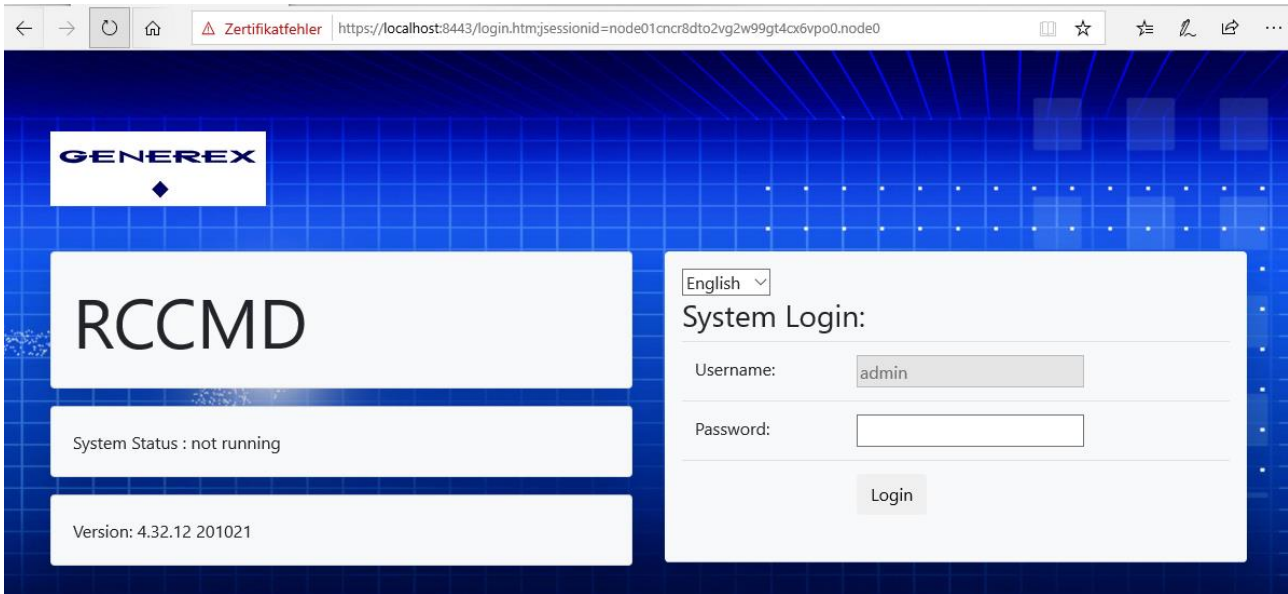
If you have assigned a password during installation, you need to enter it now for access. If you left the field blank, use this original password:

- RCCMD or the password you entered during installation.

After logging in, you can access the configuration menus:

Step 1: Click on Status > System Status
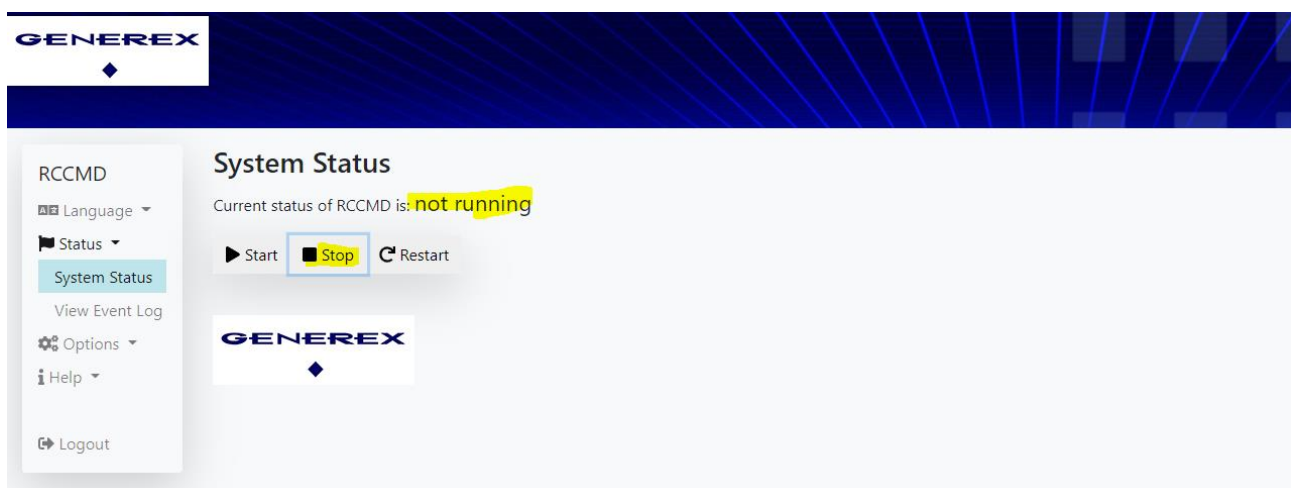
Please check that under System Status RCCMD is set to "not running". This ensures that your server cannot be accidentally shut down for now.

Step 2: Options>Connections
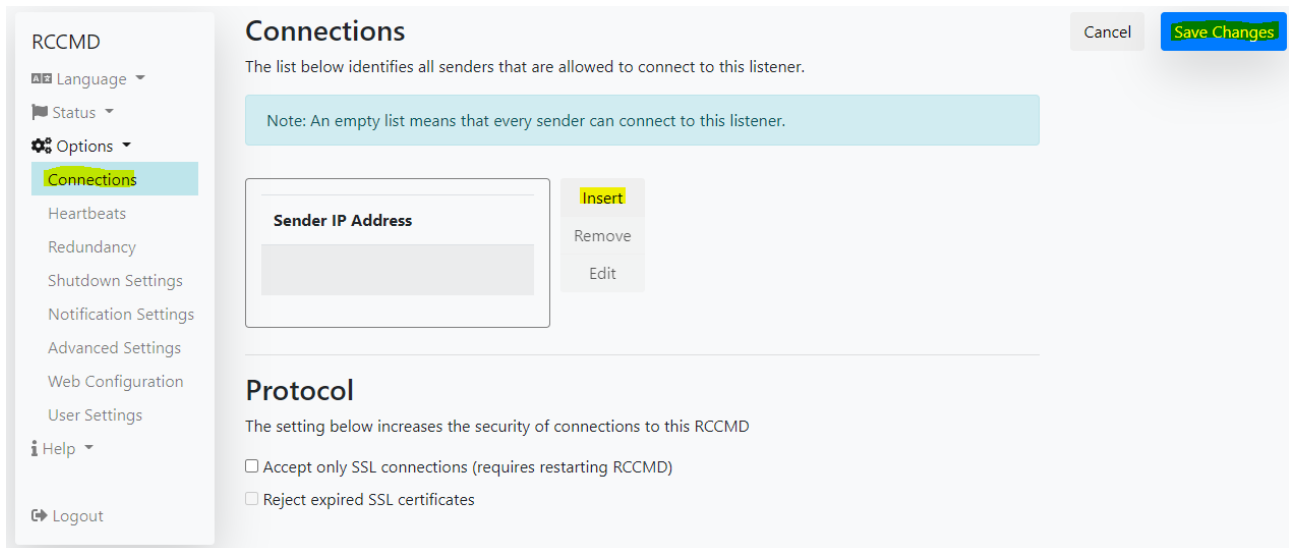
Under Connections, click "Insert" and enter the IP address of the responsible CS121/ CS141/ UPSManager, ... - in short, the valid RCCMD Shutdown Sender.

Make sure that you also click on "Save Changes" at the top right so that the stored IP address is valid.

What you do with this step:

As soon as an IP address is stored right here, the RCCMD client will only accept exactly THIS IP address as an authorized transmitter. Other signals are politely documented, but the execution is refused.

Step 3: Control Heartbeats under Options>Heartbeats
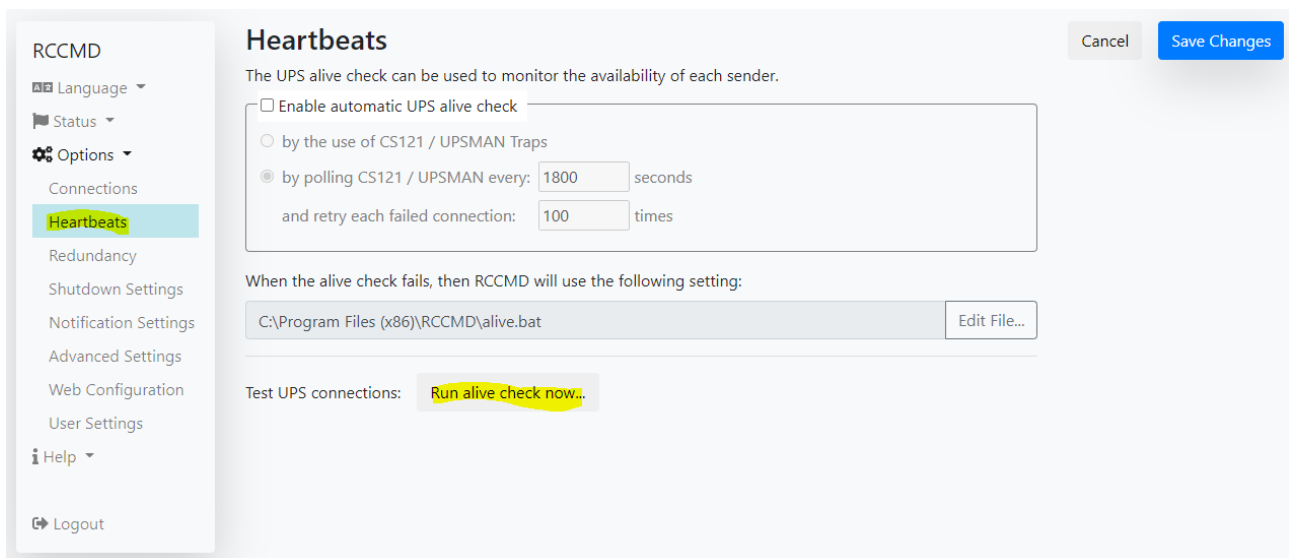
Via this function, you can determine whether the RCCMD client also reaches its CS141 and communication is running. Please note that for licensed products - i.e., manufacturers of SNMP cards that have carried out an RCCMD licensing, this function is not necessarily supported by the hardware.

All GENEREX cards (BACS / CS121/ CS141/ SITEMONITOR / SITEMANAGER) support this function, RCCMD shall provide an "OK" at this point.

CS121 / UPSMAN addresses	Alive result
10.10.10.10	Ok
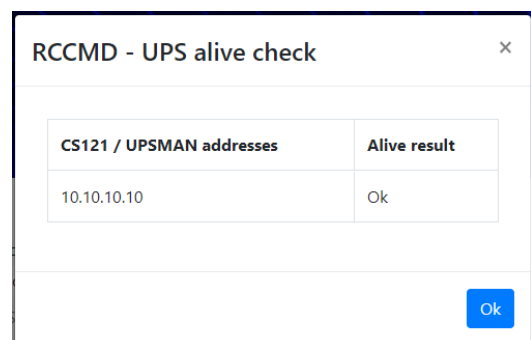
Step 4: Check the shutdown sequence

Under Options, click on Shutdown Settings
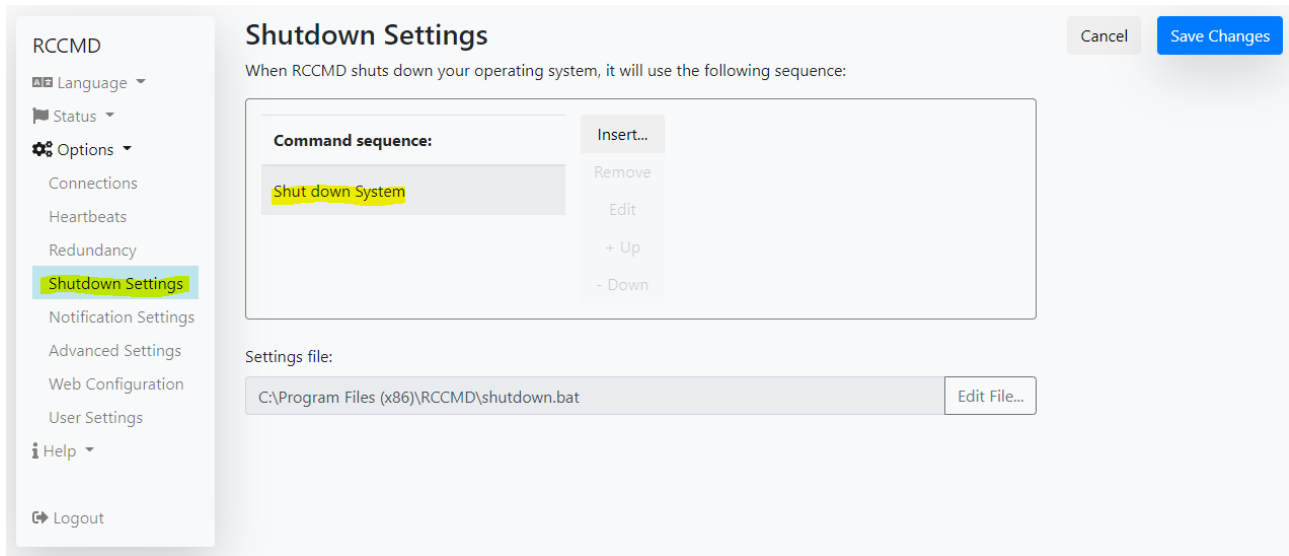
By default, the command sequence "Shut down system" should already be included:

RCCMD triggers a shutdown script that will advise the Windows operating system to shut down and switch off the hardware. If the computer should simply restart afterwards, this is set within the BIOS. Keep in mind that some settings must be done by BIOS settings that will configure. beneath other things, the mainboard directly and depends on how the entire computer shall react to a power fail.

How does the RCCMD shutdown job list work?

If an RCCMD shutdown is triggered via a valid transmitter, this list is executed from top to bottom as entered. So, make sure that "System Shutdown" is always the last item to be executed.

Step 5: Check and change licence

Open Status>System Status and click on Start
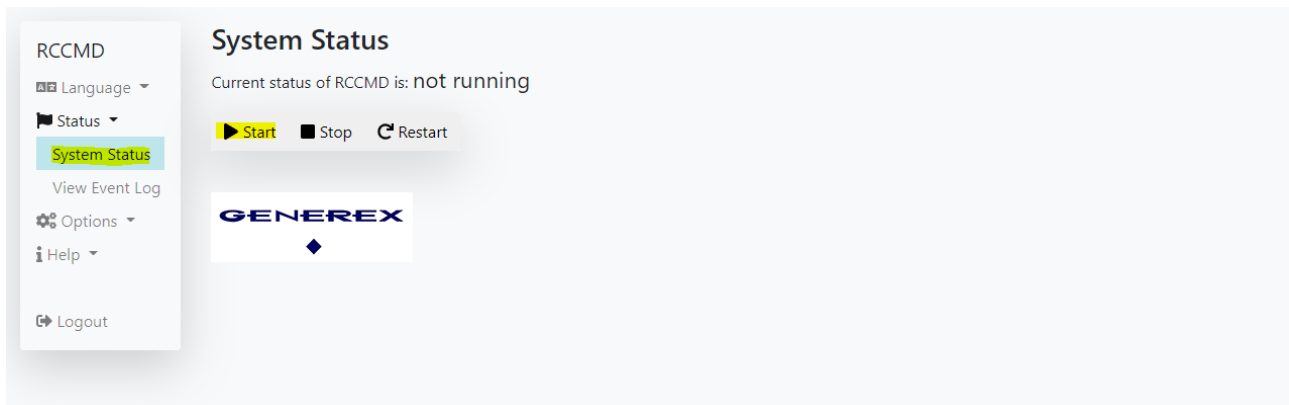
Proceed to "Event log". If you see this entry, the key you entered is not correct:
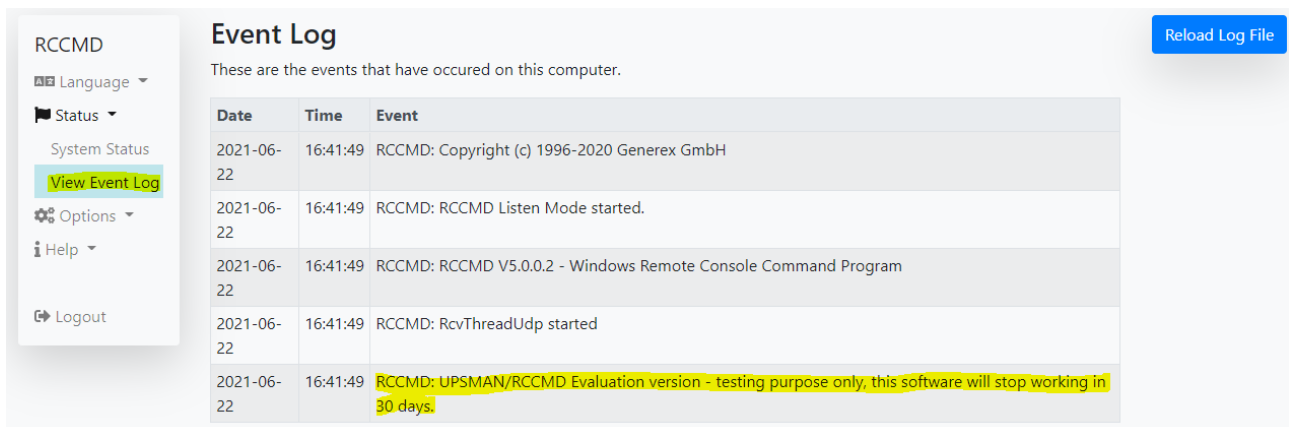
How to change the RCCMD license Key:

Click on Options>Advanced Settings

At the very bottom, you will find the setting "Update license key":

Simply enter the new key and click "Restart" under "Status". The test key log file entry appears until a valid key is entered.

Step 6: Change User Password

Click on Options>User Settings

Using the _default password is a crucial security leak_ – If not changed during installation phase to a custom password, RCCMD will grant a access to all RCCMD functions for anyone who knows how to read a manual. Due to this fact, we strongly recommend to change the password as fast as possible.

How to change the password

Current Administrator Password:	Enter the current password. If not changed during installation, enter 'RCCMD'.
New Administrator Password:	Enter a new password.
Confirm Administrator Password:	Repeat your new password to confirm your settings.

Note:

Remember to choose a "strong password", e.g. "Refl-Jobo-45&3-Hable".

The RCCMD Web Interface

All configuration menus in detail explained
For Windows, Mac OS and Linux

After installation, log in via the web interface and start with the configuration of RCCMD. The user's name is predefined by system and cannot be changed:

- All configured actions are administrative interventions in a running operating system.

Available password options

- If you did not assign a password during installation:

  In this case, use the default password RCCMD.

- If you assigned your own password during installation:

 Use the password that you assigned.

Note
On initial setup, the system status is defaultly "not running". In this system state, RCCMD will neither receive nor be able to convert valid signals. This is an intentional state because with the initial default start-up configuration state, any valid RCCMD shutdown signal will be executed accordingly.

Check system state

After logging in, you will be redirected to the current system status page. From here, RCCMD can be basically actively switched ON / OFF:
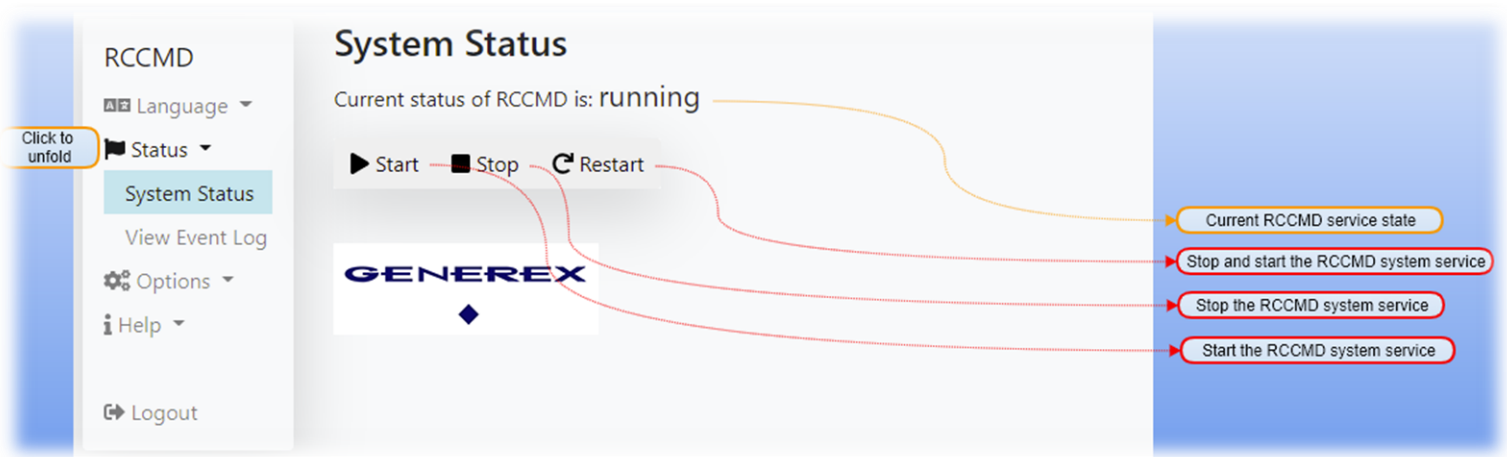
Start

Starts the RCCMD service. The configuration changes will be armed. As soon as RCCMD is active, incoming RCCMD signals will be logged executed.

Stop

This function stops the RCCMD service. The incoming signals are not monitored and RCCMD will neither log nor trigger incoming RCCMD signals.

Restart

The restart stops the RCCMD service and then starts it again. This function combines the other two functions and can be used to initialize a configuration on the fly.

Note

Why do I need an RCCMD „Restart "?

In some cases, RCCMD has to read configuration files and take them to the active configuration during initialization. However, this can only be done during a restart - the complete server does not have to be restarted for this, it is sufficient if RCCMD exits briefly and then restarts itself. If this is necessary when changing configurations, RCCMD will automatically inform you via a pop-up window.
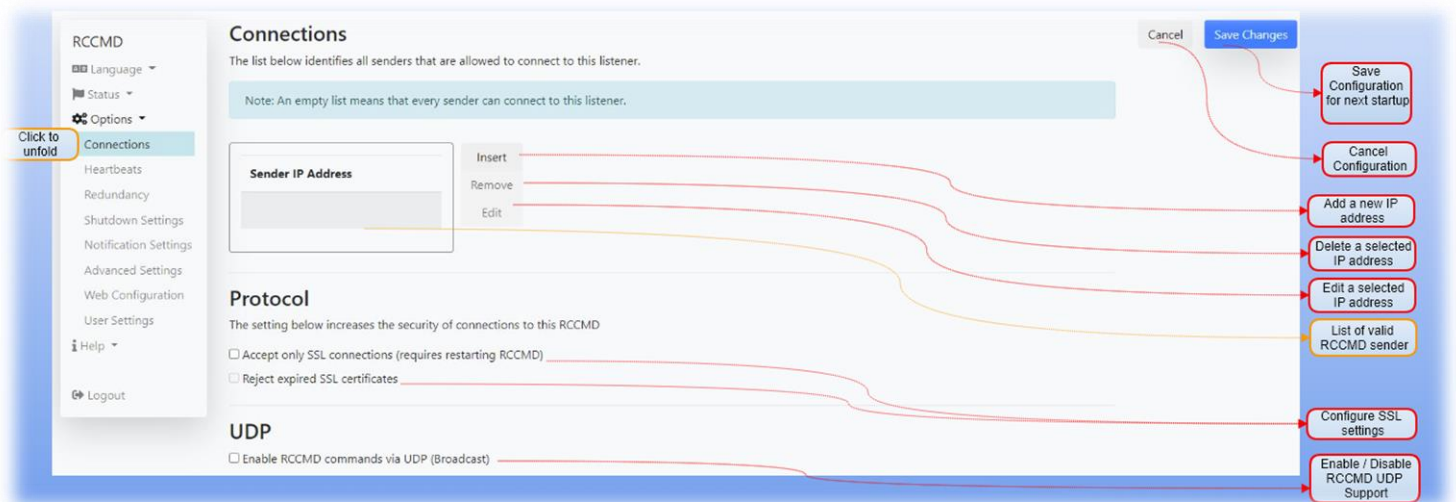

Logfiles
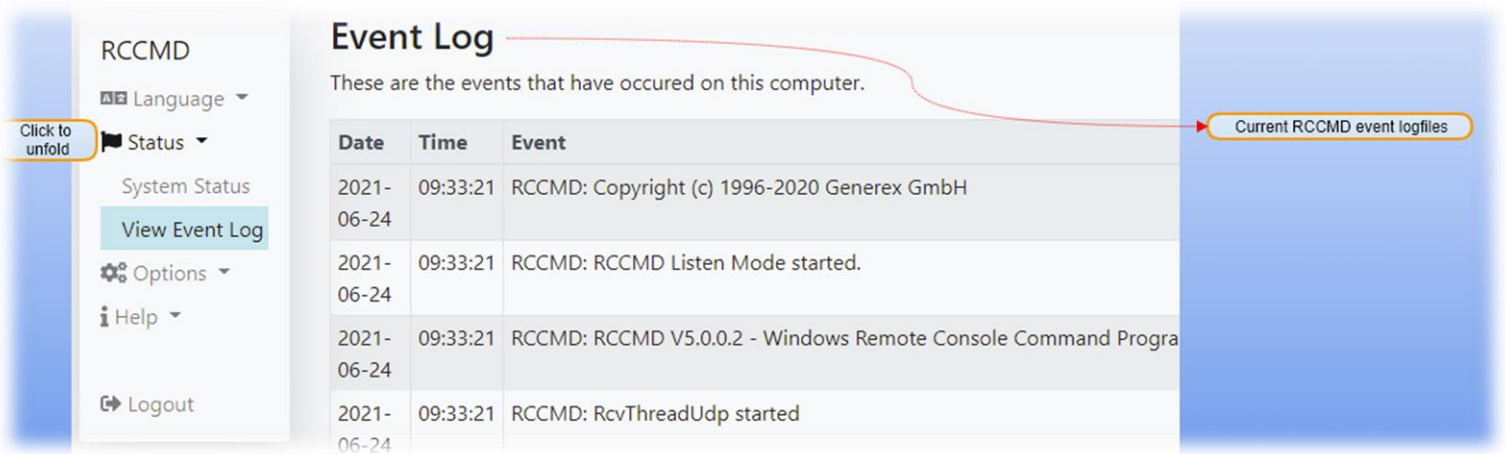
Once RCCMD is active, it will log all incoming traffic and actions.

The log file holds all system relevant information, including

- Date and timestamp
- Sender address
- Requested action or function
- Execution status

With these files, RCCMD provides options for analyzes of the path of an RCCMD signal.

Connections

Within larger installations, it may happen that some senders are not necessarily allowed to shut down a specific RCCMD managed server. A typical example would be an SQL database that is only shut down when all connections have been closed properly, or special backup servers or domain controllers that have to shut down last and start first. There are also many scenarios in which an RCCMD client is only allowed to implement a signal from certain sources and must refuse execution in any other case.

> **Note:**
>
> Within the RCCMD configuration, this setting is necessary if you want to unlock and define redundancy behaviour: As soon as two or more UPS systems are present, the corresponding transmitters must be defined within this menu.

RCCMD UDP Broadcast Support

As soon as a CS141 sends information about a job over the network and no IP address is used, the message will be carried out via unidirectional UDP. These jobs can be identyfied by the fact that no IP address is defined within the CS141 job configuration dialogue at "Parameters", or simply the option "broadcast" is available.
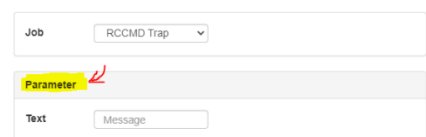

However, an RCCMD client will ignore these broadcast messages until this feature is explicitly enabled. Keep in mind that UDP data packages are not ensured by handshakes as known with TCP by design – if broadcast messages are not in use, disable this feature to reduce the risk of IP spoofing.

RCCMD Message windows

In some cases, it is necessary to restart RCCMD briefly as a service. This can be done under System Status within the configuration interface.

If this step is necessary, RCCMD will inform you directly when accepting the data:
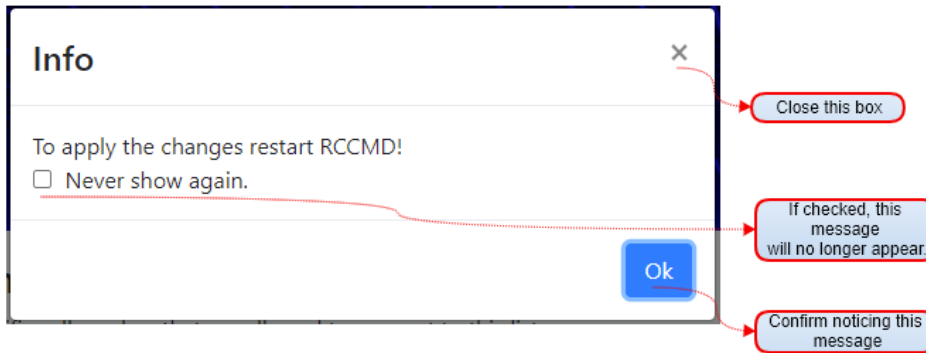
Never show again

This window is no longer displayed until you have closed the web browser and opened it again. You can therefore carry out all the configurations and then restart RCCMD.

OK

The critical RCCMD service generally waits for your instruction. This button is the general read confirmation. It will re-appear in case of any system critical changes are saved. RCCMD will only restart itself in exceptional situations if it is absolutely necessary for a configuration step.

Heartbeats
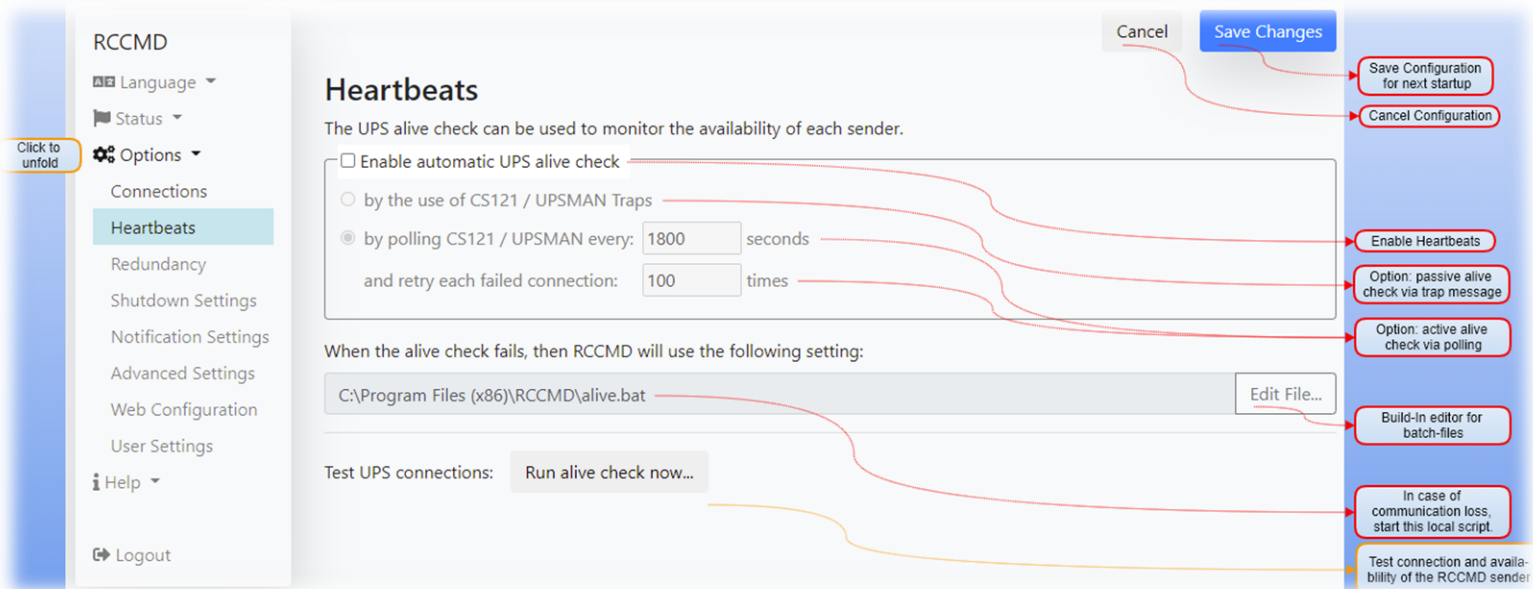
Under circumstances, the connection between RCCMD and CS141 can break down. This happens, for example, if a switch is forgotten during a power failure and simply does not work during the power loss. In this case, the CS141 would send a valid shutdown signal, but it would never reach its destination.

Another scenario would be a defective switch or router:

Since RCCMD is a pure receive program that reacts to the input of signals, it cannot know whether the connection is generally switched correctly. With Heartbeats, RCCMD will be able to interact with any IP address that is configured at Connections:

UPSMAN Traps

In this case, an RCCMD server sends an unsolicited trap message to the RCCMD client. The receipt of this message is logged accordingly.

By Polling

The RCCMD client cyclically requests a message from the RCCMD server and logs the availability of the remote station. If this connection is not possible, the process can be repeated freely definable often.

When the alive check fails, then RCCMD will use the following setting

This script is a standard file which can be freely edited. RCCMD does not give you any specifications as to what should or can be achieved with this script. Feel free to edit it as needed.

Note:

RCCMD must, of course, somehow know which devices are ultimately to be tested. The list of devices to be checked is taken from the list you enter at Connections: The reason is that these devices are of particular relevance for the RCCMD client.

Defining the redundancy level

First of all, …

Please note the distinction between the CS141 and the UPS - Normally, the UPS cannot send a message, only the CS141 connected to the UPS. This can be an external device via RS232 / RS485 or also an internal slot card. Technically they are independent devices, but if you follow the path of the signal starting from the UPS, it is easier to visualize if you consider the CS141 as a component and therefore the UPS as the "transmitter"...
If there is more than one UPS in a network, systems can be connected redundantly. In this case, the failure of one of two power supplies may not necessarily trigger an emergency shutdown.

RCCMD can be set to take this network configuration into account. The configuration will be carried out as followed:

1. Under connections, define static valid IP addresses of all valid RCCMD senders (including the UPS)
2. At redundancy, decide, which of the IP addresses will be included into the Redundancy,
3. Set up the redundancy level:

   The redundancy level follows a clear scheme: As soon as one of the selected valid transmitters sends a shutdown, the redundancy level is used to determine how many other transmitters must also send a shutdown:

   0 – No other signal is required, RCCMD will trigger shutdown process immediately.

1 – At least one ein weiterer der ausgewählten Sender muss einen Shutdown senden
2 – At least two more of the selected transmitters must confirm a shutdown.
3 – At least three more of the selected transmitters must confirm a shutdown.

The maximum redundancy is automatically adjusted to the number of IP addresses of valid transmitters selected under "Group". You can therefore never select more units than are actually available. Please keep in mind, if you select 3 devices for redundancy, you may also configure that 2 of 3 can advise a shutdown. But in this case, you will not be able to define which of them will send.

Redundancy shut down override

It can always happen that a shutdown has to be carried out even though both UPS systems are in order and the main power supply is running faultlessly - a typical scenario here would be a defective air conditioning system, which would result in the overheating of servers and other infrastructure - and only one of your CS141 monitors them additionally.

In this case, harmed server should also shut down in time before getting damaged by overheating. RCCMD offers several options to solve such a problem:

1. Write a small shut down script and place it within the RCCMD installation folder. This script can be triggered directly via the RCCMD job "RCCMD Execute".

    With this command, RCCMD offers an option to start any script that triggers any command - including a scripted shutdown routine. Since this is not the job "RCCMD shutdown", which was specifically associated with the UPS, the RCCMD client would execute this command accordingly - with an entry in the connections table, the IP address of the sender is allowed to send commands.

How to use a third CS141 independently

As an example, the third CS141 was configured to handle environmental control only:

Depending on your personal style and the configuration level, up to 8 analogue sensors and 4 digital inputs can be possible and may include fire and smoke sensors, glass breakage sensors, access control systems, gas detectors, temperature sensors, level detectors, digital alarm wires, battery management systems, motion detectors, etc.
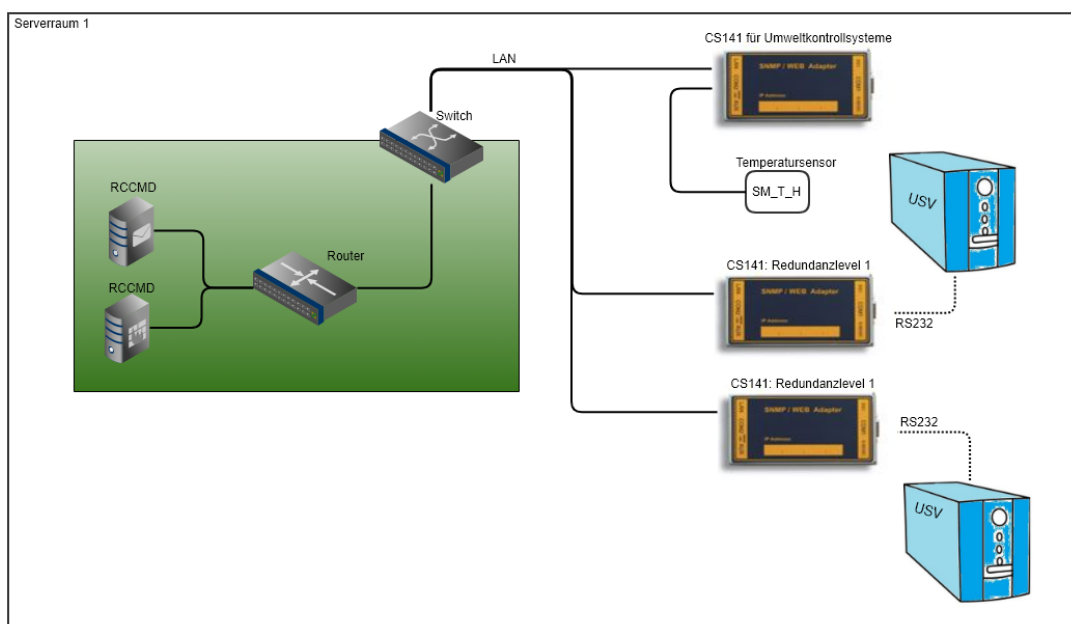
In this case, you would enter all three CS141s at Connections, but for redundancy, you would only select the two transmitters that deal directly with the UPS and the emergency shutdown in case of problems with the UPS. The third CS141, which is only responsible for the environmental control systems, could in this case send an RCCMD shutdown independently.

Withdrawal of a shutdown:

From a redundancy of 1 (= two units), a shutdown can also be reversed - this is the case, for example, when the main power supply of a UPS has been restored. This is done at the transmitter with the custom command "WAKEUP" - this is the signal for the RCCMD client that the cause of a fault has been eliminated, and the counter is corrected accordingly.

Note:

In this context, each CS141 is generally only allowed to send one shutdown signal. The RCCMD client remembers which transmitter has already sent and which transmitter has sent a corresponding counter command. The restart of the RCCMD client - normally a start after shutting down the computer or via system status - generally resets this counter to 0. Therefore, if you test the incoming signals after configuration, restart the RCCMD client again in any case to prevent an accidental shutdown.

Shutdown Settings
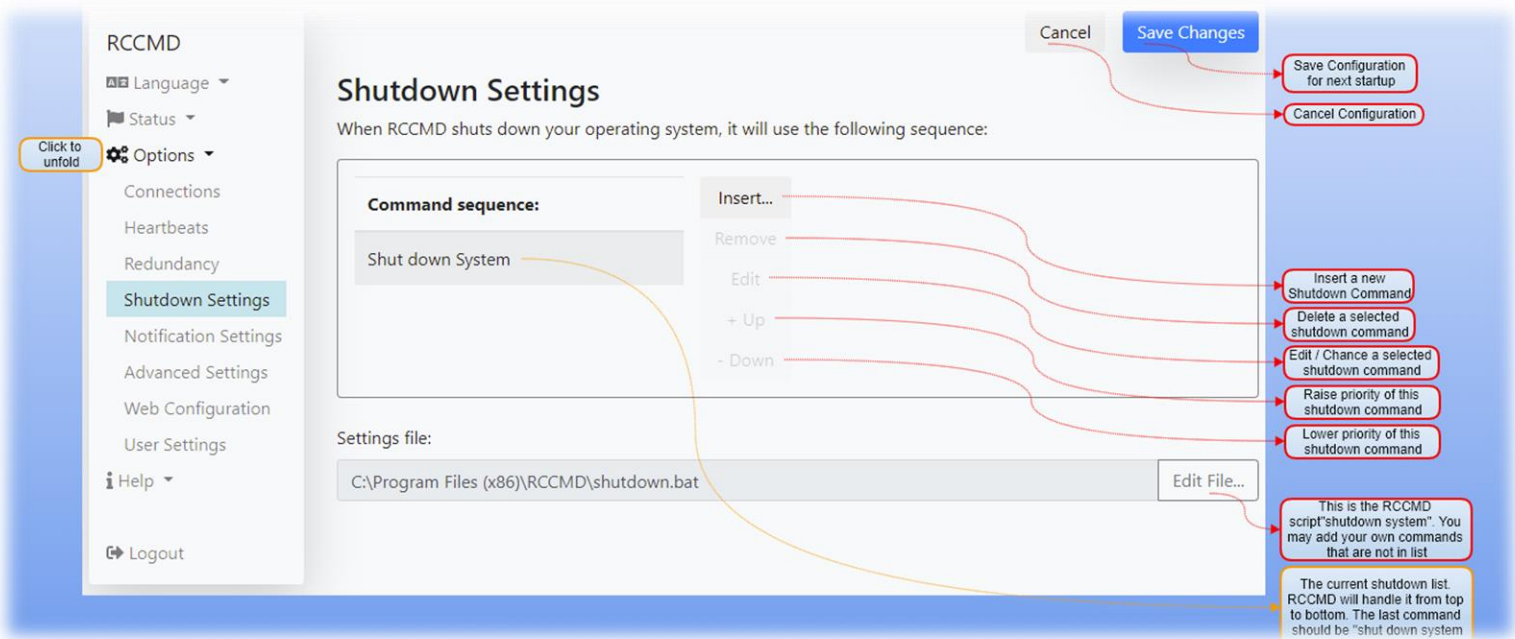
RCCMD for Windows offers extensive possibilities to run a well-structured shutdown. To provide quick configuration, the command "Shut down system" is already preconfigured as a basic setting: As soon as RCCMD receives a valid shutdown signal, the script shutdown.bat is started, which instructs the operating system to terminate all programmes and processes, shut down the operating system and switch off the associated machine.

> **Note:**
>
> This command should be the last command of the command sequence that RCCMD should execute, as RCCMD will switch itself off with this command. All commands that follow will no longer be executed.

The script that gives this command its effectiveness can be found at shutdown.bat. You will find this page below the dialogue and can adapt or change this batch file as desired by clicking "Edit file".

Adding a command to the existing command sequence

Click Insert to add a new command to the current sequence.

RCCMD provides a list of possible pre-defined commands:

| Command	Operating System	Description
Shut Down System	Linux, Windows MAC	The programs are closed, and the operating system is shut down normally..
Log off from System	Windows Linux MAC	All users are logged out, and the foreground processes are terminated. The system remains active and shows the login mask
Power Off System	Windows, Linux, MAC	All active processes are terminated and the system is turned off
Restart System	Windows, Linux, MAC	Similar to shutting down, except that instead of turning off the computer, it restarts.

Hibernate System	Windows, Linux MAC	A power saving mode in which all components not required for direct operation are switched off to save power. The operating system dumps volatile data onto the hard drive, empties the RAM and puts the computer in a powerless state.
Suspend System	Windows Linux, MAC	A power saving mode in which all components not required for direct operation are switched off to save power. The operating system stores all the data necessary for operation in RAM memory in order not to burden the hard drive. The computer goes into a deep sleep mode but is not de-energized. *If the computer is turned off, the data stored in RAM will be lost.*
Quit Lotus Notes	Windows only	Lotus Notes reacts sensitively when you simply shut down the operating system and specifically needs to be shut down beforehand.
Quit Siemens SIMATIC	Windows only	A SIMATIC server is very sensitive if you do not strictly adhere to a shutdown sequence for SIMATIC. This job cleanly terminates the SIMATIC server before the operating system can be shut down in the next step.
Wait some seconds	Windows, Linux MAC	Especially if you have your own scripts running, which in turn trigger parallel scripts or contain special save and copy commands, it may happen that the scripts do not have enough time to run cleanly to the end and fulfill their respective task. This entry in the shutdown sequence allows you to define a timer that RCCMD waits before jumping to the next point.
RCCMD shutdown relay	Windows, Linux, MAC	RCCMD can also send shutdown signals - so it is important to define valid transmitters that are authorized to instruct a shutdown. So not only can you control the redundancy behavior via UPS and CS141, but you can hand over an RCCMD shutdown across different server types.
Shut down a virtual machine	Windows Only Available with Version 4.57.12 240429	Windows PowerShell commands that can be used to shut down a virtual machine running Hyper-V. .
Shut down all Hyper-V VM's	Windows Only Available with ersion 4.57.12 240429	Windows PowerShell commands that can be used to shut down any virtual machine running Hyper-V. Be careful with Hyper-V clusters, the cluster manager will shut down ALL virtual machines that are in the cluster with this command!
Custom Command	Windows, Linux, MAC	The Manual Command gives you complete freedom to run scripts in a sequence locally on your system - you can start programs, end processes, execute command lines, etc.

The command sequence is always executed and triggered "as read" from top to bottom. Depending on the type of commands that are triggered, contradictions or problems with rights management can occur within complex structures, which can have very different effects:

A typical problem would be, for example, if you start an external backup program with its own shutdown scenarios via the "Manual command" within the command sequence and have not removed entry in the command sequence that is supposed to shut down the operating system:

Once the backup program has been started, RCCMD logically executes its next command in the chain and ultimately forces the backup program to shut down - which can lead to very different results:

a.   The operating system shuts down, the backup program reports an error

b.   The backup program refuses and takes over shutdown control

c.   The operating system becomes interactive, asks in a dialog box what should happen and waits...
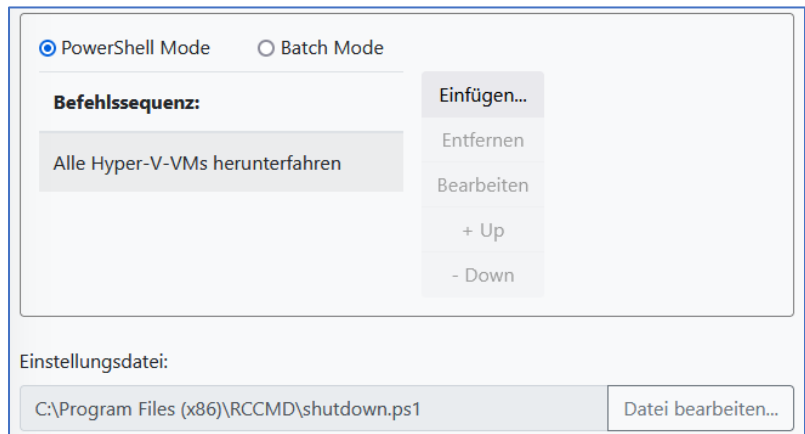
With more complex structures and your own scripts, always pay attention to possible mutual dependencies and rights management, which is strongly influenced by the operating system.

Windows ONLY:The PowerShell / BATCH – Mode Switch

Please note:

This function is available exclusively for Windows from RCCMD version 4.57.12 240429.

If your Windows version of RCCMD does not display this function, please update to the latest version of RCCMD

The Windows PowerShell mode allows you to choose between the familiar BATCH mode and the modern Windows PowerShell within Windows operating systems.

In both cases, preconfigured commands are available under "Insert".

Experienced system integrators can use the integrated data manager (Edit file) to directly adapt the included PowerShell script to their requirements for a structured system shutdown and thus automatically and structurally shut down even complex Hyper-V cluster structures with an RCCMD.

Tipp: Introduction and short tutorial to the Windows Power Shell

An introduction to Windows PowerShell can be found in Chapter 8, Getting started with RCCMD with Windows PowerShell and Hyper-V
To go directly to the corresponding chapter, -> **Click here** <-

---

Notification Settings

These batch files control the internal configuration of your RCCMD installation and determine which executable jobs as well as additional custom scripts. Via the build-in editor, they can be extended to implement additional functions and can even control complex script sequences.

Please note: These files are very sensitive!

1. The modification of the pre-set batch files is at your own risk. By changing the parameters and extending these files, you will change the basic behaviour of the RCCMD client.
2. Make a backup copy of the original file before modifying!
3. Do not rename the files - RCCMD will not be able to find them.

At this point, RCCMD uses different groups of commands that can be received. Depending on which command you send from a valid RCCMD transmitter to this client, one of these three scripts is started first.

Message Notification   This is the script that controls the RCCMD Alarm Box, which gives you this beautiful window of notices on the screen. As soon as you receive messages from a CS141, this file is called.

Execute Notification   This script accepts RCCMD commands when commands are to be executed that start programmes or scripts.

Note
These are the initial scripts within RCCMD! As soon as you send a "Custom Command", e.g., to start the batch file HalloWorld.bat, the "Execution Notation" n organizes to run the according file - Whatever is added by user will be generally executed on calling and cannot be restricted to certain "jobs".

Advanced Settings

Event Log File

Specify how many KB the log file may become before RCCMD starts to overwrite the oldest entry. The following scheme is followed:
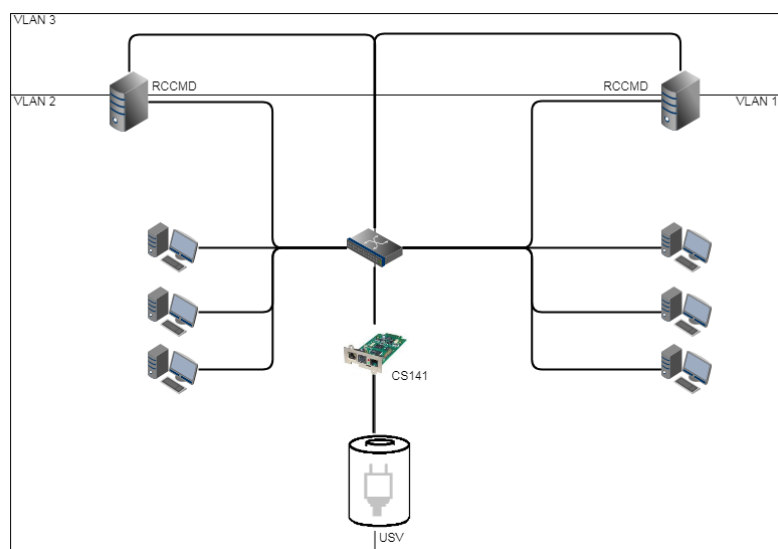
Entry 1 -> This entry will be removed.
Entry 2
Entry 3
Entry 4 -> This entry will be added

RCCMD logfiles will be read from top. The first entry is generally the oldest available entry and the most recent entry at the bottom of the event list.
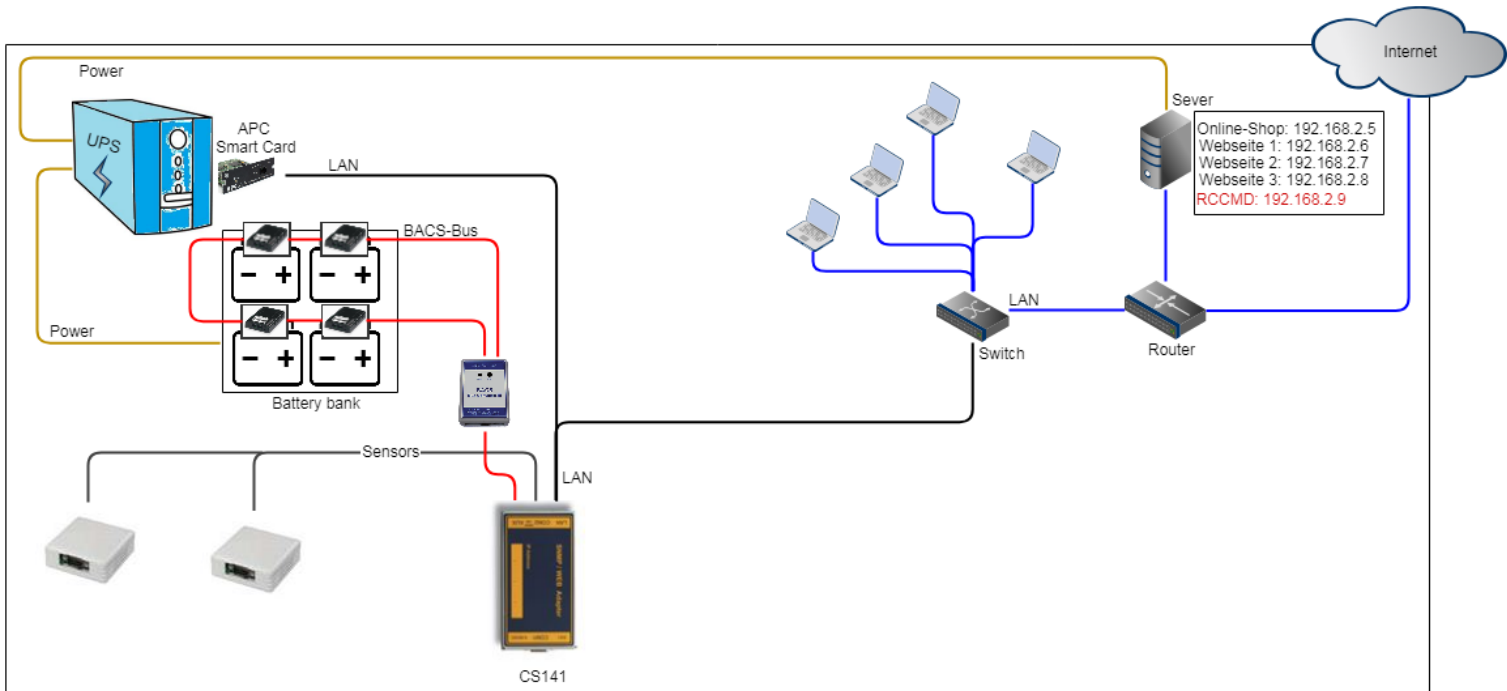
RCCMD Bindings

RCCMD Bindings is a sophisticated tool that helps you to limit traffic. Since this setting deeply affects your network setting, it should be used with caution. The bindings allow forcing RCCMD to listen on a specific network card. In case of multihoming is in use, the listener can be configured to a specific IP address within one network card. As an example, this will be used if there is a necessity to divide the network logically into a production network and an infrastructure network via VLAN:

In this example scenario, two or more network adapters can be installed. Binding RCCMD to one specific network card will prevent users to access the RCCMD client and accidentally shut down a server - this is only possible via devices that are located in VLAN 3 or have been properly enabled via a router.

Another scenario is the so-called "multihoming":

It is not absolutely necessary for modern network devices that an IP address is firmly linked to one network interface. In fact, multiple IP addresses can be connected via a network interface - they share hardware, but otherwise form self-contained instances. As an example, this could be a web server that manages different websites with a unique IP address: the server is connected by a router that determines between incoming signals and signals provided by local network. Bindings will instruct RCCMD to listen for incoming RCCMD signals only at a specific IP address that is assigned to the local network only.

Note

These configurations are used in special scenarios. Normally you can leave the setting 127.0.0.1 / local host, port 6003. In that case, RCCMD will listen on all available IP addresses for a valid incoming signal. Since you have defined the valid sender address at the menu Connections, RCCMD will notice the signal but deny execution and log this fact as an invalid RCCMD command.

Message Port

Normally, RCCMD is a background service that is not allowed to show messages on the display. For this purpose, the RCCMD service passes the information to the "Web-If", which is registered as a foreground process and therefore authorized to interact with a user and trigger or initiate foreground processes.

> *Special function: Running a job as interactive user*
>
> *This function allows RCCMD to interact with the system as a foreground process with the rights of the currently logged-in user. The operating condition is that at least one user must be logged in to execute a command. Which commands and scripts can be executed depend on the system rights of the according user.*

RCCMD License

Each RCCMD installation requires a corresponding license. If you do not have a license at hand when starting, a 30-day demonstration license will start automatically. After that, RCCMD will stop until you have entered a valid license.

Please note that RCCMD clients in the network coordinate with each other: If you have issued a duplicate license, only the first installation claiming the license will run. The other clients will disable RCCMD service with a license fraud message in the event log.

Web access
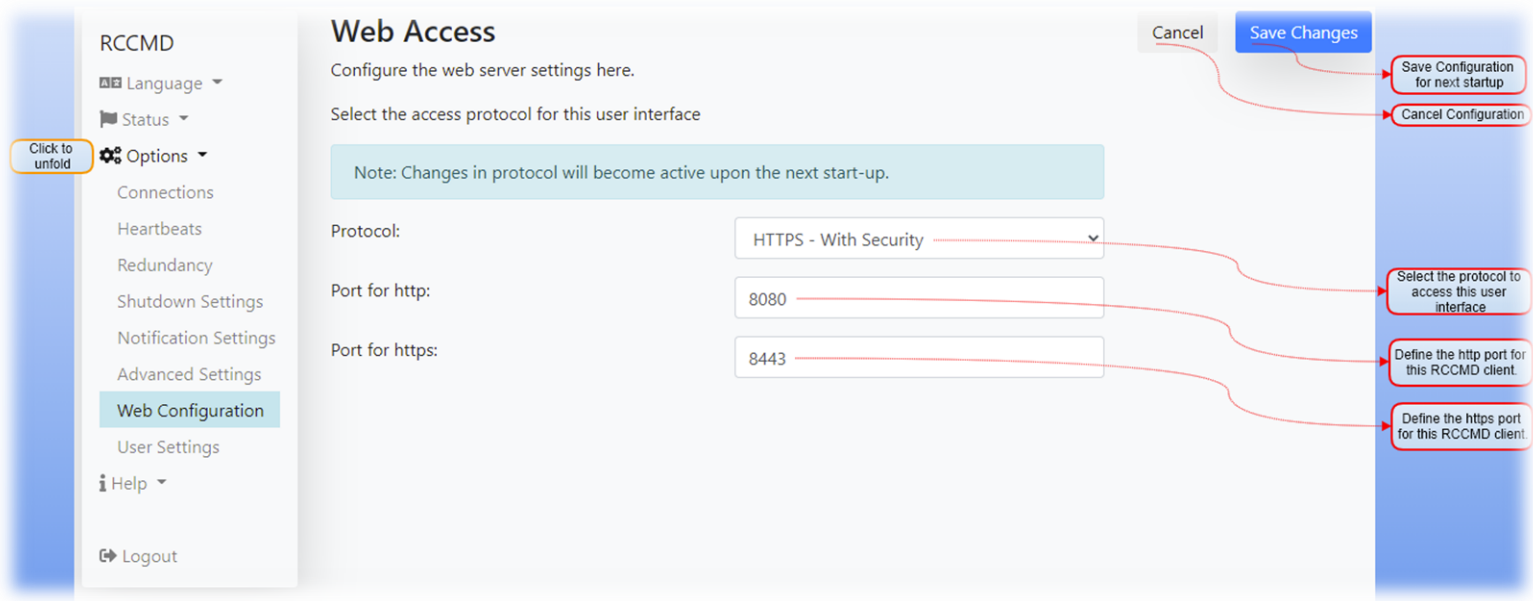
Web Interface configuration

The web access settings allow users to configure an individual access method and define the access ports. The RCCMD web interface will only respond to these queries.

Default settings:

Protocol (choose an option):	HTTP / HTTPS
Default port for http:	8080
Default port for https:	8443

Save / Restore Configuration

For this function RCCMD version v 4.49.12 231011 *or later is required*

Important: Version 4.49 introduces some changes for backup/restore

New directory at RCCMD: customfiles

RCCMD has always supported for users to launch their own scripts within the RCCMD application. With the introduction of the BACKUP / RESTORE solution, a new folder for your own scripts was introduced:
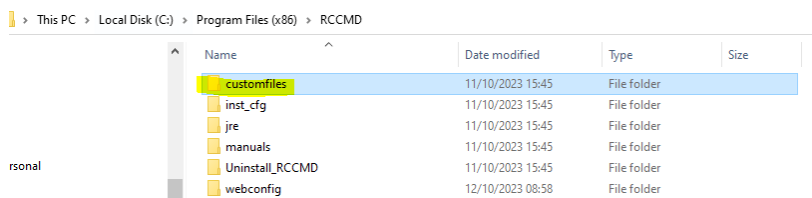
The backup not only includes the configurations used by RCCMD itself, but with version 4.49, everything you store under custom files* will be backed up and restored when you import the backup. This enables quick and convenient restoration of configurations. *Wie starte ich meine custom files aus dem Ordner customfiles*

Since the "customfiles" folder is a subfolder of the RCCMD installation, the CS141 will need a relative path name to run in the "RCCMD Execute" job in the future. For the Windows script helloworld.bat, for example, this start would look like this:

/customfiles/helloworld.bat

RCCMD will then search for the specified batch file in the "customfiles" subfolder and run it with local admin rights. However, if you store the start script in the RCCMD installation directory, the old spelling remains:

helloworld.bat

If the batch file is in the RCCMD installation directory, RCCMD will then start it directly.

How to create a backup file or restore the backup?

1. *Click „Backup"*

    RCCMD will generate and provide a clearly marked zipped backup file for download.

    > **Tip: Limited storage space in the "customfiles" folder: 20 MB**
    >
    > The backup function does not differ between file types, so you can store any information there - including special maintenance instructions, network plans, short documentation, etc. - So when you reinstall RCCMD, you have all the information bundled in one place. The only thing to note is that the folder must not be larger than 20 MB. If this is the case, there will be a corresponding error message when creating the backup.

2. *Place the zipped file as downloaded into the specified box as saved and click "Restore"*

    The integrated backup program will unzip the zip file and restore all configurations, including any self-created certificates. It should be noted that RCCMD recognizes backups and if there is an incorrect backup file:

    Depending on whether you try to import a backup Linux <-> VMware or Linux / Vmware <-> Windows, you will get one of the two error messages.

Update Web server certificate

The integrated web server can be configured to follow up company SSL / TLS certificates. For the required pem-file, refer to the local IT department. This function will be used to encrypt the communication between the web interface of the RCCMD installation and the web browser.
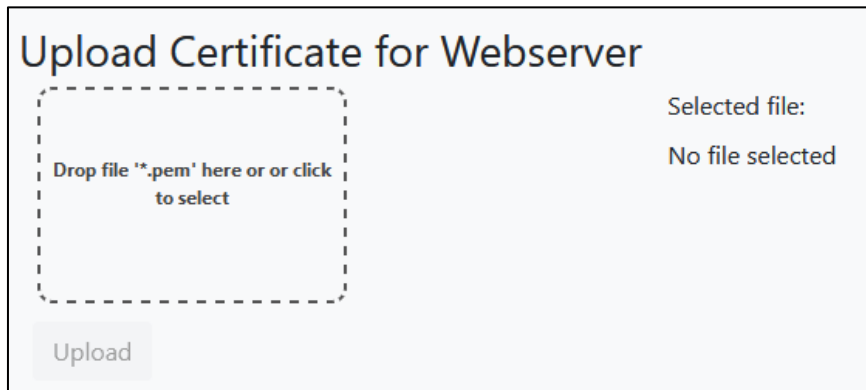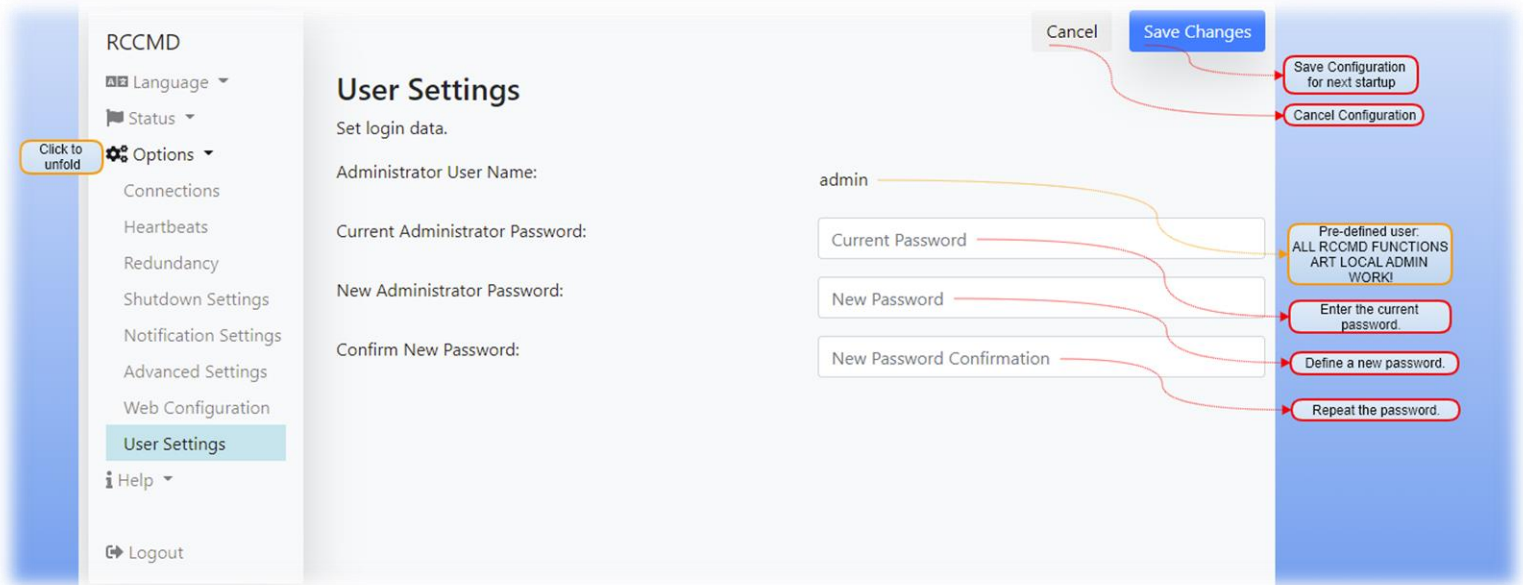

TLS certificate update function:

1. Create a backup file before using this function
2. Place the *.pem file in the according upload box
3. Click upload
4. Restart RCCMD at System status.

The Web browser should now show your own certificate. If your web browser can not access the web interface, re-install RCCMD and check the certificate.

User Settings:

Unlike the CS141, RCCMD only contains a pre-defined and hard-coded user. The password can be adjusted at any time to fit to password policies of any company:

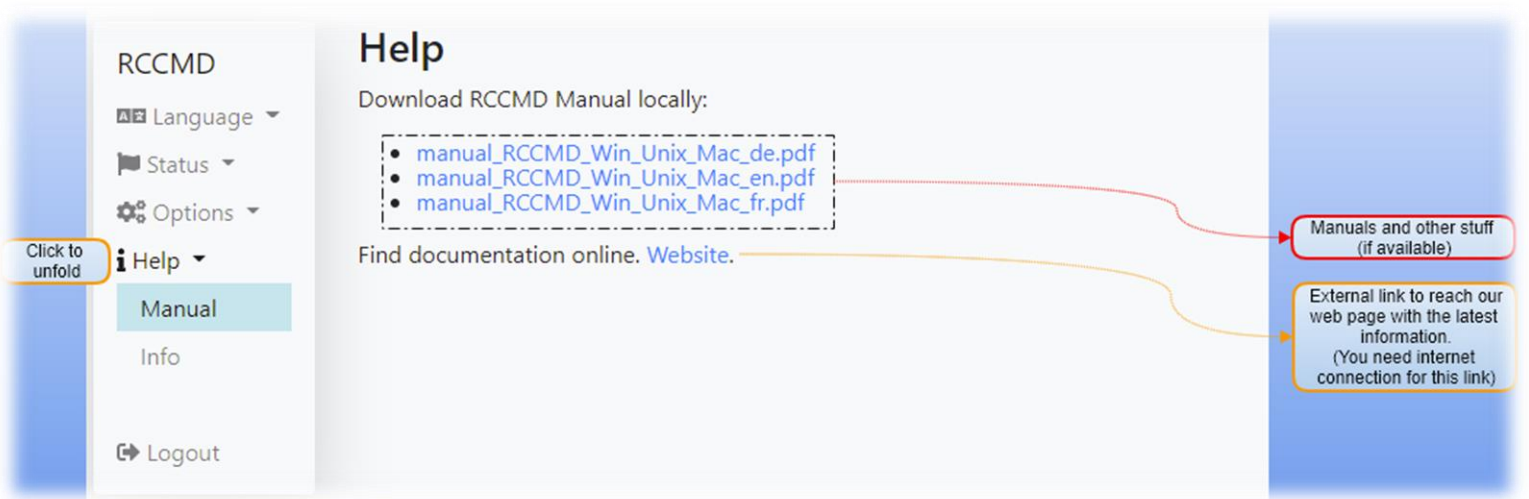*Current Administrator Password:*   *The password you are using for login.*

New Administrator Password: *change the password*

Confirm New Password: *To ensure that your new password does not contain a typo, you need to repeat it.*
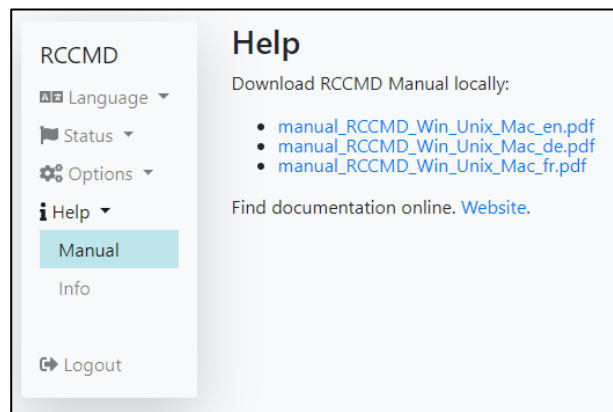
Help

Manual

You need help?

The manuals are available inside RCCMD – you do not need any additional network connection.

Due to the fact the manual is a pdf-file you may need additional software tools to open the according file.
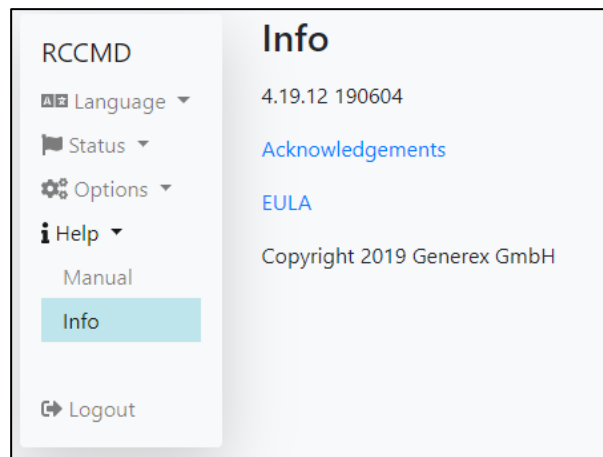

Info

Need additional information about your copy of RCCMD?

The info button will show

- Acknowledgements
- EULA
- Copyrights

7.2 Die RCCMD – Die Appliance – Options oft he web interface in Detail

In the following, we will introduce you to the functional elements of the RCCMD appliance and explain the setting options available on the RCCMD web interface.

System tab Language

For language options, select the system tab "Language
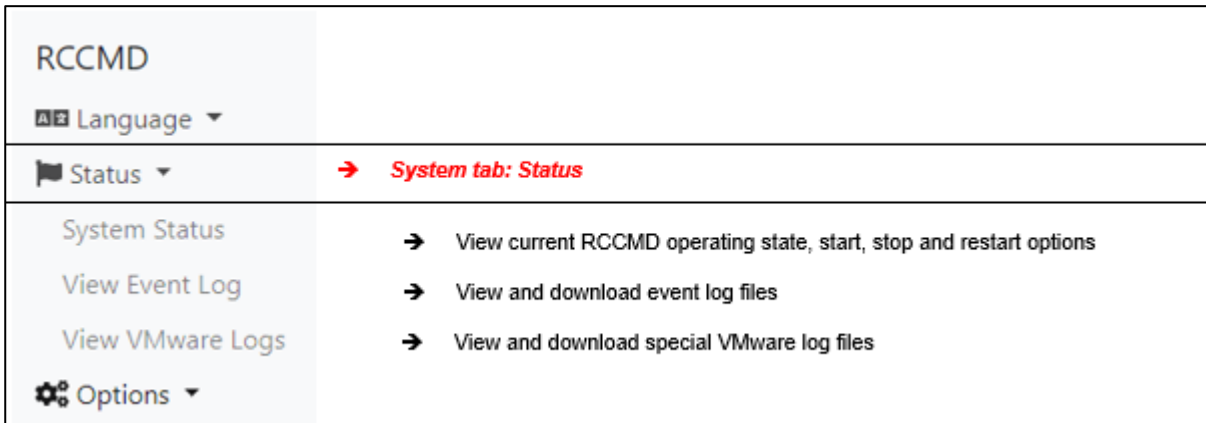

RCCMD supports the languages German, English and French.

To switch to the corresponding language pack, select the appropriate language. RCCMD will switch to the language at once without a restart.

<u>*System tab: Status*</u>

This menu contains general information about the RCCMD operating state and all available log files.

System Status

The system status is an interactive dialog which provides immediate information about the current operating status of RCCMD:

The buttons provide the following actions:

Start   Starts RCCMD when stopped
Stop   Stops RCCMD when starts
Restart   Stops and Restart RCCMD
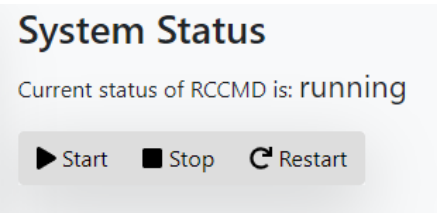
Depending on the current action, the Current status of RCCMD will be shown:

Not running

RCCMD is disabled and will not protect your server.

Running

RCCMD is online and waits for incoming signals.

The peculiarity of this function

All settings during configuration will be cached temporarily, RCCMD will continue to work in the background with the configuration of the last system start.

To activate the new configuration, it is mandatory to stop, start or restart the RCCMD service.

System tab: Event Log

2019-06-13	13:41:12	rccmd[09099]: system: Operation now in progress
2019-06-13	14:10:42	rccmd[09099]: Trying to start program/job: /usr/rccmd/rccmd_notalive.sh 192.168.2.1 06/13/2019 14:10:42
2019-06-13	14:10:42	rccmd[09099]: error: check upsman failed, could not connect to 192.168.2.1
2019-06-13	14:10:42	rccmd[09099]: system: Operation now in progress
2019-06-13	14:10:57	rccmd[09099]: Trying to start program/job: /usr/rccmd/rccmd_notalive.sh 192.168.2.2 06/13/2019 14:10:57
2019-06-13	14:10:57	rccmd[09099]: error: check upsman failed, could not connect to 192.168.2.2
2019-06-13	14:10:57	rccmd[09099]: system: Operation now in progress
2019-06-13	14:11:12	rccmd[09099]: Trying to start program/job: /usr/rccmd/rccmd_notalive.sh 192.168.2.3 06/13/2019 14:11:12
2019-06-13	14:11:12	rccmd[09099]: error: check upsman failed, could not connect to 192.168.2.3

RCCMD logs events concerning the RCCMD service:

- Notifications
- System Events
- Actions
- Executed scripts

RCCMD logging includes these information

- Date of the event
- Time when the event arrived
- IP address of the sending device
- Success / failure while executing a job

Using this event report, complex event chains can be traced back in individual steps and evaluated in conjunction with the event logs of the associated CS141.

By doing so, it is possible to track:

- When a server shuts down
- Why a server shuts down
- How fast a system reacted to an incident.

Event reports help to break down complicate issues and may show futural problems.

Downloading an event log

Larger companies require regular status reports on IT security.

RCCMD therefore allows you to download and export the log files to a CSV file that is integra table into external monitoring systems and databases.

You will find the download link below the last log entry:

2019-07-03	13:01:04	rccmd[30251]: UPSMAN/RCCMD Evaluation version - testing purpose only,
2019-07-03	13:01:04	rccmd[30251]: V4.3.0.6 - Unix Remote Command Program
2019-07-03	13:01:04	rccmd[30256]: Listen Mode started.
2019-07-03	13:01:04	rccmd[30256]: RcvThreadUdp started

Download Event log file

System tab: View VMware Logs

The RCCMD Appliance provides extensive log files to assist with the recovery of an incident.

RCCMD logs the following information:

-    Date
-    Time
-    Received signals
-    Own communication attempts
-    Executed scripts
-    Dry run results

Depending on the depth of detail of the evaluations, you can use these log files to trace the path of a shutdown even over complex network nodes and compare them with other log files.

System tab: Options

Under Options, you will find all the settings you need to configure RCCMD.

RCCMD	
🔤 Language ▼	
🚩 Status ▼	
⚙️ Options ▼	➜ **System tab: Options**
Connections	➜ Configure valid RCCMD sending device
Heartbeats	➜ Configure if RCCMD shall perform an availability test for connected devices
Redundancy	➜ Configure the redundancy mode
Notification Settings	➜ Edit the basic RCCMD scripts who trigger all RCCMD actions
VMware Settings	➜ Configure the VMWare settings for vCenter, vSAN and ESXi hosts
Advanced Settings	➜ Configure log file size, the RCCMD key as well as RCCMD bindings for multihoming
Web Configuration	➜ Configure the web access security level Backup & Restore
User Settings	➜ Change the password of your RCCMD installation
ℹ️ Help ▼	
➡️ Logout	

System tab: Connections

Define the permitted inbound connections

If you leave this field empty, all incoming RCCMD shutdown signals may trigger a shutdown.
As a surprise, this is an unfavourable condition that should be changed. By entering a sender IP, you limit which devices are in principle authorized to send a command to this RCCMD client.

RCCMD commands from unauthorized devices are logged, but the RCCMD denies an execution.

The Connections configuration dialog

Insert and Edit

With insert, add a new IP address.

Save Changes will add the IP addrss to IP white list. Close aborts the process and exits the configuration dialog. Repeat the process until all RCCMD authorized stations have been recorded.

If the settings change over time, they can be edited:

Select an IP address and press Edit. The selected IP address is offered to you in the configuration dialog and can be changed by you according to your ideas. Save Changes complete the process.

Close cancels the process and terminates the configuration dialog.

Valid is both, the IP address of the sender as well as a valid host name

Working with hostnames is always tricky:

you also need a DNS server for translation between hostname and IP address this hostname is associated with. If the DNS server is down or the communication to the server is broken, RCCMD will not be able to contact the according host and manage a shut down.

RCCMD supports host names, but in order to avoid the issue described above, we recommend to use an IP address.

RCCMD is a client that will always wait for an incoming signal! You need to configure an RCCMD sender like the CS141 Web manager:

At UPS event management, select as job *RCCMD Shutdown* – you may choose between the IP address or the host name of the RCCMD client.

In critical resource management, it is advisable to eliminate as many interfering possibilities as possible.

As an example, if you need a server that can resolve the hostnames into IP addresses, the communication between client and sender will stop working as soon as the server is unavailable.

Therefore, the general recommendation is to use a manual IP addresses: by doing so, all devices inside a network segment can communicate with each other without additional server.

Note

If you configure the CS141 and want to see if the jobs you have configured are correctly received by RCCMD, you can use connections to create an inbound log. As long as the sender is not explicitly included in Connections, RCCMD will log the execution but refuse to execute it.

However, at least one IP address must be entered in order to activate this filter function.

Preparing UPS redundancy

Some settings depend on each other. If you have several UPS systems paired in operation in order to secure the server infrastructure, it may be necessary to specify more than one UPS to trigger a shutdown command.

If you enter two or more valid IP addresses for a valid RCCMD signal, the "Redundancy" menu is automatically activated and can be used.

RCCMD can be configured to manage valid RCCMD shutdown signals from different sources. For details, refer to the menu "Redundancy".

How to delete an IP address

Click on the IP address and press Remove.
This will delete the IP address.

Remember to press Save changes at the upper right position to save your settings permanently.

Increase the connection security

Protocol

The setting below increases the security of connections to this RCCMD

☐ Accept only SSL connections (requires restarting RCCMD)

☐ Reject expired SSL certificates

This feature adds security to your network, but conversely also increases administration overhead:

You can instruct the RCCMD to explicitly accept SSL-encrypted communication with a valid certificate.
If a sender does not have an SSL certificate to identify itself, the connection is terminated.

In addition to this feature, you can instruct RCCMD to check SSL certificates are up-to-date. If the certificate becomes expired, it is considered invalid and the connection is terminated accordingly.

Note

Surely you have already noticed how often we point out that the save function changes the colour.

| Cancel | Save Changes |

If you enter or change data within a configuration dialog,
data are saved temporary, without any impact on current configuration.
If your configuration work is done, you need to write your local settings to the RCCMD configuration file.

To activate the new configuration, RCCMD needs to be restarted - just press at Status stop / start or restart. RCCMD will re-read the new configuration and take over the new configuration.

System tab: Heartbeats

The heartbeats' function provides an availability lookup. The communication between RCCMD client and the associated server can be monitored and logged:

RCCMD
- Language ▾
- Status ▾
- Options ▾
  - Connections
  - Heartbeats
  - Redundancy
  - Notification Settings
  - VMware Settings
  - Advanced Settings
  - Web Configuration
  - User Settings
- Help ▾
- Logout

Heartbeats

The UPS alive check can be used to monitor the availability of each sender.

☑ Enable automatic UPS alive check

○ by the use of CS121 / UPSMAN Traps

◉ by polling CS121 / UPSMAN every: 1800 seconds

and retry each failed connection: 5 times

When the alive check fails, then RCCMD will use the following setting:

/usr/rccmd/rccmd_notalive.sh [Edit File...]

Test UPS connections: [Run alive check now...]

[Cancel] [Save Changes]

In principle, two basic sources of interference are checked:

1. The general network accessibility
2. The UPSMan service of the CS141

This test is not designed to run complex network diagnostics. RCCMD can use this test to find out if the RCCMD signal sending device is available and as well as working properly.

The RCCMD client offers two basic options:

- Automatic mode

You can choose between two different options:

UPSMAN Traps

An RCCMD server sends a trap message to the RCCMD client. The receipt of this message is logged accordingly.

By Polling

The RCCMD client cyclically requests a message from the RCCMD server and logs the reachability of the remote station. In case of connection lost, the queries can be repeated as often as configured. If polling ends unsuccessful, an automatic script can be started.

This script can be customized freely to needs. With Edit File ... you can directly adapt the file in the web browser.

To edit this file, Linux scripting knowledge is mandatory.

When the alive check fails, then RCCMD will use the following setting:
Run this command file : /usr/rccmd/rccmd_notalive.sh

your edit and

/usr/rccmd/rccmd_notalive.sh

/usr/rccmd/rccmd_notalive.sh

```
#!/bin/sh

# rccmd_notalive.sh - This script is called by rccmd if the
# connection attempt to upsman/upstcp fails.

# available parameters are:
```

Abort   Save Changes

The Manual mode

With Test UPS connections, RCCMD provides a tool that enables quick accessibility lookup test.

Run alive check now ...

opens an additional window. All RCCMD devices entered at Connections are listed and will be queried.

Lack of communication readiness and missing availability will be displayed accordingly:

RCCMD - UPS alive check

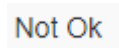| CS121 / UPSMAN addresses	Alive result
192.168.200.17	↻
192.168.222.104	Ok
192.168.222.107	Ok

Ok

↻   … Testing in progress

Ok   … Testing complete, device is available und UPSMan service is running

Not Ok   … Testing complete, device not found.

Please note: RCCMD will show the result for information and troubleshooting purposes.

An Alive Check may fail under the following conditions:

- Network failure or broken infrastructure
- Target device is switched off
- Locked or misconfigured ports
- incorrect routing
- UPSMan service does not answer

Unlike automatic polling, no automatic script is executed on failure, as RCCMD assumes that an authorized administrator is monitoring this manual lookup process.

Please note that the configuration will only take effect after you have pressed the green Save Changes, as the RCCMD Client must be restarted for this function.
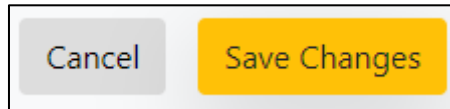
System tab: Redundancy

The redundancy behaviour depends on the settings of Connections and Heartbeats:

For the redundancy behaviour to work properly, two preconditions must be met:

1. Two valid IP addresses must be specified under Connections.

At least two IP addresses must be stored and allow inbound RCCMD commands.
Redundancy means, RCCMD should not shutdown the server until at least two transmitters have instructed to power down the host.

2. The heartbeats must be set to "Automatic UPS alive check by polling"

RCCMD is instructed by the heartbeats to automatically check the availability of registered IP addresses:
Should a registered UPS become unreachable and the redundancy system shuts down, RCCMD will assume that there is a serious problem and shut down the system ignoring the redundancy setting.

Note:
Keep in mind that the intervals between lookups can be crucial for a shutdown.

Note: The redundancy behaviour refers exclusively to the RCCMD command shutdown

Other commands are handled individually and logged accordingly. With the ability to run your own scripts, RCCMD offers options to bypass the standard procedures in case of an emergency.

Defining redundancy levels

First activate the RCCMD redundancy function.
Then select the IP addresses that are allowed to send a shutdown signal.

The Redundancy Level is depending on the number of selected devices:

Number of selected units X -1

By using two devices, both need to send an RCCMD shutdown signal. Since only two systems have been selected, only a maximum of one additional system can send this command. Thereby it is not important, which device is the first sender - this may change dynamically.

For 3 selected systems, the maximum value is 2:

If 1 unit + 2 other units instruct the shutdown, it will be executed. RCCMD does not differ which of the three systems sends the first shutdown.

Using 3 systems, you can also change the Redundancy Level to 1:

As a consequence, two out of three systems are needed for RCCMD to shut down the server. The combination may change dynamically. If you just want to pair 2 of 3 UPS systems, it is recommendable to select them and set the redundancy level to 1. By doing so, the shutdown will only be done if both selected UPS's will send a shutdown command.

Keep in mind:

With redundance, you combine several devices. Under connections, you allow general incoming shut down signals. As a consequence, it is possible to configure one redundancy shutdown as well as several single shutdown senders.
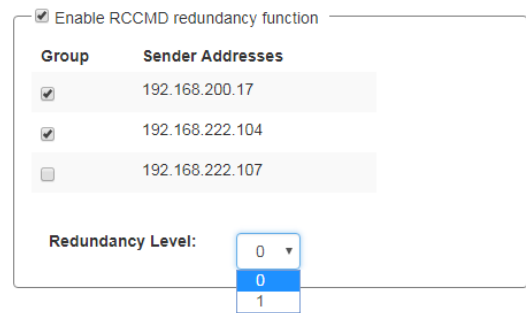
Note
Please keep in mind that a shutdown instruction remains active until the system which has instructed the shutdown explicitly withdraws it. This is controlled via the RCCMD Custom Command *wakeup*.

Shutdown behaviour with two UPS systems

In case of a shutdown signal, The redundancy will check the connectivity and the availability of the second UPS system are. If it answers properly, the shutdown signal will be suppressed with reservation until further notice:

2018/05/25 - 10:46:55
Alarm! RCCMD Shutdown Signal received - Shutdown is pending as long as redundancy is present.

As soon as the second system instructs a shutdown, this command is executed and the system shuts down. If a shutdown signal is sent by the first system and the second system is not reachable, RCCMD shuts down the system - in this case, RCCMD assumes that the second system is not available.

Shutdown behaviour with three valid devices

From three devices onwards, the redundancy behaviour can be individually adjusted to necessary conditions:

1. If one of three systems send a shutdown
2. When two out of three systems send a shutdown
3. All three systems must decide the shutdown together.

Each system can individually instruct and withdraw its shutdown via the RCCMD Custom command wakeup. In general, RCCMD will not execute the shutdown until the exact shutdown condition is met.
Redundancy-related scripting

If you use redundancy behaviour, the RCCMD client waits to execute the shutdown until the appropriate number of devices also instruct the shutdown.

When redundancy supresses a shutdown, then RCCMD will use the following setting:

Run this command file : /usr/rccmd/ShutdownSuppressed.sh   Edit File...

Because this process has a direct impact on the operation of the servers being monitored by RCCMD, a script will be launched to indicate an incident.

Use Edit File ... to customize and adapt this script to your individual requirements.

Abort will close the editor and withdraw all changes you made.

As a default, a text notification is pre-defined to indicate a redundancy-based shutdown behaviour.

System tab: Notification Settings

Depending on which command is received by a valid RCCMD transmitter, three basic scripts are executed automatically. Each script triggers an RCCMD functions. The RCCMD routines are preconfigured and normally there is no need to edit them.

However, if you want to execute your own scripts by RCCMD,

you can either write these scripts directly to the appropriate .sh - script and execute them as a custom command or you may edit these basic files.

Warming:

If you modify, customize, or extend these scripts, you change the overall behaviour of RCCMD within your system. Be sure to make a backup before editing the scripts to find back to the original system state. Changes to the original configuration may result in unpredictable behaviour of RCCMD and may cause system-wide problems.

Edit these scripts at your own risk!

When will these scripts be executed?

RCCMD differs between two different scripts:

Message Notification

This script controls the receipt of messages and is responsible for displaying them on the monitor. Because the RCCMD appliance is a non-graphical server program that runs without permanent a permanent monitoring, you should leave this script simple as it is:

Since it is triggered by each incoming RCCMD notification signal, additional content would also be executed each time.

Due to the fact, this is mostly without a function (no graphical interface) you may use it for routine scripting

> ➔ changing the complete script will cause changing the behaviour and may cause RCCMD will not run as expected.
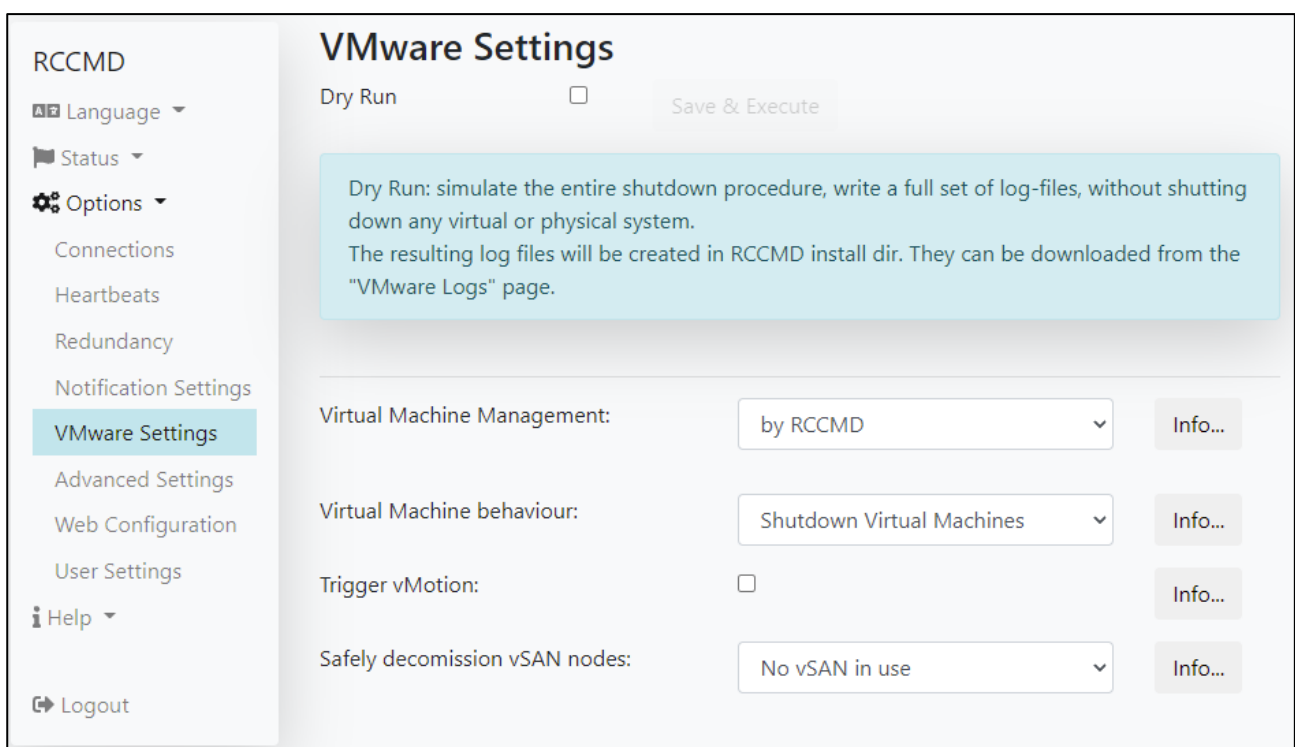> ➔ Edit it at your own risk.

Execute Notification

This script is interesting:

This script executes all valid incoming commands a CS141 may send. This script triggers the complete shutdown routine RCCMD provides

With this script, RCCMD will provide you the unique option to add and trigger your very own customized shutdown scripting solution and even program an additional non-standard routine that specifically met exactly your network.

> ➔ This script is a very powerful option as well as dangerous because changes directly interfere with all functions of the RCCMD. Any changes and enhancements you make will directly affect the shutdown behaviour.
> ➔ Advanced scripting skills in Linux are essential for changes to this script!

System tab: VMWare Settings

The VMWare settings control the overall shutdown behaviour of servers and hosts within VMware. Depending on the configuration level and configuration type, different types of configurations are necessary in order to manage a VMware based infrastructure. In addition to the mandatory basic data like IP addresses user credentials, you may need, among other things, more specific knowledge about the shutdown behaviour of your IT landscape.

Please note, some data are not static. Values may change and should be adjusted during regular system checks.

> ➔ RCCMD evaluates and displays estimated shutdown times according to entered data.

Part 1: Basic setup

The basic settings assume that you are running hosts without vCenter. You can shut down as many hosts as you want with one RCCMD appliance:

Virtual Machine Management

This menu defines whether you want the hosts and virtual machines to be managed by RCCMD or by a vCenter. If you operate the hosts in lock-down mode, e.g., the control commands are exclusively approved by a vCenter. Even if you enter the credentials correctly, the host will deny command execution.

In the default setting, "from RCCMD" is active.

Virtual machine behaviour

Use this setting to define whether you want to use vMotion or just shut down your machines. A virtual machine shutdown will be controlled directly by the host:

the virtual machines are shut down normally, and then the host are turned off.

If you enable vMotion, local shutdown of virtual machines is the secondary protocol. First, the vCenter will try to move the virtual machines to another host.

The default setting is "Shut down virtual machines".

➔ If maintenance mode is selected, additional information is required like credentials of the vCenter as well as a time window that should be available for the vCenter to move virtual machines to another host.

Safely decommission vSAN nodes auf no vSAN in use

This setting defines the shutdown behaviour in case of a vSAN is in use - The vCenter provides different basic settings, to be selected at this configuration point. If you want to use an RCCMD-managed vSAN, refer to the basic requirements that must be met.

The default setting is "No vSAN in use".

VMware running RCCMD

RCCMD needs to know the name of the virtual machine that contains the RCCMD appliance. This setting prevents a shutdown of the RCCMD Client.

The virtual machine that runs RCCMD must not be shutdown. Or else RCCMD cannot shutdown the other virtual machines and hosts. Enter the virtual machine's name on which RCCMD runs.

VM running RCCMD: hayabusa

Tell RCCMD all ESXi Hosts to shut down

Add...   Remove   Edit...   Verify

ESXi Hosts to shutdown

| ESXi Address	Shutdown duration	Verified
192.168.200.107	30 Seconds	
192.168.200.124	30 Seconds	

With this configuration dialog, declare which ESXi hosts has to be shut down by RCCMD:

The menu bar provides several functions:

- Add: Add another host. To remove a host
- Remove: Select a host and click Remove to remove it from the current list
- Edit: Select a host. With Edit you can edit the access data.
- Verify: If you press this button, the current configuration will be saved and the login data will be validated. At verified, RCCMD shows the connection attempt.

Estimated shutdown time

After the configuration job is done, RCCMD shows an estimated shutdown time:

Total estimated Shutdown time for the System with current configuration: 00:03:30.
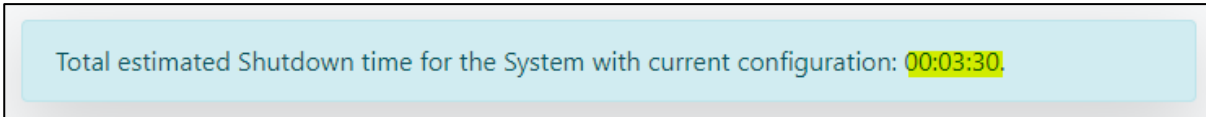
This is the current average shut down time of your IT infrastructure. Please note, this shut down time is calculated and can be used to compare it with the the emergency power time granted by the UPS.

Due to the fact this is a calculated value: Please test you shutdown setting before activating!

Dry Run installation test routine

VMware Settings

Dry Run ☑ Save & Execute
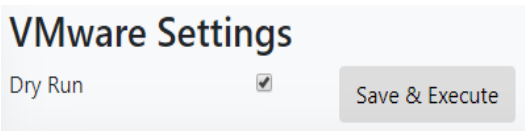
With the Dry Run RCCMD offers a unique function within the VMware settings:

The Dry Run is a simulation mode, in which your RCCMD installations simulate the behavior, but do not physically execute.

This feature is useful when installing an RCCMD installation on a production server:

Accidental shutdown is prevented in this way. With Save and Execute, this feature is enabled, protecting your future configuration from accidental shutdown.

Dry run... ✕

simulated shutdown running. Log files can be downloaded after simulation has finished.

Ok
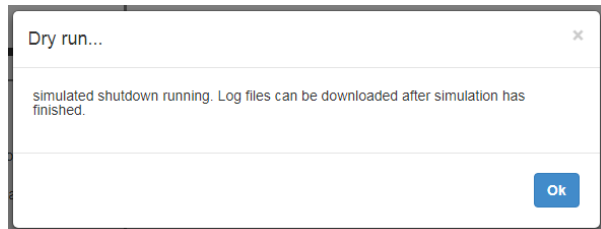
Note

Some configuration menus are locked during testing and cannot be adjusted "in between".

What a „Dry run "does …
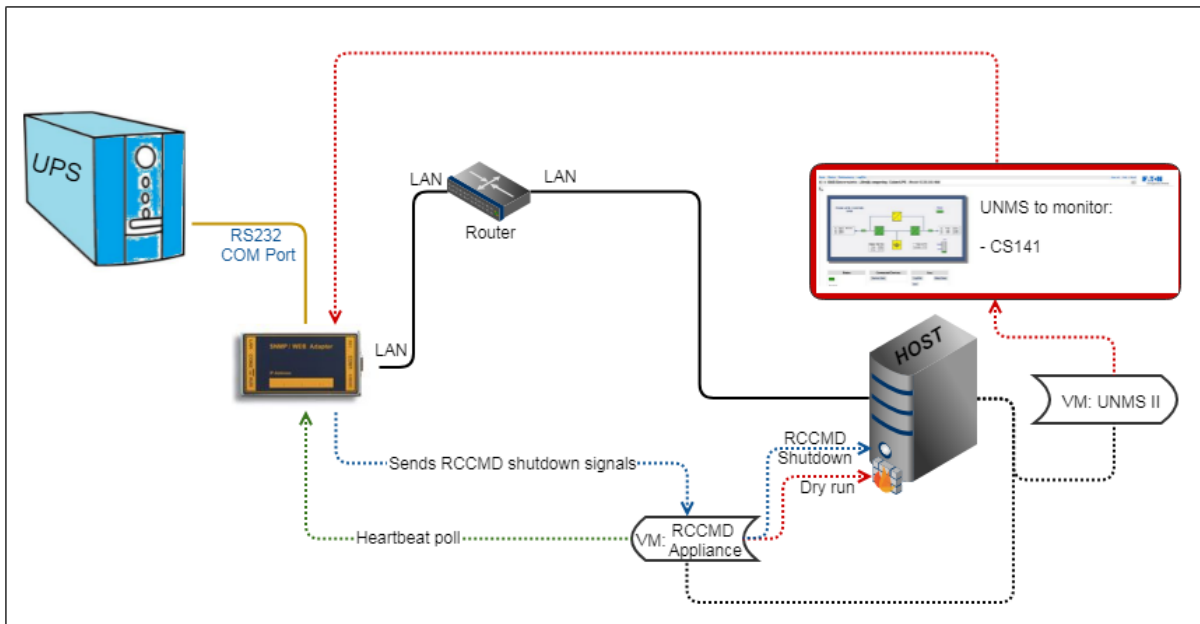
Normally, a CS141 is the RCCMD server that sends a valid RCCMD command to an RCCMD client - the RCCMD software. The command and what to trigger with it depends on the final operating scenario. Due to the fact you can use the event handling from the CS141 for sending individual commands in order to start very delicate and complex scripts, it is possible to automate a server via scripts in many parts - you do not necessarily just have to shut down a server with RCCMD.

With VMware, the RCCMD appliance differs from normal client installation:

It is designed to ensure a structured shut down sequence for all hosts within a VMware environment-

To fulfil this task, RCMMD needs access data coming with system rights to allow a shutdown. The problem that RCCMD cannot differ between a real emergency and a user who press the test job - button at CS141. During testing, this is could be a problem. As soon as RCCMD will accept a valid signal, it will start the shutdown procedure - It is comparable with the quite "OK" - console command of any normally shown „Are you sure " - Dialog inside an operating system.

Of course, you cannot simply shut down "all servers" during operation because you want to test your configuration - shutting down a real-time system with 100% availability is just for real emergency issues....

The dry run is a build-in self-running simulation mode

1. All configured hosts will be contacted
2. Credentials for the hosts will be tested
3. a protocol log will be written to log configuration issues as well as successful login tests.
4. The standard RCCMD shutdown signal is suppressed as long as simulation mode is active.

As long as dry run is active, no emergency shutdown is possible via any valid RCCMD server device.

Note:

If you change or adjust the standard scripts coming with a default installation or add new scripts, they will be executed consequently. The Dry Run only suppress its own standard scripted shutdown sequence - it does not check the changes you added manually.

This behaviour contains advantages as well as disadvantages

1. Due to the fact your "sharp" scripts are executed mercilessly, the Dry Run test should take place beforehand!

2. By adding your own scripts that trigger harmless actions, you can check if your "sharp" scripts would work and all administrative shares on the target system are met.

Part 2: Advanced settings

If Maintenance Mode (vMotion) is selected

RCCMD will present two addition menu entries:

Maintenance Mode Timeout in Seconds

This value defines the time window that RCCMD grants the vCenter to move virtual machines to host that are not going down into maintenance mode.

Virtual machines that have not been migrated within this time window will be left for shut down by the ESXi host.

vCenter credentials

In order to use vMotion, RCCMD need valid vCenter credentials. Please note, an RCMD client can shut down many hotsts, but technically only maintain one vCenter. if you need to configure several different configuration types, it may be necessary to use 2 RCCMD appliances that work together.

Check values

Test the vCenter credentials. RCCMD will try to log into the vCenter and give feedback including a reason why the login attempt failed.

Part 3: Selecting "Host are also vSAN nodes" at vSAN Safely decommission vSAN nodes

Safely decomission vSAN nodes:	Hosts are also vSAN nodes ▾	Info...

This setting enables several sub menus and a vSAN time out warning.

vSAN Timeouts
Ensure all operations complete within their timeouts! Integrity of vSAN Objects will break if any timeout interrupts a running operation.

Mode for decomissioning vSAN nodes:	No data evacuation ▾	Info...
vSAN Resync timeout in Seconds:	200	Info...
Seconds to wait before setting Maintenance Mode for vSAN:	100	Info...

Keep an eye on this warning message!

A vSAN is a little bit tricky when running a shutdown routine and the vSAN has been terminated incorrectly. It is even possible that a wrong configured shutdown routine leads into data corruption or even total data loss.

vSAN shutdown options

No data evacuation

This is the fastest way to ensure system shutdown. It shuts down the virtual machines, and then the vCenter synchronizes all the hosts that are inside the vSAN. There will be no data migration or virtual machines to be moved to other hosts.

Evacuate all data to other hosts

In principle, it is the same function that triggers vMotion. A vSAN can also be spanned across different sites, so you can also offload virtual machines to external hosts that are not in the vSAN cluster you are about to shut down. if you use vMotion, it will be executed first. Due to this fact it is possible that your vSAN host has no virtual machines that need a migration. But you may use it as "second try" to move machines away from your vSAN...

Ensure data accessibility

If larger vSAN systems provide enough capacities for redundancies, no data will be moved. Data migration will only be done for data without redundancy.

Note

With vSAN extensions, RCCMD introduces solution to allow you performing an emergency shut down of the entire vSAN system as fast as possible - virtual machines that have been previously migrated to another location via vMotion are not affected.

Due to the fact you want to stop and shut down the vSAN because there is an emergency, selecting "No data evacuation" is the best choice.

---

vSAN Resync timeout in Seconds

This setting is the basic time window RCCMD grants the vCenter synchronize the databases between the hosts before starting the next point in the shutdown sequence. This time window is a little bit tricky, because the resync time is a very relative value - in principle you can say it lasts as long as it takes ... the vCenter does not tell you an estimated resync time, you need to test it during a manual shut down. If your vCenter announces the job is done, you have the minimum time window for your emergency shutdown. Please calculate some extra time for this time window because the measured time during a manual shutdown is just a snapshot and not a general value.

Seconds to wait before setting Maintenance Mode for vSAN

Once the resync is completed, the vCenter is the last surviving virtual machine that needs to be shut down. With this setting, you define how long the vCenter has time to shut itself down before RCCMD starts the next step of the shutdown sequence.

Determine which VM is running the vCenter

| VM running vCenter:	vcsa67 (2)

Inside a vSAN, the vCenter is more:

The vCenter manages the complete data transfer within a vSAN and handles the complete post synchronization phase during a vSAN shut down. This means:

If the vCenter runs inside a vSAN or runs on a host that will be shut down too fast, the complete vSAN hung up. If the vCenter is located as a virtual machine within the vSAN, RCCMD needs to know the name of the virtual machine in order to exclude it from virtual machine shutdown.

Note:

The vCenter that handles a vSAN is not always inside this cluster – it may be installed somewhere and handled separately. If the virtual machine with the vCenter is not inside the list of the hosts to be shut down, you do not need to enter it at this point. But you need to take an eye on it if when using different RCCMD appliances – Without it's vCenter, a vSAN cannot shut down as expected.

System Tab: VMware Shutdown Management
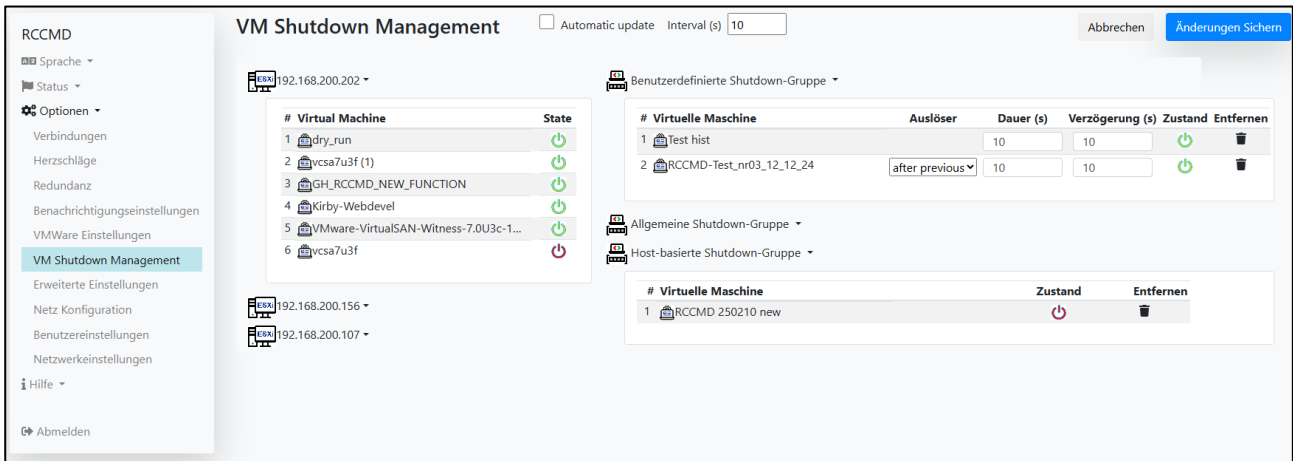
With „VMware Shutdown Management", RCCMD offers options to shut down virtual machines in direct relation to one another. To use this function, respective hosts must be configured and verified in the "VMware settings":

While the VMware settings trigger a global shutdown, in which all virtual machines shut down simultaneously, VMware Shutdown Management defines a mutual dependency between individual virtual machines in advance, as well as a clear shutdown sequence and provides an overview of respective operating status:

	The virtual machine is currently powered off. All data is backed up.
	The virtual machine is currently paused or in deep sleep mode.
	The virtual machine is running and will be affected by a power failure.
	The virtual machine stored in a static group could not be found. RCCMD will skip to the next entry according to the settings.
	Guest system: A virtual machine with this icon is a VM with any function.
	vCenter: A virtual machine with this icon is the vCenter for the respective cluster.
	The RCCMD appliance: This is the name assigned to the virtual machine.

All currently deployed virtual machines are mapped to the ESXi host, including their respective operating states. This list is updated in real time during a shutdown, so it should be possible to add a virtual machine later.
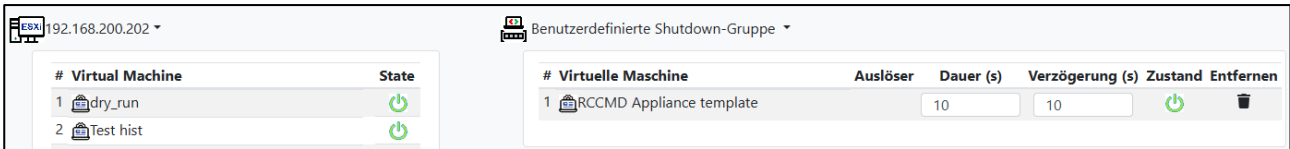
Adding and removing individual virtual machines

Adding:

To add a virtual machine to a shutdown group, drag and drop it into the desired shutdown group:
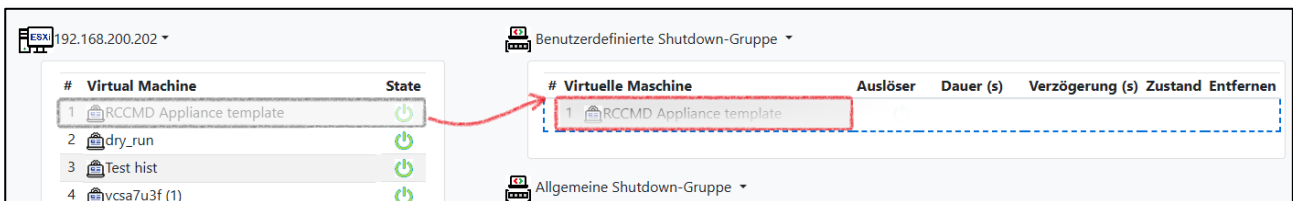
The virtual machine will no longer be displayed or managed by RCCMD at the host group, but the custom shutdown group:.

Please note that this setting is independent to ESXi host or vCenter settings. RCCMD will search for this virtual machine on all known hosts specified at VMware settings in the future to shut it down.

Remove

To remove a virtual machine from a static shutdown group, drag the virtual machine back to the according host on the left side of the screen.
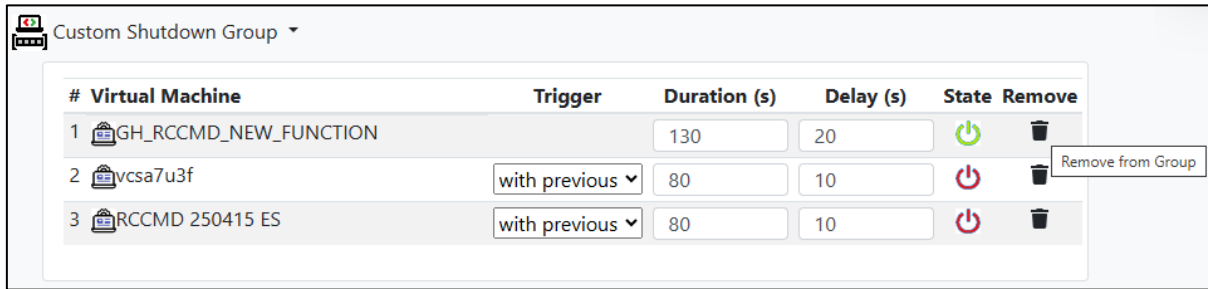
If you are unsure where the virtual machine is currently located, click the small trash can icon at "Remove." The according entry will be removed from the list and added to the ESXi host where it is currently located.

Note: RCCMD cannot delete a virtual machine!

The RCCMD Shutdown Management allows to automatically shut down virtual machines in a dependent manner. RCCMD will never delete a virtual machine from your server!

Change shutdown order and move virtual machines

RCCMD provides freely movement of virtual machines within user-specific groups. Simply drag them to the location in the shutdown logic where to shut down.

• Within a shutdown group

• Between different shutdown groups

Shutdown Group 1 - The time managed custom shutdown group

The trigger in the custom shutdown group, along with the duration (s) and delay (s), offers numerous options to customize a shutdown sequence:

Timing functions and trigger point provide custom time frame definition for dependency-based shutdown sequence. All virtual machines will then be shut down in an orderly manner based on this time-controlled schedule. When scheduling the times, please note that the values entered at this menu do not affect the shutdown time of the virtual machine itself. They are used exclusively by RCCMD's internal shutdown timing.

Trigger and time management functions for the custom shutdown group

The first virtual machine in the list offers two different time windows that affect shutdown management:
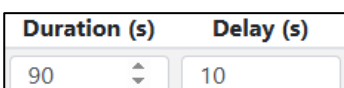
Duration defines how long a virtual machine takes to shut down. Delay specifies how long a shutdown trigger and the according duration timer start is delayed.

Starting with the second virtual machine in the list, there is also a trigger that defines when the respective counters should be started. This trigger restrictively links the shutdown to the shutdown of the previous virtual machine:

Trigger	Duration (s)	Delay (s)
	90	10
after previous ⌄	130	20

"after previous" defines that the individual delay only starts when the shutdown timer (Duration (s)) of the previous virtual machine has expired. In this example, the second virtual machine with a shutdown duration of 130 seconds will not start until the 90 seconds have elapsed + a 20-second time delay.

Trigger	Duration (s)	Delay (s)
	90	10
with previous ⌄	130	20

"with previous" defines that the delay of the subsequent virtual machine starts at the same time as the shutdown timer (duration (s)) of the previous machine: In this example, the second virtual machine will receive a shutdown signal 20 seconds after the first virtual machine and RCCMD will start the corresponding shutdown timer (duration).

As the number of virtual machines increases, the following shutdown logic results:

Machine 1 will shut down after 10 seconds.
Machine 2 will wait 90 + 20 seconds and then shut down.
Machine 3 will initiate shutdown 10 seconds after Machine 2.
Machine 4 will initiate shutdown 10 seconds after Machine 3.
Machine 5 will initiate shutdown 80 + 10 seconds after Machine 4.

#	Virtual Machine	Trigger	Duration (s)	Delay (s)	State	Remove
1	Test hist		90	10	⏻	🗑
2	GH_RCCMD_NEW_FUNCTION	after previous ⌄	130	20	⏻	🗑
3	vcsa7u3f	with previous ⌄	80	10	⏻	🗑
4	RCCMD 250415 ES	with previous ⌄	80	10	⏻	🗑
5	RCCMD Appliance template	after previous ⌄	90	10	⏻	🗑

If a virtual machine in list no longer exists or is not found, RCCMD will meticulously adhere to the specified shutdown times and simply indicate that the virtual machine cannot be found. Therefore, if virtual machines are migrated to other data centers in advance, this will not affect the shutdown procedure.

When the duration (s) of the last machine has expired, the shutdown group moves to the next one: the general shutdown group.

Shutdown Group 2: The General Shutdown Group

This group is intended for all virtual machines that can be shut down without special shutdown requirements. Global policies are applied:

- Shutdown Duration (s):   90 Seconds
- Delay (s):   0 Seconds

The list is processed directly from top to bottom, but allows you to define a rough shutdown order: Virtual machines that take longer to shut down than the estimated 90 seconds should be placed higher in list than those that shut down more quickly.

General Shutdown Group ▾

#	Virtuelle Maschine	State	Remove
1	VM-Test 2	⏻	🗑
2	VMware-VirtualSAN-Witness-7.0U3c-1...	⏻	🗑
3	Kirby-Webdevel	⏻	🗑
4	RCCMD Appliance template	⏻	🗑

After the shutdown duration (duration (s)) has expired, the shutdown group 3 becomes: The Dynamic Shutdown Group.

Shutdown Group 3: The Dynamic Group

The dynamic shutdown group is a fully automated system group that captures all virtual machines that have not been explicitly assigned to another group:

When accessing VM Shutdown Management, all known ESXi hosts are queried in real time, and the available virtual machines are listed.

The special feature of this group lies in the details:

If a virtual machine is migrated or created on one of the known ESXi hosts after configuration, RCCMD will capture it in real time upon a sharp shutdown signal and automatically assign it to this group.

Virtual machines that were previously migrated through vMotion or manual intervention are dynamically removed from this list.

This protects all virtual machines running on the hosts and shuts them down if necessary

After 90 seconds, the call is forwarded to Shutdown Group 4.

Shutdown Group 4: The Host based Shutdown Group

The host-based shutdown group includes all infrastructure-related servers

- DNS
- DHCP
- Gateway
- RADIUS
- VMware Appliance
- vCenter
- […]

ESXi 192.168.200.202 ▾

#	Virtual Machine	State
1	VMware-VirtualSAN-Witness-7.0U3c-1…	⏻
2	vcsa7u3f	⏻
3	GH_RCCMD_NEW_FUNCTION	⏻
4	dry_run	⏻

ESXi 192.168.200.156 ▾

#	Virtual Machine	State
1	test vm new	⏻

ESXi 192.168.200.107 ▾

#	Virtual Machine	State
1	vmtest	⏻

Host based Shutdown Group ▾

#	Virtual Machine	State	Remove
1	RADIUS	⏻	🗑
2	DNS / DHCP	⏻	🗑
3	Domain Controller	⏻	🗑

Servers placed in this group are shut down via the VMware settings, and then the ESXi hosts.

VM running RCCMD:	machine running RCCMD

Add... Remove Edit... Verify

ESXi Hosts to shutdown

ESXi Address	Shutdown duration	Verify
192.168.200.202	90 Seconds	
192.168.200.156	80 Seconds	
192.168.200.107	120 Seconds	

Virtual machines that are not powered off at this point will be cold powered when the hosts are shutting down.

Detailed real-time Shutdown Monitoring

RCCMD offers a more passive monitoring mode that allows you to monitor the operating state of virtual machines in real time during a shutdown:

☑ Automatic update   Interval (s) [10] ⬍

#	Virtual Machine	Trigger	Duration (s)	Delay (s)	State	Remove
1	🖥Test hist		10	10	⏻ ✗	🗑
2	🖥vcsa7u3f	after previous ⌄	10	10	⏻ ↗	🗑
3	🖥RCCMD 250210 new	after previous ⌄	10	10	⏻ ↖	🗑

Once this feature is active, the virtual machine status query will be updated every xxx seconds until the checkbox is removed. This display will continue until the RCCMD appliance is ultimately shut down with the ESXi host and is no longer accessible.

Real Time Monitoring Option:

• Status of virtual machines
• Status of machines that are no longer found on the servers
• Status of newly added machines (migrated and redeployed)
• Status of the availability of an ESXi host

Note: limited configuration options if active

Any changes to be saved will only take effect after the RCCMD Appliance is restarted. The current shutdown routine is not changed in real time. If a real shutdown occurs while real time monitoring is enabled, the currently saved configuration will be used to carry out the shutdown.

use Advanced Settings for additional settings to configure RCCMD. The menu is divided into three parts:

Event Logfile

In general, any RCCMD Signal affecting the client will be logged. Due to the fact server systems may provide limited memory resources for log files, it may be necessary to limit the size of the log file to the maximum size to consume. In case the maximum file size is reached, the oldest entry is replaced by a new entry.

RCCMD Bindings

RCCMD Bindings is a sophisticated tool that helps you to limit traffic. Since this setting deeply affects your network setting, it should be used with caution. The bindings allow forcing RCCMD to listen on a specific network card. In case of multihoming is in use, the listener can be configured to a specific IP address within one network card. As an example, this will be used if there is a necessity to divide the network logically into a production network and an infrastructure network via VLAN:

In this example scenario, two or more network adapters can be installed. Binding RCCMD to one specific network card will prevent users to access the RCCMD client and accidentally shut down a server - this is only possible via devices that are located in VLAN 3 or have been properly enabled via a router.

Another scenario is the so-called multihoming:

It is not absolutely necessary for modern network devices that an IP address is firmly linked to one network interface. In fact, multiple IP addresses can be connected via a network interface - they share hardware, but otherwise form self-contained instances. As an example, this could be a web server that manages different websites with a unique IP address: the server is connected by a router that determines between incoming signals and signals provided by local network. Bindings will instruct RCCMD to listen for incoming RCCMD signals only at a specific IP address that is assigned to the local network only.

Note
These configurations are used in special scenarios. Normally you can leave the setting 127.0.0.1 / local host, port 6003. In that case, RCCMD will listen on all available IP addresses for a valid incoming signal. Since you have defined the valid sender address at the menu Connections, RCCMD will notice the signal but deny execution and log this fact as an invalid RCCMD command.

Change RCCMD Target

The RCCMD appliance is more than just a small tool to handle just VMware hosts. On unchecking the checkbox and pressing Save changes, RCCMD changes to the local mode:

All VMware menus will be disabled and the Shutdown settings will switch to local options:
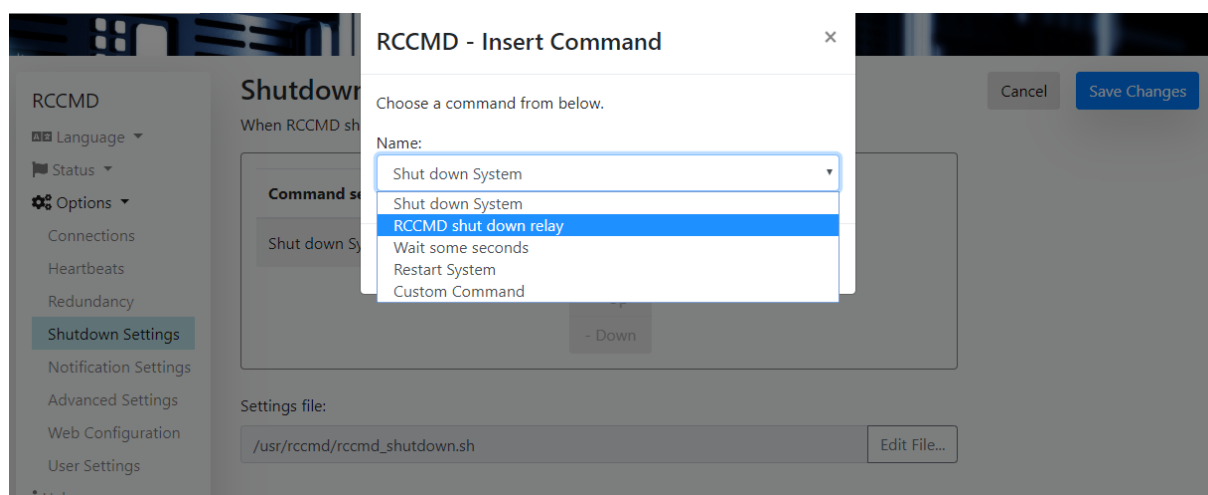
Due to the fact, RCCMD cannot just receive, but also send RCCMD shutdown signals, it is possible to use an RCCMD appliance as a central RCCMD relay that runs with complete customized additional scripting.

When local mode is active, RCCMD provides the following command sequences:

Shut down system

RCCMD will shut down the server it runs on.

RCCMD shut down relay

With this option, RCCMD will forward a valid RCCMD shutdown to

- Single IP addresses
- An IP address range

With this option, it is possible to get advanced redundancy options - as an example, you may combine a CS141 and a second RCCMD client – if both advice a shutdown, the target RCCMD system will execute the command.

Wait some seconds

RCCMD will wait a customizable time window until the next command in the list will be executed.

System restart

RCCMD will restart the complete RCCMD server that runs within a virtual machine

Custom command

Start programs, run kill-commands, run your own scripts, just enter the command and mandatory extensions and RCCMD will do the rest.

Configure the web server

If the ports are blocked or used by other applications, it is possible to change the ports for the internal web interface of RCCMD.

Set the availability of the RCCMD web console.

The default for web access is:

http: port 8080

https: port 8443

Please note changing the default values will cause the web console of RCCMD can only be reached via the ports you manually set.

Backup / Restore

Important: this function is available for program version 4.54.X.231129 onwards. Former program version backups are not compatible with this function – For more information, please refer to the chapter "Disaster Recovery".

The RCCMD Appliance provides a comfortable backup & restore function for easy appliance update:

Appliance update procedure

1. Click "Backup" to create a backup of the current RCCMD Appliance.

2. Shut down the appliance and switch of the virtual machine.

3. Deploy the new appliance.

4. Place the backup file as created inside the Drop box and click restore.

5. Test the new appliance.

If the appliance is running as expected, delete the old appliance version.

RCCMD Appliance: Update Web server certificate

The integrated web server can be configured to follow up company SSL / TLS certificates. For the required pem-file, refer to the local IT department. This function will be used to encrypt the communication between the web interface of the RCCMD installation and the web browser.

TLS certificate update function:

1. Create a backup file before using this function
2. Place the *.pem file in the according upload box
3. Click upload
4. Restart RCCMD at System status.

The Web browser should now show your own certificate. If your web browser can not access the web interface, re-install RCCMD and check the certificate.

System Tab: User Settings

Customize the administrator password according to your ideas and company policies. Please note that this password also applies to the admin user on the console. The appendix contains instructions how to set up an emergency user for password recovery

Administrator User Name: admin
This user name is hard-coded and cannot be changed.

Current Administrator Password:
This is the currently assigned password.

New Administrator Password
Assign the new password.

Confirm New Password
Repeat the password you have assigned. Please note that Copy and Paste will repeat typing errors and may lock up your RCCMD client.

Note

Depending on the program version, there are two default passwords that can be assigned.

Program versions until 5/2018: cs121-snmp
Program versions from 5/2018: RCCMD

Due to the fact RCCMD comes with two years update authorization, it is possible that you need these two default passwords.

Network settings
(For this configuration menu, version 4.49 or later is required.)

The Appliance for VMware offers you the possibility to set the IP address directly via the web interface.

Hostname / Search Domain:	If you want to communicate with RCCMD via DNS names, enter the necessary DNS names here. Please note that there is no automation here. The DNS name may need to be manually updated on the responsible DNS server if necessary. I hope this helps. Let me know if you have any other questions.
MAC:	The Media Access Control (MAC) defines the address of the network hardware. This is generated by VMware during the rollout process and cannot be changed via this interface. If you have any further questions, please let me know.
IP-Configuration:	*D*etermine whether the IP address should be assigned via a DHCP server or statically. Please note that a DHCP server can change the IP address with appropriate configuration, which can cause a shutdown signal to fail if the target IP has changed.
IP-address data (if static selected)	
IP-Adresse / Subnet Mask	Define the IP address and the associated subnet mask. You will receive the data from the responsible administrator.
Default Gateway	If RCCMD needs to communicate across networks, please define an appropriate gateway.
DNS 1/ 2	The DNS server is used for name resolution if, for example, you want to use DNS names of ESXi hosts instead of IP addresses on the appliance. Please note that, for example, ESXi-Host-1.example.local can only be reached if a DNS server is available.

Note:

When rolling out, you will be asked in an interactive system window by VMware whether you want to enter an IP address. If you do not fill in these input fields, the RCCMD appliance assumes that a DHCP server is available on the first start and assigns an IP address. You can adjust the IP address data of RCCMD as well as the startup behaviour via the network settings and choose between DHCP and manual IP address.

System tab: Help

If you do not know what to do…

Manual

You need help?

The manuals are available inside RCCMD – you do not need any additional network connection.

Due to the fact the manual is a pdf-file you may need additional software tools to open the according file.

Info

Need additional information about your copy of RCCMD?

The info button will show

- Acknowledgements
- EULA
- Copyrights

Appendix

Everything else you might want to know about RCCMD...

The Microsoft Windows „RCCM_NC" Configuration Tool

The "RCCM_NC"configuration tool, located at the installation path of RCCMD, can be used for a direct configuration of the RCCMD client. This becomes interesting as soon as RCCMD has to be configured without a web browser.

Click on the tool with the right mouse button and select "Run as administrator"!

After starting, the following configuration options are available:
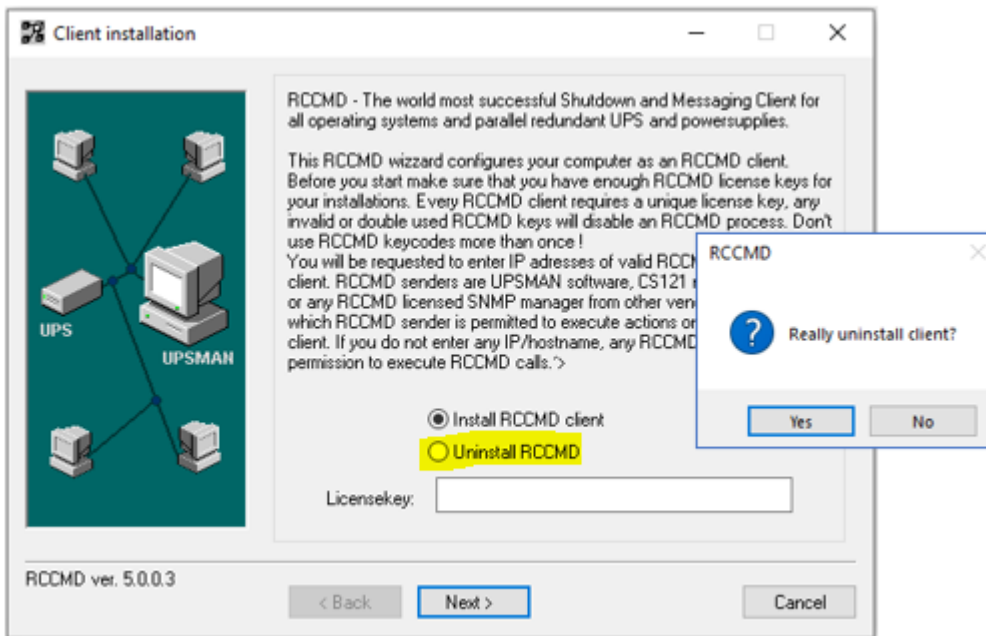
Install RCCMD client

This function starts the configuration/installation dialogue.

Uninstall RCCMD

Use this function to uninstall your copy of RCCMD.

Licensekey

Enter / change licence key.

Persistant navigation buttons:

< Back Next >	Navigate through all setup screens forward / backwards. You can re-visit any page and take your changes. Following screens and functions will be added / removed in realtime.
Cancel	Abort the configuration work: This button will withdraw all configuration changes and abort the tool.
Install	Appears dynamically – with this button, RCCMD will process your changes, write an active configuration file and than restart RCCMD. Click "Next" until this button is shown.

RCCMD IP settings, ports and bindings
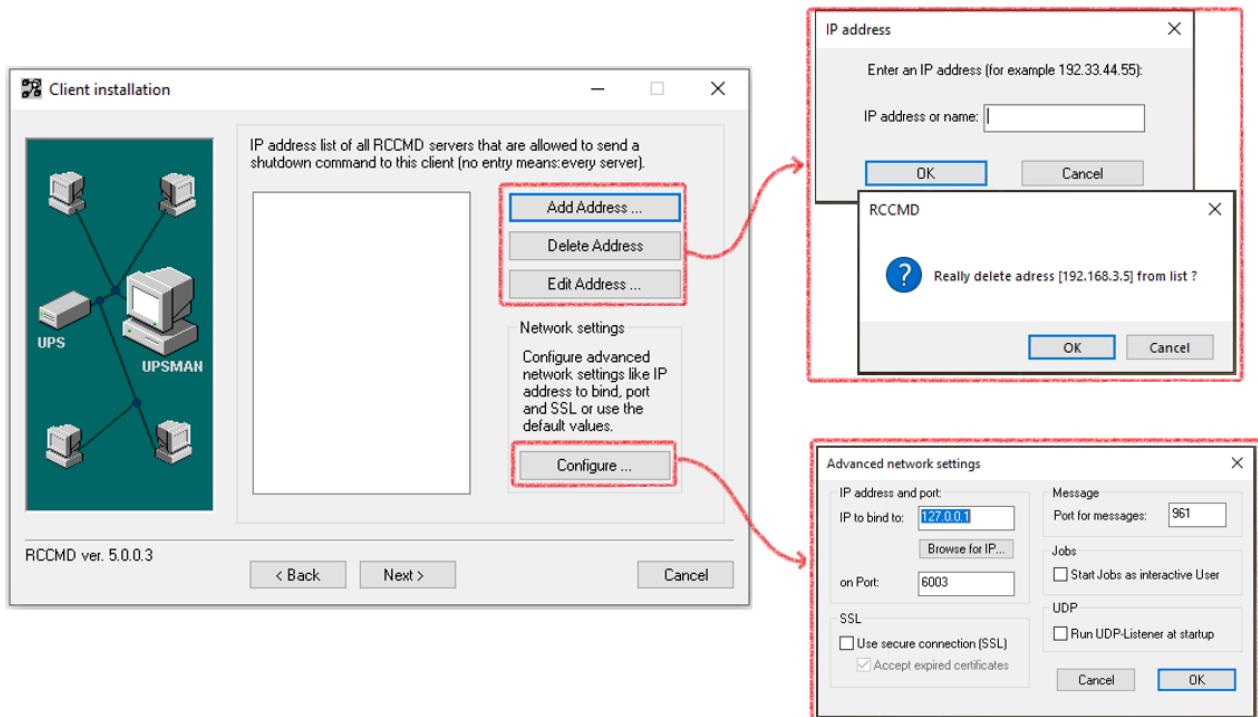
Add / Delete / Edit

Define,

a.   which IP address is allowed to send a signal to this RCCMD client at all. As soon as an IP address is entered, jobs coming from any other sender are denied. Use Add/Edit to add an IP address or edit an existing entry. Delete removes an entry from the list.

b.   whether redundancy behaviour is desired: If at least 2 or more IP addresses are entered, later configuration dialogues provide functions to enable and edit redundancy groups.

Configure / Advanced network settings

IP address and port

If wanted, RCCMD is custumizable to listen only on a special network card or a different port, enter the IP address or port number the listener should be placed.

SSL

Define whether RCCMD should use SSL encryption for communication, and if so, whether expired certificates should still be accepte.

Message Port

Define the internal port the RCCMD background service shall use to send pop-up messages to the GUI of the operating system.

Jobs as interactive User

Normally, RCCMD is a background service. Accordingly, all scripts start in the background. With this tick, the scripts are executed as foreground processes. Please note, this function is limited to the fact that a user must be logged on…

Run UDP Listener at startup

Broadcast packets are mostly Unified Data Packages (UDP) - A sender does not know whether and how a data packet has reached its destination. Since UDP packets are relatively easy to forge (all that is needed is the valid sender IP), this function is usually disabled for security reasons and must be activated manually by the user.

132

Heartbeats / UPSMan alive checking

Enable connection check

If desired, RCCMD can regularly poll the registered valid transmitters to check whether the corresponding device is still available. The *"polling rate"* defines the intervals at which this should be done, and *"Connect retries"* defines how often this connection test may fail one after the other before RCCMD assumes a problem.

Test connections

As a test, query all entered IP addresses to see whether the corresponding devices can also be reached by RCCMD.

Execute at failure

This script is executed when the number of connection attempts specified under "Connect retries" has been reached. Select your own script with "Browse", or edit the currently selected script directly with Edit file. Default settings deletes all settings and restores the original state of the start configuration.

Use RCCMD Traps

Instead of polling, an RCCMD trap message is sent by the transmitters, which is interpreted as a sign of life.

Audible Stettings

If necessary, RCCMD displays an alarm window and indicates this with a yellow warning triangle in the task bar. This function controls the formidable acoustic "BEEP", which can be customized:

turn it off, let it beep endlessly, or just emit a certain number of warning beeps.

RCCMD Redundancy

This function affects the "Next" button. In case of enabling the redundancy function, a continuative configuration screen is automatically available, which can be set on the next page.

RCCMD redundancy configuration

This screen is only available if RCCMD Redundancy in the "UPSMAN alive checking" dialogue is enabled..
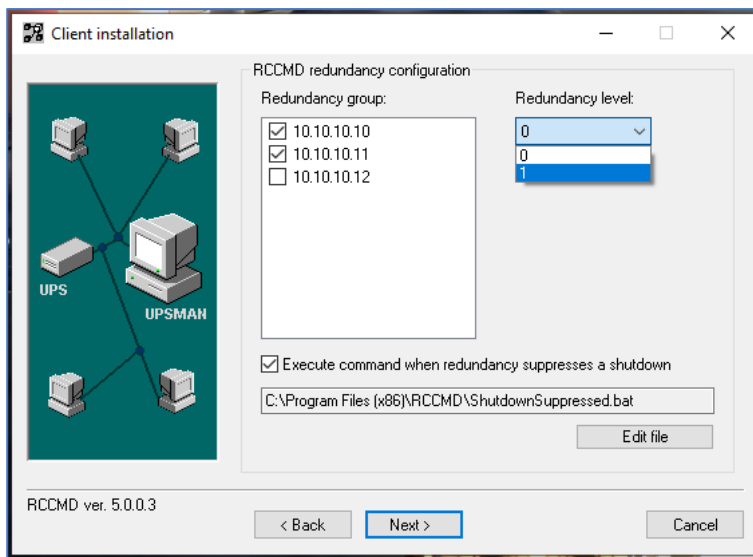
In this dialogue, RCCMD wants to know which IP addresses added at Connections are to be merged into a redundancy group.

Explanation:

At "Connections", you have added some valid RCCMD server, and thus defined which IP address may generally send RCCMD commands to this RCCMD client. From these previously entered IP addresses, you can define, which of these valid RCCMD sending devices must trigger a shutdown at the same time before the shutdown will be exectuted ...
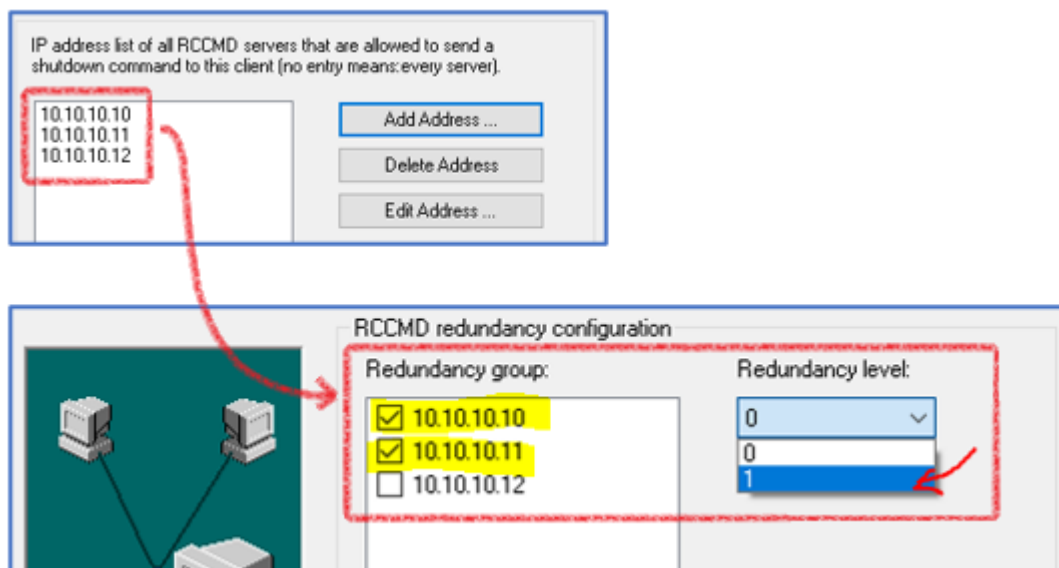
In this example, 3 valid RCCMD transmitters are generally allowed to send a shutdown. At "Redundancy", however, it was defined that both, 10.10.10.10 and 10.10.10.11 must send an RCCMD shutdown command before this command takes effect. A typical scenario would be that two CS141s are in UPS systems, while a third CS141 monitors the ambient temperatures of the protected servers with a SENSOR MONITOR.

Redundancy Level

The redundancy level determines how many transmitters must send the RCCMD shutdown command:

0 defines the first transmitter that has issued an RCCMD shutdown.

1 each additional number defines another transmitter that must also issue this RCCMD shutdown.

With two units, the maximum redundancy level is "1" because there is only one other unit. With three valid transmitters, the maximum redundancy level would therefore be 2, because one of the units gives the initial command and the other units thus agree.

Execute command when redundancy suprpesses a shutdown

This script is executed automatically when the redundancy level has suppressed a shutdown. With edit file you can add any actions to the batch file.

RCCMD Shutdown behaviour and logging
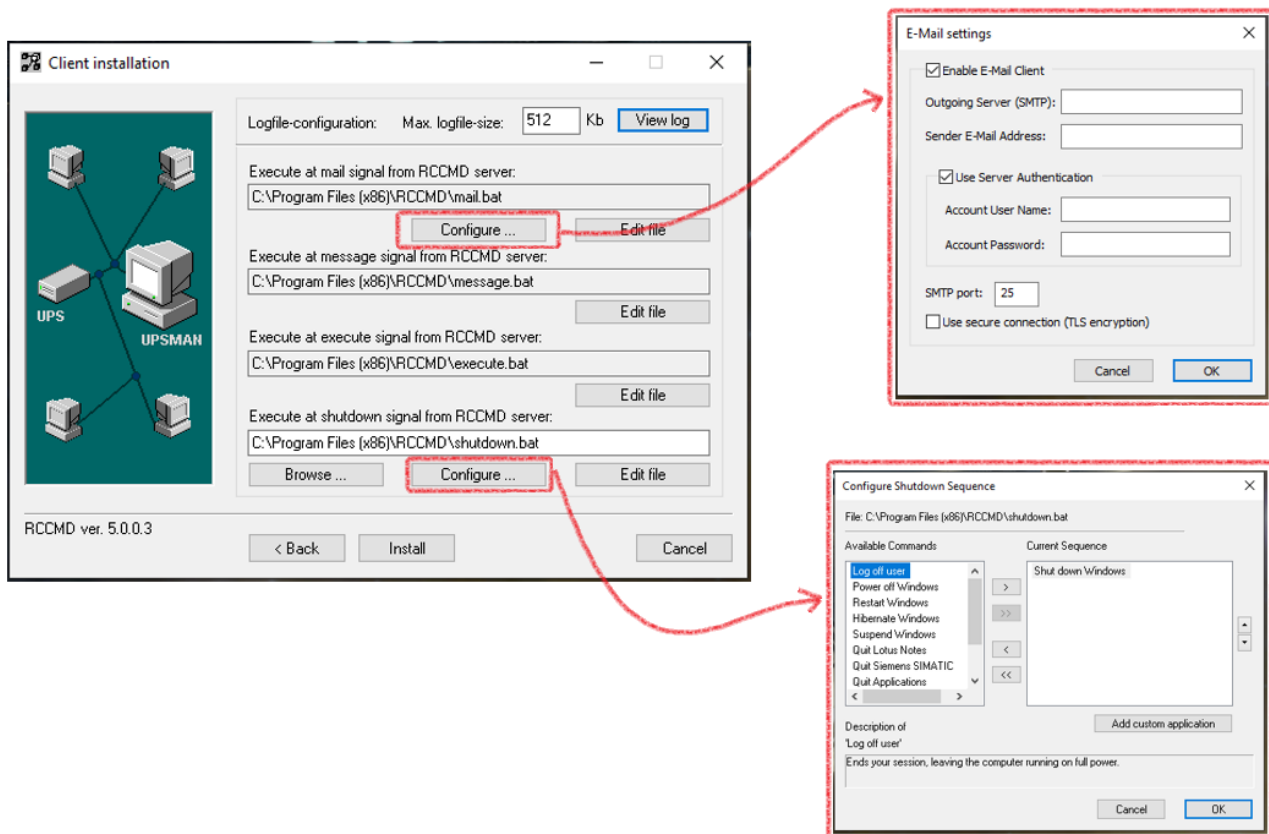
Logfile-Configuration

Define the size of the log file that RCCMD should create. When the file has reached this size, RCCMD will erase the oldest entry in order to add a new entry.

Execute at mail signal from RCCMD server

RCCMD can also run special RCCMD mail relay jobs, e.g. if a CS141 / BACS is to share information via mail from a protected area without direct connection. At Configure, enable the integrated mail client and enter the necessary access data so that RCCMD can send a mail accordingly.

Execute at message signal from RCCMD server

This script takes the CS141 / BACS job "RCCMD Message" and conjures up the message box on the desktop of an operating system. Normally, nothing needs to be changed here Please note that this script is executed for every message, regardless of the content of the RCCMD Message job!

Execute at execute signal from RCCMD server

Similar to 'message signal', except that the RCCMD job "Execute" is used to allow a CS141 starting a script file directly via the RCCMD client, with local admin rights. Again, normally nothing needs to be adjusted, the script runs exactly as it is set Out-Of-The-Box.

Execute at shutdown signal from RCCMD server

Click Configure to customize the shutdown routine to your liking. Each action is generally executed from top to bottom as filed in the list, with the last command being shut down Windows or similar. After this command, no further commands are executed, as the operating system terminates RCCMD accordingly.With the intuitive buttons, add new jobs, change the order of the jobs to be executed or remove them.

With Add custom application, insert own scripts or commands - they will be be executed within this shutdown sequence accordingly-

WARNING: EDIT FILE ALLOWS TO INDIVIDUALISE THE CHARACTER OF EACH BATCH FILE! AS THE DIRECT MANIPULATION OF THE SCRIPTS MAY DIRECTLY INTERFERES WITH THE FUNCTIONAL PROCESS, THIS IS DONE AT YOUR OWN RISK!

Install

Completes the configuration process, writes the final configuration file and restarts RCCMD. You can repeat the configuration process as often as you like, or use the "back" button to scroll through the configuration dialogue. Click install to finish the configuration work.

RCCMD Security Guide

RCCMD is a very powerful system management tool - used correctly, RCCMD can take over the complete software side of an emergency concept in a way that is transparent to existing shutdown and building management systems:

- Initiate migrations
- prepare shutdowns and carry them out independently
- Start backup systems
- Back up and copy system directories
- Inform
- Transfer shutdown sequences from one RCCMD client to another
- etc.

The web interface offers a comfortable introduction, but in the end it only shows a small part of what RCCMD can actually do within a network.

Note

RCCMD is designed for secure operation in a network. This includes that it works as inconspicuously as possible in the background to make it as difficult as possible for possible hackers to detect it.

---

1. _Password Security_

The start password is "RCCMD"! You should change it as soon as possible.

A glance at the manual is enough, and hackers have access to the convenient configuration interface.

What is a "secure password"?

First, no password is unhackable, and if someone really wants to, there are many ways to figure out a password - the trick to a good password is that a potential attacker loses interest or gives up because he has to fear being discovered before he reaches his goal.
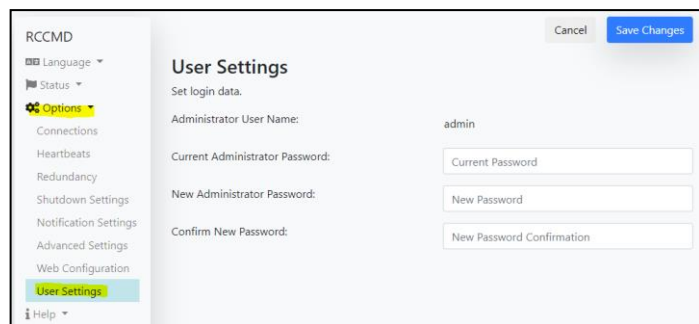
A strong password meets the following criteria:

o 8 - 12 characters long
o Upper and lower case
o Numbers
o At least one special character
o No reference to the person and his or her everyday life

2. _Authorised RCCMD senders for the shutdown: setting are now mandatory_

RCCMD has always been designed for best possible handling even by inexperienced users. In the simplest case, one could simply install RCCMD and switch it on - and the EDP on the server side was already protected against a power failure.

Now, this has been changed to meet modern :
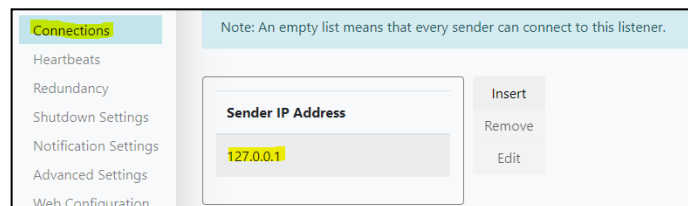
What is new is that the IP address 127.0.0.1 is now preset. This means that RCCMD actually only receives a shutdown signal from one transmitter: From itself (127.0.0.1 is the so-called "local host"). Until you have manually added a valid transmitter, RCCMD will document every incoming RCCMD - signal in the log file as outgoing.

Security recommendation:

RCCMD war schon immer auf bestmögliches Handling auch durch ungeübte Nutzer ausgelegt.
Im einfachsten Fall konnte man RCCMD einfach installieren und einschalten – schon war die EDV auf der Serverseite gegen einen Stromausfall geschützt.

Minimise the number of authorised senders! The fewer devices are allowed to send a shutdown signal or control commands (RCCMD Execute's) to am RCCMD installation, the more secure your RCCMD installation will be.

3. *UDP Broadcasts*

Under Connections, you will find the function "Enable UDP Broadcast":

This function is required if you want to broadcast one of the following jobs from the CS141:

o RCCMD Shutdown
o RCCMD Message
o RCCMD Execute

UDP has the advantage that it can be used with extremely low latency to transmit messages or control commands from the sender to any number of receivers, but it also has the disadvantage that the sender and receiver do not know each other. A hacker can evaluate intercepted UDP packets and, if necessary, forge them.

Security recommendation:

If possible, UDP should only be used if the sender and receiver are in a specially secured infrastructure network. If this is not the case, we recommend deactivating UDP.Unter Connections finden Sie die Funktion „Enable UDP Broadcast":

4. *Ports*

With this argument, in general, opinions differ a little:

Within RCCMD (and in CS141), the ports can be adjusted to ignore defaults and standards. Actually, this function is provided in case of some ports are already used and blocked for other applications.
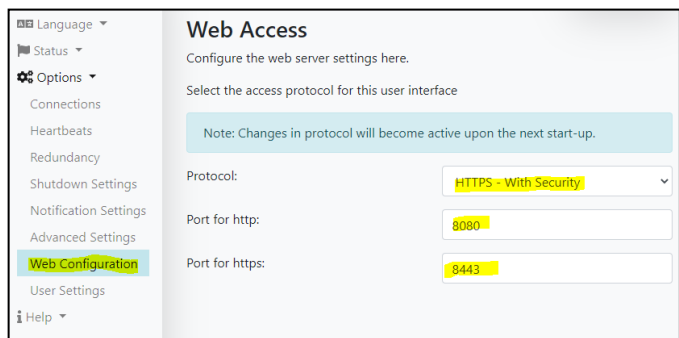
However, it has to be mentioned that the operational security increases if the RCCMD web interface - independent of http or https - does not answer on 8080 (http) or 8443 (https) at first, but for example on port "1956 (http)" or "2578 (https)" -

Even if a potential attacker knows that RCCMD is in use, he would first have to find out the necessary ports on which a web request to RCCMD is answered at all.

Security recommendation for the web interface:

Can be carried out as a flanking measure to a strong access password - then not only the password is a hurdle, but you also have to know on which port the web interface can be reached at all. Please note, however, that these changes could also possibly entail an adjustment of routers, firewalls, etc.

*Security recommendation for the communication ports (6003, 961)*

By default, the RCCMD listener is located on port 6003, and the RCCMD service communicates with the service tray via port 961. The adjustment is not necessary if there are no security concerns about standard ports, or if the port is already in use elsewhere. The same considerations apply as for whether https / http ports should be adapted and what effort would be required in the network configuration.

Why does the heartbeat with TLS encryption not work with default settings?

We changed some settings to meet modern IT compliance guidelines: One of the most significant changes are that the services at the CS141 & BACS systems are now OFF by default, except the web server (you need it to access the CS141 web interface).

At "Devices > Setup", you need to enable the UNMS & RCCMD Trap Service – this will enable the RCCMD Heartbeat function. Within RCCMD, open connections and take a look at "Protocol":
Accept only SSL/TLS connections is enabled by default.

If you intend to use "heartbeats", you will get a communication lost issue until both, CS141/BACS and RCCMD uses a harmonized configuration:
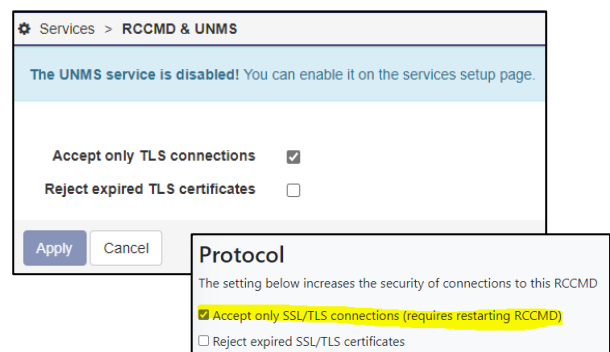
Both endpoints need to use "SSL/TLS ON or OFF" or it won't work. Depending on which certificate you use, you may also choose " Reject expired SSL/TLS certificates".

Please keep in mind:

It is in the nature of using default (or example) certificates to be rejected in case of "reject expired certificates" is selected. If this function is wanted, a set of valid certificates is needed. For valid certificates, please contact the local system administrator and ask for according certificates.

Redundancy configuration - A case study

What is needed for "redundancy"?

For a meaningful redundancy circuit, you need 2 CS141s that work together: To make things easier, in this tutorial, we assume a standard case where 2 UPS systems are in use, each connected to different circuits, and then together they ensure power supply through their outputs, for example, with a transfer switch.
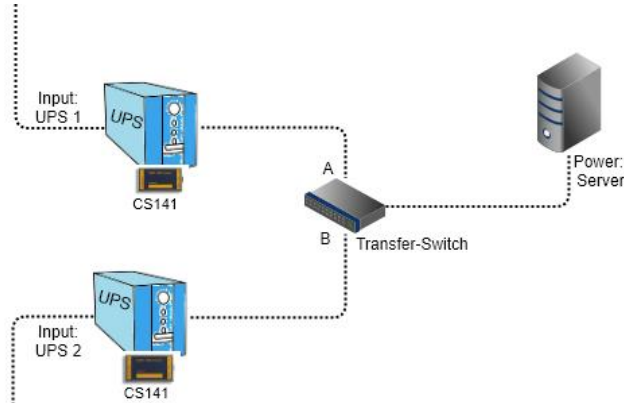
The Transferswitch will only take notice about problem if one of the two UPS systems shuts down or is completely shut down for maintenance, and, if necessary, will switch automatically to the other power source. Logically, a transfer switch has no information about the operating state of each UPS or how much remaining runtime is available:

If we assume that Input A is active and Input UPS 1 fails, the Transferswitch would switch to Input B as soon as UPS1 shuts down.

The Transferswitch would do the same if UPS Input 1 and 2 fail simultaneously, and depending on the load, UPS 2 would then take over the load generated by the server until the batteries are exhausted.
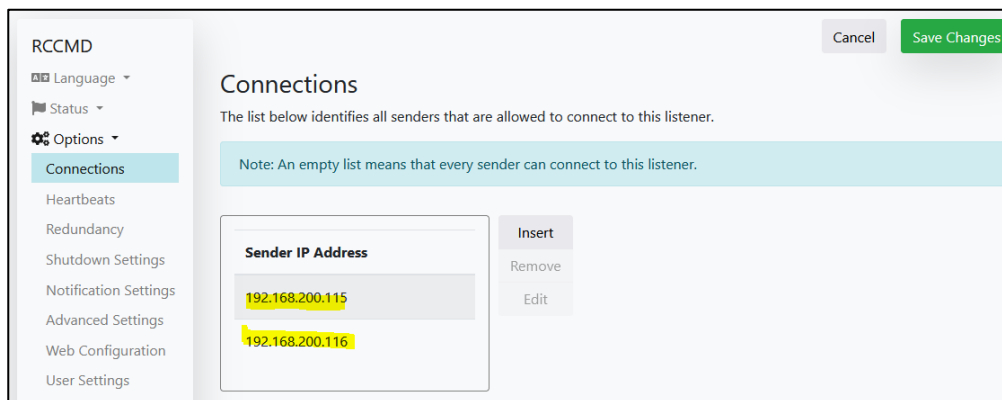
According to this logic, the server must be shut down in time before both UPS systems can no longer provide enough emergency power.

Where to configure the redundancy function?

Start with the RCCMD Client – you need to configure several entries:

1. Which device is allowed to send shutdown command?

At the RCCMD client, open options and click on „Connections":

You need to define a valid sender – in this case, you need to enter the IP addresses of both CS141 WEBMANAGER. Once entered, only these two CS141 are accepted RCCMD Command sender.

Note: The DHCP Mode may change IP addresses

If running the CS141 WEBMANAGER in DHCP mode, it is possible that the DHCP server will assign new IP addresses. Consequently, the RCCMD client will reject commands because of a changed ip address! To avoid this prolbem, ensure that the IP addresses of both CS141 WEBMANAGER are fixed. This also applies in reverse - if the DHCP server assigns a new IP address to the RCCMD client, the RCCMD shutdown commands will fail…
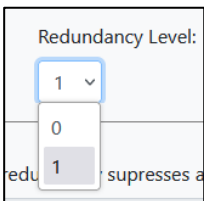

Setting up the redundancy

After setting up the IP addresses, it is time to configure the redundancy function. To start, click on „Redundancy":
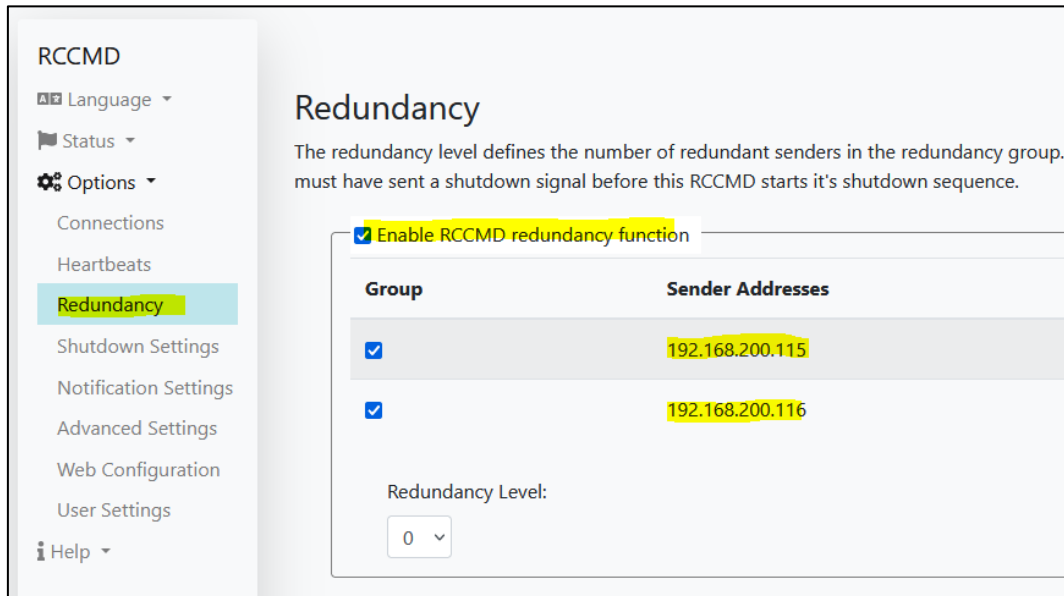
First, enable the redundancy functio, and than select the IP addresses that will form up the Redundancy group:

How to calculate the redundancy level?

The redundancy level follows a simple assumption:

With two UPS systems, there are always 2 CS141 WEBMANAGERs, one of which will inevitably send a shutdown command first. Which of the two WEBMANAGERs that is exactly depends on the individual state of charge of the batteries, the load, the power failure, etc. However, the shutdown is suppressed until all other WEBMANAGERs in this list have also sent a shutdown command. This results in the redundancy level being mathematically N + 1, where N is generally the first Webmanager to send a shutdown command, while "+1" is the number of additional Webmanagers that must send a shutdown command in this group.

This results in the following values:

0 -> No other CS141 WEBMANAGER is in charge to send a shutdown signal.

1 -> One other WEBMANAGER must send a Shutdown Command.

➔ **Since we only have two UPS systems, you should set the redundancy to 1.**

What if the second CS141 is no longer accessible, for example due to a total failure of the switch?

RCCMD accepts the shutdown command with reservation: If one of the two web managers sends a shutdown command, the redundancy function automatically checks whether all other WEBMANAGERs selected for redundancy are available and whether communication with the respective UPS is also functioning correctly:

If this condition is not met, the shutdown will be executed because there can obviously be no further shutdown command.

Connection test

In the last step, you should check whether RCCMD can reach and query both CS141 WEBMANAGERs. To do this, click "Run alive check now…" under Heartbeats in Test UPS Connections. There are two possibilities:

OK   ->   The CS141 is configured well and reachable.

Not OK   ->   Der CS141 or network is not configured well or not reachable.

- Check if Ports 5769 / 6003 TCP are available.
- Check the communication certificate.
- Check if TLS is ON / OFF on both endpoints.
- Check, if the CS141 UNMS / RCCMD trap services are active.
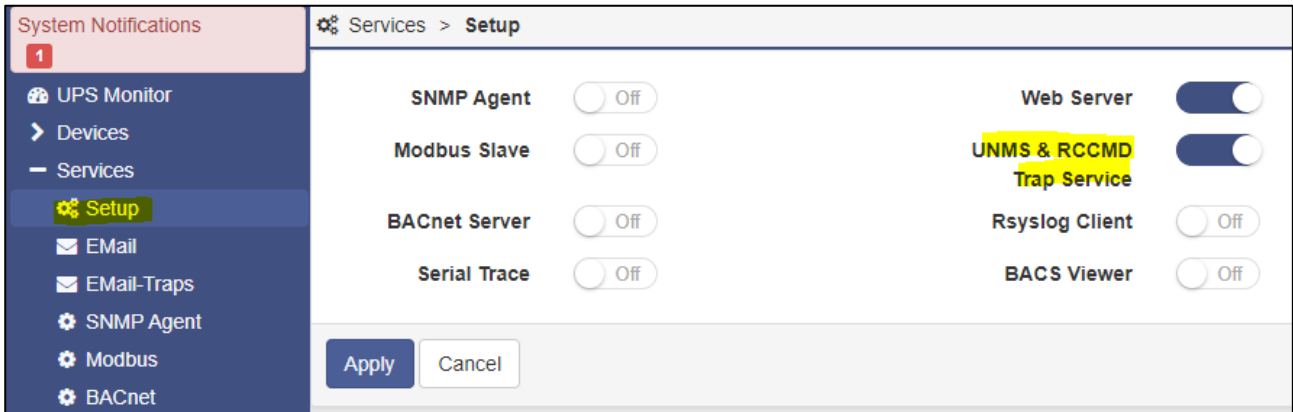- Check, if firewalls or virus scan solutions block the communication attempts.
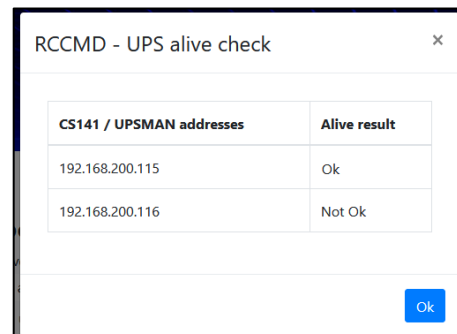
2. CS141 configuration

RCCMD is fully configured and ready to carry out a redundancy shutdown scenario.

Now, both CS141s must be configured identically. Log in to the CS141 WEBMANAGER and carry out the following configuration:

Enable UNMS & RCCMD Trap Services

This step is required to communicate with the CS141 via Port 5769 TCP and query the operation state. As long as this service is OFF, RCCMD will show „NOT OK" as a UPS alive check result.

a. Check TLS Settings
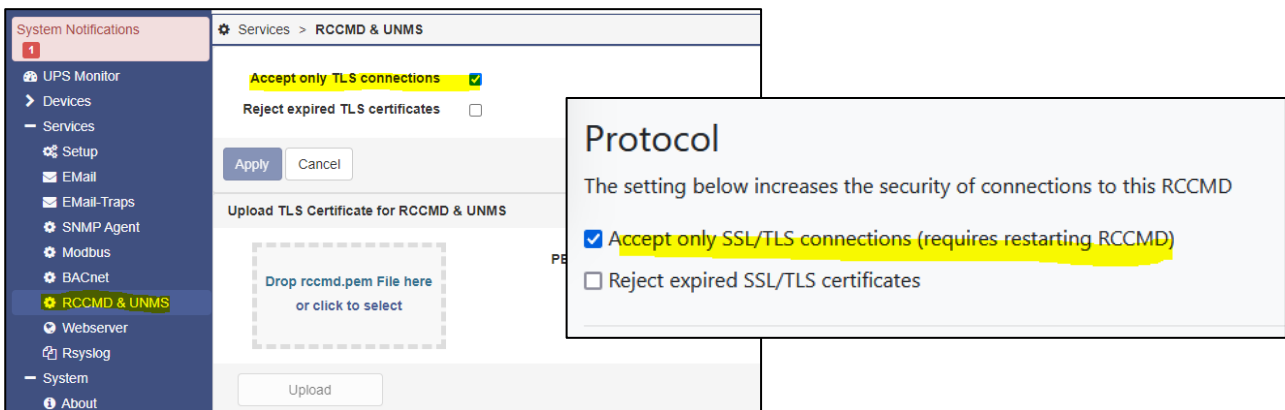
This must be identical in the CS141 and RCCMD program (found under Options>Connections), otherwise communication itself will fails

Define the RCCMD Shutdown Jobs

At the CS141 UPS events „Powerfail ", add the job „RCCMD Shutdown "

Host: Please enter the target of the job, which is the IP address of the operating system or computer on which the RCCMD client is installed

Port: The default port is 6003 TCP – Make sure that RCCMD and CS141 are sending on the same port or listening for an incoming signal

Timing: When the CS141 is triggered to send an RCCMD Shutdown job. In this example, the job is sent when a power failure is active (Event Powerfail) and the UPS reports there are 600 seconds runtime available.
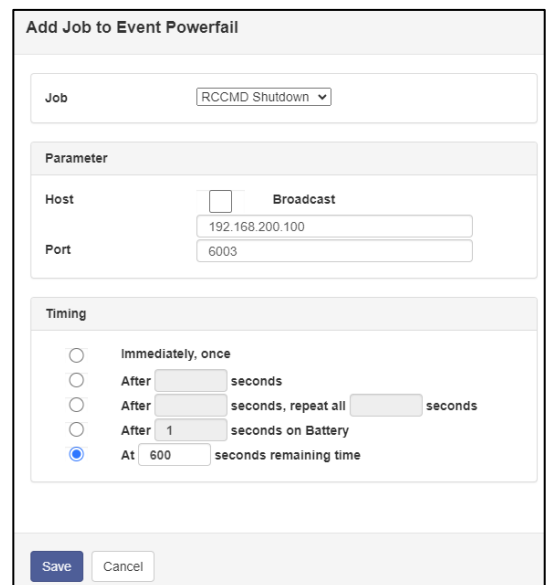
➔ **Please note, as both CS141 WEBMANAGERs must send an individually triggered shutdown signal, you need to carry out this configuration on both CS141 WEBMANAGER. RCCMD generally waits for both shutdown commands.**

3.   How to abort a partial shutdown request?
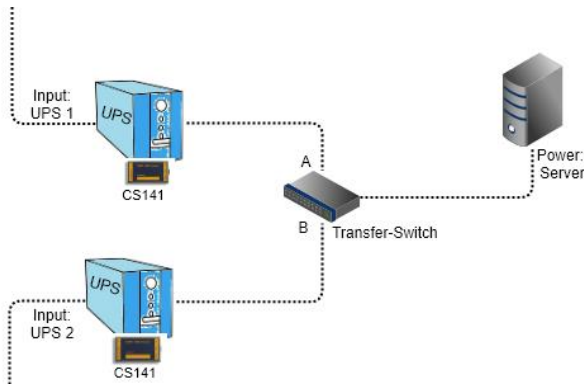
Let's recall this drawing… It is quite realistic that UPS 1 has a power failure that UPS 2 has never been affected by, since they are two separate circuits. With the current configuration, RCCMD can suppress the shutdown if both UPS systems were otherwise available but cannot independently determine whether the power failure at UPS 1 has been resolved. However, RCCMD meticulously keeps track of which UPS (or which CS141 WEBMANAGER) has already issued a shutdown command, and as soon as all UPS systems have done so, RCCMD will logically become active and shut down the server.

To meet this, the CS141 offers a special command that revokes its shutdown command:

RCCMD will then delete the shutdown command accordingly and fall back into normal operation. Since the counter event of Powerfail is Power Restored, simply define a corresponding counter job: At Power Restored, select the job "RCCMD Execute"

Job:	Select „RCCMD EXECUTE"
Host:	Please enter the target for this job, Enter the IP address of the RCCMD client you want to reach.
Port:	The default port is 6003 TCP – Make sure that RCCMD and CS141 are sending on the same port or listening for an incoming signal
.	
Command	Use the command „WAKEUP" at the command window – with this command, the CS141 will withdraw the RCCMD Shutdown command.
Timing:	When the CS141 is triggered to send an RCCMD Shutdown job. In this example, the job is sent when a power failure is active (Event Powerfail) and the UPS reports there are 600 seconds runtime available.
.	

Special case - When the CS141 detects a power failure, sends a shutdown command, and the UPS turns off to save the batteries

For now, the configuration is set up to react to end the power failure before the UPS shuts down. However, if the power failure lasts so long that the UPS decides to shut down completely to protect the batteries from deep discharge, then the next status when the UPS is started up would inevitably not be "Power Restored" because this status message is only issued by the UPS under the condition that a power failure has ended, and the UPS is still running.

When the UPS is restarted, the first event that triggers the CS141 WEBMANAGER is the "UPSMAN started" event, signalling that communication between the CS141 and the UPS has been successfully established and the CS141 is operational."

To ensure that the counter is reset on the respective RCCMD client in both cases, you should also assign the "RCCMD Execute" job with the WAKEUP command to start at UPSMAN started.

SSL TLS ON / OFF – Why an RCCMD seems to reject communication.

TLS is the abbreviation for **Transport Layer Security** and enables an encrypted connection between two IT systems. The method is always the same, regardless of whether it is communication between a web browser and a server, two infrastructure devices, or an infrastructure device and a server. During a handshake, it is verified that the sender and receiver are who they claim to be. Both endpoints then encrypt their communication with the certificates available.
Since the endpoints make themselves known to each other during this process, it is more difficult for a hacker to interfere with the communication and manipulate it

How a certificate works

Principally, an SSL certificate always consists of two parts: a public key and a private key. The private key is used to encrypt data, and the public key is used to decrypt it. The public key part is handed over to the respective recipient upon request after the handshake

From now, there are several different scenarios:

- The certificate is valid.
- The certificate is invalid, revoked, or damaged.
- The certificate is expired.
- The certificate is valid in principle, but its authenticity cannot be confirmed.
- …

From now, a communication often depends on the individual configuration of the communication partners:

1. SSL/TLS Web browser message: „Your communication is not safe "

This is because RCCMD provides for the web interface its own factory default certificate that fulfils several attributes:

- Valid time stamp
- Not revoked by a CA
- Fully functional
- In principle valid…

But: Since it is an in-house certificate, for obvious reasons there can be no signature to confirm the web browser he is communicating with exactly the RCCMD server it claims to be.
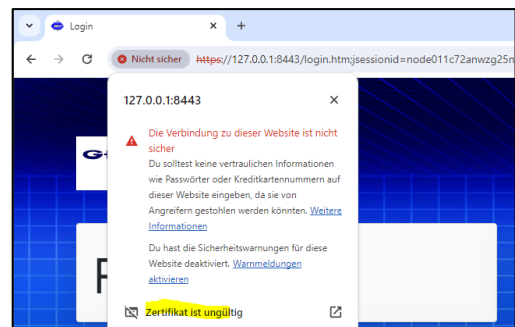
This is exactly what the web browser complains about and announces there may be a theoretical threat. A user must confirm this notification and active continue to the web interface. The web browser will show the web interface, but also the hint about an unsafe web space.

Newer versions of RCCMD provide a comfortable method to upload a valid company certificate as a standard PEM file.
At Network Configuration place the file and click on upload.
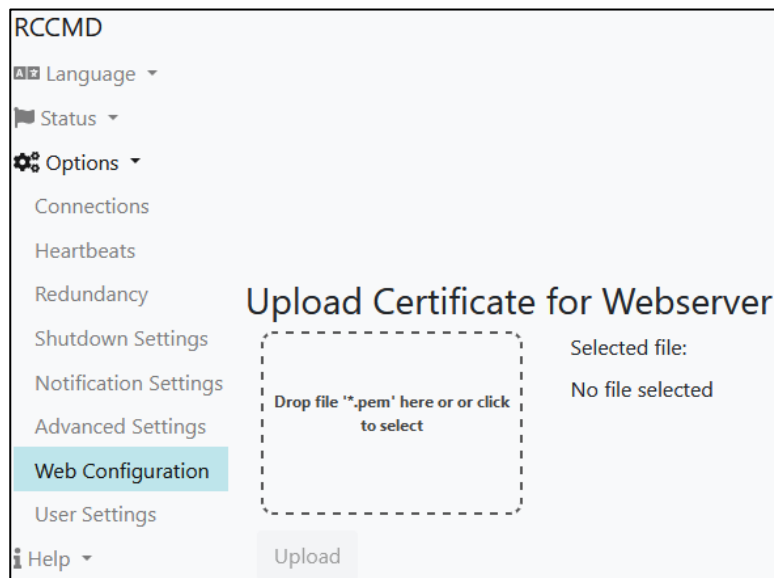
RCCMD will automatically import and activate the new certificate. If this notice still appears, it simply means that the web browser has something wrong with the new certificate.

Note:
Creating certificates made simple: In the CS141 user manual, you will find a complete tutorial on creating PEM files under Microsoft Windows. You can download the CS141 user manual at any time from the download area at www.generex.de.

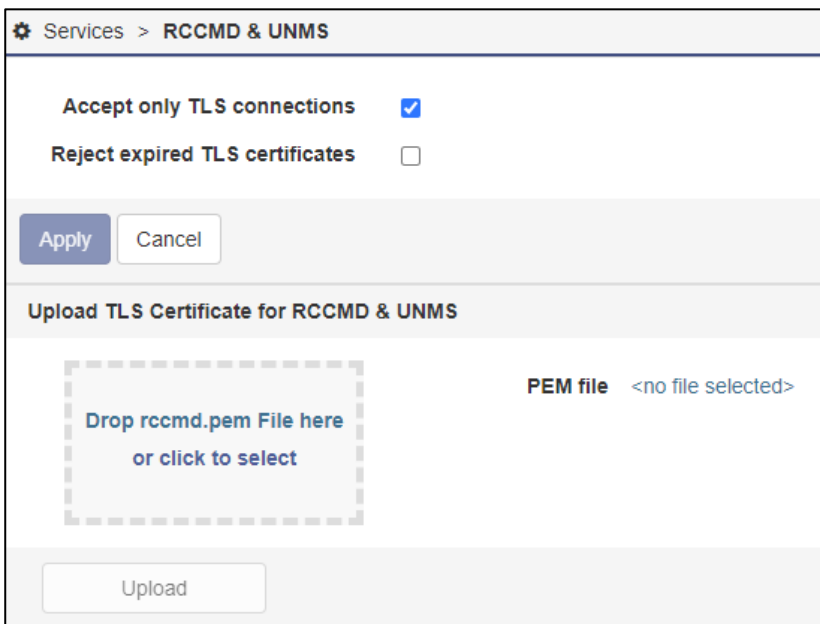*2. Communication RCCMD <-> CS141 does not work as expected*

Even though everything was set up correctly, RCCMD seems to simply refuse to communicate. There are basically 2 options that affect RCCMD:

a. At connections, SSL/TLS is not correct enabled on both (or more) endpoints:

At RCCMD:
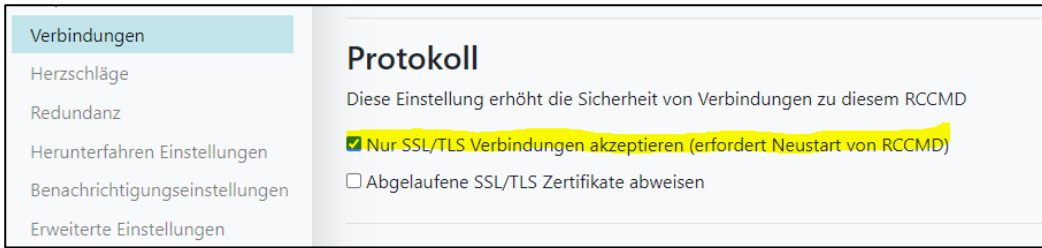
At your CS141 WEBMANAGER:

1. Problem: Using SSL / TLS is not harmonized

Accept only TLS connections must be set to either ON or OFF on all endpoints - otherwise one of the two sides will communicate unencrypted, which the other side will consequently reject-

2. Not synchronized certificates

This file can be found in the RCCMD installation folder:

This is not the PEM file for the web interface, but the certificate for communication CS141 <-> RCCMD or other RCCMD installations in your network. In order to use TLS / SSL communication, the certificate must be identical for all participants - if you have changed it, you must do the same for all other participants.

Exchange with RCCMD: Rename the rccmd.pem to rccmd.pem1 and copy your certificate as a PEM file to this location. Rename your PEM file to rccmd.pem. Restart RCCMD.

Exchange with a CS141: Rename your PEM file to rccmd.pem and drag the file into the prepared box. Press Upload. The CS141 will automatically upload and activate the file.

RCCMD on Windows Hyper-V (Windows PowerShell)

*Basic: An Introduction to Hyper-V*

HYPER-V is Microsoft's virtualization technology, which allows not only individual workstations but also entire server infrastructures to be operated within a virtual environment. The difference to VMware is that Hyper-V does not have a convenient vCenter, but is instead administered directly via PowerShell and scripts or script commands. This has its own special advantages and disadvantages.

Case 1: The stand-alone operating scenario without internal dependencies:

There are any number of Hyper-V servers that are not connected to each other. a, it would even be possible to shut down the entire Hyper-V environment with an RCCMD client and the appropriate scripts, but it is only recommended to a limited extent in this constellation, as the trust between the servers reacts very sensitively if you try to do so Execute script from one node to another.

It makes more sense here to install a separate RCCMD client on each Hyper-V node, which then executes the necessary scripts directly with local admin rights (the rules of the game change here in a failover cluster, but more on that later)

If you shut down a Hyper-V server locally in its standard configuration, the virtual machines are stopped, the respective operating state is saved and the main server is then shut down. After starting, the operating data is loaded again and the server continues to run. Whether stopping and saving works depends on what is running in the virtual machine:
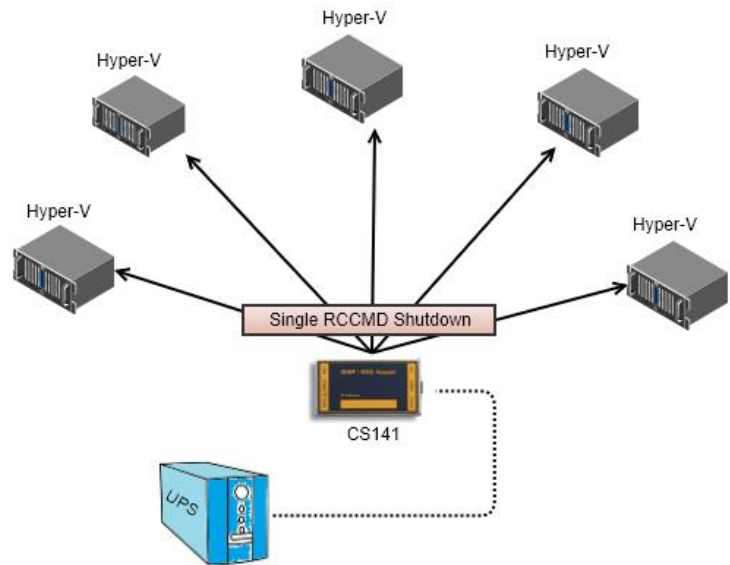
- Memory dumps can become very large

  It could happen that the available storage space on the main server is not enough to hold the operating data of all virtual machines.

- This is not possible due to the program

  Booking systems, rendering systems, programs with special shutdown routines, etc…. There are many applications that need to be turned off and shut down cleanly in the event of a shutdown.

Initiate a clean shutdown

If RCCMD receives the instruction from a CS141 / BACS system, it gives the local computer the shutdown command, but has no influence on what happens to the machines when the host operating system starts the shutdown procedure!

If you do not have Windows PowerShell installed or have disabled it, you can transfer shutdown control to the Hyper-V Manager and set there what should happen when the server is shut down:
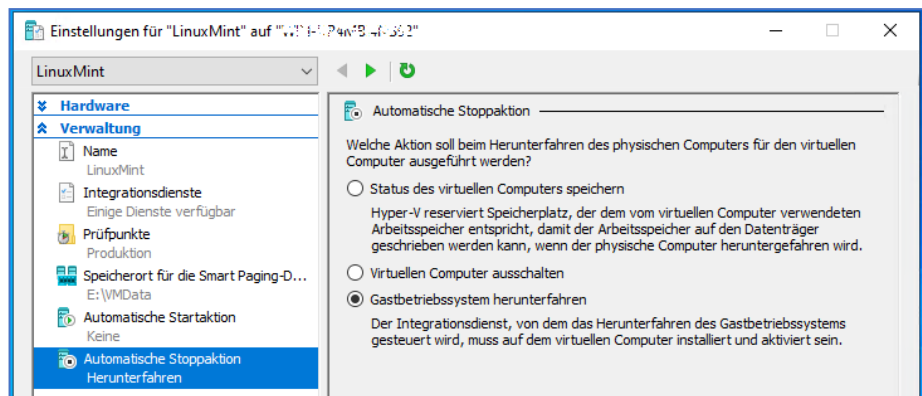
Save virtual machine state

In the event of a shutdown, a complete memory dump is created. Please check two things: Firstly, whether the server can provide enough memory, and secondly, whether the programs within the virtual machine generally support this function.

Turn off the virtual machine

The classic hard OFF on the virtual machine, depending on the operating system and usage, can lead to different problems

Shut down guest operating system.

The operating system within the virtual machine is instructed to shut down itself.

Case 2: Internal dependencies for virtual servers on a Hyper-V

This is basically the logical extension of case 1 - what if several virtualized systems are running on a Hyper-V node that have a mutual dependency or require a special shutdown order?

Now the difference to VMware becomes apparent: Instead of a graphical administration menu as used in VMware, Hyper-V uses PowerShell to implement such configurations.

In this example, 3 virtual systems are now running:

If you were to shut down Hyper-V, all 3 operating systems would definitely shut down. Two shut down while Windows 7 "saves and exits". As a user, PowerShell makes this relatively easy:

With the command **Get-VM** First get an overview of all currently running virtual machines:

The machines can then be operated with the command**Stop VM [machine name]**shut down:

To implement individual shutdowns, RCCMD offers 3 commands with which you can implement a structured server shutdown:

- Shut down a Hyper-V VM: Name a VM to shut down.
- Wait some seconds: Define a time window until the next job.
- Shut down all Hyper-V VMs: Shut down all virtual machines.
- Shut down System: Shut down the server.

With the correct sequence and time windows, you can shut down all virtual machines in a structured manner and then turn off the server.

The only condition: Windows PowerShell must be installed and activated.

Hyper-V with cluster management (PowerShell is required)

The communication in Hyper-V is very structured so that RCCMD can be operated without any further problems:
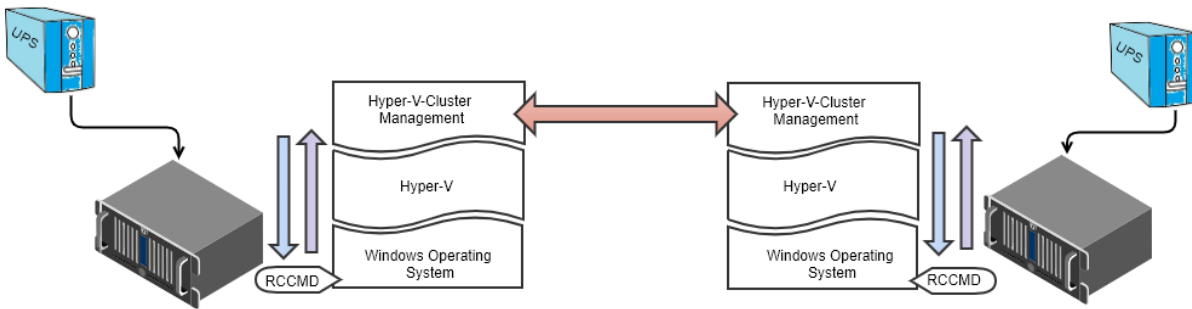
The higher-level instance is always informed first and the release is waited for accordingly. In the case of a shutdown via RCCMD, this means that the operating system announces the shutdown in Hyper-V. This organizes the structured shutdown of virtual machines. The carrier system is then shut down.

If there is a Hyper-V cluster manager, Hyper-V first informs it, which communicates with other cluster managers and organizes the migration of virtual machines. Once all machines have been moved to another server, Hyper-V then saves the remaining virtual machines and shuts them down. Once this has happened, the carrier system is shut down normally.

Planned vs. unplanned failover – preparing for simultaneous shutdown on 2 hosts

It becomes more difficult if you want to shut down both nodes (or hosts) in the event of a power failure:

To do this, you need to understand how virtual machines migrate between two nodes:

With two nodes, there is access to the VM storage, communication between the cluster nodes and a witness server through which both nodes determine who holds the so-called "quorum", i.e. who will provide the more current operating status.

In a failover cluster, a primary server is usually configured where the VM should run and a guest on which it may currently be running. In a failover cluster, the VHD file responsible for the virtual server is replicated and transferred to the registered guest and is regularly compared and updated with current operating data, with the executing node sending the data to its registered partners:

- In the event of a planned failover (e.g. a life migration or the shutdown of one of the two nodes), the cluster manager is given enough time to send its operating data and only then is the shutdown carried out

- In the event of an unplanned failover, the last available update is assumed, so some data loss may have occurred.

- If both nodes go "down" unplanned, then according to the quorum, the last saved current operating state that is available counts.

The problem lies hidden in the details:

The standard configuration of a FailOver cluster does not assume that both nodes will shut down in a planned manner. During a planned shutdown by the operating system, approximately 120 seconds are scheduled before the operating system shuts down in order to update the operating data and get the virtual machine running on another node. The catch is that with two nodes scheduled to shut down at the same time, a conflict of interest could inevitably arise: Node A will try to move all of its machines and operational data to Node B, and vice versa. This means that the machines may remain stuck in limbo and are then abruptly stalled by the shutdown of the node operating system. Depending on the size and complexity, there are different procedures:

Example: The very simple case

In the simple case, there are two nodes that form a fail-over cluster, and both nodes could host all virtual machines (or individual machines are excluded from the migration process). If you do not have PowerShell installed/activated, shut down the nodes sequentially: Node A transfers its data to Node B, hands over the virtual machines and then switches off. Afterwards, Node B will notice that the cluster has collapsed (Node A is already off

or in the process of shutting down) and will not attempt to migrate the virtual machines at all. With the RCCMD command "Shut down all virtual machines" all virtual machines can be shut down and the server switched off.
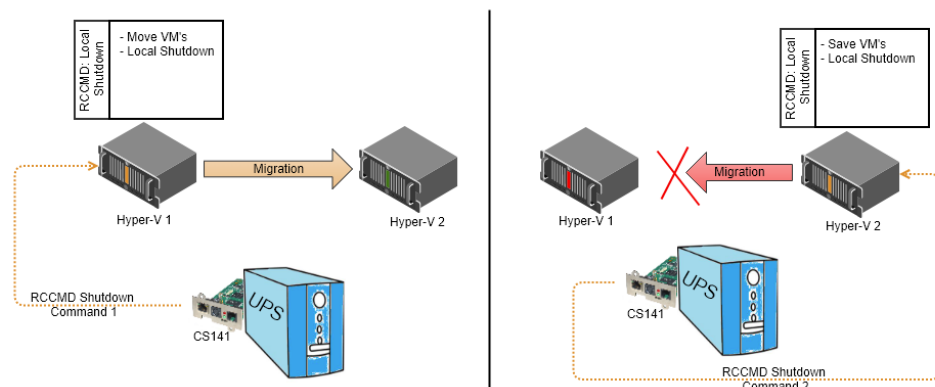
However, the shutdown via PowerStell is more recommended here:

To implement individual shutdowns, RCCMD offers 3 commands with which you can implement a structured server shutdown:

- Shut down a Hyper-V VM: Designate a VM to shut down
- Wait some seconds*: Define a time window until the next job
- Shut down all Hyper-V VMs: Shut down all virtual machines
- Wait some seconds*: Time window for the virtual machines.
- RCCMD shut down relay: Send the shutdown to the 2nd node**
- Shutdown System: Shut down the server

*Define the time windows so that the virtual machines have enough time to shut down and turn off on their own. You specify whether the virtual machines are saved or shut down in the properties of the virtual machine.

**On the second server you only need the Shut down System job, as all virtual machines have already been shut down cleanly and only the server needs to be shut down.

Advanced: Create your own Hyper-V commands for shutting down virtual machines on multiple nodes and quorum

Important: The following commands require the installation/activation of PowerShell:

PowerShell has established itself as a central component in the Microsoft environment and is indispensable for administrators and developers alike. Automating administrative tasks through scripts enables a more efficient and time-saving way of working. PowerShell 7 / Core expands the possibilities of script creation and execution with new features specifically tailored to server administration. Cross-platform availability and integration with other Microsoft products make PowerShell a universal tool for automating and optimizing IT processes.

The following versions are currently in circulation:

- **Windows Server 2012 R2:** PowerShell 3.0 is preinstalled but not enabled by default.
- **Windows Server 2016:** PowerShell 5.1 is installed and enabled by default.
- **Windows Server 2019:** PowerShell 5.1 is installed and enabled by default.
- **Windows Server 2022:** PowerShell 7.0 is installed and enabled by default.

A notice:

- Windows Server 2012 and earlier versions do not include PowerShell installed by default. However, you can manually install PowerShell on these systems.
- The latest version of PowerShell can be manually installed at any time on any Windows system, regardless of the server version.

After you have installed PowerShell, you can use two special Hyper-V commands that RCCMD offers to manage virtual machines within a Hyper-V environment:

Shut down a specific Hyper-V VM

You can use this PowerShell command to shut down a specific virtual machine. The name of the virtual machine is specified in the input dialog.

There are two different use cases here:

1. Local Hyper-V

The local Hyper-V Manager will shut down and terminate exactly this one VM. For this purpose, the

2. RCCMD is installed on the cluster manager

If the cluster manager is active, this command will be transmitted to the Hyper-V network, and the node on which the VM is currently running will execute the command.

Important: If the virtual machine migrates to a node that is not part of this cluster, the machine will no longer be shut down, even if the cluster manager knows where the virtual machine is currently located.

Shut down all virtual machines

The difference to a virtual machine is that the Hyper-V Manager asks for a list of all virtual machines with the status "running" and then shuts them down using the "stop-vm" command.

Here, too, there are two possible applications:

1. Local Hyper-V (Without Cluster Manager!)

In this case, all locally running virtual machines are shut down in a structured manner and the virtual machine is terminated properly.

2. On the cluster manager

The cluster manager requests all virtual machines that have the status "running". With the stop-vm command, the virtual machines in the cluster are shut down regularly and the VMs are terminated.
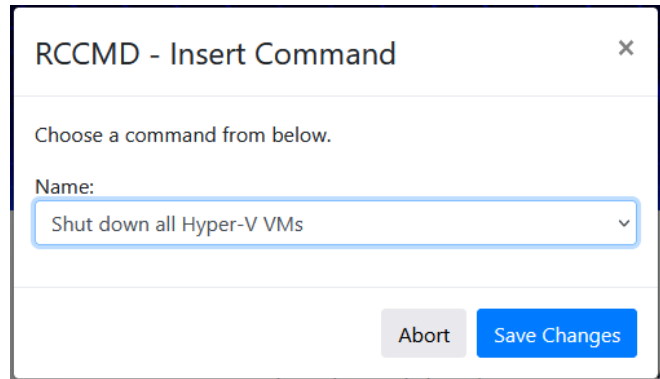
Tip: Hyper-V works context-related

These two commands allow a structured shutdown of all virtual machines on a Hyper-V server or an entire Hyper-V cluster. What is executed depends heavily on the respective context.

Shutdown command sequence with RCCMD on a Hyper-V with 3 virtual machines

1. On a Hyper-V single server

In this constellation, a separate RCCMD client is required on each Windows host. The shutdown is triggered locally and the virtual machines are to be shut down:

1. Shut down a Hyper-V VM

This would be, for example, the management server, which must be shut down before the database server. Enter the name of the virtual machine that you chose when creating it.

2. Wait a few seconds

In this example, 90 seconds were entered. So RCCMD will give the operating system 90 seconds before starting the next item in the list.

*3. Shut down all Hyper-V VMs*

RCCMD requests the Hyper-V Manager to list all virtual machines in the Running status and instructs the Hyper-V Manager to shut down the operating systems.

4. Wait a few seconds

Give the operating systems time to organize the shutdown and terminate the virtual machines in an orderly manner.

5. Shut down system

The Hyper-V PC shuts down and the server turns off. Please note that this command will hard shut down the virtual machines that are still running. Please plan a correspondingly large time window under point 5.
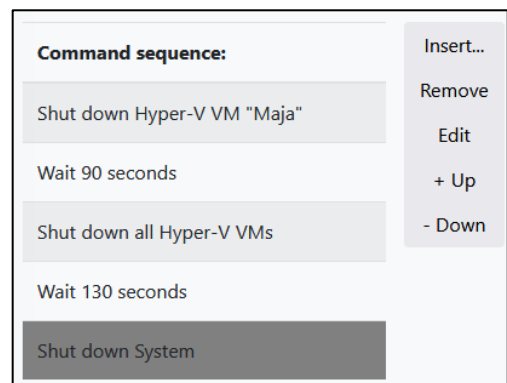
If you have a VM running that requires a special shutdown routine

As a preparatory measure, forward the RCCMD signal directly to the operating system of the corresponding virtual machine and delay the shutdown by an appropriate time window. In this case, you configure the individual shutdown within the RCCMD client to which you forwarded the shutdown.

Please note that an RCCMD client must be installed on the guest system for this function.

In this case, a guest system is first instructed to shut down before the local shutdown described above takes effect.
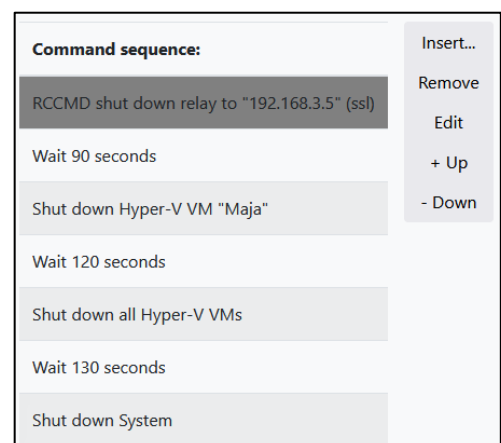
2. For a Hyper-V cluster with multiple nodes and cluster manager

If there are several nodes with a cluster manager, it is important where the shutdown commands come from: Simply shutting down nodes in a cluster locally is not recommended because this can lead to data loss and damage to the virtual machines running on the node and the operating system. The problem increases with the number of nodes that are simply shut down.

In this case it is recommended to use the cluster manager, which - unlike VMware, for example - runs as a service on every node: You can therefore initiate a structured cluster shutdown for every node that is a member.

What is important is not which node the cluster manager receives its commands from, but rather the order in which the commands are entered:

1. Shut down all Hyper-V VMs

Get-VM|Where object{$_.state-eq "Running"} |Stop VM

The cluster manager requests all virtual machines with the status "running" from the nodes in this cluster and organizes a local shutdown.

2. Backup cluster state:

Save ClusterCheckpoint <Production_1>

This command backs up the state of the cluster so that it can be restored later if necessary.

3. Cluster stop and local shutdown

Get ClusterNode|Where object{$_.state-eq "Up"} |Stop ClusterNode

After all virtual machines are shut down, you can safely stop the Hyper-V cluster and shut down the nodes using Cluster Stop.


Tip: Pay attention to loaded modules

Some commands can only be executed if the Windows PowerShell modules are installed and loaded.

How to customize the Shutdown.bat in the RCCMD:

Part 1: Creating the first Hyper-V command:

1. In the RCCMD shutdown options, use the Hyper-V command "Shut down a Hyper-V VM" and enter the name of a VM under VM name.

2. Change the backups

3. Create the job "Wait a few seconds" and assign 90 seconds, for example.

4. Press Save at the top right to write your changes to the batch file. In this case, it is not necessary to restart RCCMD as you still need to make further settings.

5. Press F5 to refresh the web display.
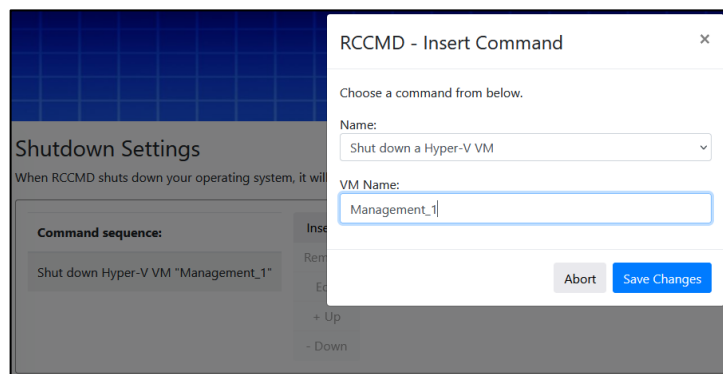
You can then edit the settings file directly in the web browser by clicking on "Edit file".

Part 2: Adjust shutdown order.

The command sequence should now contain 3 lines:

1. Shut down Hyper-V VM "XXXX".

2. Wait 90 seconds

3. Shut down system

These commands are executed in exact order from top to bottom. It is important to know: Everything that is written after the system shutdown can no longer be executed because the local operating system shuts down. Then press Edit File and add the desired commands - the previously entered commands can serve as a blueprint to expand:

Simply add the commands you need.
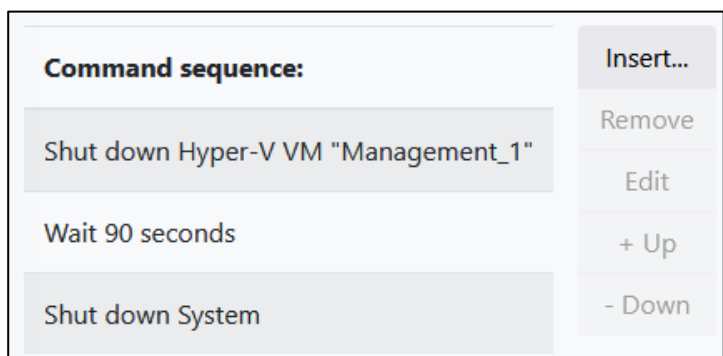
Example 1: Hyper-V WITHOUT: Cluster Manager

```
rem created by setup
@echo off
set path=%path%;C:\Program Files (x86)\RCCMD
@cls

PowerShell.exe Stop-VM "Management-Server-1"
gxSleep.exe 90
PowerShell.exe Stop-VM "Database-Server-1"
gxSleep.exe 90
PowerShell.exe Get-VM | Where-Object {$_.State -eq "Running"} | Stop-VM
gxSleep.exe 90
ExitWin.exe shutdown force
```

The command sequence would be executed from top to bottom in this order:

1. PowerShell.exe Stop-VM "Management-Server-1":	Management Server 1 is shut down
2. gxSleep.exe 90	RCCMD will wait 90 seconds
3. PowerShell.exe Stop VM "Database Server-1"	Database Server 1 is shut down
4. gxSleep.exe 90	RCCMD waits 90 seconds
5. PowerShell.exe Get-VM	Where-Object {$_.State -eq "Running"}	Stop VM	All VMs that are still marked as active are shut down
6. gySleep.exe 90	RCCMD waits 90 seconds
7. ExitWin.exe shutdown force	The host shuts down

Example 2: Hyper-V with multiple nodes and cluster manager

A few further adjustments would be necessary here:

```
rem created by setup
@echo off
set path=%path%;C:\Program Files (x86)\RCCMD
@cls

PowerShell.exe Stop-VM "Management-Server-1"
gxSleep.exe 90
PowerShell.exe Stop-VM "Database-Server-1"
gxSleep.exe 90
PowerShell.exe Get-VM | Where-Object {$_.State -eq "Running"} | Stop-VM
gxSleep.exe 180
PowerShell.exe Save-ClusterCheckpoint <Production_1>
gxSleep.exe 90
PowerShell.exe Get-ClusterNode | Where-Object {$_.State -eq "Up"} | Stop-ClusterNode
```

1. PowerShell.exe Stop-VM "Management-Server-1":	Management Server 1 is shut down
2. gxSleep.exe 90	RCCMD will wait 90 seconds
3. PowerShell.exe Stop VM "Database Server-1"	Database Server 1 is shut down
4. gxSleep.exe 90	RCCMD waits 90 seconds
5. PowerShell.exe Get-VM	Where-Object {$_.State -eq "Running"}	Stop VM	AllVMs that are still marked as active are shut down
6. gxSleep.exe 180	RCCMD waits 180 seconds
7. PowerShell.exe Save-ClusterCheckpoint <Production_1>	The current state of the "Production_1" cluster is saved.
8. gxSleep.exe 90	RCCMD waits 90 seconds
9. PowerShell.exe Get-ClusterNode	Where-Object {$_.State -eq "Up"}	Stop ClusterNode	All nodes that are running will be shut down. This includes the node from which the commands were entered.

The ExitWin.exe shutdown force command is not necessary because the server is shut down via Stop-ClusterNode.

Tip: Plan time slots

These examples assume idealized time windows (gxSleep.exe) - Adjust the time windows to the respective shutdown realities to avoid problems.

Important PowerShell Hyper-V commands:

1. Get-VM: Shows all virtual machines on the Hyper-V server.
2. Startup VM: Starts a virtual machine.
4. Stop VM: Shuts down a virtual machine.
7. Save VM: Saves the state of a virtual machine.
8. Restore VM: Restores the state of a virtual machine from a snapshot.
9. Export VM: Exports a virtual machine to a file.
10. Import VM: Imports a virtual machine from a file.

Important Hyper-V Cluster Manager commands in PowerShell:

1. Get cluster: Shows information about all clusters in the Failover Cluster Manager.
2. Get-ClusterNode: Displays information about all nodes in a cluster.
3. Get-ClusterResource: Displays information about all resources in a cluster.
4. Start ClusterNode: Starts a node in a cluster.
5. Stop ClusterNode: Shuts down a node in a cluster.
6. Stop cluster: Stops a cluster and migrates VMs to other nodes.
7. Resume Cluster: Putsa stopped cluster.
9. Move-ClusterResource: Moves a resource to another node in the cluster.

Direct PowerShell Skripting RCCMD: The Windows PowerShell- Mode

This function is available with RCCMD for Windows from version 4.57.12 240417 or later software versions.

From version 4.57.x 240417 onwards, select at "Shutdown Settings" between the PowerShell mode* and "classic batch mode":

) Windows PowerShell required, only with RCCMD for Windows

The difference is that instead of "shutdown.bat" (batch mode), the "shutdown.ps1" script is started with the necessary local administrative shares - commands are now given directly to the operating system via the more modern Windows PowerShell, which offers numerous options which can sometimes only be implemented with great effort within the batch file.

- As in batch mode, under "Insert" you will find ready-made module commands that you can use directly to shut down the operating system.
- Experienced system integrators will find "Edit File" a slim web editor with which they can adapt shutdown.ps1 directly to the respective application scenarios.

Tip: Mixing batch files and PowerShell scripts

W If you want to combine PowerShell scripts and batch files, we recommend using PowerShell mode, as it is much easier to integrate a batch file as a subprocess into a PowerShell script. A batch file would also start a PowerShell script, but it is very time-consuming to monitor the process afterwards.

The main difference to batch mode is that Windows PowerShell is specifically designed for managing servers, which allows you to manage complex server structures natively and transparently automatically in the event of problems and shut them down in a structured manner if necessary.

I keep reading about Java, and since there is a connection to RCCMD - is there potential security breach?

Well, one JRE to find them, one JRE to bind them all, one JRE to manage RCCMD functions at all... OK, nearly 84% of all software on the market uses java - due to this fact, your question is right, but we need to differ between "Java" and "These unsafe java based pieace of software press is talking about" – These FAQ'S should clear up a little with the misunderstandings:

Depending on Java, what does RCCMD use?

Das Webinterface von RCCMD verwendet eine Java Runtime Envirommemt (JRE) für bestimmte **interne** Prozesse – es gibt keine Möglichkeit, „von außen" auf diese internen Prozesse zu gelangen, um alternative Prozesse zu starten, ausgenommen natürlich grobe Fahrlässigkeit wie das Behalten der Standardpassworten …

The RCCMD web interface uses a Java Runtime Environment (JRE) for certain internal processes, and there is no way to access these internal processes from the outside to start alternative processes, except of course for gross negligence such as retaining the default passwords.

Are license fees due for the use of Java?

No, the Java Runtime Environment currently has nothing to do with what you can download and install under "Java.com" and for which companies have to pay license fees. RCCMD comes with everything you need out-of-the-box for secure operation.

Our security program shows the note that an outdated Java version has been found with the note "potential security risk".

Many inexpensive security programs declare older software to be a potential vulnerability by default - and often ignore the intended use of this software, or whether a development team at GENEREX has made special adjustments to secure professional software such as RCCMD - experts appreciate operational stability and the highest security standards: the latest program version is not always the best choice when it comes to stability and performance, not to mention innovative new security issues that did not exist before. For this reason, screening software finds (at least as of this FAQ) version 11 and complains that there is no version 18.

Can I get a list of the modules your JRE uses?

No (and we don't discuss that either…). What we can offer you is that you send us an excerpt of your security audit, and then we can explain exactly what your security scanner has found. To do this, simply contact Support@generex.de.

Glossary – Important Abbreviations

- RCCMD: Remote Control and Command, a software tool for remotely managing and shutting down computers and servers.
- VM: Virtual Machine.
- ESXi: VMware ESXi, a hypervisor for virtualizing servers.
- OVA: Open Virtual Appliance, a virtual machine format supported by many vendors.
- vCenter: VMware vCenter, a tool for managing virtual machines in a VMware environment.
- HA: High Availability, a method for ensuring server availability in the event of a failure.
- DHCP: Dynamic Host Configuration Protocol, a protocol for automatically assigning IP addresses to computers on a network.
- DNS: Domain Name System, a system for translating domain names into IP addresses.
- TLS: Transport Layer Security, a protocol for encrypting data on the Internet.
- HTTP: Hypertext Transfer Protocol, a protocol for transmitting web content.
- IP: Internet Protocol, a protocol for addressing computers on a network.
- GUI: Graphical User Interface.
- CLI: Command Line Interface.
- SSH: Secure Shell, a protocol for secure remote computer management.
- VMA: Virtual Media Assistant, a VMware tool for managing virtual media.
- IPv4:   Internet Protocol version 4, a protocol for addressing computers on a network.
- IPv6:   Internet Protocol version 6, a new protocol for addressing computers on a network.
- vSAN: Virtual SAN, a software-defined storage system from VMware.
- RAID: Redundant Array of Independent Disks, a method for increasing data security and availability by using multiple hard drives.
- NFS: Network File System, a protocol for sharing files and directories over a network.
- iSCSI: Internet Small Computer System Interface, a protocol for storing data on a server over a network.
- USB: Universal Serial Bus, a standard for connecting devices to computers.
- PCI: Peripheral Component Interconnect, a bus standard for connecting devices to computers.
- BIOS: Basic Input/Output System, a software program that runs every time a computer starts up.
- UEFI: Unified Extensible Firmware Interface, a new BIOS standard.
- MBR: Master Boot Record, a bootloader on MBR-style hard drives.
- GPT: GUID Partition Table, a new partition style for hard drives.
- PKS-1:   Public Key Cryptography Standard 1, an asymmetric encryption method.
- PKS-8:   Public Key Cryptography Standard 8, a format for storing private keys.
- CS141:   A fully qualified web manager manufactured by GENEREX. Serves as an RCCMD server for the RCCMD client.
- BACS: Battery Analysis and Care System: A fully qualified and scalable active battery management system manufactured by GENEREX. A BACS WEBMANAGER also functions as an RCCMD server for RCCMD control signals.
- Hyper-V: A free virtualization platform developed by Microsoft that is available within a Microsoft Windows operating system. Hyper-V can be installed as needed using its features and can virtualize any operating system.
- MAC OS: An operating system developed and distributed by Apple. Typically runs only on an Apple computer.

Intellectual Property Copyright Statement and Handling of Confidential Informationn

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

GENEREX, as the manufacturer of the products mentioned, assumes no obligations with this information. The products described in this manual have been given on the sole basis of information for business partners to gain a better understanding of GENEREX products.

All rights, titles and interests in and to the GENEREX Trademark BACS or logo (registered or unregistered) or GENEREX goodwill or intellectual property, copyright and product patents are owned exclusively and without restriction by GENEREX.

GENEREX will deal with any complaint about the contents of this document in a timely manner. Comments or complaints about this document should be addressed to GENEREX Systems Vertriebsgesellschaft mbH.

European Union copyright law is valid (Copyright EU).

Copyright (c) 1995-2021 GENEREX GmbH, Hamburg, Deutschland.

All rights reserved