bintec elmeg

Colibri NetManager

Virtual appliance

Copyright© Version 1.1 8/2016 Teldat

Legal Notice

Warranty

This publication is subject to change.

Teldat offers no warranty whatsoever for information contained in this manual Teldat is not liable for any direct, indirect, collateral, consequential or any other damage connected to the delivery, supply or use of this manual.

Copyright © Teldat.

All rights to the data included, in particular the right to copy and propagate, are reserved by Teldat.

Table of Contents

Chapter 1 Installation and commissioning of Virtual Colibri NetManager 1

1.1 Requirements 1
1.1.1 System requirements for the virtualization platform 1
1.1.2 Network requirements 1

1.2 Installation and configuration of virtual machines 2
1.2.1 Storage server configuration 2
1.2.2 Service configuration 8
1.2.3 Testing installation 18

1.3 Licensing 19
1.3.1 Installation of the server license 19
1.3.2 Installing device licenses 21

1.4 Managing devices 26
1.4.1 Adjusting the management URL in the device 26

1.5 Notes regarding free software 26

Chapter 1 Installation and commissioning of Virtual Colibri NetManager

1.1 Requirements

- A Virtual Colibri NetManager server license
- The installation files obtained with the purchase of a Virtual Colibri NetManager Server license
- A Virtual Colibri NetManager device license for every device that is going to be managed
- A virtualization platform that is ready for operation and in line with system requirements
- A registered user on the Colibri NetManager portal that is able to activate the license

1.1.1 System requirements for the virtualization platform

The server requires two virtual machines. The following hypervisors are considered: VMWare ESXi (5.1 or higher) or Citrix XenServer (6.0 or higher)

- Virtual machine #1 (VM1): "Storage"

- Virtual machine #2 (VM2): "Service"

Minimum requirements for up to 100 devices

Virtual Machine ID	Storage size	# CPU	CPU clock	RAM
VM1	50 GBytes	1	> 1 GHz	2 GBytes
VM2	20 GBytes	1	> 1 GHz	2 GBytes

Requirements for 5000 devices

Virtual Machine ID	Storage size	# CPU	CPU clock	RAM
VM1	1 TBytes	4	> 2 GHz	16 GBytes
VM2	64 GBytes	2	> 2 GHz	8 GBytes

The virtual machines must be able to "see" each other within the network. This generally means that the network adapter in the hypervisor has been set to **bridged**.

1.1.2 Network requirements

Those who, from a technical and firewall perspective, would like to keep the virtual machines as far from each other (and from the rest of the network) as possible should follow these steps. All other users can simply ignore this section.

- When between "Service" and "Storage", the following requirements are applicable:

- "Service" requires mysql access to "Storage" (TCP Port 3306).

- "Service" is the NFSv4 client of "Storage" (TCP Port 111 and 2049).

- "Service" requires ssh access to "Storage" (TCP Port 22) during an update to a newer service version.

- From the outside, the following is necessary:

- Devices managed by the server require HTTPS or HTTP access to the configured port for "Service" (Default: 8443, 8080).

- Users of the web interface also require HTTP(S) access to the Service computer.

The "Storage" must not be accessible from the outside.

1.2 Installation and configuration of virtual machines

Both virtual machines are, for the most part, default installations of a Debian GNU Linux server. The relevant configuration menu is displayed on the console. Logging in is not necessary. As usual, six virtual consoles are configured and it is possible to switch between them using keys **Alt-F1** to **Alt-F6**. Virtual consoles 2 to 6 show the normal login. As no valid root-password has been created, logging in is not possible at first. (An explanation on how to issue that kind of password is offered later on).

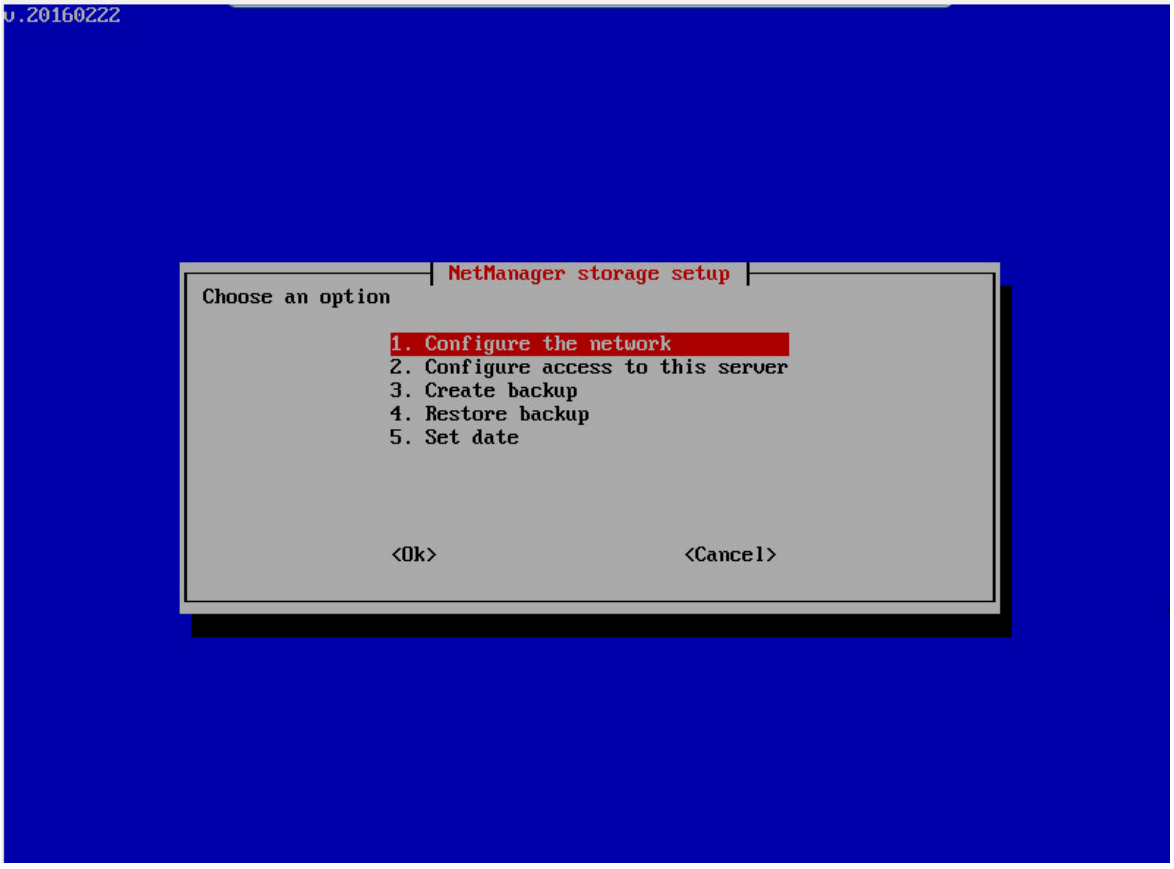
As an example, we will configure both virtual machines in a common network segment 192.168.0.0/24. "Storage" receives IP address 192.168.0.185, "Service" receives IP address 192.168.0.186, Standard Gateway and Name Server both get IP address 192.168.0.254.

1.2.1 Storage server configuration

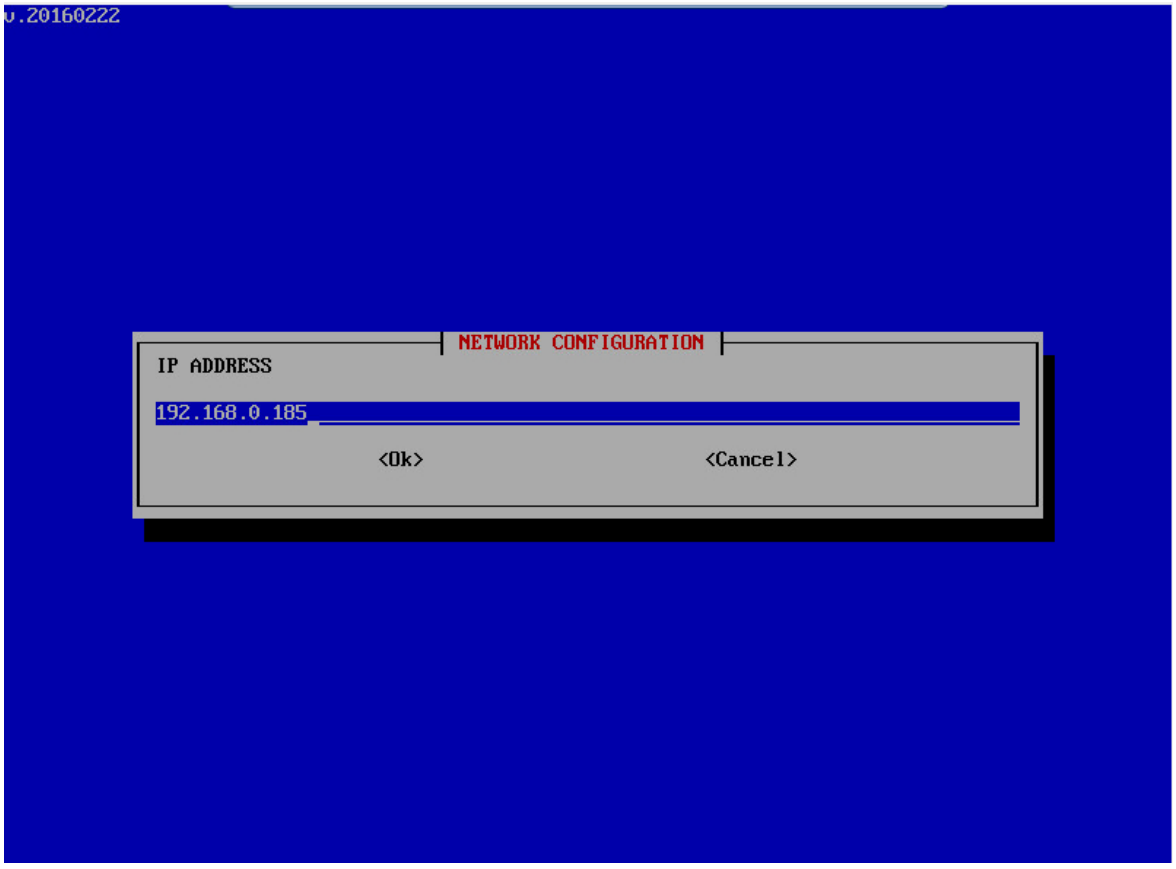
Once the storage server has started, the configuration menu appears automatically. Logging in is not necessary.

Network configuration

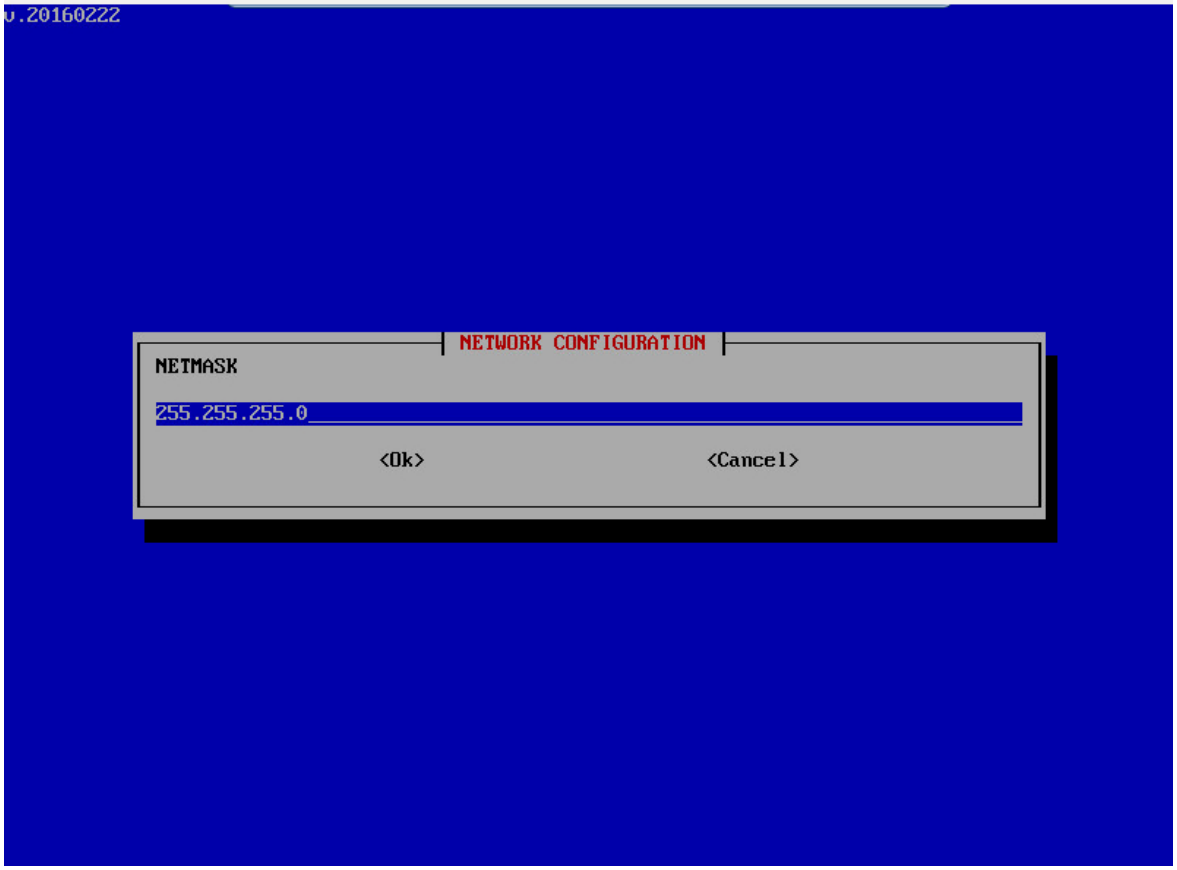
(1) To configure the **network**, select option 1 in the main menu: **Configure the network**.



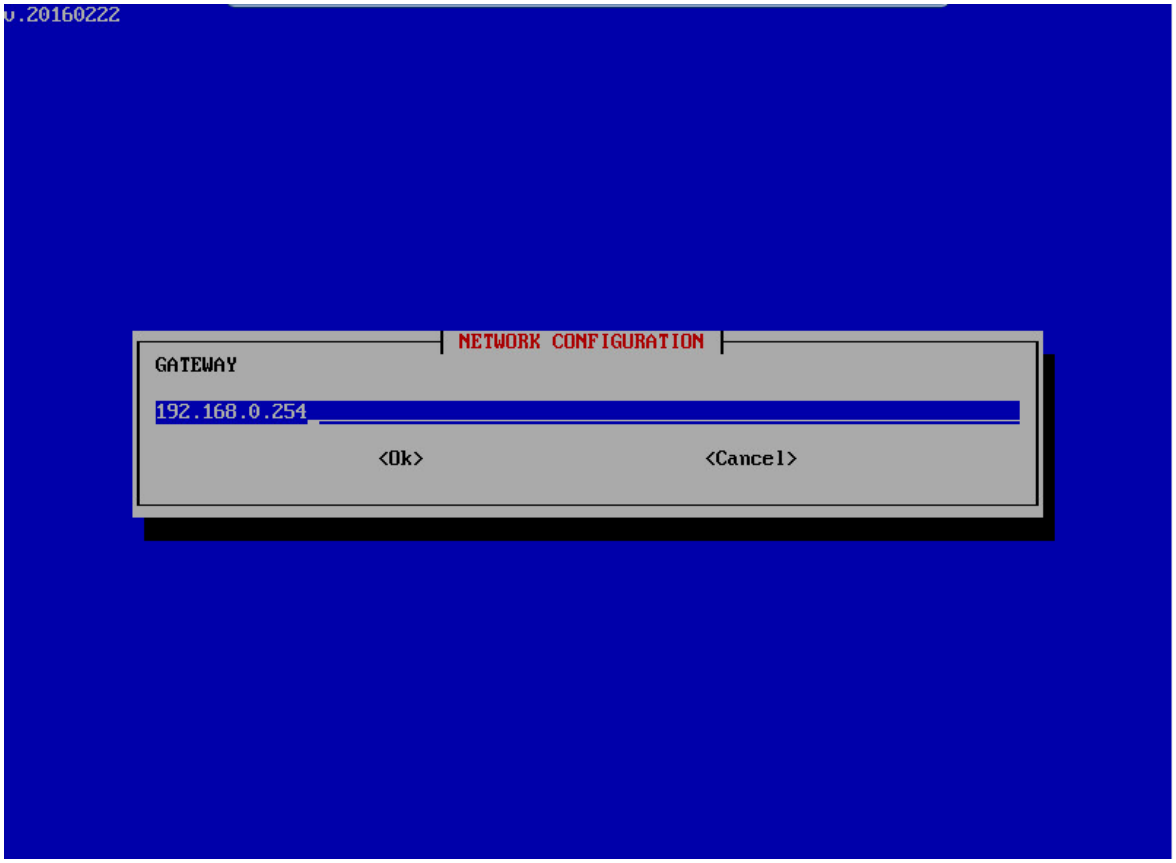
(2) Then enter the **IP address** of the storage server. In the case of our example, it is *192.168.0.185*.



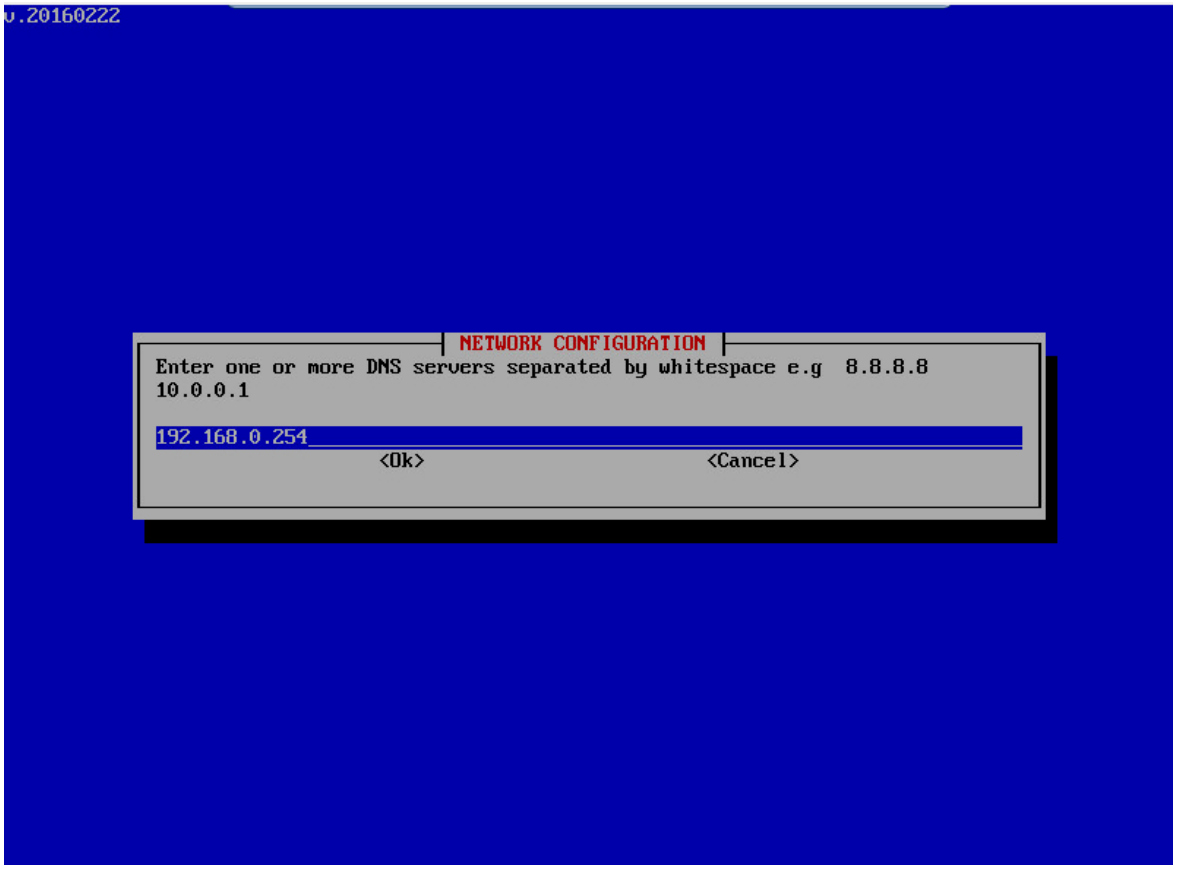
(3) The **netmask** is entered here. In our example, it is *255.255.255.0*.



(4) Then enter the **Gateway IP address**. In the case of our example, it is *192.168.0.254*.



(5) The **DNS server address** must be entered next. In our example, it is *192.168.0.254*.



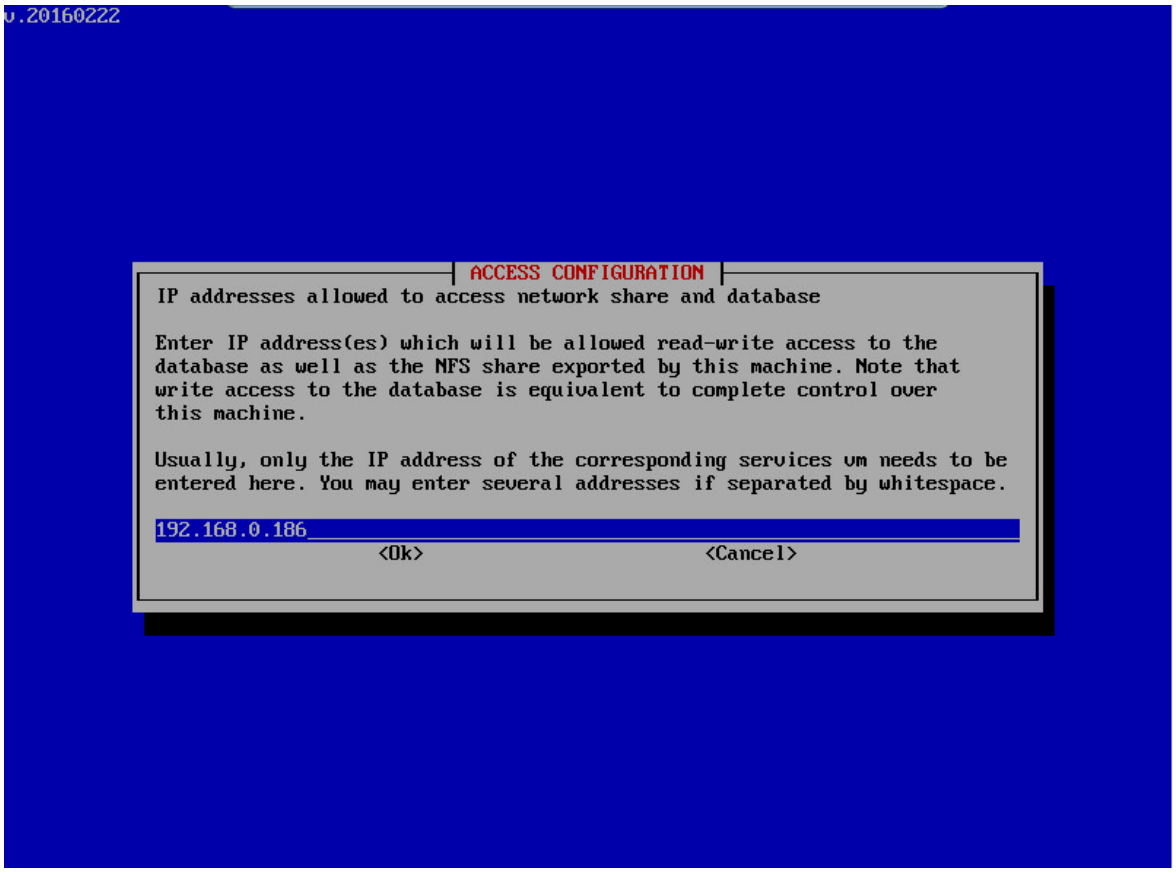
At this point, the **network configuration** is complete.

Access to the storage server

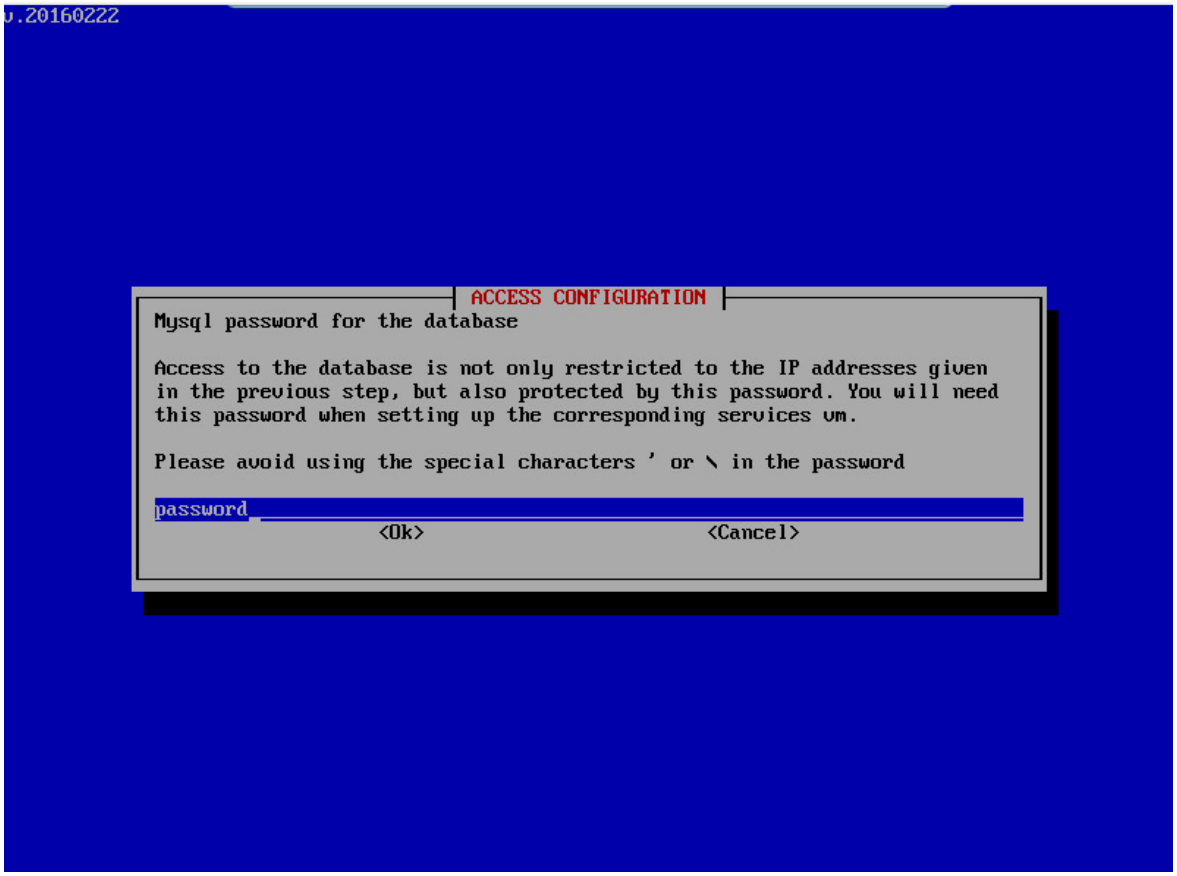
Access to the storage server must be configured next. To do so, select option 2 in the main menu: **Configure access to the storage server**.

(1) The **IP address** of the server that can access the storage server is entered first. In our example, this is

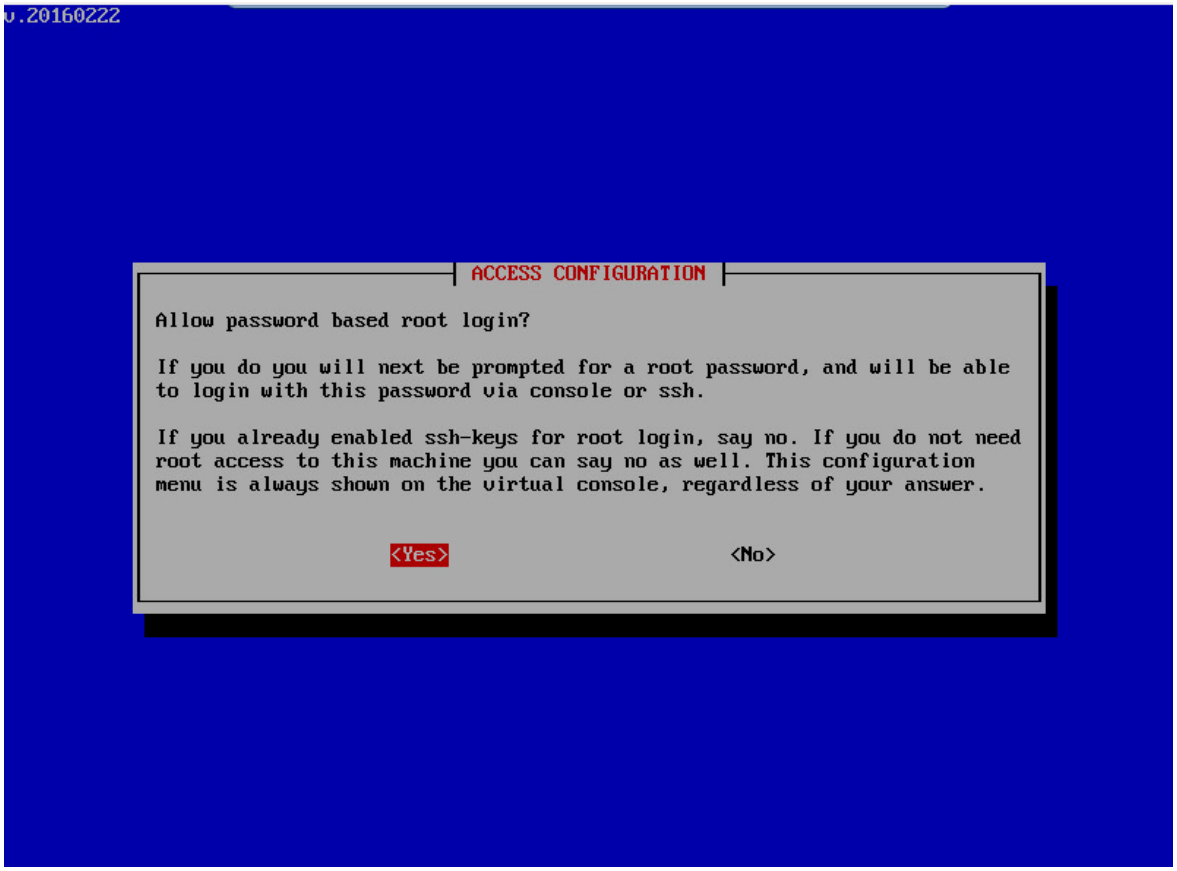
192.168.0.186.



(2) A **database password**, allowing the storage server to be reached, must be issued next.



(3) To be able to log in directly using Shell or SSH as *root*, a **root password** must be created.



When this message appears, access to the storage server has been fully configured.

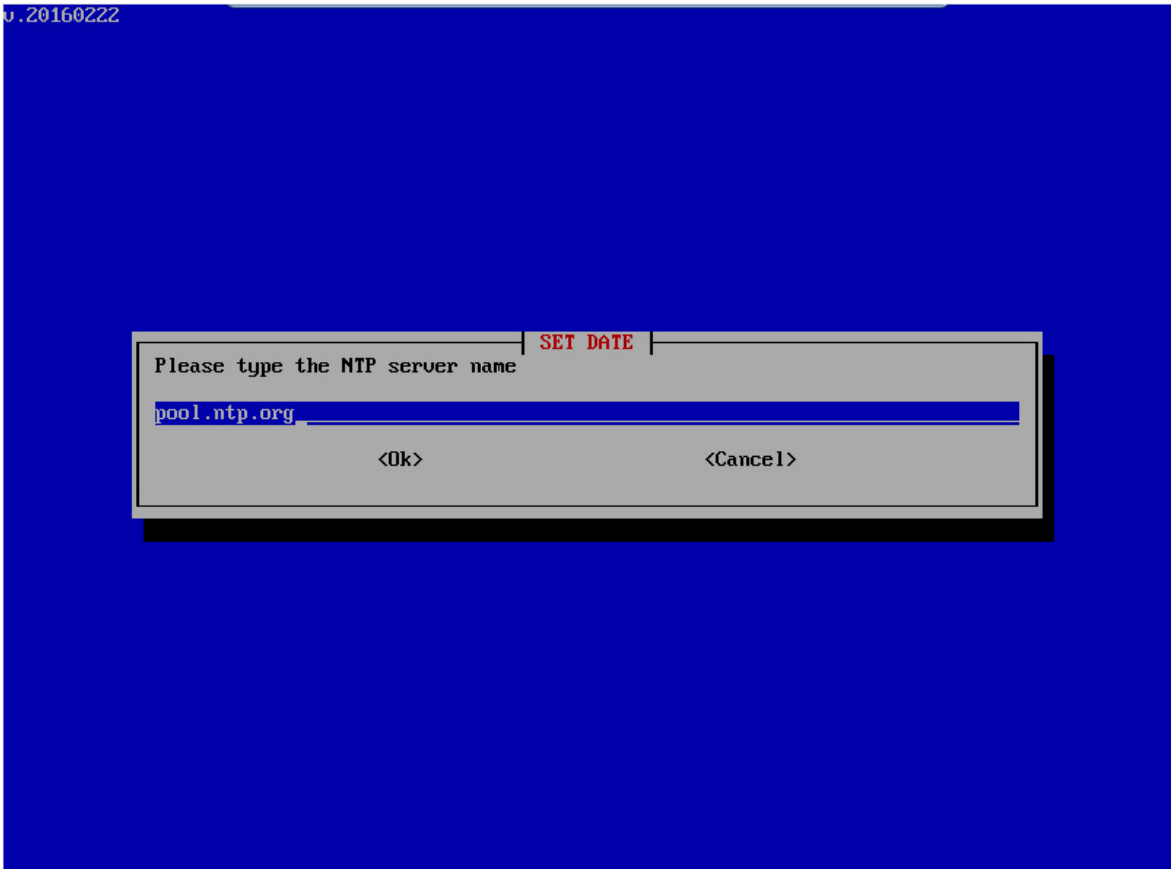
Set the storage server date

The last thing that needs to be configured is the storage server date. To do so, select the **Set date** option in the main menu.

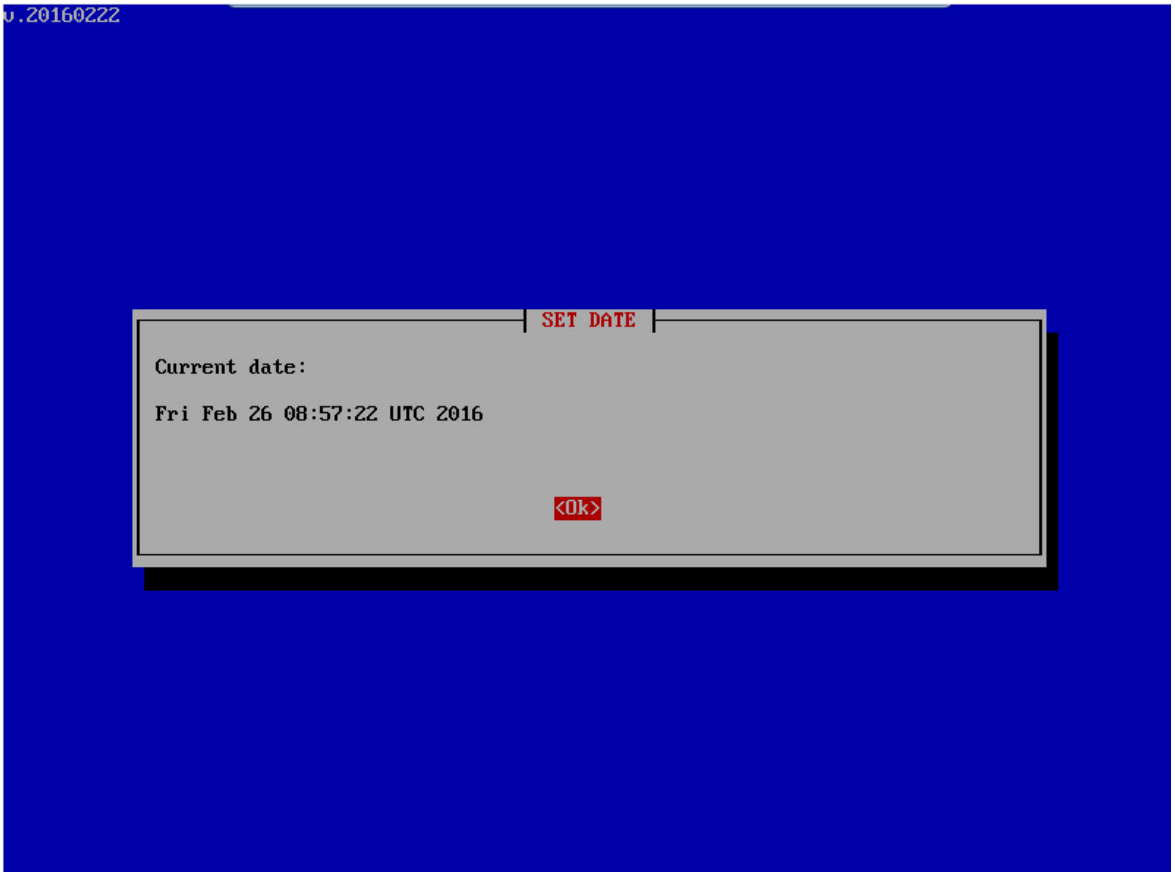
(1) You can chose one of two methods to configure the server date: NTP or Manually.

(2) If you choose the NTP method, enter the NTP server you want to use. By default, this parameter is

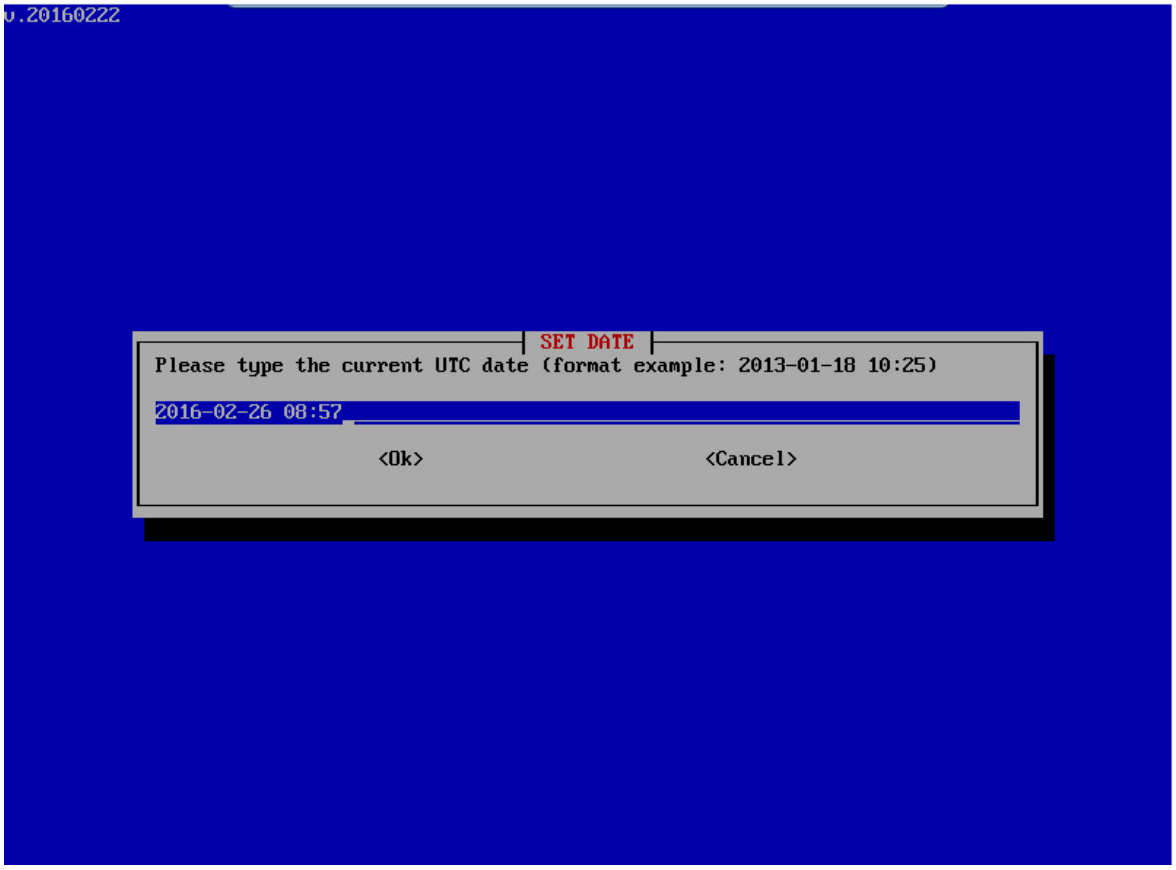
pool.ntp.org



(3) After some seconds, if connecting with the NTP server was possible, a screen pops up and a message appears showing the current server date.



(4) If you choose to do it manually, you must enter the date yourself. After this, if the date format is correct, the current date is shown in a manner similar to the way it appeared when using the NTP method.

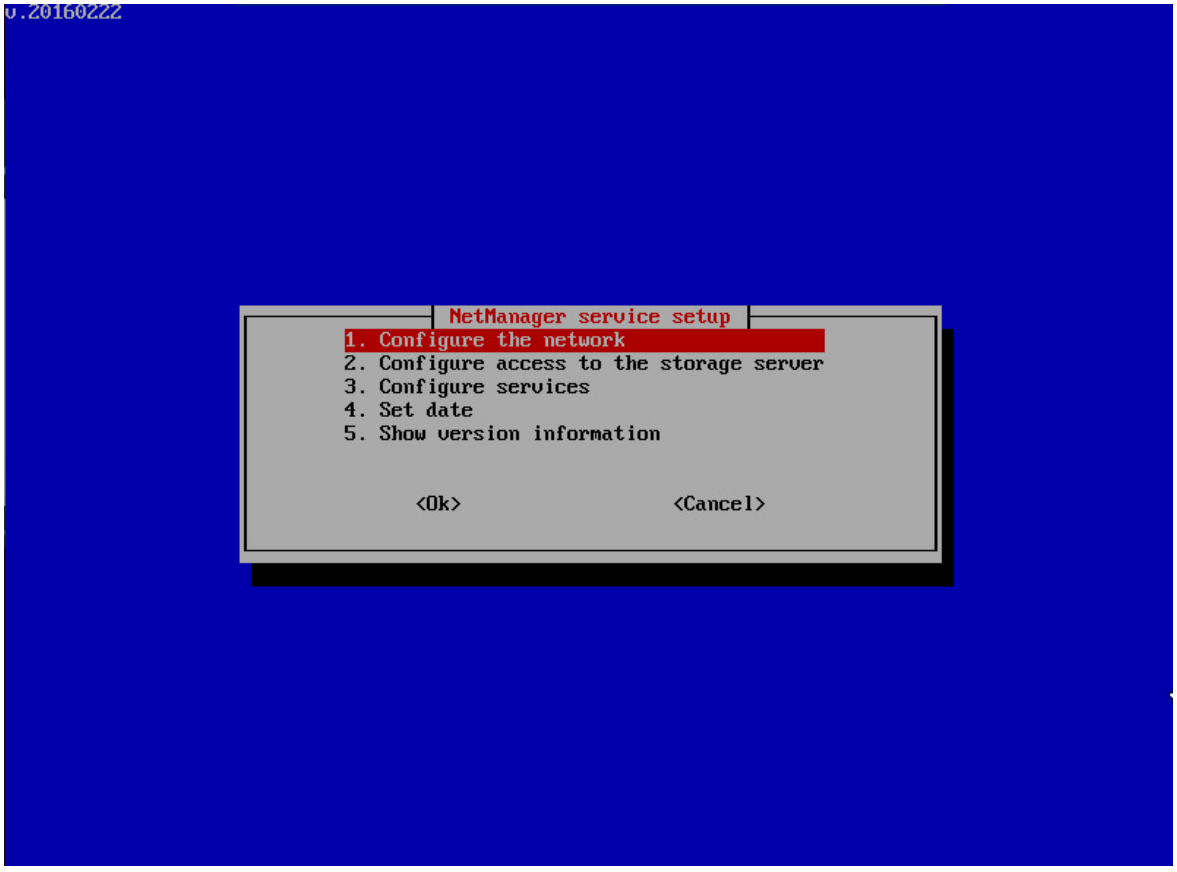


1.2.2 Service configuration

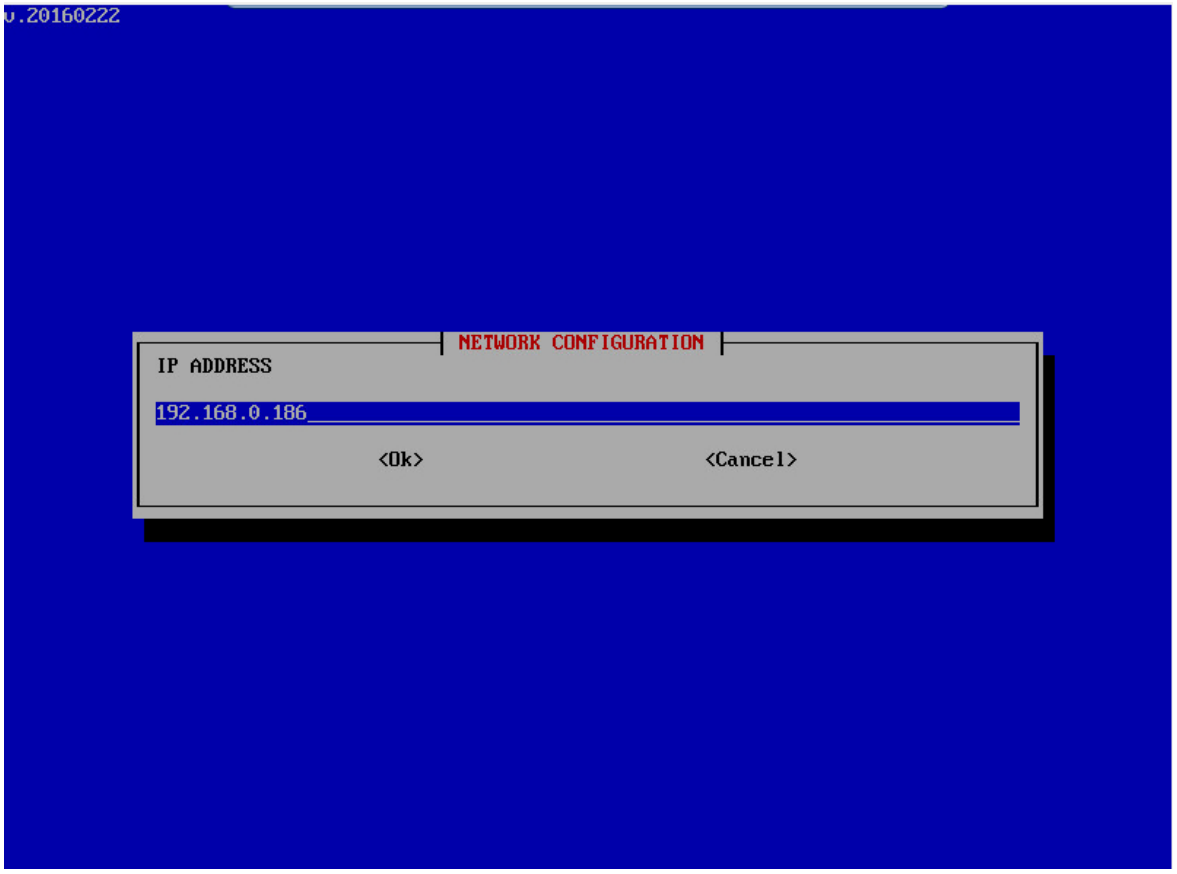
Once the server starts, the configuration menu appears automatically. Logging in is not necessary.

Network configuration

(1) The **network** is configured again in the first step. Select option 1 in the main menu, **Configure the network**.



(2) Enter the **IP address** through which the server shall be accessible. In this case, it is *192.168.0.186*.



(3) All additional values (IP address, netmask, Gateway IP address, and the DNS server address) can be transferred from the **storage server configuration**.

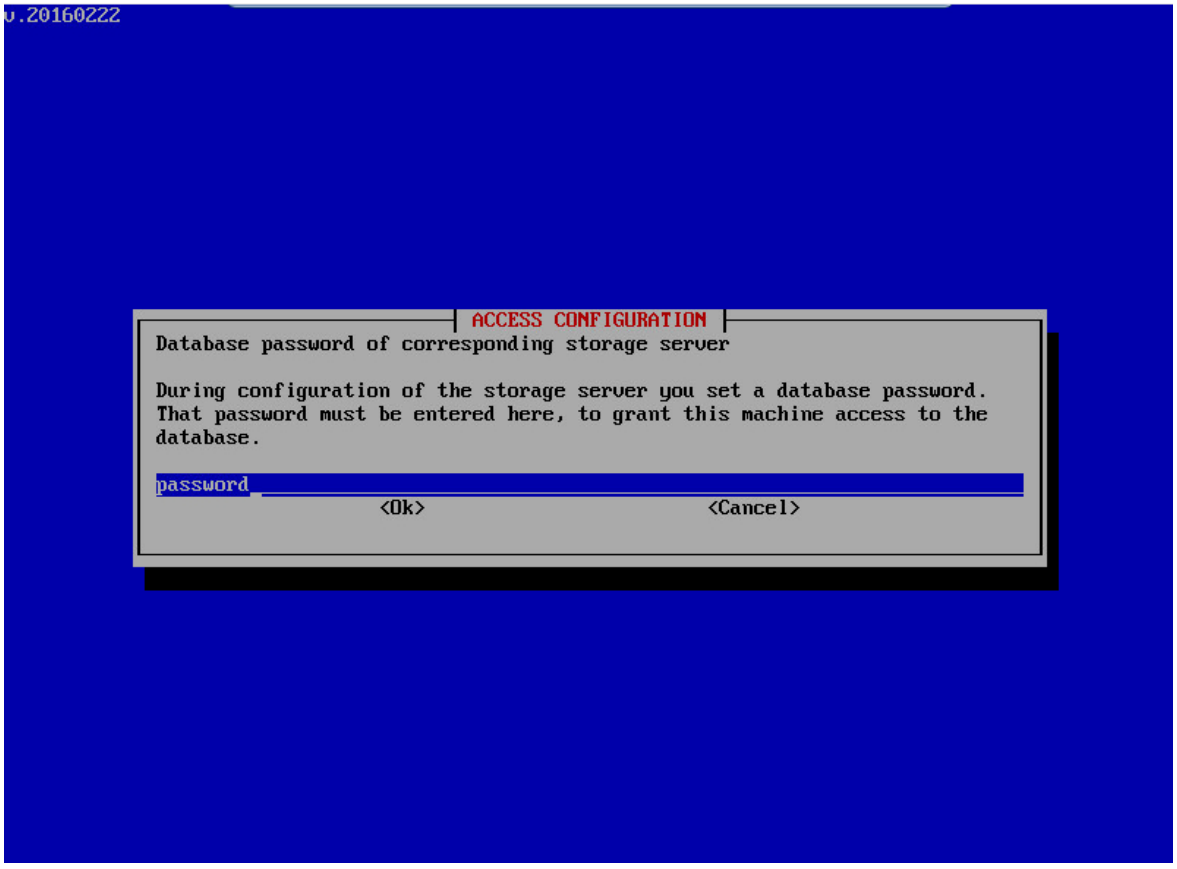
At this point, the **network configuration** is complete.

Access to the storage server

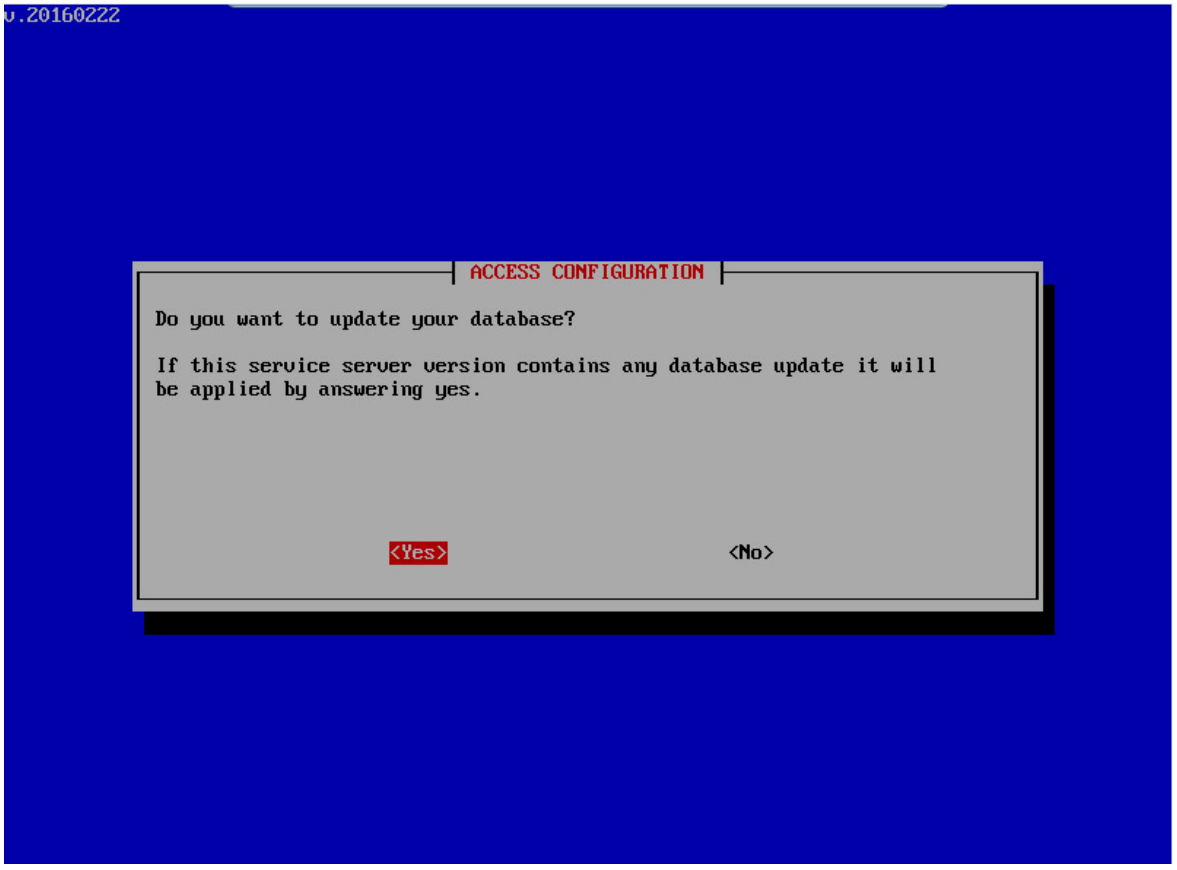
Access to the storage server must be configured next. To do so, select option 2 in the main menu: **Configure access to the storage server**.

(1) The first thing that needs to be done is to enter the IP address of the storage server. In this case, it is *192.168.0.185*.

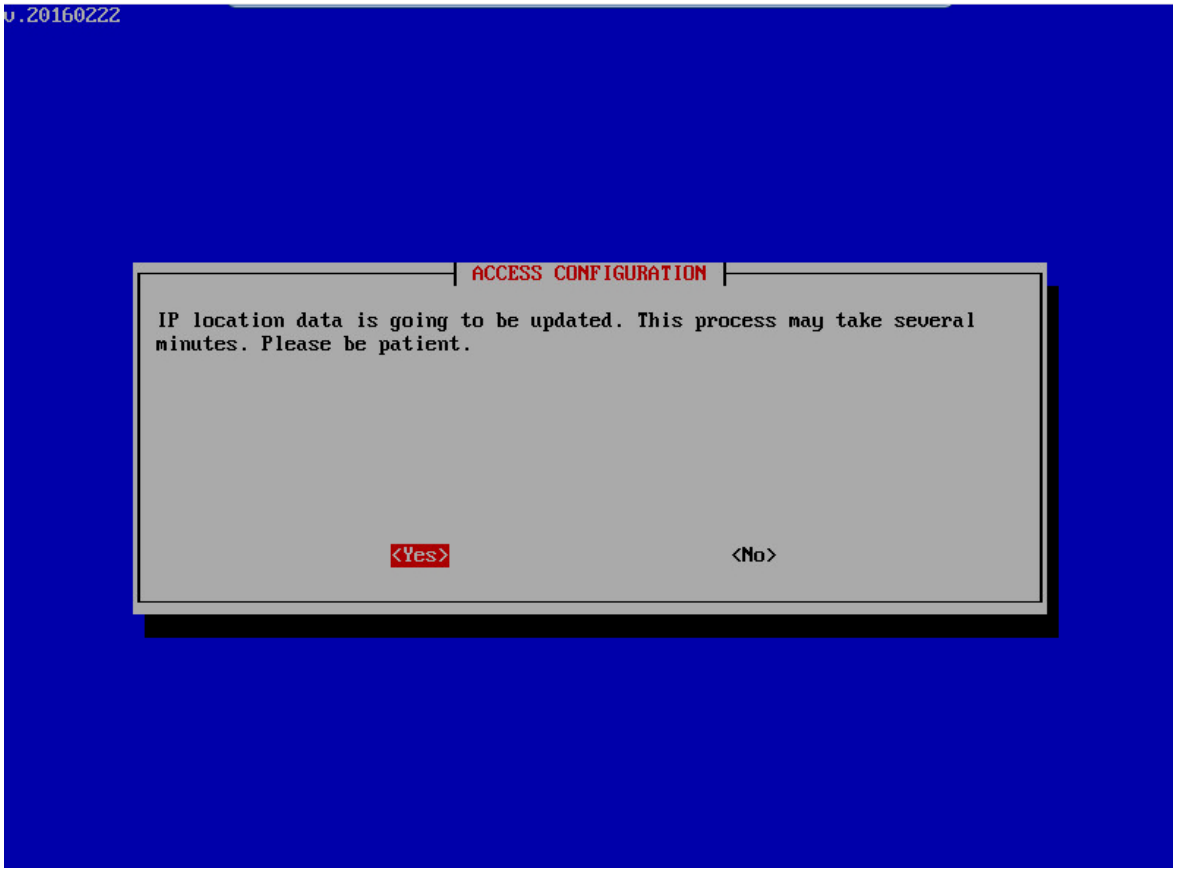
(2) The database password that was previously set in the storage server configuration is entered to communicate with the storage server. In our example, we have chosen *password* as the database password.



(3) Once here, you must update the database. Click on "Yes" in order to do so. The Service server connects with the Storage server and checks the database version to update it for Service (if necessary). If this process is a first installation, and not a Service server update, no updates are usually applied.



(4) Finally, you must update the geographic IP location information data in the database (when necessary). This operation may take several minutes.



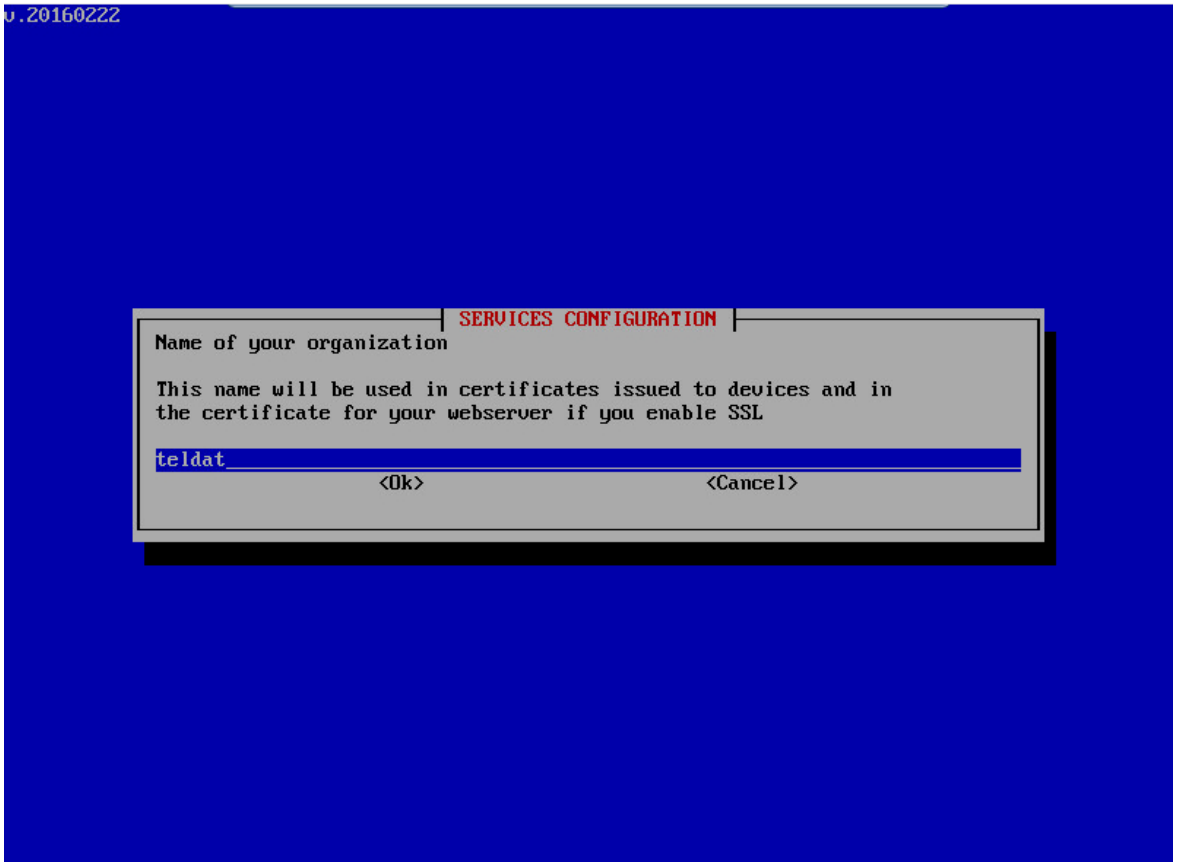
This message means that access to the storage server has been fully configured.

Colibri NetManager web server

The Colibri NetManager web server is configured next. Select option 3, **Configure services**, in the main menu

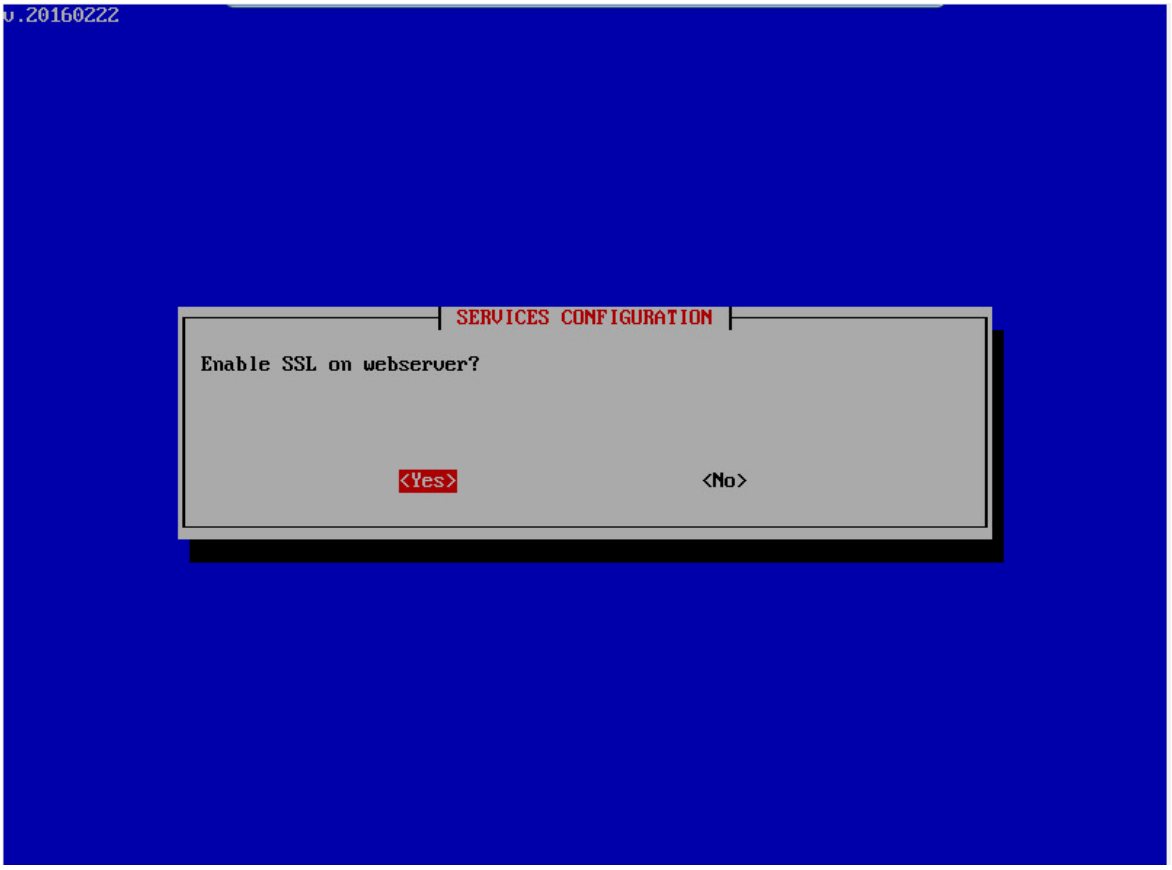
(1) Communication between the terminals to be managed and the server is encrypted and protected via certific-

ates. These certificates are created by the server itself. The only information you need to disclose is the name of your organization.



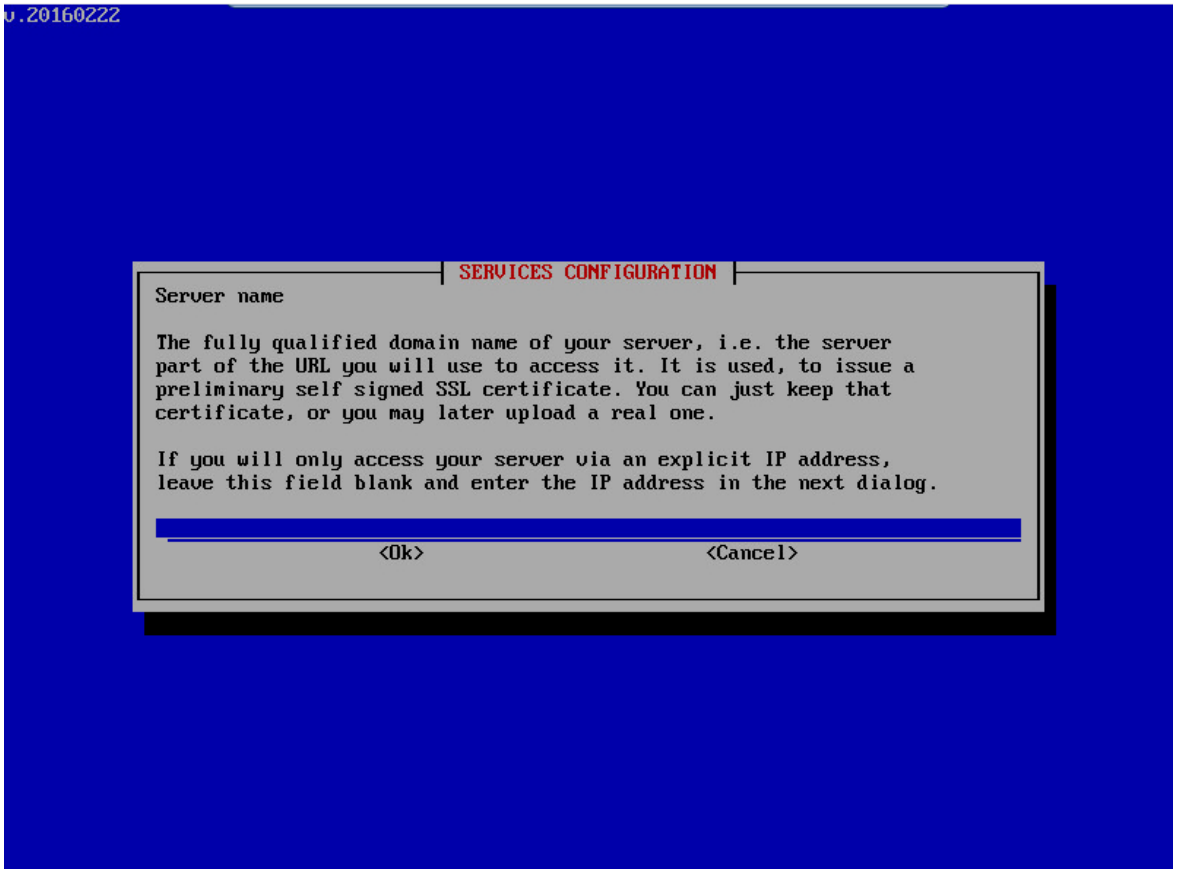
(2) Now, set the port the web server uses for HTTP calls. In this example, the port is *8080*.

(3) The configuration process then asks whether the web server should be reached via SSL. In this example, we settled for *Yes*.

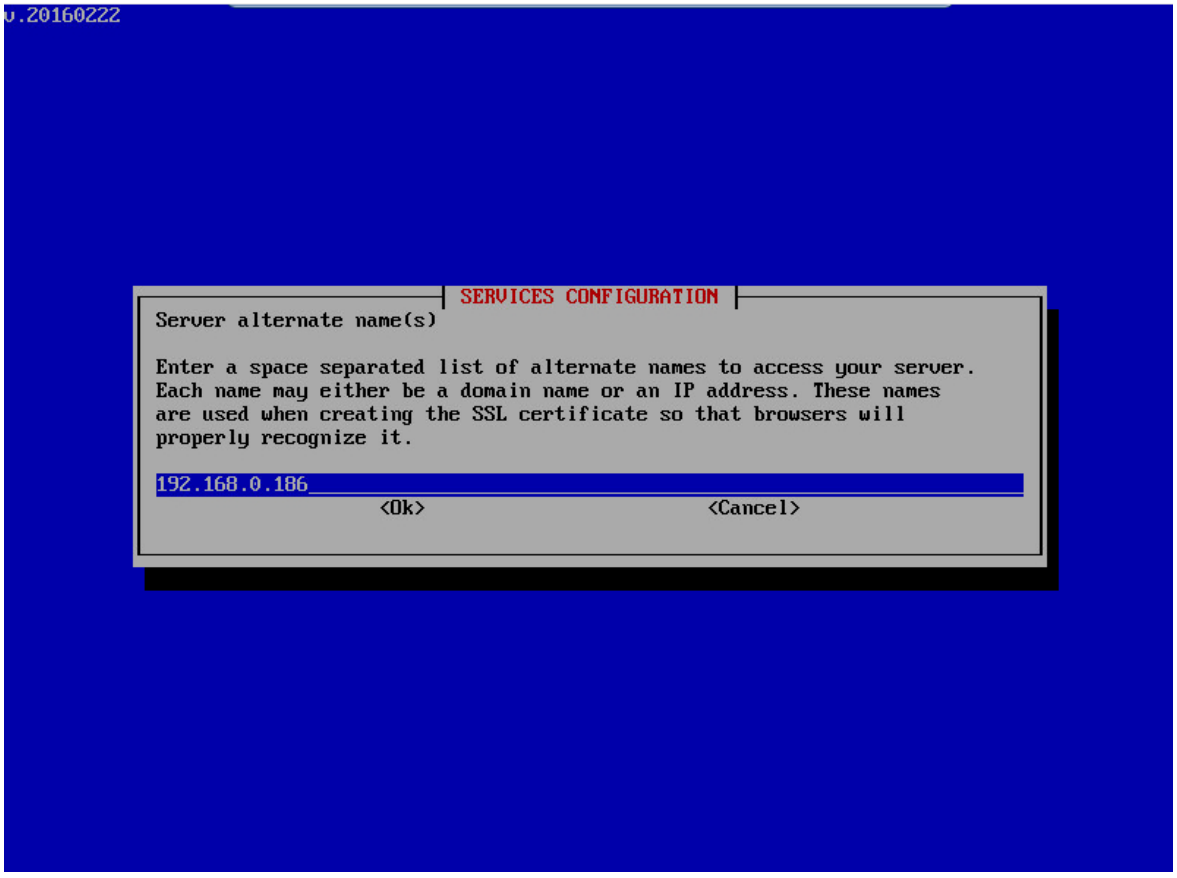


(4) The web server port defined is the one used for HTTPS communication. In our example, the port is *8443*.

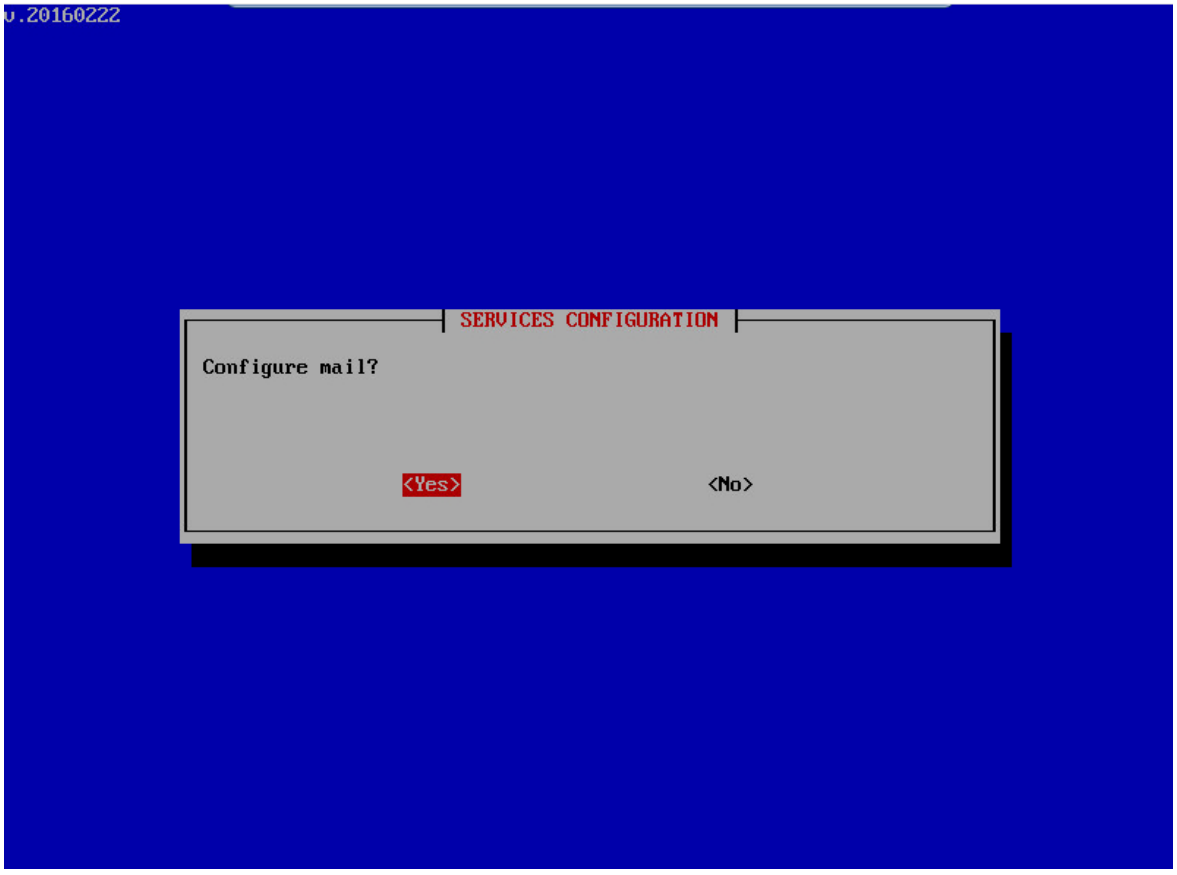
(5) If the server can be reached, later on, via a URL with HTTPS, then the full domain name of the server must be entered here (e.g. colibrinetmanager.teldat.com). If the server can only be reached through one IP address, then the field can remain empty.



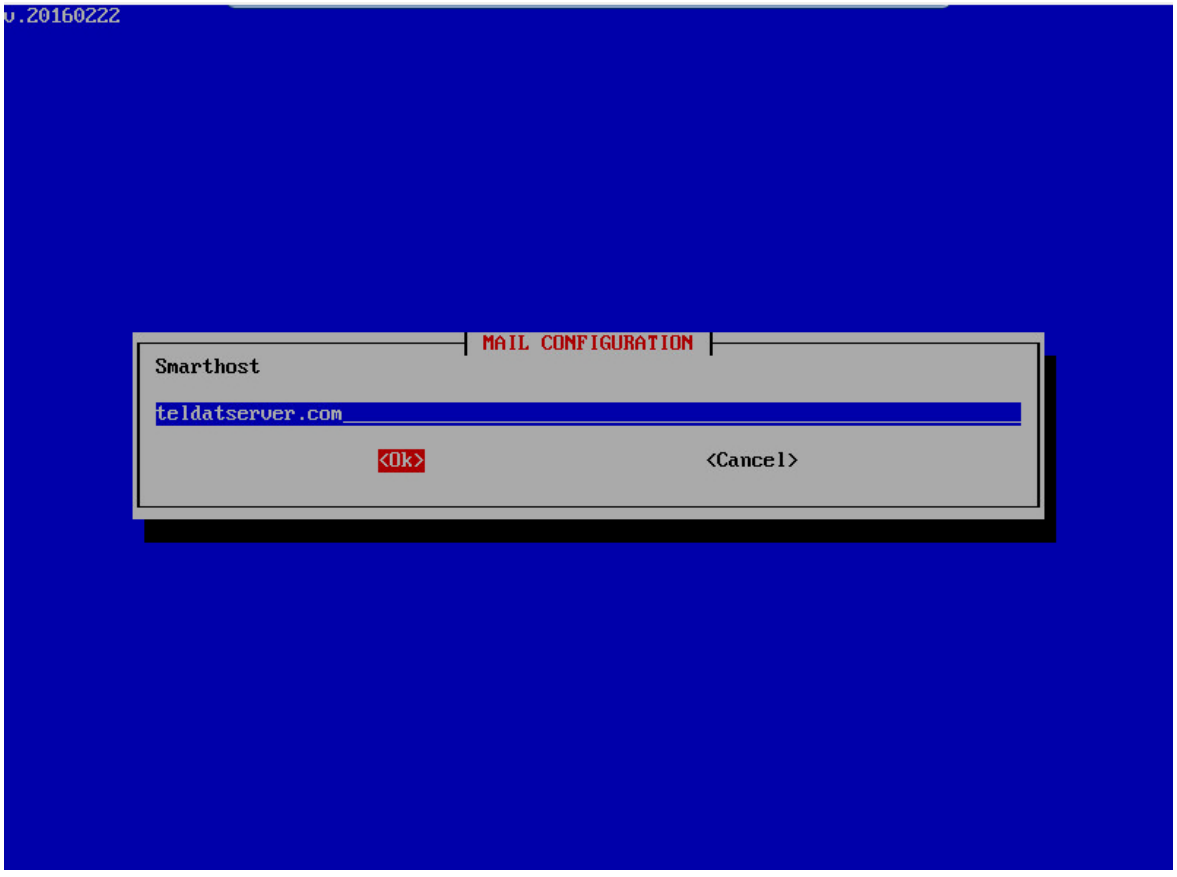
(6) This aspect is also important for HTTPS accessibility. Alternative domain names can be added here, in case the server has to be reached through other domain names via a HTTPS connection. If the server can only, or may also, be reached from an IP address via HTTPS, then the IP address must be entered here.



(7) A mail client is available, allowing the server to send emails (such as alerts). This will be configured next.

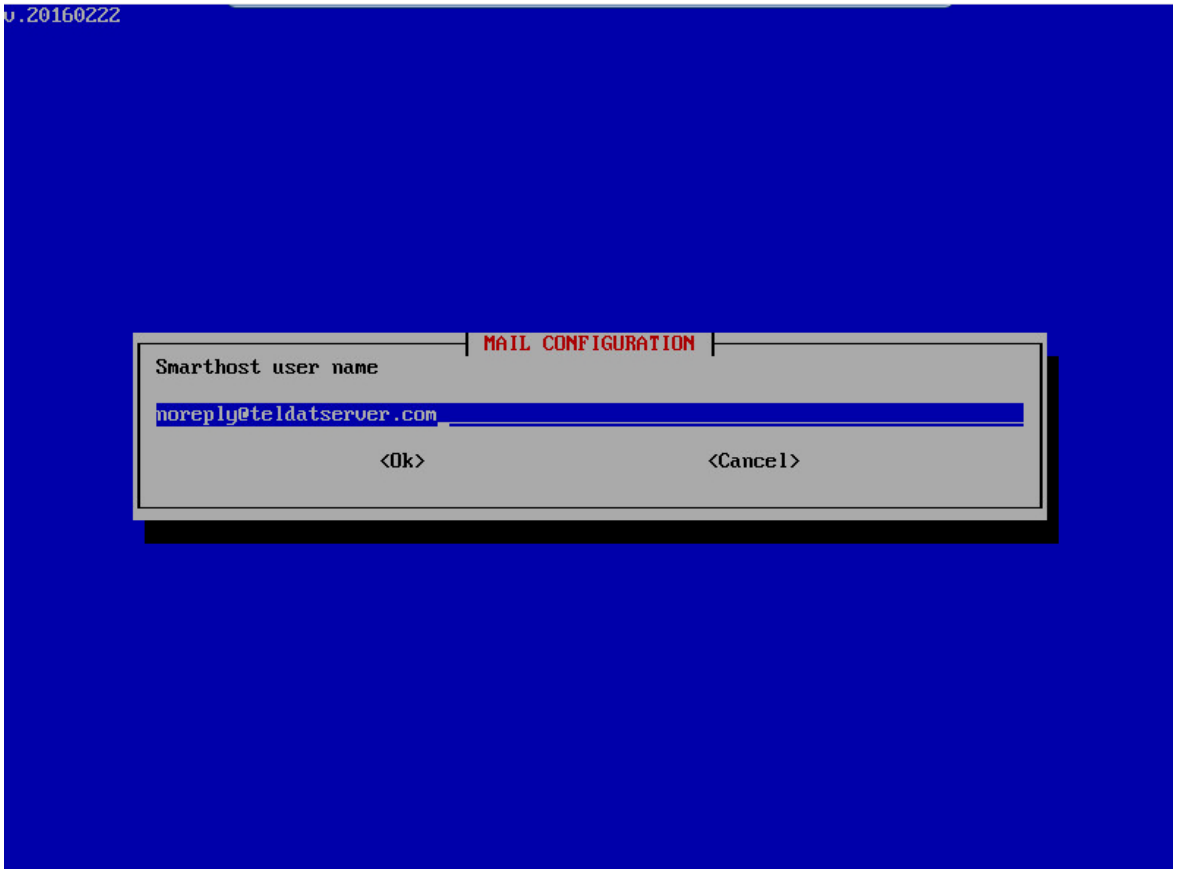


(8) The name of the mail server that should be used is entered here. In our example, this is *teldatserver.com*. Enter your own mail server. Operation with public mail servers is not provided for. Also, an encrypted connection to the mail server is not possible as we assume that the mail server is located in a private network.

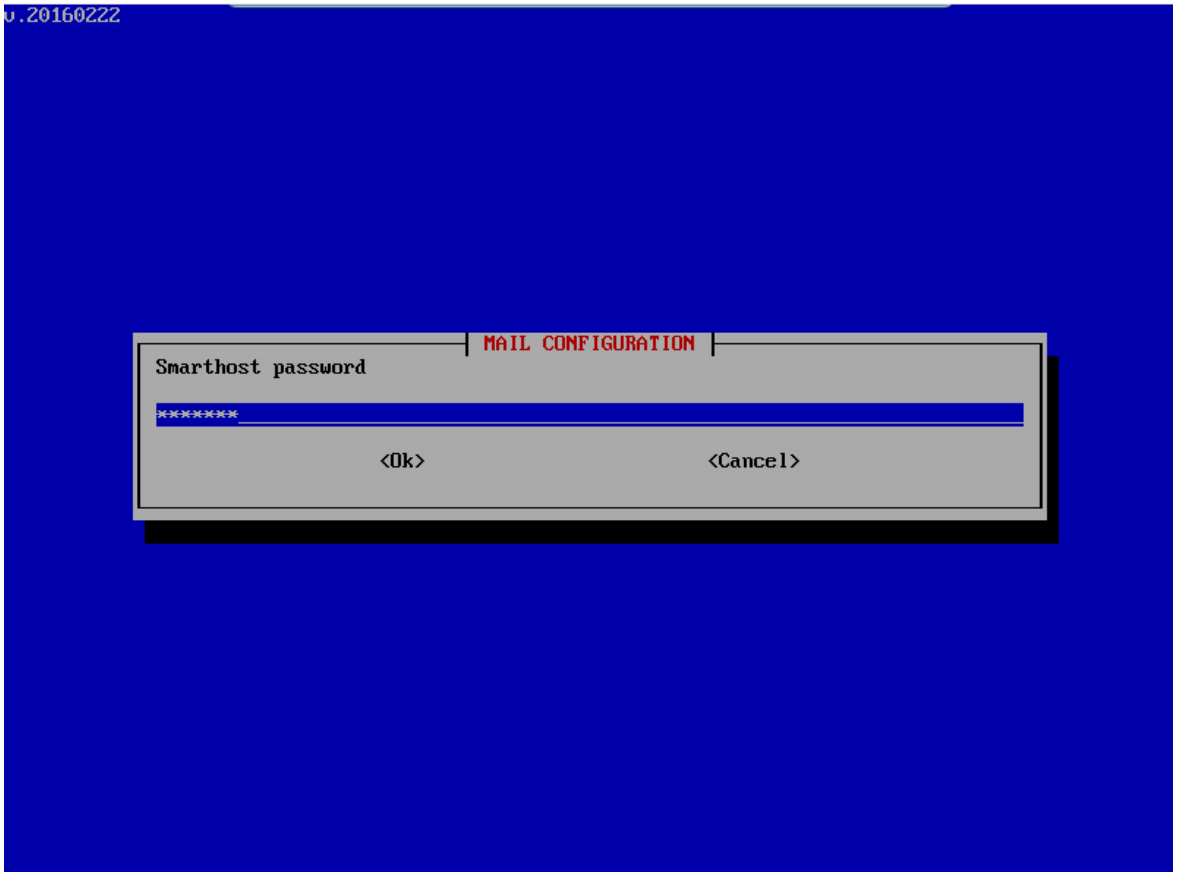


(9) The server's SMTP port is entered next.

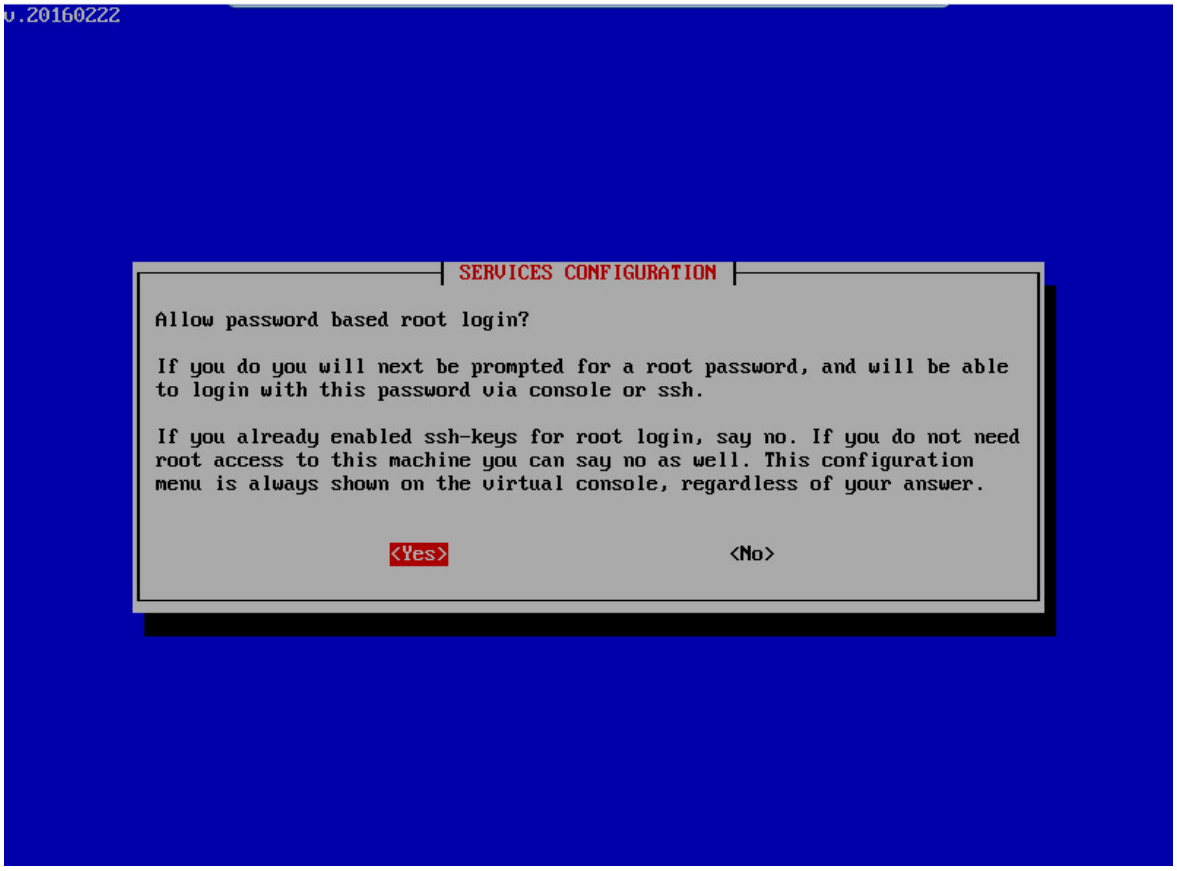
(10) The mail account username is entered here. In this example, it is *noreply@teldatserver.com*.



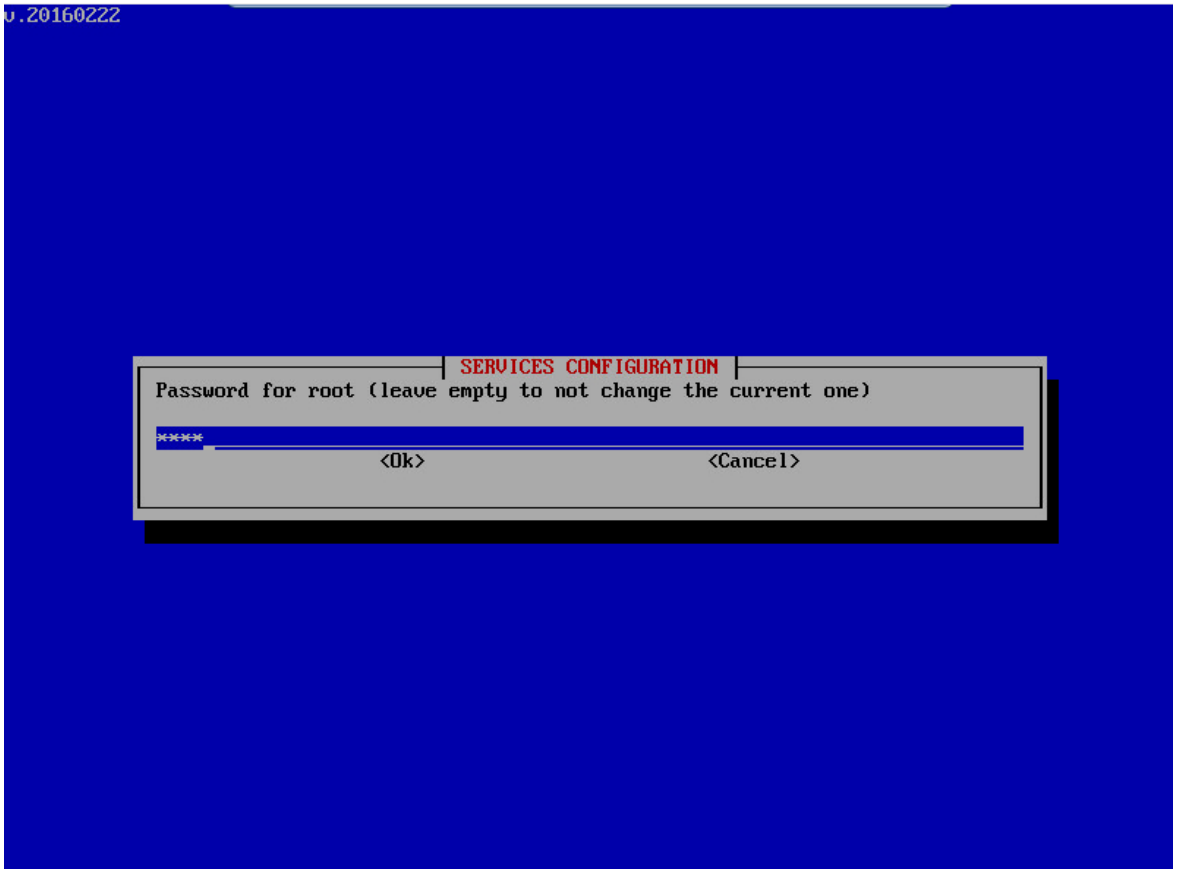
(11) Afterwards, the mail account password must be entered once again.



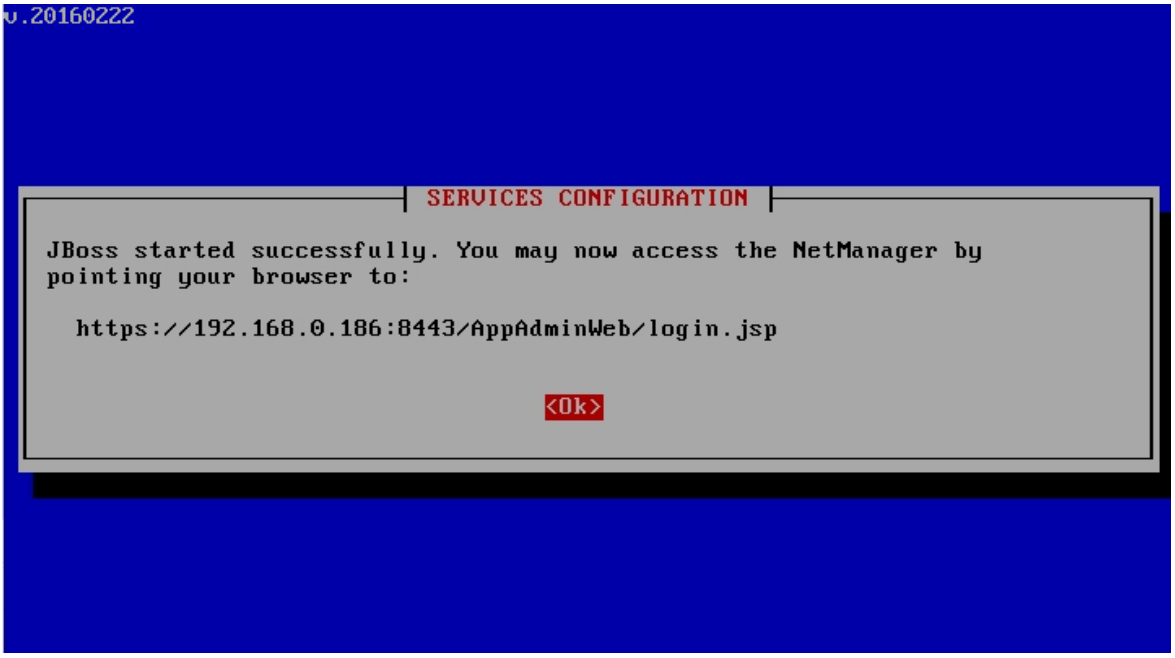
(12) To log in directly as *root* via Shell or SSH, a root password must be set.



(13) Setting a new root password.



(14) Start the web server (this can take one or two minutes). Afterwards, the following message appears:



This means that the **Colibri NetManager web server** is fully configured.

Set server date

The final step is to configure the date of the server. In the main menu, select **Set date**.

(1) To configure the date on the Service server, follow the steps set forth in the Storage server section.

1.2.3 Testing installation

When all steps have been successfully carried out, the server can be reached via a web browser.

You can now test whether both servers can be simultaneously reached via Ping by logging into the console (**ALT+F2**) and replacing the Linux command *ping 192.168.0.185* or *ping 192.168.0.186*.

Leave the virtual machines and call up the server in your local environment by means of an Internet browser. Note that it is necessary to prefix the command http:// or https:// with several browsers.

Call format:

http://192.168.0.186:8080 or *https://192.168.0.186:8443*

A certificate warning that requires confirmation when calling up a HTTPS page is displayed.

The server homepage is displayed. Default data for login is as follows:

User: `admin`

Password: `1234`

Note

It is absolutely necessary to change the default password.

1.3 Licensing

To use the Virtual Colibri NetManager, you must obtain a **Virtual Colibri NetManager license**. You may get one from your distributor. In addition, and depending on the number of devices to be managed, obtaining a device license may also be necessary. The device license has to match a certain client account and cannot be transferred to others.

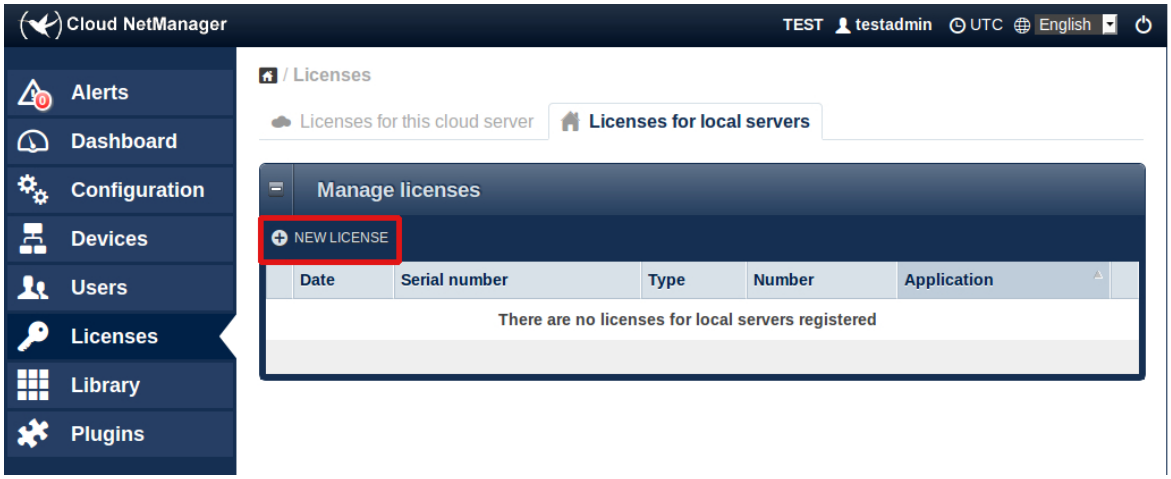
1.3.1 Installation of the server license

Together with the software for virtual machine installation, you will receive a license document containing a serial number and a PIN code.

(1) A license file must be generated first. To do this, you need a Cloud NetManager registered account.

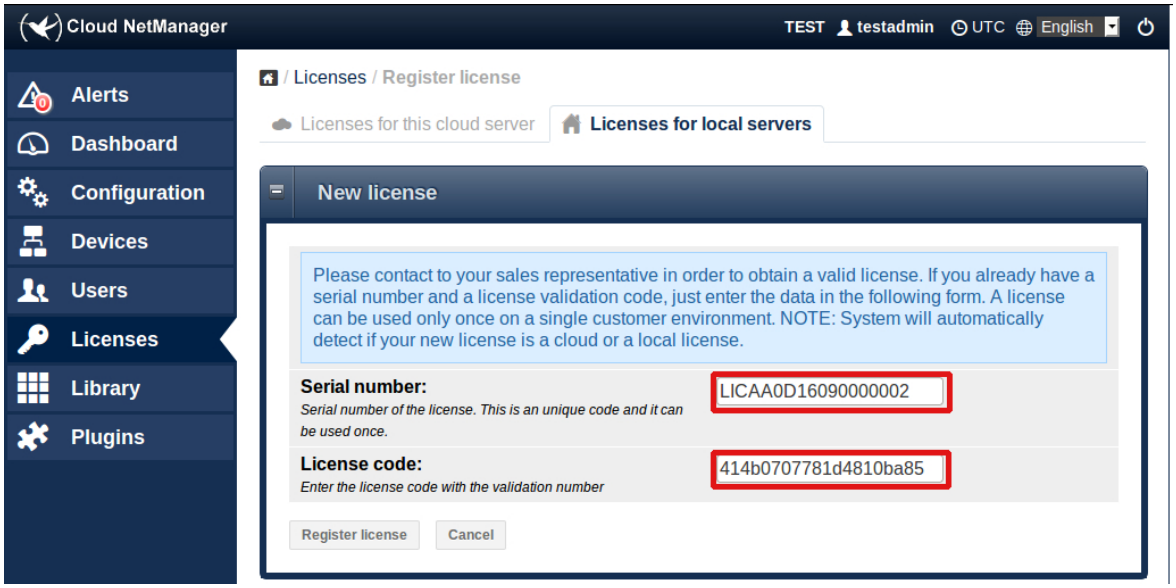
(2) Log into *https://teldat.networkcloudmanager.com* .

(3) Go to the status page under **Licenses** -> **Licenses for local servers** -> **New license**.

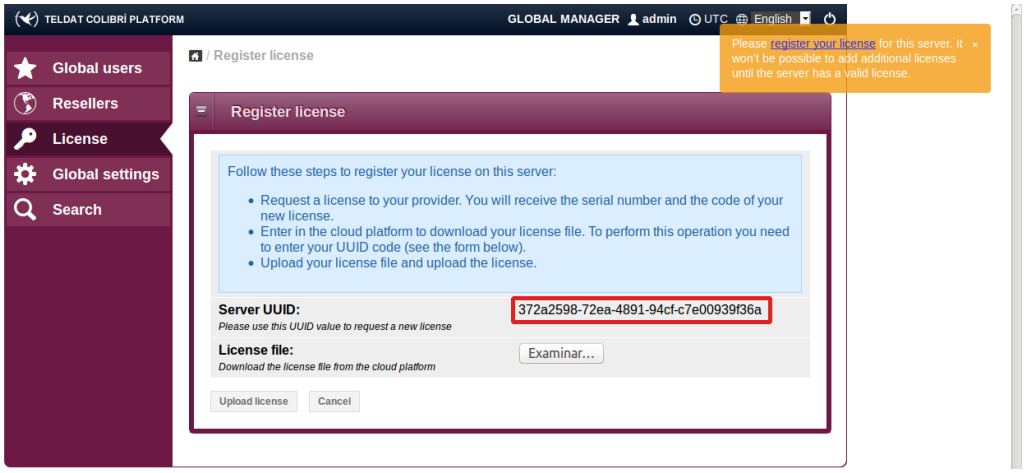


(4) Enter the serial number and the license key (PIN).

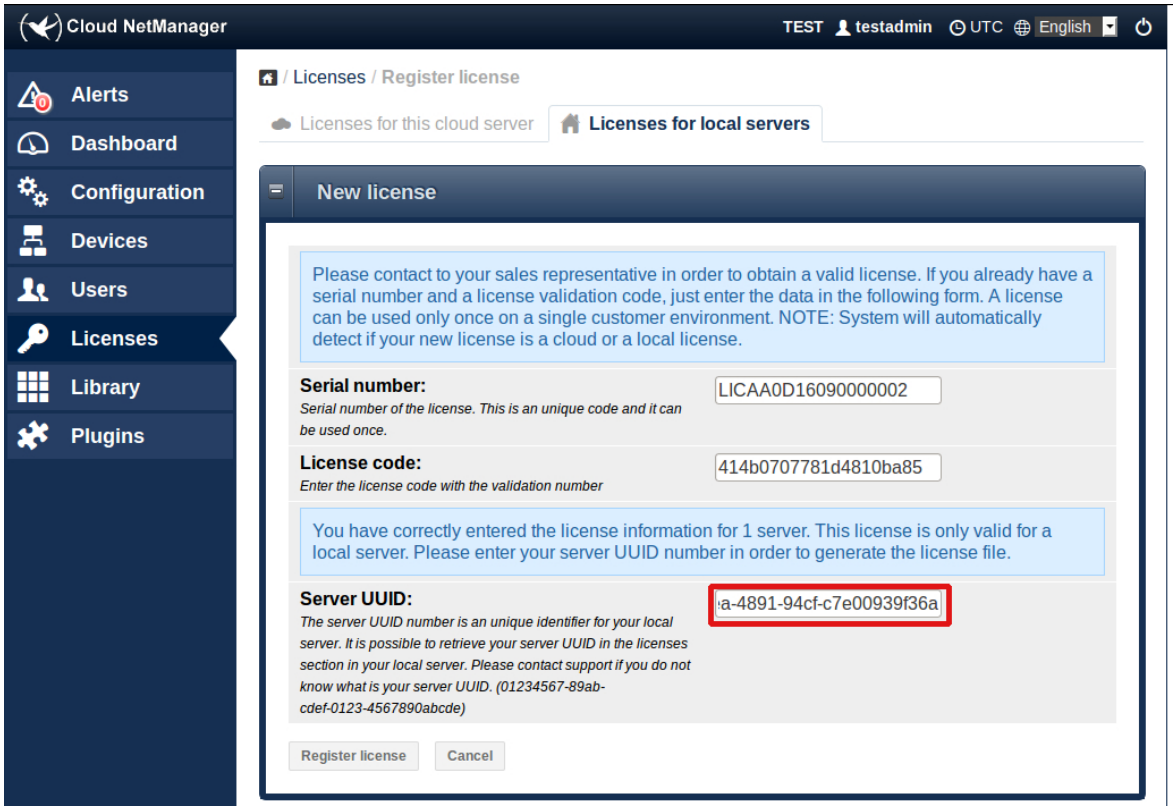
(5) Click on **Register license**.



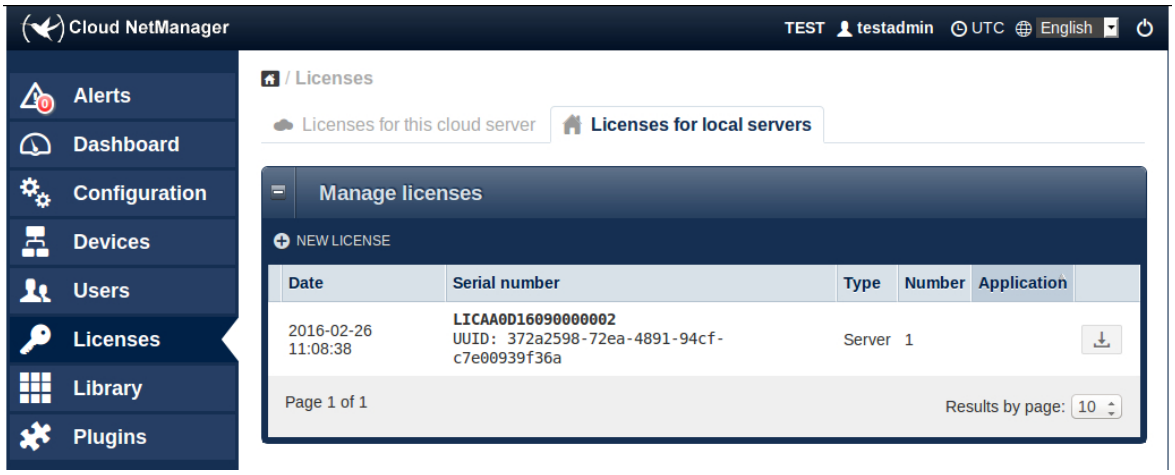
(6) If the license data is correct, the window will expand and ask for the local server's UUID. To obtain the UUID, log into a second browser window on your local server and call up the license menu.



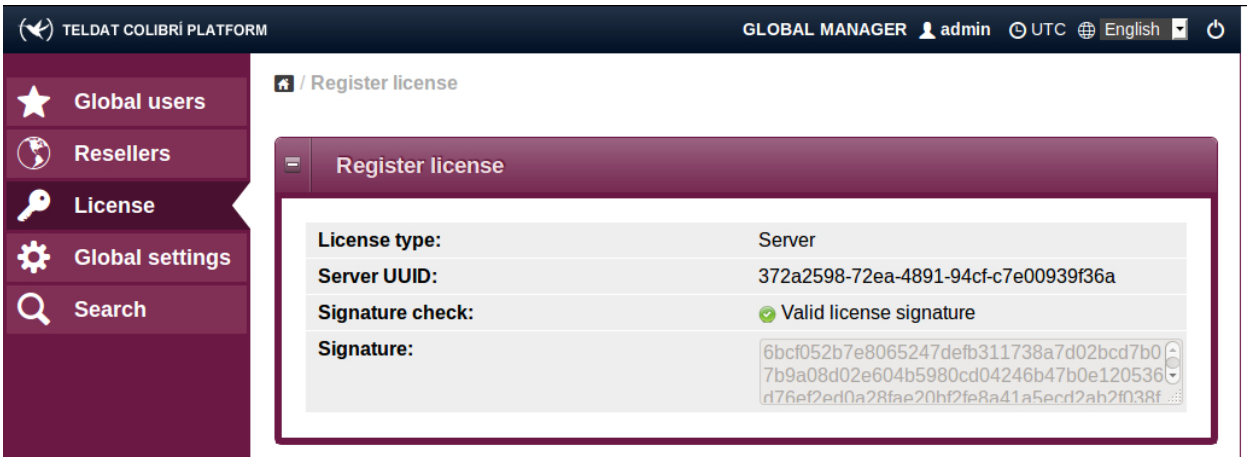
(7) Now copy the **Server UUID** into the open window of your Colibri NetManager account (teldat.networkcloudmanager.com).



(8) The server now generates an XML license file that should be saved. You can now log out of the Teldat Colibri Manager.



(9) It is now possible to upload the XML license file from the license menu of your local server and complete licensing from there.



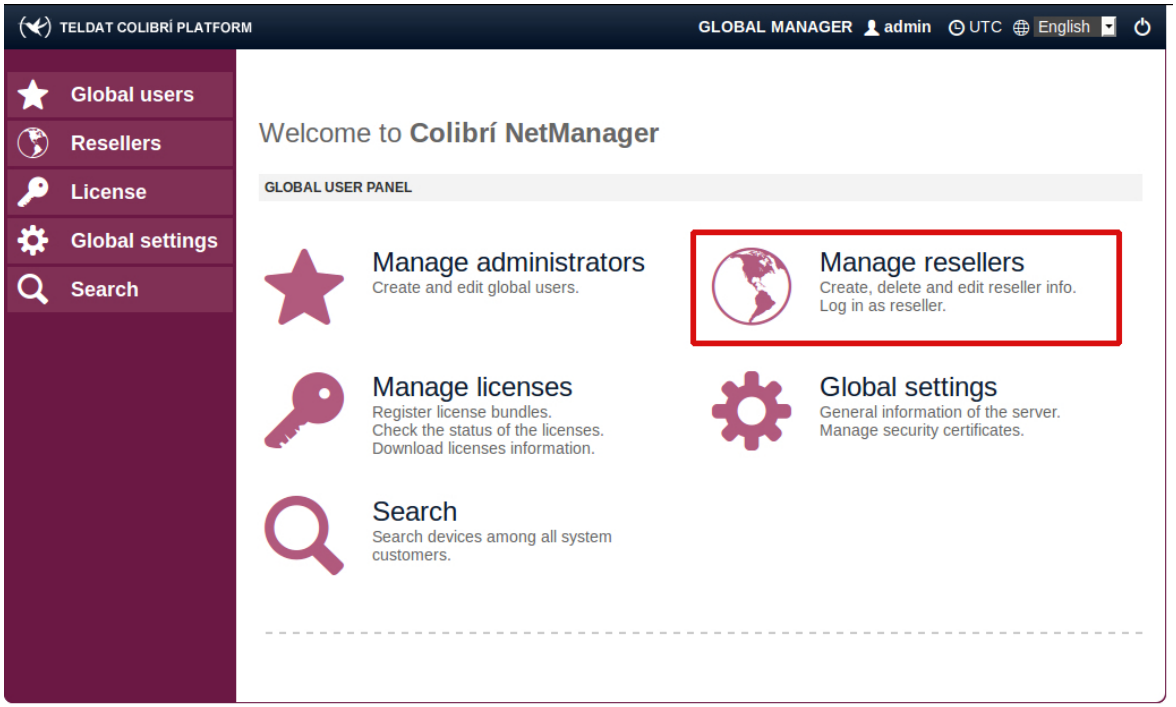
1.3.2 Installing device licenses

To manage devices, device licenses must be installed via a user account. Please take into account that the virtual machine requires device licenses.

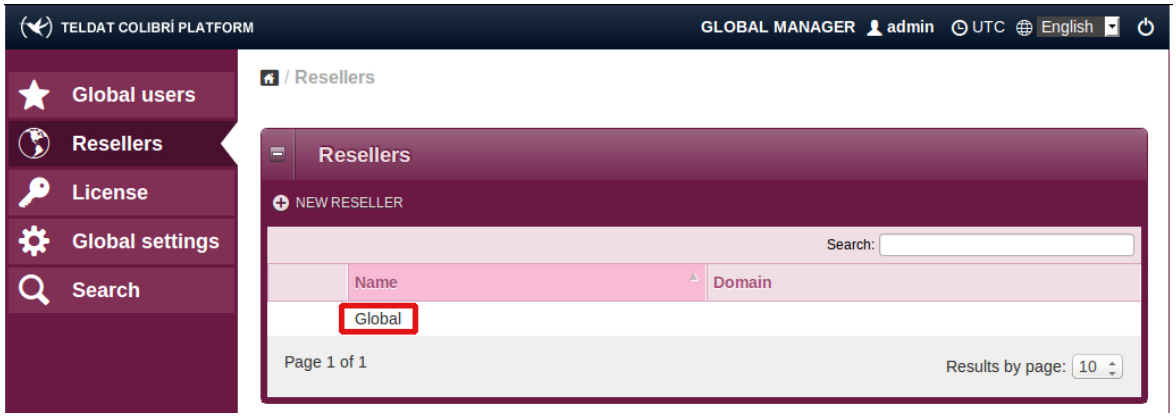
Set up a new client account

(1) To do so, first log in as an **admin** again.

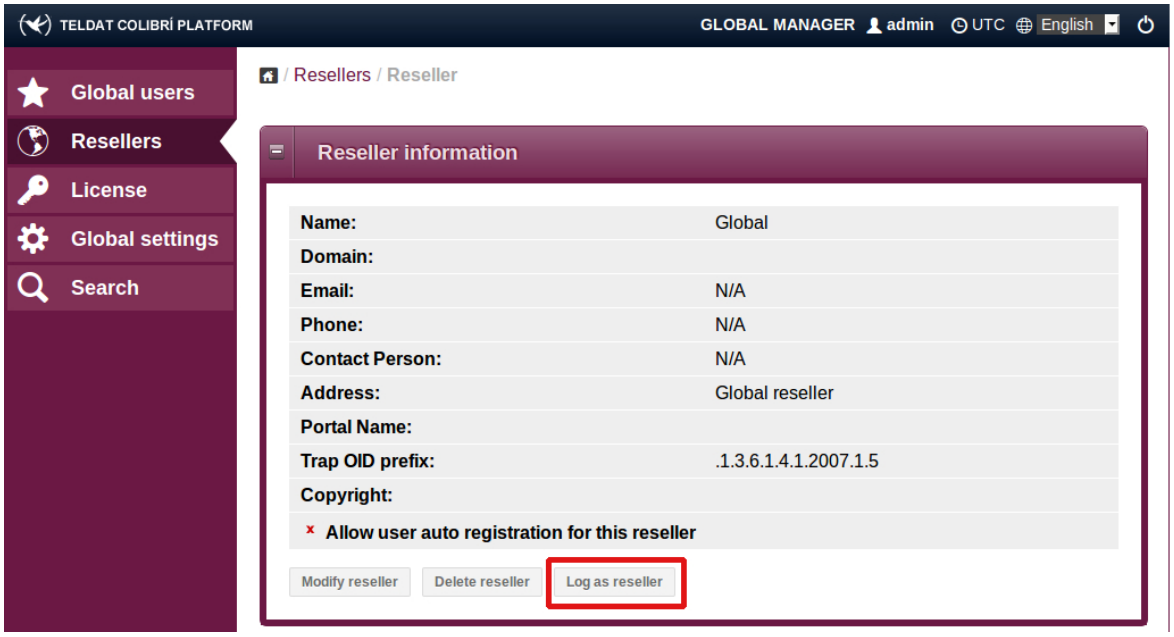
(2) Go onto the status page and access the **Manage resellers** menu.



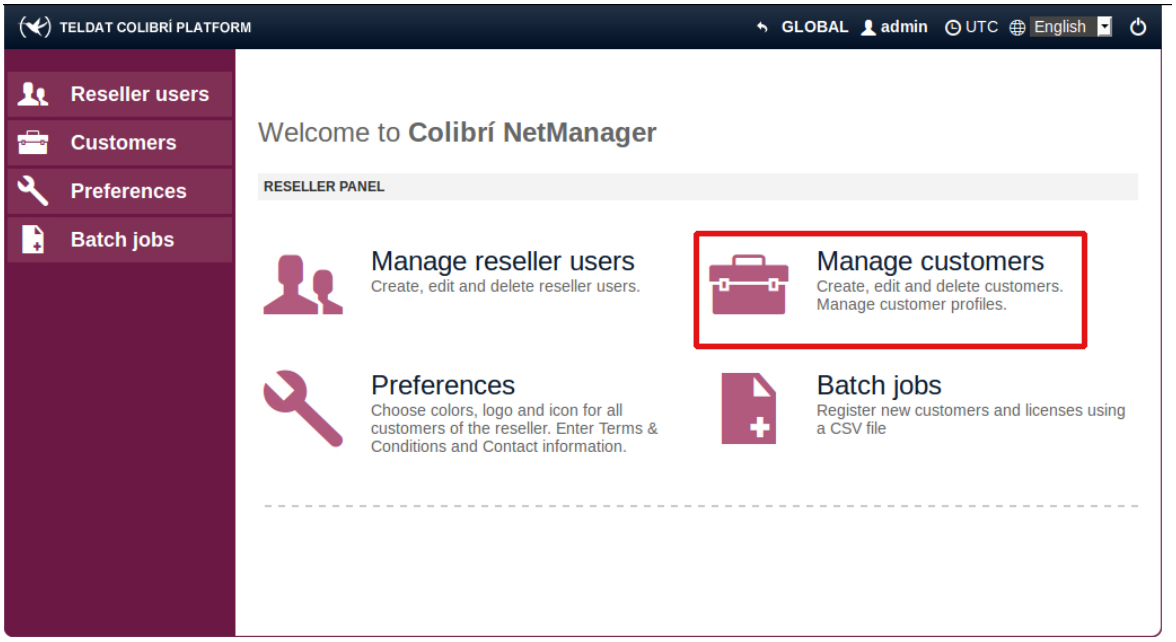
(3) Click on **Reseller** -> **Global**.



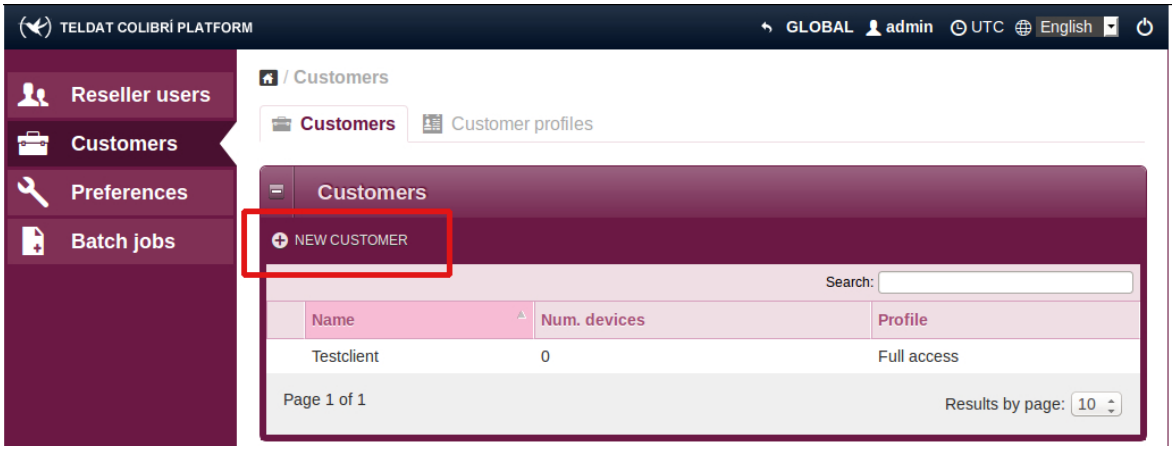
(4) When on the **Reseller information** page, click on **Log in as reseller**.



(5) Go back to the status page and call up the **Manage customers** menu.



(6) Go to **Customers** -> **New customer** menu.



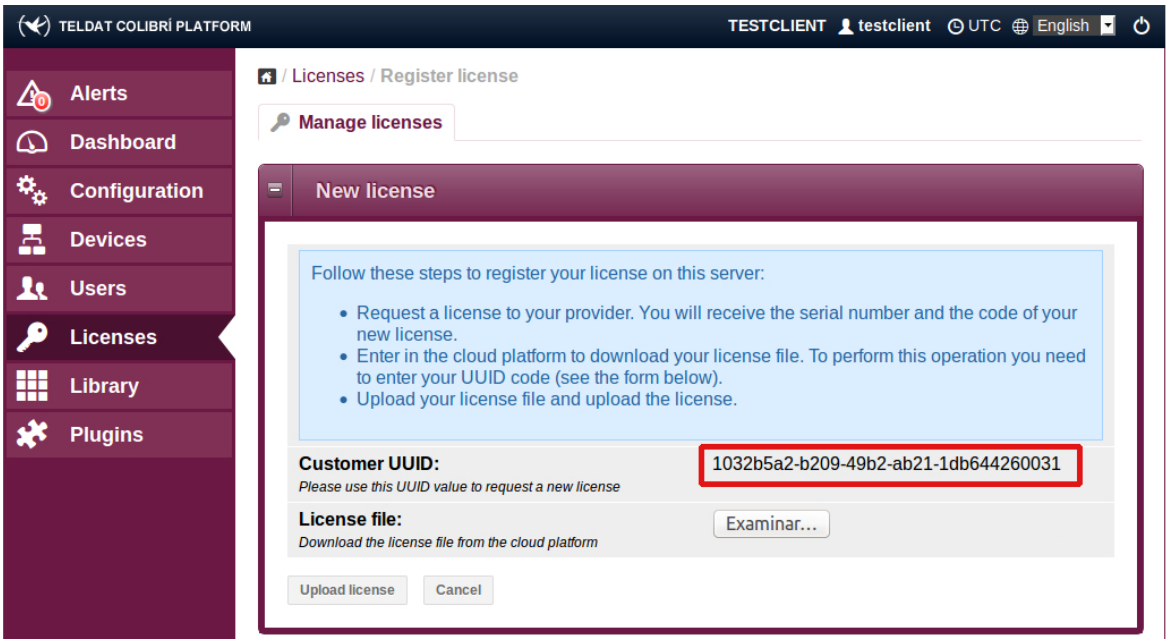
The new **client account** is now set up.

Installing a device license to the client account.

(1) The first step is to log into the newly created client account.

(2) Go to **Licenses** -> **Manage licenses**.

(3) Copy the **customer UUID** onto the clipboard.



(4) Log into your Cloud NetManager account (*https://teldat.networkcloudmanager.com*).

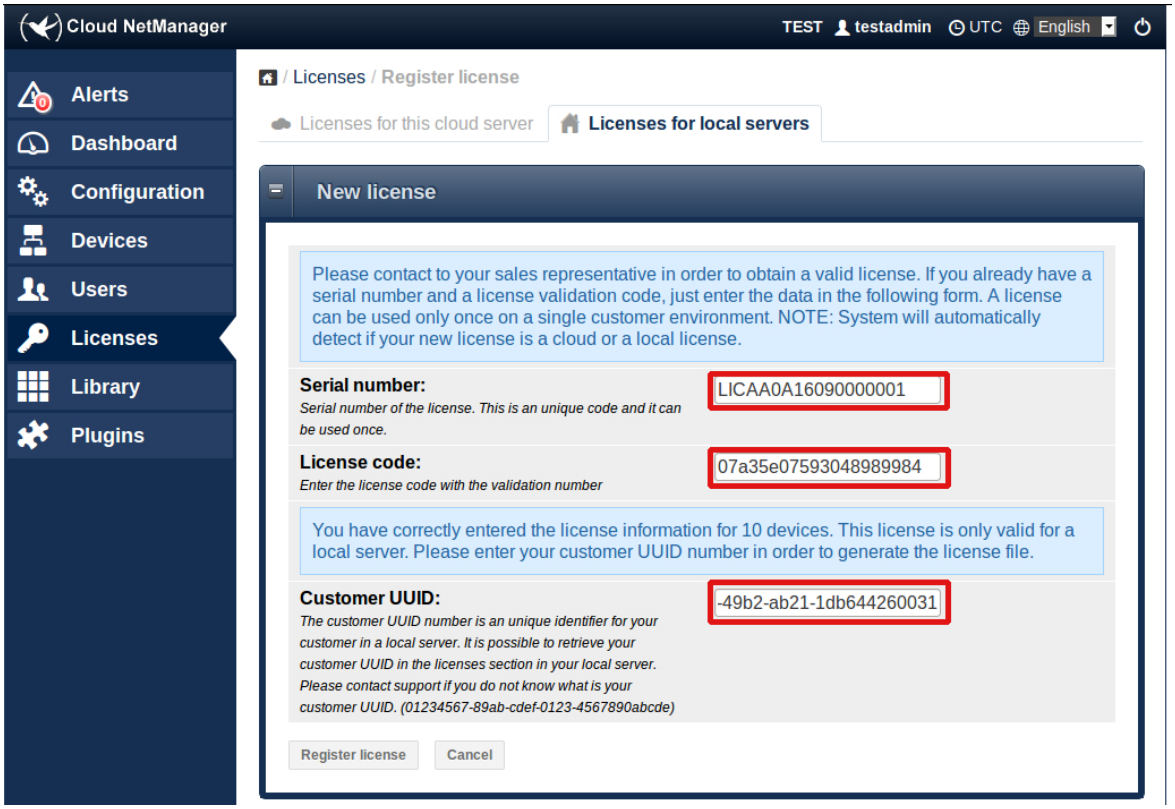
(5) Go to **Licenses** -> **Licenses for local servers** -> **New license**.

(6) Enter the license's **serial number** and **license code**.

(7) Under **Customer UUID**, enter the **UUID** from the clipboard.

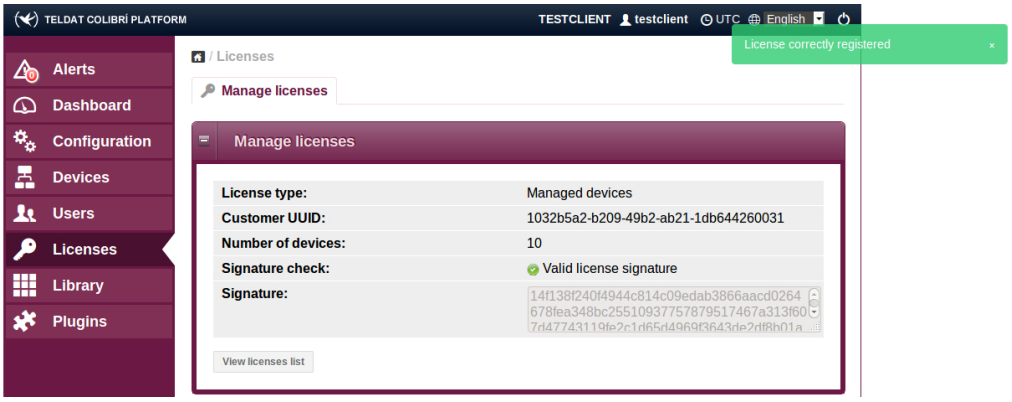
(8) Press **Register license** to create the license file.

(9) Save your data.



(10) Go back to the client account on your local server.

(11) Load the license file via the menu **Licenses** -> **Manage licenses** -> **Load license**.



Installing a device license on the reseller account.

Licenses can be installed not only on customer but also on reseller accounts. A reseller can allocate installed licenses to its customers. Resellers will be able to recover unused licenses allocated to customers (i.e., reclaim licenses when no customer devices are using them), as well as those assigned to customers that have been deleted. The following considerations should be taken into account:

- The reseller can give any of its available licenses to a customer (see the license allocation procedure below). A license cannot be divided and cannot be shared by several customers. Each customer receives a full license from the reseller.
- Reseller licenses can be reassigned to another customer only if the current license owner has been removed from the server, or if the customer has not yet used the license. In the second case, the reseller must recover the license (see the license recovering procedure below) from the customer and assign it again to another customer.

- Licenses registered by customers cannot be recovered or reassigned by the reseller in any case. If a customer is removed from the server, any licenses the customer registered are lost. However, the reseller can recover any of its allocated licenses and reassign them.

(1) The first step is to log into the reseller account.

(2) Licenses are installed on the reseller account just like on customer accounts (see above), but using the **reseller UUID** instead of the **customer UUID**. You may find the reseller UUID under **Licenses** -> **Available**-> **New license**

Assign reseller licenses to a customer

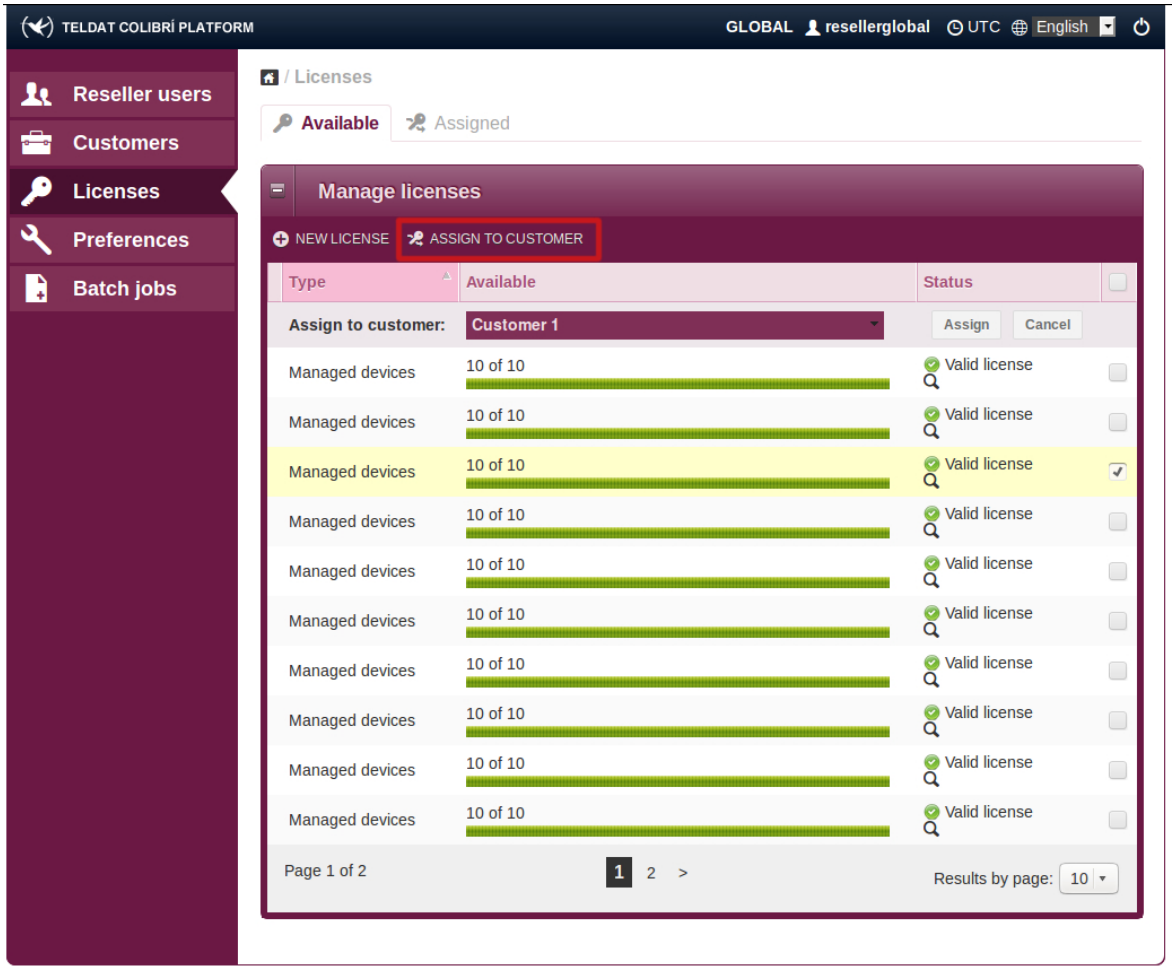
(1) The first step is to log into the reseller account.

(2) Go to **Licenses** -> **Available**. This screen shows you a table with the reseller licenses available. Available licenses can be assigned to a client and be used by his/her devices.

(3) Select one or more licenses using the checkboxes. A new button, **Assign to customer** appears.

(4) Click on **Assign to customer**. A new row appears in the table, inviting you to select the target customer.

(5) Select the customer that will receive the licenses from the list.



(6) Click on **Assign** to allocate. Afterwards, the assigned licenses disappear from the screen that shows all licenses available and appear on the assigned licenses screen.

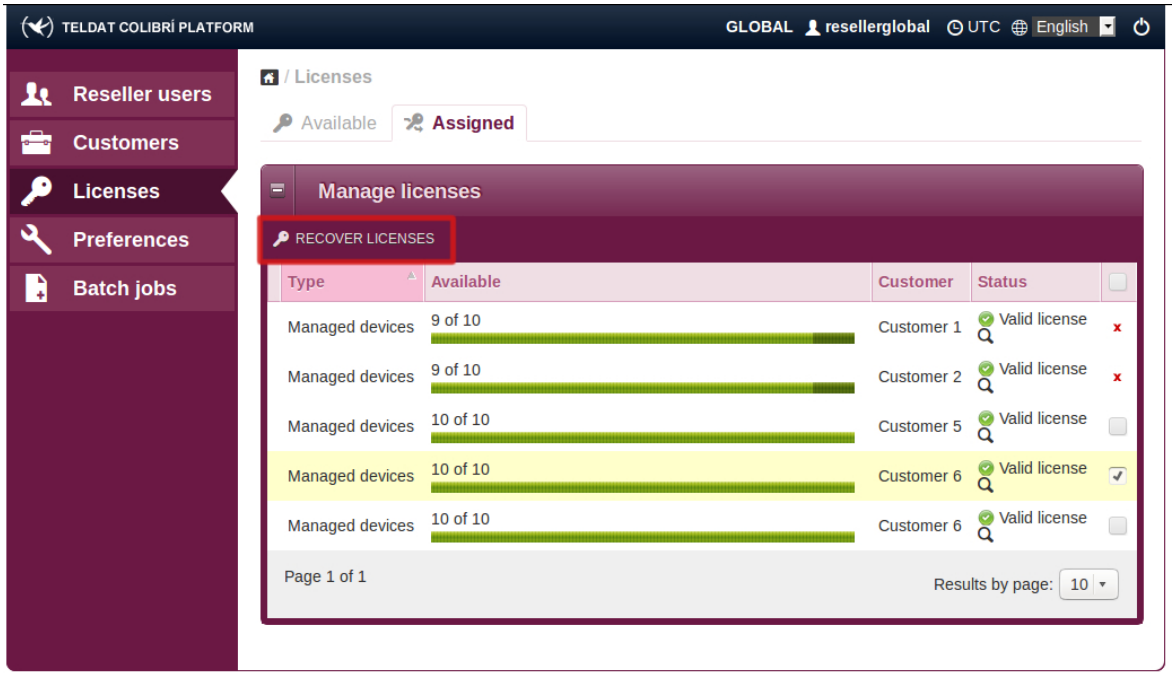
Recover reseller licenses from a customer

(1) The first step is to log into the reseller account.

(2) Go to **Licenses** -> **Assigned**. This screen shows you a table with the licenses assigned to customers.

(3) Select one or more licenses using the checkboxes. A new button, **Recover licenses** appears. You can only recover licenses that have not been used. Checkboxes are disabled for licenses in use, meaning they cannot be selected.

(4) Click on the **Recover licenses** button. Licenses are recovered from customers and may be reassigned, appearing under the reseller available licenses screen.



1.4 Managing devices

Devices can be used and managed in the same manner as with the Cloud NetManager (*https://teldat.networkcloudmanager.com*). Step-by-step instructions on how to use the Cloud NetManager can be found in the separate guide for each application. These can be downloaded from the *www.teldat.com* website.

1.4.1 Adjusting the management URL in the device

You must enter your server's address if you want your device to operate with your own virtual Colibri NetManager.

You have two options:

- Via the local GUI on the device.
- Using option 43 of your local DHCP server

1.5 Notes regarding free software

Part of the Virtual Colibri NetManager is made up of free software that is available under various open source licenses (Apache 2.0, GPL 2.0 or 3.0, LGPL, BSD, etc.). You can find more information on the software used, as well as the relevant copyright notes and licenses, under the "copyrights" directory in the data storage media. The full text (including all licenses) can be found under the "copyrights/common-licenses" directory. The sources to GPL-licensed programs are in the "repo" directory, which is structured like a Debian repository, and in the src directory.

In addition, the End User License Agreement (EULA) you received together with the Virtual Colibri NetManager also applies to this product.