

GeNUCenter 2.2 Release Notes

Information on the GeNUCenter 2.2 product family is available in these release notes. Please read this document carefully! You are advised to install this upgrade, as this release both resolves various problems, and provides new features.

Important, please read!

We strongly recommend performing a configuration backup of your GeNUCenter system BEFORE upgrading.

Detailed instructions on how to perform this upgrade are available in section 5 of these release notes.

Contents

1	Scope of Delivery	2
2	Before Upgrading	2
3	New Features in GeNUCenter 2.2	2
3.1	GUI	2
3.2	Rollout Support	2
3.3	Improved Logging	2
4	New Features in GeNUGate, GeNUScreen, GeNUCrypt, GeNUCard and GeNUBox	3
4.1	GeNUGate Administration	3
4.2	GeNUCard	3
4.3	GeNUScreen and GeNUCard	3
4.4	GeNUBox	3
4.5	GeNUScreen, GeNUCrypt and GeNUBox	4
4.6	GeNUCard, GeNUScreen, GeNUCrypt and GeNUBox	4
5	Upgrade Installation	5
6	How to Contact Us	5

1 Scope of Delivery

With the current GeNUCenter version 2.2 you have received:

- these release notes
- An ISO image of the installation CD-ROM.
The image is also available for download on the GeNUA webserver in the GeNUCenter customer area:
https://www.genua.de/k/customer/gz_support/release_download.en.html

2 Before Upgrading

- If an IPsec VPN has a phase 2 SHA2 setting greater than 256, then VPN connections only are possible between GeNUA appliances running under the same software version. Thus, a VPN connection between GeNUScreen version 2.1 and GeNUScreen version 2.2 will fail.
- GeNUCenter administrates the user master.passwd via the database. Local additions of users therefore will not be available after the GeNUCenter upgrade.

3 New Features in GeNUCenter 2.2

3.1 GUI

- The installed software version of each system now is visible in domain listings.
- It now is possible to go back and forth between pages of numerous appliances in domain listings.
- A dashboard overview of centrally administered appliances has been implemented. This dashboard displays concise information on assigned objects and system status.

3.2 Rollout Support

A new commandline tool has been implemented for the rollout of numerous appliances as well as configuration of many interfaces. Details are available from GeNUA.

3.3 Improved Logging

The performance of the extended logging was improved.

4 New Features in GeNUGate, GeNUScreen, GeNUCrypt, GeNUCard and GeNUBox

4.1 GeNUGate Administration

- **Central Administration of GeNUGate Systems**

GeNUGate appliances of version 7.0 patch or higher can be centrally administered by GeNUCenter. This feature already was introduced with GeNUCenter 2.1 patch 6.

4.2 GeNUCard

- **Communication Between Notebooks**

Activation of hub forwarding on central GeNUCrypt or GeNUScreen systems enables direct communication between notebooks, permitting video conferences or direct VOIP telephone calls.

- **Automatic Internet Connection**

GeNUCards now can use a pre-configured Internet profile to automatically connect. Telecommuters can now work via the Internet without having to manually configure their GeNUCard.

- **Automatic VPN Connection**

GeNUCards now can use a pre-configured IPsec profile to automatically initialize a VPN tunnel. Telecommuters can now work via VPN connections without having to manually configure their GeNUCard.

4.3 GeNUScreen and GeNUCard

- **Smartcard Key Renewal**

This release features key renewal by the appliances themselves, as specified in the guidelines for restricted/confidential accreditation. The administrator is automatically notified if a key is about to expire, and can initiate key renewal on GeNUCenter. The entire process can be performed from the central GeNUCenter system without disrupting operations or requiring local configuration of the appliance.

If previously initialized smartcards are to be used, please read the smartcard chapter in the product manual, or contact GeNUA support.

4.4 GeNUBox

- **Administration Of GeNUBox 3.0 Appliances**

GeNUBox appliances of version 3.0 or higher can be centrally administered by GeNUCenter. In addition, remote maintenance via a rendezvous setup now is possible.

- **Rendezvous Operator LDAP Authentication**
Operators configured on GeNUCenter can be centrally authenticated by LDAP. Thus, a `rendezvous operator` does not require passwords on the systems to administer remote maintenance setups.
- **Unprivileged Users**
In addition to `root`, other users can also be copied to/ created on GeNUBoxes to enable console login or execution of scripts.
- **Two Factor Rendezvous Maintainer Authentication**
`Rendezvous maintainers` configured on GeNUCenter can be assigned the permission to actively open a remote maintenance connection by themselves. Maintainers now can use cryptocards for the required additional authentication.

4.5 GeNUScreen, GeNUCrypt and GeNUBox

- **SSH VPNs With Dynamic IPs**
Dynamic IP addresses now can be used for one side of SSH VPN connections via the Internet. Similar to IPsec, the VPN peer will passively wait for connection initialization if the option 'NATted' is selected.
- **Address Translation for SSH and IPsec VPNs**
Both VPN implementations (SSH and IPsec) can perform IP address translation. This assigns a so-called 'visible address' to the real internal address. The sending system performs the address translation, thus enabling third party appliances to initiate IPsec VPN connections to the 'visible address'.
- **Unidirectional SSH VPNs**
SSH VPNs now can initialize unidirectional connections. Thus, a branch office can access all services on a central server as well as access the Internet, without requiring an IP address range for the remote systems.
- **Asymmetrical SSH VPNs**
Opening services on a central server for access by remote systems sometimes does not cover all needs. E.g., a central SAP system may need to access a remote printer in a branch office.
This release permits the definition of VPNs that support the export of selected addresses from the central server to a branch office.

4.6 GeNUCard, GeNUScreen, GeNUCrypt and GeNUBox

- **Hostname Transmission During Logging**
Appliances now can optionally transmit their hostnames during logging per syslog.

5 Upgrade Installation

Any patchlevel of GeNUCenter 2.1 can be upgraded to version 2.2.

Alternatively, go to <http://www.genua.de> and click on 'Customer Service' -> 'Internal Customer Area' -> 'GeNUCenter Support' .

Before starting the upgrade, please check if you have SSH access to the GeNUCenter system, and set it up if necessary. If you are using a GeNUCenter standby system, please read chapter 4 in the product manual.

To upgrade, perform the following steps:

- Log in as `root` on the GeNUCenter machine.
- Generate the database backup by executing the following command:

```
$ db_backup
```
- Copy all files in the directory `/var/center/backup/` to a different machine.
- Create the installation CD-ROM from the ISO image and insert it into the drive.
- At the prompt

```
$ (I)nstall, (U)pgrade or (S)hell?
```

select **U** for upgrade.
- You will later be prompted for a console password. The one entered here will overwrite the original password.
- The system now installs the upgrades.
- After the upgrade installation, reboot the system when prompted. To do so, remove the CD and enter

```
$ reboot
```

at the console.
- Now log in at the Web interface and check the results. It is recommended – at the very least – to check the GeNUCenter configuration itself to prevent losing access to the Management Server due to errors.

6 How to Contact Us

GeNUA Gesellschaft fuer Netzwerk– und Unix–Administration mbH

Domagkstrasse 7, 85551 Kirchheim near Munich, Germany

Phone: +49 89 99 19 50-0, Fax: +49 89 99 19 50-999

E-Mail: info@genua.de, WWW: <http://www.genua.de/>

© 2011 GeNUA mbH, Kirchheim, all rights reserved. GeNUA, GeNUGate, GeNUCenter, GeNUScreen, GeNUCrypt, GeNUBox and GeNUCard are registered trademarks of GeNUA mbH.