



# GeNUCenter 2.3 Release Notes

Information on the GeNUCenter 2.3 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.

### 1 Scope of Delivery

With the current GeNUCenter version 2.3 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](https://www.genua.de/k/customer/gz_support/release_download.en.html)

### 2 Before Upgrading

- **GeNUCard: RNDIS Support**  
**Important:** After updating the GeNUCard software, the driver on the host system also must be updated, see the section “GeNUCARD” below. If you are still running Windows XP or older, it may be necessary to install the current RNDIS version which for example is part of the current Active Sync 4.5 distribution. See <http://www.microsoft.com/download/en/details.aspx?id=15>

### 3 New Features in GeNUCenter 2.3

#### 3.1 Comm Server

- **High Availability**  
The comm server now also runs in a high availability cluster environment.
- **Outgoing Connections**  
The comm server now supports outgoing connections between the GeNUGate system and the centrally managed appliances.



## 4 NEW FEATURES FOR GENUGATE, GENUSCREEN, GENUCRYPT, GENUCARD AND GENUBOX

---

### 3.2 Rollout Support for GeNUCards

A commandline tool now is provided to simultaneously roll out numerous GeNUCards. Please contact GeNUA for details on how to use this tool.

### 3.3 Extended ACLs

GeNUCenter access per SSH or Web GUI was improved. It now is possible to reference and use several network definitions at the same time. To do so, a *network list* first needs to be created on GeNUCenter and assigned to the ACL. Then individual definitions from this object, such as *network group*, *network list* or *single network* can be used.

The extended ACLs for SSH and Web GUI access can also be used to access *GeNUScreen*, *GeNUCrypt* and *GeNUBox* appliances.

## 4 New Features for GeNUGate, GeNUScreen, GeNUCrypt, GeNU-Card and GeNUBox

### 4.1 GeNUCard

- **New GeNUCard 2 Hardware**

The current release supports both GeNUCard 1 as well as the new GeNUCard 2 hardware.

- **Enhanced WiFi Functionality**

GeNUCard now supports connections to WiFi APs with a “hidden SSID”, as well as to networks whose SSID or WPA-PSK contains non-ASCII characters. In addition, WEP encryption with Open System Authentication now is possible.

- **Simplified UMTS Configuration**

UMTS configuration now is much more straightforward. Ideally, entering the APN is all that is needed.

- **Improved Display of Connection Parameters**

The Web GUI as well as the new Tray App now display clearer and more detailed information on connection parameters such as WiFi QoS, addresses, gateway and DNS server to the user.

- **Tray App**

A Tray App has been developed for Windows operating systems to permit user login to the GeNUCard as well as setting up connections and VPNs. Important connection information always is available without the user having to use a Web browser to view the GUI. The Tray App icon is positioned in the Windows system tray (hence the name) and continuously displays the connection status.

- **RNDIS Support**

The interface to the host computer was changed to RNDIS. Current Windows versions already supply a compatible driver.

**Important:** After updating the GeNUCard software, the driver on the host system also must be



updated. If you are still running Windows XP or older, it may be necessary to install the current RNDIS version which for example is part of the current Active Sync 4.5 distribution. See <http://www.microsoft.com/download/en/details.aspx?id=15>

- **Sending Messages to a GeNUCard**

The task *Send message to appliance system* was added to the menu "Maintenance". This enables the central notification of the GeNUCard user about important news, such as upcoming maintenance.

- **Reset PIN with One Time Only VPN Initialization**

The GeNUCard IPsec-VPN can be centrally initialized via the job *Reset PIN on Smartcard and start VPN* in the "Maintenance" menu, without any intervention by the GeNUCard user. This is necessary in special cases, e.g. to open a VPN tunnel for a single time for maintenance on directory services a user no longer can log on to. If the GeNUCard is used with a smartcard, this will also reset the smartcard PIN. It will be necessary to set it again after this intervention.

## 4.2 GeNUBox

- **Rendezvous Connections with L2TP**

A remote maintainer now can access rendezvous systems using the alternative *L2TP* connection method. The subsequent connection from the rendezvous box to the target system always uses the encrypted SSH method.

To use the alternative method, the L2TP settings in the menu *System > Extended* need to be modified. In addition, an L2TP password must be entered for the remote maintainer in the appliance's *Rendezvous* menu.

The advantage of L2TP is that remote maintenance access seemingly is directly to the target systems without any modification of the maintainer's client. This connection method can be used in parallel with SSH connections.

## 4.3 GeNUScreen, GeNUCrypt and GeNUBox

- **New Interface Type 802.1ad (Q-in-Q)**

When creating VLAN interfaces, VLANs now can also inserted into Ethernet frames per 802.1ad (Q-in-Q). To do so, select the the setting *SVLAN* for the external VLAN interface.

Previously, only 802.1q VLANs were available.

## 5 Upgrade Installation

Any patchlevel of GeNUCenter 2.2 can be upgraded to version 2.3.

To download, 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.



## 6 HOW TO CONTACT US

---

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. Activate CD boot in the GeNUCenter system's BIOS, and reboot the machine.
- 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 für 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](mailto: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.