

GeNUGate 6.1 Release Notes

Information on the GeNUGate 6.1 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 a number of problems, and provides new features.

Important Note

We strongly recommend performing a configuration or preferably full backup of your GeNUGate system BEFORE installing this patch.

Detailed instructions on how to perform this upgrade are in chapter 3 of these release notes.

Contents

1	Scope of Delivery	2
2	New Features in GeNUGate 6.1	2
2.1	Security Features	2
2.2	Relays	2
2.3	Mail	4
2.4	HA	5
2.5	VPN	5
2.6	Miscellaneous	5
3	Upgrade Installation	6
3.1	Upgrade Path	6
3.2	Data Integrity	6
3.3	Minimum Available Disk Space	7
3.4	Performing the Upgrade	7
4	How to Contact Us	10

1 Scope of Delivery

With the current GeNUGate version 6.1 you have received:

- these release notes
- a bootable CD-ROM
- compressed PostScript and PDF versions of the manual on the GeNUGate CD-ROM.

2 New Features in GeNUGate 6.1

2.1 Security Features

- **Bind:** The DNS server bind was updated to version 9.3.4, thus resolving the security problems CVE-2006-4095 / VU#915404 and CVE-2006-4096 / VU#697164.
- **Sendmail:** The mail transport agent sendmail was updated to version 8.13.8.
- **Squid:** The WWW cache Squid was updated to version 2.5.STABLE14, and the security problems CVE-2007-247 and CVE-2007-248 were resolved.
- **OpenSSH:** OpenSSH was updated to version 4.5.

2.2 Relays

- **Metarelays:** To simplify configuration, “metarelays” with useful default parameters were implemented. These can be selected in the relay configuration menu in the same manner as conventional relays.

The following metarelays are available:

- ipsec
- ldap
- mssql
- mysql
- postgresql
- pptp
- rtsp
- snmptrap
- www-server

- **QoS:** Configuration of “Quality of Service” for all relays – except for Telnet relay and FTP relay – now is possible in the GUI.
Both the (older) “Type of Service” as well as the current “Differentiated Services Code Point” standards are supported. The latter standard can be configured using the recommended classes “Assured Forwarding” (RFC 2597) and “Class Selectors” (RFC 2474).
- **SIP Relay:** A new relay supporting Internet telephony via SIP (Session Initiation Protocol) and RTP (Real Time Protocol) has been implemented. Please note that this relay needs the GeNUGate hardware 200, 400, 600 or 800, and a packet filter with a USB stick to run.
- **RTSP Proxy:** A new service supporting RTSP (Real Time Streaming Protocol) now is available on the ALG. To simplify its use, the metarelay “rtsp” mapping a tcprelay with the port 554 to localhost:1554 was predefined.
- **MAX_CONNECT and FDs:** The maximum number of file descriptors per relay as well as of open files in the kernel was increased. In addition, the parameter MAX_CONNECT permits an exact definition of these settings per relay.
- **SSLify WWW Relay and TCP Relay, Certificate Management:** WWW relay and TCP relay now support SSL.
Connections between client and relay, as well between as relay and server can be encrypted by SSL. “Bridging” mode permits the inspection of the encrypted data stream.
The following operation modes are available for WWW relay and TCP relay:
 - “Client-Relay SSL”: The client (e.g. a browser) connects to the relay using SSL. An unencrypted connection to the server is established.
 - “Bridging”: The datastream is decrypted in the relay, analyzed, re-encrypted and transmitted. To avoid browser and SSL client warnings of incorrect certificates, you will need to import the GeNUGate Certificate Authority into the client.

TCP relay offers the additional operation mode “Relay-Server SSL” which secures the connection between TCP relay and the server using SSL.

The GUI menu SERVICES → SSL provides X.509 certificate management for the new functions.

Certificates can be generated or imported here in order to utilize the new SSL functionality of WWW relay or TCP relay.
- **WWW relay:**
 - **HTTPS Without Squid:** If the WWW relay is run with the setting “Direct Request to HTTP Server”, all HTTPS requests formerly were sent through the

local Squid proxy (127.0.0.1:8000). This no longer is necessary. WWW relay now can directly communicate with a server via HTTPS without a proxy.

- **Byte Ranges/Windows Updates:** So-called “range requests” now can sent by a browser to request certain parts of a file from a webserver.

However, if a virus scanner has been configured in the WWW relay , these requests are blocked for security reasons, as data downloaded in parts could be “smuggled” past the virus scanner.

If a URL or host is specifically exempted from virus scanning in the scan ACL, range requests are permitted in these cases, thus enabling automatic Windows updates over this relay.

- **HTTP Relay Functions now Performed by WWW Relay:**

HTTP relay formerly was needed to protect a webserver. This and other functions now are handled by the WWW relay . For easier configuration, a metarelay “WWW-Server” based on WWW relay has been predefined.

HTTP relay will not be supported in future releases. Please reconfigure HTTP relay connections to be handled by the new WWW relay .

- **Squid:**

- **Deletion of URLs from the Squid Cache:**

The GUI menu SERVICES → WWW CACHE → EMPTY CACHE now permits entering specific URLs to remove from the Squid cache.

To use this function, the method PURGE must be manually permitted in a Squid ACL. To do so, enter the following rules in the GUI menu SERVICES → WWW CACHE → CONFIGURATION in the field *ACL in Squid Format* for this Squid instance:

```
acl PURGE method PURGE
http_access allow PURGE localhost
http_access deny PURGE
```

To prevent purging of the Squid cache by unprivileged users, the following rule must be entered in SERVICES → RELAYS for the Request ACL for all WWW relays:

```
!PURGE *
```

This forbids the method PURGE in the WWW relay itself.

- **NTLM Authentication:**

Additional functions were implemented to permit NTLM authentication at Squid. This calls for a number of manual settings which are described in detail in the customer area of the GeNUA webserver.

2.3 Mail

- **Configure Messages:** Configuration of error messages and the handling of errors by the e-mail system have been improved in the GUI menu SERVICES → E-MAIL

→ ERROR HANDLING.

- **DSN:**

GeNUGate now is DSN capable, i.e. the mail system will send delivery status notifications as described in the Internet standard RFC 3461. Thus, a detailed notification in human and machine readable format will be sent if a mail handled by the GeNUGate system has a problem. The format of the notification can be modified (within RFC parameters) by the sender in the mail dialog.

2.4 HA

- **E-PING:** A GeNUGate HA system can check if the external router is reachable using ping packets. To do so, permanent IP addresses are needed on the external interface. Configuring these as well as an E-ping address in the GUI will activate the check by the HA daemon.

2.5 VPN

- **NAT-T:** The VPN module now complies with RFC 3947 for IKE/IPsec NAT traversal, thus enabling VPN communication with GeNULink.

2.6 Miscellaneous

- **Hardware Monitoring:**

GeNUGate 6.1 now is able to monitor various hardware parameters. If a monitored component's status is not OK, or if the value leaves a permitted range, the system will react e.g. by sending an e-mail to the administrator.

Monitoring of supported hardware is automatically configured during the installation of, or an upgrade to GeNUGate 6.1.

If the hardware is not automatically recognized, the administrator can activate monitoring in the GUI menu SYSTEM → HARDWARE → CONFIGURATION → REVISION. If the defaults do not describe your hardware, the sensors can be manually defined in SYSTEM → HARDWARE → CONFIGURATION.

- **cfgbu on USB Stick:**

As of GeNUGate 6.1, configuration backups can be written to a FAT32 formatted USB stick:

```
# cfgbu -s -F /dev/sd2i
```

Depending on the hardware platform, the stick must be specified as `/dev/sd0i` (GeNUGate 200) or `/dev/sd2i` (GeNUGate 400,600,800).

- **VLAN Support:** The GUI now permits configuring VLAN interfaces on a physical interface in the menu SYSTEM → INTERFACES. Among other possibilities, this permits combining several physical ALG interfaces to a single one, and to separate the data packets on a VLAN capable switch.
- **Support via ggsup/GUI:** The menu SYSTEM → SUPPORT → GGSUP enables sending support requests with detailed technical information to GeNUA in an encrypted mail.
The request can also be downloaded as a ZIP file to a Windows machine.
Mails generated by this form always are encrypted with the GeNUA support key, and can only be decrypted by GeNUA.
- **Recovery Installation:**
During installation, a configuration backup now can be read from floppy, USB stick or an SSH server. The SSH server can also be an HA partner.
In addition, patches can be copied during installation from USB stick, or downloaded from an SSH server, an HA partner, or from the GeNUA support server.
- **Shell Prompt:** The standard shell prompt follows the pattern `USER@HOST:/PATH$` to simplify identification of the system when working with many terminal connections.
- **Operating Key:**
In certain rare cases, a software upgrade can trigger error messages during hardware detection, stating an invalid operating key.
Please request a new operating key from our webserver if this should happen:
`https://support.genua.de/genugate/license/license.cgi`

3 Upgrade Installation

3.1 Upgrade Path

Beginning from version 6.0, GeNUGate systems can be upgraded to version 6.1.

No specific patch level within version 6.0 is necessary.

3.2 Data Integrity

As opposed to the upgrade of GeNUGate 5.1 to GeNUGate 6.0, the current upgrade to GeNUGate 6.1 does not create any new filesystems. Therefore, log files and e-mails in the system spool directory will not be lost.

Nevertheless, please back up your configuration before upgrade with:

```
# cfgbu -s
```

To back up log files and e-mails, a full system backup is necessary, as described in the manual.

3.3 Minimum Available Disk Space

Sufficient space in the partitions on the hard drive is needed for a successful upgrade. Above all, the partitions `/` and `/usr` need more than 50% available space.

3.4 Performing the Upgrade

Please note:

Physical access to the GeNUGate system itself, or to a connected serial console is necessary.

Insert the GeNUGate 6.1 CDROM in the drive, log on to the system as the user “admin”, and become “root” with the command `su`.

```
$ su
Password:
Mar 14 13:06:33 ggd138 su: admin to root on /dev/console
#
```

Enter the command `ggupgrade` to start the upgrade.

```
# /usr/local/gg/sbin/ggupgrade
Starting GeNUGate Upgrade!
Starting /cdrom/usr/local/gg/sbin/ggupgrade ...

Before the upgrade starts, the patches for the new release are
transferred. This ensures your GeNUGate system will be running with
the latest patchlevel immediately after upgrade.

Get upgrade patch from cdrom ...
Retrieving G610_000.tar
Extracting G610_000.tar

The patches for the new version can be fetched from GeNUA over the
Internet.

Patches from GeNUA (yes no) [yes]?
```

You can check for published patches before restarting the system by typing `yes`
Reboot the system now.

```
# reboot
Mar 15 13:11:09 ggd138 reboot: rebooted by admin
/etc/rc.shutdown in progress...
IP is OFF
/etc/rc.shutdown complete.
Mar 15 13:11:12 ggd138 syslogd: exiting on signal 15
syncing disks... done
rebooting...
```

Be sure the system boots from the inserted GeNUGate 6.1 CD-ROM by checking for the message **CDBOOT 1.04** in the boot prompt.

```
>> OpenBSD/i386 CDBOOT 1.04
boot>
booting cd0a:bsd.install: 4066920+776200 [52+213232+196563]=0x5028dc
entry point at 0x100120

[ using 410220 bytes of bsd ELF symbol table ]
Copyright (c) 1982, 1986, 1989, 1991, 1993
    The Regents of the University of California.  All rights reserved.
Copyright (c) 1995-2006 OpenBSD.  All rights reserved.  http://www.OpenBSD.org

OpenBSD 3.9-stable (ALG.install) #0: Fri Mar  9 21:06:56 CET 2007
bluhm@g611.genua.de:/build/gg.61/61.D016/ALG.install
...
```

After loading the kernel, the GeNUGate 6.1 installation routine will prompt you for the installation language and keyboard mapping. Afterwards, please select the installation mode *upgrade*.

```
GeNUGate Installation

Sprache auswaehlen.
Sprache/Language (de en) [de] ? en

Select the layout of the keyboard connected to the GeNUGate.
Keyboard layout (us de de.noad ... pl hu si cf cf.noad) [us] ? [RETURN]
kbd: keyboard mapping set to us

Probing system.

Choose installation, upgrade or recovery from backup.
Mode (install upgrade recover) [install] ? upgrade
```

The hard drives and file systems are checked, mounts performed and the upgrade is started.

```
Mount hard disk.
Select boot hard disk.
Detecting hard drives in system.
Boot hard disk selected.
Unmount all partitions.
Read in fstab.
Check file systems.
/dev/rwd0a: file system is clean; not checking
/dev/rwd0f: file system is clean; not checking
/dev/rwd0d: file system is clean; not checking
/dev/rwd0e: file system is clean; not checking
Mount all partitions.
Remove flags.
GeNUGate licenses.
Initialize license.
```

You are prompted for the GeNUGate license number and hardware serial number. The values from GeNUGate 6.0 still are valid. Press *[RETURN]* to accept them.

```
Enter license.
The value to be entered has the format 1234-GG-ABCD-EFGH-IJKL-MNOP.
License [1234-GG-ABCD-EFGH-IJKL-MNOP] ? [RETURN]

Enter serial number.
The value to be entered has the format 1-234567.
Serial number [1-234567] ? [RETURN]
```

You now can transfer patches from USB stick, an HA peer or over the network.

```
Get patches from USB stick.
Fetch patches from USB medium (yes no) [no] ? [RETURN]

Get patches from HA peer.
Fetch patches from HA network (yes no) [no] ? [RETURN]

Get patches from GeNUA.
Fetch patches from network (yes no) [no] ? [RETURN]
```

The new software is copied to the system and configuration starts.

```
Begin upgrade.

Copy upgrade patch from cdrom.
Retrieving G610_000.tar
...
```

At the end of the upgrade, you are prompted to set new passwords for the administrative accounts “admin” and “root”. Alternatively, keep the existing passwords by pressing *[RETURN]* to select *no*.

```
Set administrator passwords.
Set passwords (yes no) [no] ? [RETURN]
```

The upgrade is done. Press *[RETURN]* to restart the system and remove the CD-ROM from the drive.

```
Press <Enter> to reboot, remove the cdrom after the 'rebooting...' message.
Reboot now (reboot) [reboot] ? [RETURN]
```

The system now starts the new software. After the kernel has been loaded, you are prompted for the “root” password, as a bootinstall script needs to be run to upgrade the packet filter.

```
I found at least one bootinstall script. You can only run them as root.
So I will ask for the root password now. If you do not know it, enter
three times the empty string, and we will continue with booting without
executing the bootinstall scripts. Enter your root password now.

You have 60 seconds to authenticate!

Enter root password!

Password:
```

Select the script with **1** und **[RETURN]**. Start the script by entering **y**.

```
Select a list of bootinstall scripts by entering their numbers or by entering *
to select all.

=====
1) /var/gg/boot/bootinst.2007.03.16-16.48.54.exe
   Initialize packet filter disk

Choose (1) []: 1
1) /var/gg/boot/bootinst.2007.03.16-16.48.54.exe
   Initialize packet filter disk
Is this ok? (y/n) [n]: y
```

Insert the PFL floppy in the ALG drive, or insert the PFL USB stick in an available USB slot of the ALG, and rewrite the PFL medium. Follow the displayed instructions to restart the PFL.

After restart, log on to the ALG. A banner will displayed with the new version number.

```
login: admin
Password:
Last login: Thu Mar 15 13:06:29 on console

           Welcome to your GeNUGate Firewall System.

           This system is running GeNUGate Version 6.1 000 based on OpenBSD 3.9

admin@ggd138:/var/home/admin$
```

Enjoy your new GeNUGate system!

4 How to Contact Us

GeNUA Gesellschaft für Netzwerk- und Unix-Administration mbH
Domagkstraße 7, 85551 Kirchheim/ Munich,
Tel. +49 89 99 19 50-0, Fax. +49 89 99 19 50-999
E-Mail: info@genua.de, WWW: <http://www.genua.de/>

© 2007 GeNUA mbH, Kirchheim, All rights reserved. GeNUGate and GeNUA are registered trademarks of GeNUA mbH.