



GeNUGate 7.1 Release Notes

Information on the GeNUGate 7.1 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 various problems, and provides new features.

Important - Backup!

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

Detailed instructions on how to perform this upgrade are available in section 7 of these release notes.

Important - Mirroring:

The models GeNUGate 400, 600 and 800 are equipped with mirror disks.

During the upgrade procedure, systems with mirror disks (offline mirror) will DEACTIVATE mirroring. This enables testing of the upgrade.

Upgrading of systems with mirroring is performed as follows:

- Upgrade system as described in section 7. The mirror update is automatically deactivated.
- Test: It usually is sufficient to let the upgraded system run under normal conditions for a few days.
- Reactivate mirror: After testing, delete the file `/var/db/.NOMIRROR`. This reactivates the automatic mirror update and synchronizes the mirror at the next cron job run (nightly at 2.05 a.m.).

Important - Upgrade Test in Multi User Mode:

Registry data structures were changed in version 7.1. Section 6.2 describes how to run a “Test Upgrade”, generate a new registry and check for consistency.

If this test generates error messages, we recommend fixing the inconsistencies **before** the real upgrade.



CONTENTS

Contents

1	Release Note Contents	3
2	New Features in GeNUGate 7.1	3
2.1	Additional High Availability Features	3
2.1.1	Address Types	3
2.1.2	Passive Systems	3
2.1.3	Limitations and Further Development	3
2.1.4	Established HA Installations	4
2.1.5	Usability	4
2.2	New Policy: SMTP2SMTP	4
2.3	Product Manual Restructured	4
2.4	GeNUGate version 7.0 Patches	5
2.4.1	System Status in the Admin Web Interface	5
2.4.2	Logging	5
2.4.3	Further Security Improvements	6
3	Software Updates and New Product Behavior	6
3.1	Operating System	6
3.2	Web Cache: Squid Version 3.1.16	6
3.3	SSH Version 1 Deprecated and Removed	6
3.4	Changed Status when Blocking E-Mails with the SMTP Policy	7
3.5	Sophos Virus Scanner: Manual Pattern Update Necessary	7
4	Central Administration by GeNUCenter	7
5	Overview: Versions with Update Support	7
6	Before Upgrading	7
6.1	System	7
6.2	Test Upgrade in Multi User Mode	8
7	Upgrade Installation	8
7.1	Upgrade Path	8
7.2	Data Backup	8
7.3	Minimum Available Disk Space	9
7.4	Performing the Upgrade	9
8	Information in the Web	14
9	How to Contact Us	14



1 Release Note Contents

These release notes describe the changes, bugfixes and new features available by updating from GeNUGate 7.0 to the current version 7.1. The detailed product configuration is described in the GeNUGate 7.1 manual.

An electronic version of these release notes, the software itself, and the updated product manuals are available at <http://www.genua.de/index.en.html> in the *Internal Customers Area*. Please mail us at auftrag@genua.de if you prefer us to send you a CD-ROM.

2 New Features in GeNUGate 7.1

2.1 Additional High Availability Features

Upgrading from GeNUGate 7.0 to 7.1 adds two new address types to the HA option. This is a major change, as the new feature is based on CARP (“Common Address Redundancy Protocol” as already implemented on GeNUScreen and GeNUBox) instead of OSPF. This protocol reduces takeover times and facilitates distribution of connections between cluster nodes in balancing mode, thus increasing maximum throughput. The established HA mode of operation with OSPF will continue to be supported in this and future releases.

Further information is available in the GeNUGate Administration Manual in chapter 5.3.9 “GeNUGate with CARP and PF”. A configuration scenario is described in chapter 2.11 “Load Balancing with CARP-HA”.

2.1.1 Address Types

The new “failover” and “balancing” addresses now are available. Failover addresses behave much like OSPF takeover addresses, but will switch over more quickly. Every system in a given cluster is assigned a dedicated failover address via which to contact it. If a system fails, another node will take over the address within seconds. The balancing address is the other new address type. It adds new functionality to the GeNUGate HA setup. These addresses always are configured for the entire cluster and simultaneously activated. Based on the packet source and destination addresses, the kernel decides which system handles the connection via its balancing address. All other systems drop the packets. Thus connections can be automatically distributed over the entire cluster. Performance improvement depends on how well connections are distributed, as well as the protocol used.

2.1.2 Passive Systems

When using balancing addresses, individual systems within an HA cluster can be reconfigured to passive mode. These systems will finish handling existing connections, but will not accept new ones. This is useful to gradually initiate maintenance, as only very long running connections need to be terminated. This mode can be activated in the Web interface in the menu HA → CHECKS → BALANCING PASSIVE

2.1.3 Limitations and Further Development

The use of the new address types on GeNUGate version 7.1 still is somewhat limited:



2 NEW FEATURES IN GENUGATE 7.1

- OSPF still needs to be configured
- The GeNUGate intermediate networks need to be connected on layer 2
- The address ranges for OSPF and the new addresses CANNOT be shared

These limitations are described in detail in the Administration Manual, section 2.11.1. The upcoming 7.2 release will resolve part of these issues and add functionality.

2.1.4 Established HA Installations

Depending on whether the network topology can be modified as described above, the new address types can be used in existing installations. Otherwise, we recommend not to use CARP-based (“balancing” and “failover”) addresses after upgrading to this release.

A PFL DMZ is well suited for testing the new features, as the addresses are isolated by the DMZ and probably do not have to be modified.

2.1.5 Usability

The HA configuration menus have also been reworked for usability. All relevant configuration is now available under the top level HA navigation.

2.2 New Policy: SMTP2SMTP

Previously, only the SMTP policy was available for secure delivery of e-mails by the GeNUGate. This configuration defined the GeNUGate as a fully functional mail server, but a result incoming e-mails were temporarily stored on the firewall. In addition, only a single policy could be configured for delivery to any and all destinations defined on the entire GeNUGate system.

Version 7.1 now provides the addition SMTP2SMTP policy, which implements the critical parts of the SMTP policy without storing mail on the firewall. This is done by directly contacting the destination server configured for an incoming connection. Much like a classic proxy, the incoming commands are directly copied to the destination. Activating the option “Virus Scan” causes incoming data to stored, scanned and transmitted before successful delivery is signaled to the sender.

Security still can be centrally enforced at the perimeter before e-mails enter the internal network by using SSL bridging and the virus scanner. At the same time, the new policy conserves resources and improves performance. It is especially suitable for protection of dedicated anti-spam appliances, signature gateways in the ALG DMZ, or for setting up a complex e-mail infrastructure.

Further information is available in chapter 1.4.11 “SMTP2SMTP Relay” of the Administration Manual.

2.3 Product Manual Restructured

The previous GeNUGate Manual was restructured to three separate documents:

- Installation Manual
- Administration Manual
- GUI Reference



The Installation Manual contains all information needed for the initial GeNUGate installation right up to the first login on the GUI. This manual (presently only in German) is on the CD-ROM under `docs/install-de.pdf`.

The English version will shortly be available on the GeNUA Web server.

The Administration Manual covers concepts and configurations in depth. Specific setup examples and scenarios are provided. This manual (presently only in German) is on the CD-ROM under `docs/admin-de.pdf`.

The English version will shortly be available on the GeNUA Web server.

The GUI Reference describes every menu available in the GUI in detail with screenshots. This manual (presently only in German) is on the CD-ROM under `docs/guiref-de.pdf`.

The English version will shortly be available on the GeNUA Web server.

2.4 GeNUGate version 7.0 Patches

The following changes already have been published in patches for GeNUGate version 7.0 and therefore are included in the 7.1 release. As they were not described in the previous Release Notes, they are listed here. Many of the fixes mentioned were due to the CC EAL4+ certification process for version 7.0.

2.4.1 System Status in the Admin Web Interface

The status overview for the administrator was greatly extended, especially to catch HA problems.

- **HA status with remote monitoring:** Every member of an HA cluster now queries the others to assess the cluster status. Problems on individual systems are thus more easily identified.
- **NTP:** Large time errors between HA systems cause them to discontinue synchronization of files and configuration. This state now is prominently displayed on the start and status pages.
- **Bootinstall scripts:** Certain areas of the GeNUGate configuration (e.g. the processmaster) can only be modified by using bootinstall scripts. To stress the fact that the configuration displayed in the GUI was not yet activated, active bootinstall scripts now are displayed in the status overview and the respective pages.

2.4.2 Logging

Minor improvements were made in logging usability and operational transparency.

- **Operating key warnings removed:** Warnings about not finding an operating key (e.g., during boot) were removed.
- **SSL logging:** Accounting now logs for the respective policies if SSL was decrypted, and if connections were encrypted in the client or the server direction. In addition, in case of accepted SMTP connections (SMTP-Policy), a message is added to the mail header if an SSL secured ("START-TLS") connection was used.
- **Improved logwatch:** Repeated logwatch alarms now are summarized.



3 SOFTWARE UPDATES AND NEW PRODUCT BEHAVIOR

2.4.3 Further Security Improvements

General security improvements in various areas are listed here:

- **“localhost” in `/etc/hosts`:** The “localhost” now is directly resolved via the `/etc/hosts` file, thus protecting it from DNS problems.
- **Revocation of SSL certificates:** For the case in that a certificate has been compromised, the certificate authority can revoke it by using certificate revocation lists (CRL). The GeNUGate is now shipped with some important CRLs activated. Furthermore URLs for downloading CRLs are collected, so the administrator can extend the configuration as necessary.
- **Weak cryptographic algorithms replaced:** MD5 and SHA1 algorithms were replaced in all security critical areas by SHA256 and SHA512.
- **Robust proxy processes:** The existing GeNUGate code now is audited in depth with statistical code analysis tools. In addition, `smtp-gwd` now runs in a more secure mode to prevent incoming mail from having any effect on operations.
- **Errors and banners:** Any reference to the “GeNUGate” and “GeNUA” were edited from error messages and banners to remove any indication a GeNUGate firewall is involved in a connection.
- **IPv6 kernel security:** Kernel modifications were implemented to improve IPv6 operational security.

3 Software Updates and New Product Behavior

3.1 Operating System

- **Included patches:** This version includes all changes and patches of version 7.0 up to and including patch 6.
- **Update to OpenBSD version 4.9:** The operating system OpenBSD, including all components, was updated to version 4.9.

3.2 Web Cache: Squid Version 3.1.16

The Squid Web cache was updated to the current version.

3.3 SSH Version 1 Deprecated and Removed

In the course of the GeNUGate 7.0 certification, SSH version 1 was completely deactivated for security reasons. Only the current version 2 is available. This affects:

- Remote access
- Admin login
- Paniclogin

Please update your client software and any old SSH keys assigned to users, if necessary.



3.4 Changed Status when Blocking E-Mails with the SMTP Policy

Starting with version 7.1, rules associated with the SMTP policy return the permanent error '550' (instead of '421') when blocking mails based on RBL checks. Thus, SMTP and SMTP2SMTP policies behave in the same way.

3.5 Sophos Virus Scanner: Manual Pattern Update Necessary

As already is the case with the Avira virus scanner, the Sophos scanner will only be available in the newer streaming version after the upgrade. If the Sophos virus scanner is used, a manual update is necessary after upgrading 7.0 to 7.1. This can be done on the Web interface menu SYSTEM → VIRUS SCANNER → UPDATE

4 Central Administration by GeNUCenter

Central administration of GeNUGate 7.1 by GeNUCenter is not available. Starting May 2012, the future GeNUGate release will be integrated in the GZ 3 product line.

Please use GeNUGate version 7.0 if you need to administrate GeNUGate with GeNUCenter. This has the added advantage of using a certified version and extended product support until October 2014.

5 Overview: Versions with Update Support

GeNUGate version 7.0 as well as the following GeNUGate versions are currently provided with patches and security updates:

- **GeNUGate 6.3:** This CC EAL4+ certified GeNUGate version will be supported until the end of 2012.
- **GeNUGate 7.0:** Certification to CC EAL 4+ is expected for version 7.0 Z. Patch/ security update support will be available until October 2014.

As described in our contract conditions, software versions previous to GeNUGate 7.0 may not be fully supported, especially GeNUGate 6.2. Please upgrade older systems as soon as possible.

Version 7.2 already will be released in April 2012, as a six month release cycle has been instituted. Therefore, patch support for GeNUGate 7.1 will only be available until April 2013. After 7.0, certification of GeNUGate 8.0 is planned for October 2013. These certified versions also have extended patch support.

6 Before Upgrading

6.1 System

- The upgrade to version 7.1 is supported by any version 7.0 patch level.
- At least 512MB RAM in the ALG, and 128 MB RAM in the PFL system are needed to run version 7.1.



7 UPGRADE INSTALLATION

- Sufficient hard drive space is needed on the ALG to perform the upgrade. The procedure to determine hard drive space is described in chapter 7.3.

6.2 Test Upgrade in Multi User Mode

A “test upgrade” of the GeNUGate system is recommended to detect and handle problems and inconsistencies. The procedure is as follows:

- In normal multi user mode, insert the CD-ROM in the system’s drive.
- Execute the command `ggupgrade` as the user `root`.

The first thing the test upgrade does is to convert the registry and write the result to the human readable file `/etc/configfw/fw.cfg.pretty-G710_000`.

The running system’s registry itself is **not** modified. Any occurring inconsistency will trigger error messages, and serious problems must be explicitly acknowledged.

Please note the test upgrade cannot diagnose if there is sufficient hard drive space in older hardware. To determine needed space, follow the procedure described in chapter 7.3.

After the registry test conversion, the command `configfw` is executed to check if configuration files are correctly generated from the converted data.

Afterwards, normal system operation can continue with the original, unconverted configuration, or the actual upgrade can be performed as described in chapter 7.

Please contact your service partner for further support. Detailed information is available in the files `/var/gg/patches/G710_000.upgrade.log` (registry upgrade) and `/var/gg/patches/G710_000.configfw.log`.

7 Upgrade Installation

7.1 Upgrade Path

Beginning from version 7.0, GeNUGate systems can be upgraded to version 7.1.

No specific patch level within version 7.0 is necessary.

7.2 Data Backup

The upgrade to GeNUGate 7.1 will not affect log files and e-mails in the system spool directory.

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 product manual, chapter “Backup and Restore”.



7.3 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. Enter the command `df` to determine file system usage:

```
admin@ggd132:~# df -h
Filesystem      Size  Used Avail Capacity  Mounted on
/dev/sd0a       126M  40.8M  78.9M   34%     /
/dev/sd0f       1.5G  113M   1.3G    8%     /cage
mfs:6239        62.9M  2.0K  59.8M    0%     /tmp
/dev/sd0d       502M  238M  239M   50%     /usr
/dev/sd0e       251M  33.5M  205M   14%     /var
```

The column “Capacity” states the used percentage of the respective file system.

7.4 Performing the Upgrade

Please note:

Physical access to the GeNUGate system itself, or to a connected serial console is necessary, as a CD-ROM and possibly a USB stick need to be inserted or switched.

Insert the GeNUGate 7.1 CD-ROM in the drive, log on to the system as the user “admin”, and become “root” with the command `su`.

```
admin@ggd132:~# su -
Password:
Sep 18 08:06:33 ggd132 su: admin to root on /dev/console
root@ggd132:~#
```

Enter the command `ggupgrade` to start the upgrade.

```
root@ggd132:~# /usr/local/gg/sbin/ggupgrade
Executing upgrade script from cdrom.
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 G710_000.tar

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

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

You can check for published patches before restarting the system by typing **yes**.

At this point, you will be asked some questions for the installation. Simply enter [RETURN] here - the upgrade procedure will skip these questions and continue.

Now a registry test upgrade and test run of `configfw` is performed to check for problems during the procedure. If any problems occur, please contact your service partner.

Reboot the system now.



7 UPGRADE INSTALLATION

```
root@ggd132:~# reboot
/etc/rc.shutdown in progress...
2/2 addresses added.
/etc/rc.shutdown complete.
syncing disks... done
rebooting...
```

Be sure the system boots from the inserted GeNUGate 7.1 CD-ROM by checking for the message **CDBOOT 3.15** in the boot prompt.

```
>> OpenBSD/i386 CDBOOT 3.15
boot>
booting cd0a:bsd.install: 5476020+1003244 [61+247792+227242]=0x6a1f18
entry point at 0x200120

[ using 475512 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) 1995-2011 OpenBSD. All rights reserved. http://www.OpenBSD. org

OpenBSD 4.9 (ALG.install) #0: Wed Nov  9 19:14:45 CET 2011
  bluhm@g711.genua.de:/build/gg.71/71.D009/ALG.install
cpu0: Intel(R) Xeon(R) CPU X5570 @ 2.93GHz ("GenuineIntel" 686-class) 2.94 GHz
cpu0: FPU,V86,DE,PSE,TSC,MSR,PAE,MCE,CX8,APIC,SEP,MTRR,PGE,MCA,CMOV,PAT,PS E36,CF
LUSH,DS,ACPI,MMX,FXSR,SSE,SSE2,SS,HTT,TM,SBF,SSE3,MWAIT,DS-CPL,VMX,E  ST, TM2, SSSE3
,CX16,xTPR,PDCM,DCA,SSE4.1,SSE4.2,POPCNT
...
```

After loading the kernel, the GeNUGate 7.1 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) [cf.noad] ?
us
kbd: keyboard mapping set to us

Probing system.

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



7 UPGRADE INSTALLATION

```
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 7.0 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 XXXXX-XX-XXXX.  
Serial number [12345-CD-89AB] ? [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]
```

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

```
Begin upgrade.  
  
Copy upgrade patch from cdrom.  
Retrieving G710_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] ? no
```

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 PFL (packet filter) system component.



7 UPGRADE INSTALLATION

```
At least one bootinstall script was found. You can only run them as root.
You will be asked for the root password now. If you do not know it, enter
an empty string three times, and boot will continue 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** and **[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..2011.11.02-15.12.02.exe
   Create PFL boot medium
```

```
Auswahl (1) []: 1
```

```
1) /var/gg/boot/bootinst.2011.11.02-15.12.02.exe
   Create PFL boot medium
```

```
Is this ok? (y/n) [n]: y
```

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.



7 UPGRADE INSTALLATION

```
login: admin
Password:
Last login: Mon Nov 02 15:05:02 on console

                Welcome to your GeNUGate Firewall System.

This system is running GeNUGate Version 7.1 000 based on OpenBSD 4.9

admin@ggd132:/var/home/admin$
```

Enter the command `su` to become “root”, and execute the command `configfw`. This is necessary to perform syntax checks of configuration files (the upgrade does not perform these checks):

```
root@ggd132:~# configfw
zone file /cage/ALG_2_INTERN/etc/namedb/gg.de.db: new serial
(2009081061) <= current (2009081061)
zone file /cage/ALG_2_INTERN/etc/namedb/18.172.in-addr.arpa.db: new
serial (2009081061)
<= current (2009081061)
zone file /cage/ALG_2_INTERN/etc/namedb/16.172.in-addr.arpa.db: new
serial (2009081061)
<= current (2009081061)
zone file /cage/ALG_2_INTERN/etc/namedb/19.172.in-addr.arpa.db: new
serial (2009081061)
<= current (2009081061)
zone file /cage/ALG_1_EXTERN/etc/namedb/gg.de.db: new serial
(2009081061)
<= current (2009081061)
zone file /cage/ALG_1_EXTERN/etc/namedb/16.172.in-addr.arpa.db: new
serial (2009081061)
<= current (2009081061)
SYSLOG: Nov 02 15:19:17 configfw[14384]: I5200 1249910357 SubSystem:
Installiere /etc/licenses
SYSLOG: Nov 02 15:19:17 configfw[14384]: I5200 1249910357 SubSystem:
Kommando:
/usr/local/gg/sbin/licctl -M read -M store
SYSLOG: Nov 02 15:19:18 configfw[14384]: I5200 1249910358 SubSystem:
Kommando:
/usr/local/gg/sbin/cage_setup -C /cage/LOOPBACK
SYSLOG: Nov 02 15:19:19 configfw[14384]: I5200 1249910359 SubSystem:
Kommando:
/usr/local/gg/sbin/cage_setup -C /cage/ALG_1_EXTERN
SYSLOG: Nov 02 15:19:20 configfw[14384]: I5200 1249910360 SubSystem:
Kommando:
/usr/local/gg/sbin/cage_setup -C /cage/ALG_2_INTERN
SYSLOG: Nov 02 15:19:21 configfw[14384]: I5200 1249910361 SubSystem:
Kommando:
/usr/local/gg/sbin/cage_setup -C /cage/ALG_3_ADMIN
SYSLOG: Nov 02 15:19:22 configfw[14384]: I5200 1249910362 SubSystem:
Kommando:
ln -sf /usr/share/zoneinfo/CET /etc/localtime
SYSLOG: Nov 02 15:19:22 configfw[14384]: I5200 1249910362 SubSystem:
Kommando:
/sbin/pfctl -f /etc/pf.conf
...
```

To check if all files were correctly installed, run `filecop`:

```
root@ggd132:~# filecop
filecop: Phase 1 - comparing database(es) with filesystem
filecop: Phase 2 - comparing filesystem with database(es)
```



9 HOW TO CONTACT US

If the option GeNUScan is installed on your system, be sure to update the virus scanner! As **root**, execute the command `getpatterns`:

```
root@ggd132:~# getpatterns  
...
```

Enjoy your new GeNUGate system!

8 Information in the Web

These release notes also are available on our Web server in the “Customer Service” area:

<http://www.genua.de/customer/index.en.html> ,

“Internal Customers Area”.

Further information is available in the “Internal Customers Area”, “GeNUGate Support” → “Knowledge Base” (login required).

9 How to Contact Us

GeNUA Gesellschaft fuer 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/>

© 2011 GeNUA mbH, Kirchheim, All rights reserved. GeNUGate and GeNUA are registered trade marks of GeNUA mbH.