

---

PGP Command Line

Installation Guide

Version 7.0

Copyright © 1990-2000 Networks Associates Technology, Inc. All Rights Reserved. No part of this publication may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language in any form or by any means without the written permission of Networks Associates Technology, Inc., or its suppliers or affiliate companies.

PGP\* Command Line, Version 7.0.1

12-2000. Printed in the United States of America.

## LICENSE AGREEMENT

NOTICE TO ALL USERS: FOR THE SPECIFIC TERMS OF YOUR LICENSE TO USE THE SOFTWARE THAT THIS DOCUMENTATION DESCRIBES, CONSULT THE README.1ST, LICENSE.TXT, OR OTHER LICENSE DOCUMENT THAT ACCOMPANIES YOUR SOFTWARE, EITHER AS A TEXT FILE OR AS PART OF THE SOFTWARE PACKAGING. IF YOU DO NOT AGREE TO ALL OF THE TERMS SET FORTH THEREIN, DO NOT INSTALL THE SOFTWARE. IF APPLICABLE, YOU MAY RETURN THE PRODUCT TO THE PLACE OF PURCHASE FOR A FULL REFUND.

## NETWORK ASSOCIATES TRADEMARK ATTRIBUTIONS

\* *ActiveHelp, Bomb Shelter, Building a World of Trust, CipherLink, Clean-Up, Cloaking, CNX, Compass 7, CyberCop, CyberMedia, Data Security Letter, Discover, Distributed Sniffer System, Dr Solomon's, Enterprise Secure Cast, First Aid, ForceField, Gauntlet, GMT, GroupShield, HelpDesk, Hunter, ISDN Tel/Scope, LM 1, LANGuru, Leading Help Desk Technology, Magic Solutions, MagicSpy, MagicTree, Magic University, MagicWin, MagicWord, McAfee, McAfee Associates, MoneyMagic, More Power To You, Multimedia Cloaking, NetCrypto, NetOctopus, NetRoom, NetScan, Net Shield, NetShield, NetStalker, Net Tools, Network Associates, Network General, Network Uptime!, NetXRray, Nuts & Bolts, PC Medic, PCNotary, PGP, PGP (Pretty Good Privacy), PocketScope, Pop-Up, PowerTelnet, Pretty Good Privacy, PrimeSupport, RecoverKey, RecoverKey-International, ReportMagic, RingFence, Router PM, Safe & Sound, SalesMagic, SecureCast, Service Level Manager, ServiceMagic, Site Meter, Sniffer, SniffMaster, SniffNet, Stalker, Statistical Information Retrieval (SIR), SupportMagic, Switch PM, TeleSniffer, TIS, TMach, TMeg, Total Network Security, Total Network Visibility, Total Service Desk, Total Virus Defense, T-POD, Trusted Mach, Trusted Mail, Uninstaller, Virex, Virex-PC, Virus Forum, ViruScan, VirusScan, VShield, WebScan, WebShield, WebSniffer, WebStalker WebWall, and ZAC 2000* are registered trademarks of Network Associates and/or its affiliates in the US and/or other countries. All other registered and unregistered trademarks in this document are the sole property of their respective owners.

The IDEA(tm) cryptographic cipher described in U.S. patent number 5,214,703, licensed from Ascom Tech AG; and the Northern Telecom Ltd., CAST Encryption Algorithm, licensed from Northern Telecom, Ltd. IDEA is a trademark of Ascom Tech AG. Network Associates Inc. may have patents and/or pending patent applications covering subject matter in this software or its documentation; the furnishing of this software or documentation does not give you any license to these patents. The compression code in PGP is by Mark Adler and Jean-Loup Gailly, used with permission from the free Info-ZIP implementation. LDAP software provided courtesy University of Michigan at Ann Arbor, Copyright © 1992-1996 Regents of the University of Michigan. All rights reserved. This product includes software developed by the Apache Group for use in the Apache HTTP server project (<http://www.apache.org/>). Copyright © 1995-2000 The Apache Group. All rights reserved. See text files included with the software or the PGP web site for further information. Balloon help support courtesy of James W. Walker. This software is based in part on the work of the Independent JPEG Group. Soft TEMPEST font courtesy of Ross Anderson and Marcus Kuhn. Biometric word list for fingerprint verification courtesy of Patrick Juola.

---

# Table of Contents

<b>Chapter 1. Introduction</b> .....	<b>5</b>
How to contact PGP Security and Network Associates .....	5
Customer service .....	5
Technical support .....	6
Download support .....	7
Network Associates training .....	7
Comments and feedback .....	7
Recommended readings .....	7
The history of cryptography .....	7
Technical aspects of cryptography .....	8
Politics of cryptography .....	9
Network security .....	10
<b>Chapter 2. Installing PGP Command Line</b> .....	<b>11</b>
System requirements .....	11
Installing PGP Command Line on a Windows NT or Windows 2000 System .....	12
Installing PGP Command Line on a Solaris System .....	14
Installing PGP Command Line on AIX and HP-UX systems .....	16
Installing PGP Command Line on Linux Systems .....	16
Configuring PGP Command Line .....	17
<b>Index</b> .....	<b>19</b>



Welcome to PGP Command Line software! This Installation Guide provides general information about PGP Command Line and describes the system requirements and installation instructions necessary to successfully run it.

## How to contact PGP Security and Network Associates

### Customer service

Network Associates continues to market and support the product lines from each of the new independent business units. You may direct all questions, comments, or requests concerning the software you purchased, your registration status, or similar issues to the Network Associates Customer Service department at the following address:

Network Associates Customer Service  
4099 McEwen, Suite 500  
Dallas, Texas 75244  
U.S.A.

The department's hours of operation are 8 A.M. to 8 P.M. Central time, Monday through Friday.

Other contact information for corporate-licensed customers:

Phone: (972) 308-9960  
E-Mail: [services\\_corporate\\_division@nai.com](mailto:services_corporate_division@nai.com)  
World Wide Web: <http://support.nai.com>

Other contact information for retail-licensed customers:

Phone: (972) 308-9960  
E-Mail: [cust\\_care@nai.com](mailto:cust_care@nai.com)  
World Wide Web: <http://www.pgp.com/>

## Technical support

PGP Security and Network Associates are famous for their dedication to customer satisfaction. The companies have continued this tradition by making their sites on the World Wide Web valuable resources for answers to technical support issues. PGP Security encourages you to make this your first stop for answers to frequently asked questions, for updates to PGP Security and Network Associates software, and for access to news and virus information.

World Wide Web: <http://support.nai.com>

If the automated services do not have the answers you need, contact Network Associates at one of the following numbers between 8 A.M. and 8 P.M. Central time, Monday through Friday, to find out about Network Associates technical support plans.

For corporate-licensed customers:

Phone: (972) 308-9960

For retail-licensed customers:

Phone: (972) 855-7044

To provide the answers you need quickly and efficiently, the Network Associates technical support staff needs some information about your computer and your software. Please include this information in your correspondence:

- Program name and version number
- Computer brand and model
- Any additional hardware or peripherals connected to your computer
- Operating system type and version numbers
- Network name, operating system, and version
- Network card installed, where applicable
- Modem manufacturer, model, and bits-per-second rate, where applicable
- Relevant browsers or applications and their version numbers, where applicable
- How to reproduce your problem: when it occurs, whether you can reproduce it regularly, and under what conditions
- Information needed to contact you by voice, fax, or email

## Download support

To get help with navigating or downloading files from the Network Associates Web sites or FTP sites, call:

Corporate customers: (801) 492-2650

Retail customers: (801) 492-2600

## Network Associates training

For information about scheduling on-site training for any PGP Security or Network Associates product, call Network Associates Customer Service at: (972) 308-9960.

## Comments and feedback

PGP Security appreciates your comments and reserves the right to use any information you supply in any way it believes appropriate without incurring any obligation whatsoever. Please send any documentation comments to [tns\\_documentation@nai.com](mailto:tns_documentation@nai.com).

## Recommended readings

This section identifies Web sites, books, and periodicals about the history, technical aspects, and politics of cryptography, as well as trusted PGP download sites.

## The history of cryptography

- *The Code Book: The Evolution of Secrecy from Mary, Queen of Scots, to Quantum Cryptography*, Simon Singh, Doubleday & Company, Inc., 1999, ISBN 0-385-49531-5.
- *The Codebreakers: The Story of Secret Writing*, David Kahn, Simon & Schuster Trade, 1996, ISBN 0-684-83130-9 (updated from the 1967 edition). This book is a history of codes and code breakers from the time of the Egyptians to the end of WWII. Kahn first wrote it in the sixties—this is the revised edition. This book won't teach you anything about how cryptography is done, but it has been the inspiration of the whole modern generation of cryptographers.

## Technical aspects of cryptography

### Web sites

- [www.iacr.org](http://www.iacr.org)—International Association for Cryptologic Research (IACR). The IACR holds cryptographic conferences and publishes journals.
- [www.pgpi.org](http://www.pgpi.org)—An international PGP Web site, which is not maintained by PGP Security, Inc. or Network Associates, Inc., is an unofficial yet comprehensive resource for PGP.
- [www.nist.gov/aes](http://www.nist.gov/aes)—The National Institute of Standards and Technology (NIST) Advanced Encryption Standard (AES) Development Effort, perhaps the most interesting project going on in cryptography today.
- [www.ietf.org/rfc/rfc2440.txt](http://www.ietf.org/rfc/rfc2440.txt)—The specification for the IETF OpenPGP standard.

### Books and periodicals

- *Applied Cryptography: Protocols, Algorithms, and Source Code in C*, 2<sup>nd</sup> edition, Bruce Schneier, John Wiley & Sons, 1996; ISBN 0-471-12845-7. If you can only buy one book to get started in cryptography, this is the one to buy.
- *Handbook of Applied Cryptography*, Alfred Menezes, Paul van Oorschot and Scott Vanstone, CRC Press, 1996; ISBN 0-8493-8523-7. This is the technical book you should get after Schneier. There is a lot of heavy-duty math in this book, but it is nonetheless usable for those who do not understand the math.
- *Journal of Cryptology*, International Association for Cryptologic Research (IACR). See [www.iacr.org](http://www.iacr.org).
- *Advances in Cryptology*, conference proceedings of the IACR CRYPTO conferences, published yearly by Springer-Verlag. See [www.iacr.org](http://www.iacr.org).
- *Cryptography for the Internet*, Philip Zimmermann, Scientific American, October 1998 (introductory tutorial article).
- *The Twofish Encryption Algorithm: A 128-Bit Block Cipher*, Bruce Schneier, et al, John Wiley & Sons, Inc., 1999; ISBN: 0471353817. Contains details about the Twofish cipher ranging from design criteria to cryptanalysis of the algorithm.

---

# Politics of cryptography

## Web sites

- [www.epic.org](http://www.epic.org)—Electronic Privacy Information Center.
- [www.cryp.to.org](http://www.cryp.to.org)—Internet Privacy Coalition.
- [www.eff.org](http://www.eff.org)—Electronic Frontier Foundation.
- [www.privacy.org](http://www.privacy.org)—The Privacy Page. Great information resource about privacy issues.
- [www.cdt.org](http://www.cdt.org)—Center for Democracy and Technology.
- [www.pgp.com/phil](http://www.pgp.com/phil)—Phil Zimmermann’s home page, his Senate testimony, and so on.

## Books

- *Privacy on the Line: The Politics of Wiretapping and Encryption*, Whitfield Diffie and Susan Landau, The MIT Press, 1998, ISBN 0-262-04167-7. This book is a discussion of the history and policy surrounding cryptography and communications security. It is an excellent read, even for beginners and non-technical people. Includes information that even a lot of experts don’t know.
- *Technology and Privacy: The New Landscape*, Philip Agre and Marc Rotenberg, The MIT Press, 1997; ISBN 0-262-01162-x.
- *Building in Big Brother, The Cryptographic Policy Debate*, edited by Lance Hoffman, Springer-Verlag, 1995; ISBN 0-387-94441-9.
- *The Official PGP User’s Guide*, Philip Zimmermann, The MIT Press, 1995; ISBN 0-262-74017-6. How to use PGP, written in Phil’s own words.
- *The Code Book: The Evolution of Secrecy from Ancient Egypt to Quantum Cryptography*, Simon Singh, Doubleday & Company, Inc., September 2000; ISBN: 0385495323. This book is an excellent primer for those wishing to understand how the human need for privacy has manifested itself through cryptography.

## Network security

### Books

- *Building Internet Firewalls*, Elizabeth D. Zwicky, D. Brent Chapman, Simon Cooper, and Deborah Russell (Editor), O'Reilly & Associates, Inc., 2000; ISBN: 1565928717. This book is a practical guide to designing, building, and maintaining firewalls.
- *Firewalls and Internet Security: Repelling the Wily Hacker*, William R. Cheswick, Steven M. Bellovin, Addison Wesley Longman, Inc., 1994; ISBN: 0201633574. This book is a practical guide to protecting networks from hacker attacks through the Internet.
- *Hacking Exposed: Network Security Secrets and Solutions*, Stuart McClure, Joel Scambray, and George Kurtz, The McGraw-Hill Companies, 1999; ISBN: 0072121270. The state of the art in breaking into computers and networks, as viewed from the vantage point of the attacker and the defender.

This chapter describes how to install PGP Command Line for Windows NT and UNIX software. Before you begin installing PGP Command Line, be sure to review the system requirements outlined below.

## System requirements

**To install PGP Command Line on a Windows NT or Windows 2000 system, you must have:**

- Windows NT version 4.0 or higher (Service Pack 4 or later), or Windows 2000
- 32MB RAM minimum
- 8MB disk space for software

**To install PGP Command Line on a UNIX system, you must have:**

- One of these flavors of UNIX:
  - Solaris 2.6 or later
  - AIX 4.2 or later
  - HPUX 10.20 or later
  - Linux x86 Red Hat (RPM) 5.0 or later
- 64MB RAM minimum for Solaris  
32MB RAM minimum for Linux, AIX, and HPUX
- 10MB disk space for software
- 10MB disk space in `/opt` partition for Solaris

## Installing PGP Command Line on a Windows NT or Windows 2000 System

You can download PGP Command Line software from the Network Associates Web site, your company's download directory, or load the software from a CD-ROM. The self-extracting file, SETUP.EXE, automatically extracts and installs all of the necessary software components in their proper directory locations.

---

### To install PGP Command Line on a Windows NT or Windows 2000 machine:

1. Start the Windows NT or Windows 2000 system.
2. Download the PGP files to the system or insert the PGP CD-ROM into the CD-ROM drive.
3. Double-click SETUP.EXE to start the Setup program.

---

**NOTE:** If you are installing from the CD-ROM, the Setup program automatically starts. If, however, the Setup program does not initiate, double-click SETUP.EXE in the Disk 1 folder on the CD-ROM.

---

The **PGP Command Line Welcome** screen appears.

4. Review the information in the **Welcome** screen, then click **Next**.

The Network Associates license agreement appears.

5. Review the license agreement information, then click **Yes** to accept the licensing terms.

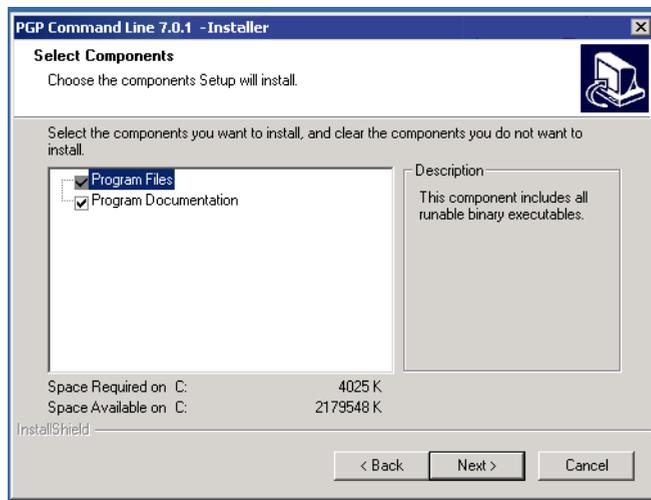
The **ReadMe.txt** file appears listing the new features and other important information regarding PGP Command Line.

6. Review the ReadMe.txt file, then click **Next**.

The **Choose a Destination Location** dialog box appears.

7. Click **Browse** to navigate to a destination directory for your PGP files or use the default directory, then click **Next**.

The **Select Components** dialog box appears, as shown in [Figure 2-1 on page 13](#).



**Figure 2-1. PGP Command Line Select Components dialog box**

8. Clear the components that you do not want to install. By default, both options are selected.
  - **Program files (required).** This option must be selected to install the PGP Command Line program.
  - **Program documentation.** Select this option to install the PGP Command Line documentation.
9. Click **Next**.

The PGP files are copied to the computer.
10. Click **Finish** to complete the PGP Command Line installation.

# Installing PGP Command Line on a Solaris System

You can download the PGP software from the Network Associates Web site, your company's download directory, or load the software from a CD-ROM.

---

## To install the Command Line Solaris package on a Sun SparcStation

The Solaris package automatically extracts and installs all of the necessary software components in their proper directory locations.

---

**NOTE:** To install the software, you must have root privileges.

---

1. Download the PGP package to the system or insert the PGP CD-ROM into the CD-ROM drive.

To install from a CD-ROM drive you must also login as root, and cd to the install directory (/cdrom). The CD mounts automatically. If, however, the CD does not mount automatically, you can mount it by going into the root directory (Cd . .), and issuing the following command:

```
#mount -F nfs -ro /dev/dsk/c0t6d0s2 /cdrom
```

2. If this is the first time you are installing the PGP Command Line product on this system, navigate to the directory where the PGPcmdln\_x.x.x\_Solaris file is located, and begin installing the package by issuing the following command:

```
pkgadd -d PGPcmdln_x.x.x_Solaris
```

(where x.x.x is the release number)

If a previous version of the Command Line is installed on this system, you must remove it before you can install the new package. If you have PGP version 6.5.x installed, you can remove it by issuing the following command:

```
pkgrm PGP
```

If you have PGP version 7.x installed, you can remove it by issuing the following command:

```
pkgrm PGPcmdln
```

---

**NOTE:** If you install from a CD-ROM drive under Sun Solaris, you may receive a warning that tells you that the file system does not conform to ISO-9660 specifications. This is because the name of the file has more than eight characters. Ignore this warning; the install will proceed without problems.

---

3. Review the license agreement information, then type `Y` to accept the licensing terms.

The installer processes the package and system information, verifies disk space requirements, and installs PGP Command Line program files.

---

**NOTE:** The program files are installed to the default installation path of `/opt/PGP/`.

---

4. When the installation is complete, you can verify that the product was installed properly by entering the following command:

```
pkginfo -l PGPcmdln
```

The status for the selected package should be “STATUS: completely installed.”

---

### To install the Command Line tarball on a Sun SparcStation

1. Download the PGP package to the system or insert the PGP CD-ROM into the CD-ROM drive.

To install from a CD-ROM drive you must first copy the PGP installation file for your operating system to a temporary location on your systems harddrive. Then change your current working directory to that same location.

2. Uncompress the package by issuing the following command:

```
gzip -d < PGPcmdln_x.x.x_Solaris.tar.gz | tar xvf -
```

(where `x.x.x` is the release number)

When the package is uncompressed, the `pgp-x.x.x/` directory is created.

3. To run PGP Command Line application, enter the following command:

```
./pgp
```

## Installing PGP Command Line on AIX and HP-UX systems

You can download the PGP software from the Network Associates Web site, your company's download directory, or load the software from a CD-ROM. To install the software, you must have root privileges.

---

### To install PGP Command Line on AIX and HP-UX systems

1. Download the PGP package to the system or insert the PGP CD-ROM into the CD-ROM drive.

To install from a CD-ROM drive you must first copy the PGP installation file for your operating system to a temporary location on your system's harddrive. Then change your current working directory to that same location.

2. Uncompress the package by issuing the following command:

```
gzip -d < PGPcmdln_x.x.x_AIX.tar.gz | tar xvf -
```

or

```
gzip -d < PGPcmdln_x.x.x_HP-UX.tar.gz | tar xvf -
```

(where x.x.x is the release number)

When the package is uncompressed, the `pgp-x.x.x/` directory is created.

3. To run PGP Command Line application, enter the following command:

```
./pgp
```

## Installing PGP Command Line on Linux Systems

You can download the PGP software from the Network Associates Web site, your company's download directory, or load the software from a CD-ROM.

---

### To install PGP Command Line on Linux RPM systems

To install the software, you must have root privileges.

1. Download the PGP files to the system or insert the PGP CD-ROM into the CD-ROM drive.

2. Install the package by issuing the following command:

```
rpm -iv PGPcmdln_x.x.x_linux.i386.rpm
```

(where x.x.x is the release number)

The PGP program files are copied to the system.

3. When installation is complete, verify the PGP signature file by adding the PGP signature in the Sample Keys.Asc file found in /usr/doc/pgp-x.x.x/ directory to your keyring.

Once the PGP signature is added to your keyring, issue the following command:

```
rpm --checksig PGPcmdln_x.x.x_linux.i386.rpm
```

(where x.x.x is the release number)

If the signature is correct, the response from this command is “OK”.

---

### To install the PGP Command Line tarball on Linux systems

1. Download the PGP package to the system or insert the PGP CD-ROM into the CD-ROM drive.

To install from a CD-ROM drive you must first copy the PGP installation file for your operating system to a temporary location on your systems harddrive. Then change your current working directory to that same location.

2. Uncompress the package by issuing the following command:

```
gzip -d < PGPcmdln_x.x.x_linux.tar.gz | tar xvf -
```

(where x.x.x is the release number)

When the package is uncompressed, the pgp-x.x.x/ directory is created.

3. To run PGP Command Line application, enter the following command:

```
./pgp
```

## Configuring PGP Command Line

For information about using PGP Command Line, refer to PGP Command Line User's Guide included with the product.



# Index

## A

AIX  
PGP Command Line [16](#)

## C

configuring  
PGP Command Line [17](#)

Customer Service  
contacting [5](#)

## H

HPUX  
PGP Command Line [16](#)

## I

installing  
PGP Command Line [11](#)  
ISO-9660 specifications [15](#)

## L

Linux (RPM)  
PGP Command Line [16](#)

## N

Network Associates  
contacting  
Customer Service [5](#)  
within the United States [6](#)  
training [7](#)

## P

PGP Command Line  
configuring [17](#)  
installing [11](#)  
on a Sun SparcStation [14](#)  
on AIX [16](#)  
on HPUX [16](#)  
on Linux [16](#)  
on Solaris [14](#)  
on Windows NT [12](#)  
on Windows 2000 [12](#)  
system requirements [11](#)  
verifying [15](#)

## R

RPM  
PGP Command Line [16](#)

## S

setup.exe, installing PGP Command Line [12](#)  
Solaris  
installing PGP Command Line [14](#)  
system requirements  
for PGP Command Line [11](#)

## T

technical support  
information needed from user [6](#)  
online [6](#)  
phone numbers for [6](#)  
training for Network Associates products [7](#)  
scheduling [7](#)

## V

verifying

PGP Command Line installed [15](#)

## W

Windows NT

installing on [12](#)

Windows 2000

installing on [12](#)