PGP

Installation Guide

Copyright © 1990-1998 Network Associates, Inc. and its Affiliated Companies. All Rights Reserved.

PGP*, Version 6.0.2 for Windows 95, 98, and NT, and Macintosh

11-98. Printed in the EC

PGP, Pretty Good, and Pretty Good Privacy are registered trademarks of Network Associates, Inc. and/or its Affiliated Companies in the US and other countries. All other registered and unregistered trademarks in this document are the sole property of their respective owners.

Portions of this software may use public key algorithms described in U.S. Patent numbers 4,200,770, 4,218,582, 4,405,829, and 4,424,414, licensed exclusively by Public Key Partners; 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 © 1995-1997 The Apache Group. All rights reserved. See text files included with the software or the PGP web site for further information. This software is based in part on the work of the Independent JPEG Group. Soft TEMPEST font courtesy of Ross Anderson and Marcus Kuhn.

The software provided with this documentation is licensed to you for your individual use under the terms of the End User License Agreement and Limited Warranty provided with the software. The information in this document is subject to change without notice. Network Associates Inc. does not warrant that the information meets your requirements or that the information is free of errors. The information may include technical inaccuracies or typographical errors. Changes may be made to the information and incorporated in new editions of this document, if and when made available by Network Associates Inc.

Export of this software and documentation may be subject to compliance with the rules and regulations promulgated from time to time by the Bureau of Export Administration, United States Department of Commerce, which restrict the export and re-export of certain products and technical data.

Network Associates, Inc.
Gatwickstraat_25
1043_GL_Amsterdam

+31(20)5866100(voice)/+31(20)5866101(fax)

info@nai.com

***** is sometimes used instead of the **®** for registered trademarks to protect marks registered outside of the U.S.

LIMITED WARRANTY

Limited Warranty. Network Associates warrants that for sixty (60) days from the date of original purchase the media (for example diskettes) on which the Software is contained will be free from defects in materials and workmanship.

Customer Remedies. Network Associates' and its suppliers' entire liability and your exclusive remedy shall be, at Network Associates' option, either (i) return of the purchase price paid for the license, if any, or (ii) replacement of the defective media in which the Software is contained with a copy on nondefective media. You must return the defective media to Network Associates at your expense with a copy of your receipt. This limited warranty is void if the defect has resulted from accident, abuse, or misapplication. Any replacement media will be warranted for the remainder of the original warranty period. Outside the United States, this remedy is not available to the extent Network Associates is subject to restrictions under United States export control laws and regulations.

Warranty Disclaimer. To the maximum extent permitted by applicable law, and except for the limited warranty set forth herein, THE SOFTWARE IS PROVIDED ON AN "AS IS" BASIS WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. WITHOUT LIMITING THE FOREGOING PROVISIONS, YOU ASSUME RESPONSIBILITY FOR SELECTING THE SOFTWARE TO ACHIEVE YOUR INTENDED RESULTS, AND FOR THE INSTALLATION OF, USE OF, AND RESULTS OBTAINED FROM THE SOFTWARE. WITHOUT LIMITING THE FOREGOING PROVISIONS, NETWORK ASSOCIATES MAKES NO WARRANTY THAT THE SOFTWARE WILL BE ERROR-FREE OR FREE FROM INTERRUPTIONS OR OTHER FAILURES OR THAT THE SOFTWARE WILL MEET YOUR REQUIREMENTS. TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, NETWORK ASSOCIATES DISCLAIMS ALL WARRANTIES, EITHER EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND NONINFRINGEMENT WITH RESPECT TO THE SOFTWARE AND THE ACCOMPANYING DOCUMENTATION. SOME STATES AND JURISDICTIONS DO NOT ALLOW LIMITATIONS ON IMPLIED WARRANTIES, SO THE ABOVE LIMITATION MAY NOT APPLY TO YOU. The foregoing provisions shall be enforceable to the maximum extent permitted by applicable law.

Table of Contents

Chapter 1. Introduction 7

How to Contact Network Associates International BV. 7

Customer service 7

Technical support 7

Network Associates training 8

Your feedback is welcome 8

Related reading 9

Chapter 2. Installing PGP 11

System requirements 11

Compatibility with other versions 12

Upgrading from a previous version 12

Installing PGP Version 6.0 for Windows 95, 98, and NT 14

Installing PGP Version 6.0 for Macintosh 17

Index 19

Introduction 1

Welcome to PGP software! This Quick Start guide provides general information about PGP and describes the system requirements and installation instructions necessary to successfully run it.

How to Contact Network Associates International BV.

Customer service

To order products or obtain product information, contact the Network Associates Customer Care department.

You can contact Customer Care at one of the following numbers Monday through Friday between 6:00 A.M. and 6:00 P.M.

Phone	+31(20)5866100

Or write to:

Network Associates International BV.
Gatwickstraat 25
1043 GL Amstermdam
Netherland

Technical support

Network Associates is famous for its dedication to customer satisfaction. We have continued this tradition by making our site on the World Wide Web a valuable resource for answers to technical support issues. We encourage you to make this your first stop for answers to frequently asked questions, for updates to Network Associates software, and for access to Network Associates news and encryption information.

World Wide Web	http://www.nai.com

Technical Support for your PGP product is also available through these channels:

Phone	+31(20)5866100
Email	tech-support-europe@nai.com

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 have this information ready before you call:

- PGP product name
- PGP product version
- Computer platform and CPU type
- Amount of available memory (RAM)
- Operating system and version and type of network
- Content of any status or error message displayed on screen or appearing in a log file (not all products produce log files)
- Email application and version (if the problem involves using PGP with an email product, for example, the Eudora plug-in)

Network Associates training

For information about scheduling on-site training for any Network Associates product, call +31(20)5866100.

Your feedback is welcome

We continually enhance PGP products and welcome customer feedback as we design new versions. We appreciate your interest in PGP products and your thoughts on product content and functionality. Feedback like yours helps us to develop richer and easier-to-use software and services. While we cannot incorporate all suggestions, we will give your input serious consideration as we develop future products.

Related reading

Here are some documents that you may find helpful in understanding cryptography:

Non-Technical and beginning technical books

- "*Cryptography for the Internet*," by Philip R. Zimmermann. Scientific American, October 1998. This article, written by PGP's creator, is a tutorial on various cryptographic protocols and algorithms, many of which happen to be used by PGP.
- "*Privacy on the Line*," by Whitfield Diffie and Susan Eva Landau. MIT Press; ISBN: 0262041677. 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, and contains information that even a lot of experts don't know.
- "*The Codebreakers*," by David Kahn. Scribner; ISBN: 0684831309. 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, and published a revised edition in 1996. This book won't teach you anything about how cryptography is accomplished, but it has been the inspiration of the whole modern generation of cryptographers.
- *"Network Security: Private Communication in a Public World,"* by Charlie Kaufman, Radia Perlman, and Mike Spencer. Prentice Hall; ISBN: 0-13-061466-1. This is a good description of network security systems and protocols, including descriptions of what works, what doesn't work, and why. Published in 1995, it doesn't have many of the latest technological advances, but is still a good book. It also contains one of the most clear descriptions of how DES works of any book written.

Intermediate books

- *"Applied Cryptography: Protocols, Algorithms, and Source Code in C,"* by Bruce Schneier. John Wiley & Sons; ISBN: 0-471-12845-7. This is a good beginning technical book on how a lot of cryptography works. If you want to become an expert, this is the place to start.
- "*Handbook of Applied Cryptography*," by Alfred J. Menezes, Paul C. van Oorschot, and Scott Vanstone. CRC Press; ISBN: 0-8493-8523-7. This is the technical book you should read after Schneier's book. There is a lot of heavy-duty math in this book, but it is nonetheless usable for those who do not understand the math.

- "*Internet Cryptography*," by Richard E. Smith. Addison-Wesley Pub Co; ISBN: 0201924803. This book describes how many Internet security protocols work. Most importantly, it describes how systems that are designed well nonetheless end up with flaws through careless operation. This book is light on math, and heavy on practical information.
- "*Firewalls and Internet Security: Repelling the Wily Hacker*," by William R. Cheswick and Steven M. Bellovin. Addison-Wesley Pub Co; ISBN: 0201633574. This book is written by two senior researchers at AT&T Bell Labs and is about their experiences maintaining and redesigning AT&T's Internet connection. Very readable.

Advanced books

- "*A Course in Number Theory and Cryptography*," by Neal Koblitz. Springer-Verlag; ISBN: 0-387-94293-9. An excellent graduate-level mathematics textbook on number theory and cryptography.
- "*Differential Cryptanalysis of the Data Encryption Standard*," by Eli Biham and Adi Shamir. Springer-Verlag; ISBN: 0-387-97930-1. This book describes the technique of differential cryptanalysis as applied to DES. It is an excellent book for learning about this technique.

Installing PGP 2

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

System requirements

To install PGP on a Windows 95, 98, or NT system, you must have:

- Windows 95, 98, or NT
- 16 MB RAM
- 15 MB hard disk space

To install PGP on a Macintosh system, you must have:

- Macintosh IIci or later model with 68030 or higher
- System software 7.5.5 or later
- 8 MB RAM
- 10 MB hard disk space
- 68K Macs must be running Apple's CFM 68K 4.0 or higher. The PGP installer installs this if necessary.

Compatibility with other versions

PGP has gone through many revisions since it was released by Phil Zimmermann as a freeware product in 1991. Although this version of PGP represents a significant rewrite of the original program and incorporates a completely new user interface, it has been designed to be compatible with earlier versions of PGP. This means that you can exchange secure email with people who are still using these older versions of the product:

- PGP 2.6 (Distributed by MIT)
- PGP 2.7.1 for the Macintosh (Released by ViaCrypt)
- PGP 4.0 (Released by ViaCrypt)
- PGP 4.5 (Released by PGP, Inc.)
- PGP for Personal Privacy, Version 5.0 - 5.5
- PGP for Business Security or PGP for Email and Files Version 5.5

NOTE: PGP products Version 5.0 and later may require the RSA add-on for backward compatibility.

Upgrading from a previous version

If you are upgrading from a previous version of PGP (from PGP, Inc., Network Associates, Inc. or ViaCrypt), you may want to remove the old program files before installing PGP to free up some disk space. However, you should be careful not to delete the private and public keyring files used to store any keys you have created or collected while using the previous version. When you install PGP, you are given the option of retaining your existing private and public keyrings, so you don't have to go to the trouble of importing all of your old keys. To upgrade from a previous version, follow the appropriate steps listed next.

To upgrade from PGP Version 2.6.2 or 2.7.1

1. Exit all programs or open applications.
2. Make backups of your old PGP keyrings on another volume. In PGP for Windows versions 2.6.2 and 2.7.1, your public keys are stored in the file titled "pubring.pgp" and your private keys are stored in the file titled "secring.pgp". In versions 5.x - 6.0, your public keys are stored in the file titled "pubring.pkr" and your private keys are stored in the file titled"secring.skr".

TIP: Make two separate backups of your keyrings onto two different floppy disks just to be safe. Be especially careful not to lose your private keyring; otherwise you will never be able to decrypt any email messages or file attachments encrypted with the lost keys. Store the keyrings in a secure place where only you have access to them.

3. When you have successfully backed up your old keyrings, remove or archive the (old) PGP software. You have two options here:
   - Manually delete the entire old PGP folder and all of its contents; or
   - Manually delete the old PGP program and archive the remaining files, especially the configuration and keyring files**.**

NOTE: If you obtain a copy of the patched PGP 2.6.4 version, your old software will be able to read the RSA keys on the new 6.0 keyrings and will not fail when it encounters the new Diffie-Hellman / DSS format keys. You can download this patch from the Network Associates Website.

4. Install PGP Version 6.0 using the provided Installer.
5. Restart your computer.

To upgrade from PGP Version 4.x or 5.x

If you are upgrading from PGP Version 4.x or 5.x, follow the installation instructions outlined in "To install PGP for Windows" on page 14 or "To install PGP for Macintosh" on page 17.

Installing PGP Version 6.0 for Windows 95, 98, and NT

You can install the PGP software from a CD-ROM or from your company file server. The self-extracting file, SETUP.EXE, automatically extracts and steps you through the installation. After you install the software, you can create your private and public key pair and begin using PGP. Refer to the PGPWinUsersGuide.pdf file included with the program for instructions on PGP.

To install PGP for Windows, start your computer and carefully follow the steps outlined below.

To install PGP for Windows

1. Exit all programs currently running on your computer.
2. **To install from a CD-ROM,** insert it into the CD-ROM drive.

   The Setup program automatically starts. If, however, the Setup program does not initiate, double-click SETUP.EXE in the PGP product folder on the CD-ROM.

   To install from your company file server, contact your security officer for information about the server from which to download PGP. Log on to the server.

   Double-click SETUP.EXE in the PGP product folder to start the Setup program.

   The PGP Installation screen appears.
3. Review the instructions in the PGP Welcome dialog box, then click Next.

   The Network Associates license agreement appears.

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

   The Setup program searches for open programs and prompts you to close them.

   If you have PGP version 4.x or 5.x currently installed, the PGP setup program prompts you to uninstall the old PGP files. Click Yes to automatically uninstall the old version.

5. Register your product by entering your name and company name in the User Information dialog box.

6. Click Next.

7. Click Browse to navigate to a destination directory for your PGP files, then click Next.

   The Select Components dialog box appears, as shown in Figure 2-1.

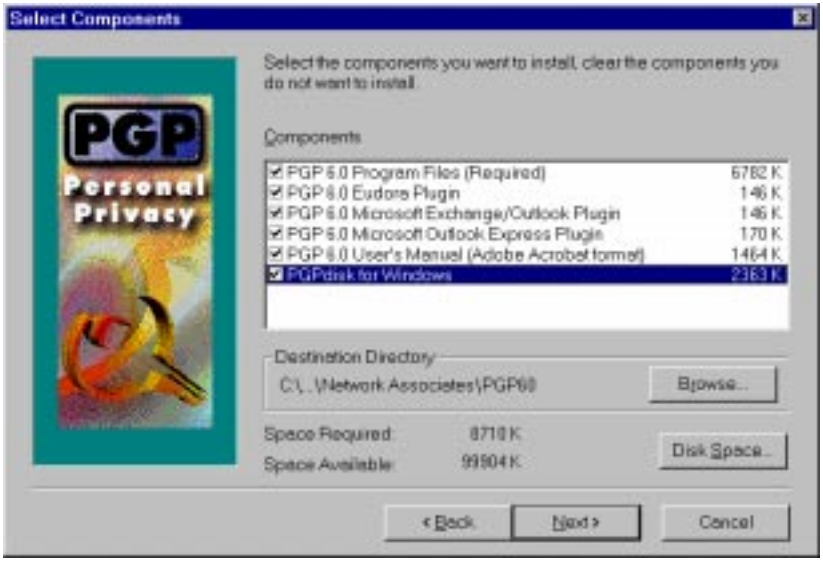

Figure 2-1. PGP for Windows Select Components dialog box

8. Clear the components that you do not want to install. By default, each option is selected. Your installation options are:

   - **PGP 6.0 Program Files (required).** To install the PGP program, this option must be selected.
   - **PGP 6.0 Eudora Plugin.** Select this option if you want to integrate PGP functionality with your Qualcomm Eudora email program. PGP 6.0 supports Eudora versions 3.05 and later.
   - **PGP 6.0 Microsoft Exchange/Outlook Plugin.** Select this option if you want to integrate PGP functionality with your Microsoft Exchange/Outlook email program. PGP 6.0 supports Outlook 97 and 98.
   - **PGP 6.0 Microsoft Outlook Express Plugin.** Select this option if you want to integrate PGP functionality with your Microsoft Outlook Express email program. PGP 6.0 supports the version that is included with Internet Explorer versions 4.01 and later.
   - **PGP 6.0 User's Manual (Adobe Acrobat format).** Select this option to install the PGP User's Guide.
   - **PGPdisk for Windows 95 and NT.** Select this option to install the PGPdisk program. PGPdisk is an easy-to-use encryption application that enables you to set aside an area of disk space for storing your sensitive data.

9. Click Next.

   The Check Setup Information dialog box appears.

10. Review the installation settings, then click Next.

    The PGP files are copied to the computer.

11. If you have keyrings on your computer from a previous version of PGP, click Yes to use your existing keyrings.

    A browse dialog box appears. Browse to locate your public keyring, Pubring.pkr, and your private keyring, Secring.skr.

12. Select "Yes, I want to view the Readme file", then click Finish to complete the installation.

13. To launch PGPkeys immediately after the installation, select "Yes, I want to run PGPkeys."

14. Click Finish to complete the PGP installation.

Installing PGP Version 6.0 for Macintosh

You can install the PGP software from a CD-ROM or from your company file server. The Installer program ( ) automatically extracts and steps you through the installation. After you install the software, you can create your private and public key pair and begin using PGP. Refer to the PGPMacUsersGuide.pdf file included with the program for instructions on using PGP.

To install PGP for Macintosh, carefully follow the steps outlined below.

To install PGP for Macintosh

1. Quit all applications running on your computer.
2. **To install from a CD-ROM,** insert it into the CD-ROM drive.

   To install from your company file server, contact your security officer for information about the server from which to download PGP. Log on to the server.
3. Double-click the installation icon ( ) to start the Installer program.

   The PGP Installation screen appears.
4. Click Continue.

   The Network Associates license agreement appears.
5. Review the license agreement information, then click Accept to continue the installation.

   The PGP Release Notes appear.
6. Review the release notes for known issues and export restrictions, then click Continue.

The installation screen appears, as shown in Figure 2-2.

Figure 2-2. PGP for Macintosh Installation screen

7. Select a type of installation:

   - **Easy Install.** Choose Easy Install to perform a full installation of PGP.
   - **Custom Install.** Choose Custom Install to install PGP with user-definable options. You are prompted to choose the components that you want to install.
   - **Uninstall.** Choose Uninstall to remove all PGP program components from the system.

8. Select a location for your PGP files, then click Install.

   A warning screen appears advising you to close all open applications.

9. Close open applications, then click Continue.

   The PGP files are copied to the computer.

10. Click Restart to reboot the computer.

    The computer restarts. PGP is now installed on the computer.

Index

C

compatibility
  versions of PGP 12
Customer Care
  contacting 7

F

feedback to Network Associates 8

I

installing
  PGP 11
  PGPdisk
    for windows 16

M

Macintosh
  system requirements 11

N

Network Associates
  contacting
    Customer Care 7
  training 8
Network Associates feedback 8

P

PGP
  compatibility 12
  installing 11
  Macintosh 17
  platforms supported 11
  system requirements 11
  upgrading from a previous version 12
  upgrading from Network Associates 12
  upgrading from ViaCrypt 12
  versions of, compatible 12
  Windows 95, 98 & NT 14
PGPdisk
  for Windows 16

R

related
  reading 9

S

setup.exe
  installing PGP 14
system requirements
  for PGP 11

T

Technical 7
technical support
  e-mail address 7
  information needed from user 8
  online 7
training for Network Associates products 8
  scheduling 8

U

upgrading
  from ViaCrypt 12

V

ViaCrypt
  upgrading from 12