

PGP

Installation Guide

COPYRIGHT

Copyright © 1999 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*, Desktop Security Version 6.5.1 for Windows 95, Windows 98, Windows NT, and Macintosh; PGP Certificate Server Version 2.0.1 for Windows NT and Solaris; and PGP Policy Management Agent for SMTP Servers Version 1.0.

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!, NetXRay, 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.

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.

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.

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.

Table of Contents

Chapter 1. Introduction	7
How to contact Network Associates	8
Customer service	8
Technical support	8
Year 2000 compliance	9
Network Associates training	9
Comments and feedback	9
Recommended Readings	10
Chapter 2. Installing PGP Desktop Security	13
System requirements	13
Compatibility with other versions	14
Upgrading from a previous version	14
Installing PGP Desktop Security version 6.5 on Windows systems	16
Installing PGP Desktop Security Version 6.5 for Macintosh	20
Chapter 3. Installing the PGP Certificate Server	23
System Requirements	23
Installing PGP Certificate Server on a Windows NT Server	24
Configuring the Server	26
Installing PGP Certificate Server on a UNIX Server	26
Chapter 4. Installing the PGP Policy Management Agent	31
System requirements	31
Installing the Policy Management Agent for SMTP on a server	32
Index	33

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

- **PGP Desktop Security.** PGP Desktop Security includes email plug-ins, key generation and management tools, and disk utilities that enable users to securely exchange and store data. You can distribute PGP Desktop Security to your users straight from the box, or pre-configure PGP with settings that enforce your security policy:
 - **PGPAdmin Wizard.** The PGPAdmin Wizard generates a client installer, which you distribute to your users. The options you set when creating the installer cannot be changed by the user, and can include permission to generate a personal key pair, key size and type, the path to the default Certificate Server, interaction with a Corporate Signing Key or Additional Decryption Key, designated key revokers, password length and strength, and so on. You can also assign the default values for the PGP Client preference settings.
 - **PGP Client.** The PGP Client is the result of running the PGPAdmin Wizard.
- **PGP Certificate Server.** The PGP Certificate (Cert) Server, also called a “key server”, stores employees’ “digital certificates.” A digital certificate consists of a PGP user’s public key, name and user ID, digital signature, and the digital signatures of others verifying the authenticity of the user’s key. In a typical implementation of PGP, employees in a company store their public keys on the corporate Certificate Server. When any PGP user wants to exchange information with others via email, PGP retrieves the recipients’ keys from the server. Users can also search the Certificate Server for particular keys, which they can then download to their personal keyrings.
- **PGP Policy Management Agent.** The Policy Management Agent for Simple Mail Transfer Protocol (SMTP) works in conjunction with a standard SMTP mail server to ensure that incoming and outgoing email complies to the security policies of a given site. It intercepts email normally bound for the SMTP server and checks to make sure that it conforms with policies configured for your organization. If the email adheres to the policies, it is forwarded to the SMTP server, where it is routed to the intended recipient. If the email does not adhere to the policies specified, a message of your choosing is sent to the sender indicating that the email was rejected.

How to contact Network Associates

Customer service

To order products or obtain product information, contact the Network Associates Customer Care department at (408) 988-3832 or write to the following address:

Network Associates, Inc.
McCandless Towers
3965 Freedom Circle
Santa Clara, CA 95054-1203
U.S.A.

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 (408) 988-3832

Email PGPSupport@pgp.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:

If the automated services do not have the answers you need, contact Network Associates at one of the following numbers Monday through Friday between 6:00 A.M. and 6:00 P.M. Pacific time.

Phone (408) 988-3832

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:

- Product name and version number
- Computer brand and model
- Any additional hardware or peripherals connected to your computer
- Operating system type and version numbers
- Network type and version, if applicable
- 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)
- Specific steps to reproduce the problem

Year 2000 compliance

Information regarding NAI products that are Year 2000 compliant and its Year 2000 standards and testing models may be obtained from NAI's Web site at <http://www.nai.com/y2k>.

For further information, email y2k@nai.com.

Network Associates training

For information about scheduling on-site training for any Network Associates product, call (800) 338-8754.

Comments and feedback

Network Associates appreciates your comments and feedback, but incurs no obligation to you for information you submit. Please address your comments about PGP product documentation to: Network Associates, Inc., 3965 Freedom Circle Santa Clara, CA 95054-1203 U.S.A.. You can also e-mail comments to tns_documentation@nai.com.

Recommended Readings

Non-Technical and beginning technical books

- Whitfield Diffie and Susan Eva Landau, “Privacy on the Line,” *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, but with information that even a lot of experts don't know.
- David Kahn, “The Codebreakers” *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 there is a revised edition published in 1996. 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.
- Charlie Kaufman, Radia Perlman, and Mike Spencer, “Network Security: Private Communication in a Public World,” *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, so it doesn't have many of the latest 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

- Bruce Schneier, “Applied Cryptography: Protocols, Algorithms, and Source Code in C,” *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.
- Alfred J. Menezes, Paul C. van Oorschot, and Scott Vanstone, “Handbook of Applied Cryptography,” *CRC Press*; 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.
- Richard E. Smith, “Internet Cryptography,” *Addison-Wesley Pub Co*; ISBN: 020192480
This book describes how many Internet security protocols. 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.

- William R. Cheswick and Steven M. Bellovin, “Firewalls and Internet Security: Repelling the Wily Hacker” *Addison-Wesley Pub Co*; ISBN: 0201633574

This book is written by two senior researcher at AT&T Bell Labs, about their experiences maintaining and redesigning AT&T's Internet connection. Very readable.

Advanced books

- Neal Koblitz, “A Course in Number Theory and Cryptography” *Springer-Verlag*; ISBN: 0-387-94293-9
An excellent graduate-level mathematics textbook on number theory and cryptography.
- Eli Biham and Adi Shamir, “Differential Cryptanalysis of the Data Encryption Standard,” *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.

This chapter describes how to install PGP Desktop Security for Windows and PGP Desktop Security 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 system, you must have:

- Windows 95, Windows 98, or Windows NT 4.0 (Service Pack 3 or later)

On Windows NT systems, you must have Administrator privileges for the workstation on which you plan to install the program, and you must have logged on to that system correctly.

- 32 MB RAM
- 16 MB Hard Disk Space

If you plan to run PGPnet on the system, you must also have:

- Microsoft TCP/IP
- Compatible LAN/WAN network adapter

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

- Power Macintosh (PowerPC processor required)
- Mac OS 7.6.1 or later
- Open Transport 1.3 or later
- 16 MB RAM
- 10 MB hard disk space

If you plan to run PGPnet on the system, you must also have:

- Compatible LAN/WAN hardware and software (refer to the PGP Read Me file for more information about PGPnet compatible software and hardware)

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
- PGP for Desktop Security or PGP for Personal Privacy Version 6.0.x

. **NOTE:** PGP desktop products that are 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 "pubring.pgp" and your private keys are stored in "secring.pgp". In versions 5.x - 6.0, your public keys are stored in "pubring.pkr" and your private keys are stored in "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 6.5 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 [“Installing PGP Desktop Security version 6.5 on Windows systems”](#) below or [“Installing PGP Desktop Security Version 6.5 for Macintosh”](#) on page 20.

Installing PGP Desktop Security version 6.5 on Windows systems

You can install the PGP Desktop Security 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 using PGP.

To install PGP Desktop Security for Windows 95, Windows 98, and Windows NT systems, carefully follow the steps outlined below.

To install PGP on Windows systems

1. Exit all programs currently running on your computer, then do one of the following:

- **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 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 folder to start the Setup program.

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

If you have PGP version 4.x - 6.x currently installed, the PGP setup program prompts you to uninstall the old PGP files. Click **Yes** to automatically uninstall the old version. Your keyring files are saved in a file named **Old Keyrings**.

You must reboot your computer after uninstalling the files. Once your computer reboots, the installer continues.

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 Whatsnew.txt file appears listing the new features and other important information regarding PGP version 6.5.1.

5. Review the Whatsnew.txt file, then click **Next**.
6. Register your product by entering your name and company name in the User Information dialog box.
7. Click **Next**.
8. Click **Browse** to navigate to a destination directory for your PGP files or accept the default directory. Click **Next** to continue.

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



Figure 2-1. PGP Select Components dialog box

9. Clear the components that you do not want to install. By default, each option is selected. Your installation options are:
 - **PGP Key Management (required)**. This item installs the PGP program. You must install the Key Management utilities.
 - **PGPdisk Volume Security**. 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.

- **PGPnet Virtual Private Networking.** Select this option to install the PGPnet program. PGPnet, a *Virtual Private Network (VPN)*, is an easy-to-use encryption application that allows you to communicate securely and economically with other PGPnet users on your own corporate intranet and with users throughout the world.
- **PGP Eudora Plug-in.** Select this option if you want to integrate PGP functionality with your Qualcomm Eudora email program. PGP version 6.5.1 supports Eudora versions 3.05 and later.
- **PGP Microsoft Exchange/Outlook Plug-in.** Select this option if you want to integrate PGP functionality with your Microsoft Exchange/Outlook email program. PGP version 6.5.1 supports Outlook 97 and 98.
- **PGP Microsoft Outlook Express Plug-in.** Select this option if you want to integrate PGP functionality with your Microsoft Outlook Express email program. PGP version 6.5.1 supports the version that is included with Internet Explorer versions 4.x.
- **PGP CommandLine.** Select this option if you want to install the command line version of PGP for Windows NT and Unix systems.
- **PGP User's Manual (Adobe Acrobat format).** Select this option to install the PGP User's Guide.

10. Click **Next**.

A dialog box appears, alerting you that the installer is ready to copy files.

11. Review the installation settings, then click **Next**.

The PGP files are copied to the computer.

12. If you chose to install the PGPnet application, the **PGPnet Network Adapter List** appears listing the network adapters found on your system, as shown in [Figure 2-2](#).

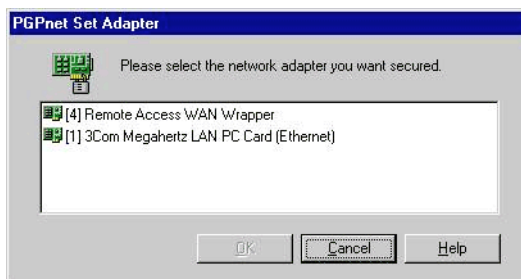


Figure 2-2. PGPnet Network Adapter List

If you want to communicate securely over a modem, select your WAN adapter (for example, Remote Access WAN Wrapper). If you want to communicate securely over an Ethernet connection, select your LAN adapter (for example, 3COM Fast Etherlink). When you have made your selection, click **OK**.

The installation program binds the PGPnet driver to the adapter you selected and configures your computer to use the PGPnet application.

13. 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.


If you do not have keyrings on your computer, click **No**. When you first open the PGPkeys application, you are prompted to create a keypair.

14. If you want to restart your computer automatically, select **Yes, I want to restart my computer now**.
15. Click **Finish** to complete the PGP installation and reboot your computer.

NOTE: You must reboot your computer if you install PGPdisk or PGPnet.


That's it! PGP is installed on your computer.

Installing PGP Desktop Security Version 6.5 for Macintosh

You can install the PGP Desktop Security 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 Desktop Security for Macintosh systems, carefully follow the steps outlined below.

To install PGP on Macintosh systems

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 Network Associates license agreement appears.
4. Review the license agreement information, then click **Accept** to continue the installation.
The PGP Release Notes appear.
5. Review the release notes for known issues and export restrictions, then click **Continue**.

The installation screen appears, as shown in [Figure 2-3](#).

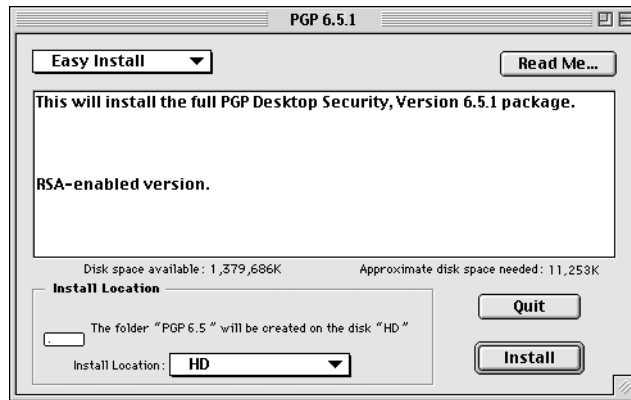


Figure 2-3. PGP Installation screen

6. 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.
7. Your installation options are:
 - **PGPkeys.** This item installs the PGP program. You must install the Key Management utilities.
 - **PGPtools.** Select this option if you want to install the PGTools component. PGTools is a toolbar that allows you to perform PGP functions from within other applications. You can encrypt and sign, decrypt and verify, or securely wipe messages and files directly from PGTools.
 - **PGPdisk Volume Security.** 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.
 - **PGPnet Virtual Private Networking.** Select this option to install the PGPnet program. PGPnet, a *Virtual Private Network (VPN)*, is an easy-to-use encryption application that allows you to communicate securely and economically with other PGPnet users on your own corporate intranet and with users throughout the world.

- **PGPmenu.** Select this option to install the PGPmenu component. PGPmenu allows you to perform most PGP functions from the Finder or from within most applications.
 - **PGPcontextmenu for Mac OS.** Select this option if you want to install the PGPcontextmenu component. The PGPcontextmenu allows you to perform encryption tasks by holding down the CONTROL KEY and clicking on a file or volume in a window or on your desktop. This feature is available on machines running Mac OS 8 or later and is equivalent to launching and using the features within PGPtools.
 - **PGP Qualcomm Eudora Plug-in.** Select this option if you want to integrate PGP functionality with your Qualcomm Eudora email program. PGP version 6.5.1 supports Eudora versions 3.05 and later.
 - **PGP Documentation and Apple Guide.** Select this option to install the PGP User's Guide and Apple Guide help.
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.

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

System Requirements

To install PGP Certificate Server on a Windows NT Server, you must have:

- Windows NT version 4.0 or higher
- 32MB RAM minimum
- 15MB disk space for software
- 10MB to 500MB disk space for the certificate database
- Network interface card
- PGP 6.5.1 (only required for key management)

To run the Configuration/Monitoring wizard, you must have:

- Web server software installed
- Microsoft Internet Explorer 4.x or greater

To install PGP Certificate Server on a UNIX Server, you must have:

- Sun Solaris for SPARC (UNIX) version 2.51 or later (Ultra SPARC recommended, version 2.6 or later required for databases larger than 2 GB)
- 64MB RAM minimum
- 30MB disk space for software
- 10MB to 500MB disk space for the certificate database
- Network interface card

To run the Configuration/Monitoring wizard, you must have:

- Perl version 5.00307 or later
- Web server software. Apache Web server version 1.3.6 software is included with the PGP Certificate Server for UNIX. You are given the opportunity to install the Apache Web server during the PGP Certificate Server installation.

Installing PGP Certificate Server on a Windows NT Server

You can download the Server software from the Network Associates Web site 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. After you install the software, run the Configuration/Monitoring wizard to customize the Server to meet the needs of your site.

To install the PGP Certificate Server on a Windows NT server:

1. Start the Windows NT server.
2. 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 Certificate Server 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 Whatsnew.txt file appears listing the new features and other important information regarding PGP Certificate Server.

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

The **User Information** screen appears.

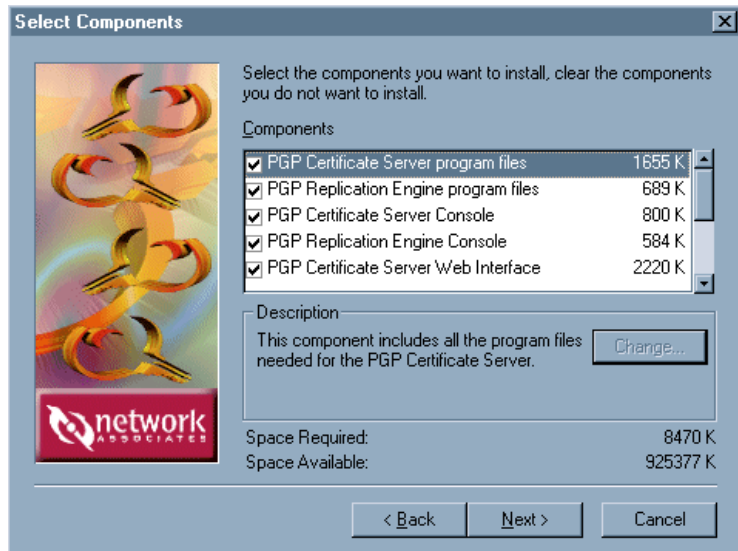
7. Register your product by entering your name and company name, then click **Next**.

A confirmation dialog box appears.

8. Click **Yes** to confirm your user information.

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

The **Select Components** dialog box appears (Figure 3-1).



**Figure 3-1. PGP Certificate Server for Windows NT
Select Components dialog box**

10. Clear the components that you do not want to install. By default, each option is selected. Your installation options are:
 - **PGP Certificate Server Program Files.** To install the PGP Certificate Server program.
 - **PGP Replication Engine Program Files.** Select this option to install the PGP Replication Engine, which allows you to replicate database entries to multiple Servers.
 - **PGP Certificate Server Web Interface.** Select this option if you want to use the PGP Certificate Server Web interface included with this product.
 - **PGP Replication Engine Console.** Select this option to install the PGP Replication Engine Console. The Replication Engine Console allows you to start the Replication Engine and specify options that control how the Replication Engine functions.
 - **PGP Certificate Server User's Manual (Adobe Acrobat format).** Select this option to install the PGP Certificate Server User's Guide.
11. Click **Next**.

The **Check Setup Information** dialog box appears.

12. Review the installation settings, then click **Next**.

The PGP files are copied to the computer.

If setup detects Microsoft's Internet Information Server (IIS) services or another Internet server on your NT machine, a question dialog box appears.

Some IIS files may need to be modified in order to run the Certificate Server's configuration wizard. Click **Yes** if you want setup to modify these files for you.

13. Click **Finish** to complete the PGP Certificate Server installation.

Configuring the Server

When you install the Server, the configuration settings are set to default values which should work for most sites. However, there are a few settings that you may want to modify before starting the Server. For more information, see the PGP Certificate Server Administrator's Guide included with the product.

Installing PGP Certificate Server on a UNIX Server

You can download the Server software from the Network Associates Web site or load the software from a CD-ROM. The file automatically extracts and installs all of the necessary software components in their proper directory locations. After you install the software, run the Configuration/Monitoring wizard to customize the Server to meet the needs of your site.

To install the Certificate Server on a Sun SparcStation

To install the software, you must have root privileges.

1. Insert the PGP CD-ROM into the CD-ROM drive.
2. If this is the first time you are installing the Certificate Server on this system, navigate to the directory where the PGPcertserv_x.x.x_Solaris file is located, and then begin installing the package by issuing the following command:

```
pkgadd -d PGPcertserv_x.x.x_Solaris
```


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

-
- 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.
4. If you do not have a Web server installed on this system, you can use the Web server included with the Certificate Server. Type `Y` to use this Web server.

If you want to configure the Web server already installed on this system to serve the Web Wizard, type `N` and continue with [Step 10](#). Consult the Certificate Server Administrator's Guide for configuration details.

5. Enter the location of the Perl executable on your system.

-
-  **IMPORTANT:** Perl version 5.00307 or greater must be installed to run the Web Configuration Wizard.
-

6. Enter a valid DNS hostname or IP Address for browser access to the Web Wizard.
7. Enter the port number that the Web server should use.
8. Type `Y` if you want the Web server services to start after installation and automatically start after restarting the computer.
9. Type `Y` if you want the Certificate Server to start after installation and automatically start after restarting the computer.
10. Type `Y` to complete the installation and run the post-install script.

-
- NOTE:** The post-install script is executed with super-user permission during the process of installing this package.
-

The installer processes the package and system information, verifies disks space requirements, checks for conflicts with other packages, and then looks for setuid and setgid programs.

The post-install script displays these instructions depending on your installation choices:

- To manually start the Web server, type:

```
/opt/PGPcertd/web/apachectl start
```

- To use the PGP Certificate Server Web Wizard, go to this URL:

```
http://(hostname):(port number)/certserver/
```

- To complete the configuration of the Web Wizard, type:

```
cd /opt/PGPcertd/web/ ; ./install.pl
```

To create administrator accounts for the server, enter administrative logins and passwords when prompted. Leave the Username: prompt blank and press ENTER to complete the Web Wizard accounts.

11. To verify that the product was installed properly, enter the following command:

```
pkginfo -l PGPcertd
```

The status for the selected package should be “Completely Installed.”

To upgrade the Certificate Server on Sun SparcStation

1. Insert the PGP CD-ROM into the CD-ROM drive.
2. If you are upgrading to a new version of the Certificate Server, you may need to modify the Solaris package administration file. Follow these steps.

- a. As root, make a copy of the package administration file:

```
cd /var/sadm/install/admin
```

```
cp default pgp.admin
```

- b. Use a text editor to change the line in the pgp.admin file from:

```
instance=unique
```

```
to:
```

```
instance=ask
```

- c. Change to the directory where the PGPcertserv_x.x.x_Solaris file (where x.x.x is the release number) is located, and install the package by issuing the following command:


```
pkgadd -d PGPcertserv_x.x.x_Solaris
-a /var/sadm/install/admin/pgp.admin
```

Replace `x.x.x` with the release number.


3. Review the license agreement information, then type `Y` to accept the licensing terms.
4. If you do not have a Web server installed on this system, you can use the Web server included with the Certificate Server. Type `Y` to use this Web server.

If you want to configure the Web server already installed on this system to serve the Web Wizard, type `N` and continue with [Step 10](#). Consult the Certificate Server Administrator's Guide for configuration details.

5. Enter the location of the Perl executable on your system.

 **IMPORTANT:** Perl version 5.00307 or greater must be installed to run the Web Configuration Wizard.

6. Enter a valid DNS hostname or IP Address for browser access to the Web Wizard.
7. Enter the port number that the Web server should use.
8. Type `Y` if you want the Web server services to start after installation and automatically start after restarting the computer.
9. Type `Y` if you want the Certificate Server to start after installation and automatically start after restarting the computer.
10. Type `Y` to complete the installation and run the post-install script.

 **NOTE:** The post-install script is executed with super-user permission during the process of installing this package.

The installer processes the package and system information, verifies disks space requirements, checks for conflicts with other packages, and then looks for `setuid` and `setgid` programs.

The post-install script displays these instructions depending on your installation choices:

- To manually start the Web server, type:

```
/opt/PGPcertd/web/apachectl start
```

- To use the PGP Certificate Server Web Wizard, go to this URL:

```
http://(hostname):(port number)/certserver/
```

- To complete the configuration of the Web Wizard, type:

```
cd /opt/PGPcertd/web/ ; ./install.pl
```

To create administrator accounts for the server, enter administrative logins and passwords when prompted. Leave the Username: prompt blank and press ENTER to complete the Web Wizard accounts.

11. To verify that the product was installed properly, enter the following command:

```
pkginfo -l PGPcertd
```

The status for the selected package should be “Completely Installed.”

Installing the PGP Policy Management Agent

4

This chapter describes how to install the PGP Policy Management Agent for SMTP software. Before you begin installing the Policy Management Agent for SMTP, however, be sure to review the system requirements outlined below.

System requirements

To install the Policy Management Agent for SMTP, the system you plan to use as your server must meet the following criteria:

- A Sun SparcStation running Solaris 2.5 or later.
- An SMTP server (such as sendmail).

-
- **NOTE:** If you are running the PGP Policy Management Agent for SMTP on the same machine as the SMTP server, then you need to re-direct the server to listen on an alternative port other than port 25. If your server does not provide this option, then you should consider using another server such as Berkeley Send Mail Version 8.8 which allows you to specify an alternative port.
-

Installing the Policy Management Agent for SMTP on a server

To install the Policy Management Agent for SMTP software, you will need root access.

To install the Policy Management Agent for SMTP in a server:

1. Insert the PGP CD-ROM into the CD-ROM drive.
2. If this is the first time you are installing the Policy Management Agent on this system, change to the directory where the PMA_x.x.x_Solaris file is located, and then begin installing the package by issuing the following command:

```
pkgadd -d PMA_x.x.x_Solaris  
(where x.x.x is the release number)
```

-
- 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.
-

The appropriate package is unpacked and all of the files are placed in their appropriate directories.

The configuration files are stored in the following directory:

```
/opt/PGPpmd/etc
```

The binary executable files are stored in the following directory:

```
/opt/PGPpmd/bin
```

3. Check that the files were extracted properly by entering the following command:

```
pkginfo -l PGPpmd
```

The only thing you need to check here is that the status is “Completely Installed” for the selected package, which indicates that it has been installed properly.

Index

C

- CommandLine [18](#)
- compatibility
 - versions of Desktop Security [14](#)
- Customer Care
 - contacting [8](#)

I

- installing
 - PGP Cert. Server [23](#)
 - PGP Desktop Security [13](#)
 - PGPdisk [17, 21](#)
 - PGPnet [18, 21](#)
 - Policy Management Agent (PMA) [32](#)
- ISO-9660 [27, 32](#)

M

- Macintosh
 - system requirements [13](#)
- Microsoft Outlook Express [18](#)

N

- Network Associates
 - contacting
 - Customer Care [8](#)
 - within the United States [8](#)
 - training [9](#)

P

- PGP Cert. Server
 - configuring the Server [26](#)
 - installing [23](#)
 - pgp.admin file [28](#)
 - removing Server software [26](#)
 - system requirements [23](#)
 - UNIX [26](#)
 - verifying installation [28, 30](#)
 - Windows NT [24](#)
- PGP CommandLine [18](#)
- PGP Desktop Security
 - compatibility [14](#)
 - installing [13](#)
 - Macintosh [16, 20](#)
 - platforms supported [13](#)
 - system requirements [13](#)
 - upgrading from a previous version [14](#)
 - upgrading from Network Associates [14](#)
 - upgrading from ViaCrypt [14](#)
 - versions of Desktop Security, compatible [14](#)
- PGP Eudora [18, 22](#)
- PGP Microsoft Exchange/Outlook [18](#)
- PGPcertserv_x.x.x_Solaris file [28](#)
- PGPdisk
 - for Windows [17, 21](#)
- PGPnet
 - installing [18, 21](#)
- plugins
 - Eudora [18, 22](#)
 - Microsoft Outlook Express [18](#)
 - PGP Microsoft Exchange/Outlook [18](#)
- Policy Management Agent (PMA)
 - installing [32](#)
 - system requirements [31](#)

S

- setup.exe, installing PGP Cert Server [24](#)
- setup.exe, installing PGP Desktop Security [16](#)
- system requirements
 - for Desktop Security [13](#)
 - for the PGPCert Server [23](#)
 - for the Policy Management Agent (PMA) [31](#)

T

- technical support
 - email address [8](#)
 - information needed from user [8](#) to [9](#)
 - online [8](#)
- training for Network Associates products [9](#)
 - scheduling [9](#)

U

- upgrading
 - from ViaCrypt [14](#)

V

- ViaCrypt
 - upgrading from [14](#)
- Virtual Private Networks (VPNs) [18](#), [21](#)