PGP

Installation Guide

LIMITED WARRANTY

<u>Limited Warranty.</u>   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.

<u>Customer Remedies.</u> 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.

<u>Warranty Disclaimer.</u> 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

Introduction

1

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 plugins, 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, Inc.

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. Pacific time.

Phone	(408) 988-3832

Or write to:

Network Associates, Inc.
3965 Freedom Circle
Santa Clara, CA 95054
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:

- 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 **(800) 338-8754**.

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 Desktop Security

2

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 95, 98, or NT system, you must have:

- Windows 95, 98, or NT
- 16 MB RAM
- 15 MB hard disk space for the Client install

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 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 6.0 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 Desktop Security for Windows" below or "To install PGP Desktop Security for Macintosh" on page 19.

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

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 PGP.

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

To install PGP Desktop Security 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_Desktop_Security_6.0.2 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_Desktop_Security_6.0.2 folder to start the Setup program.

   The PGP Desktop Security Installation screen appears.

3. Review the instructions in the PGP Desktop Security 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 Desktop Security 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 Desktop Security User's Guide.

- **Unconfigured PGP 6.0 Client Install.** Select this option if you want to create a customized PGP client installation program that you can distribute to your users.

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

    To review the Readme file immediately after the installation, select "Yes, I want to view the README file."

13. Click Finish to complete the PGP installation.

Installing PGP Desktop Security Version 6.0 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, carefully follow the steps outlined below.

To install PGP Desktop Security 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 Desktop Security 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 Desktop Security 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 Desktop Security for Macintosh
Installation screen**

7. Select a type of installation:

    • **Easy Install.** Choose Easy Install to perform a full installation of
      PGP Desktop Security.

    • **Custom Install.** Choose Custom Install to install PGP Desktop
      Security 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 Desktop Security is now installed on the
    computer.

Installing the PGP Certificate Server

3

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

- Web Server (required to run the Configuration/Monitoring wizard)

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)

- Perl 5 (required for the Configuration/Monitoring wizard)

- 64MB RAM minimum

- 15MB disk space for software

- 10MB to 500MB disk space for the certificate database

- Network interface card

- Web server (required to run the Configuration/Monitoring wizard)

> ☐ **NOTE:** Apache Web server 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.
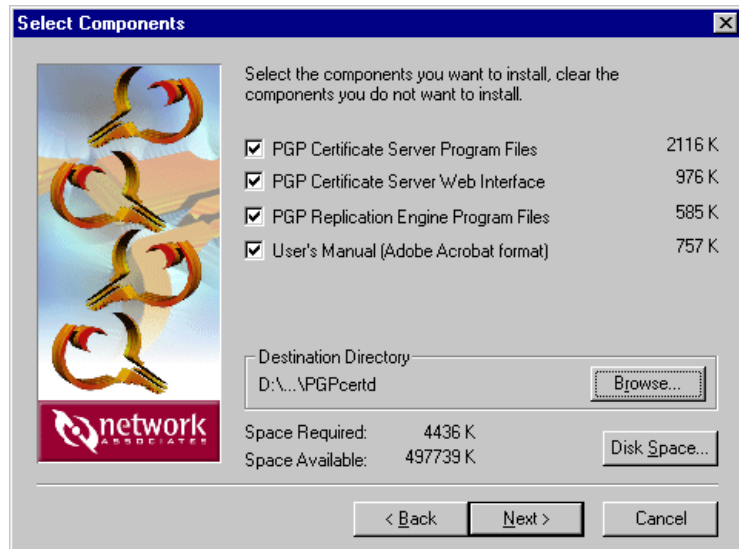
   The User Information screen appears.

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

   A confirmation dialog box appears.

7. Click Yes to confirm your user information.

8. 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 Desktop Security for Windows NT
Select Components dialog box**

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

   • **PGP Certificate Server Program Files.** To install the PGP Certificate Server program, this option must be selected.

   • **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 Program Files.** Select this option to install the PGP Replication Engine, which allows you to replicate database entries to multiple Servers.

   • **PGP Certificate Server User's Manual (Adobe Acrobat format).** Select this option to install the PGP Certificate Server User's Guide.

10. Click Next.

   The Check Setup Information dialog box appears.

11. 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 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.

12. To review the Readme file immediately after the installation, select "Yes, I want to view the README file."

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.

5. Enter the port number that the Web server should use.

    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.

    Once the program files are installed, the `postinstall` script executes.

6. 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.

5. Enter the port number that the Web server should use.

   The program files are installed and then the postinstall script executes.

6. 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/PGPpmad/etc
   ```

   The binary executable files are stored in the following directory:

   ```
   /opt/PGPpmad/bin
   ```

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

   ```
   pkginfo -l PGPpmad
   ```

   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

S

setup.exe, installing PGP Cert Server 22

setup.exe, installing PGP Desktop Security 16

system requirements
>   for Desktop Security 13
>   for the PGPCert Server 21
>   for the Policy Management Agent
>   (PMA) 29

T

Technical 8

technical support
>   e-mail address 8
>   information needed from user 9
>   online 8

training for Network Associates products 9
>   scheduling 9

U

upgrading
>   from ViaCrypt 14

V

ViaCrypt
>   upgrading from 14