PGP Desktop Security

Administrator's Guide

Version 7.0

PGP*, Version 7.0.1

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

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

(972) 308-9960 main
http://www.nai.com

LIMITED WARRANTY

Limited Warranty. Network Associates Inc. warrants that the Software Product will perform substantially in accordance with the accompanying written materials for a period of sixty (60) days from the date of original purchase. To the extent allowed by applicable law, implied warranties on the Software Product, if any, are limited to such sixty (60) day period. Some jurisdictions do not allow limitations on duration of an implied warranty, so the above limitation may not apply to you.

Customer Remedies. Network Associates Inc's and its suppliers' entire liability and your exclusive remedy shall be, at Network Associates Inc's option, either (a) return of the purchase price paid for the license, if any or (b) repair or replacement of the Software Product that does not meet Network Associates Inc's limited warranty and which is returned at your expense to Network Associates Inc. with a copy of your receipt. This limited warranty is void if failure of the Software Product has resulted from accident, abuse, or misapplication. Any repaired or replacement Software Product will be warranted for the remainder of the original warranty period or thirty (30) days, whichever is longer. Outside the United States, neither these remedies nor any product support services offered by Network Associates Inc. are available without proof of purchase from an authorized international source and may not be available from Network Associates Inc. to the extent they subject to restrictions under U.S. export control laws and regulations.

NO OTHER WARRANTIES. TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, AND EXCEPT FOR THE LIMITED WARRANTIES SET FORTH HEREIN, THE SOFTWARE AND DOCUMENTATION ARE PROVIDED "AS IS" AND NETWORK ASSOCIATES, INC. AND ITS SUPPLIERS DISCLAIM ALL OTHER WARRANTIES AND CONDITIONS, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, CONFORMANCE WITH DESCRIPTION, TITLE AND NON-INFRINGEMENT OF THIRD PARTY RIGHTS, AND THE PROVISION OF OR FAILURE TO PROVIDE SUPPORT SERVICES. THIS LIMITED WARRANTY GIVES YOU SPECIFIC LEGAL RIGHTS. YOU MAY HAVE OTHERS, WHICH VARY FROM JURISDICTION TO JURISDICTION.

LIMITATION OF LIABILITY. TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, IN NO EVENT SHALL NETWORK ASSOCIATES, INC. OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, INCIDENTAL, CONSEQUENTIAL, SPECIAL OR EXEMPLARY DAMAGES OR LOST PROFITS WHATSOEVER (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF BUSINESS PROFITS, BUSINESS INTERRUPTION, LOSS OF BUSINESS INFORMATION, OR ANY OTHER PECUNIARY LOSS) ARISING OUT OF THE USE OR INABILITY TO USE THE SOFTWARE PRODUCT OR THE FAILURE TO PROVIDE SUPPORT SERVICES, EVEN IF NETWORK ASSOCIATES, INC. HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. IN ANY CASE, NETWORK ASSOCIATES, INC'S CUMULATIVE AND ENTIRE LIABILITY TO YOU OR ANY OTHER PARTY FOR ANY LOSS OR DAMAGES RESULTING FROM ANY CLAIMS, DEMANDS OR ACTIONS ARISING OUT OF OR RELATING TO THIS AGREEMENT SHALL NOT EXCEED THE PURCHASE PRICE PAID FOR THIS LICENSE. BECAUSE SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OR LIMITATION OF LIABILITY, THE ABOVE LIMITATIONS MAY NOT APPLY TO YOU.

Table of Contents

Preface

PGP is part of your organization's overall security solution for protecting one of your most important assets: *information*. Corporations have traditionally put locks on their doors and require employees to show identification to get into the building. PGP is a valuable tool to help you protect the security and integrity of your organization's data and messages. For many companies, loss of confidentiality means loss of business.

Entire books have been written on the subject of implementing network security. The focus of this guide is on implementing PGP as a tool within your overall network security system. PGP is only one piece of an overall security system, but it is an extremely important one. PGP provides encryption, which protects data from the eyes of anyone for whom it was not intended, even those who can see the encrypted data. This protects information from both internal and external "outsiders."

This guide explains how to administer PGP in an enterprise environment. For information on encryption and cryptographic concepts and terminology, see *An Introduction to Cryptography*.

The PGP product family

The PGP product family is a set of software components designed to protect the security and integrity of an organization's data and messages. You may have purchased some or all of the following components.

- **PGP Desktop Security.** PGP Desktop Security (also referred to in this document simply as PGP) is a security software application that can be installed on individual machines of a network but managed from an administrative machine by a network administrator. PGP provides users with comprehensive email, file, folder, and disk volume security and integrity. PGP includes encryption, digital signing, and key management utilities that provide privacy, integrity, non-repudiation, and authenticity of information, whether the information is stored on a computer or exchanged over networks via PGP's Virtual Private Network feature. Also included is a personal firewall with inbound/outbound packet filtering and six customizable levels of protection, as well as a personal intrusion detection system that detects and blocks common network-based attacks.

- **PGPadmin.** PGPadmin is a software application installed on an administrative machine and used by a network administrator to select which features of PGP to deploy. PGPadmin provides robust corporate manageability features including complete product pre-configuration with optional lockdown capabilities, silent install and remote product re-configuration capabilities. PGPadmin enables the network administrator to control the PGP settings of users on a network by creating a custom PGP client installer program and then distributing it to users.

- **PGP Keyserver.** PGP Keyserver is software installed on one or more machines dedicated to storing users' digital certificates. In a typical corporate PGP implementation, administrators store PGP product settings on the Keyserver for distribution to end users, and employees store their public key certificates and key reconstruction data on the corporate Keyserver. When any PGP user wants to exchange information with others by email, PGP retrieves the recipient's key from the Keyserver. Also, users can search the Keyserver for particular keys that they can download and add to their personal keyrings. Keyserver data can be replicated to other key servers to provide improved performance and fault tolerance.

- **PGP e-Business Server**. PGP e-Business Server software is installed on a network server and used to provide automated strong encryption and authentication services. PGP e-Business Server automates batch processes and secures the transfer of information from one server to another. Confidential data can be shared amongst business partners, customers, and other third parties. Users are provided with a flexible scripting interface for effortless integration into existing or new e-Business processes.

- **Software Developer's Kit.** The SDK is a complete cryptographic toolkit that developers can use to quickly and easily build trusted and peer-reviewed PGP cryptographic capabilities into new or existing applications.

- **Net Tools PKI**. The Net Tools PKI is a full-featured, secure X.509 Certificate Authority that a network administrator can deploy for an enterprise. It stores public key information in a secure LDAP (Lightweight Directory Access Protocol) directory, allowing the administrator to store, issue, revoke, retrieve, and trust X.509 certificates.

Individual usage guides exist for each product. This *PGP Administrator's Guide* describes how to use PGPadmin to deploy and manage PGP Desktop Security within an organization.

Who should read this guide

This guide is for the person(s) who will be implementing and maintaining PGP Desktop Security throughout your organization. We refer to you throughout the PGP documentation set as the “PGP administrator.”

NOTE: If you are new to cryptography and would like an overview of the terminology and concepts you will encounter while using PGP, see *An Introduction to Cryptography*, which is included with the product.

What is PGPadmin?

PGPadmin is a software application that is one component of the PGP product family. PGPadmin is intended for use by a network administrator—the individual (presumably you) responsible for implementing an organization’s network security. You install PGP Desktop Security and then PGPadmin on a Windows or Macintosh machine (the PGP administrative machine). Then, you use PGPadmin as a tool for administering PGP Desktop Security for your organization.

You can use PGPadmin to do the following:

- You can establish the settings you want your PGP Desktop Security users to have, including regular PGP options and PGPadmin-only settings.
- You can create a PGP client installer program that is distributed to users. When they use this program to install PGP, it configures PGP with the settings you established using PGPadmin.
- You can create PGP settings files that your users download from an LDAP server and use to update their PGP configuration. These settings files can be used to change your users’ PGP configuration at any time.

Versions of PGPadmin

PGPadmin is available on both Windows and Macintosh platforms and its functionality is nearly identical on the two platforms. Some pictures in this Guide are of the Windows version and some are of the Macintosh version. Any substantially different functionality is described.

Using this Guide

The chapters and appendices in this Guide include:

- Chapter 1, "Installation," tells you how to install PGPadmin onto your PGP administrative machine.
- Chapter 2, "The Implementation Process," is an overview of the PGP and PGPadmin implementation process.
- Chapter 3, "A Quick Tour of PGPadmin," shows and describes the screens you will see while using the PGPadmin application; it also tells you how to start PGPadmin and how to exit from it.
- Chapter 4, "Setting PGP Options," explains how to set PGP options on your administrative machine.
- Chapter 5, "Setting Administrative Options," tells you about PGPadmin's administrative options and explains how to set them.
- Chapter 6, "Retrieving the Server Configuration," tells you how to retrieve the PGP settings from your LDAP server to use a starting point for PGPadmin.
- Chapter 7, "Creating a Client Installer," tells you how to create the PGP client installer program.
- Chapter 8, "Distributing the PGP Client Installer Program," tells you how to distribute the PGP client installer program to the people in your organization that you want to be using PGP.
- Chapter 9, "Updating PGPadmin Settings," tells you how to post and update your PGP administrative settings on an LDAP server so that your PGP users can easily download and implement the latest version.
- Appendix A, "Setting up a Network Security Policy," is an overview of what a network security policy is and why having one is important.
- Appendix B, "Implementing a PGP Public Key Infrastructure," tells you what a PGP public key infrastructure is and when you want to set one up.
- Appendix C, "Creating a Corporate Signing Key," describes corporate signing keys and when you should use one.
- Appendix D, "Creating Additional Decryption Keys," describes additional decryption keys and when you should use them.
- Appendix E, "Configuring Lotus Domino Servers," tells you how to use the PGP Lotus Domino Server Wizard 7.0 to configure your Domino servers.

- Appendix F, "Network Associates Support Services," describes the support services available for you Network Associates software product.

There is also a Glossary and an Index.

Other documentation included with PGP

The following resources are included in your PGP Desktop Security product package. These resources are available to help you and your users install, configure, and get up to speed on PGP. You have the option of installing these documents on your users' machines:

- The *PGP Installation Guide* tells you how to install PGP. You may wish to provide the Installation Guide to your end-users, or you may wish to provide your own, custom instructions.
- *An Introduction to Cryptography* is for anyone new to the science of cryptography. It is a high-level overview of the terminology, concepts, and processes used by PGP. It includes a chapter on security by PGP's creator, Phil Zimmermann.
- The *PGP User's Guide* tells you how to use PGP's standard features. Targeted at the end-user, it provides basic usage instructions.

How to contact PGP Security and Network Associates

Customer service

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

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

The department's hours of operation are 8:00 a.m. to 8:00 p.m. Central time, Monday through Friday.

Other contact information for corporate-licensed customers:

Phone:	(972) 308-9960
Email:	services_corporate_division@nai.com
Web:	http://support.nai.com/

Other contact information for retail-licensed customers:

Phone:	(972) 308-9960
Email:	cust_care@nai.com
Web:	http://www.pgp.com/

Technical support

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

Web:	http://support.nai.com/

If the automated services do not have the answers you need, contact Network Associates at one of the following numbers Monday through Friday between 8:00 A.M. and 8:00 P.M. Central time to find out about Network Associates technical support plans.

For corporate-licensed customers:

Phone:	(972) 308-9960

For retail-licensed customers:

Phone:	(972) 855-7044

This guide includes a summary of the PrimeSupport plans available to PGP customers. Refer to Appendix F, "Network Associates Support Services," to learn more about plan features and other details.

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

- Program name and version number

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

Download support

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

Corporate customers	(801) 492-2650
Retail customers	(801) 492-2600

Network Associates training

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

Comments and feedback

PGP Security appreciates your comments and reserves the right to use any information you supply in any way it believes appropriate without incurring any obligation whatsoever. Please send any documentation comments to **tns_documentation@nai.com**.

Recommended readings

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

The history of cryptography

- *The Code Book: The Evolution of Secrecy from Ancient Egypt to Quantum Cryptography*, Simon Singh, Doubleday & Company, Inc., September 2000; ISBN: 0385495323. This book is an excellent primer for those wishing to understand how the human need for privacy has manifested itself through cryptography.

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

Technical aspects of cryptography

Web sites

- www.iacr.org—International Association for Cryptologic Research (IACR). The IACR holds cryptographic conferences and publishes journals.

- www.pgpi.org—An international PGP Web site, which is not maintained by PGP Security, Inc. or Network Associates, Inc., is an unofficial yet comprehensive resource for PGP.

- www.nist.gov/aes—The National Institute of Standards and Technology (NIST) Advanced Encryption Standard (AES) Development Effort, perhaps the most interesting project going on in cryptography today.

- www.ietf.org/rfc/rfc2440.txt—The specification for the IETF OpenPGP standard.

Books and periodicals

- *Applied Cryptography: Protocols, Algorithms, and Source Code in C*, 2nd edition, Bruce Schneier, John Wiley & Sons, 1996; ISBN 0-471-12845-7. If you can only buy one book to get started in cryptography, this is the one to buy.

- *Handbook of Applied Cryptography*, Alfred Menezes, Paul van Oorschot and Scott Vanstone, CRC Press, 1996; ISBN 0-8493-8523-7. This is the technical book you should get after Schneier. There is a lot of heavy-duty math in this book, but it is nonetheless usable for those who do not understand the math.

- *Journal of Cryptology*, International Association for Cryptologic Research (IACR). See www.iacr.org.

- *Advances in Cryptology*, conference proceedings of the IACR CRYPTO conferences, published yearly by Springer-Verlag. See www.iacr.org.
- *Cryptography for the Internet*, Philip Zimmermann, Scientific American, October 1998 (introductory tutorial article).
- *The Twofish Encryption Algorithm: A 128-Bit Block Cipher*, Bruce Schneier, et al, John Wiley & Sons, Inc., 1999; ISBN: 0471353817. Contains details about the Twofish cipher ranging from design criteria to cryptanalysis of the algorithm.

Politics of cryptography

Web sites

- www.epic.org—Electronic Privacy Information Center.
- www.crypto.org—Internet Privacy Coalition.
- www.eff.org—Electronic Frontier Foundation.
- www.privacy.org—The Privacy Page. Great information resource about privacy issues.
- www.cdt.org—Center for Democracy and Technology.
- www.pgp.com/phil—Phil Zimmermann's home page, his Senate testimony, and so on.

Books

- *Privacy on the Line: The Politics of Wiretapping and Encryption*, Whitfield Diffie and Susan Landau, The MIT Press, 1998, ISBN 0-262-04167-7. This book is a discussion of the history and policy surrounding cryptography and communications security. It is an excellent read, even for beginners and non-technical people. Includes information that even a lot of experts don't know.
- *Technology and Privacy: The New Landscape*, Philip Agre and Marc Rotenberg, The MIT Press, 1997;ISBN 0-262-01162-x.
- *Building in Big Brother, The Cryptographic Policy Debate*, edited by Lance Hoffman, Springer-Verlag, 1995; ISBN 0-387-94441-9.
- *The Official PGP User's Guide*, Philip Zimmermann, The MIT Press, 1995; ISBN 0-262-74017-6. How to use PGP, written in Phil's own words.

- *The Code Book: The Evolution of Secrecy from Ancient Egypt to Quantum Cryptography*, Simon Singh, Doubleday & Company, Inc., September 2000; ISBN: 0385495323. This book is an excellent primer for those wishing to understand how the human need for privacy has manifested itself through cryptography.

Network security

Books

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

Installation 1

This chapter describes how to install PGPadmin for Windows and Macintosh systems. It also lists the system requirements for each platform.

PGPadmin system requirements

Windows

To install PGPadmin on a Windows system, you must have:

- Pentium 166 or compatible processor
- Windows 95, Windows 98, Windows NT 4.0 (Service Pack 4 or greater), or Windows 2000

  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
- 32 MB hard disk space

Macintosh

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

- Power Macintosh (PowerPC processor **required**)
- Mac OS 8.6.1 or later
- 16 MB RAM
- 10 MB hard disk space

Installing PGPadmin on a Windows system

You can install the PGPadmin 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.

IMPORTANT: You can't install PGPadmin unless PGP Desktop Security is already installed on the administrative machine. See the *PGP Installation Guide* for instructions on installing PGP Desktop Security.

To install PGPadmin on a Windows system:

1. Exit all programs currently running on your computer.
2. Insert the CD-ROM into the CD-ROM drive or download the PGPadmin program files:

   To install from a CD-ROM. Insert the CD-ROM into the CD-ROM drive. The Setup program automatically starts. If the Setup program does not start automatically, double-click **Setup.exe** in the PGP folder.

   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, then double-click **Setup.exe** in the PGP folder.

   The Welcome screen appears.
3. Read the information on the Welcome screen, then click **Next**.

   The License Agreement screen appears.
4. Review the license agreement information, then click **Yes** to accept the licensing terms.

   The Start Copying Files screen appears, informing you that the installer has enough information to begin copying files and showing the current settings.
5. Click **Next**.

   The PGPadmin files are copied onto the computer.

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

NOTE: You don't have to restart your computer to begin using PGPadmin.

Installing PGPadmin on a Macintosh computer

You can install the PGPadmin software from a CD-ROM or from your company file server. The install file automatically extracts and steps you through the installation.

IMPORTANT: You can't install PGPadmin unless PGP Desktop Security is already installed on the administrative machine. See the *PGP Installation Guide* for instructions on installing PGP Desktop Security.

To install PGPadmin on a Macintosh system:

1. Exit all programs currently running on your computer.
2. Insert the CD-ROM into the CD-ROM drive or download the PGPadmin program files:

   To install from a CD-ROM. Insert the CD-ROM into the CD-ROM drive. Double-click on the installer file.

   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, then double-click on the installer file.

   The License screen appears.
3. Review the license agreement information, then click **Accept** to accept the licensing terms.

   The installation screen appears.
4. To specify a location for the installation, click **Install Location** in the lower left corner of the screen, then choose **Select Folder**. Finally, specify which folder you want PGPadmin installed into.
5. Click **Install**.

   The PGPadmin files are installed onto the computer and the Installation Successful screen appears.
6. Click **Quit**.

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

NOTE: You don't have to restart your computer to begin using PGPadmin.

The Implementation Process 2

This chapter guides you through the process of planning your organization's implementation of PGP Desktop Security. It assumes you are the PGP administrator for your organization and that you are doing a corporate rollout of PGP Desktop Security.

Your corporate network

As you begin the process of implementing PGP products, consider the elements of your corporate network. As an example, the figure below shows many elements common to corporate PGP deployments. You may want to sketch a similar diagram for your network, and then use the diagram as you plan how to implement PGP products to provide protection for your network.

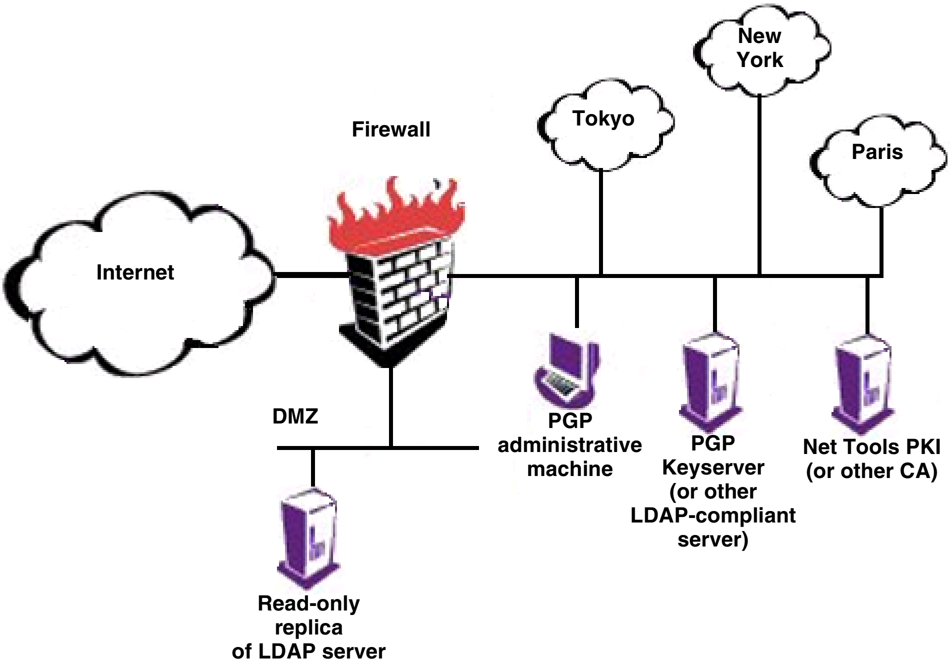

New York
Tokyo
Firewall
Paris
Internet
DMZ
PGP administrative machine
PGP Keyserver (or other LDAP-compliant server)
Net Tools PKI (or other CA)
Read-only replica of LDAP server

Figure 2-1. A simplified corporate network

The components of the corporate network shown in Figure 2-1 include:

- **The Internet.** The system of high-speed transmission lines to which your traveling employees, telecommuters, and business partners connect so that they can access your corporate network.

- **Your corporate firewall.** The boundary that defines a protected portion of your network. A server equipped with firewall software (the firewall server) lets the good guys in but keeps the bad guys out. Any traffic entering or leaving the protected portion of your network must pass through the firewall server first.

- **A DMZ (de-militarized zone).** A well-defined portion of your network that is outside your firewall and available to the Internet. You use the DMZ for services that need to be accessible to people who you don't necessarily want in your corporate network.

- **A read-only replica of your corporate LDAP server in the DMZ.** A directory containing your users' (and potentially business partners') PGP keys and/or X.509 certificates that is easily accessible to your remote employees and business partners—they don't have to go through the firewall to access it.

- **Offices in Tokyo, New York, and Paris.** Extensions of your organization that need to be connected to the corporate network without compromising security.

- **Your PGP administrative machine.** The machine(s) that houses PGP Desktop Security and PGPadmin. From this machine you can control the PGP settings of PGP users worldwide.

- **Your PGP Keyserver or other LDAP-compliant directory server.** The server(s) dedicated to storing your PGP keys and/or X.509 certificates.

- **Your Net Tools PKI or other Certificate Authority.** Your system for handling the company's certificate management requirements.

Implementing PGP in your organization

The following instructions describe the process of installing and implementing PGP in your organization.

1. Determine your PGP security policies.

Establish how you will use PGP in your organization. This involves answering some important questions regarding PGP and your network security policy, which might include:

- **Who needs to use PGP?** Depending on what information you need to protect, you may need to deploy PGP Desktop Security to every employee in your company or only to those with certain titles or within specific departments, such as Human Resources, Finance, or Legal. Perhaps you need to institute a policy that requires every employee to use PGP when communicating on specific matters, or with particular departments, or when creating certain types of information.
- **Do you have different physical office locations to protect?** You can deploy PGP Keyservers at different physical sites and then replicate information from one site to another to provide seamless key updates and retrieval.
- **Do you have remote users?** You can deploy PGPnet to provide remote users with secure, authenticated access to internal networks and protect them from attacks on the Internet with PGP's Personal Firewall and Personal IDS features.
- **Do you have different types of users with a variety of needs?** For example, do you trust your executives to use PGP in an unrestricted fashion because they are your executives, or do you need to hand-hold your executives because they are some of your most naive computer users? (Don't laugh—both types are out there.)

Refer to Appendix A, "Setting up a Network Security Policy," for more information about creating your organization's network security policy.

2. Determine your PGP and key distribution process.

Determine how you will distribute PGP and keys to your users. This is an important step because you may need to increase the security of the systems on which you will install PGP and on which you will generate and distribute keys.

Most corporate environments configure PGP in some way. This enables you to implement and enforce a public-key infrastructure that facilitates key management and to establish security policies that are enforced company-wide.

You have two choices of method for distributing keys to users:

- **Allow users to create their own keys.** If you want to allow users to create their own keys, you can have each user run the PGP Key Generation Wizard constrained by the settings you configured using PGPadmin. This allows you to make sure keys are created in a manner that adheres to your policies. ***We strongly recommend this method.***
- **Create keys yourself.** If you want to create keys for all users in your organization, you must create and distribute the keys to all who need them. Bear in mind, however, that distributing keys to many users takes a long time and is error-prone, the key generation machine is an attractive honeypot for attackers, and that the entire key generation process needs to be treated with extreme care to ensure the integrity of your cryptosystem. Anyone with access to the keys during generation, storage, or delivery to users must be exceedingly trustworthy. You also lose non-repudiation as a feature of your cryptosystem.

  As you might guess from this warning, we recommend *against* using this method.

3. Install PGP and PGPadmin on your PGP administrative machine.

Install PGP and PGPadmin on your PGP administrative machine (or some other secure machine). For detailed installation instructions, refer to the *PGP Installation Guide* and Chapter 1, “Installation.”

4. Install and configure the PGP Keyserver or X.509 PKI.

Your PGP Keyserver (also called a *cert server*) or X.509 PKI stores your company’s digital certificates. Digital certificates are more than just keys; they include identification and authentication information so your users can determine whether a particular key actually belongs to the purported owner.

The computer on which you install your PGP Keyserver or PKI should be physically and electronically secure—that is, in a locked room and behind your organization’s firewall.

For detailed installation instructions, refer to the *PGP Installation Guide*. For complete configuration instructions, refer to the *PGP Keyserver Administrator’s Guide*. For information about your X.509 PKI, refer to its documentation.

5. Create a Corporate Signing Key (if using PGP keys) or X.509 Root CA Certificate.

If you are using PGP keys instead of X.509 certificates, the first key you create should be the Corporate Signing Key. A Corporate Signing Key (usually a split key) is the root key used to authenticate all your users' keys (or to set up trusted introducers who will then authenticate keys).

IMPORTANT: This key identifies your corporation to the outside world and validates all your users to each other and to your business partners. Obviously, this is the most important key in your entire PGP deployment. Maintaining complete control of this key is paramount to preserving the integrity of your PGP environment. We recommend that you generate this key in the presence of at least two of your most highly-trusted employees and immediately split the key into multiple shares. Similarly, when using this key for signing, you should take care to reconstitute this key in the presence of at least two trusted individuals. We also recommend that you create and enforce a disaster recovery policy for secure storage of the key's shares—perhaps offsite in a physically secure location—in the event of a natural disaster (such as an earthquake or fire).

Create a key of the type and size that fits your security requirements. Later, when you are configuring PGPadmin, you will designate this key as the Corporate Signing Key. You will also need to supply the key ID information from this key when you set up your PGP Keyserver.

If you are using X.509 certificates, at this point you must generate your root CA certificate. You will designate this certificate as the root CA certificate later, while configuring PGPadmin.

For detailed instructions, refer to the *PGP User's Guide*.

Refer to Appendix C, "Creating a Corporate Signing Key," for more information about Corporate Signing Keys. For detailed instructions on creating a root CA certificate and importing it into your keyring, refer to your Certificate Authority's documentation and the *PGP User's Guide*.

6. If needed, create Incoming, Outgoing, and PGPdisk Additional Decryption Keys.

Additional Decryption Keys are a means by which you can access information encrypted to/by an employee who is unable or unwilling to recover the information.

Create a key (or keys) of the type and size that fits your security requirements. You will designate these keys as Additional Decryption Keys while configuring PGPadmin.

Refer to Appendix D, "Creating Additional Decryption Keys," for more information about Additional Decryption Keys.

7. If you are installing PGPnet for VPN-based remote access, make sure that your users can authenticate to your VPN gateway.

There are several ways that your users can authenticate to a gateway: using their PGP keypair, their X.509 certificate, or a shared secret password.

If you are using Gauntlet VPN, install an X.509 PKI supported by PGP and Gauntlet VPN (if you have not done so already) so that your users can request and retrieve X.509 certificates. If you are using a VeriSign CA, ensure your users have access to the service so that they can request and retrieve X.509 certificates.

> **NOTE:** To use shared secret passwords, the gateway must include an entry for each user that connects to it, and each of those users must have a static IP address. As a result, using shared secret passwords is only practical in small, controlled installations.

8. Add your VPN gateway and machines to PGPnet's hosts list.

Use PGPnet's Add Host/Gateway Wizard to identify your corporate network. PGPadmin can optionally include these configured hosts in the pre-configured PGP client installer.

For detailed instructions on configuring VPN hosts within PGPnet, refer to the *PGP User's Guide.*

9. Configure your organization's personal firewall and personal IDS policies.

Using PGPadmin, configure the default firewall rules and IDS policies you wish to be enforced in your pre-configured PGP client installer.

For detailed instructions on configuring personal firewall rules and IDS policies, refer to the *PGP User's Guide*.

10. Make selections for your Certificate Authority on the CA panel of the PGP Options screen.

Use the CA panel of the PGP Options screen to establish the URL for your Certificate Authority, specify your CA type, and select your root certificate.

For detailed instructions, refer to the *PGP User's Guide*.

11. Set your PGPnet user preferences.

Use the VPN panels of the PGP Options screen to set PGPnet user preferences.

For detailed instructions, refer to the *PGP User's Guide*.

12. Establish the PGPadmin settings you want to use in the PGP client installer program.

If your security policy requires a specific configuration for your PGP users, you can establish the settings you want in PGPadmin and then create a PGP client installer program configured with those settings.

You must create any Corporate Signing Keys, Additional Decryption Keys, and Designated Revoker Keys before you create the PGP client installer program. You designate each key's functionality in PGPadmin; the keys must be present on your local keyring for you to designate them.

> **NOTE:** To ensure that each user receives these keys, you must add them to the default keyring each user will receive with PGP. This is accomplished on the Keys panel of PGPadmin as described in "The Keys panel" on page 50.

Refer to Appendix C, "Creating a Corporate Signing Key," and Appendix D, "Creating Additional Decryption Keys," for more information about Corporate Signing Keys and Additional Decryption Keys, respectively.

13. Lock down any settings you want to prevent users from changing.

Using the Access Panel within PGPadmin, select the PGP settings you wish to prevent users from changing. These settings will be greyed out in the end-user's instance of PGP, but they can still view the setting's value.

For detailed instructions, refer to Chapter 5, "Setting Administrative Options."

14. Create the PGP client installer program using PGPadmin.

For detailed instructions, refer to Chapter 7, "Creating a Client Installer."

15. Configure your Domino Server if you are using the PGP Lotus Notes email plug-in.

If you are installing the PGP Lotus Notes email plug-in on your Lotus Notes client computers, you need to run the PGP Notes Plug-in Server Utility to configure the Domino server for PGP Lotus Notes plug-in use and configure individual user(s) databases so they can use the PGP Lotus Notes plug-in. Refer to Appendix E, "Configuring Lotus Domino Servers," for detailed instructions.

16. Export your Corporate Signing Key and Additional Decryption Keys to your PGP Keyserver or X.509 PKI.

For detailed instructions, refer to the *PGP User's Guide*.

17. Test your PGP client installer program on a client computer.

Use the PGP client installer program to install PGP on a computer on your corporate network ***other than*** your PGP administrative machine.

Check the installation and the initial settings to make sure that you configured the PGP client installer program appropriately for your organization's needs.

18. Use the PGP Key Generation Wizard to create your own key pair.

As you use the Key Generation Wizard, make sure the key settings you chose in PGPadmin are correct.

For instructions on generating a key, refer to the *PGP User's Guide*.

19. Sign your own key pair with the Corporate Signing Key.

Test your key-signing process. If you are using split keys, determine how you will reconstitute the key to sign all of your users' keys.

20. Export your own public key to your PGP Keyserver.

For detailed instructions on exporting your key, refer to the *PGP User's Guide*.

21. Distribute the PGP client installer program to your users.

Distribute the PGP client installer program to users either by using an enterprise software distribution method (SMS or Tivoli, for example), by posting it on a Web/file server, or by creating and distributing CD-ROMs.

For PGP installation instructions, refer to the *PGP Installation Guide.*

IMPORTANT: You might want to consider creating a quick reference install document for your users.

A Quick Tour of PGPadmin 3

This chapter shows and describes the screens you will see while using PGPadmin. It also tells you how to start PGPadmin and exit from it.

Starting PGPadmin

Use the appropriate procedure to start PGPadmin on your Windows or Macintosh computer.

To start PGPadmin on a Windows computer:

1. Click **Start —> Programs —> P G P —> PGPadmin**.

   The PGPadmin screen appears.

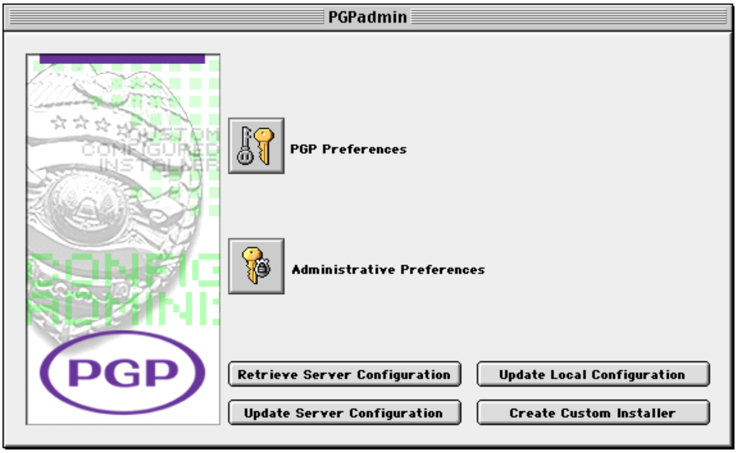
To start PGPadmin on a Macintosh computer:

1. Navigate to the PGP folder and open it.
2. Double click the PGPadmin icon.

   The PGPadmin screen appears.

The PGPadmin screen

The PGPadmin screen provides access to all of PGPadmin's functions.


PGPadmin
CUSTOM CONFIGURED INSTALLER
CONFIG ADMIN
PGP
PGP Preferences
Administrative Preferences
Retrieve Server Configuration
Update Local Configuration
Update Server Configuration
Create Custom Installer

NOTE: The PGPadmin screen on Windows does ***not*** have the **Update Local Configuration** button. The equivalent functionality is provided on Administrative Options screens in the form of an **Apply** button. Also, the Windows version of PGPadmin uses the term "options," while the Macintosh version uses the term "preferences."

The buttons on the PGPadmin screen are:

- **PGP Options** (Windows) or **PGP Preferences** (Macintosh). This button displays the PGP Options/Preferences screen, which you use to configure the PGP options that you want your users to use. These settings are part of the PGP client installer program.

  For more information about this screen, refer to Chapter 4, "Setting PGP Options."

- **Administrative Options** (Windows) or **Administrative Preferences** (Macintosh). This button displays the Administrative Options/Preferences screen, which you use to configure PGPadmin's options.

  For more information about this screen, refer to Chapter 5, "Setting Administrative Options."

- **Retrieve Server Configuration**. This button retrieves the PGP settings file from your LDAP server and brings them into PGPadmin, so that you are starting with the current PGP settings your users have rather than the settings of the version of PGP on the PGP administrative machine (which may or may not be the same settings your users have).

NOTE: You must specify the URL of the LDAP server you want to use ***before*** you can retrieve the settings file from it. To do this, go to Administrative Options/Preferences and select the Updates panel.

- **Update Server Configuration**. This button saves a new settings file to your LDAP server so that your users can download it.

NOTE: You must specify the URL of the LDAP server you want to use ***before*** you can save the settings file to it. To do this, go to Administrative Options/Preferences and select the Updates panel.

For more information about this button, refer to Chapter 9, "Updating PGPadmin Settings."

- **Create Custom Installer**. This button begins the process of creating the PGP client installer program.

  For more information about this button, refer to Chapter 7, "Creating a Client Installer."

- **Update Local Configuration** (Macintosh only). This button saves the changes you have made in PGPadmin to the version of PGP on the PGP administrative machine.

  For more information about this button, refer to Chapter 7, "Creating a Client Installer."

Exiting from PGPadmin

To exit from PGPadmin:

- On Windows, click the **Close** button (the **x** in the upper right corner) on the PGPadmin screen.
- On a Macintosh, pull down the **File** menu and select **Quit**.

Setting PGP Options 4

This chapter explains how to set the PGP options (called preferences on the Macintosh) on your PGP administrative machine so that they will be used when you create the PGP client installer program.

Why do you set PGP options in PGPadmin?

The PGP options that you establish on your PGP administrative machine will be the ones the PGP client installer program implements for each of your PGP users.

IMPORTANT: You must establish the PGP options you want on your PGP administrative machine ***before*** you create the PGP client installer program.

These PGP options are the exact same options that all PGP users have, but there are two important differences when you are setting them on your PGP administrative machine:

- The PGP options you set on your PGP administrative machine affect all of your PGP clients.
- The PGP options you set on your PGP administrative machine can be "locked down" using the PGP *administrative* options, meaning that you can prevent the PGP clients from modifying these options after they've installed PGP on their own computer.

  Refer to Chapter 5, "Setting Administrative Options," for more information about locking down PGP options for your users.

How do you set PGP options in PGPadmin?

To set PGP options for your PGP clients, perform the following procedure.

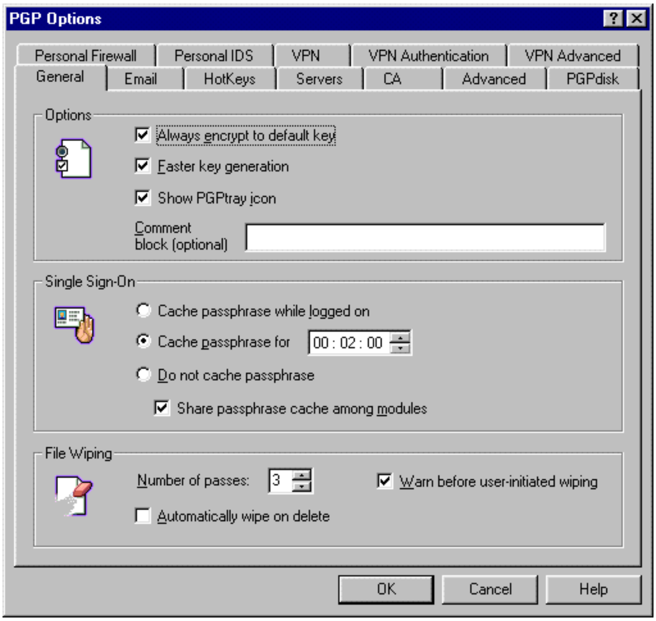
To set PGP options/preferences:

1. Open PGPadmin.

   The PGPadmin screen appears.

2. Click **PGP Options** (**PGP Preferences** on the Macintosh).

   The PGP Options screen appears.



Options

☑ Always encrypt to default key

☑ Faster key generation

☑ Show PGPtray icon

Comment block (optional)

Single Sign-On

○ Cache passphrase while logged on

● Cache passphrase for 00 : 02 : 00

○ Do not cache passphrase

☑ Share passphrase cache among modules

File Wiping

Number of passes: 3

☑ Warn before user-initiated wiping

□ Automatically wipe on delete

3. Configure the PGP options for your PGP users.

   Refer to the *PGP User's Guide* or online help for a complete description of all PGP options.

4. When you are done, click **OK**.

   The PGPadmin screen appears.

Setting Administrative Options 5

This chapter tells you about the PGP administrative options (called administrative preferences on the Macintosh), available only through PGPadmin, and explains how to set them.

What are PGPadmin administrative options?

The PGPadmin administrative options let you establish a wide variety of settings that control how PGP will run on your users' machines.

For example, you can force your users to use passphrases of a specific length or level of quality, you can specify that they create key pairs of a specific size, you can specify that they update their settings at certain intervals, and you can also control what PGP options they can't change on their machines.

How do you set PGPadmin administrative options?

All of PGPadmin's administrative options are accessed from the Administrative Options/Preferences screen.

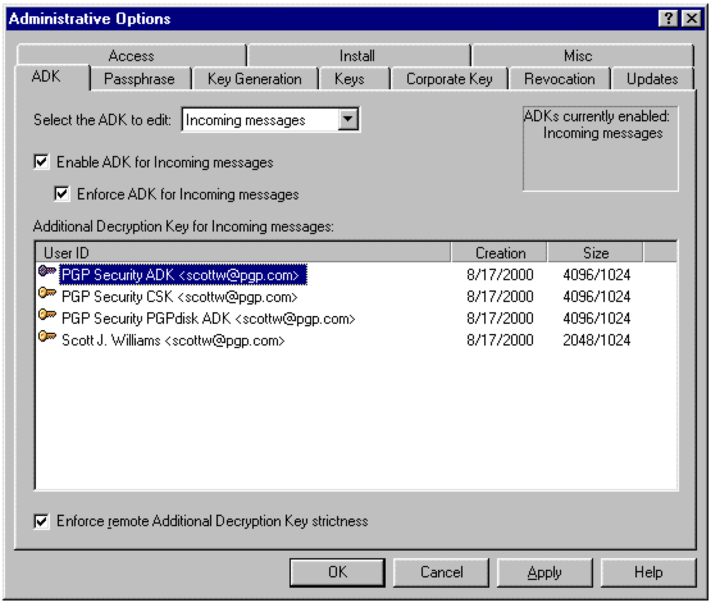
To display the Administrative Options/Preferences screen:

1. Open PGPadmin.

   The PGPadmin screen appears.

2. Click **Administrative Options** (**Administrative Preferences** on the Macintosh).

The Administrative Options/Preferences screen appears.



Select the ADK to edit: Incoming messages

ADKs currently enabled:
Incoming messages

☑ Enable ADK for Incoming messages

☑ Enforce ADK for Incoming messages

Additional Decryption Key for Incoming messages:

User ID	Creation	Size
PGP Security ADK <scottw@pgp.com>	8/17/2000	4096/1024
PGP Security CSK <scottw@pgp.com>	8/17/2000	4096/1024
PGP Security PGPdisk ADK <scottw@pgp.com>	8/17/2000	4096/1024
Scott J. Williams <scottw@pgp.com>	8/17/2000	2048/1024

☑ Enforce remote Additional Decryption Key strictness

3. Configure the administrative options on each of the panels to suit your requirements.

NOTE: Clicking the **Apply** button lets you apply the settings that you establish in PGPadmin to the version of PGP on the PGP administrative machine. This is useful if you want to test the settings you have established or you just want to run PGP with the same settings your users will have. The **Apply** button is not present on the Macintosh; to do the same thing, use the **Update Local Configuration** button on the PGPadmin screen.

4. When you are done, click **OK**.

   The PGPadmin screen appears again.

Complete information about each option on the panels of the Administrative Options/Preferences screen is available in the following sections.

Panels of the Administrative Options screen

Each panel of the Administrative Options screen is shown and described in the following sections.

The ADK panel

An Additional Decryption Key (ADK) is a powerful tool that allows an organization to decrypt messages that are encrypted to someone within the organization. This is accomplished by noting an ADK within the user's public key.

With this association, any message encrypted to the user's public key is also encrypted to the ADK. This allows the owner of the ADK to decrypt any message sent to the user.

Splitting ADKs

An ADK should always be split and the shares distributed among multiple highly trustworthy administrators. If the ADK is ever compromised, all encrypted messages sent to users with this feature enabled can be decrypted by the attacker. In light of this possibility, take great care when deciding whether to use an ADK. If used, the ADK must be secured both physically and electronically in order to prevent misuse.

IMPORTANT: We highly recommend splitting your ADK between multiple system administrators and requiring a reasonable threshold of administrators to reconstitute the key. This provides a highly secure model for data recovery. Using split ADKs also minimizes the risk of rogue administrators recovering data surreptitiously (because it forces collusion across multiple trusted administrators to recover data), and thus allows you to minimize the potential risks associated with using ADKs.

Specifying ADKs

For Diffie-Hellman and RSA keys, the Incoming ADK feature works by designating an ADK inside each user's public key. This means that the ADK request travels with the user's public key to anyone inside or outside the organization.

When someone inside or outside the organization encrypts a message to the user, the associated ADK is added to the sender's list of recipients automatically, at which time the sender is (by default) warned that this is taking place.

IMPORTANT: RSA Legacy keys *cannot* be used as the Incoming ADK.

If your organization uses PGPdisk, you may configure PGP to automatically add an ADK to all new PGPdisks created by the client. This allows the owner of the ADK to recover data from PGPdisks in an emergency. As with any ADK, the security of the ADK private key is critical; it must be kept very secure.

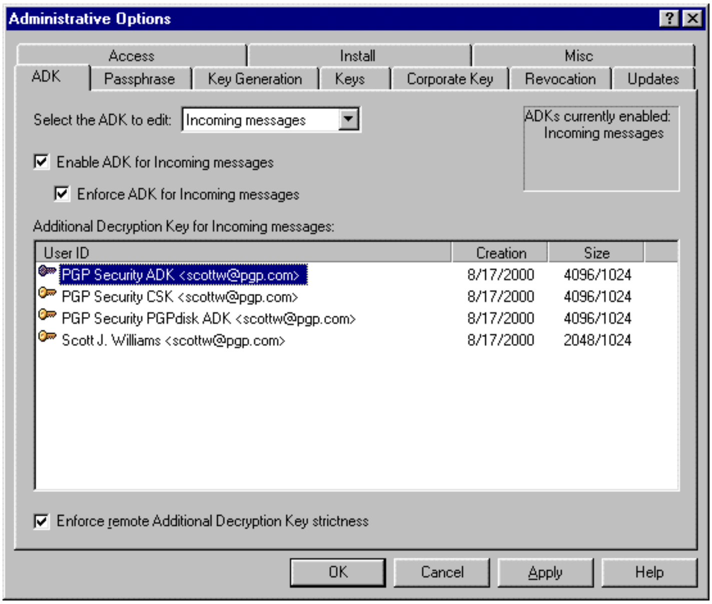
If you enable an ADK in your organization, it causes the ADK to appear in the recipient list when [a] someone encrypts data to a user in your organization, and/or [b] an internal user encrypts data. This is dependent on whether you have enabled Incoming or Outgoing ADK, or both.

Enforcing ADK use

As with any key in the recipient list, the ADK(s) can be removed from the list by the user before encrypting the data. If a mischievous user chooses to do this, you will not be able to decrypt the data using the associated ADK.

If you wish to prevent users from removing the ADK(s) from the recipient list, you must select the option of enforcing ADK use.

You should also decide whether or not to enforce the ADK policies of outside organizations. When an internal user encrypts to a user in another organization whose key was generated with an enforced Outgoing ADK, you have the option of either forcing your users to respect the enforcement requested by outside organizations or allowing your users to remove any ADK(s) associated with that key from the recipient list.



Select the ADK to edit: Incoming messages

ADKs currently enabled:
Incoming messages

☑ Enable ADK for Incoming messages

☑ Enforce ADK for Incoming messages

Additional Decryption Key for Incoming messages:

User ID	Creation	Size
PGP Security ADK <scottw@pgp.com>	8/17/2000	4096/1024
PGP Security CSK <scottw@pgp.com>	8/17/2000	4096/1024
PGP Security PGPdisk ADK <scottw@pgp.com>	8/17/2000	4096/1024
Scott J. Williams <scottw@pgp.com>	8/17/2000	2048/1024

☑ Enforce remote Additional Decryption Key strictness

If you choose to use an ADK, the key must already be on your keyring so that you can select it.

The fields on the ADK panel are:

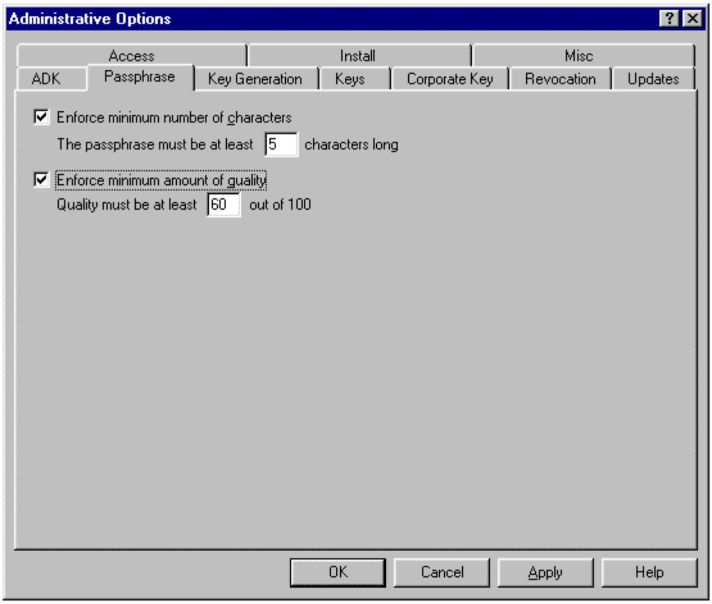
- **Select the ADK to edit**. Lets you select the type of Additional Decryption Key you are configuring. Select **Incoming Messages**, **Outgoing Messages**, or **PGPdisk**. The fields on the screen are slightly different for the different types of ADKs.
- **Enable ADK for Incoming/Outgoing/PGPdisk messages**. Check if you want to use an Incoming, Outgoing, or PGPdisk ADK.
- **Enforce ADK for Incoming messages**. Check if you want to prevent your users from removing the ADK(s) from the recipient list.
- **ADKs currently enabled**. Lists the ADKs that are currently enabled.
- **Additional Decryption Key for Incoming messages**. Lists the keys on the keyring on your PGP administrative machine. If you want to specify an ADK, the ADK key must be on the keyring so that it can be selected here.
- **Enforce remote Additional Decryption Key strictness**. Check if you want to force your users to respect the ADK enforcement requested by outside organizations. If left unchecked, your users will be able to remove any ADK(s) associated with that key from the recipient list.

The Passphrase panel

To make PGP more secure, it is helpful to minimize the security risks associated with a user's passphrase. Longer passphrases are generally harder to break. You have the option of forcing users to use a minimum passphrase length.

Some passphrases are better than others. This is a measure of the quality of a given passphrase. The passphrase is potentially the weakest link of PGP security, so it is important for users to have high-quality passphrases in order to make PGP effective.

When the user creates a key or changes their passphrase on a key, a quality bar will show the quality of the new passphrase. The quality of a passphrase is usually higher when there is a mixture of lower- and upper-case letters, numbers, and punctuation.



Administrative Options

☑ Enforce minimum number of characters

The passphrase must be at least 5 characters long

☑ Enforce minimum amount of quality

Quality must be at least 60 out of 100

The fields on the Passphrase panel are:

- **Enforce minimum number of characters**. Check if you want to require your users to enter a minimum number of characters for their passphrase. If you check this box, you must specify a minimum number of characters below.

- **The passphrase must be at least X characters long**. Specify a minimum number of characters for your users’ passphrases.

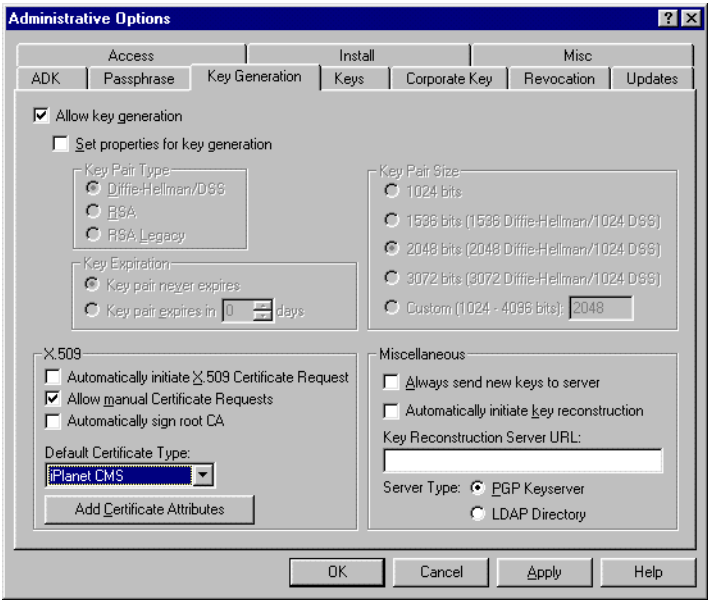
- **Enforce minimum amount of quality**. Check if you want to require your users to create a passphrase with at least a certain level of quality. If you check this box, you must specify a quality level below.
- **Quality must be at least X out of 100**. Specify the minimum level of quality for your users' passphrases.

The Key Generation panel

Normally, PGP users generate their own keys. This allows each user to choose their own passphrase and be responsible for their own keys.

You may optionally choose to disable key generation for your users. This means that someone in your organization will be responsible for generating keys for your users and handing them out. In a large organization, this sort of operation could take a long time to complete and requires extensive processes to ensure security of the key.

Disabling key generation is strongly discouraged because centralized key generation can pose risks as described in the section "Implementing PGP in your organization" on page 27. This feature should only be used if all the threats and implications of doing this have been carefully considered.



☑ Allow key generation

□ Set properties for key generation

Key Pair Type
● Diffie-Hellman/DSS
○ RSA
○ RSA Legacy

Key Expiration
● Key pair never expires
○ Key pair expires in 0 days

Key Pair Size
○ 1024 bits
○ 1536 bits (1536 Diffie-Hellman/1024 DSS)
● 2048 bits (2048 Diffie-Hellman/1024 DSS)
○ 3072 bits (3072 Diffie-Hellman/1024 DSS)
○ Custom (1024 - 4096 bits): 2048

X.509
□ Automatically initiate X.509 Certificate Request
☑ Allow manual Certificate Requests
□ Automatically sign root CA
Default Certificate Type: iPlanet CMS
Add Certificate Attributes

Miscellaneous
□ Always send new keys to server
□ Automatically initiate key reconstruction
Key Reconstruction Server URL:
Server Type: ● PGP Keyserver
○ LDAP Directory

The fields on the Key Generation panel are:

- **Allow key generation**. Check if you want your users to be able to generate their own keys.

- **Set properties for key generation**. Check if you want to establish the properties for the keys your users generate. Then, select the desired key pair type, key expiration, and key pair size. Note that your users will not be able to change the properties you establish.

- **Key Pair Type**. Select **Diffie-Hellman/DSS**, **RSA**, or **RSA Legacy**. Choose **Diffie-Hellman/DSS** if you want to take advantage of many PGP key features, including Additional Decryption Key (ADK), designated revoker, multiple encryption subkeys and photo ID.

  Choose **RSA** or **RSA Legacy** if you plan to correspond with people who are using RSA keys. The RSA key format supports PGP's ADK, designated revoker, multiple encryption subkeys and photo ID features. Previously these features were only available to users with Diffie-Hellman keys. PGP will continue to support users who have RSA keys in the older key format (now called RSA Legacy). The RSA key type is only fully compatible with PGP Version 7.0 and above and other open PGP applications. You may also wish to use RSA keys if you plan to use a VPN with X.509 certificates, as most VPN gateways only support RSA-based X.509 certificates.

  Choose the RSA Legacy key format only if those you communicate with are using older versions of PGP; otherwise choose the new RSA key format. RSA Legacy keys do not support many of the PGP key features.

- **Key Expiration**. Select when you want your users' keys to expire: Never or the number of days after key generation that you specify.

- **Key Pair Size**. Select the size you want your users' key pairs to be. For Diffie-Hellman/DSS and RSA keys, select **1024**, **1536**, **2048**, **3072**, or a **Custom** size. For RSA Legacy keys, select **1024**, **1536**, **2048**, or a **Custom** size.

- **X.509**. Make the selections you want for your users. Refer to the *PGP User's Guide* for more information about X.509 certificates.

  Automatically initiate X.509 Certificate Request. Check if you want your users to automatically initiate a request for an X.509 certificate from a Certificate Authority so that they can add it to their keypair.

  Allow manual Certificate Requests. Check if you want your users to be able to manually initiate requests for X.509 certificates.

  Automatically sign root CA. Check if you want your users to automatically sign your root CA when they generate a key.

Default Certificate Type. Select the type of Certificate Authority your users will be using: **None**, **Net Tools PKI**, **VeriSign OnSite**, **Entrust**, **iPlanet CMS**, or **Windows 2000**.

Add Certificate Attributes. Click this button and add, modify, or remove attributes for the CA type you selected as your default certificate type.

- **Miscellaneous**. Make the selections you want for your users.

  Always send new keys to server. Check if you want your users to always send new keys to your PGP Keyserver.

  Automatically initiate key reconstruction. Check if you want your users to automatically initiate reconstruction of keys they have lost.

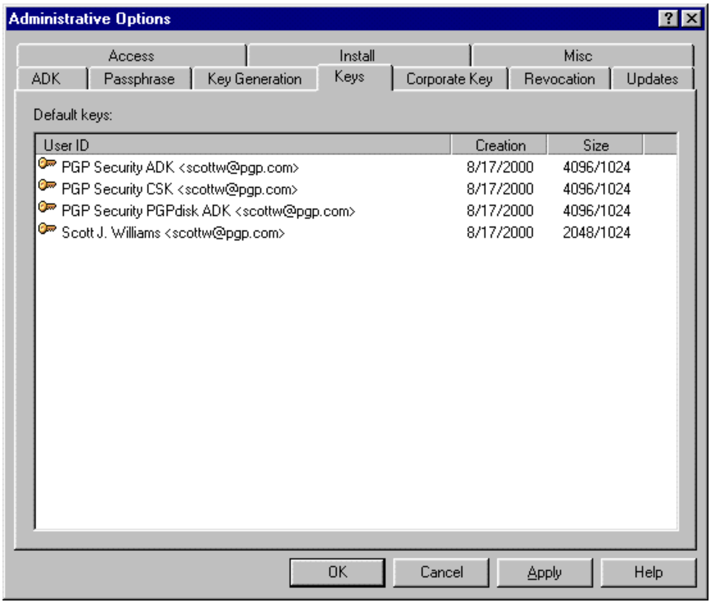
  Key Reconstruction Server URL. Enter the URL to the key reconstruction server you want your users to use. We recommend using LDAPS as the protocol, as it is strongly encrypted and authenticated.

  Server Type. Select the type of key reconstruction server whose URL you specified above: **PGP Keyserver** or **LDAP Directory**.

The Keys panel

You may choose one or more keys (from the keys on your PGP administrative machine's keyring) to appear on all of your users' keyrings when they install PGP. You should make sure to include your Corporate Signing Key, Root CA certificate, ADKs, Designated Revoker key, the keys of all your trusted introducers, and any other keys you wish to distribute to all PGP users in your environment.

NOTE: This panel is called "Default Keys" on the Macintosh.



Default keys:

User ID	Creation	Size
PGP Security ADK <scottw@pgp.com>	8/17/2000	4096/1024
PGP Security CSK <scottw@pgp.com>	8/17/2000	4096/1024
PGP Security PGPdisk ADK <scottw@pgp.com>	8/17/2000	4096/1024
Scott J. Williams <scottw@pgp.com>	8/17/2000	2048/1024

The fields on the Keys panel are:

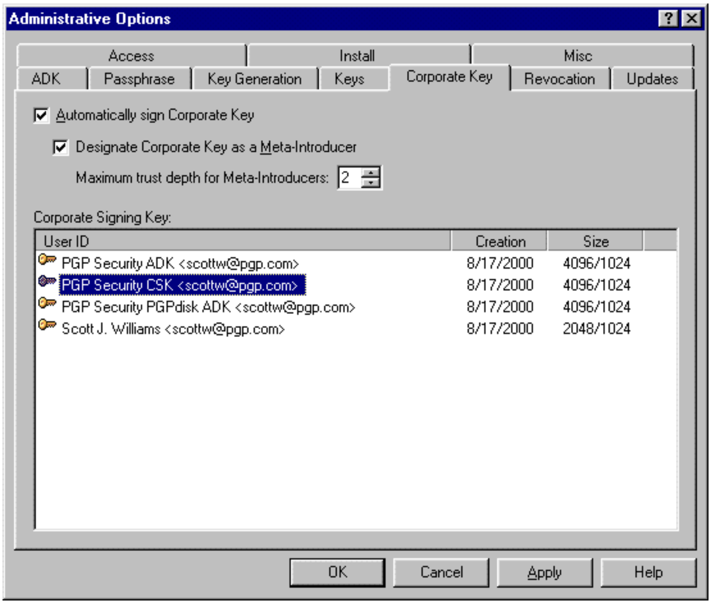
- **Default keys**. Lists all of the keys on the keyring of your PGP administrative machine.

The Corporate Key panel

A Corporate Signing Key (CSK) is a system-wide public key that establishes the validity of other keys in your organization. Key generation by your users can be configured to automatically sign the CSK, making it valid and trusted so that any other keys signed by the CSK will be considered valid by the user's installation of PGP.

The signature made by the user on the CSK can optionally designate the CSK as a Meta-Introducer. This means that keys designated by the CSK as Trusted Introducers would be automatically trusted as introducers by the user.

You can also display a warning to the user when encrypting to a key not signed by the CSK. This is generally made obvious regardless from the PGP interface, but can be useful in high security situations.



☑ Automatically sign Corporate Key

☑ Designate Corporate Key as a Meta-Introducer

Maximum trust depth for Meta-Introducers: 2

Corporate Signing Key:

User ID	Creation	Size
PGP Security ADK <scottw@pgp.com>	8/17/2000	4096/1024
PGP Security CSK <scottw@pgp.com>	8/17/2000	4096/1024
PGP Security PGPdisk ADK <scottw@pgp.com>	8/17/2000	4096/1024
Scott J. Williams <scottw@pgp.com>	8/17/2000	2048/1024

The fields on the Corporate Key panel are:

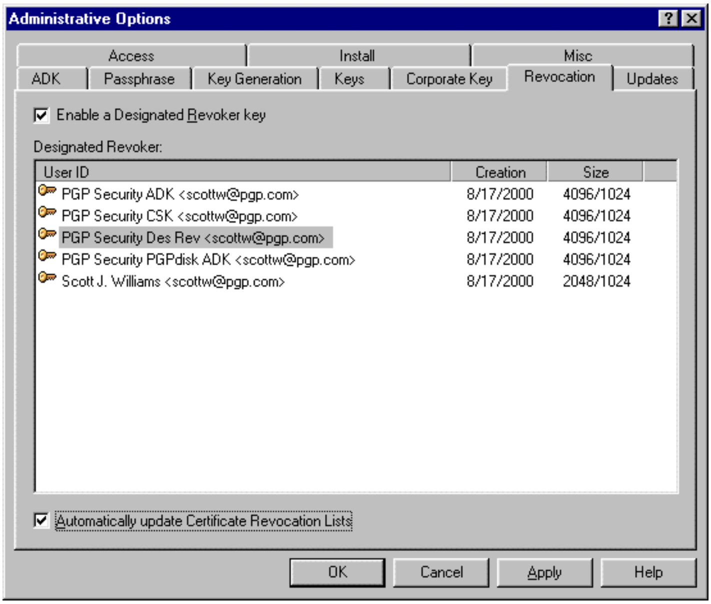
- **Automatically sign Corporate Key**. Check if you want your users to automatically sign the corporate key when they generate keys.
- **Designate Corporate Key as a Meta-Introducer**. Check if you want the CSK to automatically be designated as a meta-introducer.

- **Maximum trust depth for Meta-Introducers**. Specify how many trust levels you want the meta-introducer power to be carried. For more information about trust and meta-introducers, refer to *An Introduction to Cryptography*.
- **Corporate Signing Key**. Lists all of the keys on the keyring of your PGP administrative machine so that you can select the Corporate Signing Key.

The Revocation panel

One problem that can occur is the loss of a user's private key. If you are not using PGP's Key Reconstruction feature and a user loses his/her private key, there is no way the user can ever gain access to his/her encrypted messages again. More importantly, other users will continue to encrypt to the public key because there's no way to revoke it when the private key is lost, and there's no way to tell other users that the key is lost, short of sending each user a message.

To avoid this problem, you can select a key to be the Designated Revoker. This key will be able to revoke any key generated by the user under this installation. If any user loses their key or the key is otherwise compromised, you can revoke it using the Designated Revoker key, and have the user generate a new key. Since this key will be able to revoke any key in your organization, it must be kept very secure from theft, and it should have a strong passphrase.



☑ Enable a Designated Revoker key

Designated Revoker:

User ID	Creation	Size
PGP Security ADK <scottw@pgp.com>	8/17/2000	4096/1024
PGP Security CSK <scottw@pgp.com>	8/17/2000	4096/1024
PGP Security Des Rev <scottw@pgp.com>	8/17/2000	4096/1024
PGP Security PGPdisk ADK <scottw@pgp.com>	8/17/2000	4096/1024
Scott J. Williams <scottw@pgp.com>	8/17/2000	2048/1024

☑ Automatically update Certificate Revocation Lists

This key must be on the default keyring so PGP on users' desktops will not encrypt to revoked keys.

The fields on the Revocation panel are:

- **Enable a Designated Revoker key**. Check if you want to have a designated revoker key.
- **Designated Revoker**. Lists all of the keys on the keyring of your PGP administrative machine so that you can select the Designated Revoker Key.
- **Automatically update Certificate Revocation Lists**. Check if you want your users to automatically update certificate revocation lists from your certificate server.

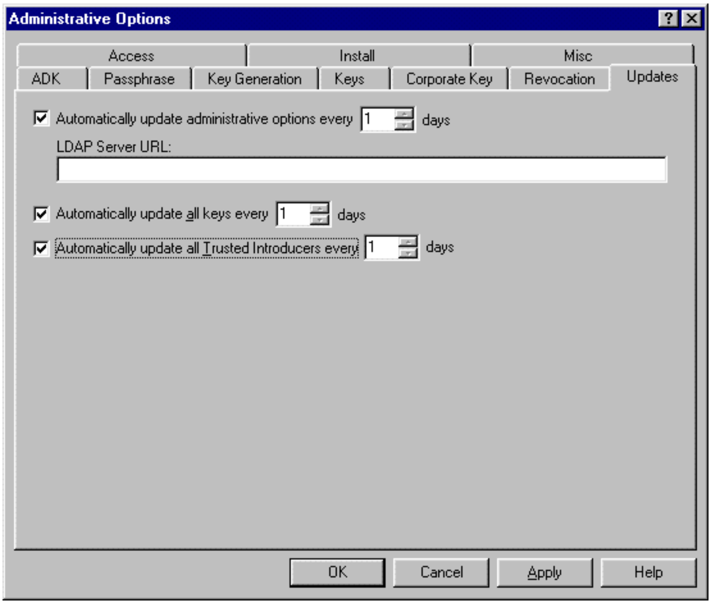
The Updates panel

The settings you establish for your users when you create the PGP client install program may very well change over time (for example, Personal Firewall settings, VPN gateway settings, and so on). So that you don't have to create a new client installer every time this happens, you can have your users automatically update the latest administrative options from your corporate LDAP server.

NOTE: This panel is called the "Automatic Updates" panel on the Macintosh.

Keys can also change over time. Their owners may add or delete user IDs, and signatures may be added or revoked. The keys themselves may be revoked if compromised. To avoid outdated keys, you can choose to have automatic updates scheduled for your users.

There are two types of updates you can schedule: Updating Trusted Introducers will fetch the latest copies of the Trusted Introducers' keys, plus any keys that they have signed. Updating all keys will simply get the latest copy of each key on the keyring.



☑ Automatically update administrative options every 1 days

LDAP Server URL:

☑ Automatically update all keys every 1 days

☑ Automatically update all Trusted Introducers every 1 days

The fields on the Updates panel are:

- **Automatically update administrative options every X days**. Check if you want your users to automatically download and implement the latest version of the PGPadmin administrative options. Make sure to specify an interval, also.

> **IMPORTANT:** We recommend you use LDAPS as the delivery protocol, as it provides both strong encryption and strong authentication of the data. This is **vital** for users who are downloading their PGP preferences over the Internet from their homes or while traveling.

- **LDAP Server URL**. Enter the URL of the LDAP server you want your users to get their PGPadmin administrative options from.

- **Automatically update all keys every X days**. Check if you want to force your users to update their keys on a regular basis. Make sure to specify an interval.

- **Automatically update all Trusted Introducers every X days**. Check if you want to force your users to update trusted introducers on a regular basis. Make sure to specify an interval.

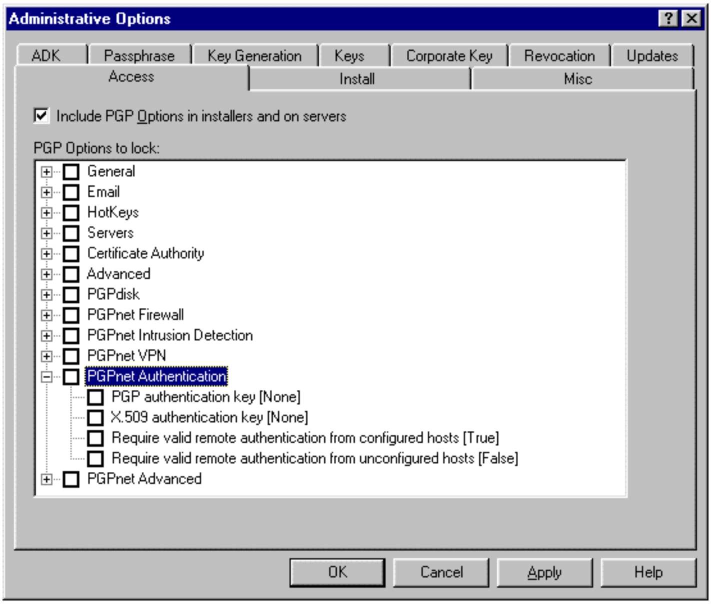
The Access panel

The Access panel lets you selectively disable your users' ability to set or change various PGP options on their machine; instead, they are restricted to using the settings you establish on your PGP administrative machine.

The **PGP Options to lock** list shows every PGP option and its current setting (shown in brackets). Before locking an option, make sure it is set the way you want.

IMPORTANT: The default setting is for all PGP options to be settable on their machines. If you want to disable one or more options you must specifically disable that option.

Your users can see what options are there, but they cannot change the settings.



☑ Include PGP Options in installers and on servers

PGP Options to lock:

- ⊞ □ General
- ⊞ □ Email
- ⊞ □ HotKeys
- ⊞ □ Servers
- ⊞ □ Certificate Authority
- ⊞ □ Advanced
- ⊞ □ PGPdisk
- ⊞ □ PGPnet Firewall
- ⊞ □ PGPnet Intrusion Detection
- ⊞ □ PGPnet VPN
- ⊟ □ PGPnet Authentication
  - □ PGP authentication key [None]
  - □ X.509 authentication key [None]
  - □ Require valid remote authentication from configured hosts [True]
  - □ Require valid remote authentication from unconfigured hosts [False]
- ⊞ □ PGPnet Advanced

The fields on the Access panel are:

- **Include PGP Options/Preferences in installers and on servers**. Check if you want to disable your users to set or change some or all PGP options on their machines.

- **PGP Options/Preferences to lock**. Lists all PGP options under the name of the tab they are on. There are two ways to lock options:

  Lock all of the options on a tab. Put a checkmark in the box next to the name of the tab (for example, General or Email). All options under that tab are locked with their current settings. Before locking all the options on a tab, make sure the options are set appropriately.

  Lock only specific options on a tab. Click on the plus sign or triangle next to the name of the tab and then putting a checkmark in the box next to the name of the option you want to lock.

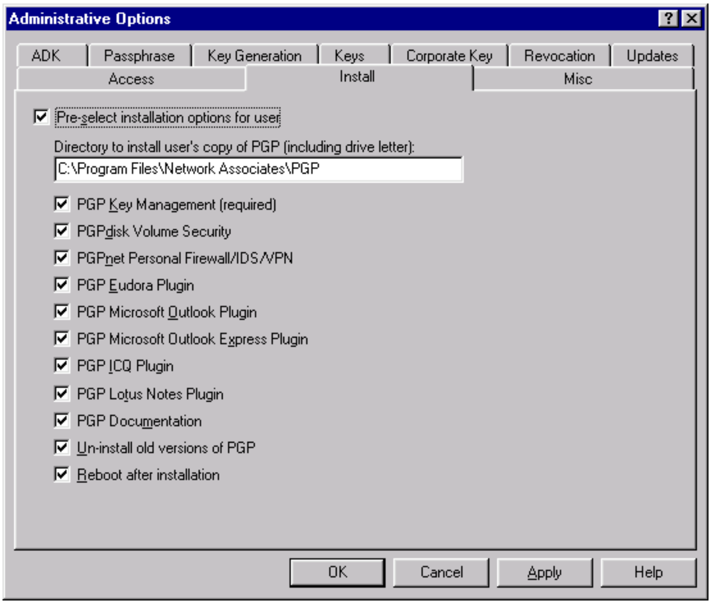
The Install panel

The Install panel on the Windows version and the Macintosh version of PGPadmin are very different. Both are shown and described below.

The Install Panel for Windows

To make it easier for your users to install PGP, you can pre-select such options as the installation directory and which PGP components will be installed. If you choose to do this, the installer will use the options you specify and won't ask your users for this information.

NOTE: Installation of the PGP key management files is required.



☑ Pre-select installation options for user

Directory to install user's copy of PGP (including drive letter):
C:\Program Files\Network Associates\PGP

☑ PGP Key Management (required)
☑ PGPdisk Volume Security
☑ PGPnet Personal Firewall/IDS/VPN
☑ PGP Eudora Plugin
☑ PGP Microsoft Outlook Plugin
☑ PGP Microsoft Outlook Express Plugin
☑ PGP ICQ Plugin
☑ PGP Lotus Notes Plugin
☑ PGP Documentation
☑ Un-install old versions of PGP
☑ Reboot after installation

The fields on the Install panel are:

- **Pre-select installation options for user**. Check if you want to specify the directory PGP will be installed into or which PGP components will be installed. If you uncheck this field, then your users will be asked to specify all of these items.
- **Directory to install user's copy of PGP (including drive letter)**. Enter the complete path of where you want PGP to be installed, including the drive letter.
- **PGP Key Management (required)**. Must be checked.
- **PGPdisk Volume Security**. Check if you want PGPdisk to be installed on your PGP users' machine.
- **PGPnet Virtual Private Networking**. Check if you want PGPnet to be installed on your PGP users' machine.
- **PGP Eudora Plugin**. Check if you want Eudora plugin to be installed on your PGP users' machine.
- **PGP Microsoft Outlook Plugin**. Check if you want the Outlook plugin to be installed on your PGP users' machine.
- **PGP Microsoft Outlook Express Plugin**. Check if you want Outlook Express plugin to be installed on your PGP users' machine.
- **PGP ICQ Plugin**. Check if you want the ICQ plugin to be installed on your PGP users' machine.
- **PGP Lotus Notes Plugin**. Check if you want the Lotus Notes plugin to be installed on your PGP users' machine.

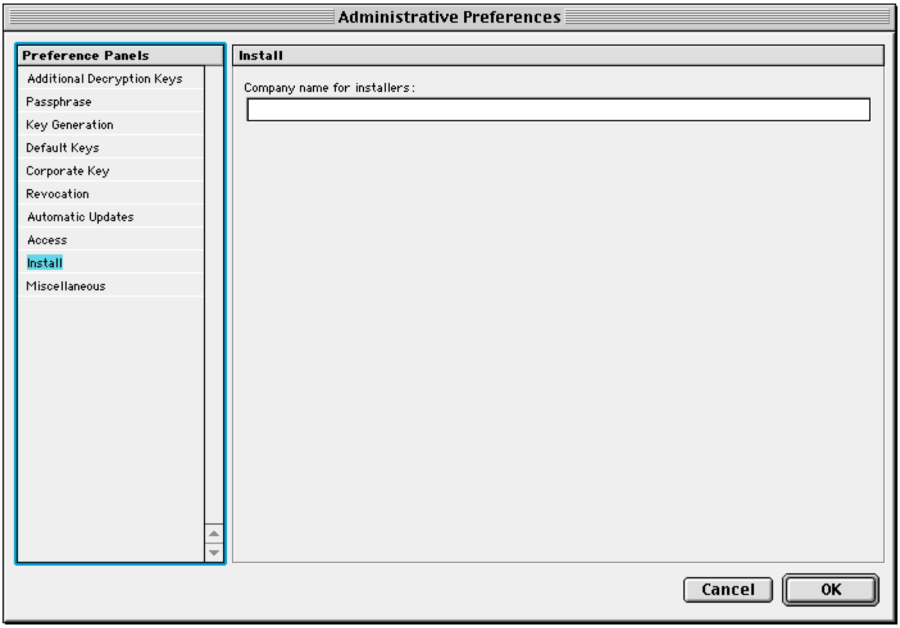
NOTE: If you are installing the PGP Lotus Notes email plug-in on your Lotus Notes client computers, you need to run the PGP Notes Plug-in Server Utility to configure the Domino server for PGP Lotus Notes plug-in use and configure individual user(s) databases so they can use the PGP Lotus Notes plug-in. Refer to Appendix E, "Configuring Lotus Domino Servers." for detailed instructions.

- **PGP Documentation**. Check if you want the PGP documentation to be installed on your PGP users' machine.
- **Un-install old versions of PGP**. Check if you want older versions of PGP on your users' machines to be uninstalled before the new version is installed.

- **Reboot after installation**. Check if you want PGP on your users' machines to automatically reboot when the new version is installed.

The Install Panel for Macintosh

If you like, PGPadmin lets you specify the name of the company that will be presented in the PGP client installation program.



The Misc panel

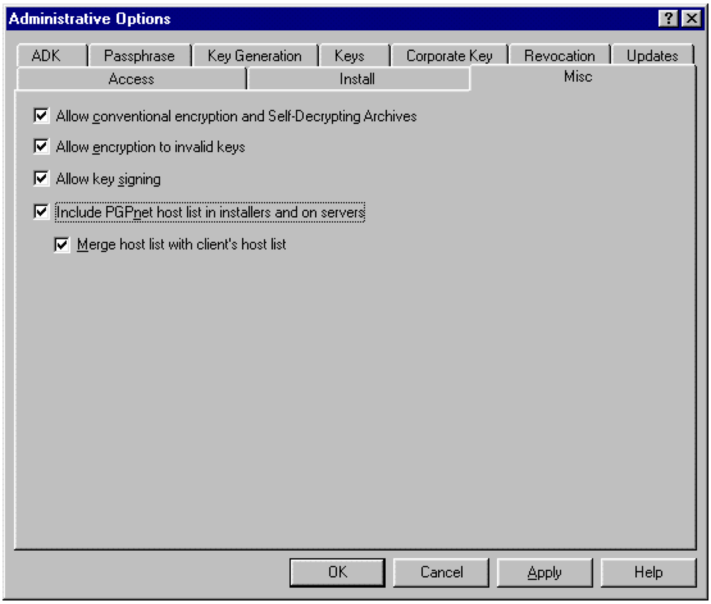
Conventional encryption is simply the encrypting of a message or document using a passphrase entered at the time of encryption. This form of encryption does not use public keys. It relies solely on the passphrase to encrypt the data.

NOTE: This panel is called the "Miscellaneous" panel on the Macintosh.

Unlike the normal usage of PGP, this allows anyone who knows (or can guess) the passphrase to decrypt the information. Care should be taken in deciding whether or not to allow conventional encryption. This option will also determine if the user is allowed to create self-decrypting archives.

You may want to restrict your users' ability to encrypt to invalid keys or sign keys. These capabilities are allowed by default, but in the interest of tighter security you can prevent your users from doing one or both.

PGPnet host lists are lists of remote hosts that PGPnet is configured to establish an SA with. You can choose to have the PGPnet host list on your PGP administrative machine be included in the PGP client installer program. If you do this, you can also choose whether to merge the host list with the PGPnet host list already on your users' machines or to overwrite their host list.



☑ Allow conventional encryption and Self-Decrypting Archives

☑ Allow encryption to invalid keys

☑ Allow key signing

☑ Include PGPnet host list in installers and on servers

☑ Merge host list with client's host list

The fields on the Misc panel are:

- **Allow conventional encryption and Self-Decrypting Archives**. Check if you want your PGP users to be able to use conventional encryption and self-decrypting archives.
- **Allow encryption to invalid keys**. Clear this box if you want to prevent your users from being able to encrypt to invalid keys.
- **Allow key signing**. Clear this box if you want to prevent your users from being able to sign keys.
- **Include PGPnet host list in installers and on servers**. Check if you want the PGPnet host list on your PGP administrative machine to be included in the PGP client installer program.
- **Merge host list with client's host list**. Check if you want to merge the PGPnet host list on your PGP administrative machine with the host list already on your users' machines. Otherwise, it will overwrite it.

Retrieving the Server Configuration 6

This chapter tells you how to retrieve the PGP settings from your LDAP server or PGP Keyserver to use a starting point for PGPadmin.

Overview

When you start PGPadmin, the settings from the version of PGP running on the PGP administrative machine are used as the starting point.

When you make changes in PGPadmin, the changes you make are *not* saved to the version of PGP running on the PGP administrative machine (unless you expressly save them using the **Apply** button on Windows or the **Update Local Configuration** button on the Macintosh). Instead, the changes are used only to create the PGP client installer program or the PGP settings file that you upload to your LDAP server.

If you want to use the PGP settings currently on your server as a starting point in PGPadmin (instead of the settings from the version of PGP running on the PGP administrative machine), you can download these settings from the server into PGPadmin.

Retrieving the settings from the server

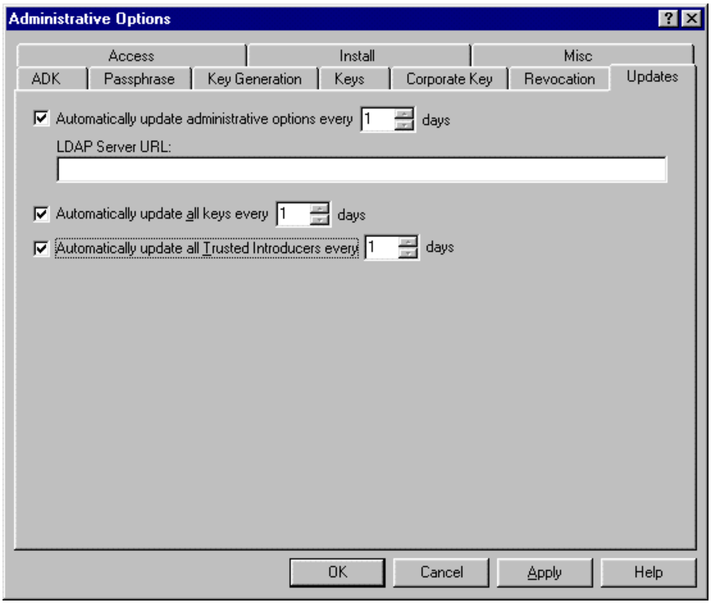
To retrieve the settings from your corporate server, you must tell PGPadmin about the server and then retrieve the settings.

To retrieve PGPadmin administrative settings:

1. Open PGPadmin on your PGP administrative machine.
2. Click **Administrative Options/Preferences**.

   The Administrative Options/Preferences screen appears.
3. Select the **Updates** panel (**Automatic Updates** on the Macintosh).

The Updates panel appears.



☑ Automatically update administrative options every 1 days

LDAP Server URL:

☑ Automatically update all keys every 1 days

☑ Automatically update all Trusted Introducers every 1 days

4. Make sure **Automatically update administrative options every X days** is selected and that **LDAP Server URL** has the URL of the LDAP server from which your PGP users get their updated PGP settings.
5. Click **OK**.

   The PGPadmin screen appears.
6. Click **Retrieve Server Configuration**.

   The current PGP settings on the LDAP server are downloaded into PGPadmin and then the PGPadmin screen appears.

Creating a Client Installer 7

This chapter tells you how to create the PGP client installer program that you will be distributing to your users.

Overview

Once you have established the PGP options and PGPadmin administrative options (preferences on the Macintosh) you want on your PGP administrative machine, you can create the PGP client installer program.

> **IMPORTANT:** Do not create the client installer program until all of the PGP options and PGPadmin administrative options (preferences on the Macintosh) are set the way you want them to be. If they are not right, you will either have to create and distribute another client installer program or put the updated settings onto an LDAP server and have your users download and implement them.

Creating the client installer program

The PGP client installer program is what you will be distributing to your users. It includes both the PGP options you want them to have and the PGPadmin administrative options (preferences on the Macintosh) you have configured.

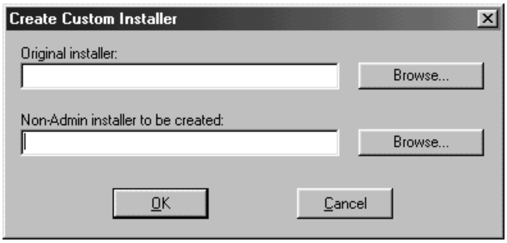
The following procedures tell you how to create the Windows and Macintosh PGP client installer programs.

To create a PGP client installer program for Windows:

1. Bring up PGPadmin on your Windows PGP administrative machine.

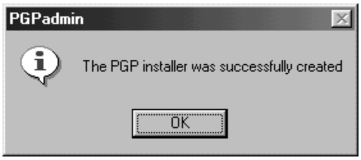
2. Click **Create Custom Installer**.

The Create Custom Installer screen appears.



3. Click the top Browse button and select the Windows PGP installation program that you want to customize with the PGP options and PGPadmin administrative options from your Windows PGP administrative machine.
4. Click the bottom Browse button and specify a location and a name for the Windows client installation program you are creating.
5. Click **OK**.

   When the Windows client installer program has been created, a message appears telling you that the installer was successfully created.



The PGP installer was successfully created

6. Click **OK**.

   The PGPadmin screen appears.

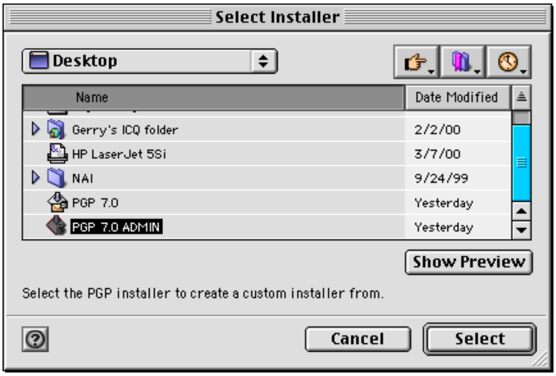
7. Distribute the client install program to your Windows PGP users.

   For ideas how to do this, refer to Chapter 8, “Distributing the PGP Client Installer Program.”

To create a PGP client installer program for Macintosh:

1. Open PGPadmin on your Macintosh PGP administrative machine.
2. Click **Create Custom Installer**.

   The Select Installer screen appears.

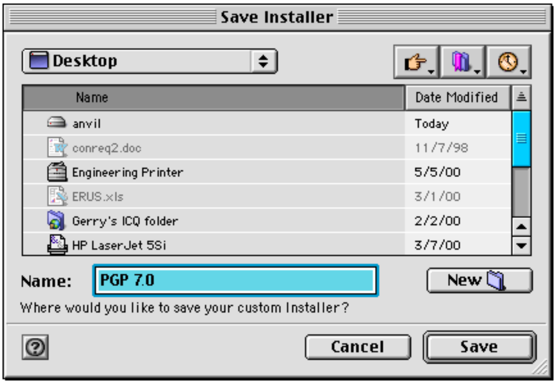


Name	Date Modified
Gerry's ICQ folder	2/2/00
HP LaserJet 5Si	3/7/00
NAI	9/24/99
PGP 7.0	Yesterday
PGP 7.0 ADMIN	Yesterday

Select the PGP installer to create a custom installer from.

3. Select the PGP installation program that you want to customize with the PGP preferences and PGPadmin administrative preferences from your Macintosh PGP administrative machine and click **Select**.

   The Save Installer screen appears.



Name	Date Modified
anvil	Today
conreq2.doc	11/7/98
Engineering Printer	5/5/00
ERUS.xls	3/1/00
Gerry's ICQ folder	2/2/00
HP LaserJet 5Si	3/7/00

Name: PGP 7.0

Where would you like to save your custom Installer?

4. Specify a location and a name for the PGP client installation program you are creating, then click **Save**.

   The PGP client installer program is created in the location you specified and the PGPadmin screen appears.

5. Distribute the PGP client installer program to your Macintosh users. For ideas how to do this, refer to Chapter 10, "Updating PGPadmin Settings."

Distributing the PGP Client Installer Program 8

This chapter gives you some ideas how to distribute the PGP client installer program to users in your organization. It also discusses whether or not to let your users create their own PGP keys.

Distributing the PGP client installer program

The most common methods of distributing the PGP client installer program are:

- Distribute using an enterprise software distribution system such as SMS or Tivoli.
- Let your users download the installer from a Web/file server
- Distribute the installer to your users on CD-ROMs

If you need to distribute the installer to a large number of users, the most expedient way is to put it on a file server. Your users can download the installer from the file server, generate their own keys, and begin using PGP.

Updating PGPadmin Settings 9

This chapter tells you how to post and update the PGPadmin administrative settings to an LDAP server or PGP Keyserver so that your users can easily download and implement the most up-to-date settings.

Overview

The settings you establish for your users when you create the PGP client install program may very well change over time. So that you don't have to create a new client installer every time this happens, you can have your users automatically update the latest administrative options from your corporate LDAP server or PGP Keyserver.

Before you can have them do this, of course, you need to put a file with the latest PGPadmin administrative settings onto the corporate LDAP server or PGP Keyserver so that your users can get to them.

Updating the settings

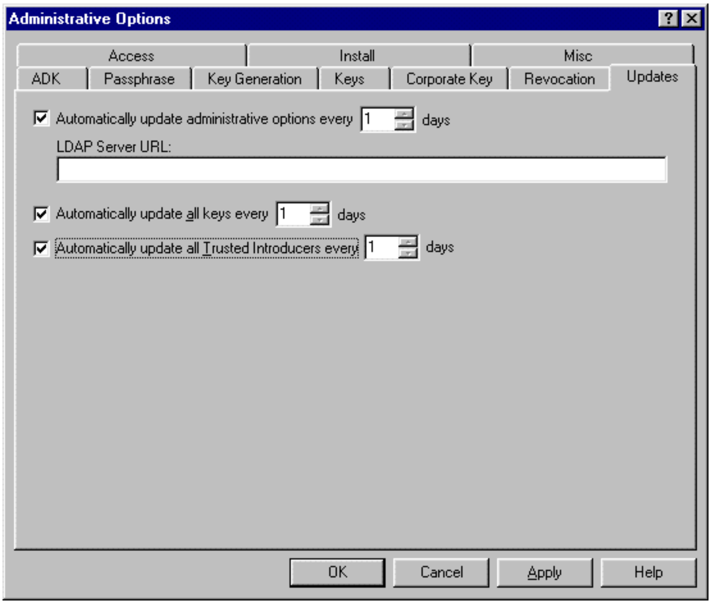
To put the PGPadmin administrative settings onto your corporate LDAP server or PGP Keyserver, you must tell PGPadmin about the server and then transfer the files.

To update PGPadmin administrative settings:

1. Open PGPadmin on your PGP administrative machine.
2. Click **Administrative Options/Preferences**.

   The Administrative Options/Preferences screen appears.
3. Select the **Updates** panel (**Automatic Updates** on the Macintosh).

The Updates panel appears.



☑ Automatically update administrative options every 1 days

LDAP Server URL:

☑ Automatically update all keys every 1 days

☑ Automatically update all Trusted Introducers every 1 days

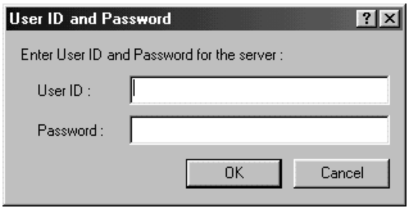
4. Make sure **Automatically update administrative options every X days** is selected and that **LDAP Server URL** has the URL of the LDAP server or PGP Keyserver your PGP users are going to get their updated PGPadmin administrative settings from.

5. Click **OK**.

   The PGPadmin screen appears.

6. Click **Update Server Configuration**.

   The login screen for your LDAP server or PGP Keyserver appears.



Enter User ID and Password for the server :

User ID :

Password :

7. Login to your LDAP server or PGP Keyserver.

   The current PGPadmin administrative settings are uploaded to the LDAP server and then the PGPadmin screen appears.

Setting up a Network Security Policy A

It's PGP's job to enforce your network security policies—but it's your job to define those policies first.

We cannot overstress the importance of developing a good, written security policy. As good a tool as PGP is, no product can protect your network without a well-constructed, organization-wide security policy. In fact, deploying a security product without a security policy can actually be worse because it can encourage a false sense of security that can lead to complacency.

Without a security policy, you cannot effectively protect your network. That's so important, we're going to repeat it in bold:

Without a security policy, you cannot effectively protect your network.

And yet, studies show that 92% of all corporations have no security policy at all. So, the single most important part of any PGP deployment is the effort you put into defining your network security objectives and then translating those objectives into a concrete set of specific policies. Configuring PGP is nothing more than instructing PGP how to implement each of those concrete policies.

Developing a network security policy

NOTE: To have real value, a network security policy must be developed as an integrated component of an organization's master security policy. The network security policy should harmonize with security policies in other areas such as physical plant integrity, employee background checks, electronic eavesdropping detection, and so forth. Because of this—and because so many organizations have no security policy at all—in this section we discuss how to develop a master security policy. But keep in mind that only the network section of your master security policy will affect the way you use PGP.

An organization-wide security policy isn't something you can buy in a store, because every organization has its own unique priorities and its own unique way of doing business. Every organization needs to develop the unique set of security policies that will work for them. And so every organization needs to do the challenging work of developing its own security policy.

Before you start

Before you start, you should understand that this work won’t be a question of setting up software, but rather a matter of:

- researching your organization’s priorities
- identifying your critical physical and data assets
- researching what options—that is, what techniques, technologies, money and people—are available for protecting them
- making a series of choices from among your options

Steps to a security policy

The five key steps in developing your security policy are:

1. Understand the goal.
2. Define a process.
3. Identify your organization’s security objectives.
4. Translate your objectives into concrete policies.
5. Create the policy document.

Once the policy document exists, your organization can proceed to deploy the new policies. Full deployment of your security policy can be logistically complex and may affect all facets of your operation including physical plant changes, the creation of new employee training programs, the development of a policy enforcement infrastructure, testing and revising the policy, and so forth.

These five steps are described in more detail below.

1. Understand the goal

You should start out knowing what you’re working towards. The end product of your policy development process is going to be a high-level, organization-wide security policy document.

Security policy documents typically lay out objectives, policies, and enforcement:

- The organization's chief security **objectives**

  Most organizations share the same basic security goals of preventing loss or damage of physical assets and preventing loss, damage, or exposure of data assets—but that's too general to be very useful here. Your policy needs to be specific about which particular assets (or categories of assets) most need to be protected and which are less mission-critical.

  For example, a public relations company couldn't do business if its media contacts database file were damaged, and an accounting firm could be seriously hurt if its client records were made public through network espionage. Those are key assets, and protecting them is an important objective.

- Detailed **policies** that support those objectives

  This will be your list of specific operational rules. The rules will be grouped into subject areas, such as:

  Controlling access: Who can access what under which conditions?

  What security vulnerabilities must be watched for, and how should they be handled when they arise?

- A security **enforcement** plan

  Typically this plan will identify a policy enforcement responsibility hierarchy within the organization and set forth the penalties for employee violations of specific policies.

Once you have an idea of what your final work product needs to looks like, you'll need to plan a process to produce it.

2. Define a process

Creating a security policy can be a large task; it is a job best tackled by a group of people working together. You'll need to figure out who should be in this working group, how the group is going to obtain the information it'll need, and how it's going to split the work up.

Unfortunately, the differences that make every organization unique mean that we can't offer very much specific guidance on how to run your group. In fact, the details of the process of developing your security policy will be every bit as unique as the policy you'll finally produce.

We can however offer a few points of general advice:

- Include the right people.
- Do your research.
- Remember that security is often low-tech.
- Get outside help if you need it.

Details on each of these points follow.

Include the right people

It takes a mixed team of people from all levels and all departments of the organization to develop a strong security policy. Your policy may potentially affect every person in the organization, and you'll need the involvement of employees who have your 'institutional knowledge' to make sure you craft a security policy that's compatible with your existing business practices and not unnecessarily annoying to your employees.

Studies have shown that security policies developed without the input of line staff frequently cause employee resentment and are less likely to be strictly observed once deployed.

Do your research

Much has been written about what makes for a good security policy and the process of developing one. You can save yourself a lot of time, stay more focused, and wind up with a better result by consulting that material.

Remember that security is often low-tech

One pitfall to watch for is the tendency of technical people to think primarily in terms of technical solutions. Real security demands a wider view—for example, password-protecting your source code won't prevent a dumpster-diver from getting the files off a discarded computer's hard drive—and you'll likely find involving experienced security specialists to be a good way of reducing the chance that you're overlooking less-technical vulnerabilities and remedies.

Get outside help if you need it

You may determine that you don't have all the internal resources you'd need to develop a strong set of policies on your own and need some help. Sources of outside assistance include:

- **Security consultants.** This is a rich and booming industry, especially in regard to network security, and you should have little trouble locating an individual or firm to work with you.
- **Major accounting firms.** Many of them now offer security consulting services, including network security consulting.
- **Network Associates.** We offer both our own network security policy consulting services and referrals to independent network security policy consultants.

Of course, you should never rely on the work of any security consultant you don't know and trust. Always get multiple references and check them before hiring any security vendor.

3. Identify your organization's security objectives

A security policy needs to reflect the organization's fundamental priorities. In other words, you have to figure out what you need to protect before you can start figuring out how to go about protecting it. This means identifying your organization's security objectives.

What's a security objective?

Security objectives are general high-level goals, usually 'what' statements of a desired outcome that don't get into the low-level 'how' of their implementation.

Typical security objectives might include:

- Keep employees' eyes off the HR files.
- Keep the marketing files company-confidential.
- Keep company information safe from visitors to the building.
- Protect mission-critical segments of the network from outside dangers.
- Protect mission-critical segments of the network from internal dangers.
- Keep company-confidential emails from being forwarded outside the company network.
- Limit access to trade secret documents in the Product Development department, and prevent their unauthorized duplication.

Before you can draw up your organization's unique list of security objectives, you'll first need to understand precisely what it is that your organization needs to protect.

Research the organization: How should *you* define 'security'?

Different organizations have different things to protect. Achieving security depends on identifying the things that matter to your organization.

Some businesses have unique kinds of information to protect. A software developer needs to protect its source code; a film studio needs to protect its release schedule and marketing plans; a photo archive needs to protect its media assets. Most businesses also have similar kinds of basic business information that needs to be kept both intact and private, such as accounting files and HR data.

But things are not always that simple, because seemingly similar information may have different security issues in different organizations. For example, a health care organization will need to take strong steps to protect the confidentiality of its client database for reasons of liability and governmental regulation, whereas a newspaper distributor can probably be a little less extreme about safeguarding its subscriber database. Both are customer files, but they need different protection.

So you need to carefully determine which assets *your* organization most depends on, and plan your security policy around protecting those—each in proportion to its importance. These key assets may be information stored on computers, or paper files, or employee know-how, and whatever physical items are required to sustain your productive capacity (for a vegetable distributor, refrigeration can be a security issue!).

It generally takes a department-by-department survey of company operating procedures to identify those key assets and capacities—and for a large organization that can take a lot of time.

TIP: We strongly suggest consulting reference material such as case studies, or working with a consultant, to make sure you aren't inadvertently missing any of the critical but sometimes non-obvious key assets in your organization. A good security consultant will know what to look for.

Drafting your objectives

You should draft your objectives and pull them together into some sort of document for the working group to review, discuss, revise, and eventually approve. This needn't be an overly formal or polished document, as it usually won't circulate beyond the working group, but producing the document will force you to clearly articulate your objectives, and having an objectives document with group buy-in will afford a strong foundation for your potentially challenging next step: translating objectives into concrete policies.

4. Translate your objectives into concrete security policies

Once you know what things need protecting, you have to decide what degree and form of protection to give each one. That means matching the items in your objectives document with appropriate practical implementation measures. These measures may include creating new business operating procedures (or modifying existing procedures), and selecting technical aids like PGP and deciding how to configure them.

In other words, you need to translate your high-level security objectives into a real-world practical implementation involving many elements—not all of them high-tech.

Translating objectives into policies is a crucial phase in the process—and frequently a tricky one. In fact, most organizations find this translation step the most challenging and time-consuming part of the policy development process. Some of it can often be done in a cookbook manner, picking and choosing good ideas from books or other companies' policies, but translation is necessarily going to require a significant amount of analysis of requirements, active researching and evaluation of your options, and some clever invention to address your unique situation. As always, we recommend you obtain outside help if you need it.

What's a 'concrete security policy'?

Concrete security policies are the particular, practical measures that implement your security objectives; they're the 'how' statements that go with the 'what' statements in your security objectives document. It will often take more than one concrete policy to implement a single objective, but there shouldn't be any concrete policies that don't flow directly from specific objectives.

Typical concrete security policies might include:

- Require all visitors to wear ID badges including a host employee's name and phone number.

  This concrete policy helps to implement the objective 'Keep company information safe from visitors to the building.'

- Keep the Product Development trade secret documents physically secure behind a checkpoint, with no access to unattended photocopiers.

  This concrete policy helps to implement the objective ‘Limit access to trade secret documents in the Product Development department, and prevent their unauthorized duplication.’

- Put mission-critical segments of the network behind firewalls.
- Observe specific password selection policies to make passwords harder to guess.

  These two concrete policies each help to implement the objective ‘Protect mission-critical segments of the network from outside dangers.’

- Limit password access to mission-critical segments of the network to highly trusted employees with a legitimate need.

  This concrete policy helps to implement the objective ‘Protect mission-critical segments of the network from internal dangers.’

- Observe specific physical security policies to make passwords harder to steal.

  This concrete policy helps to implement the objective ‘Protect mission-critical segments of the network from internal dangers.’

In a real policy document, each of these concrete policies would be fleshed-out with whatever further specific details would be needed to put the policy into practice. For example, the specific password selection rules would be set forth, or the specific firewall product to be used and its desired configuration, and so forth.

When you’ve got a set of concrete implementation policies that adequately address every security objective on your list, you’ll be ready to publish your policies in a master security policy document.

5. Create the policy document

Once you’ve puzzled out all of your concrete security policies, you should create a master security policy document that collects them all. This document will become the organization’s reference for all security matters. It can provide the basis for any employee training materials or programs you’ll need to bring the staff up to speed. It will also guide your deployment process, including your installation, configuration, and use of PGP.

Security issues

This section covers, at a very high level, some security issues to take into account when developing a security policy.

Encryption

If you want to protect data from eavesdroppers as it travels from your network to other companies over an unsecured network like the Internet, you will need encryption. Encryption is recommended for any sensitive data, such as private email, data exchanged between business partners, or customer information collected on a Web site. In addition, PGPdisk protects your current and archival files from unauthorized users.

PGP provides encryption as well as authentication, which ensures the integrity of your data.

Passwords and passphrases

Because passwords generally establish access to your network, it is wise to institute policies that dictate how and when they should be used or discarded.

Password policies that require users to change their passphrase often or insert non-alphabetic characters make it difficult for employees to remember their passwords. Many employees end up writing down their passwords and taping them to the inside of a desk drawer.

If your users must write down their passwords, consider having them create a text file on their computer desktop listing their passwords and then encrypting the file with PGP’s strong encryption. This method does not prevent employees from accidentally deleting the file, but the file should be more secure against an attacker than a Post-It adhered to the employee’s monitor.

Residual data

Residual data refers to the data remaining on the physical hard disk of a computer after an employee has deleted it. Applications generally delete the name of the file but leave the actual data intact, waiting to be overwritten by another application. Some applications also create automatic backups of file to memory, which are stored in locations a user might not expect or remember to purge.

This data is available to any attacker with a disk recovery toolkit, particularly if your company discards the old computer. *Dumpster diving* is a legal method for attackers to retrieve confidential information from discarded systems.

PGP’s disk wiping utilities permanently deletes any residual data. If you consider theft of data a threat, then your security policy may need to require users to purge their systems of discarded data on a routine basis.

Physical security

Physical security implies the protection of the actual computer systems in your company. It refers to locking doors and limiting access. Do you know who has access to your server facilities and who has access to your wiring closets? Many network disasters are caused by angry employees seeking retribution.

For example, if your company uses the PGP Keyserver, it might be a good idea to ensure that the system on which it is installed is kept behind a locked door.

Corporate Signing Keys

A *Corporate Signing Key* is a key pair used to prove that digital certificates, information, products, and so on have been validated by an authority acting on behalf of the company. The Corporate Signing Key is primarily used for signing, but can also be used for encryption. It is typically held by the Corporate Security Officer alone, or split into multiple shares (see Key splitting, below).

Some examples of uses for a Corporate Signing Key are:

- signing employees’ digital certs or keys
- signing softcopies of legal documents
- signing software produced by your company

Because the Corporate Signing Key is used to validate all keys in your organization as well as provide authentication for other data as well, it is vital that this key is never compromised, lest someone else pretend to act in the company’s name.

Additional Decryption Keys

An *Additional Decryption Key* (ADK) enables a company to access information encrypted by its employees in the event of an emergency. ADKs are useful in situations where the user to whose key information is encrypted is somehow unable to decrypt the information, either because the key or passphrase is lost or because the user is unavailable due to an accident or other absence. For an environment employing strong encryption with no available “back door,” an ADK is a prudent data recovery tool.

In environments that enforce the use of ADKs, any information encrypted to the user's key is also encrypted to the ADK. When someone inside or outside the organization encrypts information to a user, the information is also encrypted to the ADK. This allows the holder of the ADK to decrypt any information sent to the user. This operation happens automatically, and is fully integrated into the encryption process.

Consider your ADK usage policy carefully, paying attention to striking the correct balance between employee privacy and data recovery. If your policy is too strict, your users may view it as a lack of trust and choose not to use any encryption, which could leave you with vulnerabilities in your system. Recovery of stored data, such as that on a PGPdisk volume, is generally viewed more favorably than recovery of communications, such as private email.

Key validation

Every user in a public key system is vulnerable to mistaking a phony key (digital certificate) for a real one. *Validity* is confidence that a public key certificate belongs to its purported owner. Validity is essential in a public key environment where users must constantly establish whether or not a particular certificate is authentic.

When a user is assured that a certificate belonging to someone else is valid, the user can sign the copy on her local keyring to attest to the fact that she has checked the certificate and that it's a good one. If that person wants others to know that she gave the certificate her stamp of approval, she can export the signature to a certificate server so that others can see it.

Some companies designate one or more *Certification Authorities (CA)*, to check the validity of all the certificates in the organization and sign the authenticated ones. The CA is responsible for validation in an organization, and is an entity whom everyone trusts; in some public key environments, no certificate is considered valid unless it has been attested to by a CA.

Key splitting

Key splitting, also called "secret sharing" is the ability to split a private key into multiple pieces or *shares*, and share those pieces among a group of people. To use the key, a designated number of the keyholders must bring their shares of the key together to reconstitute the key.

Splitting or sharing the private key used for signing ensures that any one person cannot compromise the key and greatly reduces the possibility of abuse.

PGP uses a secure TLS connection during key reconstitution, which allows the process to be completed securely over an untrusted network without requiring any shareholders to be physically present.

Designated revokers

When a private key or its passphrase is lost, the key's security is compromised. The safest action to take in such a situation is to prevent others from encrypting information to the key by revoking it. The difficulty in a scenario such as this is that the passphrase and private key are required to revoke a key.

A designated revoker is another key pair that has been authorized to revoke the key on behalf of the owner. You can configure the PGP client installer program to add a designated revoker key for all keys generated with the PGP Key Generation Wizard.

Determining your email policy

Because PGP is widely used for privacy of email, we'll use email examples in demonstrating what to consider when creating a network security policy.

Employee email privacy

PGP software makes possible an unprecedented increase in privacy for personal and corporate email. Within the confines of the work environment, employees must understand that they must reconcile their personal privacy with corporate security, but employers should consider that there is a legitimate need for personal privacy in the workplace. Businesses operate on trust, trust that employees know their jobs and trust that they do their work in the best interests of the organization. However, there may be occasions when a compelling reason for monitoring, accessing, or reading employees' email arises, for example, death or other unavailability of an employee, forgotten passwords, or unethical and/or illegal activity by an employee.

If your company reserves the right to monitor, read, intercept, or access employees' email messages, it is imperative to have a clear, definitive policy statement and to make sure that everyone reads and understands it.

Creating a written email policy

Here are some things to consider when creating your organization's email policy. (Adapted with permission of the Cyberspace Law Institute.)

Purposes for which company email may be used

- Email may be used only for company business.
- Email may be used for incidental personal purposes.
- Email may be used for personal purposes without restriction.

Encryption and labeling

- Encryption of any kind is permitted.
- Only specified forms of encryption are permitted.
- Personal email must be labeled as such.
- Signature files or message text must disclose limitations of the employee’s authority.

Systemic monitoring

- No systemic monitoring.
- Monitoring allowed for any business purpose.
- Monitoring allowed only with good-cause legal obligations.

Access and disclosure without consent in specific cases

- No access without consent unless required by law or other duty.
- Access or disclosure with good cause and appropriate measures.
- Access or disclosure for any business by those with authority.
- Notification after the fact of any access or disclosure.

Substantive rules

- Company email may not be used for illegal or wrongful purposes.
- Company email may not be used to download software without checking for viruses.
- Electronic snooping is prohibited.
- Electronic mail may not be used for sexual harassment, chain mail messages, or other purposes against organizational rules of conduct.

Protection of proprietary information

Policies and safeguards should be put into place requiring that proprietary information transmitted via email be encrypted. You should specify which types of information must be encrypted and which types may be sent in clear text.

Regular destruction of email archives

Are there legal timebombs in your email archives? Keeping email archives forever is an unnecessary exposure to the risk of litigants subpoenaing your archives and investigators sifting through the contents of employees' email.

Your company should take the following actions:

- Have a policy that says how long email is to be kept or how often the archive must be purged.
- Have a procedure or process in place to guarantee that the destruction or purging actually happens.
- Communicate your email archive policies to users.
- Decide whether the email of certain classes of users is archived longer than others. You may choose to only archive the email of special classes of users, such as corporate officer's or key technical contributors, after a given period of time.

Any email message that pertains to any kind of legal case can be subpoenaed as evidence. If you don't have an email destruction policy and procedure in place, you could find yourself accused of intentionally destroying evidence years after the actual destruction took place.

This is particularly important if your organization uses additional decryption keys associated with users' keys. Consider carefully how to achieve a balance between your potential exposure to litigation and the need to have information available—for example, consider making policy the regular destruction of your ADKs.

Implementing a PGP Public Key Infrastructure B

Many companies are composed of various and highly diverse organizations and departments that need to work together in complex ways. Users trying to communicate with others in a public key environment need to understand how to find and validate a complete certification path from the public keys of people they have never met to completely trusted Certification Authorities. Alert and knowledgeable users are less likely to encrypt information to counterfeit keys.

A *public key infrastructure* is necessary if public-key-based technologies are to support a large or diverse user population. It provides a framework of relationships between certification authorities, ways to validate keys, digital certificate management and so on.

What is a Public Key Infrastructure?

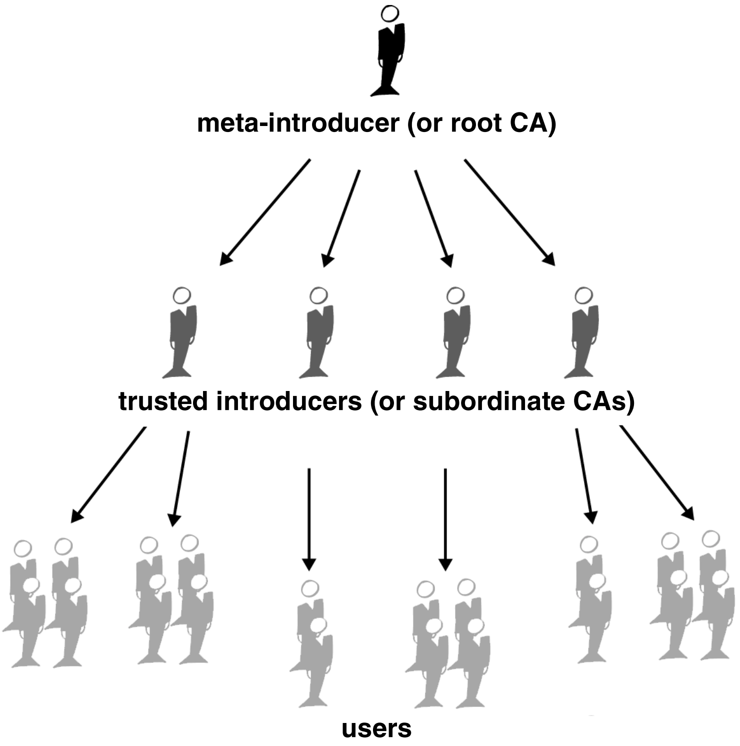
A PKI contains the certificate storage facilities of a certificate server (also called a key server), but also provides certificate management facilities (the ability to issue, revoke, store, retrieve, and trust certificates). The main feature of a PKI is the introduction of what is known as a *Certification Authority*, or *CA*, which is a human entity—a person, group, department, company, or other association—that an organization has authorized to issue certificates to its computer users. (A CA's role is analogous to a country's government's Passport Office.)

A CA creates certificates and digitally signs them using the CA's private key. Because of its role in creating certificates, the CA is the central component of a PKI. Using the CA's public key, anyone wanting to verify a certificate's authenticity verifies the issuing CA's digital signature, and hence, the integrity of the contents of the certificate (most importantly, the public key and the identity of the certificate holder).

Validating users' keys

Every user in a public key system is vulnerable to mistaking a phony key (certificate) for a real one. *Validity* is confidence that a public key certificate belongs to its purported owner. Validity is essential in a public key environment where you must constantly establish whether or not a particular certificate is authentic.

Some companies designate one or more Certification Authorities (CAs) to indicate certificate validity. In an organization using a PKI with X.509 certificates, it is the job of the CA to *issue* certificates to users—a process which generally entails responding to a user's request for a certificate. In an organization using PGP certificates without a PKI, it is the job of the CA to check the authenticity of all PGP certificates and then sign the good ones. Basically, the main purpose of a CA is to bind a public key to the identification information contained in the certificate and thus assure third parties that some measure of care was taken to ensure that this binding of the identification information and key is valid.


meta-introducer (or root CA)
trusted introducers (or subordinate CAs)
users

Trust models

A *trust model* is a convention that governs how validation works in a public-key environment. In relatively closed systems, such as within a company, it is easy to trace a certification path back to the root CA. However, users must often communicate with people outside of their corporate environment, including some whom they have never met, such as vendors, customers, clients, associates, and so on.

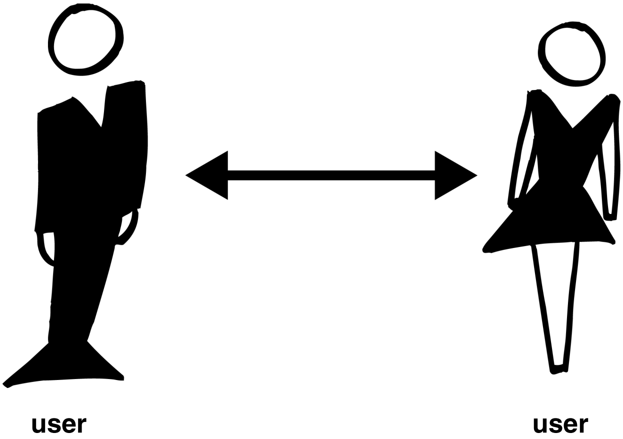
There are three different trust models:

- Direct trust
- Hierarchical trust
- A Web of trust

Direct trust

Direct trust is the simplest trust model. In this model, a user trusts that a key is valid because he or she knows where it came from. All cryptosystems use this form of trust in some way. For example, in web browsers, the root CA keys are directly trusted because they were shipped by the manufacturer. If there is any form of hierarchy, it extends from these directly trusted certificates. In PGP, a user who validates keys herself and never sets another certificate to be a trusted introducer is using direct trust.

Small organizations with no central certification authority would probably use direct trust as their trust model, an example of which is shown in the following figure.



Hierarchical trust

In a hierarchical system, there are a number of “root” certificates from which trust extends. These certificates may trust certificates themselves, or they may trust certificates that trust still other certificates down some chain. Consider it as a big trust “tree.” The “leaf” certificate's validity is verified by tracing backward from its certifier, to other certifiers, until a directly trusted root certificate is found.

This model is the one most commonly used in corporations.

Web of trust

A web of trust encompasses both of the other models, but also adds the notion that trust is in the eye of the beholder (which is the real-world view) and the idea that more information is better. It is thus a cumulative trust model. A certificate might be trusted directly, or trusted in some chain going back to a directly trusted root certificate (the meta-introducer), or by some group of introducers.

PGP uses digital signatures as its form of introduction. When any user signs another’s key, he or she becomes an introducer of that key. As this process goes on, it establishes a *web of trust.*

In a PGP environment, *any* user can act as a certifying authority. Any PGP user can validate another PGP user’s public key certificate. However, such a certificate is only valid to another user if the relying party recognizes the validator as a trusted introducer. (That is, you trust my opinion that others’ keys are valid only if you consider me to be a trusted introducer. Otherwise, my opinion on other keys’ validity is moot.)

Stored with each key on a user’s public keyring file are indicators of:

- whether or not the user considers a particular key to be valid
- the level of trust the user places on the key that the key’s owner can serve as a certifier of others’ keys

You indicate, on your copy of my key, whether you think my judgement counts. It’s really a reputation system: certain people are reputed to give good signatures, and people trust them to attest to other keys’ validity.

Validating keys with a Corporate Signing Key

Manually validating all keys in an organization can be a daunting task. More importantly, it is a task that must be accomplished methodically so that invalid keys are not accidentally mingled with valid keys. PGP provides a mechanism to prevent accidental posting of invalid keys on the server.

This mechanism is a holding, or *pending*, area for any keys sent to the server that do not meet security policy requirements.

(See the *PGP Keyserver Administrator's Guide* for more information on setting up a key acceptance policy on the server.)

A commonly enforced practice is to require only those certificates which have been signed by the Corporate Signing Key (or authorized trusted introducers) to be accepted by the certificate server. The PGP Keyserver automatically redirects any keys that do not adhere to corporate policy to the "pending area." You can search this pending area periodically and validate any keys in there. You can then send them to the server.

The typical process for validating corporate keys is as follows:

1. The user generates a new key.
2. The key is automatically sent to the certificate server.
3. Any keys that do not adhere to policy are held in the pending area of the certificate server.
4. Periodically, the CA checks the pending area for new keys. Upon finding a new key, the CA manually authenticates the key—that is, checks its fingerprint against the one on the user's private key (either by phone or in person).
5. The CA signs the key to validate it.
6. The CA moves the key to the certificate server where it is available to other PGP users.

By holding keys in a pending area and allowing only valid keys to be moved to the certificate server, you can ensure that only valid keys are available to your user community.

Creating a Corporate Signing Key C

What is a Corporate Signing Key?

A *Corporate Signing Key* is a key pair used to prove that digital certificates, information, products, and so on have been validated by an authority acting on behalf of the company. The holder(s) of the Corporate Signing Key acts as a root *Certification Authority (CA)*.

Typically held by the corporate security officer alone or split into multiple shares and held by an entire security team, the Corporate Signing Key is used primarily for validating employees' keys. To ensure that all keys in an organization are valid, many companies institute a policy dictating that digital certificates signed by the Corporate Signing Key are valid and that employees should be cautious of keys or documents not signed by the Corporate Signing Key (or trusted introducers created by the key) because they have not been authenticated by a known certifying authority. The Corporate Signing Key can be the meta-introducer for an organization.

Some examples of uses for the Corporate Signing Key are:

- signing employees' digital certs or keys
- creating trusted introducer signatures on trusted keys
- signing softcopy of legal documents
- signing software produced by your company
- signing official corporate email and announcements

A Corporate Signing Key is typically used for signing only. Some companies use a Corporate Signing Key for encryption as well, but it is a less common practice to encrypt with the corporate key. If you use a Diffie-Hellman/DSS key as a Corporate Signing Key, you can remove the encryption portion of the key (the encryption *subkey*) and designate the key as a *signing-only* key. For more information on creating and deleting encryption subkeys for a Corporate Signing Key, see the section on creating new subkeys in the *PGP User's Guide*.

Protecting a Corporate Signing Key

This key identifies your corporation to the outside world and validates all your users to each other and to your business partners as well as provide authentication for other data as well (files, personnel information, legal documents, your products). Therefore, maintaining complete control of this key is paramount to preserving the integrity of your PGP environment. Thus it is a good idea to implement key splitting for the Corporate Signing Key so no one individual can use it alone.

We recommend that you generate this key in the presence of at least two of your most highly-trusted employees and immediately split the key into multiple shares. Similarly, when using this key for signing, you should take care to reconstitute this key in the presence of at least two trusted individuals.

It is important to add some measure of physical security to the storage of a Corporate Signing Key or its share files, however. For example, the machine used for reconstituting the Corporate Signing Key should be secure, possibly behind a locked door. You may wish to lock the key share files or the key itself in a safe.

We also recommend that you create and enforce a disaster recovery policy for secure storage of the key's shares—perhaps offsite in a physically secure location—in the event of a natural disaster (such as an earthquake or fire).

Creating a Corporate Signing Key

Use the **Key Generation Wizard** to create a Corporate Signing Key that meets your security needs. This key pair will appear on your local keyring. You designate it as the Corporate Signing Key when you establish the settings for the PGP client installer program; not during key generation.

After you designate a key as the Corporate Signing Key, you can use it to sign all the other keys in your organization, including your own personal key. You can also configure the PGP client installer program so that any key generated by a user automatically signs the Corporate Signing Key.

The sections below provide some additional information you may find useful as you generate your key.

Key type

The Corporate Signing Key is generally used for signing, not encryption. If you use a Diffie-Hellman/DSS key, you can make sure the Corporate Signing Key is used only for that purpose by making it a signing-only key. This is only possible with a Diffie-Hellman/DSS key.

Key size

The Corporate Signing Key should be at least 2048-bit.

Splitting

Most companies split the Corporate Signing Key and distribute the shares among multiple individuals. PGP implements a secure network connection so that shareholders of a split key do not need to be physically present throughout the reconstitution process.

As stated above, we recommend that you always split and reconstitute the key in the presence of witnesses. Some companies go so far as to videotape these processes.

For more information on key splitting, see the *PGP User's Guide.*

Subkeys

After you have created your Corporate Signing Key, you may wish to prevent the key from being used for encryption. To do so, you can delete any encryption subkeys associated with the key. For more information on creating and deleting encryption subkeys for a Corporate Signing Key, see the section on creating new subkeys in the *PGP User's Guide*.

Using the Corporate Signing Key

The following suggestions will help you establish trust in the Corporate Signing Key throughout your company.

- **Distribute the key with the PGP client installer program.** Add the key to the default keyring installed with the PGP client installer program so that every PGP user receives a copy of the Corporate Signing Key on his or her local keyring.
- **Publish the key's fingerprint.** Once you have created the Corporate Signing Key, you should publish the key's fingerprint in a non-electronic format so that users can verify its validity or distribute it through other trusted means.
- **Use your key server's validation features.** You can configure the Certificate Server to send any keys not signed by the Corporate Signing Key to a pending area, where the keys will remain until you can validate them. For more information, see the *PGP Keyserver Administrator's Guide.*

- **Make the key available to the public.** If you plan to use your Corporate Signing Key to sign information distributed or sold outside the company, you may want to post the key on a public key server so that recipients of the signed information can verify the signature.

Creating Additional Decryption Keys D

What are Additional Decryption Keys?

Suppose your chief scientist is hit by a bus and is hospitalized for months. Or that your lead engineer, in a rage, encrypts his entire hard drive and leaves the company. What happens to all that data, which is so securely encrypted? Can you retrieve it, or is it gone forever?

An Additional Decryption Key (ADK) is a data recovery tool. In an environment that enforces use of an ADK, any information encrypted to a user's key is also encrypted to the Additional Decryption Key. When someone inside or outside the organization encrypts information to a user, the information is also encrypted to the Additional Decryption Key. This allows the owner of the Additional Decryption Key to decrypt any information sent to the user. This process happens automatically, and is fully integrated into the encryption process.

Recover data in an emergency

An ADK is a powerful security tool in situations where an employee is injured, incapacitated, or terminated, leaving valuable information encrypted. Because PGP has no "back door," recovery of this information would be otherwise infeasible.

While you may not ordinarily use your ADKs, there may be circumstances when it is necessary to recover someone's data, for example, if someone is out of work for some time or if you are subpoenaed by a law enforcement agency and must decrypt messages or files for a court case.

Data recovery versus key recovery

Do not confuse data recovery with key recovery. An Additional Decryption Key lets you recover information that has been encrypted to a particular key, not the key itself. The difference is crucial. If a mechanism exists to obtain a copy of a user's key, one major feature of a public-key cryptosystem—non-repudiation—is lost. If more than one copy of a key exists, then a user can deny having signed information with the key.

Retaining copies of users' keys has an added security risk: the machine storing the keys is an obvious target for attack, as is the administrator of the machine.

An Additional Decryption Key is far easier to protect, and it enables you to retain non-repudiation, which is a major advantage inherent to public-key cryptography.

Types of ADKs

PGP offers three types of ADKs: Incoming ADKS, Outgoing ADKs, and PGPdisk ADKs.

Incoming Additional Decryption Keys

An Incoming ADK causes encrypted mail sent to people in your organization to be encrypted to the Incoming ADK as well as to the intended recipient.

When users generate Diffie-Hellman/DSS keys, their keys contain a pointer to the Incoming ADK.

You can select Enforce Incoming Additional Decryption Key as an option in PGPadmin; this causes the PGP client to list the Incoming ADK as another recipient of the encrypted information in the sender's PGP Recipients List. The user is unable to remove the Incoming ADK from the list.

Incoming ADKs can be Diffie-Hellman or RSA keys. RSA Legacy keys cannot be Incoming ADKs.

Outgoing Additional Decryption Keys

The Outgoing ADK causes encrypted mail sent from people in your organization to also be encrypted to the Outgoing ADK.

If you check Enforce Additional Decryption when establishing settings in PGPadmin, all outgoing encrypted mail must be encrypted to the Outgoing ADK.

Outgoing ADKs can be either RSA or Diffie-Hellman keys. One Diffie-Hellman key can serve as both an Incoming and Outgoing ADK.

TIP: Consider whether you want to have multiple Additional Decryption Keys to minimize the risk of having one key become the object of a single point of attack. If you have multiple Additional Decryption Keys, if one is compromised, the rest of your encrypted data that is encrypted to other Additional Decryption Keys is not in danger of being decrypted.

PGPdisk ADKs

As its name implies, a PGPdisk ADK enables you to recover information in a PGPdisk volume.

Additional Decryption Key policy

As security officer, you decide whether your company enforces the use of ADKs. You should have a policy that governs how and when they will be used and should communicate this policy to everyone who will be affected by it. Obviously, this policy should consider employee privacy.

Protecting your Additional Decryption Key

Additional Decryption Keys must be secured both physically and electronically in order to prevent a security breach. If either the Incoming or Outgoing ADK is ever compromised, all encrypted messages sent to users with additional decryption enabled could be decrypted by the attacker.

To prevent unauthorized additional decryption and problems with liability, your organization should enforce a policy that the key should be shared by at least two individuals.

IMPORTANT: Do *not* use ADKs unless you can ensure their security. In an environment that enforces use of an ADK, security of these keys determines the security of all encrypted messages in your entire organization.

Creating Additional Decryption Keys

The ADKs should be the next sets of keys you create after you create the Corporate Signing Key.

If you want separate keys for the Incoming ADK and the Outgoing ADK, you must go through the Key Generation Wizard twice, once for each key.

Key type

Select a key type, either Diffie-Hellman/DSS or RSA. (RSA is an option only if the version of PGP you are using provides RSA support.)

NOTE: RSA Legacy keys cannot be used as Incoming ADKs. Outgoing Additional Decryption Keys can be either Diffie-Hellman, RSA, or RSA Legacy. If users have RSA keys, only another RSA key can be used as the ADK. If users have Diffie-Hellman keys, then you must use another Diffie-Hellman key as the Additional Decryption Keys. If users have both RSA and Diffie-Hellman keys, you will need both types of Additional Decryption Keys.

Diffie-Hellman/DSS

Diffie-Hellman/DSS keys can be used as both Incoming and Outgoing ADKs.

- If your users correspond with people who have PGP Version 5.0 or later, you can take advantage of the new technology and generate a pair of Diffie-Hellman/DSS keys.
- If your users want to be able to exchange email with all PGP users, you should make a pair of RSA keys and a pair of Diffie-Hellman/DSS keys and then use the appropriate pair depending on the version of PGP used by the recipient with whom you are communicating.

RSA

For RSA keys, Outgoing ADKs work by specifying the ADK in a read-only setting on the machine. This means that the ADK is enabled only within the organization. When someone inside the organization encrypts a message to the user, the message will also be encrypted to the ADK. However, encrypted messages from outside users to an internal user are not encrypted to the ADK.

NOTE: If your users correspond with people who are using RSA keys, you will probably want to generate an RSA key pair that is compatible with older versions of the program.

Key size

Your Additional Decryption Keys should be as large as possible.

Select a key size that is 2048 bits or higher. The key size corresponds to the number of bits used to construct your digital key. The larger the key, the less chance that someone will ever be able to crack it, but the longer it takes to perform the decryption and encryption process. Note that RSA keys are limited to 2048 bits in order to maintain compatibility with older versions of PGP.

NOTE: A custom-sized key may take a few minutes to generate, depending on the computer you are using.

Expiration

Once you create your key pairs and have distributed your ADK to your organization, you may continue to use the same keys from that point on. However, under certain conditions, you may want to create a special pair of keys that you plan to use for only a limited period of time. In this case, when the public key expires it can no longer be used to encrypt mail for you but it can still be used to verify your digital signature. Similarly, when your private key expires, it can still be used to decrypt mail that was sent to you before your public key expired but can no longer be used to sign mail for others.

Splitting

Most companies split the Additional Decryption Key and distribute the shares among multiple individuals. PGP implements a secure network connection so that shareholders of a split key do not need to be physically present throughout the reconstitution process.

For more information, see the section on key splitting in the *PGP User's Guide.*

Passphrase

Additional Decryption Keys' passphrases should have a security score of at least 50.

Configuring Lotus Domino Servers E

This appendix tells you how to use the PGP Lotus Domino Server Wizard 7.0 to configure your Domino servers.

Configuring the Lotus Notes plug-in on a Domino Server

If you installed the PGP Lotus Notes email plug-in on your Lotus Notes client machines, you need to run the PGP Lotus Domino Server Wizard 7.0 to configure the Domino server. This wizard lets you configure the Domino server for PGP Lotus Notes plug-in use and configure individual user(s) databases so they can use the plug-in.

Before you run the PGP Lotus Domino Server Wizard 7.0, make sure that you have the following information:

- Name of target Domino server
- Path to your organization's Notes Mail template (if you are creating/refreshing the PGP Notes Plug-in Template on the target server)
- Path(s) of Notes Mail databases to configure (if you plan on running the utility to configure the databases)
- Path to the PGP Notes Plug-in Template on the target server (if you plan to enable specific mail databases with PGP)

To configure the Lotus Notes plug-in on your Domino server:

1. Make sure PGP Desktop Security is installed on each Notes Mail client machine.
2. Start the PGP Lotus Domino Server Wizard 7.0 by double-clicking the **PGPnotesconfig.exe** file on your PGP CD.

   The PGP Notes Plug-in utility searches for the Notes install directory and then displays the path in the Lotus Notes Install Directory dialog box.
3. Click **Next** to continue or **Browse** to change the directory.

   The Lotus Notes Data Directory dialog box appears displaying the path to your Lotus Notes Data directory.

4. Click **Next** to continue or **Browse** to change the directory.

   The PGP Notes Plug-in screen appears.

5. Choose to configure the PGP Lotus Notes plug-in on your Domino server by selecting the corresponding option button, then click **Next**.

   The Domino Server dialog box appears.

6. Enter the name of the Domino server to configure in the **Server** text box, then click **Next**.

   The **Select Task** dialog box appears.

7. Select the task(s) you want to perform:

   Create-Refresh PGP E-mail Template. Select this check box if you are installing the plug-in in your organization's Domino environment for the first time, or you want to update the template already on the target Domino server.

   If you choose this option, the Lotus Notes Mail Template dialog box appears. Enter the path to the Notes Mail template on the target Domino server, then click **Next.**

NOTE: The PGP Notes Plug-in does not change your Notes Mail template in any way. The PGP Plug-in template database works alongside your Notes Mail template within its Domino environment (or at least on those servers hosting PGP-enabled Notes Mail users). This architecture currently requires that all PGP-enabled Notes Mail databases within a Domino environment inherit their design from the **same** Notes Mail template. As a result, enabling PGP in both Notes 4.5 and 4.6 Notes Mail databases within the same Domino environment is not supported.

   PGP Enable specific Notes Mail database(s). Select this checkbox to configure the Notes Mail databases to use the PGP plug-in.

   If you choose this option, the Database Filename(s) dialog box appears. Enter the file paths to the specific Notes Mail database(s) that you want to enable with PGP in the **Database** text box.

   If you have more than one Domino Server in your network to configure, see "Configuring networks with more than one Domino Server" for additional instructions.

8. When the Verify Information screen appears, check the information in the **Current Settings** text box.

9. Click **Next** to begin configuring or **Back** to make changes.
10. Wait while the PGP Notes Plug-in utility begins to configure the server.

    Before the configuration is complete, you may be prompted to enter your Lotus Notes password.
11. Enter your Lotus Notes passphrase, then click **OK**.

Configuring networks with more than one Domino Server

To successfully configure a multiple Domino server environment using the PGP Lotus Domino Server Wizard 7.0, follow the instructions outlined on page 101 but only run the Create/Refresh PGP Plug-in Template task on one server within the target Domino environment.

Do not run the task on the other server(s) hosting Notes Mail databases. Instead, before running the utility on that or any other Domino server, replicate the **PGP Plugin Template.nsf** database (which is deposited during the install onto the first server) to any other servers hosting Notes Mail databases that need to be PGP enabled.

Adhering to this technique allows you to leverage standard Domino technology such that design changes or updates to the PGP Plug-in Template can be made in one place and then migrated automatically throughout your Domino environment (utilizing standard Domino replication and the servers “Design” add-in task).

Network Associates Support Services

F

Adding value to your PGP product

Choosing PGP Security software helps to ensure that the critical technology you rely on functions smoothly and effectively. Taking advantage of a Network Associates support plan extends the protection you get from your software by giving you access to the expertise you need to install, monitor, maintain and upgrade your system with the latest Network Associates technology. With a support plan tailored to your needs, you can keep your system or your network working dependably in your computing environment for months or years to come.

Network Associates support plans come under two general headings. If you are a corporate customer, you can choose from four levels of extended support under the Network Associates Corporate PrimeSupport* program. If you are a home user, you can choose a plan geared toward your needs from the Home User PrimeSupport program.

PrimeSupport options for corporate customers

The Corporate PrimeSupport program offers these four support plans:

- PrimeSupport KnowledgeCenter plan
- PrimeSupport Connect plan
- PrimeSupport Priority plan
- PrimeSupport Enterprise plan

Each plan has a range of features that provide you with cost-effective and timely support geared to meet your needs. The following sections describe each plan in detail.

The PrimeSupport KnowledgeCenter plan

The PrimeSupport KnowledgeCenter plan gives you access to an extensive array of technical support information via a Network Associates online knowledge base, and download access to product upgrades from the Network Associates Web site. If you purchased your Network Associates product with a subscription license, you receive the PrimeSupport KnowledgeCenter plan as part of the package, for the length of your subscription term.

If you purchased a perpetual license for your Network Associates product, you can purchase a PrimeSupport KnowledgeCenter plan for an annual fee.

To receive your KnowledgeCenter password or to register your PrimeSupport agreement with Network Associates, visit:

http://www.nai.com/asp_set/support/introduction/default.asp

Your completed form will go to the Network Associates Customer Service Center. You must submit this form before you connect to the PrimeSupport KnowledgeCenter site.

With the PrimeSupport KnowledgeCenter plan, you get:

- Unrestricted, 24-hour-per-day online access to technical solutions from a searchable knowledge base within the Network Associates Web site
- Electronic incident and query submission
- Technical documents, including user's guides, FAQ lists, and release notes
- Online data file updates and product upgrades

The PrimeSupport Connect plan

The PrimeSupport Connect plan gives you telephone access to essential product assistance from experienced technical support staff members. With this plan, you get:

- In North America, unlimited toll-free telephone access to technical support from Monday through Friday, 8 A.M. to 8 P.M. Central Time
- In Europe, the Middle East, and Africa, unlimited telephone access to technical support, at standard long-distance or international rates, Monday through Friday, from 9 A.M. to 6 P.M. local time
- In the Asia-Pacific region, unlimited toll-free, telephone access to technical support, Monday through Friday, from 8 A.M. to 6 P.M. AEST
- In Latin America, unlimited telephone access to technical support, at standard long-distance or international rates, Monday through Friday, from 9 A.M. to 5 P.M. Central Time
- Unrestricted, 24-hour-per-day online access to technical solutions from a searchable knowledge base within the Network Associates Web site
- Electronic incident and query submission
- Technical documents, including user's guides, FAQ lists, and release notes
- Data file updates and product upgrades via the Network Associates Web site

The PrimeSupport Priority plan

The PrimeSupport Priority plan gives you round-the-clock telephone access to essential product assistance from experienced Network Associates technical support staff members. You can purchase the PrimeSupport Priority plan on an annual basis when you purchase a Network Associates product, either with a subscription license or a one-year license.

The PrimeSupport Priority plan has these features:

- In North America, unlimited toll-free telephone access to technical support from Monday through Friday, 8 A.M. to 8 P.M. Central Time
- In Europe, the Middle East, and Africa, unlimited telephone access to technical support, at standard long-distance or international rates, Monday through Friday, from 9 A.M. to 6 P.M. local time
- In the Asia-Pacific region, unlimited toll-free, telephone access to technical support, Monday through Friday, from 8 A.M. to 6 P.M. AEST
- In Latin America, unlimited telephone access to technical support, at standard long-distance or international rates, Monday through Friday, from 9 A.M. to 5 P.M. Central Time
- Priority access to technical support staff members during regular business hours
- Responses within one hour for urgent issues that happen outside regular business hours, including those that happen during weekends and local holidays
- Unrestricted, 24-hour-per-day online access to technical solutions from a searchable knowledge base within the Network Associates Web site
- Electronic incident and query submission
- Technical documents, including user's guides, FAQ lists, and release notes
- Data file updates and product upgrades via the Network Associates Web site

The PrimeSupport Enterprise plan

The PrimeSupport Enterprise plan gives you round-the-clock, personalized, proactive support from an assigned technical support engineer. You'll enjoy a relationship with a support professional who is familiar with your Network Associates product deployment and support history, and who will call you at an interval you designate to verify that you have the knowledge you need to use and maintain Network Associates products.

By calling in advance, your PrimeSupport Enterprise representative can help to prevent problems before they occur. If, however, an emergency arises, the PrimeSupport Enterprise plan gives you a committed response time that assures you that help is on the way. You may purchase the PrimeSupport Enterprise plan on an annual basis when you purchase a Network Associates product, either with a subscription license or a one-year license.

With the PrimeSupport Enterprise plan, you get:

- Unlimited, toll-free telephone access to an assigned technical support engineer on a 24-hour-per-day, seven-day-per-week basis, including during weekends and local holidays.

> **NOTE:** The availability of toll-free telephone support varies by region and is not available in some parts of Europe, the Middle East, Africa, and Latin America.

- Proactive support contacts from your assigned support engineer via telephone or e-mail, at intervals you designate
- Committed response times from your support engineer, who will respond to pages within half an hour, to voice mail within one hour, and to e-mail within four hours
- Assignable customer contacts, which allow you to designate five people in your organization who your support engineer can contact in your absence
- Optional beta site status, which gives you access to the absolute latest Network Associates products and technology
- Unrestricted, 24-hour-per-day online access to technical solutions from a searchable knowledge base within the Network Associates Web site
- Electronic incident and query submission
- Technical documents, including user's guides, FAQ lists, and release notes
- Online data file updates and product upgrades

Ordering a corporate PrimeSupport plan

To order any PrimeSupport plan, contact your sales representative, or

- In North America, call Network Associates at (972) 308-9960, Monday through Friday from 8 A.M. to 7 P.M. Central Time. Press 3 on your telephone keypad for sales assistance.
- In Europe, the Middle East, and Africa, contact your local Network Associates office.

Table 9-1. Corporate PrimeSupport Plans at a Glance

Plan Feature	Knowledge Center	Connect	Priority	Enterprise
Technical support via website	Yes	Yes	Yes	Yes
Software updates	Yes	Yes	Yes	Yes
Technical support via telephone	—	Monday–Friday North America: 8 a.m.–8 p.m. CT Europe, Middle East, Africa: 9 a.m.-6 p.m. local time Asia-Pacific: 8 a.m.-6 p.m. AEST Latin America: 9 a.m.-5 p.m. CT	Monday–Friday, after hours emergency access North America: 8 a.m.–8 p.m. CT Europe, Middle East, Africa: 9am-6pm local time Asia-Pacific: 8 a.m.-6 p.m. AEST Latin America: 9 a.m.-5 p.m. CT	Monday–Friday, after hours emergency access North America: 8 a.m.–8 p.m. CT Europe, Middle East, Africa: 9am-6pm local time Asia-Pacific: 8 am-6 p.m. AEST Latin America: 9 a.m.-5 p.m. CT
Priority call handling	—	—	Yes	Yes
After-hours support	—	—	Yes	Yes
Assigned support engineer	—	—	—	Yes
Proactive support	—	—	—	Yes
Designated contacts	—	—	—	At least 5
Response charter	E-mail within one business day	Calls answered in 3 minutes, response in one business day	Within 1 hour for urgent issues after business hours	After hours pager: 30 minutes Voicemail: 1 hour E-mail: 4 hours

The PrimeSupport options described in the rest of this chapter are available only in North America. To find out more about PrimeSupport, Training and Consultancy options available outside North America, contact your regional sales office.

PrimeSupport options for home users

If you purchased your Network Associates product through a retail vendor or from the Network Associates Web site, you also receive support services as part of your purchase. The specific level of support you receive depends on which product you purchased. Services you might receive include:

- For anti-virus software products, free data file updates for the life of your product via the Network Associates Web site, your product's automatic update feature, or the SecureCast service. You can also update your data files by using your web browser to visit:

  http://www.nai.com/asp_set/download/dats/find.asp

- Free program (executable file) upgrades for one year via the Network Associates Web site. If you purchased a deluxe version of a Network Associates product, you receive free program upgrades for two years. You can also upgrade your software by using your Web browser to visit:

  http://www.nai.com/asp_set/download/upgrade/login.asp

- Free 24-hour-per-day, seven-days-per-week access to online or electronic support through the Network Associates voice and fax system, the Network Associates Web site, and through such other electronic services as America Online and CompuServe.

  To contact Network Associates electronic services

  – Call the automated voice and fax system at (408) 346-3414

  – Visit the Network Associates Web site at http://support.nai.com

  – Visit the Network Associates CompuServe forum at GO NAI

  – Visit Network Associates on America Online: keyword MCAFEE

- Free access to the PrimeSupport KnowledgeBase: online access to technical solutions from a searchable knowledge base, electronic incident submission, and technical documents such as user's guides, FAQs, and release notes. Visit the KnowledgeBase at:

  http://www.nai.com/asp_set/support/technical/intro.asp

- Thirty days of complimentary technical support from a Network Associates support technician during regular business hours, Monday through Friday from 9 A.M. to 5:30 P.M. Central Time. Your 30-day support period starts from the date of your first support phone call for all Network Associates products. To contact technical support, call:

  (972) 855-7044

If you need additional support, Network Associates offers a variety of other support plans that you can purchase either with your Network Associates product or after your complimentary 30-day support period expires. These include:

NOTE: The support plans described here are available only in North America—contact your regional sales representative to learn about local support options.

- **Small Office/Home Office Annual Plan.** This plan gives you unlimited toll-free access to technical support during regular business hours, Monday through Friday from 9 A.M. to 5 P.M. Central Time.

- **Pay-Per-Incident Plan.** This plan gives you support on a per-incident basis during business hours, Monday through Friday from 7 A.M. to 6 P.M. Pacific Time. You call a toll-free number, use a credit card to take care of the transaction, and get transferred to the technical support team within minutes. Your cost will be $35 per incident.

All McAfee products	(800) 950-1165

- **Pay-Per-Minute Plan.** This plan gives you support only when you need it. You get 900-number access to technical support staff members on a priority basis to minimize your hold time. Your first two minutes are free.

All products except PGP encryption software	(900) 225-5624

- **Online Upgrades Plan.** This plan gives you the convenience of automatic access to product upgrades via Network Associates online or electronic services.

- **Quarterly Disk/CD Plan.** This plan gives you automatic quarterly delivery of upgrade disks or CDs if you cannot obtain product upgrades online. This service is available for McAfee VirusScan and NetShield software only.

How to reach international home user support

The following table lists telephone numbers for technical support in several international locations. The specific costs, availability of service, office hours and plan details might vary from location to location. Consult your sales representative or a regional Network Associates office for details.

Country or Region	Phone Number*	Bulletin Board System
Germany	+49 (0)69 21901 300	+49 89 894 28 999
France	+33 (0)1 4993 9002	+33 (0)1 4522 7601
United Kingdom	+44 (0)171 5126099	+44 1344-306890
Italy	+31 (0)55 538 4228	+31 (0)20 586 6128
Netherlands	+31 (0)55 538 4228	+31 (0)20 586 6128
Europe	+31 (0)55 538 4228	+31 (0)20 688 5521
Latin America	+55-11-3794-0125	+55-11-5506-9100

* long distance charges might apply

Ordering a PrimeSupport plan for home users

To order the PrimeSupport Small Office/Home Office Annual Plan, Pay-Per-Incident Plan, Pay-Per-Minute Plan, Online Upgrades Plan, or Quarterly Disk/CD Plan for your Network Associates products:

- In North America, call Network Associates Customer Service at (972) 855-7044
- In international locations, contact the Network Associates retail technical support center closest to your location for more information. Some support options may not be available in some locations.

Network Associates consulting and training

The Network Associates Total Service Solutions program provides you with expert consulting and comprehensive education that can help you maximize the security and performance of your network investments. The Total Service Solutions program includes the Network Associates Professional Consulting arm and the Total Education Services program.

Professional Services

Network Associates Professional Services is ready to assist you during all stages of your network growth, from planning and design, through implementation, and with ongoing management. Network Associates consultants provide an expert's independent perspective that you can use as a supplemental resource to resolve your problems.

You'll get help integrating Network Associates products into your environment, along with troubleshooting assistance or help in establishing baselines for network performance. Network Associates consultants also develop and deliver custom solutions to help accomplish your project goals—from lengthy, large-scale implementations to brief problem-solving assignments.

Jumpstart Services

For focused help with specific problem resolution or software implementation issues, Network Associates offers a Jumpstart Service that gives you the tools you need to manage your environment. This service can include these elements:

- **Installation and optimization.** This service brings a Network Associates consultant onsite to install, configure, and optimize your new Network Associates product and give basic operational product knowledge to your team.
- **Selfstart knowledge.** This service brings a Network Associates consultant onsite to help prepare you to perform your new product implementation on your own and, in some cases, to install the product.
- **Proposal Development.** This service helps you to evaluate which processes, procedures, hardware and software you need before you roll out or upgrade Network Associates products, after which a Network Associates consultant prepares a custom proposal for your environment.

Network consulting

Network Associates consultants provide expertise in protocol analysis and offer a vendor-independent perspective to recommend unbiased solutions for troubleshooting and optimizing your network. Consultants can also bring their broad understanding of network management best practices and industry relationships to speed problem escalation and resolution through vendor support.

You can order a custom consultation to help you plan, design, implement, and manage your network, which can enable you to assess the impact of rolling out new applications, network operating systems, or internetworking devices.

To learn more about the options available:

- Contact your regional sales representative.
- In North America, call Network Associates at (972) 308-9960, Monday through Friday from 8 A.M. to 7 P.M. Central Time.
- Visit the Network Associates Web site at:

  http://www.nai.com/asp_set/services/introduction/default.asp

Total Education Services

Network Associates Total Education Services builds and enhances the skills of all network professionals through practical, hands-on instruction. The Total Education Services technology curriculum focuses on network fault and performance management and teaches problem-solving at all levels. Network Associates also offers modular product training so that you understand the features and functionality of your new software.

You can enroll in Total Education Services courses year-round at Network Associates educational centers, or you can learn from customized courses at your location. All courses follow educational steps along a learning path that takes you to the highest levels of expertise. Network Associates is a founding member of the Certified Network Expert (CNX) consortium.

To learn more about these programs:

- Contact your regional sales representative.
- Call Network Associates Total Education Services at (800) 395-3151 Ext. 2670 (for private course scheduling) or (888) 624-8724 (for public course scheduling).
- Visit the Network Associates Web site at:

  http://www.nai.com/asp_set/services/educational_services/education_intro.asp

Glossary

Additional recipient request key

a special key whose presence indicates that all messages encrypted to its associated base key should also be automatically encrypted to it. Sometimes referred to by its marketing term, *additional decryption key.*

Algorithm (encryption)

a set of mathematical rules (logic) used in the processes of encryption and decryption.

Algorithm (hash)

a set of mathematical rules (logic) used in the processes of message digest creation and key/signature generation.

API (Application Programming Interface)

provides the means to take advantage of software features, allowing dissimilar software products to interact upon one another.

Asymmetric keys

a separate but integrated user key-pair, comprised of one public key and one private key. Each key is one way, meaning that a key used to encrypt information can not be used to decrypt the same data.

Authentication

to prove genuine by corroboration of the identity of an entity.

CA (Certificate Authority)

a trusted third party (TTP) who creates certificates that consist of assertions on various attributes and binds them to an entity and/or to their public key.

Certificate (digital certificate)

an electronic document attached to a public key by a trusted third party, which provides proof that the public key belongs to a legitimate owner and has not been compromised.

Cipher text

the result of manipulating either characters or bits via substitution, transposition, or both.

Clear text

characters in a human readable form or bits in a machine-readable form (also called *plain text*).

Corporate Signing Key (CSK)
a key pair used to prove that digital certificates, information, products, and so on have been validated by an authority acting on behalf of the company. The Corporate Signing Key is primarily used for signing, but can also be used for encryption. It is typically held by the Corporate Security Officer alone, or split into multiple shares. Some examples of uses for a Corporate Signing Key include signing employees' digital certs or keys, softcopies of legal documents, and software produced by your company. Because the Corporate Signing Key is used to validate all keys in your organization as well as provide authentication for other data as well, it is vital that this key is never compromised, lest someone else pretend to act in the company's name.

CRL (Certificate Revocation List)
an online, up-to-date list of previously issued certificates that are no longer valid.

Cryptanalysis
the art or science of transferring cipher text into plain text without initial knowledge of the key used to encrypt the plain text.

Cryptography
the art and science of creating messages that have some combination of being private, signed, unmodified with non-repudiation.

Cryptosystem
a system comprised of cryptographic algorithms, all possible plain text, cipher text, and keys.

Data integrity
a method of ensuring information has not been altered by unauthorized or unknown means.

Decryption
the process of turning cipher text back into plain text.

Dictionary attack
a calculated brute force attack to reveal a password by trying obvious and logical combinations of words.

Diffie-Hellman
the first public key algorithm, invented in 1976, using discrete logarithms in a finite field.

Diffie-Hellman/DSS keys

one of the three types of PGP keys you can create (the other two are RSA and RSA Legacy).
Diffie-Hellman/DSS keys let you take advantage of many PGP key features, including Additional Decryption Key (ADK), designated revoker, multiple encryption subkeys, and photo ID.

Digital signature

an electronic identification of a person or thing created by using a public key algorithm. Intended to verify to a recipient the integrity of data and identity of the sender of the data.

Encryption

the process of disguising a message in such a way as to hide its substance.

Fingerprint

a unique identifier for a key that is obtained by hashing specific portions of the key data.

Firewall

a combination of hardware and software that protects the perimeter of the public/private network against certain attacks to ensure some degree of security.

Hierarchical trust

a graded series of entities that distribute trust in an organized fashion, commonly used in ANSI X.509 issuing certifying authorities.

Integrity

assurance that data is not modified (by unauthorized persons) during storage or transmittal.

Key

a means of gaining or preventing access, possession, or control represented by any one of a large number of values.

Key length

the number of bits representing the key size; the longer the key, the stronger it is.

Key management

the process and procedure for safely storing and distributing accurate cryptographic keys; the overall process of generating and distributing cryptographic key to authorized recipients in a secure manner.

Key splitting

a process for dividing portions of a single key between multiple parties, none having the ability to reconstruct the whole key.

LDAP (Lightweight Directory Access Protocol)

a simple protocol that supports access and search operations on directories containing information such as names, phone numbers, and addresses across otherwise incompatible systems over the Internet.

Meta-introducer

a trusted introducer of trusted introducers.

MIME (Multipurpose Internet Mail Extensions)

a freely available set of specifications that offers a way to interchange text in languages with different character sets, and multimedia email among many different computer systems that use Internet mail standards.

Non-repudiation

preventing the denial of previous commitments or actions.

Passphrase

an easy-to-remember phrase used for better security than a single password; key crunching converts it into a random key.

Password

a sequence of characters or a word that a subject submits to a system for purposes of authentication, validation, or verification.

Pretty Good Privacy (PGP)

an application and protocol (RFC 1991) for secure e-mail and file encryption developed by Phil R. Zimmermann. Originally published as Freeware, the source code has always been available for public scrutiny. PGP uses a variety of algorithms, like IDEA, RSA, DSA, MD5, SHA-1 for providing encryption, authentication, message integrity, and key management. PGP is based on the “Web-of-Trust” model and has worldwide deployment.

PGP/MIME

an IETF standard (RFC 2015) that provides privacy and authentication using the Multipurpose Internet Mail Extensions (MIME) security content types described in RFC1847, currently deployed in PGP 5.0 and later versions.

PKI (Public Key Infrastructure)

a widely available and accessible certificate system for obtaining an entity's public key with some degree of certainty that you have the "right" key and that it has not been revoked.

Plain text (or clear text)

the human readable data or message before it is encrypted.

Pseudo-random number

a number that results from applying randomizing algorithms to input derived from the computing environment, for example, mouse coordinates. See *random number*.

Private key

the privately held "secret" component of an integrated asymmetric key pair, often referred to as the decryption key.

Public key

the publicly available component of an integrated asymmetric key pair often referred to as the encryption key.

Random number

an important aspect to many cryptosystems, and a necessary element in generating a unique key(s) that are unpredictable to an adversary. True random numbers are usually derived from analog sources, and usually involve the use of special hardware.

Revocation

retraction of certification or authorization.

RSA

a public-key cryptosystem developed by MIT professors Ronald L. Rivest, Adi Shamir, and Leonard M. Adleman in 1977 in an effort to help ensure Internet security.

RSA keys

one of the three types of PGP keys you can create (the other two are Diffie-Hellman/DSS and RSA Legacy). RSA keys support for PGP features ADKs, designated revoker, multiple encryption subkeys, and photo ID. RSA keys are only fully compatible with PGP versions 7.0 and above and other open PGP applications.

RSA Legacy keys

one of the three types of PGP keys you can create (the other two are Diffie-Hellman/DSS and RSA). RSA Legacy keys are only used for communication with PGP users using older versions of PGP. RSA Legacy keys do not support many of PGP key features.

Secret key

either the “private key” in public key (asymmetric) algorithms or the “session key” in symmetric algorithms.

Self-signed key

a public key that has been signed by the corresponding private key for proof of ownership.

S/MIME (Secure Multipurpose Mail Extension)

a proposed standard developed by Deming software and RSA Data Security for encrypting and/or authenticating MIME data. S/MIME defines a format for the MIME data, the algorithms that must be used for interoperability (RSA, RC2, SHA-1), and the additional operational concerns such as ANSI X.509 certificates and transport over the Internet.

Trust

a firm belief or confidence in the honesty, integrity, justice, and/or reliability of a person, company, or other entity.

TTP (Trusted Third-Party)

a responsible party in which all participants involved agree upon in advance, to provide a service or function, such as certification, by binding a public key to an entity, time-stamping, or key-escrow.

Validation

a means to provide timeliness of authorization to use or manipulate information or resources.

Verification

to authenticate, confirm, or establish accuracy.

VPN (Virtual Private Network)

allows private networks to span from the end-user, across a public network (Internet) directly to the Home Gateway of choice, such as your company's Intranet.

Web of Trust

a distributed trust model used by PGP to validate the ownership of a public key where the level of trust is cumulative based on the individual's knowledge of the "introducers."

X.509

an ITU-T digital certificate that is a recognized electronic document used to prove identity and public key ownership over a communication network. It contains the issuer's name, the user's identifying information, and the issuer's digital signature, as well as other possible extensions in version 3.

Index