PGP CORPORATION

PGP 8.0

Administrator's Guide

Version Information

PGP 8.0 Administrator's Guide. Released November 2002.

Copyright Information

Trademark Information

Licensing and Patent Information

The IDEA cryptographic cipher described in U.S. patent number 5,214,703 is licensed from Ascom Tech AG. The CAST encryption algorithm is licensed from Northern Telecom, Ltd. PGP Corporation may have patents and/or pending patent applications covering subject matter in this software or its documentation; the furnishing of this software or documentation does not give you any license to these patents.

Acknowledgments

The compression code in PGP is by Mark Adler and Jean-Loup Gailly, used with permission from the free Info-ZIP implementation. This software is based in part on the work of the Independent JPEG Group. Soft TEMPEST font courtesy of Ross Anderson and Marcus Kuhn. Biometric word list for fingerprint verification courtesy of Patrick Juola.

Export Information

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

Limitations

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

About PGP Corporation

PGP Corporation, the recognized worldwide leader in secure messaging and data storage, builds products that allow corporations to ensure confidential customer and individual information remains secure. Over the last 10 years, PGP technology has developed a global reputation for enabling open, trusted, and highly reliable security products. PGP has thousands of corporate/government users and millions of individual users worldwide, including many of the world's largest and most security sensitive enterprises, government agencies, individuals, and cipher experts. Contact PGP Corporation at www.pgp.com or toll free at 866.747.5483 (866.PGP.LIVE).

Table of Contents

Introduction

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.

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.*

What is PGP Admin?

PGP Admin is intended for use by a network administrator—the individual (presumably you) responsible for implementing an organization's network security. You install PGP and then PGP Admin on a Windows or Macintosh machine (the PGP administrative machine). Then, you use PGP Admin as a tool for administering PGP for your organization.

Note: PGP Admin will not work on your computer unless you have purchased a PGP Enterprise license.

You use PGP Admin to do the following:

- You can establish the settings you want your PGP users to have, including regular PGP options and PGP Admin-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 PGP Admin.
- 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 PGP Admin

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

Who should read this guide

This guide is for the person(s) who will be implementing and maintaining PGP throughout your organization. We refer to you throughout this document 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 was installed when PGP was installed.

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.** 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.
- **PGP Admin.** PGP Admin is a software application installed on an administrative machine and used by a network administrator to select which features of PGP to deploy. PGP Admin provides robust corporate manageability features including complete product pre-configuration with optional lockdown capabilities, silent install, and remote product re-configuration capabilities. PGP Admin 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 Software Developer's Kit.** The PGP 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.

Using this Guide

The chapters and appendices in this Guide include:

- Chapter 1, Installation, tells you how to install PGP Admin onto your PGP administrative machine.
- Chapter 2, The Implementation Process, is an overview of the PGP and PGP Admin implementation process.
- Chapter 3, A Quick Tour of PGP Admin, shows and describes the screens you will see while using the PGP Admin application; it also tells you how to start PGP Admin 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 PGP Admin’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 PGP Admin.
- 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 PGP Admin 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 Notes in Your Network, tells you how to use the PGP Lotus Domino Server Wizard 7.0 to configure your Domino servers.

There is also a Glossary and an Index.

Recommended readings

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

The history of cryptography

- *The Code Book: The Evolution of Secrecy from Mary, Queen of Scots, to Quantum Cryptography*, Simon Singh, Doubleday & Company, Inc., 1999, ISBN 0-385-49531-5.
- *The Codebreakers: The Story of Secret Writing*, David Kahn, Simon & Schuster Trade, 1996, ISBN 0-684-83130-9 (updated from the 1967 edition). This book is a history of codes and code breakers from the time of the Egyptians to the end of WWII. Kahn first wrote it in the sixties; this is the revised edition. This book won't teach you anything about how cryptography is done, but it has been the inspiration of the whole modern generation of cryptographers.
- Aegean Park Press, www.aegeanparkpress.com. The Aegean Park Press publishes a number of interesting historic books ranging from histories (such as "The American Black Chamber," an exposé of U.S. cryptography during and after WWI) to declassified government documents.

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 Corporation, 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 IETF OpenPGP specification, written by Jon Callas, Lutz Donnerhacke, Hal Finney, and Rodney Thayer.
- www.ietf.org/rfc/rfc3156.txt. The IETF OpenPGP/MIME specification, written by Michael Elkins, Dave del Torto, Raph Levien, and Thomas Roessler.

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.
- *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, privacy.org. Great information resource about privacy issues.
- www.cdt.org, Center for Democracy and Technology.
- www.philzimmermann.com, 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.
- *Crypto: How the Code Rebels Beat the Government--Saving Privacy in the Digital Age*, Steven Levy, Penguin USA, 2001; ISBN 0140244328.

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. Available on the Web at www.wilyhacker.com.
- *Network Security: Private Communication in a Public World*, Second Edition, Charles Kaufman, Radia Perlman, and Mike Speciner, Pearson Education, 2002; ISBN: 0130460192. This book describes many network protocols, including Kerberos, IPsec, SSL, and others. It includes some basics of cryptography and works up from there to show how actual systems are constructed.

Symbols

Notes, Cautions, and Warnings are used in the following ways.

Notes are extra, but important, information.

Note: A Note adds important information, but you could still use the product if you didn't have that information.

Cautions indicate the possibility of loss of data or minor damage to equipment.

Caution: A Caution tells you about a situation where there is the potential for loss of data or minor damage to equipment. Pay attention to Cautions.

Warnings indicate the possibility of significant damage to equipment or injury to human beings.

Warning: A Warning means that your equipment may be damaged or someone could be injured. Please take Warnings seriously.

1 Installation

This chapter describes how to install PGP Admin for Windows and Mac OS X systems. It also lists the system requirements for each platform.

Note

Note: On Windows systems, if you have PGP and PGP Admin installed, and then you uninstall PGP, PGP Admin will be uninstalled as well.

PGP Admin system requirements

Windows

To install PGP Admin on a Windows system, you must have:

- Pentium 166 or compatible processor
- Windows 98, Windows NT 4.0 (Service Pack 6a), Windows 2000 (Service Pack 3), or Windows XP (Service Pack 1)
- 32 MB RAM
- 32 MB hard disk space

Macintosh

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

- Power Mac G3, G4, G4 Cube; iMac; PowerBook G3, G4; iBook; or eMac
- Mac OS X 10.2.1 or greater
- 128 MB of RAM (required for Mac OS X)
- 15 MB of available hard disk space

Note

Note: The Macintosh OS X version of PGPadmin is not available with this release. If you need to use PGPadmin on a Macintosh system, use Mac OS 9 and PGP Corporate Desktop 7.2.

Installing PGP Admin on a Windows system

You can install PGP Admin from a CD or from a download from the Web.

Note: You can't install PGP Admin unless PGP is already installed on your PGP administrative machine. Also, the versions of PGP and PGP Admin **must** be the same.

To install PGP Admin on a Windows system:

1. Exit all programs currently running on your computer.
2. Begin the installation:
    - **To install from a CD.** Insert the CD into the drive. The installer automatically opens. Follow the on-screen instructions.
    - **To install from the Web.** Download the install program and double-click it to open the installer. Follow the on-screen instructions.

Note: You don't have to restart your computer to begin using PGP Admin.

Installing PGP Admin on a Mac OS X system

You can install PGP Admin from a CD or from a download from the Web.

Note: You can't install PGP Admin unless PGP is already installed on the administrative machine. Also, the versions of PGP and PGP Admin **must** be the same.

To install PGP Admin on a Mac OS X system:

1. Exit all programs currently running on your computer.
2. Begin the installation:
    - **To install from a CD.** Insert the CD into the drive. Double click the PGP Admin package. Follow the on-screen instructions.
    - **To install from the Web.** Download the install program and double-click it to open the installer. Follow the on-screen instructions.

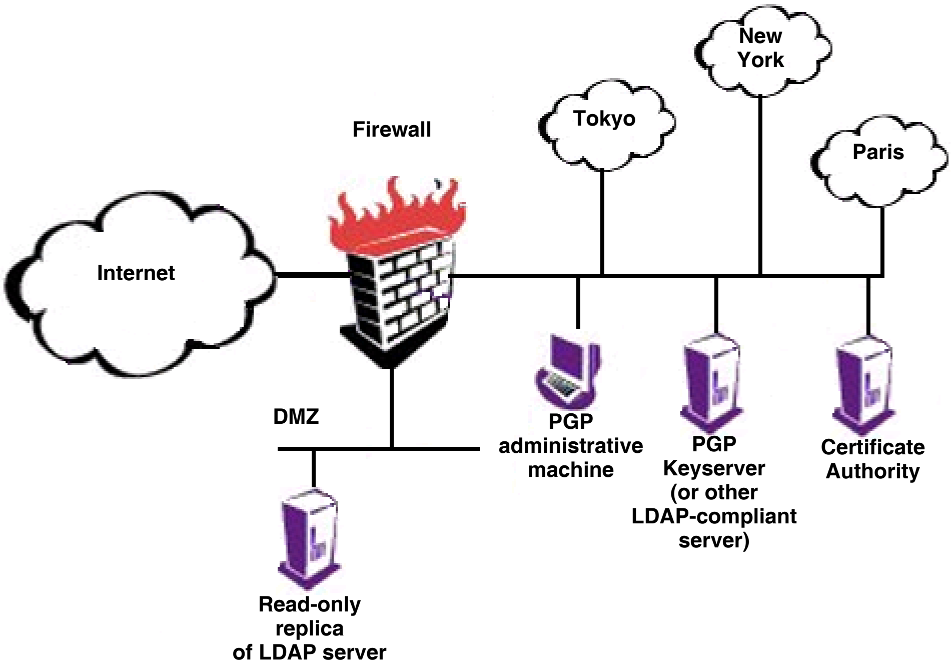
Note: You don't have to restart your computer to begin using PGP Admin.

2 The Implementation Process

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

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)
Certificate Authority
Read-only replica of LDAP server

The components of the corporate network shown above 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 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 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. By convention, this server should be named "keys.company.com" where "company.com" is your organization's domain name. This will make it easier for external entities to correspond with your organization securely.
- **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 that houses PGP and PGP Admin. From this machine you can control the PGP settings of your corporate 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 corporate Certificate Authority.** Your system for handling the company's certificate management requirements. This machine is only necessary if you plan to deploy an X.509 PKI as part of your PGP deployment.

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 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 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 PGP Admin. 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 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.

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

Install PGP and PGP Admin on your PGP administrative machine. For detailed installation instructions, refer to Chapter 1, Installation.

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

Your PGP Keyserver (also called a Certificate 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 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) and/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).

Caution: Your Corporate Signing 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 PGP Admin, 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 PGP Admin.

For more information about X.509 certificates, 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.

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 PGP Admin.

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

7. 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 more information, refer to the *PGP User's Guide*.

8. Establish the PGP Admin 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 PGP Admin 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 PGP Admin; 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 PGP Admin as described in "The Keys panel" on page 17.

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.

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

Using the Access Panel within PGP Admin, 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."

10. Create the PGP client installer program using PGP Admin.

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

11. 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 Lotus Domino Server wizard 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 Notes in your Network," for detailed instructions.

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

For detailed instructions, refer to the PGP Keyserver documentation and the documentation that came with your PKI.

13. 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.

14. 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 PGP Admin are correct.

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

15. 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.

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

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

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

Distribute the PGP client installer program 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.

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

---

3 A Quick Tour of PGP Admin

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

Starting PGP Admin

Use the appropriate procedure to start PGP Admin.

To start PGP Admin on a Windows computer:

1. Click **Start** —> **Programs** —> **PGP** —> **PGPadmin**.

   The PGP Admin screen appears.

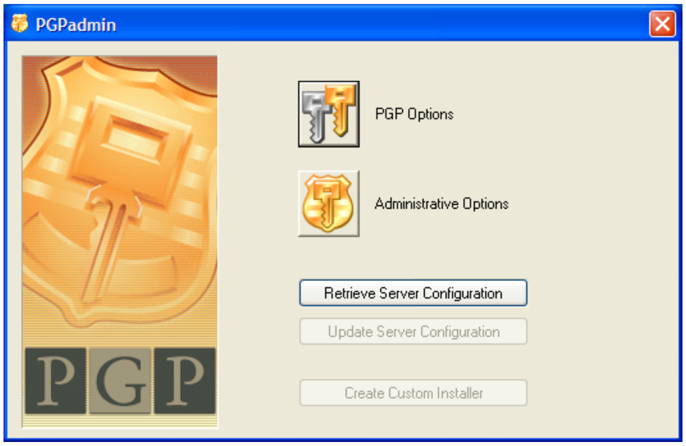
To start PGP Admin on Mac OS X:

1. Navigate to your Applications folder and open PGP Admin.

   The PGP Admin screen appears.

The PGP Admin screen

The PGP Admin screen provides access to all PGP Admin functions.



The buttons on the PGP Admin screen are:

- **PGP Options**. This button displays the PGP Options screen, which you use to configure the PGP settings 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**. This button displays the Administrative Options screen, which you use to configure PGP Admin settings.

  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 PGP Admin, 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 or save the settings file to it. To do this, go to Administrative Options 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.

  For more information about this button, refer to Chapter 9, Updating PGP Admin 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 PGP Admin 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 PGP Admin

To exit from PGP Admin:

- On Windows, click the **Close** button (the **x** in the upper right corner) on the PGP Admin screen.
- On a Mac OS X, pull down the **PGPadmin** menu and select **Quit PGPadmin**.

4

Setting PGP Options

This chapter explains how to set the PGP options 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 PGP Admin?

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.

Note: 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 PGP Admin?

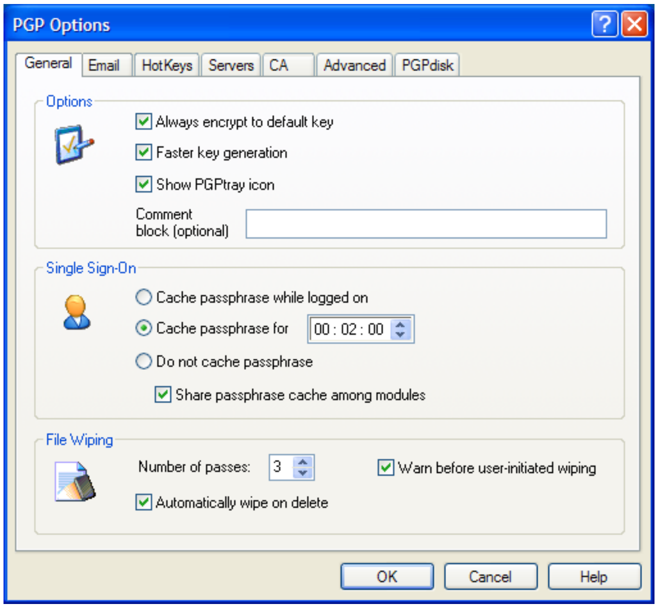
To set PGP options/preferences:

1. Open PGP Admin.

   The PGP Admin screen appears.

2. Click **PGP Options**.

The PGP Options screen appears.



☑ Always encrypt to default key
☑ Faster key generation
☑ Show PGPtray icon
Comment block (optional)

○ Cache passphrase while logged on
● Cache passphrase for 00 : 02 : 00
○ Do not cache passphrase
☑ Share passphrase cache among modules

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 PGP Admin screen appears.

5

Setting Administrative Options

This chapter tells you about the PGP administrative options, available only through PGP Admin, and explains how to set them.

What are PGP Admin administrative options?

The PGP Admin 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 PGP Admin administrative options?

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

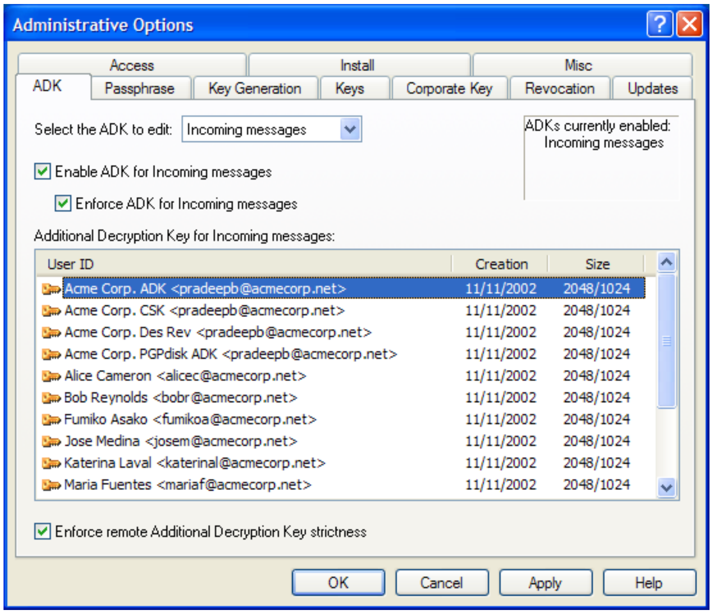
To display the Administrative Options screen:

1. Open PGP Admin.

   The PGP Admin screen appears.

2. Click **Administrative Options**.

The Administrative Options 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
Acme Corp. ADK <pradeepb@acmecorp.net>	11/11/2002	2048/1024
Acme Corp. CSK <pradeepb@acmecorp.net>	11/11/2002	2048/1024
Acme Corp. Des Rev <pradeepb@acmecorp.net>	11/11/2002	2048/1024
Acme Corp. PGPdisk ADK <pradeepb@acmecorp.net>	11/11/2002	2048/1024
Alice Cameron <alicec@acmecorp.net>	11/11/2002	2048/1024
Bob Reynolds <bobr@acmecorp.net>	11/11/2002	2048/1024
Fumiko Asako <fumikoa@acmecorp.net>	11/11/2002	2048/1024
Jose Medina <josem@acmecorp.net>	11/11/2002	2048/1024
Katerina Laval <katerinal@acmecorp.net>	11/11/2002	2048/1024
Maria Fuentes <mariaf@acmecorp.net>	11/11/2002	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 PGP Admin 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.

---

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

   The PGP Admin screen appears again.

Complete information about each option on the panels of the Administrative Options 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.

Caution: 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.

Note: 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:

- someone encrypts data to a user in your organization
- an internal user encrypts data

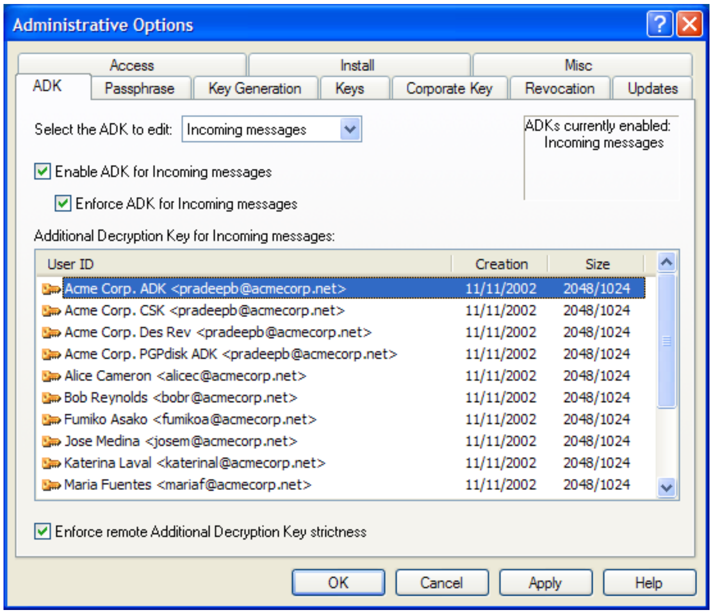
This is dependent on whether you have enabled Incoming or Outgoing ADK, or both.

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
Acme Corp. ADK <pradeepb@acmecorp.net>	11/11/2002	2048/1024
Acme Corp. CSK <pradeepb@acmecorp.net>	11/11/2002	2048/1024
Acme Corp. Des Rev <pradeepb@acmecorp.net>	11/11/2002	2048/1024
Acme Corp. PGPdisk ADK <pradeepb@acmecorp.net>	11/11/2002	2048/1024
Alice Cameron <alicec@acmecorp.net>	11/11/2002	2048/1024
Bob Reynolds <bobr@acmecorp.net>	11/11/2002	2048/1024
Fumiko Asako <fumikoa@acmecorp.net>	11/11/2002	2048/1024
Jose Medina <josem@acmecorp.net>	11/11/2002	2048/1024
Katerina Laval <katerinal@acmecorp.net>	11/11/2002	2048/1024
Maria Fuentes <mariaf@acmecorp.net>	11/11/2002	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:

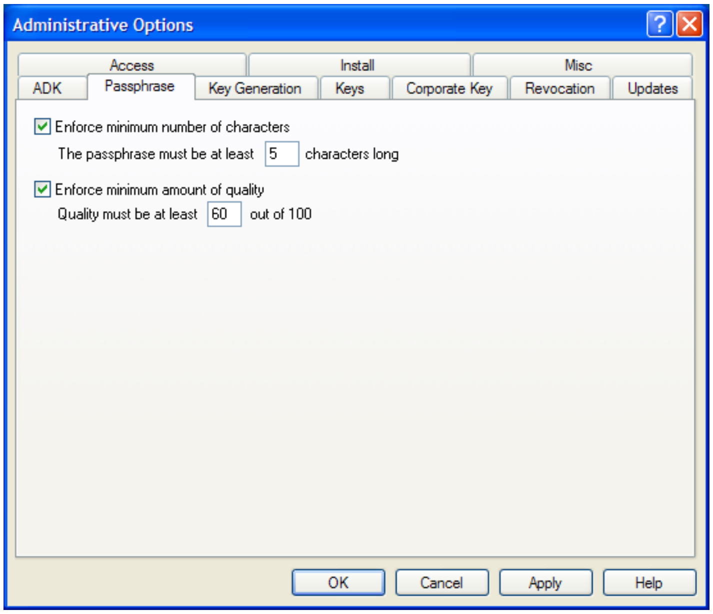
- **Select the ADK to edit**. Lets you select the type of Additional Decryption Key you are configuring. Select **Incoming Messages**, **Outgoing Messages**, or **PGPdisk**. The fields on the screen are slightly different for the different types of ADKs.
- **Enable ADK for Incoming/Outgoing/PGPdisk messages**. 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.



☑ 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

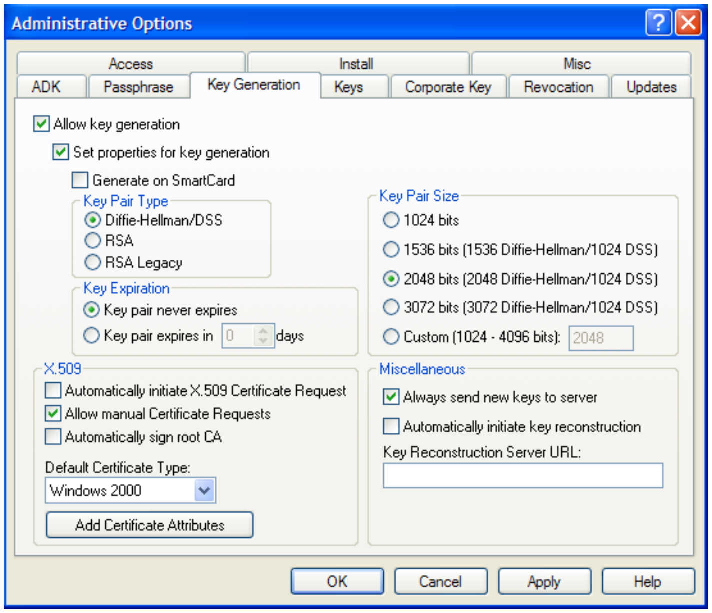
The fields on the Passphrase panel are:

- **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.



☑ Allow key generation
☑ Set properties for key generation
☐ Generate on SmartCard

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: Windows 2000
Add Certificate Attributes

Miscellaneous
☑ Always send new keys to server
☐ Automatically initiate key reconstruction
Key Reconstruction Server URL:

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.
- **Generate on SmartCard**. Check if you want your users' keys to be generated on a Smart Card. Refer to the chapter called "Making and Exchanging Keys" in your *PGP User's Guide* for more information.
- **Key Pair Type**. Select **Diffie-Hellman/DSS**, **RSA**, or **RSA Legacy**.

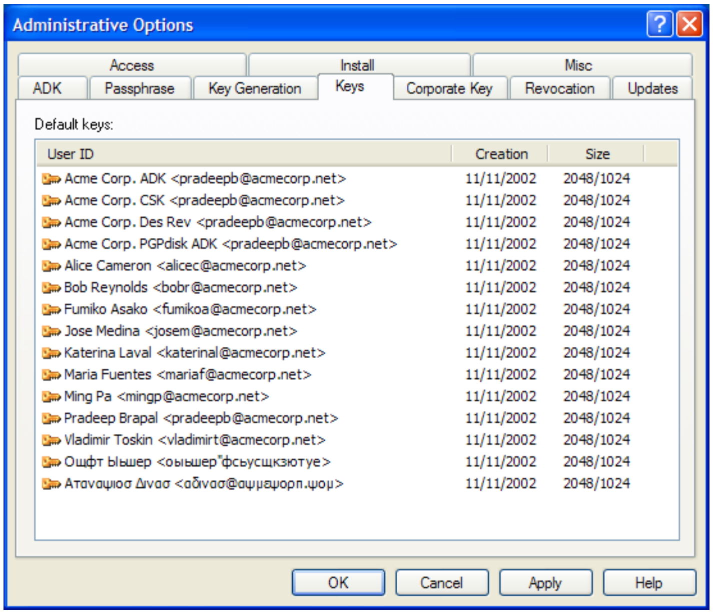
  Choose **RSA** or **RSA Legacy** if you plan to correspond with people who are using RSA keys. The RSA key format supports PGP's ADK, designated revoker, multiple encryption subkeys and photo ID features. Previously these features were only available to users with Diffie-Hellman keys. PGP will continue 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.

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.



Default keys:

User ID	Creation	Size
Acme Corp. ADK <pradeepb@acmecorp.net>	11/11/2002	2048/1024
Acme Corp. CSK <pradeepb@acmecorp.net>	11/11/2002	2048/1024
Acme Corp. Des Rev <pradeepb@acmecorp.net>	11/11/2002	2048/1024
Acme Corp. PGPdisk ADK <pradeepb@acmecorp.net>	11/11/2002	2048/1024
Alice Cameron <alicec@acmecorp.net>	11/11/2002	2048/1024
Bob Reynolds <bobr@acmecorp.net>	11/11/2002	2048/1024
Fumiko Asako <fumikoa@acmecorp.net>	11/11/2002	2048/1024
Jose Medina <josem@acmecorp.net>	11/11/2002	2048/1024
Katerina Laval <katerinal@acmecorp.net>	11/11/2002	2048/1024
Maria Fuentes <mariaf@acmecorp.net>	11/11/2002	2048/1024
Ming Pa <mingp@acmecorp.net>	11/11/2002	2048/1024
Pradeep Brapal <pradeepb@acmecorp.net>	11/11/2002	2048/1024
Vladimir Toskin <vladimirt@acmecorp.net>	11/11/2002	2048/1024
Ощфт Ыышер <оыышер"фсьусщкзютуе>	11/11/2002	2048/1024
Ατοναψιοσ Δινασ <αδινασ@αψμαψορπ.ψομ>	11/11/2002	2048/1024

The fields on the Keys panel are:

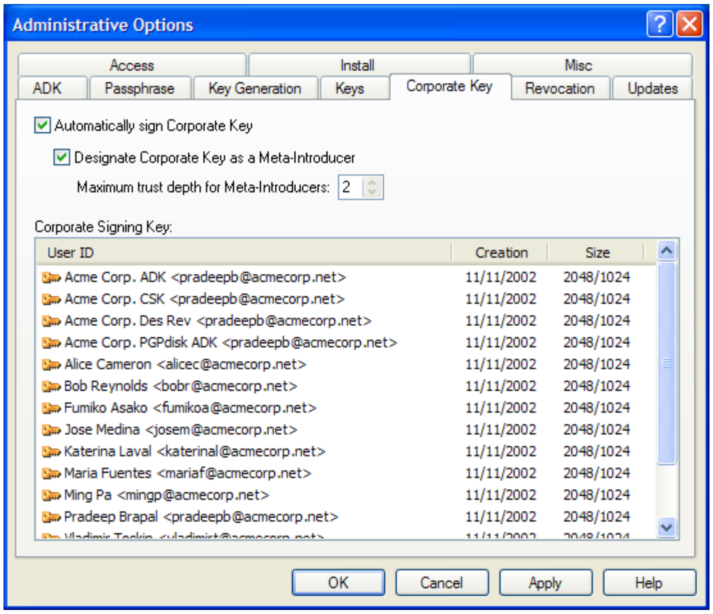
- **Default keys**. Lists all of the keys on the keyring of your PGP administrative machine.

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
Acme Corp. ADK <pradeepb@acmecorp.net>	11/11/2002	2048/1024
Acme Corp. CSK <pradeepb@acmecorp.net>	11/11/2002	2048/1024
Acme Corp. Des Rev <pradeepb@acmecorp.net>	11/11/2002	2048/1024
Acme Corp. PGPdisk ADK <pradeepb@acmecorp.net>	11/11/2002	2048/1024
Alice Cameron <alicec@acmecorp.net>	11/11/2002	2048/1024
Bob Reynolds <bobr@acmecorp.net>	11/11/2002	2048/1024
Fumiko Asako <fumikoa@acmecorp.net>	11/11/2002	2048/1024
Jose Medina <josem@acmecorp.net>	11/11/2002	2048/1024
Katerina Laval <katerinal@acmecorp.net>	11/11/2002	2048/1024
Maria Fuentes <mariaf@acmecorp.net>	11/11/2002	2048/1024
Ming Pa <mingp@acmecorp.net>	11/11/2002	2048/1024
Pradeep Brapal <pradeepb@acmecorp.net>	11/11/2002	2048/1024

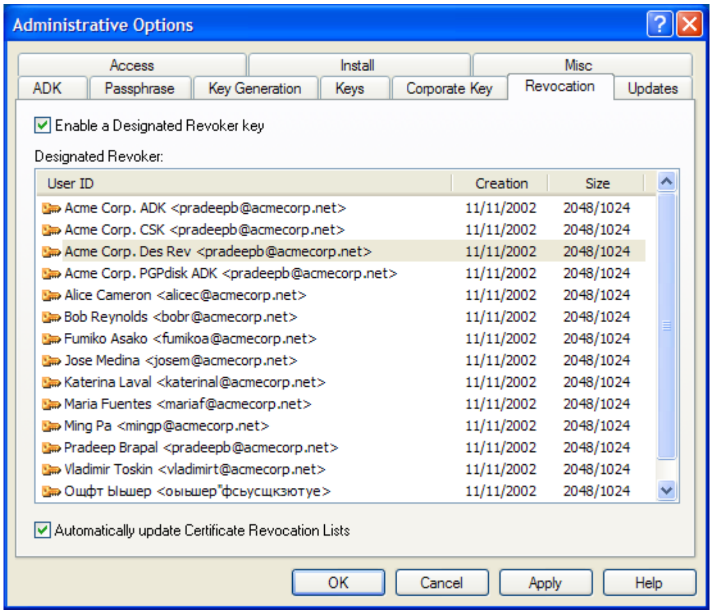
The fields on the Corporate Key panel are:

- **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
Acme Corp. ADK <pradeepb@acmecorp.net>	11/11/2002	2048/1024
Acme Corp. CSK <pradeepb@acmecorp.net>	11/11/2002	2048/1024
Acme Corp. Des Rev <pradeepb@acmecorp.net>	11/11/2002	2048/1024
Acme Corp. PGPdisk ADK <pradeepb@acmecorp.net>	11/11/2002	2048/1024
Alice Cameron <alicec@acmecorp.net>	11/11/2002	2048/1024
Bob Reynolds <bobr@acmecorp.net>	11/11/2002	2048/1024
Fumiko Asako <fumikoa@acmecorp.net>	11/11/2002	2048/1024
Jose Medina <josem@acmecorp.net>	11/11/2002	2048/1024
Katerina Laval <katerinal@acmecorp.net>	11/11/2002	2048/1024
Maria Fuentes <mariaf@acmecorp.net>	11/11/2002	2048/1024
Ming Pa <mingp@acmecorp.net>	11/11/2002	2048/1024
Pradeep Brapal <pradeepb@acmecorp.net>	11/11/2002	2048/1024
Vladimir Toskin <vladimirt@acmecorp.net>	11/11/2002	2048/1024
Ощфт Ыьшер <оыьшер"фсьусщкзютуе>	11/11/2002	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:

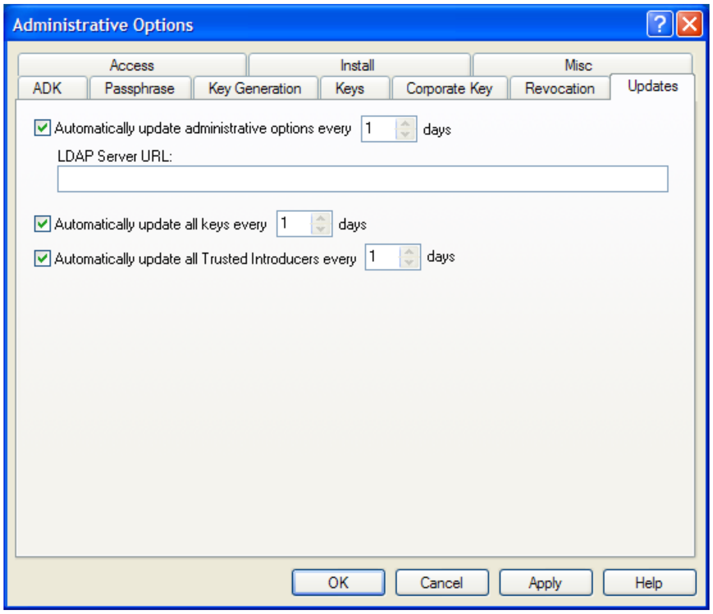
- **Enable a Designated Revoker key**. Check if you want to have a designated revoker key.
- **Designated Revoker.** Lists all of the keys on the keyring of your PGP administrative machine so that you can select the Designated Revoker Key.
- **Automatically update Certificate Revocation Lists.** Check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

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 PGP Admin administrative options. Make sure to specify an interval, also.

Caution: 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 PGP Admin 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.

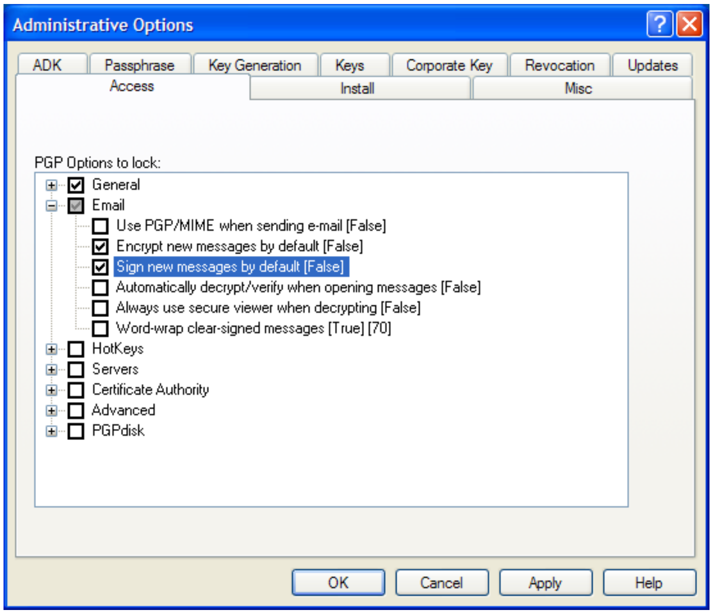
The Access panel

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.

Note: 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.



PGP Options to lock:

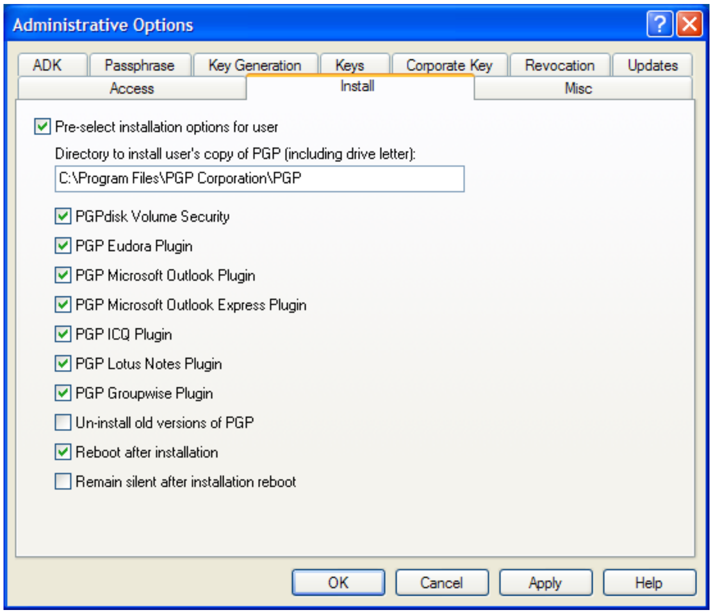
- ☑ General
- ☑ Email
  - ☐ Use PGP/MIME when sending e-mail [False]
  - ☑ Encrypt new messages by default [False]
  - ☑ Sign new messages by default [False]
  - ☐ Automatically decrypt/verify when opening messages [False]
  - ☐ Always use secure viewer when decrypting [False]
  - ☐ Word-wrap clear-signed messages [True] [70]
- ☐ HotKeys
- ☐ Servers
- ☐ Certificate Authority
- ☐ Advanced
- ☐ PGPdisk

The fields on the Access panel are:

- **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

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.



☑ Pre-select installation options for user

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

☑ PGPdisk Volume Security
☑ PGP Eudora Plugin
☑ PGP Microsoft Outlook Plugin
☑ PGP Microsoft Outlook Express Plugin
☑ PGP ICQ Plugin
☑ PGP Lotus Notes Plugin
☑ PGP Groupwise Plugin
☐ Un-install old versions of PGP
☑ Reboot after installation
☐ Remain silent after installation reboot

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.
- **PGPdisk Volume Security**. Check if you want PGPdisk 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 Notes in Your Network, for detailed instructions.

- **PGP Groupwise Plugin**. Check if you want the Groupwise plugin 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.
- **Remain silent after installation reboot**. Check if you want PGP to remain silent after the installation reboot. PGP will not be set up on your users’ systems until they access it directly via the PGPkeys or PGPmail items on the Start menu.

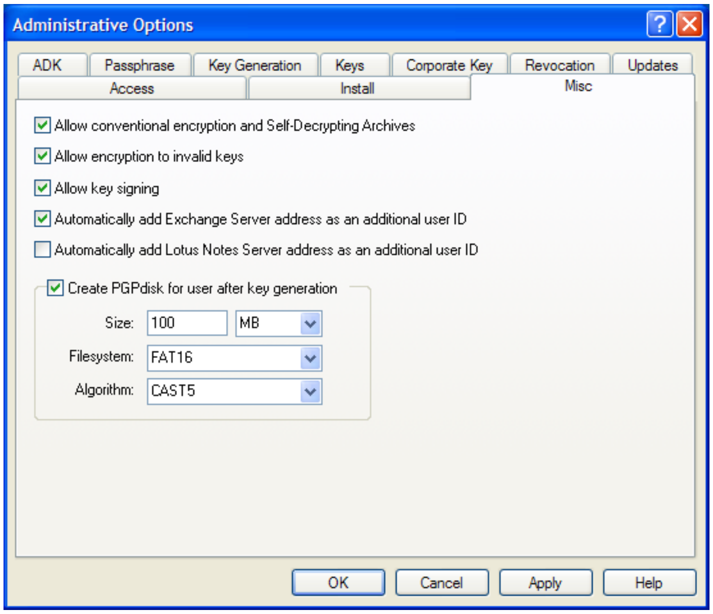
The Misc panel

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.

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.

You may also want to have your users automatically create a PGPdisk for storing sensitive data.



☑ Allow conventional encryption and Self-Decrypting Archives

☑ Allow encryption to invalid keys

☑ Allow key signing

☑ Automatically add Exchange Server address as an additional user ID

☐ Automatically add Lotus Notes Server address as an additional user ID

☑ Create PGPdisk for user after key generation

Size: 100 MB

Filesystem: FAT16

Algorithm: CAST5

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.
- **Automatically add Exchange Server address as an additional user ID**. Check if you want your PGP users to have their email user ID retrieved from your Microsoft Exchange server and added to their PGP key during the key generation process. Naturally, this only happens if PGP detects that the computer is in an Exchange server environment.
- **Automatically add Lotus Notes Server address as an additional user ID**. Check if you want your PGP users to have their email user ID retrieved from your Lotus Notes server and added to their PGP key during the key generation process. Naturally, this only happens if PGP detects that the computer is in a Lotus Notes server environment.
- **Create PGPdisk for user after key generation**. Check this box if you want your users to automatically create a PGPdisk after they generate their key. Make the following selections:
  - **Size.** Enter a number and then select **KB** (kilobytes), **MB** (megabytes), or **GB** (gigabytes).
  - **Filesystem.** Select **FAT12**, **FAT16**, **FAT32**, or **NTFS**.
  - **Algorithm.** Select **CAST5** or **Twofish**.

6

Retrieving the Server Configuration

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

Overview

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

When you make changes in PGP Admin, 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). 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 PGP Admin (instead of the settings from the version of PGP running on the PGP administrative machine), you can download these settings from the server into PGP Admin.

Retrieving the settings from the server

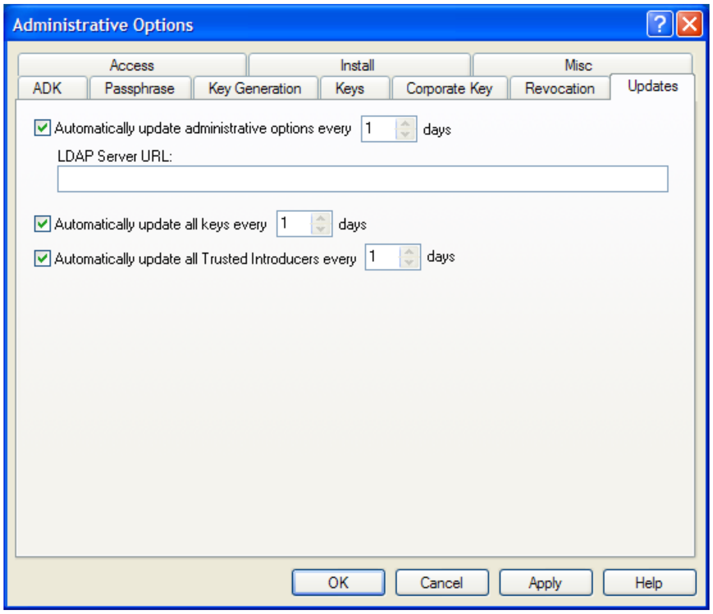
To retrieve the settings from your corporate server, you must tell PGP Admin about the server and then retrieve the settings.

To retrieve PGP Admin administrative settings:

1. Open PGP Admin on your PGP administrative machine.
2. Click **Administrative Options**.

   The Administrative Options screen appears.
3. Select the **Updates** panel.

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 PGP Admin screen appears.
6. Click **Retrieve Server Configuration**.

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

7

Creating a Client Installer

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 PGP Admin administrative options you want on your PGP administrative machine, you can create the PGP client installer program.

Note: Do not create the client installer program until *all* of the PGP options and PGP Admin administrative options 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

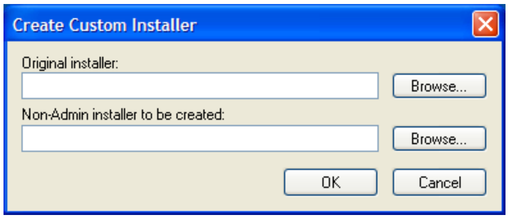
The PGP client installer program is what you will be distributing to your users. It includes both the PGP options you want them to have and the PGP Admin administrative options you have configured.

The following procedures tell you how to create Windows client installer programs.

To create a PGP client installer program:

1. Bring up PGP Admin on your Windows PGP administrative machine.
2. Click **Create Custom Installer.**

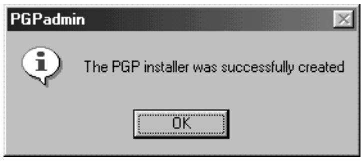
   The Create Custom Installer screen appears.



3. Click the top Browse button and select the Windows PGP installation program that you want to customize with the PGP options and PGP Admin 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 PGP Admin 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.

8

Distributing the PGP Client Installer Program

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

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.

9

Updating PGP Admin Settings

This chapter tells you how to post and update the PGP Admin 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 PGP Admin administrative settings onto the corporate LDAP server or PGP Keyserver so that your users can get to them.

Updating the settings

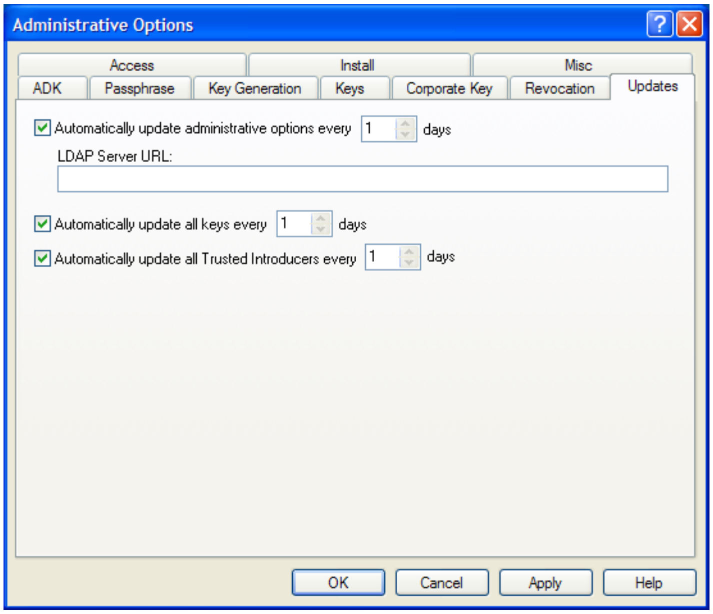
To put the PGP Admin administrative settings onto your corporate LDAP server or PGP Keyserver, you must tell PGP Admin about the server and then transfer the files.

To update PGP Admin administrative settings:

1. Open PGP Admin on your PGP administrative machine.
2. Click **Administrative Options**.

   The Administrative Options screen appears.
3. Select the **Updates** panel.

The Updates panel appears.



☑ Automatically update administrative options every 1 days

LDAP Server URL:

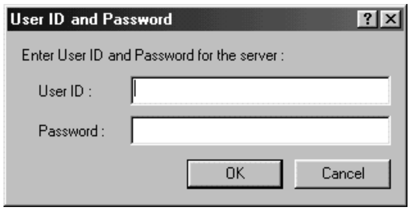
☑ Automatically update all keys every 1 days

☑ 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 PGP Admin administrative settings from.
5. Click **OK**.

   The PGP Admin 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 PGP Admin administrative settings are uploaded to the LDAP server and then the PGP Admin screen appears.

A

Setting Up a Network Security Policy

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.
- **PGP Corporation.** 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.

Note

Note: 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.

B

Implementing a PGP Public Key Infrastructure

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?

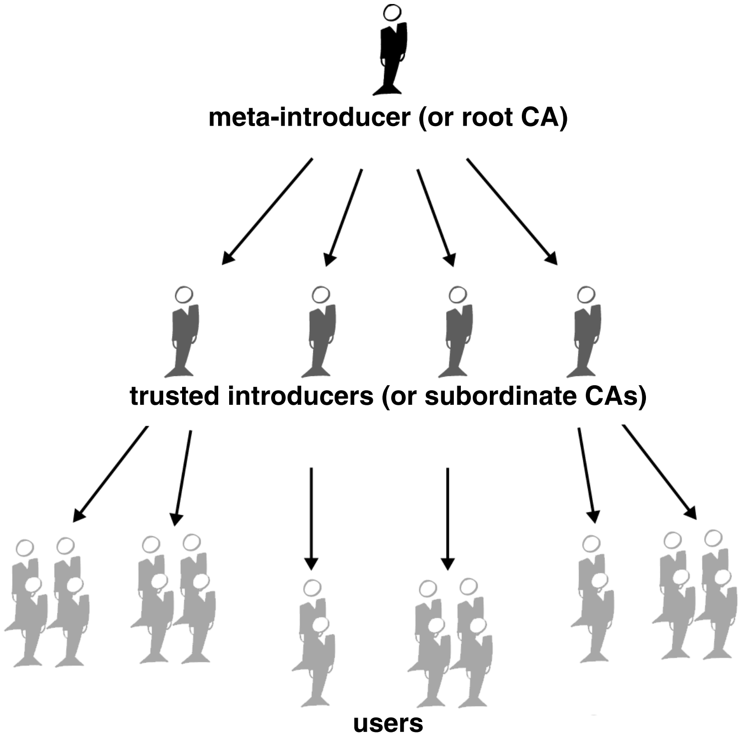
A PKI contains the certificate storage facilities of a certificate server (also called a key server), but also provides certificate management facilities (the ability to issue, revoke, store, retrieve, and trust certificates). The main feature of a PKI is the introduction of what is known as a *Certification 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.

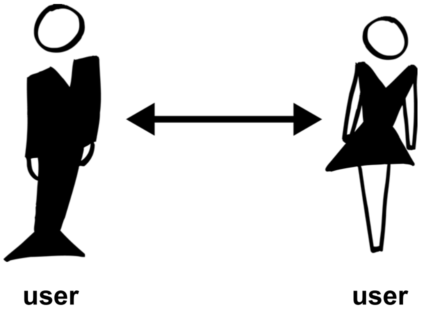
There are three different trust models:

- 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.

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.

C Creating a Corporate Signing Key

This appendix gives you information about how to create a Corporate Signing Key.

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 bits.

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.

D

Creating Additional Decryption Keys

This appendix describes Additional Decryption Keys.

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 PGP Admin; 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 PGP Admin, 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.

Note

Note: 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.

Caution: 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

You need to create a key for each key type your users use. That is, if your users only use Diffie-Hellman/DSS PGP keys, you only need to create Diffie-Hellman/DSS keys to use as ADKs. If your users have both RSA and Diffie-Hellman keys, however, you will need both types of Additional Decryption Keys.

Select a key type:

- **Diffie-Hellman/DSS:** Can be used as Incoming or Outgoing ADK.
- **RSA:** Can be used as Incoming or Outgoing ADK.
- **RSA Legacy:** Cannot be used as Incoming ADKs. Should only be used if your users correspond with other users of RSA Legacy keys.

Key size

Your Additional Decryption Keys should be at least 2048 bits.

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 Legacy keys are limited to 2048 bits in order to maintain compatibility with older versions of PGP.

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

Passphrases for ADKs or the passphrases to the shares of the key should be well constructed. We recommend using passphrases that meet the 100% mark on the passphrase quality display.

E

Configuring Lotus Notes in Your Network

This appendix tells you how to integrate the PGP Lotus Notes plug-in into your organization.

Overview

The PGP Lotus Notes Plugin uses the PGP Plugin Template database to allow PGP-enabled and non-PGP-enabled Notes Mail users to coexist peacefully within your Lotus Domino environment. That is to say, the PGP Notes Plugin does not change your organization's Notes Mail template in any way.

Coexistence is accomplished by placing the PGP Plugin Template database alongside your organization's Notes Mail template within its Domino environment (or at least on those servers hosting PGP-enabled Notes Mail users).

Note: The Notes PGP Plug-In supports only Notes client-based Notes Mail. Web browser-based Notes Mail is ***not*** supported. PGP's Use Current Window feature can be used to decrypt mail in Web-based mail applications.

To add PGP into your organization where your users are using Lotus Notes for email requires two things:

- First, that PGP be installed onto your users' computers.
- Second, that your Domino servers be correctly configured.

Until both items are done, your users cannot use PGP from within Lotus Notes.

Note: This appendix assumes that Lotus Notes 4.5.x, 4.6.x, or 5.x is installed and functioning on your users' computers and that your network is running Lotus Domino server software 4.6.x or 5.x. We also assume you are the Lotus Notes administrator for your company or at least familiar with Notes administration and have commensurate access rights into your Lotus Notes infrastructure.

To correctly configure your Domino servers to support the use of PGP by your users, you need to run the PGP Lotus Domino Server wizard. This wizard basically lets you do two things:

- **Create/refresh your PGP email template:** You need to do this when you are installing the PGP Lotus Notes plug-in in your organization's Domino environment for the first time, or when you want to update the plug-in template already on the target Domino server. Selecting this option copies the PGP plug-in templates to the Domino server, which from then on can be replicated to any other

Domino mail servers in your network. By use of the standard Domino Design add-in task, any updates made to the PGP template will be propagated to all end-user mail databases previously PGP-enabled.

- **PGP enable specific Notes Mail databases:** This feature enables the selected mail databases to use the PGP Notes mail extension. This is accomplished by enhancing the design of the selected databases with the PGP-enabled email forms that reside in the PGP Plug-In template resident on the server.

If you are just upgrading the PGP Plug-In template to a more recent version—which means the selected databases have already been enabled for PGP—then you can deselect this option provided that the standard Domino Design add-in task is running on the server.

Note: The PGP Lotus Domino Server wizard also lets you remove the PGP Lotus Notes plug-in support from selected mail databases, or completely from your Domino server. To do this, simply select Un-configure PGP Lotus Notes Plug-in on your Domino server from the PGP Lotus Notes Plugin Options menu and follow the on-screen instructions.

Installing PGP

To install PGP with the Lotus Notes plug-in included, refer to the chapters of this Administrator’s Guide. You’ll want to pay particular attention to Chapters 5 through 8.

Once your users have installed PGP with the Lotus Notes plug-in onto their computers, you can proceed to configuring your Lotus Domino server(s) to support the use of PGP in Lotus Notes.

Configuring your Domino servers

Your Lotus Notes users cannot use PGP to secure their email messages until you have configured your Domino server(s) to support this. Refer to Configuring networks with multiple Domino servers for information about how to configure PGP support on networks with multiple Domino servers.

Note: We recommend running the PGP Lotus Domino Server wizard from the Notes administrator’s workstation. This normally ensures that an ID file with Manager permissions on all databases is being used.

Before you run the PGP Lotus Domino Server wizard, make sure you have the following information:

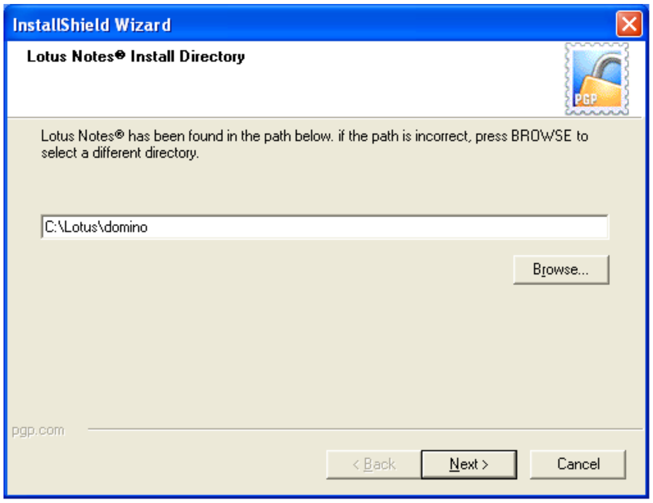
- Name of the target Domino server

- 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 configuring the databases)
- Path to the PGP Notes Plug-in Template on the target server (if you plan on enabling specific mail databases with PGP)

To configure your Domino servers to support PGP:

1. If you are not running the wizard directly on the server machine, make sure you are logged on as a Lotus Notes administrator so that you have the appropriate permissions.
2. If you are installing via CD, insert the CD and choose to install the PGP Lotus Notes Plugin, then follow the on-screen instructions.
3. If you are installing from the Web, download the installer, double click it to being the install, then follow the on-screen instructions.

   The Lotus Notes Install Directory screen appears.



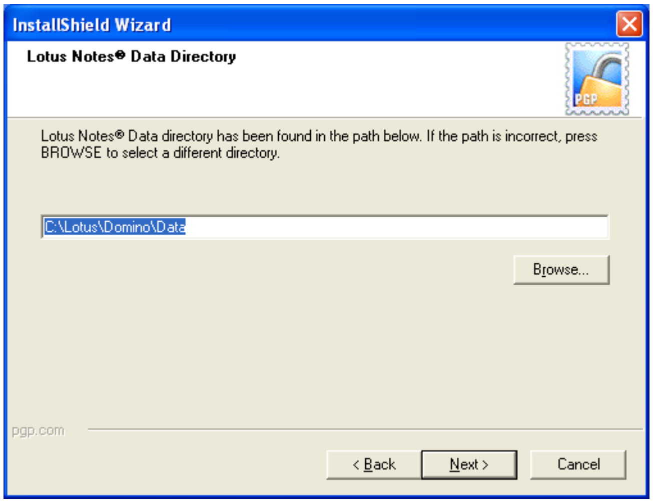
Lotus Notes® Install Directory

Lotus Notes® has been found in the path below. if the path is incorrect, press BROWSE to select a different directory.

C:\Lotus\domino

4. Verify the path to the Notes install directory, then click **Next**.

The Lotus Notes Data Directory screen appears.



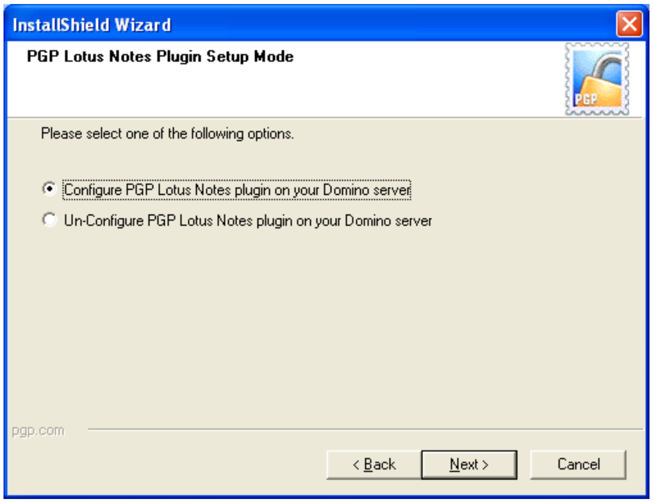
Lotus Notes® Data Directory

Lotus Notes® Data directory has been found in the path below. If the path is incorrect, press BROWSE to select a different directory.

C:\Lotus\Domino\Data

5. Verify the path to the Notes data directory, then click **Next**.

   The PGP Lotus Notes Plugin Options menu screen appears.



PGP Lotus Notes Plugin Setup Mode

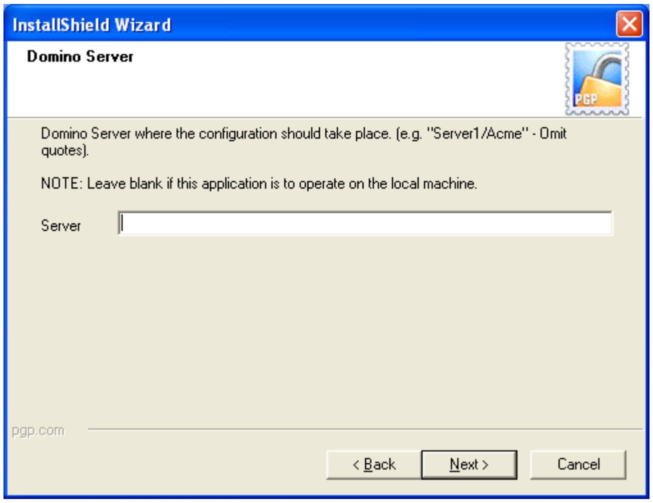
Please select one of the following options.

● Configure PGP Lotus Notes plugin on your Domino server

○ Un-Configure PGP Lotus Notes plugin on your Domino server

6. Select Configure PGP Lotus Notes Plugin on your Domino server, then click **Next**.

The Domino Server screen appears.



Domino Server where the configuration should take place. (e.g. "Server1/Acme" - Omit quotes).

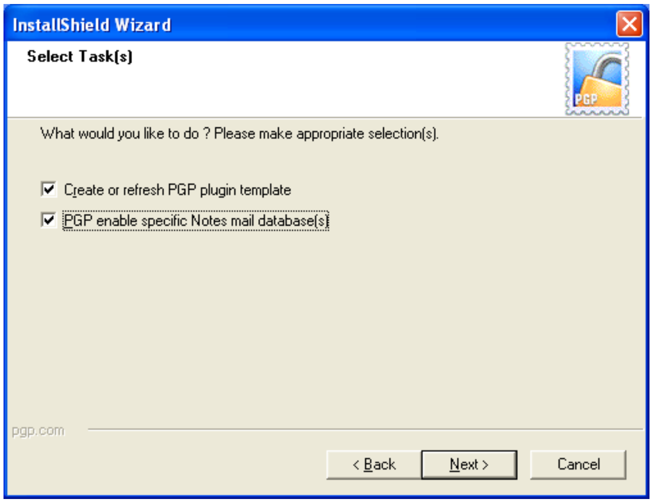
NOTE: Leave blank if this application is to operate on the local machine.

Server

7. Enter the name of the Domino server that you are configuring, then click **Next**.

   If you are running the PGP Lotus Domino Server wizard from the Domino server, leave this field empty.

   The Select Task(s) screen appears.



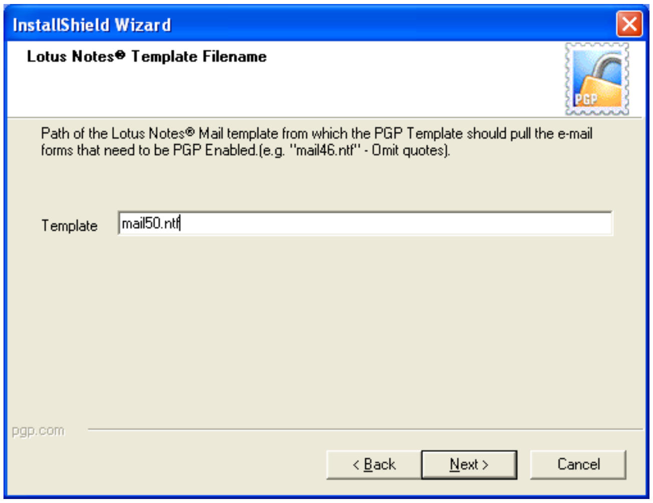
What would you like to do ? Please make appropriate selection(s).

☑ Create or refresh PGP plugin template

☑ PGP enable specific Notes mail database(s)

8. Select **Create-Refresh PGP Plugin Template** and/or **PGP Enable specific Notes Mail database**(s), then click **Next**.
   - Select **Create or refresh PGP plugin template** if you are installing the PGP Lotus Notes plug-in in your organization's Domino environment for the first time, or when you want to update the template already on the target Domino server.
   - Select **PGP enable specific Notes mail database**(s) so that you can enable selected mail databases to use the PGP Plug-In template.

If you selected **PGP enable specific Notes mail database**(s), the Lotus Notes Template Filename screen appears.

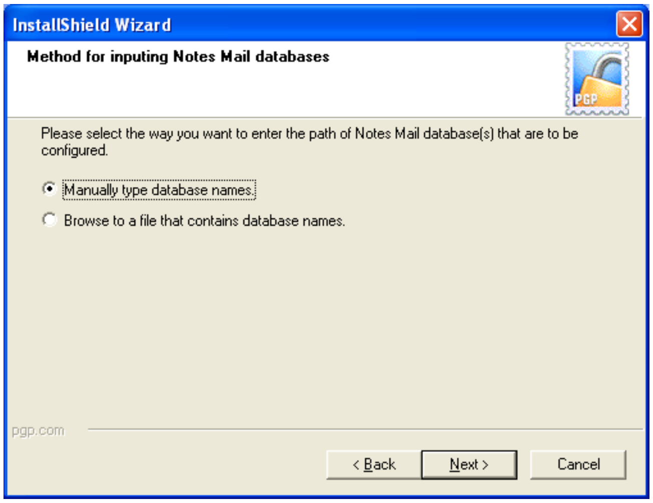


Path of the Lotus Notes® Mail template from which the PGP Template should pull the e-mail forms that need to be PGP Enabled.(e.g. "mail46.ntf" - Omit quotes).

Template mail50.ntf

9. Enter the path to the mail template used on your Domino servers (*mail50.ntf*, for example), then click **Next**.

   If you selected **Create or refresh PGP Plugin Template**, the Method for inputing Notes Mail databases screen appears.



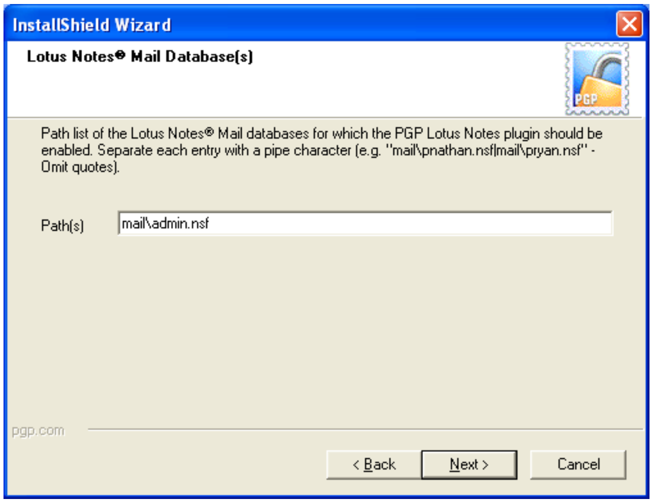
Please select the way you want to enter the path of Notes Mail database(s) that are to be configured.

● Manually type database names.

○ Browse to a file that contains database names.

10. Select **Manually type database names**, then click **Next**.

The Lotus Notes Mail Database(s) screen appears.



Lotus Notes® Mail Database(s)

Path list of the Lotus Notes® Mail databases for which the PGP Lotus Notes plugin should be enabled. Separate each entry with a pipe character (e.g. "mail\pnathan.nsf|mail\pryan.nsf" - Omit quotes).

Path(s) mail\admin.nsf

11. Do one of the following:
    - Enter the file name of a database on the server to PGP enable it.
    - Enter list of databases to PGP enable. Use the pipe (|) character to separate each database in the list.
    - Enter the keyword "users.txt" to batch process a list of databases from a file. (You could also browse to this file if you select the Browse option on the Method for inputing Notes Mail databases screen.) If you choose this option, the installer will look for a file named users.txt in the Lotus Notes program directory. The format of users.txt should resemble the following:

      database1.nsf

      database2.nsf

      database3.nsf4

    Or, if the mail databases reside in a subdirectory of the server root directory, include the relative path. For example:

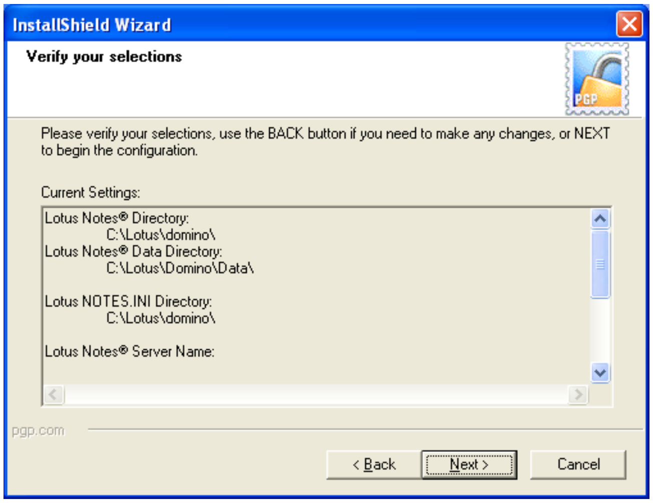
      mail\database1.nsf

      mail\database2.nsf

      mail\database3.nsf

12. When you've made your selection, click **Next**.

The Verify your selections screen appears.



Verify your selections

Please verify your selections, use the BACK button if you need to make any changes, or NEXT to begin the configuration.

Current Settings:

```
Lotus Notes® Directory:
          C:\Lotus\domino\
Lotus Notes® Data Directory:
          C:\Lotus\Domino\Data\

Lotus NOTES.INI Directory:
          C:\Lotus\domino\

Lotus Notes® Server Name:
```

13. Verify that the settings are correct, then click **Next**.

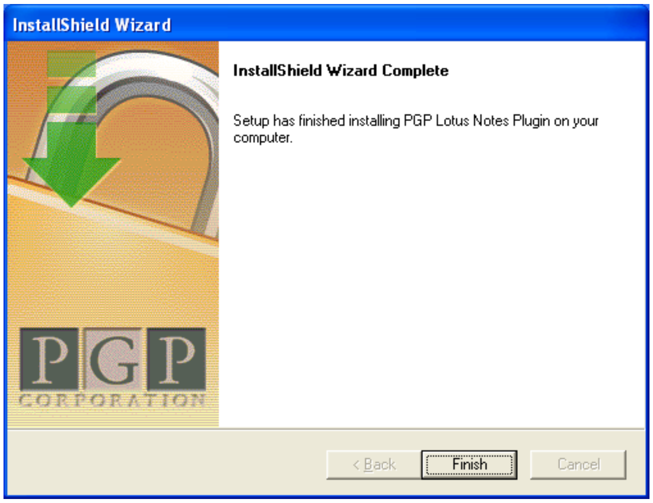
    You are prompted for the password for the user ID file.

14. Enter the appropriate password, then click **OK**.

    The configuration of the Domino server begins. This process can take quite a while depending on your hardware and the number of databases to be configured.

    In the event that any databases failed to be PGP-enabled, a log file is generated (PGPlog.txt) in your current workstation's Lotus Notes Program directory.

    When the Domino server is configured, the PGP Install Wizard Complete screen appears.



InstallShield Wizard Complete

Setup has finished installing PGP Lotus Notes Plugin on your computer.

15. Click **Finish**.

    Notify your users that they can now use PGP from within Lotus Notes.

Configuring networks with multiple Domino servers

To successfully configure a multiple Domino server environment using the PGP Lotus Domino Server wizard, follow the instructions in "Configuring your Domino servers" on page 14, 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 servers hosting Notes Mail databases. Instead, before running the wizard 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.

Using this technique allows you to leverage standard Domino technology such that design changes or updates tot he PGP Plus-in Template can be made in one place and then migrated automatically throughout your Domino environment using standard Domino replication and the server's "Design" add-in task.

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. Applies only to X.509 PKIs.

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.

PGP/MIME

an IETF standard (RFC 3156) 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