

IBM® Lotus Protector for Mail Encryption

User's Guide

Version Information

Lotus Protector for Mail Encryption User's Guide. Lotus Protector for Mail Encryption Version 2.1.0. Released December 2010.

This edition applies to version 2, release 1, modification 0, fixpack 1 of IBM Lotus Protector for Mail Encryption (product number 5724-Z72) and to all subsequent releases and modifications until otherwise indicated in new editions.

Copyright Information

Copyright © 1991-2010 by PGP Corporation. All Rights Reserved. No part of this document can be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without the express written permission of PGP Corporation.

© Copyright IBM Corporation 1994, 2010. US Government Users Restricted Rights - Use, duplication or disclosure restricted by GSA ADP Scheduled Contract with IBM Corp..

Trademark Information

PGP, Pretty Good Privacy, and the PGP logo are registered trademarks of PGP Corporation in the US and other countries. IDEA is a trademark of Ascom Tech AG. Windows and ActiveX are registered trademarks of Microsoft Corporation. AOL is a registered trademark, and AOL Instant Messenger is a trademark, of America Online, Inc. Red Hat and Red Hat Linux are trademarks or registered trademarks of Red Hat, Inc. Linux is a registered trademark of Linus Torvalds. Solaris is a trademark or registered trademark of Sun Microsystems, Inc. AIX is a trademark or registered trademark of International Business Machines Corporation. HP-UX is a trademark or registered trademark of Hewlett-Packard Company. SSH and Secure Shell are trademarks of SSH Communications Security, Inc. Rendezvous and Mac OS X are trademarks or registered trademarks of Apple Computer, Inc. All other registered and unregistered trademarks in this document are the sole property of their respective owners.

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at "Copyright and trademark information" at <http://www.ibm.com/legal/copytrade.shtml>.

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.

Subject to the terms of the license that accompanied the Program, Licensee may redistribute PGP Universal Satellite.

Notices

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A

For license inquiries regarding double-byte character set (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan Ltd.
1623-14, Shimotsuruma, Yamato-shi
Kanagawa 242-8502 Japan

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact: IBM Corporation.

INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

Lotus Software
IBM Software Group

One Rogers Street
Cambridge, MA 02142
USA

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.

If you are viewing this information softcopy, the photographs and color illustrations may not appear.

Contents

About IBM® Lotus Protector for Mail Encryption **1**

Understanding Lotus Protector for Mail Encryption Server Policy	1
Getting Assistance	2

Installing Lotus Protector for Mail Encryption **3**

System Requirements	3
Compatible Email Clients	3
Starting the Lotus Protector for Mail Encryption Installer	4
Enrolling with the Lotus Protector for Mail Encryption Server	4
Uninstalling Lotus Protector for Mail Encryption	5

Sending Email Messages **7**

Using Lotus Protector for Mail Encryption in Lotus Notes	7
Using Lotus Protector for Mail Encryption in Microsoft Outlook	9
Verifying Encryption Status of Email Messages	10

Receiving Email Messages **11**

Viewing Incoming Email Messages	11
---------------------------------	----

1

About IBM® Lotus Protector for Mail Encryption

IBM® Lotus Protector for Mail Encryption Client provides IBM Lotus® enterprise customers with an automatic, transparent encryption solution for securing internal and external confidential email communications. Lotus Notes offers a native encryption solution for secure messaging within an organization. While Lotus Protector for Mail Encryption Client can be used for internal-to-internal secure messaging, it is intended to secure the internal component of a message which is being delivered to an external recipient. With Lotus Protector for Mail Encryption Client, you can minimize the risk of a data breach and better comply with partner and regulatory mandates for information security and privacy.

Note: References to "PGP key" in this document refer to both OpenPGP keys as well as X.509 certificates.

In This Chapter

Understanding Lotus Protector for Mail Encryption Server Policy	1
Getting Assistance	2

Understanding Lotus Protector for Mail Encryption Server Policy

Lotus Protector for Mail Encryption automatically encrypts email messages you send, based on policy defined by your Lotus Protector for Mail Encryption Server. By default, Lotus Protector for Mail Encryption encrypts messages tagged for encryption within your email client, typically via the **Encrypt** check box in the standard Lotus Notes message template, or a custom button added to Microsoft Outlook. Additionally, some messages may be encrypted automatically based on a subject/body tag, external domains, or other properties. For more information about what policy applies to you, contact your Lotus Protector for Mail Encryption Server Administrator.

Getting Assistance

For additional information about Lotus Protector for Mail Encryption and how to obtain support, see *Lotus Protector for Mail Encryption* (<http://www.ibm.com/software/lotus/products/protector/mailencryption/>).

2

Installing Lotus Protector for Mail Encryption

This section describes how to install Lotus Protector for Mail Encryption onto your computer and how to get started after installation.

In This Chapter

System Requirements	3
Compatible Email Clients	3
Starting the Lotus Protector for Mail Encryption Installer	4
Enrolling with the Lotus Protector for Mail Encryption Server	4
Uninstalling Lotus Protector for Mail Encryption	5

System Requirements

Before you begin the installation, verify that your system meets these minimum requirements:

- Microsoft Windows 2000 (Service Pack 4), Windows Server 2003 (Service Pack 1 and 2), Windows XP Professional 32-bit (Service Pack 2 or 3), Windows XP Professional 64-bit (Service Pack 2), Windows XP Home Edition (Service Pack 2 or 3), Microsoft Windows XP Tablet PC Edition 2005 (requires attached keyboard), Windows Vista (all 32- and 64-bit editions, including Service Pack 1 and 2), Windows 7 (all 32- and 64-bit editions).

Note: The above operating systems are supported only when all of the latest hot fixes and security patches from Microsoft have been applied.

Compatible Email Clients

Lotus Protector for Mail Encryption Client is compatible with the following email clients:

- Lotus Notes 7.0.3 (7.0.4), 8.0.2, 8.5 (8.5.1)
- Microsoft Outlook® XP SP3, Microsoft Outlook 2003 SP3, Microsoft Outlook 2007 SP2

Note: Lotus Protector for Mail Encryption is compatible with Microsoft Outlook only with Microsoft Exchange servers.

Starting the Lotus Protector for Mail Encryption Installer

Note: You must have administrative rights on your system in order to install Lotus Protector for Mail Encryption.

Before you begin, be sure that you have exited your email application (Lotus Notes or Microsoft Outlook).

► To install Lotus Protector for Mail Encryption on your Windows system

- 1 Locate the Lotus Protector for Mail Encryption installation program. The installer program is an .MSI file, which your Lotus Protector for Mail Encryption Server Administrator may have distributed to you using deployment tools.

In addition to the .msi installation file, you also need to specify the location of the Lotus Protector for Mail Encryption Server. This is called the Lotus Protector for Mail Encryption Server Stamp. The server stamp can be embedded into the .msi package itself, be specified in a configuration file, or specified in your notes.ini file.

- Your administrator may decide to distribute the Lotus Protector for Mail Encryption Server stamp information via the notes.ini file. If that is the case, the installer will automatically locate the Server Stamp information during installation.
 - If your administrator provided a PMECONF.dat file, ensure that this file is located in the same directory as the .msi installer.
- 2 Double-click the Lotus Protector for Mail Encryption installer.
 - 3 Follow the on-screen instructions.
 - 4 If prompted to do so, restart your system.

Enrolling with the Lotus Protector for Mail Encryption Server

When you enroll with the Lotus Protector for Mail Encryption Server, you are prompted to enter your authentication credentials. When prompted, enter your primary user name and password from your company's directory service. Typically this will be your Lotus Domino user name (Internet address) and Internet password in a Lotus Notes environment, or your Active Directory or Windows credentials in a Microsoft Exchange environment.

Uninstalling Lotus Protector for Mail Encryption

Uninstall Lotus Protector for Mail Encryption using the Windows **Add or Remove Programs** feature.

Note: You must have administrative rights on your system in order to uninstall Lotus Protector for Mail Encryption.

Before you begin, be sure that you have exited your email application (Lotus Notes or Microsoft Outlook).

► To uninstall Lotus Protector for Mail Encryption

- 1 Click the **Start** menu and select **Settings > Control Panel**.
- 2 Double-click **Add or Remove Programs**.
- 3 Locate and double-click the Lotus Protector for Mail Encryption Client item.
- 4 Click **Yes** to continue with the uninstall process. The Lotus Protector for Mail Encryption software is removed from your system.
- 5 If prompted, restart your computer to complete the uninstall process.

3

Sending Email Messages

If your Lotus Protector for Mail Encryption Server Administrator has specified, outgoing email messages that you send (using either Lotus Notes or Microsoft Office) can include a comment. Generally this type of comment indicates that the message has been secured by Lotus Protector for Mail Encryption, but can be customized by your Lotus Protector for Mail Encryption Server Administrator. This section describes how to send email using either Lotus Notes or Microsoft Outlook.

In This Chapter

Using Lotus Protector for Mail Encryption in Lotus Notes	7
Using Lotus Protector for Mail Encryption in Microsoft Outlook.....	9
Verifying Encryption Status of Email Messages	10

Using Lotus Protector for Mail Encryption in Lotus Notes

Lotus Protector for Mail Encryption Client is designed to work with the encryption built into Lotus Notes. By default, Notes native encryption will be preferred, so that if a message can be encrypted by Notes, it will be. However, if Notes cannot encrypt a message which needs to be secured, Lotus Protector for Mail Encryption Client will encrypt the message. This can occur in a number of cases, for example when sending a secure email:

- To a person outside your organization.
- To a Lotus Protector for Mail Encryption Client user inside your organization on a Microsoft Exchange server.
- To a Lotus Protector for Mail Encryption Client user inside your organization on a Lotus Notes server but without a Notes key.
- To a person using an SMTP address (acameron@example.com) instead of a Lotus Notes address (CN=Alice Cameron/O=Example Corp).

Lotus Notes Native Encryption enables Notes users to send internal email encrypted to the user's Notes key. When Lotus Protector for Mail Encryption is configured to use Notes native encryption, confidential information can be sent encrypted to internal users by selecting a checkbox when composing the message. Most Lotus Notes users have a Notes ID within which the encryption key is stored.

If the recipient in the To: field is within the same Domino Domain, the recipient has a personal document in the Domino directory, and Notes native encryption is enabled, Lotus Protector for Mail Encryption allows the email to be sent encrypted using Lotus Notes Native Encryption. If the email address in the To: field is an SMTP address (acameron@example.com) whose address is NOT in the same Notes domain or whose personal document cannot be found in the Domino directory, Lotus Protector for Mail Encryption encrypts the email to your PGP key.

Lotus Protector for Mail Encryption is fully integrated into the Lotus Notes client. It evaluates the security policies for all outgoing Lotus Notes messages and automatically selects the appropriate encryption type whenever a message is sent.

► To Sign and/or Encrypt an Email Message

- 1 Compose the message in Lotus Notes.
- 2 Select the check boxes for **Sign** and/or **Encrypt** in the message's **Delivery Options** (if available in the template). If not, choose Delivery Options and under the Security Options section, select the boxes for **Sign** and/or **Encrypt**.

Note: These check boxes must be selected each time you want to send an email using Notes native encryption unless the boxes are checked in the Default security options.

- 3 Send the message.
 - If mail policy is set to encrypt and the email recipient is a Notes user, the message is sent encrypted using Notes native encryption.
 - If mail policy is set to encrypt and the email recipient is an SMTP address, Lotus Protector for Mail Encryption looks up the recipient's key from the Lotus Protector for Mail Encryption Server and the message is sent encrypted using the Lotus Protector for Mail Encryption Client.
 - If mail policy is set to encrypt and the email recipient is an SMTP address and the email recipient is actually an internal Notes user, Lotus Notes tries to resolve the SMTP address to the Lotus Notes address. If successful, the message is then sent using Notes native encryption. If the SMTP address cannot be resolved into a Lotus Notes address, Lotus Protector for Mail Encryption encrypts the message if a PGP key is found.
 - If mail policy is set to sign, Lotus Notes signs the message with your Notes key. No encryption occurs using Lotus Notes or Lotus Protector for Mail Encryption. Note that if the check box to Sign the message is not selected, Lotus Protector for Mail Encryption signs the message using your PGP key.

If mail policy is set to sign, Lotus Notes signs the message with the sender's Notes key. No encryption occurs using Lotus Notes or Lotus Protector for Mail Encryption. Note that if the box to **Sign** the message is not selected, Lotus Protector for Mail Encryption signs the message using the sender's PGP key.

Using Lotus Protector for Mail Encryption in Microsoft Outlook

Lotus Protector for Mail Encryption encrypts your email messages when you are using Microsoft Outlook 2002 SP3, 2003 (XP) SP3, and 2007 when used with Microsoft Exchange (MAPI) and SMTP email accounts. This feature provides **Sign** and **Encrypt** buttons to explicitly sign, encrypt, or sign and encrypt an email message.

Your Lotus Protector for Mail Encryption Server administrator will have specified if this feature is available and may have disabled this feature by policy.

When enabled in Microsoft Outlook 2002/2003, both buttons appear on the toolbar. When enabled in Microsoft Outlook 2007, both buttons appear on the Message ribbon.





Outgoing email policy determines how the email message is sent. Your Lotus Protector for Mail Encryption Server Administrator will have defined this policy.

The **Sign** and **Encrypt** buttons are an additional feature where you have control over which email needs to be encrypted and/or signed. The buttons are not a replacement for the email proxying used in Lotus Protector for Mail Encryption.

Note: If you reply to or forward an email message that you want to encrypt and/or sign, be sure to select the appropriate buttons. Forwards or replies are treated as new messages and require you explicitly select the options to secure the message.

Use the following procedure whether you are creating a new email message, or forwarding or replying to an email message.

► To sign, encrypt, or sign and encrypt a email message

- 1 Begin composing your email message.
- 2 Do one of the following:
 - To sign only, click **Sign** (). Note that when you choose to sign only, the email will be sent in cleartext.
 - To encrypt only, click **Encrypt** ().
 - To sign *and* encrypt, click both **Sign** and **Encrypt** ( .

Tip: If you have selected one or both buttons and then save the email message as a draft, the buttons remain selected when you continue composing the message.

- 3 Continue composing your email message and send it. The Outlook notifier displays the result of sign and/or encrypt process.

Verifying Encryption Status of Email Messages

When sending email messages in Microsoft Outlook, the Outlook notifier will inform you that the message has been encrypted with the statement "Protector Secured Message."

4

Receiving Email Messages

This section describes how incoming email messages are processed by Lotus Protector for Mail Encryption.

In This Chapter

Viewing Incoming Email Messages.....	11
--------------------------------------	----

Viewing Incoming Email Messages

Lotus Protector for Mail Encryption manages incoming mail messages based on the content of the message.

- **Message not encrypted nor signed.** Lotus Protector for Mail Encryption does nothing to the content of these messages; it simply passes the message along to your email client.
- **Message encrypted and/or signed.** Lotus Protector for Mail Encryption first checks if the message is PGP or S/MIME encrypted. If so, Lotus Protector for Mail Encryption decrypts the message. If Lotus Protector for Mail Encryption fails to decrypt it and the message is S/MIME encrypted, Lotus Protector for Mail Encryption passes the message through so that the Lotus Notes client can decrypt it.

If Lotus Protector for Mail Encryption is unable to either decrypt or verify a message, you might want to consider contacting the sender of the message. If the message could not be decrypted, make sure the sender was using your real public key. If the message could not be verified, ask the sender to publish their key on the PGP Global Directory — older PGP versions or other OpenPGP products can access the web version of this directory at *PGP Global Directory* (<https://keyserver.pgp.com>) , or ask them to send their public key to you directly by email.