IBM® Lotus Protector for Mail Encryption Server

Upgrade Guide

2.1.1

Version Information

Lotus Protector for Mail Encryption Server Upgrade Guide. Lotus Protector for Mail Encryption Server Version 2.1.1. Released December 2012.

This edition applies to version 2, release 1, modification 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

Trademark Information

Symantec, the Symantec Logo, PGP, Pretty Good Privacy, and the PGP logo are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

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 product described in this document is distributed under licenses restricting its use, copying, distribution, and decompilation/reverse engineering. No part of this document may be reproduced in any form by any means without prior written authorization of Symantec Corporation and its licensors, if any.

THE DOCUMENTATION IS PROVIDED"AS IS"AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID. SYMANTEC CORPORATION SHALL NOT BE LIABLE FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES IN CONNECTION WITH THE FURNISHING, PERFORMANCE, OR USE OF THIS DOCUMENTATION. THE INFORMATION CONTAINED IN THIS DOCUMENTATION IS SUBJECT TO CHANGE WITHOUT NOTICE.

The Licensed Software and Documentation are deemed to be commercial computer software as defined in FAR 12.212 and subject to restricted rights as defined in FAR Section 52.227-19 "Commercial Computer Software - Restricted Rights" and DFARS 227.7202, et seq. “Commercial Computer Software and Commercial Computer Software Documentation”, as applicable, and any successor regulations. Any use, modification, reproduction release, performance, display or disclosure of the Licensed Software and Documentation by the U.S. Government shall be solely in accordance with the terms of this Agreement.

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.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510 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

1 About the Lotus Protector for Mail Encryption Server Upgrade Guide

This Upgrade Guide describes how to upgrade previous versions of Lotus Protector for Mail Encryption Server to version 2.1.1.

This section provides a high-level overview of Lotus Protector for Mail Encryption Server.

What is Lotus Protector for Mail Encryption Server

With Lotus Protector for Mail Encryption Server management server, you can manage your organization's security policies, users, keys and configurations, deliver messages to external recipients with or without encryption keys, and defend sensitive data to avoid the financial loss, legal ramifications, and brand damage resulting from a data breach.

Lotus Protector for Mail Encryption Server automatically creates and maintains a Self-Managing Security Architecture (SMSA) by monitoring authenticated users and their email traffic. You can also send protected messages to addresses that are *not* part of the SMSA. The Lotus Protector for Mail Encryption Server encrypts, decrypts, signs, and verifies messages automatically, providing strong security through policies you control.

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, managed by the Lotus Protector for Mail Encryption Server. 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.

The management capabilities of the Lotus Protector for Mail Encryption Server can be extended to managing the Lotus Protector for Mail Encryption Client applications that provide encryption of data on disks, removable media, and mobile devices as well as security of files for collaborating teams.

Using the Lotus Protector for Mail Encryption Server with the Command Line

You can use the Lotus Protector for Mail Encryption Server command line for read-only access to, for example, view settings, services, logs, processes, disk space, query the database, and so on.

Note: If you modify your configuration using the command line, and you do not follow these procedures, your IBM Support agreement is void.

Changes to the Lotus Protector for Mail Encryption Server using command line must be:

- Authorized in writing by IBM Support.
- Implemented by IBM's partner, reseller, or internal employee who is certified in the PGP Advanced Administration and Deployment Training.

- Summarized and documented in a text file in `/var/lib/ovid/customization` on the Lotus Protector for Mail Encryption Server.

Changes made through the command line may not persist through reboots and may become incompatible in a future release. When troubleshooting new issues, IBM Support can require you to revert custom configurations on the Lotus Protector for Mail Encryption Server to a default state.

Symbols

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

Note: Notes are extra, but important, information. A Note calls your attention to important aspects of the product. You can use the product better if you read the Notes.

Caution: Cautions indicate the possibility of loss of data or a minor security breach. A Caution tells you about a situation where problems can occur unless precautions are taken. Pay attention to Cautions.

Warning: Warnings indicate the possibility of significant data loss or a major security breach. A Warning means serious problems will occur unless you take the appropriate action. Please take Warnings very seriously.

Getting Assistance

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

Related Publications

The following documents are companions to the *Lotus Protector for Mail Encryption Server Upgrade Guide* and are available for downloading from the *IBM Lotus Protector for Mail Encryption web site* (*http://www.ibm.com/software/lotus/products/protector/mailencryption*).

- *IBM Lotus Protector for Mail Encryption Server Administrator's Guide*
- *IBM Lotus Protector for Mail Encryption Server Installation Guide*
- *IBM Lotus Protector for Mail Encryption Server Release Notes*
- Online help is installed and is available within the Lotus Protector for Mail Encryption Server product.

2 Upgrading the Lotus Protector for Mail Encryption Server

This chapter describes how to upgrade a previous version of Lotus Protector for Mail Encryption Server to version 2.1.1 for a single server.

Backing Up the Data and Organization Key

Before you upgrade, back up the Organization Key and all the data from your Lotus Protector for Mail Encryption Server. You must back up your data to an external location, because installing the software deletes all data stored on your Lotus Protector for Mail Encryption Server. If you do not (or cannot) use FTP to back up your data to an external location, contact IBM Corporation Support.

To back up your data and organization key

1. Navigate to **Keys > Organization Keys**.
2. Click **Organization Key**.
3. Click **Export**.
4. Select **Export Keypair** and type the passphrase.
5. Click **Export**.

   This saves the Organization Keypair to your desktop.
6. Back up the server data and configuration to an external server location.
7. Select **System > Backups**.
8. Click **Backup Location**.
9. Select **Save Backups to a remote location**.
10. Type the relevant details.
11. Click **Save**.

    You must save the data in a location other than the Lotus Protector for Mail Encryption Server, because the data on the Lotus Protector for Mail Encryption Server is erased during installation.
12. Click **Backup Now** to back up the data.
13. Type a name for your backup.
14. Click **Backup**.

Overview

You can upgrade your Lotus Protector for Mail Encryption Server in the following ways:

- **Migration**, where you back up data to an external source, install the new software version from a CD/DVD, and restore your data. For more information about installing from a CD/DVD, see the *Lotus Protector for Mail Encryption Server Installation Guide*.
- **PUP update**, where you upload and install a PGP Update Package (PUP) file from your Lotus Protector for Mail Encryption Server's administrative interface. This method automatically preserves your data and system settings. However, it is good practice to back up your Lotus Protector for Mail Encryption Server prior to performing the update. For more information on performing a PUP update, see *Upgrading with a PUP Update* (on page 4). The *Lotus Protector for Mail Encryption Server Administrator's Guide* as well as the online help available in your Lotus Protector for Mail Encryption Server also contain detailed instructions.

The following information applies to Lotus Protector for Mail Encryption Servers that are running as stand-alone systems or clusters:

- Before you upgrade to Lotus Protector for Mail Encryption Server 2.1.1, you must back up your data and your organization key to an external location.
- You can upgrade to Lotus Protector for Mail Encryption Server 2.1.1 from 2.1.0.1 using a PUP update.

  Note: You cannot upgrade to 2.1.1 from 2.1. If you are running 2.1, you must first upgrade to 2.1.0.1, then upgrade to 2.1.1
- If you migrate and do a fresh install, the data on your system is deleted. You need the backed up data file and the organization key to encrypt and decrypt the backup file. For more information on installing the software from a DVD, see the *Lotus Protector for Mail Encryption Server Installation Guide*. There are two ways to migrate:
  - Using the Restore setup type in the Setup Assistant
  - Performing a new installation of the software and then restoring your backup through the administrative interface.
  - For details, see *Restoring Configuration and Data* (on page 7).

Caution: It is not possible to upload backups of 2GB or larger through the Lotus Protector for Mail Encryption Server administrative interface. Contact IBM Support for help restoring your data.

Upgrading with a PUP Update

The following describes the steps required to perform an upgrade from a previous version of Lotus Protector for Mail Encryption Server for a single server, using a PUP update file.

If an update is available, you can obtain it from the IBM Corporation web site and save it on your hard drive.

On the **System** > **Updates** page, the **Upload Update Packages** link lets you retrieve update packages saved on your hard drive. You can upload the package, then install it as you would any other update package.

1 Click **Upload Update Packages** to upload an update package from your hard drive.

2 From the **Upload Update** dialog box, browse to find the files you want, then click **Upload**. For Lotus Protector for Mail Encryption Server 2.1.1 use these PUP files:

- LotusPMEServer2.1.1 pup (where *xxx* is the build number)

3 Click the **Install** column to manually install an update. You must install them in the order listed above. The text in the **Date of Last Action** column says *Currently Installing* while the install is in progress.

4 Reboot, when the install completes. Upgrading to 2.1.1 includes an update to the kernel, and if you do not reboot, the system cannot use the updated kernel.

5 Log back into the server.

Note: The **System Settings** screen will not display the correct build number.

Verifying Your Upgrade

After you upgrade to the latest version of Lotus Protector for Mail Encryption Server, you can verify whether the upgrade was successful.

To verify your upgrade

1 Upgrade in one of the following ways:

- Migration
- PUP update

2 After Lotus Protector for Mail Encryption Server restarts, log in.

3 If you upgraded by migrating, select **System > Backups**.

The following links appear:

- **Download migration log file**
- **Download backup log file**

The backup log contains pointers to the line numbers in the migration log, where migration errors are detected. A typical error message in the backup log will look like:

error found at line xxx in <migration log>

The migrated database schema may differ from the default schema in the current release. At the end of the migration, a schema diff tool detects schema discrepancies. If discrepancies are found, an error message is written to the backup log.

4 If you upgraded by PUP updating, select **System > Updates**

The following links appear:

- **Download migration log file**
- **Download update log file**

The update log contains pointers to the line numbers in the migration log, where update errors are detected. A typical error message in the update log will look like:

error found at line xxx in <migration log>

The migrated database schema may differ from the default schema in the current release. At the end of the upgrade, a schema diff tool detects schema discrepancies. If discrepancies are found, an error message is written to the update log

5 Click the appropriate link and open or save the log file.

6 Review the log file. Call IBM Support to resolve the errors and stop them from appearing.

The download links will continue to appear until you resolve your errors and have upgraded successfully.

Best Practices for an Upgrade

The information in this list helps you ensure that your upgrade is successful:

- Install and test the upgrade in a lab or staging environment before you integrate the upgrade into your network.
- Back up the Organization Key and all the data from your Lotus Protector for Mail Encryption Server before you upgrade.

  You must back up your data to an external location, because the upgrade process deletes the data stored on your Lotus Protector for Mail Encryption Server. If you do not (or cannot) use FTP to back up your data to an external location, contact IBM Support (*IBM Lotus Protector Support* (*http://www.ibm.com/software/lotus/products/protector/mailencryption/*)).
- Save a copy of the original installation media, in case you need to revert to the previous version.
- During upgrade, the Lotus Protector for Mail Encryption Server does not process email.

  Before you upgrade Lotus Protector for Mail Encryption Server, you must temporarily remove it from the mail flow.

Reconfiguring the MTA

If your network includes an MTA, you should reconfigure it to prevent email routing through the Lotus Protector for Mail Encryption Server.

To reconfigure the MTA

1. Do one of the following:
   - If your company's email routes through your Lotus Protector for Mail Encryption Server, configure your MTA to halt outbound email processing.
   - If email that matches the criteria in your MTA content filter routes through the Lotus Protector for Mail Encryption Server, configure the MTA to queue this email.
2. Configure the MTA to queue incoming email that passes through the Lotus Protector for Mail Encryption Server, such as signed and/or encrypted email.
3. Review the Lotus Protector for Mail Encryption Server log files to ensure that email is not passing through the Lotus Protector for Mail Encryption Server.
4. Upgrade your Lotus Protector for Mail Encryption Server and restore your user data.
5. Reconfigure your MTA to resume routing email to the Lotus Protector for Mail Encryption Server.

Supported Client and Lotus Protector for Mail Encryption Server Version Combinations

IBM Corporation supports backward compatibility for clients only. Lotus Protector for Mail Encryption Server 2.1.1 supports managing policy of these versions (and subsequent maintenance releases of each) of Lotus Protector for Mail Encryption Client:

- 2.1
- 2.1.0.1

Note: Limited backward compatibility support means that legacy features, such as enrollment, policy download, logging and reporting are supported, but legacy clients cannot access the latest client features in Consumer Policy.

We recommend that you upgrade your Lotus Protector for Mail Encryption Server and your clients, so that they are eventually on the same release.

Lotus Protector for Mail Encryption Server 2.1.1 supports managing policy of these versions (and subsequent maintenance releases of each) of PGP Universal Satellite:

- 3.0
- 3.0.1

Note: Policy options for features that do not exist in supported legacy versions are ignored by those installations.

Restoring Configuration and Data

If you have backed up your data and organization key and performed a new installation of the 2.1.1 software, you can restore your backed-up data in one of the two following ways.

To re store backed up data after installing the server

1. Access the Setup Assistant in the new server.
2. Proceed through the wizard and click **Forward**.
3. Read the License Agreement and the text of the non-IBM terms, then click **I accept both the IBM and non-IBM terms**.
4. In the Setup Type page, select **Restore**, then click **Forward**.
5. In the Import Organization Key page, upload a file containing your Organization Key, then click **Forward.**
6. In the **U**pload Current Backup File page, click **Choose File**, select the backup file from which you want to restore, then click **OK.**
7. When the Upload Current Backup File page appears again, click **Forward**.

   Caution: It is not possible to upload backups of 2GB or larger through the Lotus Protector for Mail Encryption Server web interface. Contact IBM Support (*IBM Lotus Protector Support* (*http://www.ibm.com/software/lotus/products/protector/mailencryption/*)) for help restoring your data.

   After the backup has installed, the **Network Configuration Changed** page appears and the server restarts automatically. You can also check the update or migration logs for the *Database migration check completed* message. You are redirected to the Lotus Protector for Mail Encryption Server administrative interface and the server is configured with the settings from the backup file you selected.

   Your mail policy and proxy settings have been reproduced in the new mail policy feature. For more information on mail policy and reproducing your previous settings, see *Reconsidering Mail Policy Rules* (on page 8) and the *Lotus Protector for Mail Encryption Server Administrator's Guide*.
8. Proceed through the Setup Assistant until you have finished.

   Lotus Protector for Mail Encryption Server runs in Learn Mode.

For more information on configuring the Lotus Protector for Mail Encryption Server after the Setup Assistant is complete, see the *Lotus Protector for Mail Encryption Server Administrator's Guide*.

To restore backed up data on-demand

There are two ways to restore server data from a backup:

- On the Systems Backups page, click the icon in the **Restore** column of the backup from which you want to restore.
- If you have a backup file on your system that is not on the list of backups but from which you would like to restore, click **Upload Backup**, locate the backup file, and then click **Restore**. The Lotus Protector for Mail Encryption Server is restored from the backup file you specified.

Caution: It is not possible to upload backups of 2GB or larger through the Lotus Protector for Mail Encryption Server web interface. Contact IBM Support (*IBM Lotus Protector Support* (*http://www.ibm.com/software/lotus/products/protector/mailencryption/*)) for help restoring your data.

The Lotus Protector for Mail Encryption Server is restored to the state when the backup was performed.

Updating Your IBM Universal Web Messenger Complete Customizations

As a result of some new IBM Universal Web Messenger features, such as PDF Messenger Secure Reply and the ability to provide X.509 certificates to external users, after you upgrade to Lotus Protector for Mail Encryption Server 2.1.1, you must also update your IBM Universal Web Messenger Complete Customizations. For more information on customizing Web Messenger, see "Customizing IBM Universal Web Messenger" in the *Lotus Protector for Mail Encryption Server Administrator's Guide*.

To update your IBM Universal Web Messenger Complete Customization:

9 Select **Services > Web Messenger**.

10 In the **Customization** panel, click **Add New Template**.

11 Read the Customization Notice and click **Continue**.

12 Select **Complete Customization** and click **Next**.

13 Click **Download** next to one of the displayed options.

14 Select a location to save the file and click **Next**.

You should save the downloaded files in the same location as the older customization files. This way, the appropriate files are updated.

15 Zip the locally updated files.

16 Type a template name and click **Next**.

The other fields are optional.

17 Click **Browse** to locate the local Zip file and click **Next**.

The uploaded customization template appears on the Web Messenger page.

Reconsidering Mail Policy Rules

Mail policies, which define the inbound and outbound policy chains, exist in two forms:

- Default mail policy, defined in the product
- Active mail policy, defined by you to reflect your business rules

After a fresh install, default mail policies are in effect. You can change those default policies to reflect your customized business rules, which become the active mail policies.

Following an upgrade, any active mail policies are left intact:

- After a PUP update, your active mail policies remain in effect
- After a migration, you restore your active mail policies from your backed-up data

Even though the upgrade to a next release installs new default mail policies reflecting any changed functionality, any active mail policies override them.

To take advantage of the new default mail policies, click **Restore To Factory Defaults** from the **Mail Policy** screen. Your active business rules are overwritten.

Highlights of the new functionality contained in Lotus Protector for Mail Encryption Server 2.1.1's default mail policy include:

- Opportunistic encryption is no longer used.
  - Mail is secured only if the sender indicates it (uses the **Encrypt** button).
  - The "Excluded Signed" and "Excluded Unsigned" rules are removed.
- An attempt is made to encrypt email if the subject contains "PDF," and a secure PDF message will be delivered if the key is not found.
- PDF Messenger now has a Secure Reply option enabled.

If you overlay your active mail policies by restoring the default mail policies, and then want to reinstate some or all of your customized policies, you will need to add them back manually. For instructions, see "About Restoring Mail Policy Rules" in the *Lotus Protector for Mail Encryption Server Administrator's Guide*.