IBM® Lotus Protector for Mail Encryption Server

Installation Guide

2.1.1

Version Information

Lotus Protector for Mail Encryption Server Installation 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

Limitations

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 Installation Guide

The *Lotus Protector for Mail Encryption Server Installation Guide* provides important IBM® Lotus Protector for Mail Encryption Server concepts and presents a high-level overview of the tasks required to install, set up, and use Lotus Protector for Mail Encryption Server. This guide provides information about how your Lotus Protector for Mail Encryption Server processes email, which helps you integrate your Lotus Protector for Mail Encryption Servers into your network. There is also information on using Microsoft® Exchange Server and Lotus® Domino® Server with PGP Universal Satellite.

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 Installation 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 Add the Lotus Protector for Mail Encryption Server to Your Network

This chapter provides information about how your Lotus Protector for Mail Encryption Server processes email, which can help you decide how to integrate your Lotus Protector for Mail Encryption Servers into your network. It also includes information about using Microsoft Exchange Server and Lotus Domino Server with PGP Universal Satellite.

Server Placement

A Lotus Protector for Mail Encryption Server can be placed in your network in either of two locations in the logical flow of data:

- **Gateway placement**. The Lotus Protector for Mail Encryption Server is located between your external facing mail server and the Internet in the logical flow of data.

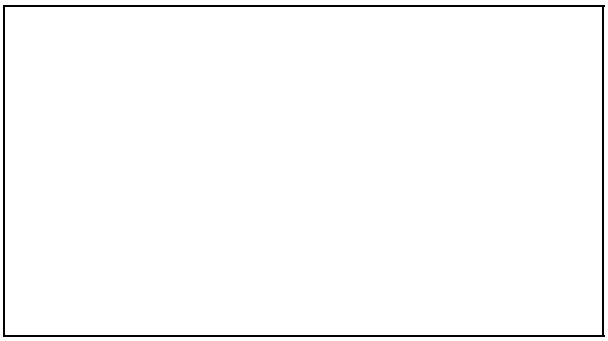
  This is the placement that should be used for the Lotus Protector for Mail Encryption Server in a Lotus Notes environment.

- **Internal placement**. The Lotus Protector for Mail Encryption Server is located between your email users and their local mail server in the logical flow of data.

The Gateway placement is described in more detail in the next section. For information about an internal placement, see the example *Internal Placement Configuration* (on page 38) located in the Configuration Examples section at the end of this guide.

Gateway Placement

With a gateway placement, your Lotus Protector for Mail Encryption Server sits between your mail server and the Internet in the logical flow of data.



1	Lotus Protector for Mail Encryption Server gateway placement
2	Example Corp. DMZ
3	External email user

4	Logical flow of data
5	Example Corp. internal network
6	Example Corp. email users
7	Example Corp. email server

Note: The physical locations of the Lotus Protector for Mail Encryption Server and the mail server are not important. What is important is that, from a mail relay point of view, the Lotus Protector for Mail Encryption Server is between the mail server and the Internet. Both can be on the internal network or in the DMZ.

With a gateway placement, email messages are secured before they are sent to the Internet (on the way to their destination) and decrypted/verified when received from the Internet, over SMTP in both cases.

Note: Email users on your internal network should not be allowed direct access to a Lotus Protector for Mail Encryption Server in gateway placement. Lotus Protector for Mail Encryption Server attempts to enforce this automatically based on your configuration. Configure the mail server to verify From addresses if you intend to use the signing features of Lotus Protector for Mail Encryption Server.

With a gateway placement, messages are stored unsecured on the mail server (unless PGP Universal Satellite is being used).

For Lotus Protector for Mail Encryption Server to create the SMSA, you must make sure to correctly configure your mail server when you are using Lotus Protector for Mail Encryption Servers in gateway placements.

Mail Relay

After processing outgoing email, Lotus Protector for Mail Encryption Server can forward the email to a central mail gateway, which acts as a mail relay. Sites that use explicit mail routing can use mail relay to forward outgoing email to a mail relay that performs explicit routing.

You cannot configure the mail relay during the initial configuration in the Setup Assistant. Instead, you have to configure the server for gateway placement and configure the mail relay in the administrative interface. For more information on configuring the relay on the Outbound or Unified SMTP proxy, see "Creating New or Editing Existing Proxies" in the *Lotus Protector for Mail Encryption Server Administrator's Guide*.

Lotus Domino Server

Lotus Domino Servers and the Lotus Notes email client (versions 7.0.3 and later) are supported in Lotus Protector for Mail Encryption Client and PGP Universal Satellite for Windows®.

For more information about using the Lotus Notes email client, see Lotus Domino Server with PGP Client Software and "Lotus Notes Support" in the *Lotus Protector for Mail Encryption Server Administrator's Guide*.

Microsoft Exchange Server

Messaging Application Programming Interface (MAPI) support is available for Microsoft Exchange Server environments by using Lotus Protector for Mail Encryption Client or PGP Universal Satellite for Windows. MAPI support is not available in PGP Universal Satellite for Mac OS X because there are no MAPI email clients for Mac OS X.

For more information about using MAPI, see *Microsoft Exchange Server with Lotus Protector for Mail Encryption Client Software* (on page 48) and "MAPI Support" in the *Lotus Protector for Mail Encryption Server Administrator's Guide*.

Installation Overview

The following steps are a broad overview of what it takes to plan, set up, and maintain your Lotus Protector for Mail Encryption Server environment.

Steps 1 and 4 are described in detail in this book. The remaining tasks are described in the *Lotus Protector for Mail Encryption Server Administrator's Guide*.

Note that these steps apply to the installation of a new, stand-alone Lotus Protector for Mail Encryption Server. If you plan to install a cluster, you must install and configure one Lotus Protector for Mail Encryption Server following the steps outlined here. Subsequent cluster members will receive most of their configuration settings from the initial Lotus Protector for Mail Encryption Server through data replication.

The steps to install and configure a Lotus Protector for Mail Encryption Server are as follows:

1 **Plan where in your network you want to locate your Lotus Protector for Mail Encryption Server(s).**

Where you put Lotus Protector for Mail Encryption Servers in your network, how many Lotus Protector for Mail Encryption Servers you have in your network, and other factors all have a major impact on how you add them to your existing network.

Create a diagram of your network that includes all network components and shows how email flows; this diagram details how adding a Lotus Protector for Mail Encryption Server impacts your network.

For more information on planning how to add Lotus Protector for Mail Encryption Servers to your existing network, see *Add the Lotus Protector for Mail Encryption Server to Your Network* (on page **Error! Bookmark not defined.**).

2 **Perform necessary DNS changes.**

Add IP addresses for your Lotus Protector for Mail Encryption Servers, an alias to your keyserver, update the MX record if necessary, add keys.<domain>, hostnames of potential Secondary servers for a cluster, and so on.

Properly configured DNS settings (including root servers and appropriate reverse lookup records) are required to support Lotus Protector for Mail Encryption Server. Make sure both host and pointer records are correct. IP addresses must be resolvable to hostnames, as well as hostnames resolvable to IP addresses.

3 **Prepare a hardware token Ignition Key.**

If you want to add a hardware token Ignition Key during setup, install the drivers and configure the token before you begin the Lotus Protector for Mail Encryption Server setup process. For information on how to prepare a hardware token Ignition Key, see "Protecting Lotus Protector for Mail Encryption Server with Ignition Keys" in the *Lotus Protector for Mail Encryption Server Administrator's Guide*.

Note: In a cluster, the Ignition Key configured on the first Lotus Protector for Mail Encryption Server in the cluster will also apply to the subsequent members of the cluster.

4 Install and configure this Lotus Protector for Mail Encryption Server.

The Setup Assistant runs automatically when you first access the administrative interface for the Lotus Protector for Mail Encryption Server. The Setup Assistant is where you can set or confirm a number of basic settings such as your network settings, administrator password, server placement option, mail server address and so on. The details of this process are described in *About Setting Up Lotus Protector for Mail Encryption Server* (on page **Error! Bookmark not defined.**).

Note: If you plan to configure multiple servers as a cluster, you must configure one server first in the normal manner, then add the additional servers as cluster members. You can do this through the Setup Assistant when you install a server that will join an existing cluster, or you can do this through the Lotus Protector for Mail Encryption Server administrative interface. For more information see *Configuring a Cluster Member* (on page 29).

5 Import the PGP key you want to use as your Organization Key with Lotus Protector for Mail Encryption Server and back it up.

Your organization key is used to sign all user keys the Lotus Protector for Mail Encryption Server creates and encrypt Lotus Protector for Mail Encryption Server backups. This key represents the identity of your organization and is the root of the Web-of-Trust for your users.

If your organization uses Lotus Protector for Mail Encryption Client and has a Corporate Key or Organization Key that you want to use with Lotus Protector for Mail Encryption Server, you should import it after configuring your server. If your organization does not have a key to use as your Organization Key, you can use the Organization Key that the Setup Assistant automatically creates with default values. For more information, see "Managing Organization Keys" in the *Lotus Protector for Mail Encryption Server Administrator's Guide*.

Note: Regardless of which key you use as your Organization Key, you must back up the key.

Since Lotus Protector for Mail Encryption Server's built-in backup feature always encrypts backups to this key, you must provide a copy of your Organization Key to restore your data. For more information, see "Organization Certificate" in the *Lotus Protector for Mail Encryption Server Administrator's Guide*.

6 Add the PGP Additional Decryption Key (ADK) that you want to use with Lotus Protector for Mail Encryption Server.

An Additional Decryption Key (ADK) allows you to recover an email message if the recipient is unable or unwilling to do so; every message that is encrypted to the ADK can be opened by the holder(s) of the ADK. You cannot create an ADK with the Lotus Protector for Mail Encryption Server, but if you have an existing PGP ADK generated by Lotus Protector for Mail Encryption Client, you can add it to your Lotus Protector for Mail Encryption Server and use it. For more information, see "Additional Decryption Key (ADK)" in the *Lotus Protector for Mail Encryption Server Administrator's Guide*.

7 Create an SSL/TLS certificate or obtain a valid SSL/TLS certificate.

The Setup Assistant automatically creates a self-signed certificate for use with SSL/TLS traffic. Because this certificate is self-signed, however, it might not be trusted by email or Web browser clients. IBM Corporation recommends that you obtain a valid SSL/TLS certificate for each of your Lotus Protector for Mail Encryption Servers from a reputable Certificate Authority.

This is especially important for Lotus Protector for Mail Encryption Servers that are accessed publicly. Older Web browsers might reject self-signed certificates or not know how to handle them correctly when they encounter them via Protector for Mail Encryption Web Messenger or Mail Encryption Smart Trailer.

For more information, see "Working with Certificates" in the *Lotus Protector for Mail Encryption Server Administrator's Guide*.

8 Configure the Directory Synchronization feature to synchronize an LDAP directory with your Lotus Protector for Mail Encryption Server.

You must have an LDAP directory configured and Directory Synchronization enabled for user enrollment to work. By default user enrollment assumes that you have an LDAP directory configured.

There are two parts to configuring LDAP for user enrollment:

- You must have LDAP enabled on the Domino server to which the Lotus Protector for Mail Encryption Server is communicating.
- To enable LDAP in the Lotus Protector for Mail Encryption Server do the following:
    - Log in to the Lotus Protector for Mail Encryption Server administrative interface, go to **Consumers > Directory Synchronization**, and click **Add LDAP Directory...**
    - You will need to provide information about your LDAP directory:
      - credentials to use to contact the LDAP server (the Bind DN)
      - the addressing information of the server (hostname, port, and protocol)
      - one or more Base DNs to use for lookup.
    - Set **Directory Type** as follows:
      - For a Lotus Domino mail server, select **Lotus Domino**
      - For an MS Exchange mail server, select **Active Directory**
    - When you have tested that Lotus Protector for Mail Encryption Server can communicate with the LDAP directory, you can enable directory synchronization on the **Consumers > Directory Synchronization** page.

For more detailed information, see "Using Directory Synchronization to Manage Users" in the *Lotus Protector for Mail Encryption Server Administrator's Guide*.

9 Add trusted keys, configure consumer policy, and establish mail policy.

All these settings are important for secure operation of Lotus Protector for Mail Encryption Server.

- For more information on adding trusted keys from outside the SMSA, see "Managing Trusted Keys and Certificates".

- For more information about user policy settings, see "Setting Internal User Policy" and "Setting External User Policy".
- For information on setting up mail policy, see "Setting Mail Policy".

All these topics are covered in the *Lotus Protector for Mail Encryption Server Administrator's Guide.*

Note: When setting policy for Consumers, Lotus Protector for Mail Encryption Server provides an option called Out of Mail Stream (OOMS) support. OOMS specifies how the email gets transmitted from the client to the server when Lotus Protector for Mail Encryption Client cannot find a key for the recipient and therefore cannot encrypt the message.

OOMS is enabled by default, as this is the most secure setting. With OOMS enabled, sensitive messages that can't be encrypted locally are sent to Lotus Protector for Mail Encryption Server "out of the mail stream." Lotus Protector for Mail Encryption Client creates a separate, encrypted network connection to the Lotus Protector for Mail Encryption Server to transmit the message. However, archiving solutions, outbound anti-virus filters, or other systems which monitor or proxy mail traffic will not see these messages.

You can elect to disable OOMS, which means that sensitive messages that can't be encrypted locally are sent to Lotus Protector for Mail Encryption Server "in the mail stream" like normal email. Importantly, this email is sent in the clear (unencrypted). Mail or Network administrators could read these messages by accessing the mail server's storage or monitoring network traffic. However, archiving solutions, outbound anti-virus filters, or other systems which monitor or proxy mail traffic will process these messages normally.

During your configuration of your Lotus Protector for Mail Encryption Server you should determine the appropriate settings for your requirements. This option can be set separately for each policy group, and is set through the Consumer Policy settings. For more details on the effects of enabling or disabling OOMS, see "Out of Mail Stream Support" in the *Lotus Protector for Mail Encryption Server Administrator's Guide*.

---

10 Add your Domino domain as a managed domain.

Usually, you specify your Internet domain during installation through the Setup Assistant. If your Lotus Protector for Mail Encryption Server is also managing a Domino server, you must add your Domino domain name manually through the Managed Domains page (**Consumers** > **Managed Domains**).

11 **Install and configure additional cluster server members.**

You can do this through the Setup Assistant when you install a server that will join an existing cluster, or you can do this through the Lotus Protector for Mail Encryption Server administrative interface. Remember that you must configure one server in the normal manner before you can add and configure additional servers as cluster members. For more information, see "Clustering your Lotus Protector for Mail Encryption Servers" in the *Lotus Protector for Mail Encryption Server Administrator's Guide*.

12 **Reconfigure the settings of your email clients and servers, if necessary.**

Depending on how you are adding the Lotus Protector for Mail Encryption Server to your network, some setting changes might be necessary. For example, if you are using a Lotus Protector for Mail Encryption Server placed internally, the email clients **must** have SMTP authentication turned on. For Lotus Protector for Mail Encryption Servers placed externally, you must configure your mail server to relay SMTP traffic to the Lotus Protector for Mail Encryption Server.

13 **Enable SNMP Polling and Traps.**

You can configure Lotus Protector for Mail Encryption Server to allow network management applications to monitor system information for the device on which Lotus Protector for Mail Encryption Server is installed and to send system and application information to an external destination. For more information see "Configuring SNMP Monitoring" in the *Lotus Protector for Mail Encryption Server Administrator's Guide*.

14 **Configure and distribute Lotus Protector for Mail Encryption Client to your users as appropriate.**

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.

Before you can distribute the Lotus Protector for Mail Encryption Client installation file, you need to make the location of the Lotus Protector for Mail Encryption Server available to the client software. For more information, see *Distributing the Lotus Protector for Mail Encryption Client* (on page **Error! Bookmark not defined.**).

15 **Analyze the data from Learn Mode.**

In Learn Mode, your Lotus Protector for Mail Encryption Server sends messages through mail policy without actually taking action on the messages, decrypts and verifies incoming messages when possible, and dynamically creates a SMSA. You can see what the Lotus Protector for Mail Encryption Server would have done without Learn Mode by monitoring the system logs.

Learn Mode lets you become familiar with how the Lotus Protector for Mail Encryption Server operates and it lets you see the effects of the policy settings you have established before the Lotus Protector for Mail Encryption Server actually goes live on your network. Naturally, you can fine tune settings while in Learn Mode, so that the Lotus Protector for Mail Encryption Server is operating just how you want before you go live.

For more information, see "Operating in Learn Mode" in the *Lotus Protector for Mail Encryption Server Administrator's Guide*.

16 **Adjust policies as necessary.**

It might take a few tries to get everything working just the way you want. For example, you might need to revise your mail policy.

17 **Perform backups of all Lotus Protector for Mail Encryption Servers before you take them out of Learn Mode.**

This gives you a baseline backup in case you need to return to a clean installation. For more information, see "Backing Up and Restoring System and User Data" in the *Lotus Protector for Mail Encryption Server Administrator's Guide*.

18 **Take your Lotus Protector for Mail Encryption Servers out of Learn Mode.**

Once this is done, email messages are encrypted, signed, and decrypted/verified, according to the relevant policy rules. Make sure you have licensed each of your Lotus Protector for Mail Encryption Servers. Take them out of Learn Mode.

19 **Monitor the system logs to make sure your Lotus Protector for Mail Encryption Server environment is operating as expected.**

3 About Open Ports

This chapter provides information on the ports a Lotus Protector for Mail Encryption Server has open and on which ports it listens.

TCP Ports

Port	Protocol/Service	Comment
21	**File Transfer Protocol (FTP)**	Used for transmitting encrypted backup archives to other servers. Data is sent via passive FTP, so port 20 (FTP Data) is not used.
22	**Secure Shell (SSH)**	Used for remote shell access to the server for low-level system administration.
25	**Simple Mail Transfer Protocol (SMTP)**	Used for sending mail. With a gateway placement, the Lotus Protector for Mail Encryption Server listens on port 25 for both incoming and outgoing SMTP traffic.
80	**HyperText Transfer Protocol (HTTP)**	Used to allow user access to the Mail Encryption Verified Directory. If the Mail Encryption Verified Directory is not enabled, access on this port is automatically redirected to port 443 over HTTPS. Also used for Universal Services Protocol (USP) keyserver connection.
110	**Post Office Protocol (POP)**	Used for retrieving mail by users with POP accounts with internal placements only. Closed for gateway placements.
143	**Internet Message Access Protocol (IMAP)**	Used for retrieving mail by users with IMAP accounts with internal placements only. Closed for gateway placements.
389	**Lightweight Directory Access Protocol (LDAP)**	Used to allow remote hosts to look up public keys of local users.
443	**HyperText Transfer Protocol, Secure (HTTPS)**	Used for Lotus Protector for Mail Encryption Client, PGP Universal Satellite policy distribution and Protector for Mail Encryption Web Messenger access. Used for access over HTTPS if the Verified Directory is not enabled. Also used for Universal Services Protocol

Port	Protocol/Service	Comment
		(USP) over SSL for keyserver connection.
444	**Simple Object Access Protocol, Secure (SOAPS)**	Used for clustering replication messages.
465	**Simple Mail Transfer Protocol, Secure (SMTPS)**	Used for sending mail securely with internal placements only. Closed for gateway placements. This is a non-standard port used only by legacy mail servers. We recommend not using this port, and instead always using STARTTLS on port 25.
636	**Lightweight Directory Access Protocol, Secure (LDAPS)**	Used to securely allow remote hosts to look up public keys of local users.
993	**Internet Message Access Protocol, Secure (IMAPS)**	Used for retrieving mail securely by users with IMAP accounts with internal placements only. Closed for gateway placements.
995	**Post Office Protocol, Secure (POPS)**	Used for retrieving mail securely by users with POP accounts with internal placements only. Closed for gateway placements.
9000	**HyperText Transfer Protocol, Secure (HTTPS)**	Used to allow access to the Lotus Protector for Mail Encryption Server administrative interface.

UDP Ports

Port	Protocol/Service	Comment
53	**Domain Name System (DNS)**	Used to look up a Fully Qualified Domain Name (FQDN) on the DNS server and translate to an IP address.
123	**Network Time Protocol (NTP)**	Used to synchronize the system's clock with a reference time source on a different server.
161	**Simple Network Management Protocol (SNMP)**	Used by network management applications to query the health and activities of Lotus Protector for Mail Encryption Server and the computer on which it is installed.

4 About Naming your Lotus Protector for Mail Encryption Server

This chapter describes how and why to name your Lotus Protector for Mail Encryption Server using the **keys.<domain>** convention.

How to Name Your Lotus Protector for Mail Encryption Server

Unless a valid public key is found locally, Lotus Protector for Mail Encryption Servers automatically look for valid public keys for email recipients by attempting to contact a keyserver at a special hostname, **keys.<domain>**, where <domain> is the recipient's email domain.

For example, an internal user at example.com sends an email to susanjones@widgetcorp.com. If no valid public key for Susan is found on the Example Lotus Protector for Mail Encryption Server, it automatically looks for a valid public key for Susan at keys.widgetcorp.com, even if there is no domain policy for widgetcorp.com on Example's Lotus Protector for Mail Encryption Server. Keys are found locally if they are cached, or if Susan was an external user who explicitly supplied her key through Protector for Mail Encryption Web Messenger. If the Widgetcorp Lotus Protector for Mail Encryption Server is named using the keys.<domain> convention, the Example Corp. Lotus Protector for Mail Encryption Server can find a valid public key for susan@widgetcorp.com at keys.widgetcorp.com.

Caution: IBM Corporation strongly recommends you name your Lotus Protector for Mail Encryption Server according to this convention, because it allows other Lotus Protector for Mail Encryption Servers to easily find valid public keys for email recipients in your domain. You must also use this convention to name your externally visible Lotus Protector for Mail Encryption Server.

If your organization uses email addresses, such as mingp@example.com and mingp@corp.example.com, your Lotus Protector for Mail Encryption Server must be reachable at **keys.example.com** and **keys.corp.example.com.** If you have multiple Lotus Protector for Mail Encryption Servers in a cluster that are managing an email domain, only one of those Lotus Protector for Mail Encryption Servers needs to use the keys.<domain> convention.

Note: Keys that are found using the keys.<domain> convention are treated as valid and trusted.

Keys.<domain> should be the address of a load-balancing device, which distributes connections to your Lotus Protector for Mail Encryption Server's keyserver service. The ports that need to be load balanced are the ports on which you are running your keyserver service, port 389 for LDAP and 636 for LDAPS. You can also name your Lotus Protector for Mail Encryption Server according to your company's required naming convention and ensure that the server has a DNS alias of keys.<domain>.com.

If you are administering multiple email domains, you should establish the keys.<domain> convention for each email domain. If your Lotus Protector for Mail Encryption Server is behind your corporate firewall, you must ensure that ports 389 (LDAP) and 636 (LDAPS) are open to support the keys.<domain> convention.

Naming Methods

To support the keys.<domain> convention, you can name your Lotus Protector for Mail Encryption Server in one of the following ways:

- In the Setup Assistant, name your Lotus Protector for Mail Encryption Server with the keys.<domain> convention in the **Host Name** field on the **Network Setup** page.
- On the **Network Settings** page, change the host name of your Lotus Protector for Mail Encryption Server to keys.<domain> .
- Create a DNS alias to your Lotus Protector for Mail Encryption Server that uses the keys.<domain> convention that is appropriate for your DNS server configuration.

5 About Installing Lotus Protector for Mail Encryption Server

This chapter provides information about the following:

- Setting up your Lotus Protector for Mail Encryption Server
- System requirements

Installing your Lotus Protector for Mail Encryption Server For a higher-level view of this process, see *Installation Overview* (on page 7).

About Installation

Install and test the installation in a lab or staging environment before integrating the Lotus Protector for Mail Encryption Server into your network.

Lotus Protector for Mail Encryption Server is a customized Linux® installation; it cannot be installed on a Windows server. Every Lotus Protector for Mail Encryption Server requires a dedicated computer that meets the system requirements described in the *Lotus Protector for Mail Encryption Server Release Notes*. Installation deletes all data on the system and reconfigures it as a Lotus Protector for Mail Encryption Server.

Warning: Make sure all data on the system is backed up before you begin the installation.

Note: IBM Corporation strongly recommends locating your Lotus Protector for Mail Encryption Servers in secured areas with restricted access. Only authorized individuals should be granted physical access to Lotus Protector for Mail Encryption Servers.

System Requirements

For the latest system requirements, see the *Lotus Protector for Mail Encryption Server Release Notes*.

You must install the Lotus Protector for Mail Encryption Server software on Lotus Protector for Mail Encryption Server Certified Hardware. You can find the latest Lotus Protector for Mail Encryption Server Certified Hardware List available on IBM Corporation's website.

Lotus Protector for Mail Encryption Server on a VMware ESX Virtual Machine

Before you install Lotus Protector for Mail Encryption Server version 2.1 or later on a virtual machine, ensure that:

- VMware ESXi 4.1, Update 1 is installed.
- You are an administrator with sufficient privileges to perform the required functions.

- You have used the **New Virtual Machine Wizard** to create a virtual machine on the host VMware ESX server with the following requirements:
  - Guest operating system is Linux:
    - Other Linux kernel 2.6 (32 bit)

    This is a required setting.
  - IBM Corporation recommends that you configure at least two virtual CPUs for Lotus Protector for Mail Encryption Server.
  - Have the following as minimums for memory:
    - 4GB of memory on a single server instance
    - 8GB on a two server cluster configuration
    - For additional servers, IBM Corporation recommends additional memory.

    The minimum requirements may also increase depending upon the features in use upon the Lotus Protector for Mail Encryption Servers, such as Gateway Email, PGP Whole Disk Encryption or PGP NetShare.
  - LSI Logic SCSI Adapter as the I/O Adapter type.
    This is a required setting.

    Lotus Protector for Mail Encryption Server does not support the BusLogic SCSI Adapter. If you configure your virtual machine to use this adaptor, a partitioning error occurs during installation.

The remaining options can be configured as appropriate. IBM Corporation recommends that you configure the VMware hardware as if you were configuring a physical server.

Installing VMware Tools for Lotus Protector for Mail Encryption Server

Before you use these commands on the Lotus Protector for Mail Encryption Server, see *Using the Lotus Protector for Mail Encryption Server with the Command Line* (on page 1).

After installing Lotus Protector for Mail Encryption Server, you must install VMware Tools.

To install VMware Tools:

1. Access the Lotus Protector for Mail Encryption Server using the command line with SSH and log in to the server as `root`.

   To set up command line access to the Lotus Protector for Mail Encryption Server, see the instructions in *Accessing the Lotus Protector for Mail Encryption Server using SSH* (on page 19).
2. Run this script:

   ```
   # /usr/bin/install-vmware-tools.sh --version 4.1
   ```
3. When prompted, type `reboot`.

   During reboot, the console messages should indicate that the VMware modules have been loaded correctly (`[OK]`).
4. Run `# lsmod | grep vm` to confirm that the modules have been installed.

   This step should list the VMware modules for ESX 4.1.
5. Run the following commands to confirm that the appropriate processes are running:
   - `# chkconfig --list vmware-tools`

     This step shows whether the VMware modules are correctly set to load during system startup. They should be ON for runlevel 3.

`# ps aux | grep guestd` This should show that /usr/sbin/vmware-guestd is running.

Accessing the Lotus Protector for Mail Encryption Server using SSH

To gain command line access to a Lotus Protector for Mail Encryption Server, you will need to create an SSHv2 key, and add it to the superuser administrator account on the Lotus Protector for Mail Encryption Server. You can do this using a utility such as PuTTYgen to create an SSHv2 key and PuTTY to log in to the command line interface. You add the SSHv2 key to your superuser administrator account through the Lotus Protector for Mail Encryption Server administrative interface.

PuTTY is a free suite of SSH tools. The PuTTY suite includes PuTTYgen, PuTTY, PSFTP, and Pageant the PuTTY authentication agent. The PuTTYgen and PuTTY.exe files are also available to be downloaded separately from many Internet software repositories.

Many SSH utilities can be used to gain command line access. For clarity, the following instructions refer specifically to PuTTY version 0.60.

To create a keypair using PuTTYgen

1. Run PuTTYgen.
2. Confirm the type of key to generate in the Parameters area. The parameters of the key must use one of the SSH-2 options.
3. Create a key pair by clicking on the **Generate** button in the Actions section. Generate some randomness for the key by moving the mouse over the blank area.

Note: The minimum key size when generating a key is 1024 bits. Intermittently PuTTYgen may generate a 1024 bit key as a 1023 bit key due to a bug in PuTTYgen, thereby causing the key not to work properly. The best practice is to generate a key of at least 1025 bit to avoid the potential problem.

To import the SSH V2 key into a Lotus Protector for Mail Encryption Server administrator account

1. Log in as a SuperUser to the Lotus Protector for Mail Encryption Server administrator interface.
2. Go to the **System > Administrators** page then click on a SuperUser administrator account.
3. Click the plus icon (+) at the end of the SSHv2 Key line. This opens the Update SSH Public Key window.
4. Click the **Import Key Block** radio button, paste the public key block that you just generated with PuTTYgen directly into this block, and click the **Import** button.

   After you upload the key block you will notice the hex fingerprint of the key will now show up in SSHv2 Key line.
5. Click **Save** and close the administrative interface.
6. Go back to your desktop and save the public and private key within PuTTYgen.

Note: If your public key is not accepted by the Lotus Protector for Mail Encryption Server when you are trying to paste it in from the PuTTYgen window, make sure you are not accidentally adding whitespace when pasting the keyblock. If it still doesn't work go through the entire key generation process again. From within Puttygen make sure you have clicked at the very bottom: SSH-2 for the type of key to generate. Also, make sure you selected a key size greater than 1024.

To Access the Lotus Protector for Mail Encryption Server using PuTTY

1. Run PuTTY.
2. Enter the Lotus Protector for Mail Encryption Server hostname (keys.<domain>) or IP address in the hostname field.
3. If not already entered, change the **Port** field to use port 22.
4. Select the **SSH** radio button as the protocol.
5. Select **Auth** (under **Category: Connection > SSH**).
6. Browse to your saved private key and select the key file, then click Open in the PuTTy window to start a session.
7. You are prompted to enter a user name. Type `root` and press Enter.

The first time you log on to the Lotus Protector for Mail Encryption Server with PuTTY you are given a security warning. If you trust the host and want to avoid this message in the future, click Yes and proceed as above. You can also click No, PuTTY will connect to the host, but will not add the key to its cache.

Saving your session for future use

You can save your session parameters to simplify logon to Lotus Protector for Mail Encryption Server in the future:

1. Go back to the **Category: Session** tab and type a descriptive name in the box directly under **Saved Sessions**. If you do this and click **Save**. PuTTy will save the current settings you have entered.

   You will notice that the name you typed appears in the larger box as a Saved Session.
2. To access your configured logon for this Lotus Protector for Mail Encryption Server in the future, just double-clicking on the saved session name.

Installation Options

Note: Your system must be set to boot from the DVD.

When you insert the installation DVD and reboot the server, you can select **customnet** as the installation boot option. This option installs the Lotus Protector for Mail Encryption Server using a standard partitioning scheme and configures the network settings based on your inputs during installation. IBM Corporation recommends you perform this default installation to ensure that your Lotus Protector for Mail Encryption Server runs properly when you finish. If the media is invalid, you can use the **mediacheck** boot option to verify the DVD contents before you begin the installation. For more information, see *Verifying the Media on your DVD* (on page 22).

During the default installation, you are prompted to provide the following information:

- IP address
- Subnet mask
- Default gateway
- DNS information
- Hostname

For more information on the information you need to provide, see *Default Installation Procedure* (on page 21).

If you provide the network information during installation, it is pre-loaded into the Setup Assistant. The default installation also simplifies the steps to connect to the Lotus Protector for Mail Encryption Server and continue with the setup. Other installation boot options provide combinations of installation and configuration steps for expert system administrators. If you are considering one of these installation boot options, talk to your Technical Support representative. These options may complicate your ability to connect to and set up your Lotus Protector for Mail Encryption Server. For more information about these options, see *Alternate Installation Procedures* (on page 23).

Default Installation Procedure

To install the Lotus Protector for Mail Encryption Server software using the default installation

1. Set up the system that will be hosting the server in a secure location.
2. Attach a keyboard and monitor to the server on which you are installing Lotus Protector for Mail Encryption Server.
3. Make sure the system is set to boot from the DVD.
4. Insert the Lotus Protector for Mail Encryption Server Installation DVD into the drive.
5. Reboot the system.

   When the system reboots, the install begins.
6. At the prompt, you can either

   Press **Enter** to run the default installation without verifying the DVD or

   - Type **customnet mediacheck** and **Enter** to perform a DVD verification prior to the installation, if you suspect there may be problems with the DVD (this is not usual).

   For details of the media check procedure see *Verifying the Media on your DVD* (on page 22).

A warning appears stating that the installation process erases and repartitions the system's disk.

7 The pre-installation runs for approximately 2 minutes.

When the pre-installation is finished, the **Network Configuration** screen appears. If your system contains multiple network interfaces, these are presented in a list.

Notice that all the network interfaces are set to "Active on boot." If you plan to use multiple interfaces, you should configure them all with IP addresses during this installation step.

8 If you have more than one network interface, highlight the network interface you want to configure and select **Edit**.

The fields for entering the IP address and Netmask appear.

9 Type the IP address and Prefix/Netmask for the selected network interface.

You can enter the Netmask in either dotted quad notation (for example, 255.255.255.0) or in Classless Inter-Domain Routing (CIDR) notation (/24).

10 Select **OK** to return to the list of network interfaces. Note that as you configure each interface, its IP address appears in the list of interfaces.

11 When you have configured the IP address and Netmask for all the network interfaces, select **OK** to continue.

The **Miscellaneous Network Settings** screen appears.

12 Type the IP addresses of the Gateway, Primary DNS, and Secondary DNS, and select **OK**.

The **Hostname Configuration** screen appears.

13 Type the Hostname for the Lotus Protector for Mail Encryption Server, and select **OK**.

The hostname must be the name of the first network interface, as the Lotus Protector for Mail Encryption Server listens on the first interface by default.

IBM Corporation strongly recommends you name your externally visible Lotus Protector for Mail Encryption Server according to the keys.<domain> convention, which allows other Lotus Protector for Mail Encryption Servers to easily find valid public keys for email recipients in your domain. For more information, see *About Naming your Lotus Protector for Mail Encryption Server* (on page **Error! Bookmark not defined.**).

Installation takes approximately 15 minutes, depending on the speed of your disk and type of processor.

When the software is installed, the system automatically ejects the DVD and reboots. After the system reboots, a login prompt appears. **Do not log in here.** You do not need to log in to complete the setup.

14 Connect to the server through the Setup Assistant browser interface at **https://<hostname>:9000** or **https://<IP address>:9000**. To continue with the installation and setup, see *Initial Configuration with Setup Assistant* (on page 25).

Verifying the Media on Your DVD

Before you install Lotus Protector for Mail Encryption Server, verify that the media from which you are installing is error-free by adding **mediacheck** to your installation command.

To complete the media verification:

1 In a default installation, type `customnet mediacheck` and press **Enter**.

2 Click **OK**.

If you click **Skip**, proceed to step 3.

3 Click **Test**.

If the DVD does not pass, eject it, and insert another DVD, but if the DVD passes, click **OK**.

Alternate Installation Procedures

The Lotus Protector for Mail Encryption Server installation provides a variety of installation options, depending on the special needs of your installation. These enable different options for partitions, driver installation, and network configuration.

- Press **F2** at the initial prompt after the installation process has begun to access the alternate installation options.

The following installation options are available:

- **customnet**. The default option: it clears the disk partitions and creates default partitions, then prompts for network configuration information. For instructions about performing this installation, see *Default Installation Procedure* (on page 21).
- **quick**. Clears the disk partitions and makes default partitions. Assigns IP address 192.168.1.100.
- **standard**. Clears disk partitions, but does not make default partitions. Prompts for network configuration information.
- **ks**. The same as standard.
- **expert**. Clears disk partitions, but does not make default partitions. Allows partitioning of removable media, and prompts for a driver disk. Prompts for network configuration information.
- **noautopart**. Clears disk partitions, but does not make default partitions. Assigns non-routable IP address 192.168.1.100.
- **memtest86**. Does not perform the installation, but runs memtest86+ to test the RAM of the system. This test is recommended if you are installing on new hardware that has not been used previously.

You can perform a media verification prior to running the installation by including the **mediacheck** keyword after any of these installation commands. For more information, see *Verifying the Media on your DVD* (on page 22).

Caution: Some of these options may make it more complicated to connect and continue the configuration using a web browser. IBM Corporation strongly recommends that you consult your IBM Technical Support representative before you attempt to use an alternate installation procedure.

---

6 About Setting Up Lotus Protector for Mail Encryption Server

This chapter describes how to access and use the Setup Assistant to configure your Lotus Protector for Mail Encryption Server.

About the Setup Assistant

The Setup Assistant appears the first time you access the Lotus Protector for Mail Encryption Server after installing the software. The Setup Assistant displays a series of screens that ask you questions about your network and about how you want your Lotus Protector for Mail Encryption Server to work; the Setup Assistant uses the answers to those questions to configure your Lotus Protector for Mail Encryption Server.

In many cases, the Setup Assistant performs the majority of the configuration for your Lotus Protector for Mail Encryption Server. You can change any settings you establish with the Setup Assistant anytime after you run it using the administrative interface of the Lotus Protector for Mail Encryption Server; you can also use the administrative interface to configure those features not covered in the Setup Assistant.

The Setup Assistant supports four types of setups:

- **New Installation**. You are configuring a Lotus Protector for Mail Encryption Server to be your only Lotus Protector for Mail Encryption Server or the first server in a cluster.
- **Cluster Member**. This Lotus Protector for Mail Encryption Server will join an existing cluster.
- **Restore**. You are restoring backed-up data from another Lotus Protector for Mail Encryption Server onto a new Lotus Protector for Mail Encryption Server. You need the backed-up data file and the Organization Key used to encrypt the backup file.
- **Keyserver**. You are migrating the keys and data from a PGP Keyserver to a Lotus Protector for Mail Encryption Server.

All four setup types have a common beginning: you read the End User License Agreement, specify the type of setup, and configure the network settings for your Lotus Protector for Mail Encryption Server, then the Lotus Protector for Mail Encryption Server is restarted. Once the Lotus Protector for Mail Encryption Server is restarted, you can connect to it via a Web browser and continue with the rest of the Setup Assistant.

Initial Configuration with Setup Assistant

The Setup Assistant guides you through establishing the Lotus Protector for Mail Encryption Server's network configuration and setup type.

After the software installs and the server restart, you can connect to the Lotus Protector for Mail Encryption Server via a Web browser at the configured IP address and finish running the Setup Assistant.

1 Open a Web browser and connect to the Lotus Protector for Mail Encryption Server:

- If you chose the default installation (**customnet**) or the **standard**, **ks**, or **expert** installation options, connect to **https://<hostname>:9000**, using the hostname or IP address you assigned to the Lotus Protector for Mail Encryption Server.
- If you chose the **quick** or **noautopart** installation, and you are using a client computer with a fixed IP address, connect to https://192.168.1.100:9000**,** as explained in the section *Preparing for Setup after a "quick" Install* (on page 30).

The Welcome screen of the Setup Assistant appears.

2 Read the text, then click the **Forward** arrow to continue.

The Software License Agreement page appears.

3 Select from the drop-down menu the language in which you want the agreement to appear.

4 Read the text of the License Agreement, and the text of the non-IBM terms, then click the **I accept both the IBM and non-IBM terms** button.

The Setup Type screen appears.

5 Make the appropriate selection:

- Select **New Installation** if this is a new Lotus Protector for Mail Encryption Server installation, and this server will be the only Lotus Protector for Mail Encryption Server in your network, or it will be the first server in a cluster.
- Select **Cluster Member** if this Lotus Protector for Mail Encryption Server will join an existing Lotus Protector for Mail Encryption Server cluster.

  You must have one Lotus Protector for Mail Encryption Server already installed and configured before you can install a second Lotus Protector for Mail Encryption Server as a cluster member. The initial Lotus Protector for Mail Encryption Server acts as the sponsor for the second Lotus Protector for Mail Encryption Server, and must initiate an Add Cluster Member request for the cluster member you plan to install.

  For more information, see "Clustering your Lotus Protector for Mail Encryption Servers" in the *Lotus Protector for Mail Encryption Server Administrator's Guide*.
- Select **Restore** if you want to restore the data from a server backup. You need your Organization Key and access to the backup file to proceed with this installation.
- Select **Keyserver** if you want to migrate the keys on an existing PGP Keyserver to the Lotus Protector for Mail Encryption Server you are configuring. .

6 Click the **Forward** arrow to continue.

The Date & Time screen appears.

Your server preforms many time-based operations, so it is important to set up the correct time.

7 From the **Time Zone** menu, select your location.

8 Choose **Time Format** and **Date Format** settings.

9 Set the correct **Time** and **Date**.

10 Optionally, specify an NTP time server in the **NTP Server** field. The Lotus Protector for Mail Encryption Server automatically synchronizes the time when the Setup Assistant is finished.

11 Click the **Forward** arrow to continue.

The Network Setup screen appears.

12 If you chose the default (**customnet**) or standard installation, this information is already present. Otherwise, type the appropriate information:

a In the **Hostname** field, type a name for this Lotus Protector for Mail Encryption Server. This must be a fully-qualified domain name of the external, untrusted interface.

IBM Corporation strongly recommends you name your externally visible Lotus Protector for Mail Encryption Server according to the keys.<domain> convention, which allows other Lotus Protector for Mail Encryption Servers to easily find valid public keys for email recipients in your domain.

For example, Example Corporation names its externally visible Lotus Protector for Mail Encryption Server "keys.example.com." For more information, see *About Naming your Lotus Protector for Mail Encryption Server* (on page **Error! Bookmark not defined.**).

b In the **IP Address** field, type an IP address for this Lotus Protector for Mail Encryption Server.

c In the **Subnet Mask** field, type a subnet mask for this Lotus Protector for Mail Encryption Server.

d In the **Gateway** field, type the IP address of the default gateway for the network.

e In the **DNS Servers** field, type the IP address(es) of the DNS servers for your network.

13 Click the **Forward** arrow to continue.

The Confirmation screen appears.

14 Make sure the information is correct, then click **Done**.

Click the **Back** arrow if you need to go back and make any changes.

The Network Configuration Changed dialog box appears, while the server restarts automatically.

If you chose the default installation (**customnet**) or the **standard**, **ks**, or **expert** installation options, skip step 15 and go on to the next section, *New Installation Configuration* (on page 27).

If you chose the **quick** or **noautopart** installation, go on to the next step. At this point, your Lotus Protector for Mail Encryption Server has accepted the new network settings you typed, so you can disconnect the temporary setup.

15 Disconnect the cable between the client computer and the Lotus Protector for Mail Encryption Server, return the settings of the client computer back to what they were, connect the two computers back to the original network, and continue with the Setup Assistant.

New Installation Configuration

If you selected **New Installation** as the configuration type for the Lotus Protector for Mail Encryption Server, the Administrator Name & Passphrase page appears automatically.

1 On the Administrator Name & Passphrase page, type the administrator's login name in the **Login Name** field.

2 In the **Passphrase** field, type the administrator's passphrase.

3 In the **Confirm** field, type the same passphrase.

4 In the **Email Address** field, type the administrator's email address. This is optional and enables the administrator to receive a daily status email.

5 Click the **Forward** arrow to continue.

The Mail Processing page appears.

6 Specify the placement of this Lotus Protector for Mail Encryption Server in your network:

- Select **Gateway Placement** if your Lotus Protector for Mail Encryption Server is logically located between your mail server and the Internet.
- Select **Internal Placement** if your Lotus Protector for Mail Encryption Server is logically located between your email users and your mail server, or if your Lotus Protector for Mail Encryption Server is out of the mailstream.

7 Click the **Forward** arrow to continue.

The Mail Server Selection page appears.

8 In the **Mail Server** field, type the hostname or IP address of the mail server that this Lotus Protector for Mail Encryption Server interacts with.

9 In the **Proxy Server** field, type an optional additional mail server to which all outbound mail is sent. This only applies if you are installing your Lotus Protector for Mail Encryption Server in gateway placement.

10 In the **Primary Domain** field, type the email domain that the Lotus Protector for Mail Encryption Server manages.

11 Click the **Forward** arrow to continue.

The Ignition Keys page appears.

Ignition Keys protect the data on your Lotus Protector for Mail Encryption Server if an unauthorized person gets control of it. If you want to use a hardware Ignition Key, prepare the token before you add it to the system here. See "Protecting Lotus Protector for Mail Encryption Server with Ignition Keys" in the *Lotus Protector for Mail Encryption Server Administrator's Guide* for information on how to prepare a hardware token Ignition Key.

Note: If this Lotus Protector for Mail Encryption Server will be used as the initial member in a cluster, this Ignition Key is replicated to all additional cluster members. New cluster members that are sponsored by this Lotus Protector for Mail Encryption Server will be initially locked with this Ignition Key.

Click **Skip** to proceed with the Setup Assistant without configuring an Ignition Key.

12 To configure an ignition key, select the type of Ignition Key you would like to use, then click the **Forward** arrow.

The appropriate Ignition Key page appears.

13 Type a name for the Ignition Key, a passphrase, confirm the passphrase, then click the **Forward** arrow.

The Backup Organization Key page appears.

The Lotus Protector for Mail Encryption Server generates an Organization Key for you. If you want to generate an S/MIME Organization Certificate, do so immediately after finishing setup. For information about the Organization Key and Organization Certificate, see "Managing Organization Keys" in the *Lotus Protector for Mail Encryption Server Administrator's Guide*.

14 Type and confirm a passphrase to protect the Organization Key (optional, but strongly recommended), then click **Backup Key** to back up the key. Be aware that without a backup of your Organization Key, you cannot restore your Lotus Protector for Mail Encryption Server from backed-up data.

To skip backing up your Organization Key (not recommended), click **Forward** without backing up the key.

15 Click the **Forward** arrow to continue.

The Confirmation page appears.

This page summarizes the configuration of your Lotus Protector for Mail Encryption Server.

16 Click **Done** to finish setup.

The Configuration Changed page appears, and the server restarts automatically.

You are redirected to the administrative interface of the Lotus Protector for Mail Encryption Server you just configured.

Your Lotus Protector for Mail Encryption Server is initially configured in Learn Mode. For more information, see "Operating in Learn Mode" in the *Lotus Protector for Mail Encryption Server Administrator's Guide*.

Configuring a Cluster Member

Note: In order to set up a Lotus Protector for Mail Encryption Server as a cluster member, it must be sponsored by an existing Lotus Protector for Mail Encryption Server. The sponsoring Lotus Protector for Mail Encryption Server must initiate an Add Cluster Member request, specifying the server that will be joining the cluster.

On the sponsoring server, the Administrator must perform an **Add Cluster Membe**r request, specifying the Lotus Protector for Mail Encryption Server you are installing as a cluster member (the joining server). The joining server is then added as a pending member of the cluster, with a **Contact** button available that allows the sponsor to initiate the join process.

See "Clustering your Lotus Protector for Mail Encryption Servers" in the *Lotus Protector for Mail Encryption Server Administrator's Guide* for more detailed instructions on adding a cluster member.

If you selected **Cluster Member** as the configuration type for the Lotus Protector for Mail Encryption Server, the Join Cluster page appears automatically.

1 Type the Hostname or IP Address of the Lotus Protector for Mail Encryption Server that is acting as the sponsor for this joining server, then click the **Forward** arrow.

The Lotus Protector for Mail Encryption Server again reboots, and then the Waiting for Cluster Host page appears. This message continues to be displayed until an administrator logs into the sponsoring server's administrative interface, and click the **Contact** button to initiate the join with this server you are installing.

When contact is received from the sponsoring Lotus Protector for Mail Encryption Server the Waiting message is replaced by the Replicating Cluster Data page. This displays a progress bar that indicates the progress of the data replication process.

The configuration settings for the Lotus Protector for Mail Encryption Server you are installing as a cluster member (administrator login and password, primary domain, ignition key (if any)) are replicated from the sponsoring server.

When the replication process is complete, the Lotus Protector for Mail Encryption Server Administrative Interface Login page is displayed.

Note: The replication process has copied many of the configuration settings from the sponsor Lotus Protector for Mail Encryption Server. This includes the administrator login name(s) and password(s), and a number of other settings.

Important: If the sponsoring server was configured to use an Ignition Key, that key is replicated to this Lotus Protector for Mail Encryption Server and thus when the server restarts it is automatically locked, and must be unlocked using the ignition key or organization key (also a global key).

Restore From a Server Backup

To configure a Lotus Protector for Mail Encryption Server with data that you backed up, you need to have the appropriate backup file and the Organization Key on the setup computer. When you restore from a backup, everything that was configured, including network, proxy and policy settings, keys, and user information is restored.

For information on configuring a Lotus Protector for Mail Encryption Server through the Setup Assistant with data from a backup, see the *Lotus Protector for Mail Encryption Server Upgrade Guide*.

Preparing for Setup after a "quick" Install

If you chose the default installation option (**customnet**) or the **standard**, **ks**, or **expert** options, go to Initial Configuration with Setup Assistant. All these installation options configure your network settings as part of the installation process.

If you chose the **quick** or **noautopart** installation, you must gather materials and information before you can continue with the setup.

Hardware

Before you configure your Lotus Protector for Mail Encryption Server using the Setup Assistant, you must have the following:

- A Web browser on a Windows or Mac OS X computer, which allows you to run Setup Assistant.
- A crossover Ethernet cable to connect a Windows or Mac OS X computer to the Lotus Protector for Mail Encryption Server.

System Information

You also need some information to configure your Lotus Protector for Mail Encryption Server:

- Connect through the temporary IP address and subnet of the newly installed Lotus Protector for Mail Encryption Server, which will be used for the initial configuration portion of the Setup Assistant:

  IP: 192.168.1.100:9000

  Subnet: 255.255.255.0

  Use this data to connect to the Lotus Protector for Mail Encryption Server you are configuring in the initial configuration portion of the Setup Assistant, before the Lotus Protector for Mail Encryption Server is available via a Web browser.
- An IP address, name, gateway, and DNS server information for the Lotus Protector for Mail Encryption Server.
- You can also need other data, such as your Organization Key or a saved backup, depending on the type of setup you are performing.

Connecting to the Lotus Protector for Mail Encryption Server

To continue the installation and setup, you must have a crossover Ethernet cable to connect to the Lotus Protector for Mail Encryption Server. Configure the client computer with a fixed IP address and access the Lotus Protector for Mail Encryption Server from this computer.

To connect to the Lotus Protector for Mail Encryption Server

2 Type the following information to configure the client computer:

IP: `192.168.1.99`

Subnet: `255.255.255.0`

If you are using a Mac OS X client computer, save this temporary setup as a separate location in **Network Preferences** (for example, `setup`).

3 Continue your set up as described in Initial Configuration with Setup Assistant.

7 Distributing the Lotus Protector for Mail Encryption Client

The 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.

This section describes how to prepare the client installation file for distribution to your end users.

Preparing the Lotus Protector for Mail Encryption Client for Installation

The client installer program is an .MSI file that you distribute to your Lotus Notes and Microsoft Exchange users.

Before you can distribute the Lotus Protector for Mail Encryption Client installation file, you need to make the location of the Lotus Protector for Mail Encryption Server available to the client software. This is called the Lotus Protector for Mail Encryption Server Stamp. In addition, there are switches you set to indicate whether the client will support both Lotus Notes and Microsoft Exchange (MAPI), and how Lotus Protector for Mail Encryption Client functionality will affect PGP Desktop if both are installed concurrently on the user's system.

There are several methods you can use for providing this configuration information for the client installer:

- Providing an edited Notes.ini file for your Lotus Notes clients that contains the Lotus Protector for Mail Encryption Server Stamp and other configuration settings.
- Setting switches in the .msi file using Microsoft's msiexec application, or by using a transform file.
- Providing a PMEConf.dat file with the Lotus Protector for Mail Encryption Client configuration information.

There are four configuration settings that you can set in one of the configuration files, or in the .msi file. These are:

- PME_SERVER_CONFIG: This is the server stamp - set it to the location of the Lotus Protector for Mail Encryption Server. This must be in the form `<name>.<domain>` - for example `pme.example.com`.
- PME_INSTALL_NOTES: Values are 1 (default) or 0. This flag indicates whether the client should be installed for use with Lotus Notes.
- PME_INSTALL_MAPI: Values are 1 (default) or 0. This flag indicates whether the client should be installed for use with Microsoft Outlook.

- PME_OVERRIDE_DESKTOP: Values are 0(default) or 1. This flag is used only when Lotus Protector for Mail Encryption Client and PGP Desktop are both installed on the same system.

  When PME_OVERRIDE_DESKTOP=1, Lotus Protector for Mail Encryption Client will encode and decode messages instead of PGP Desktop. By default (when PME_OVERRIDE_DESKTOP=0) PGP Desktop takes priority over Lotus Protector for Mail Encryption Client.

Editing the Notes.ini File

You can add the Lotus Protector for Mail Encryption Client configuration options to the Notes.ini file that is distributed to your Notes users.

The Lotus Protector for Mail Encryption Client options need to be under the "[Notes]" section as follows:

```
[Notes]

PME_SERVER_CONFIG=pme.example.com

PME_INSTALL_NOTES=1

PME_INSTALL_MAPI=1

PME_OVERRIDE_DESKTOP=1
```

Note that because PME_OVERRIDE_DESKTOP is set to 1, the Lotus Protector for Mail Encryption Client will always perform message encoding and decoding, even if PGP Desktop is also installed.

Configuring the .MSI File

You can use Microsoft's msiexec to set the values of the PME options in the .msi file.

The syntax of the command is:

`> msiexec /I <msi file> PME_<option>=<value>` For example:

```
> msiexec /I pmeclient.msi PME_SERVER_CONFIG=pme.example.com
```

You can set multiple Lotus Protector for Mail Encryption Client options using a single command. For example:

```
> msiexec /I pmeclient.msi PME_SERVER_CONFIG=pme.example.com
PME_INSTALL_NOTES=1 PME_INSTALL_MAPI=1 PME_OVERRIDE_DESKTOP=1
```

Editing the PMEConf.dat File

You can add the Lotus Protector for Mail Encryption Client configuration options to a PMEConf.dat file that you distribute to your Outlook-only users.

The first line of the PMEConf.dat file should be "[Notes]".

The following is a sample PMEConf.dat file:

```
[Notes]

PME_SERVER_CONFIG=pme.example.com

PME_INSTALL_NOTES=1

PME_INSTALL_MAPI=1
```

Note that because the PME_OVERRIDE_DESKTOP option is not specified, if PGP Desktop is installed concurrently with Lotus Protector for Mail Encryption Client, the PGP Desktop will take priority for encoding and decoding PGP messages.

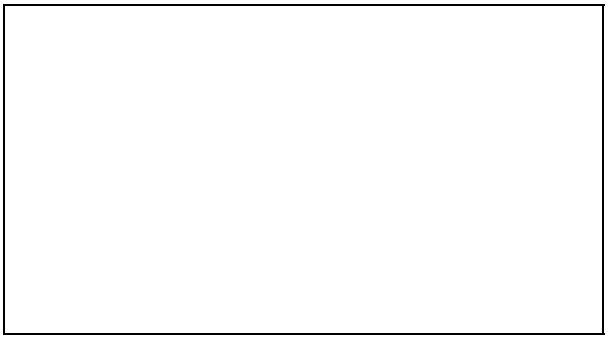
If both Notes.ini and PMEConf.dat are present, the configuration in Notes.ini will be used.

A Configuration Examples

This section shows and describes potential configurations for Lotus Protector for Mail Encryption Server:

Gateway Placement Configuration

In this example, Example Corporation has its Lotus Protector for Mail Encryption Server in a gateway placement.



1	Lotus Protector for Mail Encryption Server gateway placement
2	Example Corp. DMZ
3	External email user

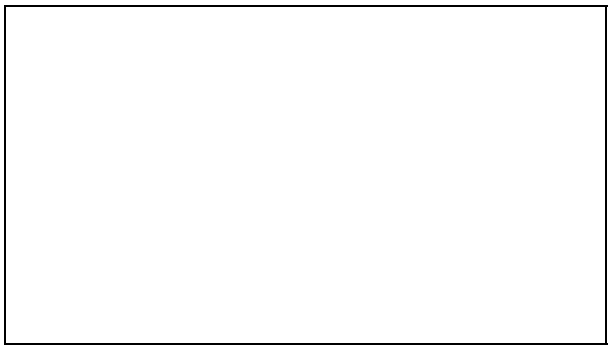
4	Logical flow of data
5	Example Corp. internal network
6	Example Corp. email users
7	Example Corp. email server

Settings for 1:	Notes:
Server type: **New Installation** Mail processing: **Gateway placement** Hostname: **mail-gw.example.com** Mail server: **mail.example.com** IP Address, Subnet Mask, Gateway, and DNS Servers: **As appropriate**	Add or modify the MX record for **example.com** to point to Lotus Protector for Mail Encryption Server's IP address on **mail-gw.example.com**. Also in DNS, create an alias **keys.example.com** that points to **mail-gw.example.com**. Mail server must be configured to relay through the Lotus Protector for Mail Encryption Server.

Gateway placement also supports external email users via Mail Encryption Smart Trailers or Protector for Mail Encryption Web Messenger mail.

Internal Placement Configuration

In this example, Example Corporation has one main office but wants to support external email users.



1	Lotus Protector for Mail Encryption Server internally placed
2	Example Corp. email server
3	External email user
4	Logical flow of data
5	Example Corp. internal network
6	Example Corp. email users

Settings for 1:	Notes
Server type: **New Installation** Mail processing: **Internal placement** Hostname: **mail.example.com** Mail server: **mail-1.example.com** IP Address, Subnet Mask, Gateway, and DNS Servers: **As appropriate**	Change the name of the mail server (previously **mail.example.com)** to **mail-1.example.com,** and name the Lotus Protector for Mail Encryption Server **mail.example.com**. End users might require no changes to their configuration; SMTP Authentication might need to be enabled for end users. Create a DNS alias for **keys.example.com** to point to the Lotus Protector for Mail Encryption Server.

By placing the server in the DMZ, the company can use an internal placement (which means its messages are encrypted even while on its mail server) and still support external email users via Mail Encryption Smart Trailers, Protector for Mail Encryption Web Messenger mail, or PGP Universal Satellite.

Note: The physical location of the Lotus Protector for Mail Encryption Server and the mail server are not important. What is important is that, from a mail relay point of view, the Lotus Protector for Mail Encryption Server is between the email users and the mail server. Both can be on the internal network or in the DMZ. From a performance perspective, it is generally advisable to put them next to each other on the same network.

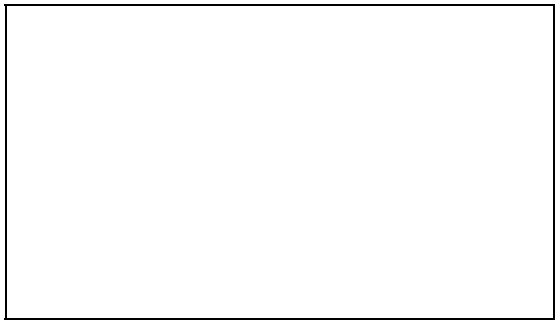
With an internal placement of your Lotus Protector for Mail Encryption Server, messages are secured based on the applicable policies when they are sent to the mail server using SMTP; they are decrypted and verified when they are retrieved from the mail server using POP or IMAP.

With an internal placement, messages are stored secured on the mail server. Messages are only transmitted unencrypted between the internal user and the Lotus Protector for Mail Encryption Server, then only if PGP Universal Satellite has not been deployed globally to your internal users. If your mail server is configured for SSL/TLS communications with the email client, the messages can be passed through that encrypted channel thus maintaining encryption along the entire path.

For Lotus Protector for Mail Encryption Server to create the SMSA, email clients must have SMTP authentication turned on when they are communicating with a Lotus Protector for Mail Encryption Server in an internal placement.

Non-mailstream Placement Configuration

In this example, Example Corporation has a Lotus Protector for Mail Encryption Server placed outside the mailstream. The Lotus Protector for Mail Encryption Server integrates with Lotus Protector for Mail Encryption Client to provide automated user enrollment and real-time end-user security policy management.



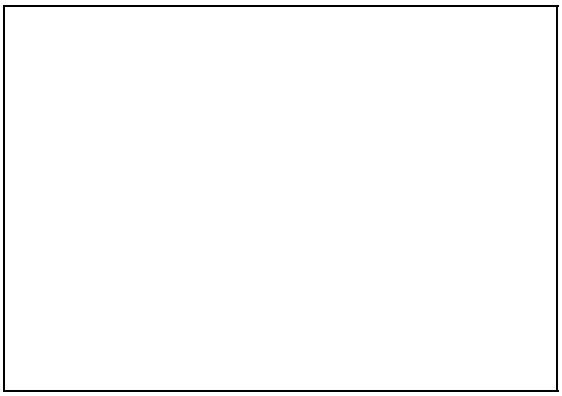
1 Lotus Protector for Mail Encryption Server policy/management

2	Example Corp. email server
3	Example Corp. DMZ
4	External email user
5	Logical flow of data
6	Example Corp. internal network
7	Example Corp. email users

Settings for 1:	Notes:
Server type: **New Installation** Mail processing: **None** IP Address, Subnet Mask, Gateway, and DNS Servers: **As appropriate**	Lotus Protector for Mail Encryption Server is outside of mailstream. All encryption, decryption, signing, and verification is done through Lotus Protector for Mail Encryption Client.

Cluster Configuration

In this example, Example Corporation has a cluster, with multiple Lotus Protector for Mail Encryption Servers proxying messages on its internal network, and another server in the DMZ that performs keyserver and Protector for Mail Encryption Web Messenger functions only.



1	Lotus Protector for Mail Encryption Server Keyserver/Web Messenger
2	Example Corp. email server
3	Logical flow of data
4	Example Corp. internal network
5	Manufacturing - Lotus Protector for Mail Encryption Server internally placed
6	Development - Lotus Protector for Mail Encryption Server internally placed
7	Administration - Lotus Protector for Mail Encryption Server internally placed
8	Example Corp. DMZ

Notes:

One internally placed Lotus Protector for Mail Encryption Server configured as the first server in the Cluster; the others and the keyserver configured as cluster members.

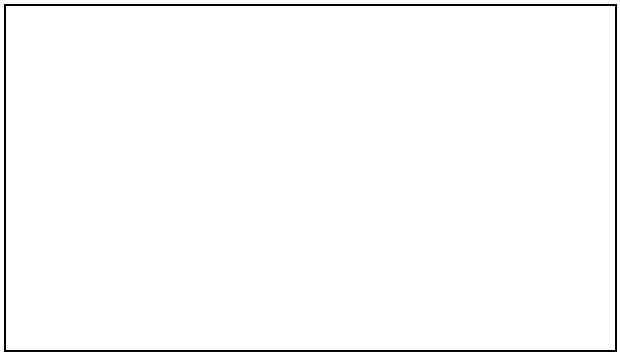
Mail server does not relay through the keyserver Lotus Protector for Mail Encryption Server.

Cluster port (444) on firewall between the internally placed servers and the keyserver must be opened.

No mail proxies configured on the keyserver.

Clustered Proxy and Keyserver Configuration

In this example, Example Corporation has a cluster, with one Lotus Protector for Mail Encryption Server proxying messages on its internal network, and another server in the DMZ that performs keyserver and Protector for Mail Encryption Web Messenger functions only.



1	Lotus Protector for Mail Encryption Server internally placed
2	Lotus Protector for Mail Encryption Server Keyserver/Web Messenger
3	Example Corp. email server
4	Example Corp. DMZ
5	External email user
6	Logical flow of data
7	Example Corp. internal network
8	Example Corp. email users

Settings for 1:	Settings for 2:
Server type: **New Installation** (first server in the cluster) Mail processing: **Internal placement** Hostname: **mail.example.com** Mail server: **mail-1.example.com** IP Address, Subnet Mask, Gateway, and DNS Servers: **As appropriate**	Server type: **Cluster Member** Mail processing: determined by first server in the cluster (Server 1) Hostname: **keys.example.com** IP Address, Subnet Mask, Gateway, and DNS Servers: **As appropriate**

Notes:

mail.example.com becomes **mail-1.example.com**. Lotus Protector for Mail Encryption Server becomes **mail.example.com**.

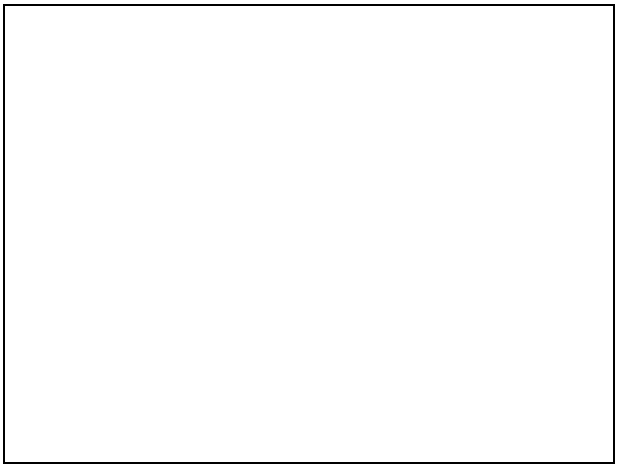
Mail server does not relay through **2**.

Cluster port (444) on firewall between the two servers *must* be opened.

To support external users via Protector for Mail Encryption Web Messenger, designate the keyserver as a Protector for Mail Encryption Web Messenger server.

Gateway Cluster with Load Balancer

In this example, Example Corporation is using an F5 BIG-IP load balancer to handle address rotation between the Lotus Protector for Mail Encryption Servers in the cluster, ensuring that traffic goes through all of them.



1	F5 BIG-IP Load Balancer
2	Lotus Protector for Mail Encryption Server 1
3	Lotus Protector for Mail Encryption Server 2
4	Lotus Protector for Mail Encryption Server 3
5	Logical flow of data

6	Example Corp. internal network
7	Example Corp. email users
8	Example Corp. DMZ
9	Example Corp. email server

Settings for 1:

Virtual server for trusted interface: **cluster-gw-internal.example.com**

Virtual server addresses: **Trusted interfaces for hosts 2, 3, and 4, port 25**

Virtual server for untrusted interface: **cluster-gw.example.com**

Virtual server addresses: **Untrusted interfaces for hosts 2, 3, and 4, ports 25 and 389**

IP Address, Subnet Mask, Gateway, and DNS Servers: **As appropriate**

Settings for 2:

Server type: **New Installation**

Mail processing: **Gateway placement**

Hostname: **cluster1-gw.example.com**

Mail server: **mail.example.com**

IP Address, Subnet Mask, Gateway, and DNS Servers: **As appropriate**

Settings for 3:

Server type: **Cluster Member**

Hostname: **cluster2-gw.example.com**

IP Address, Subnet Mask, Gateway, and DNS Servers: **As appropriate**

Settings for 4:

Server type: **Cluster Member**

Hostname: **cluster3-gw.example.com**

IP Address, Subnet Mask, Gateway, and DNS Servers: **As appropriate**

Notes:

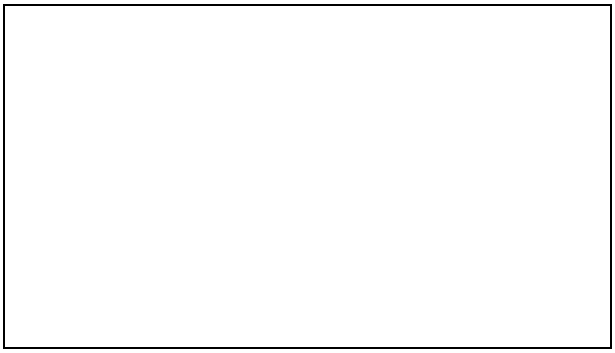
Add DNS MX record that points to **cluster-gw.example.com**.

Also in DNS, create an alias from **cluster-gw.example.com** to **keys.example.com**.

The mail server must be reconfigured to relay through **cluster-gw-internal.example.com**.

Encircled Configuration

Using Lotus Protector for Mail Encryption Server in an encircled configuration is an alternative to placing two Lotus Protector for Mail Encryption Servers in a clustered internal/gateway placement, when you have internal MAPI clients running PGP Universal Satellite in addition to non-MAPI clients using POP, IMAP, and SMTP.



1	Lotus Protector for Mail Encryption Server internally placed
2	Example Corp. email server
3	Example Corp. DMZ
4	External email user
5	Example Corp. internal network
6	Example Corp. email users

Settings for 1:

Server type: **New Installation**

Mail processing: **Internal placement**

Hostname: **mail.example.com**

Mail server: **mail-1.example.com**

IP Address, Subnet Mask, Gateway, and DNS Servers: **As appropriate**

Protector for Mail Encryption Web Messenger and keyserver functionality enabled

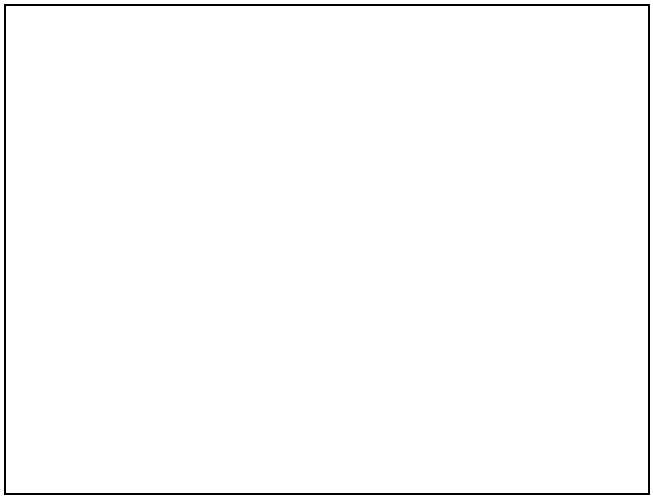
Notes:

Add DNS MX record that points to **mail.example.com**.

Optional: to hide internal Lotus Protector for Mail Encryption Server IP from outside, use 2nd IP in the DMZ.

Large Enterprise Configuration

As a large enterprise, Example Corporation has a sophisticated network that includes multiple Lotus Protector for Mail Encryption Servers that are load balanced, a separate Lotus Protector for Mail Encryption Server for Protector for Mail Encryption Web Messenger and keyserver support, and a standalone Mail Transfer Agent (MTA).



1	Lotus Protector for Mail Encryption Server Keyserver/Web Messenger
2	Example Corp. DMZ
3	Example Corp. email server
4	F5 BIG-IP Load Balancer
5	Lotus Protector for Mail Encryption Server 1
6	Lotus Protector for Mail Encryption Server 2
7	Lotus Protector for Mail Encryption Server 3
8	MTA
9	Example Corp. internal network
10, 11	Example Corp. email user

The company uses its MTA to perform static email routing and to establish rules that govern which email messages are processed by Lotus Protector for Mail Encryption Server and which are not. Naturally, the features of the MTA being used govern what it can be used for.

Note: IBM Corporation does not recommend any specific MTA for use with Lotus Protector for Mail Encryption Server. Make sure the MTA you decide to use is correctly configured for use with Lotus Protector for Mail Encryption Server.

Spam Filters and Lotus Protector for Mail Encryption Server

Example Corporation has both a content-based and a Realtime Blackhole List (RBL) spam filter that it wants to use in conjunction with its Lotus Protector for Mail Encryption Server. (An RBL is a list of servers that are known to send out spam or to be open relays.)

The company is careful to locate the respective spam filters in the appropriate locations in the logical flow of data and to configure them correctly.

Lotus Protector for Mail Encryption Server internally placed

1	Example Corp. email user
2	Content-based spam filter
3	Lotus Protector for Mail Encryption Server internally placed
4	Example Corp. email server
5	RBL-based spam filter

Lotus Protector for Mail Encryption Server in gateway placement

1	Example Corp. email user
2	Example Corp. email server
3	Content-based spam filter
4	Lotus Protector for Mail Encryption Server externally placed
5	RBL-based spam filter

Notes:

The content-based spam filter sits between the internal email users and the Lotus Protector for Mail Encryption Server in the logical flow of data so that messages are decrypted before they are checked for spam. This allows even Lotus Protector for Mail Encryption Server–encrypted messages to be checked. Other SMTP filtering devices (such as a standalone antivirus gateway, for example) would be placed in the same location.

Both spam filters must be correctly configured. For example, the content-based spam filter must not treat the Lotus Protector for Mail Encryption Server as a “trusted mail relay” to avoid creating an open relay; this might require disabling the spam filter's reverse MX lookups feature.

For the gateway placement scenario, the content-based spam filter must be configured on the Lotus Protector for Mail Encryption Server as a mail server. This is done on the inbound or Unified SMTP proxy.

With an internal placement, the content-based spam filter is not filtering SMTP, only POP/IMAP, so no special configuration on the Lotus Protector for Mail Encryption Server is required.

Alternatively, put both spam filters between the Lotus Protector for Mail Encryption Server and the firewall in the logical flow of data. This configuration assumes Lotus Protector for Mail Encryption Server–encrypted messages do not contain spam because they are scanned while encrypted. However, spam in unencrypted messages is still detected.

Caution: If you begin receiving encrypted spam, relocate or add another content-based spam filter to sit between the internal email users and the Lotus Protector for Mail Encryption Server. Receiving unencrypted spam is unlikely because it is CPU-intensive and inefficient.

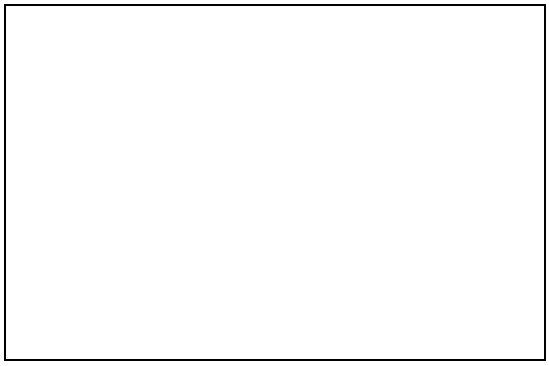
Note: You might require this alternative configuration if the content-based spam filter requires reverse MX lookups.

Lotus Domino Server with Lotus Protector for Mail Encryption Client Software

Lotus Domino Server environments, including the Lotus Notes email client, are supported in Lotus Protector for Mail Encryption Client for both internal and external Lotus Protector for Mail Encryption Server users, and in PGP Universal Satellite for Windows for external Lotus Protector for Mail Encryption Server users.

Internal Lotus Notes Configuration

For internal PGP Universal Satellite users, Lotus Notes requires a slightly different configuration because the Lotus Notes email client must connect directly to its Domino Server.



1	Lotus Protector for Mail Encryption Server
2	Example Corp. DMZ
3	Example Corp. internal network
4	Domino server
5	Internal Lotus Notes user (with PGP Universal Satellite)
6	Keys and policies

In this configuration, email goes from the internal Lotus Notes user to the Domino Server, then on to its destination. PGP Universal Satellite gets its keys and policies from a Lotus Protector for Mail Encryption Server to which it is “bound." For more information, see "Binding" in the *Lotus Protector for Mail Encryption Server Administrator's Guide*.

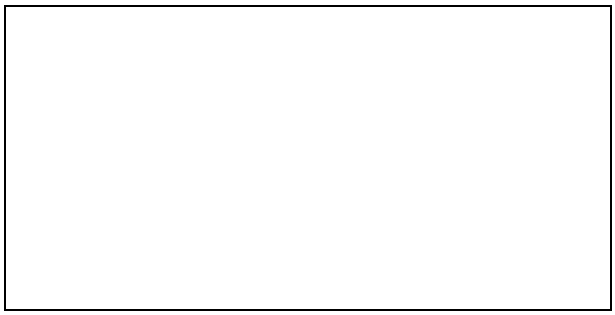
The advantages to this configuration include full support for Lotus Notes features and full security for email messages, as messages are stored encrypted on the Domino Server and stay encrypted all the way to the computer of the Lotus Notes email user.

In some cases with internal Server Key Mode (SKM) users connecting to a Lotus Protector for Mail Encryption Server in External Mode, messages are decrypted by the Lotus Protector for Mail Encryption Server before arriving at the client; use Client Key Mode (CKM) keys to ensure end-to-end security. For more information, see "Key Modes" in the *Lotus Protector for Mail Encryption Server Administrator's Guide*.

External Lotus Notes Configuration

For external email users, using a Lotus Notes email client is no different than using a POP or IMAP email client.

The external PGP Universal Satellite gets its policies from a Lotus Protector for Mail Encryption Server in the managed domain. This is the same Lotus Protector for Mail Encryption Server that sent the Mail Encryption Smart Trailer or Protector for Mail Encryption Web Messenger message.



1	Lotus Protector for Mail Encryption Server
2	Domino server
3	External Lotus Notes user (with PGP Universal Satellite)
4	Example Corp. internal network
5	Example Corp. email user
6	Example Corp. DMZ

It does not matter if the Lotus Protector for Mail Encryption Server in the managed domain is in Internal or External Mode, as long as it is accessible to the external PGP Universal Satellite via HTTPS on the well-known port 443.

Microsoft Exchange Server with Lotus Protector for Mail Encryption Client Software

Microsoft Exchange Server environments (MAPI) are supported by the clients for internal and external Lotus Protector for Mail Encryption Server users and in PGP Universal Satellite for Windows for external users.

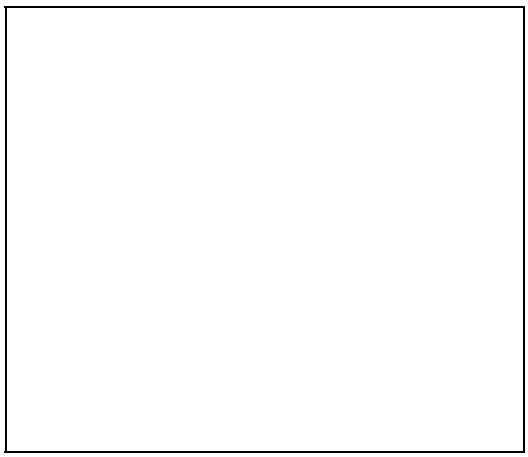
For more information about Microsoft Exchange Server environments and MAPI support, see "MAPI Support" in the *Lotus Protector for Mail Encryption Server Administrator's Guide*.

Unsupported Configurations

The following Lotus Protector for Mail Encryption Server deployment scenario is an unsupported configuration.

Multiple Gateway–Placed Servers

You cannot have multiple Lotus Protector for Mail Encryption Servers operating in gateway placements in one DMZ.



1	Lotus Protector for Mail Encryption Server 1
2	Lotus Protector for Mail Encryption Server 2
3	Lotus Protector for Mail Encryption Server 3
4	Lotus Protector for Mail Encryption Server 4
5	Acmecorp email server
6	Example Corp. DMZ
7	Logical flow of data
8	Example Corp. email user
9	Example Corp. internal network

Notes:

This configuration will not work as expected because the mail server will only route outbound email through one of the Lotus Protector for Mail Encryption Servers.

You can use load balancing to achieve a similar result. For more information, see *Gateway Cluster with Load Balancer* (on page 42).