IBM(R) Lotus Protector for Mail Encryption Version 2.1.0.1 Release Notes

Thank you for using this IBM(R) Corporation product. These Release Notes contain important information regarding this release of Lotus Protector for Mail Encryption. IBM Corporation strongly recommends you read this entire document.

IBM Corporation welcomes your comments and suggestions. Please use the information provided in Getting Assistance to contact us.

Product: Lotus Protector for Mail Encryption

Version: 2.1.0.1

About Lotus Protector for Mail Encryption

Lotus Protector for Mail Encryption provides your enterprise with secure messaging: it transparently protects your messages without user interaction. It 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, providing strong security through policies you control. PGP Universal Satellite provides security for email messages all the way to the computer of the email user, it allows external users to become part of the SMSA, and it gives end users the option to create and manage their keys on their own computer.

Lotus Protector for Mail Encryption Client provides IBM Lotus(R) enterprise customers with an automatic, transparent encryption solution for securing internal and external confidential email communications. Lotus Notes(R) 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.

What's Included in This File

System Requirements

Lotus Protector for Mail Encryption Server Requirements

Lotus Protector for Mail Encryption Server is a customized Linux(R) OS installation; it cannot be installed on a Windows(R) server. Every Lotus Protector for Mail Encryption Server requires a dedicated system that meets the system requirements listed in the Server Certified Hardware list that follows. The installation process deletes all data on the system and reconfigures it as a Lotus Protector for Mail Encryption Server.

Lotus Protector for Mail Encryption Client Requirements

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

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

Lotus Protector for Mail Encryption Server Certified Hardware List

Please obtain the latest copy of this list for hardware purchasing decisions after 04/07/10.

The following systems are certified for use as the hardware for Lotus Protector for Mail Encryption Server:

1. **Dell PowerEdge R610** - Two Quad-Core Intel(R) Xeon(R) E5504 @ 2GHz - 4 GB RAM
   Two 146 GB 10K 2.5" SAS HD - SAS 6/iR RAID
   Broadcom BCM5709 network controller
   Small/medium environment production unit
2. **Dell PowerEdge R710** - Two Quad Core Intel Xeon E5530 @ 2.4GHz - 8 GB RAM
   Two 146 GB 15K SAS HD - SAS 6/iR RAID
   Broadcom BCM5709 network controller
   Medium/large environment production unit, cluster member
3. **IBM System x(R)3650 M3** - Two Quad Core Intel Xeon E5630 @ 2.53 GHz - 16 GB RAM
   Two x 300 GB SAS 10K RPM - IBM ServeRAID-MR 10i disk controller
   Broadcom BCM5709 network controller
   Medium/large environment production unit, cluster member
4. **IBM BladeCenter(R) HS22** - Two Intel Xeon E5530 @ 2.4 GHz - 8 GB RAM
   Two 146 GB SAS 10K RPM - LSI Logic 1068E iR RAID
   Broadcom BCM5709S network controller
   Small/medium environment production unit
5. **HP Proliant DL120 G5** - Intel Xeon X3330 2.66 GHz - 2 GB RAM
   Two 250 GB SATA
   Broadcom BCM5722 network controller
   Small/medium environment production unit
6. **HP ProLiant DL380 G6**- Intel Xeon E5530 @ 2.4 GHz - 6 GB RAM

Two 146 GB SAS 10K RPM - Smart Array P410i RAID
Broadcom BCM5709 network controller
Medium/large environment production unit, cluster member

7. **VMWare ESX 3.5.0, 4.0, ESXi 3.5.0** - Supported platform, non-hardware.
   Sufficient processing power equivalent to a 3 GHz Intel Xeon must be dedicated to the Lotus Protector for Mail EncryptionServer VM.
   VMWare tools must be installed and configured inside the Lotus Protector for Mail Encryption Server operating system.
   VMWare ESX 4.0 is certified without VMotion.
   Disk space requirements:
   - Small/medium environment - 50 GB minimum allocated to the VMWare instance; 4 GB RAM dedicated to the VMWare instance.
   - Medium/large environment - 100 GB minimum allocated to the VMWare instance; 8 GB RAM dedicated to the VMWare instance.

While a broad array of other hardware may work well with Lotus Protector for Mail Encryption Server, **incompatibilities related to hardware that is not one of the above systems will not be supported.**

To qualify as Lotus Protector for Mail Encryption Server Certified Hardware, the server must be one of the models listed and all components must be configured as specified.

Changing the sizes of hard disks within the same type of drive (for example, 36 GB SCSI to 73 GB SCSI), increasing memory configurations, and increasing processor speeds within the same type and family qualifies as the same system for Support purposes.

Email Client and Server Requirements

Lotus Protector for Mail Encryption Server and Protector for Mail Encryption Client are compatible with the following mailservers:

- Lotus Domino(R) Server 8.5
- Lotus Domino Server 8.0.2
- Lotus Domino Server 7.0.3
- Microsoft Exchange Server 2007 SP1
- Microsoft Exchange Server 2003 SP3
- Microsoft Exchange Server

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

- Lotus Notes 7.0.3 (7.0.4)
- Lotus Notes 8.0.2 (Basic and Standard)
- Lotus Notes 8.5 (8.5.1) (Basic and Standard)
- Microsoft Outlook 2007 SP1
- Microsoft Outlook 2003 SP3
- Microsoft Outlook XP SP3

Note: Support for Outlook is only with Exchange.

Protector for Mail Encryption Client supports the following messaging protocols:

- Notes RPC for Lotus Notes
- MAPI for Outlook

Protector for Mail Encryption Client does not support IMAP/SMTP/POP.

Lotus Protector for Mail Encryption Server supports the following messaging protocols:

- POP/POPS
- IMAP/IMAPS
- SMTP/SMTPS
- STARTTLS for POP/IMAP/SMTP

Lotus Protector for Mail Encryption Server Administrative Interface Web Browser Requirements

Windows	Internet Explorer 6 and greater Firefox 1.0 and greater
Mac OS X	Safari 1.0 and greater Firefox 1.0 and greater

Protector for Mail Encryption Web Messenger Web Browser Requirements

Windows	Internet Explorer 6 and greater Firefox 1.0 and greater
Mac OS X	Safari 1.0 and greater Firefox 1.0 and greater

PGP Universal Satellite for Windows Requirements

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

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

- 512 MB of RAM
- 64 MB hard disk space

PGP Universal Satellite for Mac OS X Requirements

- Mac OS X 10.5.x or 10.6.x (Intel or PowerPC)

- 512 MB of RAM
- 64 MB hard disk space
- 10.4.x removed, 10.6.x added. Nov. 2, 2009

Supported External Authentication Products

Lotus Protector for Mail Encryption Server is compatible with the following LDAP directory products:

- Lotus Notes/Domino Directory 8.5
- Lotus Notes/Domino Directory 8.0.2
- Lotus Notes/Domino Directory 7.0.3
- Microsoft Active Directory 2003
- Microsoft Active Directory 2000
- OpenLDAP 2.3.x
- PGP Global Directory

For directory synchronization, Lotus Protector for Mail Encryption supports:

- LDAPv2
- LDAPv3
- LDAPS

For Protector for Mail Encryption Web Messenger external authentication, Lotus Protector for Mail Encryption supports:

- LDAPv2
- LDAPv3
- RSA Radius Server with RSA Authentication Manager 7.1

Additional Information

The following sections provide information related to specific features of Lotus Protector for Mail Encryption.

Please see the *PGP Universal Satellite Release Notes* installed with PGP Universal Satellite for additional information about that product.

Installation

- When you back up data on one Lotus Protector for Mail Encryption Server and then restore the data onto a different Lotus Protector for Mail Encryption Server, MAC address information is incorrect. The MAC address on the restored Lotus Protector for Mail Encryption Server is set to the MAC address of the backed-up Lotus Protector for Mail Encryption Server. This cannot be fixed through the user interface. Contact IBM Support to correct the MAC address. [19895]
- Installing Lotus Protector for Mail Encryption Server will reformat your hard disk, removing any existing operating system. Please do NOT insert the Lotus Protector for Mail Encryption installation disk into any machine you do not intend on formatting for Lotus Protector for Mail Encryption Server alone. [18616]

- Do not use international characters when specifying file names for backup files. [10834]
- When the Lotus Protector for Mail Encryption Client is uninstalled, the PME Client registry information under HKEY_CURRENT_USER is not removed. [NBN]

Deployment

- When a NIC is set to a custom link mode, rather than auto-negotiate, the network driver no longer advertises other link speeds. Lotus Protector for Mail Encryption Server requires access to the list of possible link speeds to populate the Network Settings Link Speed menu. If you want to change the Link Speed from a custom setting, and no other custom settings appear, select Auto from the menu. Restart Lotus Protector for Mail Encryption Server. After restart, the Link Speed menu is populated with all available options for the NIC. [19287]
- MAC ID, MTU, and Link Speed are not applicable to Lotus Protector for Mail Encryption Server hosted on VMWare because the ESX server controls the network settings. However, when you create a new virtual interface, those settings are automatically populated. If your Lotus Protector for Mail Encryption Server runs on VMWare and you want to create a new interface or edit an existing interface, you cannot save your changes until you clear the auto-populated MTU, MAC ID, and Link Speed settings. [19810]
- Organization Keys with Japanese passphrases cannot be imported. [18620]
- You cannot use spaces in the name of the backup FTP server. [15491]
- HTTP-based services do not support port numbers higher than 32767. [25784]
- If you configure multiple LDAP servers, and the first is unavailable, Lotus Protector for Mail Encryption does not continue to search for users in the other listed servers. [25587]
- Lotus Protector for Mail Encryption does not provide out-of-the-box support for LDAP synchronization in environments where multiple LDAP servers contain identical samAccountName values for different users. If your environment contains multiple LDAP domains with some users having identical samAccountName values, please contact PGP Support for guidance on how to deploy Lotus Protector for Mail Encryption into your environment. [25299]
- If you add Lotus Protector for Mail Encryption to its own keyserver list at **Keys > Keyservers**, you must add it using the IP address. If you add it using the Lotus Protector for Mail Encryption hostname, key lookups on that keyserver fail. [24698]
- If communication between Lotus Protector for Mail Encryption and your HSM is interrupted, you must re-start Lotus Protector for Mail Encryption once communication has been re-established. [23739]
- To create a mail policy rule for expanding the To list for messages to mailing lists, make sure the conditions are in the correct order, or the rule is not applied. The correct order for the conditions must be:
    1. Recipient domain <is/contains/matches>.
    2. 'Recipient address is mailing list'
    3. 'Mailing list user count is' <greater than/fewer than>

  [23723]

- Sometimes, after you request the deletion of a cluster member, the deletion may not propagate fully around the cluster. In this case, it is safe to repeat the deletion action as necessary. [23694]

- Lotus Protector for Mail Encryption Server 2.1 does not support SSL v1.0 certificates. [25378]
- With Microsoft Internet Explorer 8, security can be set to a HIGH state, which disables Javascript on most web pages. With Javascript disabled, Lotus Protector for Mail Encryption Server's management console (administrative interface) and Protector for Mail Encryption Web Messenger login will not function. Make security exceptions for Lotus Protector for Mail Encryption Server in IE 8's security settings, or use a different browser to access the administrative interface. [23688]

PGP Keys

- Exporting or deleting tens of thousands of user keys at a time can take hours, or can fail. Export fewer keys at a time, or contact IBM Support for help. [15998]
- When making any changes that affect which TLS client certificates are permitted to access the keyserver service, you must disable, and re-enable the keyserver service for these changes to take effect. [6533]

Messaging

- Messages encrypted by Lotus Protector for Mail Encryption in this release are intended to maintain secure data privacy until the email is opened with decryption by the recipient. For this reason please note: An **unopened** encrypted message **is not** decrypted when dragged and dropped into Quickr and Connections. [NBN]
- In Lotus Protector for Mail Encryption Server 2.1.0.1, the server no longer returns an unverified key for encryption purposes when the key lookup request by clients is for a verified key. Administrators must select the unverified keys for their users, especially for external users using PGP Universal Satellite, and must manually trust these unverified keys by signing them with a key that the server trusts. [25836]
- Microsoft Outlook 2007 uses extensive processing time to handle extremely large HTML attachments. The connection with the Lotus Protector for Mail Encryption Server may time out before the message can be sent. [12545]
- Characters added in versions of Unicode after 3.0 are not supported in Lotus Protector for Mail Encryption Server Dictionaries. [10367]
- Some of the more obscure authentication methods for POP/IMAP/SMTP may not work through Lotus Protector for Mail Encryption Server. We recommend always activating SSL/TLS between your client machines and Lotus Protector for Mail Encryption Server. If you are also deploying PGP Universal Satellite internally, it will automatically probe for SSL/TLS on the server and upgrade mail connections to use it whenever possible. Plain, Login, MSN, NTLM, and CRAM- MD5 authentication are officially supported in this release. [NBN]
- Microsoft Outlook:
    - Microsoft Outlook: Messages that have been processed by PGP Desktop cannot be modified from the Microsoft Outlook Outbox. [20269]
    - MAPI/Exchange users and inline objects:

      If you are a MAPI/Exchange user, and you are sending messages containing embedded content in a proprietary format (inline objects), PGP Desktop will secure the complete message. This will cause inline objects to be readable/viewable only by recipients in a MAPI/Exchange environment. [5530]
- Lotus Notes:

- Lotus Notes and disabled users: When a user has been disabled, email sent by the user is initially blocked. To work around this issue, send the email again and email is sent in the clear, as expected. [12234]
- Lotus Notes and disabled users: When a user has been disabled, and then re-enabled, the user must restart Lotus Notes to send encrypted email. [12236]
- Starting with Lotus Notes 8.5.2, Lotus Protector for Mail Encryption Client will be integrated into Lotus Notes and will not be available as a separate installer package. [NBN]
- When sending PGP encrypted email, there is a minor inconsistency in Russian text font conversions. [26719]

Protector for Mail Encryption Web Messenger

- Depending on your Microsoft Windows version, opening files with non-Latin filenames directly from Protector for Mail Encryption Web Messenger may result in garbled filenames. To avoid this problem, save attachments to your desktop before opening them. [12011]
- Replies to Protector for Mail Encryption Web Messenger email messages may not work if a load balancer is directing traffic for the untrusted interfaces of a cluster of Lotus Protector for Mail Encryption Servers in gateway placement. A workaround is to disable any rules your hardware may enforce that prohibit traffic to a virtual server from a member of the load balancing pool. Check with your hardware vendor to determine if this is possible. [NBN]
- Protector for Mail Encryption Web Messenger mailbox quotas of up to 2 GB are supported for this release. [7986]
- Sending concurrent Mail Encryption PDF Messenger messages to large numbers of recipients is not recommended. Limit the number of concurrent recipients to 200 at a time. [17751]
- When a Mail Encryption PDF Messenger message with a large attachment is sent out of the mail stream, the connection to the Lotus Protector for Mail Encryption Server times out before the mail is sent. [15916]

Getting Assistance

For additional information about Lotus Protector for Mail Encryption and how to obtain support, see Lotus Protector for Mail Encryption.

Copyright

worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at "Copyright and trademark information" at http://www.ibm.com/legal/copytrade.shtml .

Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.

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

Intel, Intel logo, Intel Inside, Intel Inside logo, Intel Centrino, Intel Centrino logo, Celeron, Intel Xeon, Intel SpeedStep, Itanium, and Pentium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.