POLICY MANAGEMENT AGENT FOR SMTP1.0

Flexible Security Policy Enforcement for Email

PGP[®] Policy Management Agent for SMTP helps to protect an organization's vital information by enforcing corporate security policies for email communications across internal and external networks. This important component of the PGP Business Security Suite transparently integrates with the desktop to ensure that incoming and outgoing email messages adhere to the policies established for a given corporate site.

Reliable prevention of policy violations

PGP Policy Management Agent works with standard SMTP mail servers, intercepting and checking email to ensure that it conforms with desired security policies. A typical policy established for encryption software, for example, is that encrypted email must also be encrypted to a corporate message recovery key to enable data recovery. Email that adheres to the policy is automatically routed to the intended recipient. Email that fails to adhere to any of the established policies is rejected by the server and sent back to the client with a configurable SMTP error message, depending upon the policy failure.

Built-in reporting capabilities

PGP Policy Management Agent for SMTP provides automatic logging for each request that is processed. IS managers can choose among multiple levels of information, as well as the destination of the output.

Transparent client interaction

Once installed, PGP Policy Management Agent for SMTP performs its functions without any change of client software. All operations are transparent to the client, unless policy is failed. Rejection messages are configurable for each installation and policy violation.

- Policy enforcement for email within intranets and over the Internet
- Automatic enforcement of encryption and corporate message recovery policy
- Support for standard SMTP servers
- Transparent integration with all PGP clients
- Easy installation and operation
- Multiple logging levels
- Configurable error messages for non-conformance to policy



PRETTY GOOD PRIVACY

POLICY MANAGEMENT AGENT FOR SMTP 1.0

AVAILABLE POLICIES

- Corporate message recovery: Rejects all encrypted messages which have not also been encrypted to one or more corporate message recovery keys.
- Digital signatures: Allows, Disallows, or Requires the use of digital signatures on messages.
- Encryption: Determines whether all email and attachments must be encrypted before passing policy requirements.
- Conventional encryption: Allows the rejection of all messages that have been encrypted with only conventional encryption. Conventional (also known as symmetric) encryption requires the recipient to have the same passphrase as the sender.
- Forbidden keys: Disallows the use of encryption to specific keys.
- Specified address: Limits the checking of policies to be enforced for a specified IP address or domain. Through a simple configuration value, which includes wildcard support, policies can be designated for an entire domain, network, subnet, or IP address.



SYSTEM REQUIREMENTS

SMTP SERVER CAN BE RUN IN EITHER OF **TWO CONFIGURATIONS:**

SMTP server that can listen on a port other than 25 (the standard SMTP port) and will only allow connections from its own machine.

SMTP server configured to allow connections only from the server running the Policy Management Agent for SMTP.

An error occurred sending mail. The mail server responded: You have voltated corporate policy with this messay You must also encrypt this message to the corporate The message has been RFL/ECTED. Please check the message and try again.

OPERATING SYSTEMS SUPPORTED

- 🗆 ×

× *

602.944.0773

888.747.3011

www.pqp.com

telephone:

toll free:

internet:

N

Sun Solaris (SPARC) 2.5.1 or later, or Microsoft Windows NT (Intel) 4.0

Insert Format Tools Communicator Help

Second Street

Edit

6 3

View

To: 🍋 maryt@pgp.com

Subject: company confidential information Variable W Netscape

file://C:\public\pgppma.txt - Microsoft Internet Explorer	An error occurred sending mail. The mail server responded: You have violated corporate policy with this message You must also encrypt this message to the corporate key The message has been REJECTED.	<u>^</u>
Eile Edit View Go Favorites Help	DBw04DA Please check the message and try again.	uhO
Links @Best of the Web @Microsoft @Product News @Today's Links @Web Gallery	D8Eg42sJfq frPU SHUCeRby ОК Хко	
← · → · ② ③ ▲ ② ▲ ④ ▲ Ø ▲ ▲ Address ■ pgppma.txt	FhR7Svf2Dtcp+1169r1vgjvssse+1wpDtc1z6zi4DHnu5Dj2F6H0wazV+v	rwK
<pre>Sep 4 13:28:37 : Currentconnections: 0 Sep 4 13:28:37 : [205.180.136.125] EHLO client1 Sep 4 13:28:37 : [205.180.136.32] 250 keydev.pgp.com Hello keydev.pgp.com [205.180.136. Sep 4 13:28:37 : [205.180.136.125] MAIL FROM:<luke@ultradev.pgp.com> Sep 4 13:28:38 : [205.180.136.32] 250 <luke@ultradev.pgp.com> Sender ok</luke@ultradev.pgp.com></luke@ultradev.pgp.com></pre>	S9BzvjYXgw5rviYwad/ChSEjDdtJOCArEtwDZFJzV4u0Rm1IIYN1z1 mmuVwDxKsxf0QBsaVBsCDNGg9LhgEcOeYpDTSSFYNPTfWToX VGvBBI/kidY0/zpyu82V1wMZeqn9SEatpVN7Jv7kfc79OPrHLjRAYx	CAC c6lu 🚽
<pre>Sep 4 13:28:38 : [205.180.136.125] RCPT TO: <ben@keydev.pgp.com> Sep 4 13:28:38 : [205.180.136.32] 250 <ben@keydev.pgp.com> Recipient ok Sep 4 13:28:38 : [205.180.136.125] DATA Sep 4 13:28:38 : [205.180.136.125] Found recovery key <0xD870BED04A7C4C15> Sep 4 13:28:38 : [205.180.136.125] Cleartext message not permitted Sep 4 13:28:38 : [205.180.136.125] message REJECTED</ben@keydev.pgp.com></ben@keydev.pgp.com></pre>	Email that doesn't adhere to policy is automatically re and returned to the sender.	ejecte
<pre>Sep 4 13:28:48 : [205.180.136.125] EHLO client1 Sep 4 13:28:48 : [205.180.136.32] 250 keydev.pgp.com Hello keydev.pgp.com [205.180.136. Sep 4 13:28:48 : [205.180.136.125] MALL FROM:<luke@ultradev.pgp.com> Sep 4 13:28:48 : [205.180.136.32] 250 <luke@ultradev.pgp.com> Sep 4 13:28:48 : [205.180.136.125] RCFT T0: them@keydev.pgp.com></luke@ultradev.pgp.com></luke@ultradev.pgp.com></pre> Sep 4 13:28:48 : [205.180.136.125] CFT T0: them@keydev.pgp.com> Sep 4 13:28:48 : [205.180.136.125] DATA Sep 4 13:28:49 : [205.180.136.125] MALA Sep 4 13:28:49 : [205.180.136.125] DATA Sep 4 13:28:49 : [205.180.136.125] MALA Sep 4 13:28:49 : [205.180.136.126] MALA Sep 4 13:28:40 : [205.180.136.126] MALA Sep 4 13:28:40 : [205.180.136.126] MALA<	FOR MORE INFORMATIO address: Pretty Good Privacy 2121 S. El Camino Rec	al
	San Mateo, CA, 94403	3

PGP Policy Management Agent for SMTP maintains a log file of all activities at the server.

© 1997 Pretty Good Privacy, Inc. All rights reserved. PGP and Pretty Good Privacy are registered trademarks of Pretty Good Privacy, Inc. This software uses public key algorithms described in U.S. patent numbers 4,200,770, 4,218,582, 4,405,829, and 4,424,414, licensed exclusively by Public Key Partners; the IDEA cryptographic cipher described in U.S. patent number 5,214,703, licensed from Ascom Tech AG; and the Northern Telecom Ltd. CAST Encryption Algorithm, licensed from Northern Telecom, Ltd. IDEA is a trademark of Ascom Tech AG. Other product names are trademarks of their respective owners.

301-600-000003

PRETTY GOOD PRIVACY