Policy Management Agent for SMTP
Version 1.0

For
UNIX

Administrator's Guide

Network Associates, Inc.

Copyright © 1990-1998 Network Associates, Inc. and its Affiliated Companies. All Rights Reserved.

PGP* Policy Management Agent for SMTP, Version 1.0.2
2-98. Printed in the United States of America.

PGP, Pretty Good, and Pretty Good Privacy are registered trademarks of Network Associates, Inc. and/or its Affiliated Companies in the US and other countires. All other registered and unregistered trademarks in this document are the sole property of their respective owners.

Portions of this software may use 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(tm) 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. Network Associates Inc. may have patents and/or pending patent applications covering subject matter in this software or its documentation; the furnishing of this software or documentation does not give you any license to these patents. The compression code in PGP is by Mark Adler and Jean-Loup Gailly, used with permission from the free Info-ZIP implementation. LDAP software provided courtesy University of Michigan at Ann Arbor, Copyright © 1992-1996 Regents of the University of Michigan. All rights reserved. This product includes software developed by the Apache Group for use in the Apache HTTP server project (http://www.apache.org/). Copyright © 1995-1997 The Apache Group. All rights reserved. See text files included with the software or the PGP web site for further information.

The software provided with this documentation is licensed to you for your individual use under the terms of the End User License Agreement and Limited Warranty provided with the software. The information in this document is subject to change without notice. Network Associates Inc. does not warrant that the information meets you requirements or that the information is free of errors. The information may include technical inaccuracies or typographical errors. Changes may be made to the information and incorporated in new editions of this document, if and when made available by Network Associates Inc.

Export of this software and documentation may be subject to compliance with the rules and regulations promulgated from time to time by the Bureau of Export Administration, United States Department of Commerce, which restrict the export and re-export of certain products and technical data.

Network Associates, Inc.
2805 Bowers Ave.
Santa Clara, CA 95051

(408) 988-3832 main
(408) 970-9727 fax
http://www.nai.com
info@nai.com

***** is sometimes used instead of the ® for registered trademarks to protect marks registered outside of the U.S.

LIMITED WARRANTY

Limited Warranty. Network Associates Inc. warrants that the Software Product will perform substantially in accordance with the accompanying written materials for a period of sixty (60) days from the date of original purchase. To the extent allowed by applicable law, implied warranties on the Software Product, if any, are limited to such sixty (60) day period. Some jurisdictions do not allow limitations on duration of an implied warranty, so the above limitation may not apply to you.

Customer Remedies. Network Associates Inc's and its suppliers' entire liability and your exclusive remedy shall be, at Network Associates Inc's option, either (a) return of the purchase price paid for the license, if any or (b) repair or replacement of the Software Product that does not meet Network Associates Inc's limited warranty and which is returned at your expense to Network Associates Inc. with a copy of your receipt. This limited warranty is void if failure of the Software Product has resulted from accident, abuse, or misapplication. Any repaired or replacement Software Product will be warranted for the remainder of the original warranty period or thirty (30) days, whichever is longer. Outside the United States, neither these remedies nor any product support services offered by Network Associates Inc. are available without proof of purchase from an authorized international source and may not be available from Network Associates Inc. to the extent they subject to restrictions under U.S. export control laws and regulations.

NO OTHER WARRANTIES. TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, AND EXCEPT FOR THE LIMITED WARRANTIES SET FORTH HEREIN, THE SOFTWARE AND DOCUMENTATION ARE PROVIDED "AS IS" AND NETWORK ASSOCIATES, INC. AND ITS SUPPLIERS DISCLAIM ALL OTHER WARRANTIES AND CONDITIONS, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, CONFORMANCE WITH DESCRIPTION, TITLE AND NON-INFRINGEMENT OF THIRD PARTY RIGHTS, AND THE PROVISION OF OR FAILURE TO PROVIDE SUPPORT SERVICES. THIS LIMITED WARRANTY GIVES YOU SPECIFIC LEGAL RIGHTS. YOU MAY HAVE OTHERS, WHICH VARY FROM JURISDICTION TO JURISDICTION.

LIMITATION OF LIABILITY. TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, IN NO EVENT SHALL NETWORK ASSOCIATES, INC. OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, INCIDENTAL, CONSEQUENTIAL, SPECIAL OR EXEMPLARY DAMAGES OR LOST PROFITS WHATSOEVER (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF BUSINESS PROFITS, BUSINESS INTERRUPTION, LOSS OF BUSINESS INFORMATION, OR ANY OTHER PECUNIARY LOSS) ARISING OUT OF THE USE OR INABILITY TO USE THE SOFTWARE PRODUCT OR THE FAILURE TO PROVIDE SUPPORT SERVICES, EVEN IF NETWORK ASSOCIATES, INC. HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. IN ANY CASE, NETWORK ASSOCIATES, INC'S CUMULATIVE AND ENTIRE LIABILITY TO YOU OR ANY OTHER PARTY FOR ANY LOSS OR DAMAGES RESULTING FROM ANY CLAIMS, DEMANDS OR ACTIONS ARISING OUT OF OR RELATING TO THIS AGREEMENT SHALL NOT EXCEED THE PURCHASE PRICE PAID FOR THIS LICENSE. BECAUSE SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OR LIMITATION OF LIABILITY, THE ABOVE LIMITATIONS MAY NOT APPLY TO YOU.

Preface

This book describes how to install and configure the Policy Management Agent for SMTP and is for System Administrators or others who are responsible for setting up and running the server that filters email to ensure that it complies with the policies that have been specified for a particular site.

See “What’s in this book” for more information about each chapter.

Conventions used in this book

The following section explains the conventions used in this manual to delineate and emphasize important terms, concepts and instructions.

Typographical conventions

Certain words or phrases are shown in a different style or font to help distinguish them from the surrounding text. New terms are shown in *italics* and are generally defined in context or, if necessary, are elaborated on in greater detail in the Glossary. Commands are shown in **bold** while information which appears on the screen and code samples are shown in `Courier font (this is an example of Courier).`

Special advisements

The following special advisements are used to call attention to a particular situation that requires your consideration.

NOTE:	Notes provide supplemental information which emphasizes a particular concept or explains a caveat with regard to the current topic of discussion.
TIP:	Tips provide specific guidelines you should follow or precautions you should take when carrying out a particular task.
ALERT:	Alerts provide warnings about conditions or procedures that could result in unwanted consequences unless specific measures are observed.

Registration information

Users are asked to register on-line. This information is for our internal use only and will enable us to serve you better in the future. This data will remain confidential—we respect your privacy (that's why we do what we do). Look for the “Register On-line” option in your PGP product’s Help menu.

For more information

There are several ways to find out more about Network Associates and its products.

From the Web

The Network Associates, Inc. web site provides information about our organization, our products, product updates, and related topics such as Privacy Matters. Please visit us at:

http://www.nai.com

You can also reach us from both AOL and Compuserve as:

Go NAI

Support

Technical Support for your PGP product is available through an number of channels. You can:

- visit us on the web at: http://www.pgp.com/service
- email us at: PGPSupport@pgp.com.
- phone us at: (408) 988-3832
- fax us at: (408) 970-9727

To ensure quick resolution, please have the following information ready before contacting Technical Support:

- PGP product name
- PGP product version
- Computer platform and CPU type
- Amount of available memory (RAM)
- Network operating system and version
- Content of any status or error message displayed on screen, or appearing in a log file (not all products produce log files)
- Email application and version (if the problem involves using PGP with an email product, for example, the Eudora plug-in)
- Your PGP registration number

Your feedback is welcome

We continually enhance PGP and welcome customer feedback as we design new versions. We appreciate your interest in PGP and your thoughts on product content and functionality, especially as we plan features to enhance the products for corporate settings. Feedback like yours helps us to develop richer and easier-to-use software and services. We cannot incorporate all suggestions, but we will give your input serious consideration as we develop future products.

Please send your comments to:

pma-doc@pgp.com

Recommended introductory readings

Bacard Andre, “Computer Privacy Handbook,” Peachpit Press, 1995.

Garfinkel Simson, “Pretty Good Privacy,” O’Reilly & Associates, 1995.

Schneier Bruce, “Applied Cryptography: Protocols, Algorithms, and Source Code in C, Second Edition,” John Wiley & Sons, 1996

Schneier Bruce, “Email Security,” John Wiley & Sons, 1995.

Stallings William, “Protect Your Privacy,” Prentice Hall, 1994.

Other readings:

Lai Xuejia, “On the Design and Security of Block Ciphers,” Institute for Signal and Information Processing, ETH-Zentrum, Zurich, Switzerland, 1992

Lai Xuejia, Massey James L., Murphy Sean” Markov Ciphers and Differential Cryptanalysis,” Advances in Cryptology—EUROCRYPT’91

Rivest Ronald, “The MD5 Message Digest Algorithm,” MIT Laboratory for Computer Science, 1991

Wallich Paul, “Electronic Envelopes,” Scientific American, Feb. 1993, page 30.

Zimmermann Philip, “A Proposed Standard Format for RSA Cryptosystems,” Advances in Computer Security, Vol. III, edited by Rein Turn, Artech House, 1988.

What’s in this book

Chapter 1 *The Policy Management Agent for SMTP*

This chapter provides an overview describing the Policy Management Agent and how it functions.

Chapter 2 *Installation and Configuration*

This chapter describes how to install and configure the policy management agent.

Chapter 3 *Operation and Maintenance*

This chapter describes how to operate and maintain the policy management agent.

Contents

Chapter 1

The Policy Management Agent for SMTP

This chapter describes the features offered by the Policy Management Agent for SMTP and how it works.

General features

The Policy Agent works in conjunction with a standard SMTP mail server to ensure that incoming and outgoing email adheres to the policies that are specified for a given site. It intercepts email normally bound for the SMTP server and checks to make sure that it conforms with policies configured for your site. If the email adheres to the policies for your site, it is forwarded to the SMTP server where it is routed to the intended recipient. If the email does not adhere to the policies specified for your site, a message of your choosing is sent to the client indicating that the email was rejected. The Policy Management Agent for SMTP provides the following features:

- Makes sure that email has been encrypted using certain designated recovery keys. Only those messages which have been encrypted to the required keys are allowed to pass through the gateway.
- Ensures that all email messages are encrypted before allowing them to be delivered. You can also specify that email should not be encrypted from certain sites.
- Specifies whether email must be signed or not before it is allowed to pass the policy requirement. The agent can also reject email that has been encrypted using certain keys which are designated as forbidden.

- Specifies whether conventional encryption is allowed.
- Maintains a log file listing all of the attempts to route email along with a description of the outcome.

Overview

The Policy Management Agent for SMTP serves as a proxy mail server that monitors the port normally assigned to the SMTP mail server. When a mail client generates a User Agent (UA) request, the policy agent creates a new socket and connects to the SMTP server. It then allows the transaction to proceed until it encounters an SMTP “DATA” command indicating that the client is about to send the data portion of the email message. The policy agent evaluates this information to determine if it contains encrypted data then, based on the policy established in the configuration file, decides whether to send the mail onto the SMTP server or to reject it and close the connection. When email is rejected for a policy violation, a message (specified in the configuration file) is output to the client.

NOTE: The current version of the SMTP Policy Agent only supports SMTP servers, but future releases will support other types.

Chapter 2

Installation and Configuration

This chapter describes how to install and configure the Policy Management Agent for SMTP software.

System requirements

In order to install the Policy Management Agent for SMTP, the system you plan to use as your server must meet the following criteria:

- A Sun SparcStation running Solaris 2.5 or later.
- An SMTP server (such as sendmail).

> **NOTE:** If you are running the PGP Policy Management Agent for SMTP on the same machine as the SMTP server, then you need to re-direct the server to listen on an alternative port other than port 25. If your server does not provide this option, then you should consider using another server such as Berkeley Send Mail Version 8.8 which allows you to specify an alternative port.

Installing the software

To install the Policy Management Agent for SMTP software, you will need root access. Here are the steps you should follow to install the software:

1. Go to the directory where the pgppmad.pkg file is located, and then install the package by issuing the following command:

   ```
   pkgadd -d <path> /PMA_x.x.x_Solaris
   ```

   (where x.x.x is the release number)

   The appropriate package is unpacked and all of the files are placed in their appropriate directories.

   The configuration files are stored in the following directory:

   /opt/PGPpmad/etc

   The binary executable files are stored in the following directory:

   /opt/PGPpmad/bin

2. Check that the files were extracted properly by entering the following command:

   ```
   pkginfo -l PGPpmad
   ```

   The only thing you need to check here is that the status is “Completely Installed” for the selected package, which indicates that it has been installed properly.

Configuring the policy agent

Before running the policy agent, you need to provide some information for your site and specify certain settings in the configuration file. The SMTP Policy Agent adheres to the policies specified in the pgppmad.conf configuration file, which is located in the following location:

/opt/PGPpmad/etc

You will need to have super user privileges in order to access this file, which you can edit using your favorite text editor.

Configuration Settings

In order to begin using the Policy Management Agent for SMTP, you must redirect email from the standard server and supply other details, which set up the server. Here are the setting and their values:

smtphost *<IP address> or <server name>*

Specifies the host name of the SMTP mail server currently installed at your site.

smtpport *<port number> or <server name>*

Specifies the number of the port where the SMTP mail server should listen for mail requests generated by the Policy Management Agent for SMTP. If you are running the Policy Management Agent on the same machine as the SMTP server, then you need to specify an alternate port other than port 25.

NOTE: If you are running the Policy Management Agent for SMTP on the same machine as the SMTP server, then you also need to redirect the SMTP server to the specified port by using the configuration tools supplied with your SMTP server. See “Tips for Reconfiguring your SMTP Server” on page 24 for more details.

agentport *<port number>*

Specifies the port where the Policy Management Agent will listen for User Agent (UA) mail requests. This is the port originally monitored by the SMTP server which is generally port number 25.

checkhost *<IP address> or <host name>*

Allows you to limit the policy checking to the mail traffic coming across a particular subnet by using wildcards. For example, 201.010.* or *.pgp.com would only act on the specified subnet. This setting is useful when you don’t want to monitor the whole address space. You can list multiple IP addresses on the same line, where each is separated by a space or you can enter a separate “checkhost” for each of the addresses.

syslog *true | false*

Specifies that logging information should be sent to the system log file when this setting is set to true. Otherwise, the output is sent to the standard error device (stderr) or a specified log file. The default value for this setting is false.

> **NOTE:** If you are sending logging information to the system log file, you will probably want to add the line “local4.debug /var/adm/pgppmad.log” in the /etc/syslog.conf file. You can then use the “log file” configuration option to tell the policy management agent to send its output to this file. If you do not make this change, then not only the policy management agent messages, but all messages will be sent to the default log file.

logging *none | error | warning | info | verbose*

Specifies the level of information that is recorded in the log file. You can view the contents of this file to determine what email requests have been processed by the policy management agent and how they were resolved. Here are the options for this setting:

none	No logging is performed. This is the default value.
error	Logs all error messages.
warning	Logs all errors and warning messages.
info	Logs all errors, warnings and informational messages.
verbose	Logs all messages.

logfile *<filename>*

Specifies the name and location of the log file used to record the activity processed by the policy management agent. By default, the file is stored in the following location:

/var/adm/messages

mustencrypt *true | false*

Indicates whether all email must be encrypted before being allowed to pass through the mail server. A value of true specifies that all email messages and file attachments must be encrypted whereas a value of false specifies that messages do not need to be encrypted. By default, this option is set to false. The “recoverykeys” setting, described next, lists all of the keys for which email must be encrypted.

recoverykeys *<list>*

Specifies the 64-bit key IDs for all of the entities who must be encrypted to in order for email to be considered deliverable. Placing all of the key IDs (separated by a blank space) on a single line indicates that the email must be encrypted to all those keys. If you want to specify that all email must be encrypted by at least one or another key, then you should list each key ID on a separate line.

forbidkeys *<list>*

Specifies the key IDs for those keys that are not allowed to be used for encryption purposes.

signatures *allow | disallow | require*

Specifies whether email should be signed or not. The default value for this setting is “allow”.

NOTE: See “Extracting Key IDs for Configuration Purposes” on page 23 for information on how to extract key IDs.

conventionalencrypt *allow | disallow*

Specifies whether email that uses “conventional encryption” is allowed to pass through the server. Conventional encryption uses a single cipher that requires a single key to be decrypted. This is in contrast to email that has been encrypted using “public key encryption” which is encrypted with a public key and decrypted with a private key. The default values is disallow.

recovererror *<error message>*

Specifies the error message that is sent to the client when an email message is not encrypted using a required key specified with the “encryptkeys” setting. In order to make the message readable, it should be spread out over several lines as in the following example:

```
recovererror 550-  You have violated corporate policy with this message
recovererror 550-  You must encrypt this message to the required key.
recovererror 550   Do it again, and severe punishment may be forthcoming!
```

You will notice that the standard SMTP 550 - parameter is used to indicate that another line is to follow and no dash is used on the final line.

forbiderror *<error message>*

Specifies the error message that is sent to the client when an email message has been encrypted using a forbidden key. Forbidden keys are defined with the “forbidkey” setting. In order to make the message readable, it should be spread out over several lines as in the previous example.

signatureerror *<error message>*

Specifies the error message that is sent to the client when a signature policy violation occurs. In order to make the message readable, it should be spread out over several lines as in the previous example.

encrypterror *<error message>*

Specifies the error message that is sent to the client when a clear text message is encountered and encryption is required. You specify that encryption is required through the “mustencrypt” setting. In order to make the message readable, it should be spread out over several lines as in the previous example.

conventionalencrypterror *<error message>*

Specifies the error message that is sent to the client when an attempt is made to send conventionally encrypted email when this practice is disallowed by the “conventionalencrypt” setting. In order to make the message readable, it should be spread out over several lines as in the previous example.

Extracting Key IDs for Configuration Purposes

When performing the configuration, you will need to determine the 64-bit key IDs for recovery and forbidden keys. Rather than go through the time consuming process of looking up each key, you can run a useful utility that parses all of these IDs automatically for you using the following command:

```
pgpkeyid [-e]
pgpkeyid [-k] <keyring>
   or
pgpkeyid [-a] <asciiarmor>
```

-e	Lists the encryption portion of the DSS / Diffie-Hellman key, which is the portion used for the “forbidkeys” and “RecoveryKeys” configuration options. Without this switch you will get the signing portion of the key.
-k	Parses the key IDs from a PGP keyring or
-a	Parses the key IDs from an ASCII armored file.

Here is an example of the command line used to list all of the encryption keys in a keyring file:

```
pgpkeyid -e -k keyring.pgp > keyring.new
```

Tips for Reconfiguring your SMTP Server

If you are running the Policy Management Agent program and the SMTP server on the same machine, you will need to redirect the server to listen on a port other than port 25. To do this, you use the “smtpport configuration option to specify the new port. However, you also need to reconfigure your SMTP server to begin listening on the alternate port.

Some SMTP servers do not provide the option of specifying an alternate port, and if this is the case, you will need to install one that does allow you to configure this option such as Berkeley Send Mail 8.8.

If you are using Berkeley Send Mail 8.8, you should add an entry for the alternate port in the /etc/services configuration file as follows:

```
smtp2     (alternate port)/tcp     mail2
```

To prevent remote machines from being able to bypass the Policy Management Agent for SMTP, you should also modify the sendmail configuration file (which is located at /etc/mail/sendmail.cf by default) by locating the following line:

```
0 DaemonPortOptions=port=smtp
```

You need to modify this line as follows:

```
0 DaemonPortOptions=port=smpt2,Addr=127.0.0.1
```

This tells the server to listen on “smpt2” (the alternate port) and to only accept connections from the local host.

Chapter 3

Operation and Maintenance

This chapter describes how to run and maintain the Policy Management Agent for SMTP.

Starting the Policy Management Agent

Once you have supplied the appropriate information and specified the desired policy enforcements in the configuration file, you can run the policy agent. To run the policy agent go to the directory where the binary files are located, and issue the following command:

```
pgppmad -d -f <config file>
```

The Policy Management Agent is initialized based on the values in the specified configuration file and then begins intercepting email for policy enforcement. The -d option allows you to run the Policy Management Agent for SMTP as a background process.

Stopping the Policy Management Agent

To stop the Policy Agent, you need to kill the Policy Management Agent process. A special file called /etc/pgppmad.pid is created when you run the Policy Management Agent for SMTP which captures the process ID so you do not have to search for this ID yourself. All you need to do to stop the policy management agent is issue the following command:

kill [-HUP] ‘cat /etc/pgppmad.pid‘

The optional “HUP” switch allows you to stop the server and then start it up again with any new configuration values. This option is useful when you are making minor adjustments to the configuration file.

NOTE: You should be aware that when you stop the Policy Management Agent, no email will be allowed to pass through the server until you re-route it back through your SMTP server. If you have redirected the port assignment, you will need to re-configure your SMTP server to listen at the appropriate port.

Examining the log file

Depending on the level of logging you select in the configuration file, information is recorded in a log file for each request that is processed by the Policy Management Agent. By default, this information is stored in the /var/adm/messages file but you can have the information directed to any file of your choosing by specifying the name and location with the “log file” option in the configuration file. Here is an example of kind of information you will encounter in the log file:

```
Sep 16 21:37:28 keydev.pgp.com 250-EXPN

Sep 16 21:37:28 keydev.pgp.com 250-VERB

Sep 16 21:37:28 keydev.pgp.com 250-8BITMIME

Sep 16 21:37:28 keydev.pgp.com 250-SIZE

Sep 16 21:37:28 keydev.pgp.com 250-DSN

Sep 16 21:37:28 keydev.pgp.com 250-ONEX

Sep 16 21:37:28 keydev.pgp.com 250-ETRN

Sep 16 21:37:28 keydev.pgp.com 250-XUSR

Sep 16 21:37:28 keydev.pgp.com 250 HELP

Sep 16 21:37:24 keydev.pgp.com pgppmad[3567]: [205.180.136.33] MAIL
From:<root@ultratest.pgp.com> SIZE=29412

Sep 16 21:37:25 keydev.pgp.com pgppmad[3567]: Current connections: 0

Sep 16 21:37:25 keydev.pgp.com pgppmad[3567]: Connection from:
[205.180.136.33]
```

Index