

# PreciseMail Anti-Spam Gateway Installation Guide, UNIX Edition

July 2010

This manual provides installation and setup instructions for PreciseMail Anti-Spam Gateway.

<b>Operating System and Version:</b>	Solaris 8 or later RedHat Linux 7.2 or later Tru64 UNIX V4.0D or later
<b>PMDF Version:</b>	PMDF V6.2-1 or later
<b>Sendmail Version:</b>	Sendmail 8.12 or later
<b>Sun Messaging Server Version:</b>	Sun Messaging Server 5.2 or later
<b>Software Version:</b>	PreciseMail Anti-Spam Gateway V3.2

**Process Software**

---

**20 July 2010**

Copyright (c) 2010 Process Software, LLC. All Rights Reserved. Unpublished — all rights reserved under the copyright laws of the United States

No part of this publication may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language or computer language, in any form or by any means electronic, mechanical, magnetic, optical, chemical, or otherwise without the prior written permission of:

Process Software, LLC  
959 Concord Street  
Framingham, MA 01701-4682 USA  
Voice: +1 508 879 6994; FAX: +1 508 879 0042  
info@process.com

Process Software, LLC (“Process”) makes no representations or warranties with respect to the contents hereof and specifically disclaims any implied warranties of merchantability or fitness for any particular purpose. Furthermore, Process Software reserves the right to revise this publication and to make changes from time to time in the content hereof without obligation of Process Software to notify any person of such revision or changes.

Use of PreciseMail Anti-Spam Gateway software and associated documentation is authorized only by a Software License Agreement. Such license agreements specify the number of systems on which the software is authorized for use, and, among other things, specifically prohibit use or duplication of software or documentation, in whole or in part, except as authorized by the Software License Agreement.

*Restricted rights legend*

Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013 or as set forth in the Commercial Computer Software — Restricted Rights clause at FAR 52.227-19.

MultiNet is a registered trademark of Process Software, LLC.

TCPware is a trademark of Process Software, LLC.

PMDF is a trademark of Process Software, LLC.

All other trademarks are the property of their respective owners.

---

# Contents

---

PREFACE	vii
---------	-----

---

<b>CHAPTER 1</b>	<b>PREPARING TO INSTALL PRECISEMAIL ANTI-SPAM GATEWAY</b>	<b>1-1</b>
------------------	---	------------

---

1.1	PREREQUISITE SOFTWARE	1-1
1.2	ACCESSING THE ONLINE RELEASE NOTES	1-1
1.3	INSTALLATION PROCEDURE REQUIREMENTS	1-1

---

<b>CHAPTER 2</b>	<b>INSTALLING PRECISEMAIL ANTI-SPAM GATEWAY</b>	<b>2-1</b>
------------------	---	------------

---

2.1	INVOKING INSTALL	2-1
2.2	DISK AND DIRECTORY SELECTION	2-1
2.3	THE INSTALLATION COMPLETES	2-2
2.4	UPGRADING TO PRECISEMAIL ANTI-SPAM GATEWAY V3.1	2-2
2.4.1	Uninstalling PreciseMail 3.0 Or Greater	2-2
2.4.2	Uninstalling PreciseMail Versions Prior To 3.0 On Solaris	2-3
2.4.3	Uninstalling PreciseMail Versions Prior To 3.0 On Linux	2-3
2.4.4	Uninstalling PreciseMail Versions Prior To 3.0 On Tru64	2-3

---

<b>CHAPTER 3</b>	<b>POST-INSTALLATION TASKS FOR PMDF</b>	<b>3-1</b>
------------------	---	------------

---

3.1	PRECISEMAIL ANTI-SPAM GATEWAY LICENSE INFORMATION	3-1
3.2	PMDF CONFIGURATION FOR RUNNING PRECISEMAIL ANTI-SPAM GATEWAY	3-1

## Contents

3.2.1	Configuring the PMDF PIPE and PMAS channels _____	3-1
3.2.2	Define PreciseMail Anti-Spam Gateway Channel in job_controller.cnf_site _____	3-2
3.2.3	Create an alias for a PIPE address _____	3-2
3.2.4	Create a PIPE option file _____	3-3
3.2.5	Adding the PMAS Routing to mappings _____	3-3
3.2.6	Recompiling the PMDF configuration _____	3-4
<hr/>		
3.3	CREATING CRON ENTRIES FOR PERIODIC JOBS	3-4
<hr/>		
3.4	STARTING PRECISEMAIL	3-4
<hr/>		
3.5	VERIFYING PRECISEMAIL ANTI-SPAM GATEWAY IS RUNNING	3-5
<hr/>		
<b>CHAPTER 4</b>	<b>POST-INSTALLATION TASKS FOR SUN MESSAGING SERVER</b>	<b>4-1</b>
<hr/>		
4.1	PRECISEMAIL ANTI-SPAM GATEWAY LICENSE INFORMATION	4-1
<hr/>		
4.2	SUN MESSAGING SERVER CONFIGURATION FOR RUNNING PRECISEMAIL ANTI-SPAM GATEWAY	4-1
4.2.1	Configuring the Sun Messaging Server PMAS channel ____	4-1
4.2.2	Define PreciseMail Anti-Spam Gateway Channel in job_controller.cnf _____	4-2
4.2.3	Create the PreciseMail User _____	4-2
4.2.4	Configuring the PIPE channel program _____	4-2
4.2.5	Adding the PMAS Routing to mappings _____	4-3
4.2.6	Recompiling the Sun Messaging Server configuration ____	4-3
<hr/>		
4.3	CREATING CRON ENTRIES FOR PERIODIC JOBS	4-3
<hr/>		
4.4	STARTING PRECISEMAIL	4-4
<hr/>		
4.5	VERIFYING PRECISEMAIL ANTI-SPAM GATEWAY IS RUNNING	4-4

---

<b>CHAPTER 5</b>	<b>POST-INSTALLATION TASKS FOR SENDMAIL</b>	<b>5-1</b>
<hr/>		
5.1	PRECISEMAIL ANTI-SPAM GATEWAY LICENSE INFORMATION	5-1
<hr/>		
5.2	SENDMAIL CONFIGURATION FOR RUNNING PRECISEMAIL ANTI-SPAM GATEWAY	5-1
5.2.1	Configuring Sun-Supplied Sendmail _____	5-1
5.2.2	Configuring Compiled Sendmail _____	5-2
<hr/>		
5.3	CREATE THE PROCESSOR ALIAS	5-2
<hr/>		
5.4	CREATING CRON ENTRIES FOR PERIODIC JOBS	5-2
<hr/>		
5.5	ACTIVATING PRECISEMAIL ANTI-SPAM GATEWAY	5-3
<hr/>		
5.6	VERIFYING PRECISEMAIL ANTI-SPAM GATEWAY IS RUNNING	5-4
<hr/>		
<b>CHAPTER 6</b>	<b>POST-INSTALLATION TASKS FOR THE PASS-THROUGH PROXY</b>	<b>6-1</b>
<hr/>		
6.1	PRECISEMAIL ANTI-SPAM GATEWAY LICENSE INFORMATION	6-1
<hr/>		
6.2	PRECISEMAIL PASS-THROUGH SMTP SERVER CONFIGURATION	6-1
6.2.1	Configuring the Pass-Through SMTP Server _____	6-2
<hr/>		
6.3	CREATING CRON ENTRIES FOR PERIODIC JOBS	6-2
<hr/>		
6.4	STARTING THE PMAS PASS-THROUGH SMTP SERVER	6-3
<hr/>		
6.5	VERIFYING THE PASS-THROUGH PROXY IS RUNNING	6-3

## Contents

---

<b>CHAPTER 7</b>	<b>CONFIGURING THE WEB-BASED USER INTERFACE</b>	<b>7-1</b>
7.1	CONFIGURING THE APACHE WEB SERVER	7-2
7.2	CONFIGURING THE SUNONE WEB SERVER	7-2
7.3	CHANGING THE PMAS_ADMIN AND PMAS_REPORTS PASSWORDS	7-3

---

<b>APPENDIX A</b>	<b>SAMPLE PRECISEMAIL ANTI-SPAM GATEWAY INSTALLATION</b>	<b>A-1</b>
-------------------	--	------------

---

<b>APPENDIX B</b>	<b>FILES CREATED DURING INSTALLATION</b>	<b>B-1</b>
-------------------	--	------------

---

**INDEX**

---

**TABLES**

B-1	PreciseMail Anti-Spam Gateway files created during installation	—	B-1
-----	---	---	-----

---

# Preface

This guide describes how to install PreciseMail Anti-Spam Gateway on the Solaris, Linux, and Tru64 operating systems.

---

## Intended Audience

This manual is intended for use by the system manager or any individual responsible for installing and maintaining the PreciseMail Anti-Spam Gateway product.

---

## Document Structure

This guide consists of eight chapters and two appendices.

Chapter 1	Contains pre-installation information.
Chapter 2	Describes the PreciseMail Anti-Spam Gateway installation procedure.
Chapter 3	Contains post-installation information for PMDF.
Chapter 4	Contains post-installation information for Sun Messaging Server.
Chapter 5	Contains post-installation information for Sendmail.
Chapter 6	Contains post-installation information for the pass-through proxy server.
Chapter 7	Contains information on configuring the web user interface.
Chapter 8	Contains information on uninstalling PreciseMail Anti-Spam Gateway.
Appendix A	Contains a listing of a sample installation.
Appendix B	Contains a list of the files created by an installation.

---

## Related Documents

You can find additional information in the following documents:

- *PreciseMail Anti-Spam Gateway User's Guide* describes the PreciseMail Anti-Spam Gateway user interface.
- *PreciseMail Anti-Spam Gateway Management Guide* describes the PreciseMail Anti-Spam Gateway message scanner.
- *PreciseMail Anti-Spam Gateway Release Notes* contain information and updates not included in this manual. The release notes are part of the software distribution kit.





# 1

---

## Preparing to Install PreciseMail Anti-Spam Gateway

This chapter describes the steps that should be taken prior to installing the PreciseMail Anti-Spam Gateway product.

---

### 1.1 Prerequisite Software

PreciseMail Anti-Spam Gateway requires one of the following operating systems:

- Sun Solaris 8 or later
- RedHat Linux 7.2 or later
- SuSE Linux 9.0 or later
- HP Tru64 UNIX V4.0D or later

The PMDF version of PreciseMail Anti-Spam Gateway requires PMDF V6.2-1 or later, available from Process Software.

The Sun Messaging Server version of PreciseMail Anti-Spam Gateway requires Sun Messaging Server 5.2 or later, available from Sun Microsystems.

The Sendmail version of PreciseMail Anti-Spam Gateway requires Sendmail 8.12 or greater with milter support.

Sophos Anti-Virus must be installed on the same system as PreciseMail Anti-Spam Gateway if you wish to enable the Sophos virus-scanning feature of the pass-through proxy server.

---

### 1.2 Accessing the Online Release Notes

Before any changes are made to the system, the PreciseMail Anti-Spam Gateway installation process will give you the option to read the release notes. After installing PreciseMail Anti-Spam Gateway, you can read the release notes by viewing the file `/pmas/doc/release_notes.txt`

---

### 1.3 Installation Procedure Requirements

Before installing PreciseMail Anti-Spam Gateway, ensure that the following privileges, resources, and requirements are met:

- All the normal privileges of the system administrator (root) account.
- Approximately 5 to 10 minutes, depending on your system configuration, distribution medium, and options selected.
- Approximately 40 MB of free space on a disk for use during the installation procedure.

## Preparing to Install PreciseMail Anti-Spam Gateway

- Approximately 30 MB of free space on a disk for a full installation.

# 2

---

## Installing PreciseMail Anti-Spam Gateway

Before beginning the PreciseMail Anti-Spam Gateway installation, you should be logged into the root account or another suitably privileged account.

---

### 2.1 Invoking install

Change your current directory to the directory containing the PreciseMail kit you wish to install, and run the install program. (In the example below, PreciseMail is being installed as a proxy on a Solaris SPARC system. Choose the appropriate operating system and MTA for your system.)

```
# cd pmas031_solsparc_proxy
# ./install
Verifying manifest integrity...OK
Verifying system...OK
Verifying kit
integrity.....
.....
.....OK
```

The install program will check the kit to make sure it is complete and that it can be installed on the current system.

```
PreciseMail Anti-Spam Gateway 3.1
SunOS (sparc)
Copyright (c) Process Software. All rights reserved
Would you like to read the release notes for this kit [y/n]?
```

If you wish to read the release notes before installing the kit, type  and then press . If you do not, type  and then press .

---

### 2.2 Disk and Directory Selection

PreciseMail Anti-Spam Gateway can reside on any disk. The installation prompts you for the name and location of the top-level directory where you wish PreciseMail Anti-Spam Gateway to be installed.

```
Configuring PreciseMail Directories
-----

PreciseMail places its files in a private directory structure. This
directory structure can be located on any disk, but the disk must have
sufficient free space to hold all of the PreciseMail images, temporary
files, and log files.

A symbolic link will be created that links '/pmas' to the
directory that you specify. For example, if you specify
'/opt/pmas' as the installation location, a directory
'/opt/pmas' will be created and a symbolic link will be created
that links '/pmas' to '/opt/pmas'.

PreciseMail install directory [/opt/pmas]:
```

At the prompt, enter the name of the directory in which you wish PreciseMail to be installed.

## Installing PreciseMail Anti-Spam Gateway

Once a directory has been specified, the directory is created (if it doesn't already exist) and a symbolic link /pmas is created which points to that directory.

---

### 2.3 The Installation Completes

After the configuration questions, the PreciseMail Anti-Spam Gateway software and related files are installed. Informational messages about the individual components are displayed as needed.

After the installation completes, perform the post-installation tasks appropriate for your platform. System administrators should perform the actions described in Chapter 3 for PMDF systems, Chapter 4 for Sun Messaging Server systems, Chapter 5 for Sendmail systems, and Chapter 6 for the pass-through proxy server (PTSMTP).

Information on configuring web servers to display the web-based user interface is contained in Chapter 7.

---

### 2.4 Upgrading To PreciseMail Anti-Spam Gateway V3.1

If you are upgrading to PreciseMail Anti-Spam Gateway V3.1 from a previous version, uninstall the previous version before installing V3.1.

Once the previous version of PreciseMail Anti-Spam Gateway has been successfully uninstalled, install the new version. If you are running PreciseMail Anti-Spam Gateway with the Sendmail MTA, you will need to restart the pmas\_milter process after the upgrade installation completes.

**Note: The uninstallation procedures will only remove PreciseMail Anti-Spam Gateway images and distribution files. All site-specific configurations, user information, quarantined messages, and discarded messages will be left on the system. Future installations of PreciseMail Anti-Spam Gateway will restore site-specific configuration files saved during uninstall.**

---

#### 2.4.1 Uninstalling PreciseMail 3.0 Or Greater

To uninstall PreciseMail V3.0 or greater on any UNIX operating system, run the following command as root:

```
# /pmas/bin/uninstall
```

```
PreciseMail Anti-Spam Gateway 3.0  
SunOS (sparc)  
Copyright (c) Process Software. All rights reserved
```

```
NOTE: Site-specific data, such as configuration files, will not  
be removed from your system by this uninstall process.
```

```
Are you sure you want to uninstall this product [y/n]? y
```

---

## 2.4.2 Uninstalling PreciseMail Versions Prior To 3.0 On Solaris

To uninstall a previous version of PreciseMail Anti-Spam Gateway on Solaris, run the following command as root:

```
# pkgrm PMAS
The following package is currently installed:
  PMAS          PreciseMail Anti-Spam Gateway
                (sparc) 2.4

Do you want to remove this package? y
## Removing installed package instance <PMAS>

This package contains scripts which will be executed with super-user
permission during the process of removing this package.

Do you want to continue with the removal of this package [y,n,?,q] y
## Verifying package dependencies.
## Processing package information.
## Executing preremove script.

[...]

## Updating system information.
Removal of <PMAS> was successful.
```

---

## 2.4.3 Uninstalling PreciseMail Versions Prior To 3.0 On Linux

To uninstall a previous version of PreciseMail Anti-Spam Gateway on Linux, run the following command as root:

```
# rpm -e pmas-2.4-0
```

---

## 2.4.4 Uninstalling PreciseMail Versions Prior To 3.0 On Tru64

To uninstall a previous version of PreciseMail Anti-Spam Gateway on Tru64, run the following command as root:

```
# setld -d PMAS024
Deleting "PreciseMail Anti-Spam Gateway" (PMAS024).
#
```



# 3

---

## Post-Installation Tasks For PMDF

This chapter contains important information about the PreciseMail Anti-Spam Gateway configuration and startup options.

---

### 3.1 PreciseMail Anti-Spam Gateway License Information

When you purchase a PreciseMail Anti-Spam Gateway license, you will receive a license key. The license key data must be placed verbatim in a file named `/pmas/PMAS.license`. If this file is not found, or if the included license data is invalid, PreciseMail Anti-Spam Gateway will not run.

For example, the contents of `/pmas/PMAS.license` would look something like:

```
Issuer: PSC
Authorization Number: 0310218718
Product name: PMAS
Producer: PSC
Number of Units: 0
Key Termination Date: 20-OCT-2010
Availability Table Code: P
Activity Table Code: Solaris
Checksum: 1-6322-BC0C-A6E9-9947
```

If you have already enabled web access to PMAS as described in Chapter 7 of this manual, you can enter license information in the web-based administration interface.

---

### 3.2 PMDF Configuration for running PreciseMail Anti-Spam Gateway

Before PreciseMail Anti-Spam Gateway can run, PMDF has to be configured to pass incoming mail messages to PreciseMail Anti-Spam Gateway. This is done by configuring PIPE and PMAS channels and setting up an alias, rewrite rules, and a mapping entry for PreciseMail Anti-Spam Gateway. The sections below cover the steps necessary to properly configure PMDF for PreciseMail Anti-Spam Gateway to run; for more details on PMDF configuration, please consult the PMDF documentation.

---

#### 3.2.1 Configuring the PMDF PIPE and PMAS channels

The hooks between PMDF and PreciseMail Anti-Spam Gateway are implemented using the PMDF PIPE and PMAS channels. The PIPE channel is provided by PMDF; the PMAS channel is provided with PreciseMail Anti-Spam Gateway. `/pmdf/table/pmdf.cnf` can be modified to add rewrite rules for the PIPE and PMAS channels at the top of the file (somewhere among the other rewrite rules):

## Post-Installation Tasks For PMDF

```
!  
! PreciseMail Anti-Spam Gateway processor rewrite rules  
!  
pipe.example.com                $U%pipe.example.com@PIPE-DAEMON  
!  
! Rewrites for pmas channel  
!  
pmas                            $U%pmas.example.com@PMAS-DAEMON  
pmas.example.com                $U%pmas.example.com@PMAS-DAEMON
```

and add definitions for the channels themselves to the channel definition part of `/pmdf/table/pmdf.cnf`:

```
!  
! Pipe channel  
!  
pipe  
PIPE-DAEMON  
  
!  
! PreciseMail Anti-Spam Gateway  
!  
pmas  
PMAS-DAEMON
```

---

### 3.2.2 Define PreciseMail Anti-Spam Gateway Channel in `job_controller.cnf_site`

In order for PMDF to process mail enqueued to the PreciseMail Anti-Spam Gateway channel, a channel master program must be defined inside the PMDF Job Controller. This definition should be added to the `/pmdf/table/job_controller.cnf_site` file. The entry should look like this:

```
[CHANNEL=pmas]  
master_command=/pmas/bin/pmas_master
```

---

### 3.2.3 Create an alias for a PIPE address

Mail sent to the PreciseMail Anti-Spam Gateway user interface is routed by means of an alias that forwards to the PIPE channel. This alias should be added to your `/pmdf/table/aliases` file or to your directory, if you're using a directory channel. The alias should look something like this:

```
precisemail: precisemail@pipe.example.com
```

The specified domain for the alias's value should match the domain specified in the rewrite rule for the PIPE channel.



### 3.2.4 Create a PIPE option file

An option file, `pipe_option`, must be created in `/pmdf/table/` for the PIPE channel. It should contain a line similar to the following:

```
precisemail@pipe.example.com=/pmas/bin/pmas_process < %s
```

The left-hand side of the equal sign must match the alias established in the preceding section, because the PIPE channel hands mail sent to that address to the program associated with that address in the `pipe_option` file.

### 3.2.5 Adding the PMAS Routing to mappings

The last addition is a mapping entry that tells PMDF to route incoming mail messages to the PreciseMail Anti-Spam Gateway channel, `pmas`. This can be done using the `CONVERSIONS` or `SCRIPT` mapping table entries. (The `SCRIPT` mapping is supported by PMDF V6.2 with the `PMDF_SCRIPT_ECO`. PMDF V6.1 sites must use the `CONVERSIONS` entry.) A `CONVERSIONS` or `SCRIPT` table entry should be added to `/pmdf/table/mappings` and should look something like this:

```
!
! The SCRIPT channel (process incoming mail for local users)
!
SCRIPT
  IN-CHAN=tcp_*;OUT-CHAN=l;SCRIPT      CHANNEL=pmas,maxblocks=200,maxlines=2000,Yes
  IN-CHAN=*;OUT-CHAN=*;SCRIPT        No
```

You can choose to use a `CONVERSIONS` entry in the same way; the only difference is that the `MAXBLOCKS` and `MAXLINES` parameters (which limit messages processed by PMAS based on file sizes) are not available via the `CONVERSIONS` entry.

```
!
! The CONVERSIONS > PMAS entry
!
CONVERSIONS
  IN-CHAN=tcp_*;OUT-CHAN=l;CONVERT    CHANNEL=pmas,Yes
  IN-CHAN=*;OUT-CHAN=*;CONVERT      No
```

If you already have a `CONVERSION` channel in place, simply add the appropriate lines with `"CHANNEL=pmas"` to your existing channel.

The `SCRIPT` entry works much like the entry for a conversion channel. The `IN-CHAN` and `OUT-CHAN` keywords determine which messages get routed to the `SCRIPT` channel. In the example above, incoming SMTP mail from all of the `"tcp"` channels being routed to the local `"l"` channel will be forwarded to the `PMAS` channel first. The second line serves as a default, so any other mail (say, from `tcp_*` to `tcp_*`) will not get routed.

If you use the PMDF `popstore` or `MessageStore`, you'll need to add routing lines for them as well.

## Post-Installation Tasks For PMDF

PreciseMail Anti-Spam Gateway will ignore messages larger than 500 KB for performance reasons (most spam messages are typically not that large, so PreciseMail Anti-Spam Gateway typically should not be run on large messages, as it is just wasted processing). The MAXBLOCKS and MAXLINES keywords in the example above limit the size of messages that will be handed to the PMAS channel; messages larger than 200 blocks (100KB) or longer than 2000 lines will not be processed by the PMAS channel (and thus not by PreciseMail Anti-Spam Gateway).

---

### 3.2.6 Recompiling the PMDF configuration

When all the changes above have been made to your PMDF configuration, you need to recompile your configuration (if you're running a compiled configuration) and restart the PMDF dispatcher. This is typically done using commands like the following. For more details, please see the PMDF documentation.

```
# pmdf cnbuild
# pmdf restart
```

---

### 3.3 Creating cron entries for periodic jobs

PreciseMail Anti-Spam Gateway contains several programs that perform periodic tasks such as notifying users of quarantined messages, maintaining statistics, and managing log files.

Six periodic jobs need to be scheduled with cron to run these programs. It is recommended that quarantine notification be performed twice a day at 7:00am and 3:30pm, and log file management be performed once a day between midnight and 1:00am. Statistics collection should be performed every hour, and cluster jobs should be performed every 15 minutes. If you don't enable PreciseMail's Data Synchronization Cluster functionality, the cluster job won't perform any actions.

The default scheduling for the cron jobs is located in `/pmas/com/cronjobs`. Edit the `pmdf` user's crontab file (use the command `crontab -e pmdf`), and add the following commands:

```
0 7 * * * /pmas/bin/notify_quarantined >> /pmas/log/pmas_notify.log 2>&1
30 15 * * * /pmas/bin/notify_quarantined >> /pmas/log/pmas_notify.log 2>&1
5 0 * * * /pmas/com/run_nightly.sh > /dev/null 2>&1
0 * * * * /pmas/bin/bastats >> /pmas/log/bastats.log 2>&1
0,15,30,45 * * * * /pmas/bin/clu_batch > /dev/null 2>&1
0 * * * * /pmas/bin/pmas_update > /dev/null 2>&1
```

---

### 3.4 Starting PreciseMail

Before messages are processed, PreciseMail should be started by running the following command:

```
# /etc/init.d/pmas start
```

This command performs setup work and starts any daemon processes that PreciseMail requires. To call the `pmas` control script during system boot, create a symbolic link in the `/etc/rc2.d` directory to the control script.

For example, the following command could be used to create a symbolic link to the pmas control script:

```
# ln -s /etc/init.d/pmas /etc/rc2.d/S88pmas
```

For more information about how the contents of the `/etc/init.d` and `/etc/rc*.d` directories are used during system boot, consult the *Solaris System Administration Guide*. The *Guide* is included with the Solaris operating system and is available online from <http://docs.sun.com>.

---

### 3.5 Verifying PreciseMail Anti-Spam Gateway is running

If everything is configured correctly, incoming SMTP mail messages destined for local users should now be processed by PreciseMail Anti-Spam Gateway. To verify that messages are being routed properly, you can check the `/pmdf/log/mail.log_current` file to see that messages are being routed to the pmas channel. If the PreciseMail Anti-Spam Gateway script is being invoked properly, you'll also find a `pmas.log` file in the `/pmas/log/` directory.



# 4

---

## Post-Installation Tasks For Sun Messaging Server

This chapter contains important information about the PreciseMail Anti-Spam Gateway configuration and startup options.

---

### 4.1 PreciseMail Anti-Spam Gateway License Information

When you purchase a PreciseMail Anti-Spam Gateway license, you will receive a license key. The license key data must be placed verbatim in a file named `/pmas/PMAS.license`. If this file is not found, or if the included license data is invalid, PreciseMail Anti-Spam Gateway will not run. For example, the contents of `/pmas/PMAS.license` would look something like:

```
Issuer: PSC
Authorization Number: 0310218718
Product name: PMAS
Producer: PSC
Number of Units: 0
Key Termination Date: 20-OCT-2010
Availability Table Code: P
Activity Table Code: Solaris
Checksum: 1-6322-BC0C-A6E9-9947
```

If you have already enabled web access to PMAS as described in Chapter 7 of this manual, you can enter license information in the web-based administration interface.

---

### 4.2 Sun Messaging Server Configuration for running PreciseMail Anti-Spam Gateway

Before PreciseMail Anti-Spam Gateway can run, Sun Messaging Server has to be configured to pass incoming mail messages to PreciseMail Anti-Spam Gateway. This is done by configuring PIPE and PMAS channels and setting up a user, rewrite rules, and a mapping entry for PreciseMail Anti-Spam Gateway. The sections below cover the steps necessary to properly configure the Messaging Server for PreciseMail Anti-Spam Gateway to run; for more details on Messaging Server configuration, please consult the Sun Messaging Server documentation.

---

#### 4.2.1 Configuring the Sun Messaging Server PMAS channel

The hooks between Sun Messaging Server and PreciseMail Anti-Spam Gateway are implemented using the Sun Messaging Server PIPE and PMAS channels. The PIPE channel is provided by the Messaging Server; the PMAS channel is provided with PreciseMail Anti-Spam Gateway. `server-root/msg-instance/imta/config/imta.cnf` can be modified to add rewrite rules for the PMAS channel at the top of the file (somewhere among the other rewrite rules):

## Post-Installation Tasks For Sun Messaging Server

```
!  
! Rewrites for pmas channel  
!  
pmas $U%pmas.example.com@pmas-daemon  
pmas.example.com $U%pmas.example.com@pmas-daemon
```

and add a definition for the channel itself to the channel definition part of *server-root/msg-instance/imta/config/imta.cnf*:

```
!  
! PreciseMail Anti-Spam Gateway  
!  
pmas  
pmas-daemon
```

---

### 4.2.2 Define PreciseMail Anti-Spam Gateway Channel in *job\_controller.cnf*

In order for the Sun Messaging Server to process mail enqueued to the PreciseMail Anti-Spam Gateway channel, a channel master program must be defined inside the Job Controller. This definition should be added to the *server-root/msg-instance/imta/config/job\_controller.cnf* file. The entry should look like this:

```
[CHANNEL=pmas]  
master_command=/pmas/bin/pmas_master
```

---

### 4.2.3 Create the PreciseMail User

Mail sent to the PreciseMail Anti-Spam Gateway user interface is routed by means of a "dummy" user that calls out to the PIPE channel. This user should be added by using commands similar to these:

```
imadmin user create -D ServiceAdmin -F PreciseMail -L Processor \  
-l precisemail -n example.com -W pmas.secret -w secret
```

Note that the command has been line-wrapped for readability. This command creates a user named "precisemail" in the example.com domain with a password of "pmas.secret".

---

### 4.2.4 Configuring the PIPE channel program

Before it can be used by the Messaging Server's PIPE channel, the *pmas\_process* program must be registered with the Messaging Server. First, a symbolic link must be created that links the PreciseMail processor to the Messaging Server's PIPE channel programs directory:

```
ln -s /pmas/bin/pmas_process server-root/msg-instance/imta/programs/pmas_process
```

Next, register the program with the Sun Messaging Server:

```
imsimta program -a -m pmas_process -p pmas_process -e postmaster
```

Now, configure the precisemail user so that all mail sent to it is passed to the *pmas\_process* program:

```
imadmin user modify -D ServiceAdmin -l precisemail -n example.com -w secret \  
-A+maildeliveryoption:program  
imadmin user modify -D ServiceAdmin -l precisemail -n example.com -w secret \  
-A+mailprogramdeliveryinfo:pmas_process
```

Note that the above commands have been line-wrapped for readability.

---

### 4.2.5 Adding the PMAS Routing to mappings

The last addition is a mapping entry that tells Messaging Server to route incoming mail messages to the PreciseMail Anti-Spam Gateway channel, pmas. This can be done using the CONVERSIONS mapping table entries. A CONVERSIONS table entry should be added to *server-root/msg-instance/imta/config/mappings* and should look something like this:

```
!  
! The CONVERSIONS > PMAS entry  
!  
CONVERSIONS  
  
IN-CHAN=tc*_*;OUT-CHAN=1;CONVERT CHANNEL=pmas, Yes  
IN-CHAN=*;OUT-CHAN=*;CONVERT No
```

If you already have a CONVERSION channel in place, simply add the appropriate lines with "CHANNEL=pmas" to your existing channel.

---

### 4.2.6 Recompiling the Sun Messaging Server configuration

When all the changes above have been made to your Sun Messaging Server configuration, you need to recompile your configuration and restart the messaging server. This is typically done using commands like the following. For more details, please see the Sun Messaging Server documentation.

```
# imsimta cbuild  
# imsimta restart
```

---

## 4.3 Creating cron entries for periodic jobs

PreciseMail Anti-Spam Gateway contains several programs that perform periodic tasks such as notifying users of quarantined messages, maintaining statistics, and managing log files.

Six periodic jobs need to be scheduled with cron to run these programs. It is recommended that quarantine notification be performed twice a day at 7:00am and 3:30pm, and log file management be performed once a day between midnight and 1:00am. Statistics collection should be performed every hour, and cluster jobs should be performed every 15 minutes. If you don't enable PreciseMail's Data Synchronization Cluster functionality, the cluster job won't perform any actions.

## Post-Installation Tasks For Sun Messaging Server

The default scheduling for the cron jobs is located in `/pmas/com/cronjobs`. Edit the `mailsrv` user's crontab file (use the command `crontab -e mailsrv`), and add the following commands:

```
0 7 * * * /pmas/bin/notify_quarantined >> /pmas/log/pmas_notify.log 2>&1
30 15 * * * /pmas/bin/notify_quarantined >> /pmas/log/pmas_notify.log 2>&1
5 0 * * * /pmas/com/run_nightly.sh > /dev/null 2>&1
0 * * * * /pmas/bin/bastats >> /pmas/log/bastats.log 2>&1
0,15,30,45 * * * * /pmas/bin/clu_batch > /dev/null 2>&1
0 * * * * /pmas/bin/pmas_update > /dev/null 2>&1
```

---

### 4.4 Starting PreciseMail

Before messages are processed, PreciseMail should be started by running the following command:

```
# /etc/init.d/pmas start
```

This command performs setup work and starts any daemon processes that PreciseMail requires. To call the `pmas` control script during system boot, create a symbolic link in the `/etc/rc2.d` directory to the control script.

For example, the following command could be used to create a symbolic link to the `pmas` control script:

```
# ln -s /etc/init.d/pmas /etc/rc2.d/S88pmas
```

For more information about how the contents of the `/etc/init.d` and `/etc/rc*.d` directories are used during system boot, consult the *Solaris System Administration Guide*. The *Guide* is included with the Solaris operating system and is available online from <http://docs.sun.com>.

---

### 4.5 Verifying PreciseMail Anti-Spam Gateway is running

If everything is configured correctly, incoming SMTP mail messages destined for local users should now be processed by PreciseMail Anti-Spam Gateway. To verify that messages are being routed properly, you can check the `server-root/msg-instance/log/imta/mail.log_current` file to see that messages are being routed to the `pmas` channel. If the PreciseMail Anti-Spam Gateway script is being invoked properly, you'll also find a `pmas.log` file in the `/pmas/log/` directory.



# 5

---

## Post-Installation Tasks For Sendmail

This chapter contains important information about the PreciseMail Anti-Spam Gateway configuration and startup options.

---

### 5.1 PreciseMail Anti-Spam Gateway License Information

When you purchase a PreciseMail Anti-Spam Gateway license, you will receive a license key. The license key data must be placed verbatim in a file named `/pmas/PMAS.license`. If this file is not found, or if the included license data is invalid, PreciseMail Anti-Spam Gateway will not run. For example, the contents of `/pmas/PMAS.license` would look something like:

```
Issuer: PSC
Authorization Number: 0310218718
Product name: PMAS
Producer: PSC
Number of Units: 0
Key Termination Date: 20-OCT-2010
Availability Table Code: P
Activity Table Code: Solaris
Checksum: 1-6322-BC0C-A6E9-9947
```

If you have already enabled web access to PMAS as described in Chapter 7 of this manual, you can enter license information in the web-based administration interface.

---

### 5.2 Sendmail Configuration for running PreciseMail Anti-Spam Gateway

PreciseMail Anti-Spam Gateway is integrated with Sendmail through the use of a milter named `"pmas_milter"`.

You must be running Sendmail 8.12.x or later, with milter functionality enabled. You can determine if your installation of Sendmail supports milters by running the command:

```
/usr/lib/sendmail -bt -d0.4 < /dev/null
```

If milters are supported, the token `"MILTER"` will appear in the output. If not, you need to re-compile Sendmail with milter functionality enabled. Consult your Sendmail documentation for more information.

---

#### 5.2.1 Configuring Sun-Supplied Sendmail

Sun supplies a customized version of Sendmail with the Solaris operating system. If you compiled your own version of Sendmail, rather than using the version of Sendmail that Solaris provides, follow the instructions in Section 5.2.2.

## Post-Installation Tasks For Sendmail

If you are using the custom version of Sendmail that Sun supplies with the Solaris operating system, edit the `/etc/mail/sendmail.cf` file. Near the top of the file, add an `InputMailFilters` option for `pmas_milter`:

```
O InputMailFilters=/pmas/bin/pmas_milter
```

Just above the `MAILER DEFINITIONS` block of the `sendmail.cf` file, add the following line to specify the milter options:

```
X/pmas/bin/pmas_milter, S=local:/pmas/tmp/pmas.sock, F=T, T=C:90s;S:90s;R:90s;E:90s
```

---

### 5.2.2 Configuring Compiled Sendmail

If you are using a standard Sendmail binary, edit the `sendmail.mc` file located in the `sendmail-8.xx.x/cf/cf` directory of your source distribution. Add the following `INPUT_MAIL_FILTER` macro to the bottom of the file:

```
INPUT_MAIL_FILTER(`/pmas/bin/pmas_milter', `S=local:/pmas/tmp/pmas.sock,F=T, T=C:90s;S:90s;R:90s;E:90s')
```

Save the `sendmail.mc` file, then run the following command to generate a new `sendmail.cf` file and install it in `/etc/mail`:

```
# make install-cf
```

---

### 5.3 Create the Processor Alias

For Sendmail to route user request messages to PreciseMail Anti-Spam Gateway, a “precisemail” alias must be created. Edit the `/etc/mail/aliases` file, and add the following line:

```
precisemail:    |/pmas/bin/pmas_process
```

Rebuild the Sendmail alias database by issuing the following command:

```
# newaliases
```

---

### 5.4 Creating cron entries for periodic jobs

PreciseMail Anti-Spam Gateway contains several programs that perform periodic tasks such as notifying users of quarantined messages, maintaining statistics, and managing log files.

Six periodic jobs need to be scheduled with cron to run these programs. It is recommended that quarantine notification be performed twice a day at 7:00am and 3:30pm, and log file management be performed once a day between midnight and 1:00am. Statistics collection should be performed every hour, and cluster jobs should be performed every 15 minutes. If you don't enable PreciseMail's Data Synchronization Cluster functionality, the cluster job won't perform any actions.

The default scheduling for the cron jobs is located in `/pmas/com/cronjobs`. Edit the daemon user's crontab file (use the command `crontab -e daemon`), and add the following commands:

```

0 7 * * * /pmas/bin/notify_quarantined >> /pmas/log/pmas_notify.log 2>&1
30 15 * * * /pmas/bin/notify_quarantined >> /pmas/log/pmas_notify.log 2>&1
5 0 * * * /pmas/com/run_nightly.sh > /dev/null 2>&1
0 * * * * /pmas/bin/bastats >> /pmas/log/bastats.log 2>&1
0,15,30,45 * * * * /pmas/bin/clu_batch > /dev/null 2>&1
0 * * * * /pmas/bin/pmas_update > /dev/null 2>&1

```

## 5.5 Activating PreciseMail Anti-Spam Gateway

To activate the PreciseMail Anti-Spam Gateway milter, you must start the milter and restart Sendmail. To start the milter, run the following command as the root user:

```
# /etc/init.d/pmas start
```

Next, restart Sendmail. Most systems have a Sendmail control script located in the `/etc/init.d` directory that can be used to restart Sendmail. If this script is present on your system, restart Sendmail by issuing the following commands as root:

```
# /etc/init.d/sendmail stop
# /etc.init.d/sendmail start
```

If you do not have a Sendmail control script, restart Sendmail by manually killing all of the Sendmail processes and then starting Sendmail:

```
# ps -ef | grep sendmail
  root 29651      1  0 14:05:06 ?    0:00 /usr/lib/sendmail -bd
# kill 29651
# /usr/lib/sendmail -bd
```

**Note:** The PreciseMail Anti-Spam Gateway milter must always be started before starting Sendmail. Sendmail will display an error message and immediately terminate if it is started when `pmas_milter` is not running.

Most sites use the Sendmail control script in `/etc/init.d` to automatically start SendMail as part of the system boot procedure. PreciseMail Anti-Spam Gateway provides a `pmas_milter` control script in `/etc/init.d` that can be used to start `pmas_milter` before Sendmail is started during system boot. To call the `pmas_milter` control script during system boot, create a symbolic link in the `/etc/rc2.d` directory that has the same sequence number as the Sendmail control script.

For example, if there is a symbolic link to the Sendmail control script named `S88sendmail` in the `/etc/rc2.d` directory, the following command could be used to create a symbolic link to the `pmas_milter` control script:

```
# ln -s /etc/init.d/pmas /etc/rc2.d/S88pmas
```

For more information about how the contents of the `/etc/init.d` and `/etc/rc*.d` directories are used during system boot, consult the *Solaris System Administration Guide*. The *Guide* is included with the Solaris operating system and is available online from <http://docs.sun.com>.

---

### 5.6 Verifying PreciseMail Anti-Spam Gateway is running

If everything is configured correctly, incoming SMTP mail messages destined for local users should now be processed by PreciseMail Anti-Spam Gateway. If the `pmas_milter` is being invoked properly, you'll also find a `pmas.log` file in the `/pmas/log/` directory.

# 6

---

## Post-Installation Tasks For The Pass-Through Proxy

This chapter contains important information about the PreciseMail Anti-Spam Gateway configuration and startup options.

---

### 6.1 PreciseMail Anti-Spam Gateway License Information

When you purchase a PreciseMail Anti-Spam Gateway license, you will receive a license key. The license key data must be placed verbatim in a file named `/pmas/PMAS.license`. If this file is not found, or if the included license data is invalid, PreciseMail Anti-Spam Gateway will not run. For example, the contents of `/pmas/PMAS.license` would look something like:

```
Issuer: PSC
Authorization Number: 0310218718
Product name: PMAS
Producer: PSC
Number of Units: 0
Key Termination Date: 20-OCT-2010
Availability Table Code: P
Activity Table Code: Solaris
Checksum: 1-6322-BC0C-A6E9-9947
```

If you have already enabled web access to PMAS as described in Chapter 7 of this manual, you can enter license information in the web-based administration interface.

---

### 6.2 PreciseMail Pass-Through SMTP Server Configuration

The PreciseMail Pass-Through SMTP (PTSMTP) Server acts as a proxy server for all incoming mail. The PTSMTP server does not replace your existing SMTP server, but instead works with your existing SMTP server, passing incoming messages directly to your existing server for delivery. Messages are scanned by the PreciseMail engine as they pass through. Quarantined or discarded messages are never actually sent to your primary SMTP server.

To properly set up the PTSMTP server, you must configure it to run on the well-known SMTP port (port 25) and reconfigure your actual SMTP server to run on an alternate port. SMTP clients will open a connection to the PTSMTP server on port 25, which will in turn open a pass-through connection to your actual SMTP server on its alternate port. Messages will be scanned and diverted or passed through as appropriate according to your PMAS configuration settings.

For more information on the PMAS Pass-Through SMTP Server, please see the *PreciseMail Anti-Spam Gateway Management Guide*.

### 6.2.1 --- Configuring the Pass-Through SMTP Server

The PMAS Pass-Through SMTP server will be started if the configuration variables `PTSMTP_LISTEN_PORT`, `PTSMTP_MAILSERVER_PORT`, and `PTSMTP_MAILSERVER_HOST` are defined. These configuration variables are documented in the *PreciseMail Anti-Spam Gateway Management Guide*. The first one specifies the SMTP port (which is normally the default, port 25), and the other two should be defined to point to the host and port number on which your reconfigured primary SMTP server is listening. For example:

```
#
# Listen for incoming SMTP connections on port 25
#
ptsmtp_listen_port      25
#
# PMDF's SMTP server is running on port 2525
# on this same system
#
ptsmtp_mailserver_host  127.0.0.1
ptsmtp_mailserver_port  2525
```

If you have already configured the web-based PMAS GUI, you can define the variables using the administrator's interface. If you have not, you can define the variables by editing the configuration file (`/pmas/data/pmas_config.dat`) and adding them.

There are variables that control the PTSMTP worker processes that run. `PTSMTP_WORKER_MIN` is the minimum number of worker processes that will run. `PTSMTP_WORKER_MAX` is the maximum number of temporary worker processes than can be running simultaneously. The amount of time a temporary process can be idle before it exits is `PTSMTP_IDLE_TIME`.

### 6.3 --- Creating cron entries for periodic jobs

PreciseMail Anti-Spam Gateway contains several programs that perform periodic tasks such as notifying users of quarantined messages, maintaining statistics, and managing log files.

Six periodic jobs need to be scheduled with cron to run these programs. It is recommended that quarantine notification be performed twice a day at 7:00am and 3:30pm, and log file management be performed once a day between midnight and 1:00am. Statistics collection should be performed every hour, and cluster jobs should be performed every 15 minutes. If you don't enable PreciseMail's Data Synchronization Cluster functionality, the cluster job won't perform any actions.

The default scheduling for the cron jobs is located in `/pmas/com/cronjobs`. Edit the daemon user's crontab file (use the command `crontab -e daemon`), and add the following commands:

```
0 7 * * * /pmas/bin/notify_quarantined >> /pmas/log/pmas_notify.log 2>&1
30 15 * * * /pmas/bin/notify_quarantined >> /pmas/log/pmas_notify.log 2>&1
5 0 * * * /pmas/com/run_nightly.sh > /dev/null 2>&1
0 * * * * /pmas/bin/bastats >> /pmas/log/bastats.log 2>&1
0,15,30,45 * * * * /pmas/bin/clu_batch > /dev/null 2>&1
0 * * * * /pmas/bin/pmas_update > /dev/null 2>&1
```

---

## 6.4 Starting the PMAS Pass-Through SMTP server

When the PTSMTMP configuration variables are defined, the pass-through SMTP server is started when the following command is run:

```
# /etc/init.d/pmas start
```

The pass-through SMTP server can be automatically started during system boot. To call the pmas control script during system boot, create a symbolic link in the /etc/rc2.d directory to the control script.

For example, the following command could be used to create a symbolic link to the pmas control script:

```
# ln -s /etc/init.d/pmas /etc/rc2.d/S88pmas
```

For more information about how the contents of the /etc/init.d and /etc/rc\*.d directories are used during system boot, consult the *Solaris System Administration Guide*. The *Guide* is included with the Solaris operating system and is available online from <http://docs.sun.com>.

---

## 6.5 Verifying The Pass-Through Proxy Is Running

After the proxy server has been started, there will be one or more PTSMTMP daemon processes running on the system. You can verify this with the ps command:

```
$ ps -ef | grep ptsmtp
      root 15872      1  0   Aug 27 ?           0:48 /pmas/bin/ptsmtp -D
      root 15874 15872  0   Aug 27 ?           0:32 /pmas/bin/ptsmtp -D
```





# 7

---

## Configuring the Web-Based User Interface

PreciseMail Anti-Spam Gateway includes a web-based user interface. The software requires that you run a web server on the same system running PreciseMail Anti-Spam Gateway. For UNIX, the following web servers can be used:

- Apache
- SunONE Web Server
- Any web server that supports the CGI 1.1 interface

The Apache server is free to run. If you do not currently run a web server on your system, you can download Apache for free from <http://httpd.apache.org/>.

The SunONE web server is available from Sun Microsystems. Please visit the Sun website at <http://www.sun.com/> for more information.

The PreciseMail Anti-Spam Gateway HTML templates are found in the directory `/pmas/html`, supporting files are found in `/pmas/www/htdocs`, and the CGI scripts used by the web interface are found in `/pmas/www/cgi-bin`.

The sections below describe how to configure each of the servers to allow them to serve the PreciseMail Anti-Spam Gateway GUI web pages and scripts.

The steps needed to enable the web-based GUI are as follows:

- 1 Modify your web server configuration to serve the PMAS pages and images.
- 2 Define the `gui_uri_host` variable in `/pmas/data/pmas_config.dat` as the name of the system running the web server that's serving the pages. You may need to define other variables, depending on how you configure your server.
- 3 Edit the file `/pmas/www/htdocs/index.html` to specify the correct URL path for the form's "ACTION" tag, if necessary.

Once configured, the PreciseMail Anti-Spam Gateway User Interface will be accessible to users via the following URL:

`http://yourhost.example.com/pmas/index.html`

**Note:** The sections below describe the changes that should be applied to fresh installations of the web servers. The instructions may differ some for those sites that have previously run these web servers. Please adapt the instructions to suit your particular web server environment.

---

### 7.1 Configuring the Apache Web Server

The following steps are required to modify the Apache Web Server to serve the PreciseMail Anti-Spam Gateway files. Note that the instructions assume that Apache was installed in the `/opt/apache` directory - modify them as appropriate for your installation.

- 1 Edit the file `/opt/apache/conf/httpd.conf`. Add the `FollowSymLinks` directive to the `Options` field of the `cgi-bin` directory:

```
<Directory "/opt/apache/cgi-bin">
    AllowOverride None
    Options FollowSymLinks
    Order allow,deny
    Allow from all
</Directory>
```

- 2 After modifying `httpd.conf`, it is necessary to restart the web server with this command:

```
/opt/apache/bin/apachectl restart
```

- 3 Create a symbolic link named `pmas` in the Apache `cgi-bin` directory that points to the PreciseMail Anti-Spam Gateway `cgi-bin` directory:

```
ln -s /pmas/www/cgi-bin /opt/apache/cgi-bin/pmas
```

- 4 Create a symbolic link named `pmas` in the Apache `htdocs` directory that points to the PreciseMail Anti-Spam Gateway `htdocs` directory:

```
ln -s /pmas/www/htdocs /opt/apache/htdocs/pmas
```

---

### 7.2 Configuring the SunONE Web Server

Recent versions of the SunONE web server are administered through a web-based interface. The following instructions assume that your site is running SunONE Web Server 6.0 or later.

- 1 Connect to the SunONE Web Server administration interface with a web browser. In a default SunONE Web Server configuration, the administration interface is available on port 8888 of the web server system.
- 2 Select the web server you are integrating with PMAS from the drop-down list in the Manage Servers section, and click the Manage button. Click the Virtual Server Class tab at the top of the page that appears, then select the virtual server class that the web server system belongs to from the drop-down list. Click the Manage button next to the drop-down list.
- 3 Click on the Programs tab at the top of the page. Set the value of URL Prefix to be `/cgi-bin/pmas/` and the value of CGI Directory to be `/pmas/www/cgi-bin/`. Click the OK button to add the PMAS CGI mapping.

- 4 Click on the Content Mgmt tab at the top of the page, then choose Additional Document Directories from the menu on the left side of the page. Set the value of URL Prefix to be /pmas/ and the value of Map To Directory to be /pmas/www/htdocs/. Make sure that NONE appears in the Apply Style drop down box, then click the OK button.
- 5 Click the Apply button in the top right corner of the page, and choose to load the new configuration.

---

### 7.3 Changing the `pmas_admin` and `pmas_reports` Passwords

The web-based GUI features a special PreciseMail Anti-Spam Gateway Administrator interface that allows you to easily modify the PMAS configuration and view reports about PMAS processing. To access the administrator pages, you must log in as the user `pmas_admin`. The password for the `pmas_admin` “account” is stored in the PMAS user database (`/pmas/data/pmas_user_db.dat`).

Similarly, there is a special `pmas_reports` login that can be used to access only the PMAS processing reports pages.

When PMAS is first installed, default passwords are supplied for `pmas_admin` and `pmas_reports`. The default `pmas_admin` password is “secret”; the default password for `pmas_reports` is “secrettoo”. You should immediately change the `pmas_admin` and `pmas_reports` passwords using the `/pmas/bin/pmasadmin` utility. To change the `pmas_admin` password from its default value, use the “user `set_password`” command and specify the new password: `new password`:

```
$ pmasadmin user set_password pmas_admin somethingelse
$ pmasadmin user set_password pmas_reports somethingelsetoo
```



# A

## Sample PreciseMail Anti-Spam Gateway Installation

This appendix includes a sample PreciseMail Anti-Spam Gateway installation.

```
# ./install
Verifying manifest integrity...OK
Verifying system...OK
Verifying kit
integrity.....

PreciseMail Anti-Spam Gateway 3.1
SunOS (sparc)
Copyright (c) Process Software. All rights reserved

Would you like to read the release notes for this kit [y/n]? n

Configuring PreciseMail Directories
-----

PreciseMail places its files in a private directory structure. This
directory structure can be located on any disk, but the disk must have
sufficient free space to hold all of the PreciseMail images, temporary
files, and log files.

A symbolic link will be created that links '/pmas' to the
directory that you specify. For example, if you specify
'/opt/pmas' as the installation location, a directory
'/opt/pmas' will be created and a symbolic link will be created
that links '/pmas' to '/opt/pmas'.

PreciseMail install directory [/opt/pmas]: 

Installing PreciseMail Anti-Spam Gateway

/opt/pmas/api
/opt/pmas/api/userdb
/opt/pmas/api/userdb/userdb_api_example1.c
/opt/pmas/api/userdb/userdb_api_example2.c
/opt/pmas/api/userdb/userdb_api_example3.c
/opt/pmas/api/userdb/userdb_api_example4.c
/opt/pmas/api/userdb/userdb_api_example5.c
/opt/pmas/api/userdb/userdb_api_example6.c
/opt/pmas/api/userdb/userdb_api_makefile
/opt/pmas/api/userdb/userdb_api.h
/opt/pmas/bin
/opt/pmas/bin/authdebug

[...]

/opt/pmas/www/htdocs/prefs_icon.gif
/opt/pmas/www/htdocs/purple_bar.gif
/opt/pmas/www/htdocs/quar_icon.gif
/opt/pmas/www/htdocs/red_bar.gif
/opt/pmas/www/htdocs/report_icon.gif
/opt/pmas/www/htdocs/rulelist_icon.gif
/opt/pmas/www/htdocs/up_arrow.gif
/opt/pmas/www/htdocs/yellow_bar.gif
```

## Sample PreciseMail Anti-Spam Gateway Installation

The PMAS administration interface is accessed by logging into the web interface as the pmas\_admin user. The default password for this user is "secret". Please change this password to something more secret as quickly as possible.

# B

## Files Created During Installation

The files in Table B–1 are created during the installation of the PreciseMail Anti-Spam Gateway software.

**Table B–1 PreciseMail Anti-Spam Gateway files created during installation**

File name	Description
	<b>Files in /pmas/bin/</b>
authdebug	Executable image for testing GUI authentication.
bastats	Executable image that gathers PMAS statistics.
bayes	Stand-alone Bayesian executable image.
clu_batch	Data Synch Cluster batch job.
dnsblplug.so	DNSBL plugin shareable used by the PTSMTMP proxy server.
import_config	Executable image that merges updated pmas_config.dat template information.
libcrypto.*	TLS support shareable.
liblber.*	LDAP support shareable.
libldap.*	LDAP support shareable.
libssl.*	TLS support shareable.
notify_quarantined	Executable image for the quarantine notification job.
pcretest	Executable image for testing regular expressions.
pmas_cluster	Data Synch Cluster daemon.
pmas_master	Executable image for the PreciseMail Anti-Spam Gateway channel.
pmas_milter	Executable image for the PreciseMail Anti-Spam Gatewaymilter.
pmas_process	Executable image for the PreciseMail Processor user interface.
pmas_stats	Executable image to parse the contents of pmas.log and generate a report on PreciseMail activities.
pmas_version	Displays summary information for installed PMAS version.
pmasadmin.so	PMAS administrator command-line utility.
pmasplug.so	PMAS shareable used by the PTSMTMP server.
precisemail	Image that can be run from the command line to filter messages.
ptsmtmp	Pass-through SMTP proxy server image.
sophplug.so	Sophos shareable used by the PTSMTMP server.
tls_certreq	Executable image to generate TLS certificates.

## Files Created During Installation

**Table B–1 (Cont.) PreciseMail Anti-Spam Gateway files created during installation**

<b>File name</b>	<b>Description</b>
<b>Files in /pmas/com/</b>	
cronjobs	Example cron table entries for PreciseMail.
run_nightly.sh	Script responsible for maintaining the log directory.
update.sh	Script run by the autoupdate procedure to unpack and install new rules.
<b>Files in /pmas/doc/</b>	
release_notes.txt	Release notes for PreciseMail Anti-Spam Gateway
pmas_install_guide_platform.pdf	PreciseMail Anti-Spam Gateway Installation Guide (Adobe PDF)
pmas_install_guide_platform.ps	PreciseMail Anti-Spam Gateway Installation Guide (PostScript)
pmas_install_guide_platform.txt	PreciseMail Anti-Spam Gateway Installation Guide (ASCII)
pmas_mgmt_guide_platform.pdf	PreciseMail Anti-Spam Gateway Management Guide (Adobe PDF)
pmas_mgmt_guide_platform.ps	PreciseMail Anti-Spam Gateway Management Guide (PostScript)
pmas_mgmt_guide_platform.txt	PreciseMail Anti-Spam Gateway Management Guide (ASCII)
pmas_users_guide.pdf	PreciseMail Anti-Spam Gateway User's Guide (Adobe PDF)
pmas_users_guide.ps	PreciseMail Anti-Spam Gateway User's Guide (PostScript)
pmas_users_guide.txt	PreciseMail Anti-Spam Gateway User's Guide (ASCII)
<b>Files in /pmas/html</b>	
Various	HTML template files for the PMAS GUI.
<b>Files in /pmas/www/cgi-bin</b>	
adminconfig	Executable image for the Administrative Configuration module.
admingroups	Executable image for the Administrative Groups Configuration module.
adminlicense	Executable image for the Administrative License module.
adminreports	Executable image for the Administrative Reports module.
allowlist	Executable image for the Allow List page.
blocklist	Executable image for the Block List page.
pmaslogin	Executable image for the PMAS Login page.
pmaslogout	Executable image for the PMAS Logout.
pmasprefs	Executable image for the PMAS Preferences page.
pmasstart	Executable image for the PMAS Start page.
quarantine	Executable image for the PMAS Quarantine page.
quarcgi	Executable image for the PMAS Quarantine options.
rulelist	Executable image for the PMAS Rules List page.



**Table B-1 (Cont.) PreciseMail Anti-Spam Gateway files created during installation**

<b>File name</b>	<b>Description</b>
<b>Files in /pmas/www/htdocs/</b>	
Various	HTML, JavaScript and CSS files for the PMAS GUI.
<b>Files in /pmas/help/</b>	
pmas_process_help.txt	Help file for the user interface.
pmas_process_help.template	HTML template for the help file

## Files Created During Installation

**Table B–1 (Cont.) PreciseMail Anti-Spam Gateway files created during installation**

File name	Description
<b>Files in /pmas/data/</b>	
00_allowblocklists.cf	Local allow and block rules
00_local_tests.cf	Local rules and scores
20_anti_ratware.cf	Rules to try to identify “legitimate” mail clients.
20_body_tests.cf	Rules applied to message bodies.
20_compensate.cf	Rules to compensate for some of the aggressive rules.
20_head_tests.cf	Rules applied to message headers.
20_html_tests.cf	Rules applied to HTML messages.
20_meta_tests.cf	Meta rules made up of header and body meta tests.
20_phrases.cf	Rules for identifying popular spam phrases.
20_porn.cf	Rules for identifying words associated with porn messages.
20_ratware.cf	Rules for identifying messages sent by popular spam software.
20_uri_tests.cf	Rules applied to URIs in the message body.
50_scores.cf	Scores for the rules in the 20_* files.
50_version.cf	Ruleset version.
99_local_scores.cf	Local scores to override the scores in 50_scores.cf.
aliases.txt	Sample aliases file.
internal_ip.txt	List of IP addresses and CIDR blocks for the pass-through proxy to treat as internal systems.
optional_rules.cf	Optional rules that may not be appropriate for all sites.
quarantine_message.template	Template used for user quarantine notification messages.
pmas_config.template	Sample configuration file for PreciseMail.
pmas_confirm_msg.template	Sample template for the confirmation message generated by the PMAS Processor.
pmas_dnsbl.template	Template configuration file for the DNSBL features
pmas_process_reply.template	Sample template for the replies sent by the PMAS processor.
pmas_sophos_config.template	Sample template for Sophos AV engine configuration variables.
ptsmtplib.conf	Read-only configuration file for the pass-through proxy server.
ptsmtplib_plugins.conf	Secondary configuration file for the PTSMTPLIB controller; generated from PMAS config variables.
ptsmtplib_pmas.conf	Secondary configuration files for the pass-through proxy server.
ptsmtplib_spf.template	Sample template for PTSMTPLIB SPF configuration.
ptsmtplib_sophos.conf	Configuration file that sets debug level for Sophos plugin to Pass-through proxy server.
quarantine_message.template	Template used for user quarantine notification messages.
rdns_exceptions.template	Sample template for rDNS exceptions.
virus_replacement.template	Template for the text that replaces a virus attachment.
vmf_exceptions.template	Sample template for VMF (Verify MAIL FROM) exceptions.

**Table B–1 (Cont.) PreciseMail Anti-Spam Gateway files created during installation**

<b>File name</b>	<b>Description</b>
<b>Files in /pmas/api/userdb</b>	
example1.c	User database API example program.
example2.c	User database API example program.
example3.c	User database API example program.
example4.c	User database API example program.
example5.c	User database API example program.
example6.c	User database API example program.
makefile	Make file to build the UserDB API example programs.
userdb_api.h	User database API include file.



---

# Index

---

---

## A

---

Accessing online release notes • 1–1  
Adding SCRIPT mapping • 3–3, 4–3

---

---

## C

---

Configuring PMDF PIPE and PMAS channels • 3–1  
Configuring the PMAS channel • 4–1  
Creating an alias  
    PIPE address • 3–2  
Creating cron entries  
    Periodic jobs • 3–4, 4–3, 5–2, 6–2  
Creating PIPE option file • 3–2

---

---

## D

---

Disk and directory selection • 2–1

---

---

## F

---

Files created during installation • A–2

---

---

## I

---

Installation procedure requirements • 1–1  
Installing PreciseMail Anti-Spam Gateway • 2–1

---

---

## P

---

Pass-Through SMTP Server configuration • 6–1  
PMDF configuration for running PreciseMail Anti-Spam Gateway • 3–1  
Post-installation tasks for PMDF • 2–3  
Post-installation Tasks Proxy • 5–4

---

Post-installation Tasks Sendmail • 4–4  
Post-installation Tasks Sun Messaging Server • 3–5  
PreciseMail Anti-Spam Gateway  
    Sample installation • 7–3  
    Verifying • 3–5, 4–4, 5–3, 6–3  
Preparing to install  
    Prerequisite software • 1–1

---

---

## R

---

Recompiling PMDF configuration • 3–4  
Recompiling Sun Messaging Server configuration • 4–3

---

---

## S

---

Sample PreciseMail Anti-Spam Gateway installation • 7–3  
Sendmail configuration for running PreciseMail Anti-Spam Gateway • 5–1  
SunONE configuration for running PreciseMail Anti-Spam Gateway • 4–1

---

---

## U

---

User Interface  
    Configuring • 6–3  
        Apache Web Server • 7–1  
        SunONE Web Server • 7–2

---

---

## V

---

Verifying PreciseMail Anti-Spam Gateway is running • 3–5, 4–4, 5–3  
Verifying the pass-through proxy is running • 6–3

---

