

SOPHOS



Startup guide

Version 3.0
Notes/Domino
December 2006



This page intentionally left blank

Contents

- 1 About this guide4
- 2 System requirement5
- 3 Preparing for installation.....6
- 4 Installing PureMessage.....8
- 5 Opening PureMessage.....9
- 6 Setting up email alerts..... 10
- 7 Setting up mail scanning 11
- 8 Setting up a scheduled database scan.....13
- 9 Blocking email attachments..... 14
- 10 Adding disclaimers to email 18
- Technical support.....19

1 About this guide

This guide tells you how to:

- install PureMessage
- open PureMessage
- set up email alerts
- set up mail scanning
- set up a scheduled database scan
- block email attachments
- add disclaimers to email.

For information on all the configuration options, see the *PureMessage Notes/Domino user manual*, which is available from the **PureMessage Groupware Solutions CD** or the Sophos website.

2 System requirement

- Lotus Domino Server 6 or later.
- CD drive or internet access.
- RAM: 128 MB minimum. 256 MB recommended.
- Disk space: 250 MB minimum. 500 MB recommended. The space required depends on the log size and the number of email alerts.

3 Preparing for installation

Before installing PureMessage for Notes/Domino, you must:

- prepare Notes and Domino for installation (section 3.1)
- install and configure Sophos Anti-Virus 6 or later (section 3.2).

3.1 Prepare Notes and Domino

- Log on to the server as an administrator.
- In the Notes Name and Address Book, create a multi-purpose user group called “puremessage-admin” for the administrator(s) that you want to receive email alerts. If you already have a suitable group, you can configure PureMessage to use that instead (this is covered in section 6).
- Stop your Domino server.
- Make a backup of the Domino server. Back up the log.ntf, mailbox.ntf and statrep.ntf/statrep5.ntf files. Your own templates will be preserved during the installation.

3.2 Install and configure Sophos Anti-Virus

Sophos Anti-Virus provides virus scanning for PureMessage. If you don't already have it, you must install it. You must also configure it to exclude some directories from scanning.

1. At the computer where you run your Domino server, insert the **Sophos Groupware Solutions Install CD**. On the CD home page, click **Install PureMessage for Notes/Domino**. At the next page, click **Install Sophos Anti-Virus** and follow the instructions.

2. When Sophos Anti-Virus has been installed, configure on-access scanning so that the directories below are not scanned. These directories are used by PureMessage.

c:\temp

c:\tmp

c:\lotus notes\Puremessage

-  To configure Sophos Anti-Virus, right-click the blue shield icon in the system tray and select **Open Sophos Anti-Virus**. Then click **Configure Sophos Anti-Virus**.

You are ready to install PureMessage (section 4).

4 Installing PureMessage

❗ The computer where you install PureMessage will need to be restarted after installation.

1. At the computer where you run your Domino server, insert the **Sophos Groupware Solutions Install CD**. On the CD home page, click **Install PureMessage for Notes/Domino**. At the next page, select your version of Notes.

Alternatively, download and run the installer from the Sophos website. Visit www.sophos.com/products/es/email and follow the links for PureMessage for Notes/Domino. Select PureMessage for your version of Notes.

2. In the welcome dialog box, click **Next**.
3. In the **License agreement** dialog box, select **I accept the terms in the license agreement** if you want to continue. Click **Next**.
4. In the **Setup type** dialog box, select **Standard**.
- ❗ Select **Advanced** if you want to install PureMessage to a custom location or in a replicated environment.
5. In the **Installation settings** dialog box, check your settings. Click **Next**.
6. In the **Ready to install the program** dialog box, click **Next**. A command window opens and indicates progress.
7. When installation is complete, the **InstallShield Wizard Completed** dialog is displayed. Click **Finish**.
8. You are prompted to restart the computer.

When the computer has restarted, you are ready to open the PureMessage database (section 5).

5 Opening PureMessage

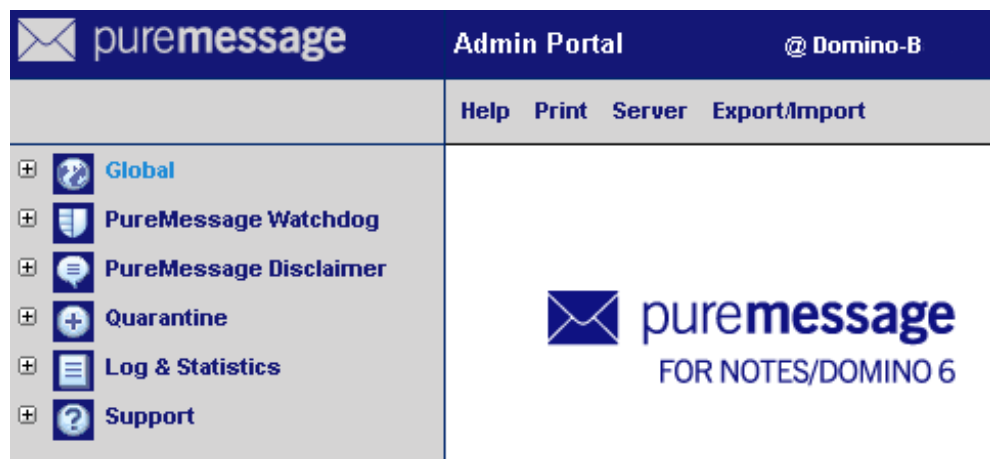
To open PureMessage for the first time:

1. Ensure you are logged on as an administrator.
2. Open your Notes client. Select **File|Database|Open**. Double-click the server where PureMessage is installed. Double-click the PureMessage data directory. Then double-click the **PureMessage Admin 3** database.
- ❗ Alternatively, open your web browser and go to <http://<myserver>/PureMessage data directory/nav.nsf>.
3. The PureMessage user interface is displayed.

The left-hand pane contains a menu that gives access to the product components, e.g. **PureMessage Watchdog** for email scanning.

The right-hand pane is used to display lists of tasks or configuration pages. A menu bar will give you options for editing, saving or printing these pages.

Now you should set up email alerts (section 6).



6 Setting up email alerts

Before you begin using PureMessage to scan email or databases, you should enable it to send email alerts to administrators when it detects viruses.

1. In the PureMessage user interface, in the left-hand pane, open the **Global** menu (click the plus sign beside it). Click **Global parameters**.
2. In the right-hand pane, a list of parameters is displayed. Double-click **PureMessage administrators (person/group)**.
3. On the menu bar, click **Edit** so that you can make changes. On the **Basics** tab, ensure that **Value(s)** is set to the name of the user group you want to send alerts to. Set the **Status** to **Active**. You will now see a **Save** option in the menu bar. Click it.



Now you are ready to set up mail scanning (section 7).

7 Setting up mail scanning

1. In the PureMessage user interface, in the left-hand pane, open the **PureMessage Watchdog** menu. Click **Mail Jobs**.
2. In the right-hand pane, a list of job templates is displayed. You create a new job by copying a template. Right-click **DEFAULT - Virus Check all Mails** and select **Copy**. Then right-click in the list again and select **Paste**.
 - ❗ Creating a copy ensures that you always keep a template on which you can base other jobs.
3. Double-click on the new job to display its settings.
4. On the menu bar, click **Edit**. On the **Basics** tab, change the **Job name** to **SOPHOS -Virus Check all Mails**. Set the **Status** to **Active**. Set **Runs on** to **All mails**. You will now see a **Save** option in the menu bar. Click it.
- ❗ On the other tabs, you can change the notifications sent or the action taken. See the *PureMessage Notes/Domino user manual*.

Help Print Previous Next Save New

'SOPHOS - Virus Check all Mails' Windows

PureMessage Watchdog Mail Job

Basics	
Job name	SOPHOS - Virus Check all Mails
Status	<input checked="" type="radio"/> Active <input type="radio"/> Not active
Priority	8000
Runs on	<input checked="" type="radio"/> All mails <input type="radio"/> Selected mails

5. After you close the mail job page, you should see **SOPHOS - Virus Check all Mails** listed under **Active** jobs.

By default, PureMessage will now:

- scan all incoming and outgoing mail
- alert the administrator and the recipient if a virus is found
- place a copy of any infected mail in quarantine, together with a report
- delete infected mail.

To check that PureMessage is working, download a harmless test file from www.eicar.org, attach it to an email and send it.

Next you can set up a scheduled scan of databases (section 8).

8 Setting up a scheduled database scan

You set up a scheduled scan of your mail databases as follows.

1. Open the **PureMessage Watchdog** menu and click **Database jobs**.
 2. In the list of jobs, find **DEFAULT - DB Virus Check** and create a copy (as described in section 7).
 3. Double-click the new job to display its settings.
 4. On the menu bar, click **Edit**. On the **Basics** tab, set the **Job name** to **SOPHOS - DB Virus Check**. Set the **Execution mode** to **Scheduled**. Set a **Start time** for the first scan and the **Interval** at which the scan will be run thereafter. Set the **Status** to **Active**. When you have finished, click **Save** on the menu bar.
- ❗ If you do not want to scan all your mail databases, you can enter database details in the database selection field.
5. In the list of scanning jobs, you should now see **SOPHOS - DB Virus Check** in the list of **Active** jobs.

By default, PureMessage will now:

- scan all mail databases
- scan new or modified items only
- alert the administrator and the recipient if a virus is found in a mail database
- place a copy of any infected mail in quarantine, together with a report
- delete infected mail.

Now you can (if you wish) block email attachments (section 9) or add disclaimers to your email (section 10).

9 Blocking email attachments

You can block some or all email attachments. To do this, you

- set up a new mail scanning job for attachment blocking
- set up a file restrictions rule and attach it to the attachment blocking job.

9.1 Set up an attachment blocking job

1. Open the **PureMessage Watchdog** menu and click **Mail Jobs**.
2. In the list of jobs, find the **SAMPLE - Denied Attachments all users** job and create a copy (as described in section 7).
3. Double-click the new job to display its settings.
4. In the menu bar, click **Edit**. On the **Basics** tab, set the **Job name** to **SOPHOS - Denied Attachments all users**. Set the **Status** to **Active**. Set **Runs on** to **Selected mails**.

- ❗ The **Selected mails** setting ensures that PureMessage does not take action against emails released from quarantine and emails to and from the administrator.

The screenshot shows the configuration window for a mail job. At the top, there is a menu bar with 'Help', 'Print', 'Previous', 'Next', 'Save', and 'New'. Below the menu bar, the window title is "'SOPHOS - Denied Attachments all users' vWindows' PureMessage Watchdog Mail Job'. There are five tabs: 'Basics', 'Operations', 'Advanced', 'Misc.', and 'Comments'. The 'Basics' tab is selected. The configuration fields are as follows:

Job name	「SOPHOS - Denied Attachments all users」
Status	<input checked="" type="radio"/> Active <input type="radio"/> Not active
Priority	「5000」
Runs on	<input type="radio"/> All mails <input checked="" type="radio"/> Selected mails

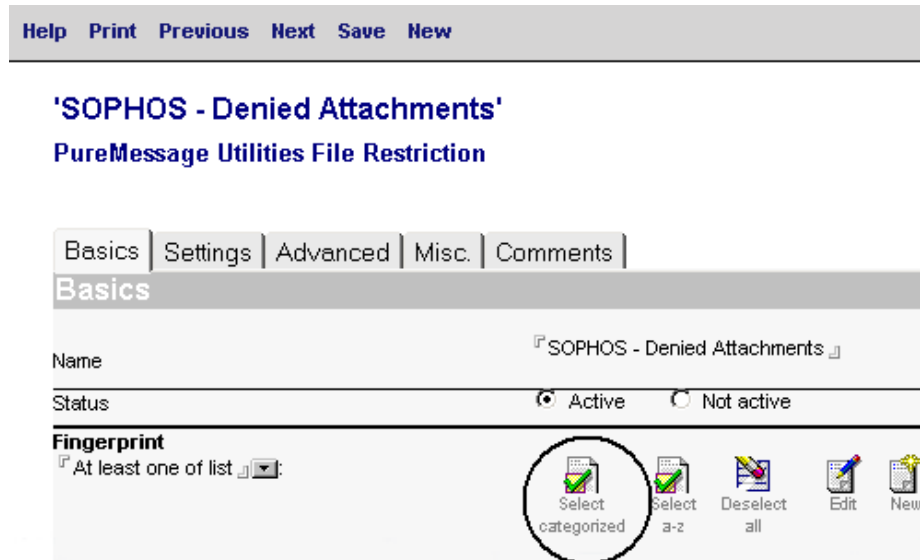
- Click the **Operations** tab. In the further set of tabbed pages displayed, select the **Denied Attachments** tab. Set **Use file restrictions** to **Yes**. Then specify whether you want to **Perform general modify option** (by default, this removes attachments) and whether you want to send notifications to the administrator, recipient and sender. Click **Save** on the menu bar. Now set up a file restriction rule (section 9.2).

The screenshot shows the configuration window for a mail job named "'SOPHOS - Denied Attachments all users'". The window has a menu bar with 'Help', 'Print', 'Previous', 'Next', 'Save', and 'New'. Below the menu bar, the title bar reads 'PureMessage Watchdog Mail Job'. The main area contains several tabs: 'Basics', 'Operations', 'Advanced', 'Misc.', and 'Comments'. The 'Operations' tab is selected and contains a 'General modify option' section with a dropdown menu set to 'Remove affected attachments'. Below this, there are more tabs: 'No Alert', 'Virus', 'Denied Attachments', 'Encryption', and 'Password Protection'. The 'Denied Attachments' tab is selected and contains three settings: 'Use file restrictions' (radio buttons for 'Yes' and 'No', with 'Yes' selected), 'Perform general modify option (Delete mail)' (radio buttons for 'Yes' and 'No', with 'No' selected), and 'Category in Quarantine report' (a dropdown menu set to 'Denied Attachments').

9.2 Set up a file restriction rule

- Open the **PureMessage Watchdog** menu and click **Utilities** and then **File Restrictions**.
- A list of file restriction rules is displayed. Find **SAMPLE - Denied Attachments** and create a copy.
- Double-click the new file restriction rule to display its settings.

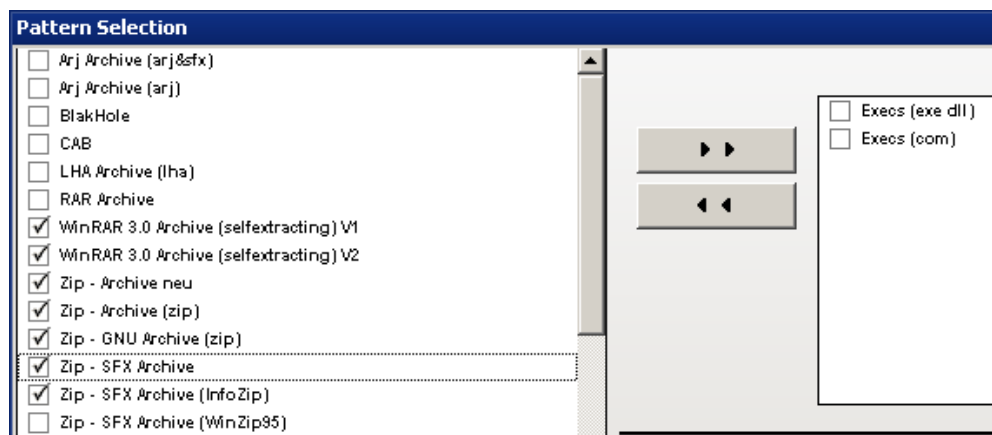
- On the menu bar, click **Edit**. On the **Basics** tab, set the **Job name** to **SOPHOS - Denied Attachments**. Click **Select Categorised** to specify the types of attachment that will be blocked.



- In the **Pattern Selection** dialog box, a list of attachment types is displayed.

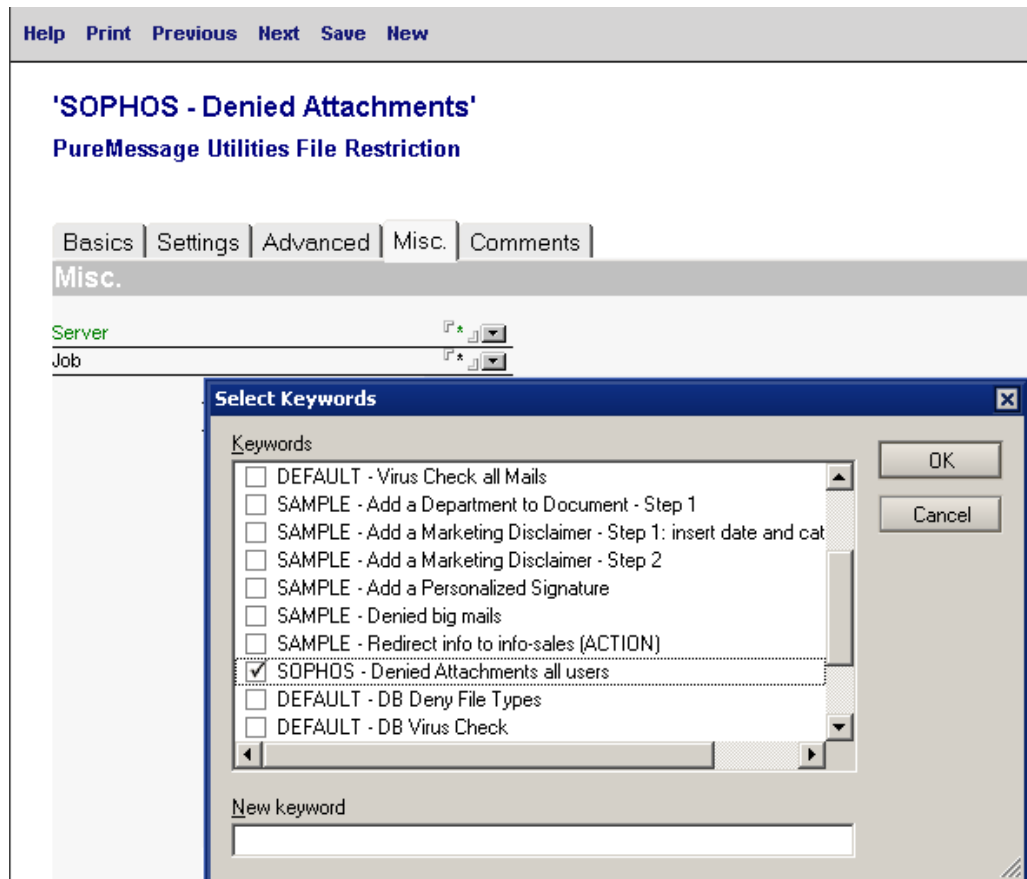
To block an attachment, select it (tick its checkbox) and click the arrow button to add it to the list on the upper right-hand side.

If you have blocked an attachment type, e.g. MS Office, but you want to allow a certain sub-type, e.g. MS Word, add it to the list of exceptions on the lower right-hand side (not shown in the screenshot below). Click **OK** to return to the **Basics** tab.



- On the **Basics** tab, set the **Status** to **Active**.

- Click the **Misc.** tab. The **Job** field shows which scanning jobs the file restriction rule is applied to. By default the field shows an asterisk, which indicates “all jobs”. To change this, click **Job**. In the **Select keywords** dialog, in the list of jobs, clear the checkbox beside * (asterisk). Select the checkbox next to **SOPHOS - Denied Attachments all users**. Click **OK**.



- On the menu bar, click **Save**.

You have set up attachment blocking. Now you can add disclaimers to your email (section 10).

10 Adding disclaimers to email

You can configure PureMessage to add disclaimers or signatures to your email.

1. Click **PureMessage Disclaimer**.
2. In the list of jobs, find the disclaimer type you want, for example **DEFAULT - Add a Legal Disclaimer**, and create a copy.
3. Double-click the new job to display its settings.
4. On the menu bar, click **Edit**. On the **Basics** tab, set the **Job name** to (for example) **SOPHOS - Add a Legal Disclaimer**.
5. Click the **Operations** tab and edit the **Trailer** text (at the bottom of the tab) to meet your needs.
6. Click the **Basics** tab and set the **Status** to **Active**. Finally, on the menu bar, click **Save**.

Technical support

For technical support, visit www.sophos.com/support.

If you contact technical support, provide as much information as possible, including the following:

- Sophos software version number(s)
- Operating system(s) and patch level(s)
- The exact text of any error messages

Copyright 2006 Sophos Group. All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording or otherwise unless you are either a valid licensee where the documentation can be reproduced in accordance with the licence terms or you otherwise have the prior permission in writing of the copyright owner.

Sophos and Sophos Anti-Virus are registered trademarks of Sophos plc and Sophos Group. All other product and company names mentioned are trademarks or registered trademarks of their respective owners.