SOPHOS

simple + secure

PureMessage for Microsoft Exchange 2013

startup guide

Product version: 4.0
Document date: July 2013

Contents

1 About this guide

This guide tells you how to do the following:

- install PureMessage 4.0 for Microsoft Exchange 2013
- start PureMessage
- integrate PureMessage with Active Directory
- set up alerts
- ensure that anti-virus scanning is enabled
- block file types that may contain threats
- set up spam blocking (if your license permits)
- set up Exchange store scanning
- deal with quarantined items
- enable end-users to access and deal with quarantined items
- monitor system activity

2 Planning your PureMessage deployment

You can deploy PureMessage to a single or multiple Exchange servers, as described below.

2.1 Deploying PureMessage to a single Exchange server

If your network has only one Exchange server, deploying PureMessage is straightforward: install PureMessage on the Exchange server and configure it according to your email security policy.

2.2 Deploying PureMessage to multiple Exchange servers

PureMessage can protect both front-end (hub transport) servers and back-end (mailbox) servers.

At the time of this release, the Edge Transport server role is not available in Microsoft Exchange Server 2013. However, if you don't want to expose your Mailbox servers directly to the internet, you can continue to use an existing or install a new Exchange Server 2007 or Exchange Server 2010 Edge Transport server in your perimeter network. For more information, see *Use an Edge Transport Server in Exchange 2013*.

Note: In such hybrid environments, it is recommended that you perform anti-spam scanning on the edge server to filter spam, and install the anti-virus only version of PureMessage on your back-end servers that do not require anti-spam scanning.

Example: Exchange 2007 or 2010 Edge Transport server and Exchange 2013 Mailbox server

This example illustrates how PureMessage can be installed on several Exchange servers with dedicated roles.

Note: Install the appropriate version of PureMessage on each server. For PureMessage system requirements, see *http://www.sophos.com/en-us/support/knowledgebase/118640.aspx*

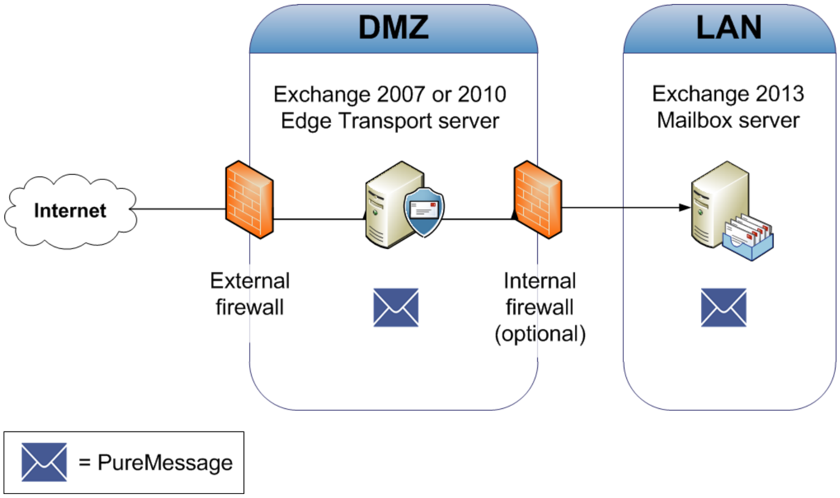


Figure 1: Exchange 2007 or 2010 Edge Transport server and Exchange 2013 Mailbox server

3 Installing PureMessage

This section describes how to install PureMessage.

Note: If you are installing PureMessage to an Exchange cluster, check the system requirements and then go to *Appendix A: Deploying PureMessage to Exchange clusters* (section 13).

The PureMessage product consists of two components:

- The PureMessage service.
- The PureMessage administration console.

This section tells you how to install both on a single server and also how to install a separate administration console in order to manage remote PureMessage servers.

Installation involves the following steps:

- Checking the system requirements.
- Preparing for installation.
- Preconfiguring updates (Sophos Enterprise Console customers only).
- Installing PureMessage.
- Installing a PureMessage console on a separate computer (optional).

3.1 System requirements

PureMessage 4.0 can be installed on Microsoft Exchange Server 2013. The minimum requirement for the database is Microsoft SQL Server 2008.

For a full list of PureMessage system requirements, see *http://www.sophos.com/en-us/support/knowledgebase/118640.aspx*

3.2 Preparing for installation

Note:

- If you are running Windows 2008 or Windows 2008 R2 Server, read *http://www.sophos.com/support/knowledgebase/article/109664.html* before installing PureMessage.

Before you begin installation, you should do the following:

- Read the *PureMessage for Microsoft Exchange release notes* for details of new features and known issues. The release notes are published at *http://www.sophos.com/en-us/support/documentation/puremessage-for-microsoft-exchange.aspx*.
- Make sure that a backup has been made of the mailboxes and databases.

- Make sure that the Exchange Autodiscover service is configured correctly. The service is used by PureMessage during scanning of Exchange stores. For more information, see *http://www.sophos.com/en-us/support/knowledgebase/119506.aspx*.
- PureMessage installation may require a restart, so schedule the installation for a time when restarting the server will cause the least inconvenience.

If you want to use spam blocking:

- Make sure that you have a valid anti-spam license and download credentials from Sophos so that you can download anti-spam updates.
- Make sure that PureMessage is installed on a computer with Internet access, as anti-spam updates are only available direct from Sophos.
- If you use Sophos Enterprise Console to protect your PureMessage server, make sure that the server is configured to download anti-spam updates directly from Sophos as described in *Preconfiguring updates* (section 3.3).

If you are installing PureMessage on multiple servers, make sure that your SQL server is set up for remote access. See the *PureMessage for Microsoft Exchange release notes* for further details.

3.3 Preconfiguring updates

If you use PureMessage for spam blocking, it needs to update regularly with the latest rules for detecting spam. These spam rules can only be downloaded directly from Sophos via the internet.

If you are going to install PureMessage on a computer that does not already have Sophos Anti-Virus installed, updating will be set up for you and you need take no further action. Go to *Installing PureMessage* (section 3.4).

If you are going to install PureMessage on a computer already running Sophos Anti-Virus and managed by Sophos Enterprise Console, you must follow the instructions below.

Note: You will need the username and password that you use for downloads from the Sophos website.

1. Go to the computer running Enterprise Console and start Enterprise Console.
2. Ensure that the computer(s) running PureMessage are in a group of their own or have their own policy setting.
3. Create an Updating policy (or edit the existing policy) for the group.
4. In the **Updating Policy** dialog box, click the **Secondary server** tab.
5. In the **Secondary server** dialog box, select **Specify secondary server details**. Then in the **Address** field, click the drop-down arrow and select **Sophos**. Enter your username and password.
6. If necessary, enter proxy details.

You have preconfigured updating and are ready to install PureMessage.

3.4 Installing PureMessage

To install PureMessage, do as follows:

Note: The following services (and any dependent services) may be stopped and started during the installation of PureMessage:

- Internet Information Services (IIS)
- Microsoft Exchange Transport service
- Microsoft Exchange Frontend Transport service
- Microsoft Exchange Information Store service
- Distributed File System Replication (DFSR) service

1. Log on to the server as an administrator, based on your environment:
   - If you are in a domain, log on with domain administrative privileges.
   - If you are in a workgroup, log on with local administrative privileges.

   Note: Make sure you are a member of the Exchange Organization Management group.
2. Visit the Sophos product download page at *http://www.sophos.com/support/updates/*. You will need credentials to download products and documentation.
3. Browse to the PureMessage page and download the PureMessage for Microsoft Exchange installer package you require. Choose **Anti-virus and anti-spam** or **Anti-virus only** (as your license permits).
4. Using Windows Explorer, browse to your download folder and start the installer package. The installation wizard begins.

   Note: Ensure that the installer is not run from a network share.
5. In the **Welcome** dialog box, click **Next**.
6. In the **License Agreement** dialog box, read the agreement. If you agree with the terms, click **I accept the terms of the license agreement** and click **Next**.
7. In the **Select Features** dialog box, select the components you want to install and click **Next**.
8. In the **Choose Destination Location** dialog box, you see the default folder where PureMessage will be installed. If you want to install it in a different folder, click **Browse** and select a folder. Click **Next**.
9. In the **Sophos Download Credentials** dialog box, enter the **User name** and **Password** that were supplied by Sophos.

   If you access the internet via a proxy, click **Proxy Details** and enter your proxy settings. Otherwise, click **Next**.

10. In the **PureMessage Database settings** dialog box, specify the database (SQL Server) where PureMessage will store reporting data, central quarantine, and policy configuration information. Click **Next**.

    PureMessage will automatically detect any local SQL database instances. If a local database instance is detected, you choose it by selecting the **Local** option. If no database is detected and **Local** is chosen, then PureMessage will install a local instance of SQL Server Express. To use a database instance located on a different computer, choose the **Remote** option. The database **Browse** dialog displays only SQL Server instances with the current domain.

    Important: If a SQL Server instance has previously been used by an earlier version of PureMessage, you cannot use it for this version of PureMessage because this version doesn't support upgrading from earlier versions. Create a new SQL Server instance for this installation.

    Note: For information on how to configure database mirroring, see *Appendix F: Database Mirroring* (section 18).

11. In the **PureMessage Service Credentials** dialog box, click **Create** and enter a password and confirm it to create a SophosPureMessage user. If the user account already exists, you will be prompted to enter its password. This account is used by Sophos PureMessage services. Click **Next**.
12. In the **PureMessage Configuration Group** dialog box, select a group you want to join or create a new group. Click **Next**.

    PureMessage installations can be grouped together to share the same policy configuration and be managed from a single management console. For more information, see *PureMessage Configuration Group* (section 3.6).

13. If you are installing PureMessage on an Exchange server that is configured as a mailbox-only role, the **PureMessage Mailbox Role Settings** dialog box is displayed. Select the Exchange transport server which PureMessage should use to send alert email messages. Click **Next**.
14. In the **PureMessage Administration Settings** dialog box, enter an Administrator email address. PureMessage will send alerts to this email address. You can change this address later too. Click **Next**.

    Note: PureMessage creates a security group in Active Directory called Sophos PureMessage Administrators, which includes all PureMessage administrators. By default, the current user will be added to this group.

15. In the **PureMessage Routing settings** dialog box, do as follows.

    a) Enter your company's email domain(s), such as mycompany.com, in the top panel.

       Note: You need not specify sub-domains. When you specify a domain, the sub-domains are included automatically.

    b) Enter the IP addresses of any trusted email relays, such as your ISP's SMTP server and any email gateway server or appliance upstream of your Exchange servers. Click **Next**.

    Note: PureMessage uses the upstream relays configuration to determine mail direction. Not configuring an upstream relay can cause PureMessage to classify mail from upstream relays as internal, and hence skip spam scanning for those messages. For information on configuring upstream (trusted) relays, see *Appendix B: How to configure upstream (trusted) relays* (section 14).

16. In the **Company Information** dialog box you can enter details relating to the size, location, and market sector of your company or organization. This valuable feedback helps SophosLabs analyse email security trends. Click **Next**.
17. In the **Start Copying Files** dialog box, ensure the settings are correct. If they are not, use the back button to return to previous dialog boxes and change the settings. When they are correct, click **Next**.
18. PureMessage displays the installation progress and installs Sophos Anti-Virus and Sophos AutoUpdate (if not already installed). Sophos AutoUpdate automatically downloads updates to virus data and anti-spam rules.

    Note: In certain circumstances the installation may require you to restart the server. The installation will continue after restarting.

19. When installation is complete, the InstallShield Wizard Complete dialog box is displayed. Click **Finish**.

If you also want to install a separate PureMessage administration console, see *Installing a PureMessage console on a separate computer* (section 3.5).

Note: If you have Microsoft Exchange server installed on your network, you may need to disable or exclude files from scanning. For more information see the Sophos support knowledgebase article *http://www.sophos.com/support/knowledgebase/article/40065.html*.

To start using PureMessage, see *Getting started with PureMessage* (section 4.1).

3.5 Installing a PureMessage console on a separate computer

The PureMessage administration console can be installed on a computer without the PureMessage service in order to manage remote PureMessage services.

To install PureMessage console onto a separate computer:

1. On the computer where you want to install the console, start the PureMessage installer.
2. In the **Welcome** dialog box, click **Next**.
3. In the **License Agreement** dialog box, click **I accept** if you agree to the terms.
4. In the **Select Features** dialog box, clear the **PureMessage Service** check box and leave the **Administration Console** check box selected. Click **Next**.
5. In the **Choose Destination Location** dialog box, select your preferred destination folder, and click **Next**.
6. When installing in a Workgroup, the **PureMessage Service Credentials** dialog box will appear. Click **Create** and enter a password and confirm it to create a SophosPureMessage user. If the user account already exists, you will be prompted to enter its password. This account is used to connect to Sophos PureMessage services. Click **Next**.

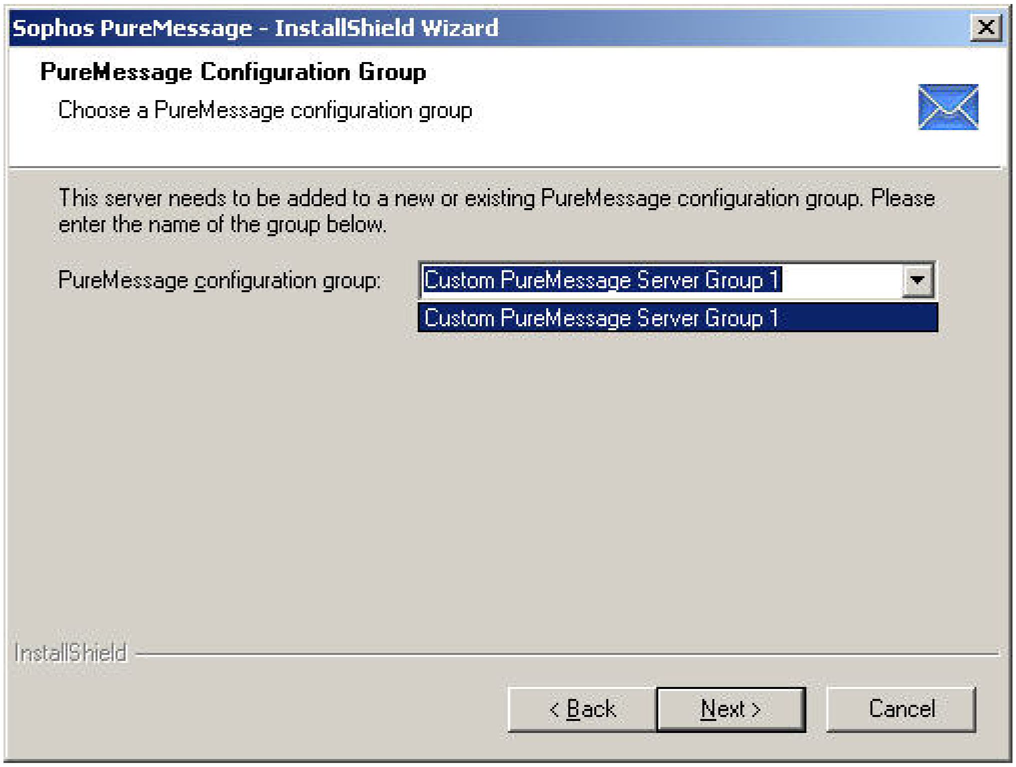
7. In the **Start Copying Files** dialog box, click **Next**.
8. When installation is complete, the **InstallShield Wizard Complete** dialog box is displayed. Click **Finish**.
9. Double-click the PureMessage icon on your desktop to start the PureMessage administration console.

In certain circumstances the installation may require you to restart the server. The installation will continue after restarting.

3.6 PureMessage Configuration Group

If several PureMessage servers are required to implement the same policy then they should be installed to the same PureMessage group. This is achieved by selecting the same database and PureMessage group name during installation.

Once the first PureMessage server has been installed in a group, the group name becomes available from the **PureMessage Configuration Group** dialog box so that additional servers can be easily installed to the same group:



Sophos PureMessage - InstallShield Wizard

PureMessage Configuration Group

Choose a PureMessage configuration group

This server needs to be added to a new or existing PureMessage configuration group. Please enter the name of the group below.

PureMessage configuration group: Custom PureMessage Server Group 1

Custom PureMessage Server Group 1

All PureMessage servers in a group should be in the same Windows domain or Workgroup. If your Exchange 2007/2010 Edge servers are in a separate Workgroup then they should be managed separately.

For more information on installing PureMessage to an Exchange cluster, see *Appendix A: Deploying PureMessage to Exchange clusters* (section 13).

4 Starting and configuring PureMessage

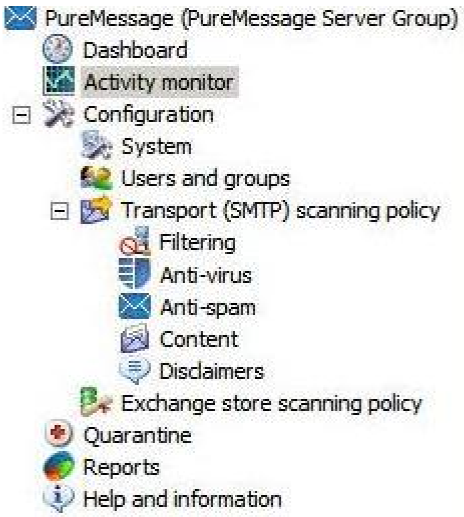
This section tells you how to:

- Start PureMessage
- Configure PureMessage to acknowledge your mail domain and upstream trusted email relay (if not done during installation)
- Connect to your directory server.

4.1 Getting started with PureMessage

To start PureMessage, do as follows:

1. Double-click the **PureMessage** icon on your desktop.
2. In the PureMessage console, the left-hand pane (console tree) gives you access to the features you can configure. The right-hand pane (details) displays information or configuration options.



If you set up a mail domain and upstream email relay during installation, see *Connect to Active Directory* (section 4.3).

If you have not yet set up a mail domain, see *Set up a mail domain and upstream trusted relay* (section 4.2).

4.2 Set up a mail domain and upstream trusted relay

For PureMessage to determine inbound, outbound and internal mail correctly, you should configure your mail domains and any upstream (trusted) relays.

For information on configuring upstream (trusted) relays, see *Appendix B: How to configure upstream (trusted) relays* (section 14).

1. In the console tree, click **Configuration | System** and then click **Routing**.
2. In the **Routing** dialog box, do as follows:

   a) Click **Add**, and enter an address in the **Mail domains** panel, such as mycompany.com.

   Note: You need not specify sub-domains. When you specify a domain, the sub-domains are included automatically.

   b) To add an upstream trusted relay, click **Upstream (trusted) relays**.

3. In the **Upstream (trusted) relays** dialog box, click **Add** to specify an upstream trusted relay address or range of addresses.
4. In the **Specify Host IP Addresses** dialog box, enter a single IP address or a range of addresses. You can also enter a comment for administrative use and click **OK**.
5. In the **Upstream (trusted) relays** dialog box, click **OK** to save your relay(s).
6. In the **Manage changes** menu, click **Save changes**.

PureMessage now recognizes your specified mail domains and upstream (trusted) relays.

Now connect to Active Directory. See *Connect to Active Directory* (section 4.3).

4.3 Connect to Active Directory

You can configure PureMessage to integrate with Microsoft Active Directory. You can then use recipient validation features and create message policies based on users and groups already configured in the directory server. If you do not need to use these features, skip this section.

Note: To configure directory server settings when using ADAM/AD LDS, see the *PureMessage for Microsoft Exchange user manual.*

1. In the console tree, click **Configuration | Users and groups** and click **Active Directory**.
2. In the **Active Directory** dialog box, click **Detect Active Directory**. The directory server settings should be filled in automatically. If not, you may need to fill in the directory server settings manually.
3. Enter the user name and password in the Logon Credentials pane if you are synchronizing with an instance of ADAM/AD LDS or if you are synchronizing with the Active Directory Global Catalog Server. Otherwise, PureMessage will log on using the SophosPureMessage service account.
4. Click **Verify settings**. PureMessage will attempt to log on to your directory server.

5. Ensure the **Synchronize with Active Directory checkbox** is checked. You can then configure PureMessage to synchronize with Active Directory (refresh its local copy) automatically or periodically.

   PureMessage keeps a local copy (cache) of the users and groups from Active Directory for performance reasons.

6. Click **Synchronize now** to start the synchronization process instantly.

If you have selected **Automatic synchronization** and if a change is made to an entity in Active Directory, it may take about 15 minutes for the change to reflect in PureMessage.

Before you can set up your transport (SMTP) and Exchange store configuration, you need to set up alerts. See *Setting up alerts* (section 5).

5 Setting up alerts

In order to receive PureMessage administrator alerts, you must configure this feature. You can also set up a template for alerts.

5.1 Setting up an address for alerts

1. In the console tree, click **Configuration | System** and then click **Alert configuration**.
2. In the **Email addresses** tab of the **Alert configuration** dialog box, click **Add**. Enter the administrator's email address in the **Send administrator alerts to** panel.
3. Enter an email address in the **Sender email address** panel. The email address will be used for sending out alerts and other PureMessage-generated messages.
4. Click **OK** to save your changes.

5.2 Setting up a template for email alerts

The default email template for alerts is sufficient for some users' needs. However, you can customize the template as described below.

1. In the console tree, click **Configuration | System | Alert configuration** and then click the **Alert template** tab.
2. In the **Alert subject** panel, enter the subject line of the alert. Right-click in the edit panel to view available substitution symbols.

   Substitution symbols can insert variables such as date or other information specific to the message.

3. In the **Alert body text** panel, create the main body of your alert. Right-click within the text field to view substitution symbols.
4. In the **Text for each incident** panel, enter any unique per-incident text you want to display.
5. In the **Alert Templates** tab, click **OK**.
6. In the **Manage changes** menu, click **Save changes**.

PureMessage alerting is now configured.

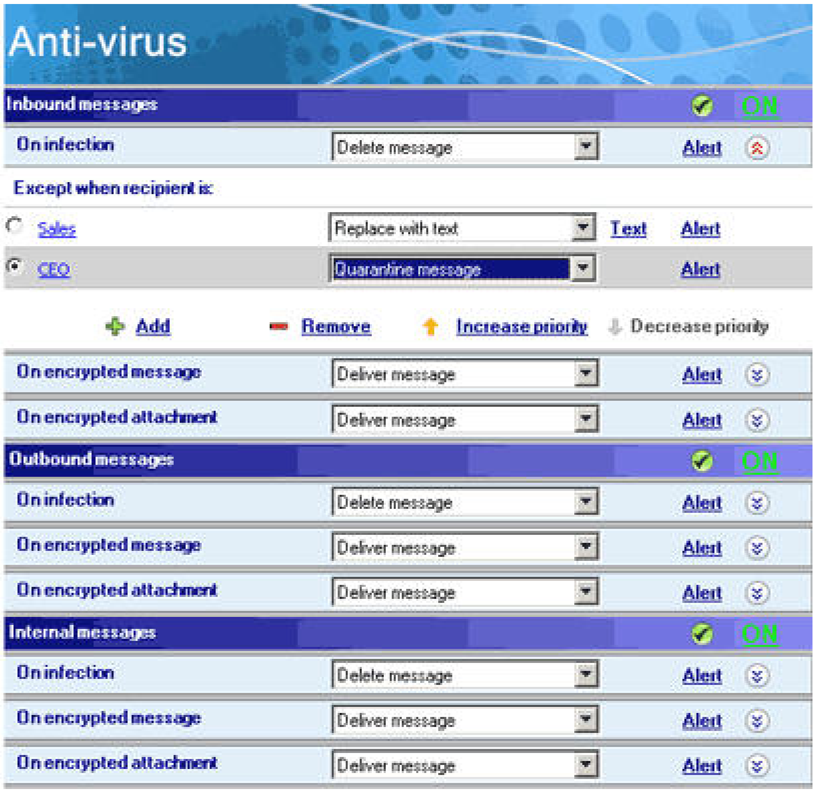
Now see *Ensuring anti-virus scanning is enabled* (section 6).

6 Ensuring anti-virus scanning is enabled

By default, anti-virus scanning is enabled for inbound, outbound, and internal mail.

To check that anti-virus scanning is enabled, follow these steps:

1. In the console tree, click **Configuration | Transport** (**SMTP**) **scanning policy** and then click **Anti-virus**.
2. In the **Anti-virus** screen, ensure that the scanning status icons in the inbound, outbound, and internal message title bars are Green, and display **ON**.



Anti-virus

Inbound messages			✓	ON
On infection	Delete message		Alert	
Except when recipient is:				
○ Sales	Replace with text	Text	Alert	
● CEO	Quarantine message		Alert	
Add	Remove	Increase priority	Decrease priority	
On encrypted message	Deliver message		Alert	
On encrypted attachment	Deliver message		Alert	
Outbound messages			✓	ON
On infection	Delete message		Alert	
On encrypted message	Deliver message		Alert	
On encrypted attachment	Deliver message		Alert	
Internal messages			✓	ON
On infection	Delete message		Alert	
On encrypted message	Deliver message		Alert	
On encrypted attachment	Deliver message		Alert	

Note: You can define separate policies for each direction of mail, and you can define specific policies for exempt users and groups. For more information, see the *PureMessage for Microsoft Exchange user manual*.

PureMessage now protects against viral threats.

Next, see *Blocking files which may contain threats* (section 7).

7 Blocking files which may contain threats

Sophos recommends that you block inbound email attachments that are most likely to contain threats.

The **On suspicious attachment policy** rule is preconfigured to block file types that are commonly used to transport email threats, such as executable files (.exe, .scr, .com, .pif, etc). By default this rule is turned off.

1. In the console tree, click **Configuration | Transport (SMTP) scanning policy** and then click **Content**.
2. In the **Content filtering** screen, ensure the status icon for inbound mail title bar is Green and displays **ON**.
3. Select the **On suspicious attachment** checkbox. Click **Define** to view and edit file types predefined by Sophos as suspicious attachments.
4. In the **Inbound messages - Suspicious attachment type** dialog box, click the **Attachment types** tab.
5. In the **Attachment types** tab, the attachment types in the **Executable** and **Object Code** groups are selected by default. On the **Attachment names** tab the **Block multiple extensions** option is selected by default.
6. Check the **Block potentially unwanted applications (PUAs) except** checkbox.
7. If you wish to allow users access to otherwise blocked applications, click **Add** to enter a PUA that you want to allow. PUA names can be found at *http://www.sophos.com/security/analyses/*.
8. Click **OK** to save your changes and return to the **Content filtering** pane.
9. In the **Content filtering** dialog box, under the **Inbound messages** bar, in the **On suspicious attachment** panel, select **Quarantine message** from the drop-down menu.
10. Under the **Inbound messages** bar, in the **On suspicious attachment** panel, click **Alert**.
11. In the **Alert configuration** dialog box, check one or more checkboxes to specify who will be notified in the event of PureMessage quarantining a suspicious attachment. Click **OK** to save your changes and return to the **Content filtering** pane.
12. In the **Manage changes** menu, click **Save changes**.

    Note: For information on configuring the content settings of your policy, see the *PureMessage for Microsoft Exchange user manual.*

PureMessage now

- blocks and quarantines inbound messages with suspicious attachments.
- sends alerts to those you specified.

Now you can enable spam blocking, scan the Exchange message store, and tell users about quarantined mail. These functions are described in the sections that follow.

8 Blocking spam

You can configure PureMessage to deal with spam (unwanted incoming email). A typical anti-spam setting would be to delete spam and quarantine suspected spam.

1. In the console tree, click **Configuration | Transport (SMTP) scanning policy** and then **Anti-spam**.
2. In the **Anti-spam** screen, in the **Inbound messages** bar, ensure the ON/OFF icon displays **ON**. If it displays **OFF**, click the icon to turn it on.
3. In the **On-spam** panel, select **Delete message** (or your preferred setting) from the drop-down menu.
4. In the **On suspected spam** panel, select **Quarantine message** (or your preferred setting) from the drop-down menu.
5. In the **Manage changes** menu, click **Save changes**.

Next you specify which mails you will categorise as spam and suspected spam by setting the spam ratings for PureMessage.

8.1 Change anti-spam settings

PureMessage gives each email a spam rating. The higher the rating, the more likely the email is to be spam. PureMessage uses this rating to decide whether the email should be treated as spam or suspected spam.

1. In the console tree, click **Configuration | Transport (SMTP) scanning policy | Anti-spam** and then **Change anti-spam settings**.
2. In the **Anti-spam settings** dialog box, use the slider controls to adjust the threshold, above which PureMessage regards an email as spam or suspected spam.

   Note: Sophos recommends you set your ratings above 50 to avoid legitimate mail being classed as spam or suspected spam.

3. Ensure the **Check reputation of message relays against external DNS block lists** checkbox is checked. Enabling this option will check incoming messages against the IP addresses of known spam sources and will filter out any messages coming from these IP addresses.
4. In the **Anti-spam settings** dialog box, you can check the **Check reputation of first external relay only** checkbox only after configuring upstream (trusted) relays correctly. This option will only check the first external relay, for more deterministic spam scoring.
5. If you want to add the spam score as a SCL rating, check the **Add spam score to message as Microsoft Spam Confidence Level (SCL) rating** checkbox. Messages delivered to end users with a SCL rating higher than a particular value are diverted into the user's Junk mail folder in Microsoft Outlook. Click **OK** to save your changes.
6. In the **Manage changes** menu, click **Save changes**.

For optimal spam detection, ensure PureMessage has up-to-date information regarding the addresses of any upstream (trusted) relays. For more information on configuring the anti-spam settings of your policy, see the *PureMessage for Microsoft Exchange user manual*.

9 Scanning Exchange Message Stores

You can configure PureMessage to run background scans of both private and public Exchange stores. Background scanning is done continuously at off-peak times.

For more information, see *Exchange Store scanning* (section 16.2).

Note: On-access and proactive scanning options are not supported on Exchange Server 2013.

9.1 Enable store scanning and alerts

1. In the console tree, click **Configuration | Exchange store scanning policy**.
2. In the **Anti-virus** dialog box, in the **Exchange store scanning** panel, ensure the ON/OFF icon displays **ON**. If it displays **OFF**, click the icon to turn it on.
3. In the **On infection** panel, select "Replace attachment with text" from the drop down menu. The **Text** button appears. If you click the **Text** button, you can edit the text shown when PureMessage replaces an infected attachment.
4. In the **On infection** panel, click **Alert**.
5. In the **Alert configuration** dialog box, ensure the **Administrator** checkbox is checked and click **OK** to save your changes and return to the **Anti-virus** (**Exchange store scanning**) pane.
6. In the **Manage changes** menu, click **Save changes**.

PureMessage now

- scans the Exchange information store for viruses, and replaces the attachment with the configured text.
- sends an alert to the Administrator.

Now configure scanning of Exchange stores.

9.2 Configure scanning of Exchange stores

Note: The Exchange Store is made up of both public and private stores.

- A public store is a database that is accessible to multiple users.
- A private store (example, a mailbox) is usually only accessible to a single user.

You can configure PureMessage to run background scans at scheduled times on both the private and public stores.

1. In the console tree, click **Configuration | Exchange store scanning policy** and then click **Change exchange store scan settings**.

2. In the **Exchange store scan settings** dialog box, on the **Exchange 2013** tab, select the **Enable background scanning** check box in the **Exchange private store** panel, **Exchange public store** panel, or both.

   Note: On-access and proactive scanning options are not supported on Exchange Server 2013.

3. If you want background scanning to be enabled only outside office hours, select the **Enable background scanning only for out of working hours** check box, and select your working days and times.
4. Click **OK** to save your changes.
5. In the **Manage Changes** menu, click **Save changes**.

PureMessage now scans items as configured by your settings.

10 Dealing with quarantined items

Depending on your configuration, PureMessage can quarantine mail that:

- is infected.
- is spam, or suspected spam.
- is encrypted, or has an encrypted attachment.
- has a suspicious or unwanted attachment.
- contains a blocked phrase or offensive language.
- is unscannable, or creates a scanning error.

Quarantined messages are isolated in a secured format in a central location on disk. Administrators can deal with these messages in a number of ways, such as disinfect, delete, or deliver them.

You can also enable users to access a spam quarantine website, where they can review and deal with their quarantined spam messages.

This section tells you how to:

- do quarantine database housekeeping.
- deal with quarantined messages.
- enable end-users to access the spam quarantine website.
- set up digests to tell users about spam and suspected spam.

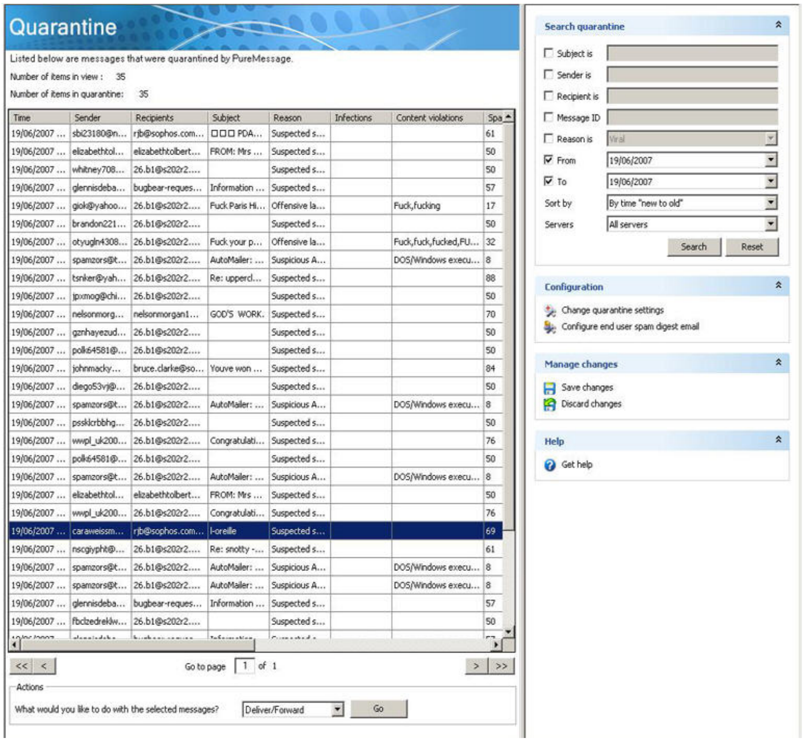
10.1 Quarantine housekeeping

You can specify the number of days to keep quarantined mail before deleting it.

1. In the console tree, click **Quarantine**.
2. In the **Configuration** menu, click **Change quarantine settings**.
3. In the **Quarantine settings** dialog box, specify the number of days you want to keep quarantined mail before deleting it in the **Number of days to keep mails in quarantine before deletion** box.
4. Click **OK** to save your settings, and return to the **Quarantine** pane.
5. In the **Manage Changes** menu, click **Save changes**.

10.2 Dealing with quarantined messages

1. In the console tree, click **Quarantine**.



Quarantine

Listed below are messages that were quarantined by PureMessage.

Number of items in view : 35

Number of items in quarantine: 35

Time	Sender	Recipients	Subject	Reason	Infections	Content violations	Spa
19/06/2007 ...	sbi23180@n...	rjb@sophos.com...	□□□ PDA...	Suspected s...			61
19/06/2007 ...	elizabethtol...	elizabethtolbert...	FROM: Mrs ...	Suspected s...			50
19/06/2007 ...	whitney708...	26.b1@s202r2....		Suspected s...			50
19/06/2007 ...	glennisdeba...	bugbear-reques...	Information ...	Suspected s...			57
19/06/2007 ...	giok@yahoo...	26.b1@s202r2....	Fuck Paris Hi...	Offensive la...		Fuck,fucking	17
19/06/2007 ...	brandon221...	26.b1@s202r2....		Suspected s...			50
19/06/2007 ...	otyugln4308...	26.b1@s202r2....	Fuck your p...	Offensive la...		Fuck,fuck,fucked,FU...	32
19/06/2007 ...	spamzors@t...	26.b1@s202r2....	AutoMailer: ...	Suspicious A...		DOS/Windows execu...	8
19/06/2007 ...	tsnker@yah...	26.b1@s202r2....	Re: upperd...	Suspected s...			88
19/06/2007 ...	jpxmog@chi...	26.b1@s202r2....		Suspected s...			50
19/06/2007 ...	nelsonmorg...	nelsonmorgan1...	GOD'S WORK.	Suspected s...			70
19/06/2007 ...	gznhayezud...	26.b1@s202r2....		Suspected s...			50
19/06/2007 ...	polk64581@...	26.b1@s202r2....		Suspected s...			50
19/06/2007 ...	johnmacky...	bruce.clarke@so...	Youve won ...	Suspected s...			84
19/06/2007 ...	diego53vj@...	26.b1@s202r2....		Suspected s...			50
19/06/2007 ...	spamzors@t...	26.b1@s202r2....	AutoMailer: ...	Suspicious A...		DOS/Windows execu...	8
19/06/2007 ...	pssklcrbbhg...	26.b1@s202r2....		Suspected s...			50
19/06/2007 ...	wwpl_uk200...	26.b1@s202r2....	Congratulati...	Suspected s...			76
19/06/2007 ...	polk64581@...	26.b1@s202r2....		Suspected s...			50
19/06/2007 ...	spamzors@t...	26.b1@s202r2....	AutoMailer: ...	Suspicious A...		DOS/Windows execu...	8
19/06/2007 ...	elizabethtol...	elizabethtolbert...	FROM: Mrs ...	Suspected s...			50
19/06/2007 ...	wwpl_uk200...	26.b1@s202r2....	Congratulati...	Suspected s...			76
19/06/2007 ...	caraweissm...	rjb@sophos.com...	l-oreille	Suspected s...			69
19/06/2007 ...	nscgiyphl@...	26.b1@s202r2....	Re: snotty -...	Suspected s...			61
19/06/2007 ...	spamzors@t...	26.b1@s202r2....	AutoMailer: ...	Suspicious A...		DOS/Windows execu...	8
19/06/2007 ...	spamzors@t...	26.b1@s202r2....	AutoMailer: ...	Suspicious A...		DOS/Windows execu...	8
19/06/2007 ...	glennisdeba...	bugbear-reques...	Information ...	Suspected s...			57
19/06/2007 ...	fbclzedreklw...	26.b1@s202r2....		Suspected s...			50

Go to page 1 of 1

Actions

What would you like to do with the selected messages? Deliver/Forward

Search quarantine

□ Subject is

□ Sender is

□ Recipient is

□ Message ID

□ Reason is: Viral

☑ From: 19/06/2007

☑ To: 19/06/2007

Sort by: By time "new to old"

Servers: All servers

From this pane, you can enter search criteria in the **Search** panel, searching on subject, sender, recipient, message ID, reason for quarantine, or any combination of these. You can also filter your search by date using the **To** and **From** fields.

2. The list of quarantined messages is displayed in the details pane. Double-click an item for more details such as reasons for quarantining.
3. To deal with an item, highlight it, select an action from the drop-down menu in the **Actions** pane, and then click **Go**. You can delete a quarantined item or, remove the virus(es) and deliver it. If you believe mail to be wrongly classified please submit the item to Sophos for analysis. If you selected **Deliver/Forward**, go to step 4, otherwise the selected action is performed.
4. If you choose **Deliver/Forward** from the drop-down **Actions** menu, the **Deliver message(s)** dialog box appears. In the **Deliver messages** dialog box you can deliver the selected message(s) to intended recipients or to specified recipients. You can use this feature to forward quarantined items to an administrator to review the content of the email.

   For more information, see the *PureMessage for Microsoft Exchange user manual*.

5. Note that PureMessage delivers a copy of the email. The original file remains in the quarantine folder for the number of days specified in the **Quarantine settings** dialog box, unless you choose to **Automatically delete message(s) from quarantine after delivery**.
6. If you want to add the sender to your list of trusted senders, check the **Add sender to allowed list (skip spam scanning for this sender)** checkbox.
7. Click **OK** to save your changes.

10.3 Enabling end-users to access the spam quarantine website

There are two ways to enable end-users access the spam quarantine website.

You can set a task to send all users with quarantined spam mail an email notification, so they can click a link to access the website. See *Setting up quarantine digest emails to users* (section 10.4).

Alternatively, if you use Active Directory, users can visit the spam quarantine website directly at any time using a web browser such as Internet Explorer, at the following address:

```
http://servername:port/
```

Where `servername` is the name of the server on which PureMessage is installed and `port` is the port number for the quarantine digest website (port 8081 by default).

When the user accesses the website, Internet Information Services (IIS) will authenticate the user with Windows Authentication. If the user owns multiple email addresses (aliases), the spam quarantine website will show email messages quarantined for all the addresses.

If you want to distribute written instructions to your users that explain how to access the spam quarantine website, see the *PureMessage for Microsoft Exchange user manual*.

10.4 Setting up quarantine digest emails to users

PureMessage can send each user a message informing them that some of their email has been quarantined as spam. The user can follow a link to the web-based spam quarantine where they can delete unwanted mail, or retrieve wanted mail. To do this, set up spam quarantine digest email and schedule times when PureMessage should send it out.

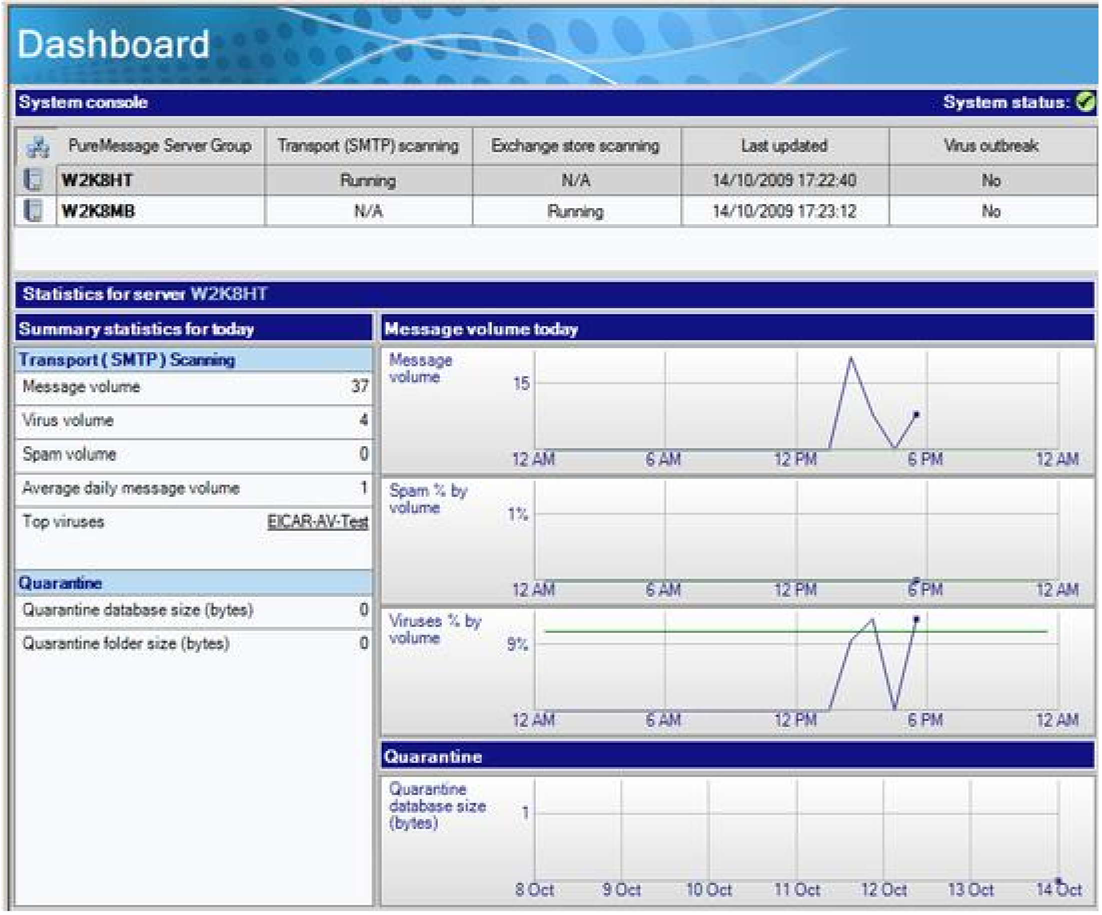
1. In the console tree, click **Configuration | Users and groups** and click **End user spam digest email**.
2. In the **End user spam digest email** dialog box, enter a subject in the **Digest subject** text box.
3. In the **Digest body text** panel, edit the digest as appropriate, or accept the default text. To enter or edit a substitution symbol, right-click and select a substitution symbol from the drop-down menu.
4. In the **Send digests on** panel, select the days and times you want to send out digests. Click **OK** to save your changes.
5. In the **Manage Changes** menu, click **Save changes**.

PureMessage now sends quarantine digest emails to users at specific times.

11 Monitoring system activity

The dashboard shows the system status and displays current statistics that provide the information about the health of all the servers on the system.

In the console tree, click **Dashboard**.



Dashboard

System console — System status: ✓

PureMessage Server Group	Transport (SMTP) scanning	Exchange store scanning	Last updated	Virus outbreak
W2K8HT	Running	N/A	14/10/2009 17:22:40	No
W2K8MB	N/A	Running	14/10/2009 17:23:12	No

Statistics for server W2K8HT

Summary statistics for today

Transport (SMTP) Scanning	
Message volume	37
Virus volume	4
Spam volume	0
Average daily message volume	1
Top viruses	EICAR-AV-Test

Quarantine	
Quarantine database size (bytes)	0
Quarantine folder size (bytes)	0

By default, the servers are listed in alphabetical order on the dashboard, unless one or more registers a system failure. In this case, the System Status traffic light becomes red, the faulty server is marked with a warning icon, and the server is displayed at the top of the list.

For each server, the **System console** panel displays the following information:

- Whether Transport (SMTP) Scanning is Running, Stopped (by user), or Unavailable. If the status is unavailable, an alert is displayed.

- Whether Exchange Store scanning is Running, Stopped (by user), or Unavailable. If the status is unavailable, an alert is displayed.
- Whether the last update succeeded, and if so, the time and date it took place. If it did not succeed, an alert is displayed.
- Whether there is a virus outbreak, and if so, on which server.
- For the selected server, the **Summary statistics for today** panel displays scanning and quarantine information for today (that is, since midnight) and shows the trends for each main category of information in the form of a graph. The information includes:
  - The current day's transport (SMTP) scanning statistics (including message volume, spam and viruses).
  - The current day's Exchange store scanning statistics (including attachments processed, and viruses detected).
  - The current day's quarantine statistics.

All information is refreshed every two minutes.

12 Uninstalling PureMessage

To uninstall PureMessage, do as follows:

1. If the PureMessage Administration console is open on any server, close it.
2. At the taskbar, click **Start | Settings | Control Panel**.
3. In **Control Panel**, double-click **Add/Remove Programs**.
4. In the **Add/Remove Programs** dialog box, select **Sophos PureMessage** and click **Remove**.
5. In the **Confirm Uninstall** message box, click **Yes**.

   A progress bar is displayed. Wait for uninstallation to complete.

13 Appendix A: Deploying PureMessage to Exchange clusters

13.1 How PureMessage works with Exchange clusters

PureMessage incorporates a cluster-aware service that can be installed across multiple nodes. This allows PureMessage to be used with clustered Microsoft Exchange servers and to take advantage of the increased resilience that a cluster offers.

Clustered systems are inherently more complicated than non-clustered systems and we recommend that you read the whole of this section before starting to install PureMessage on a cluster.

If you still have questions about installing PureMessage on a cluster after reading this section, contact Sophos technical support.

13.2 Before you install

13.2.1 Database requirements

For cluster server installations, PureMessage cannot use a local MSDE or SQL Server Express instance.

Alternatively, you may connect to any one of the following:

- A local clustered virtual SQL Server instance
- A remote SQL Server instance
- A remote MSDE or SQL Server Express instance

Note: In cluster scenarios, remote MSDE is not supported due to performance issues.

More than one PureMessage group or cluster can share a remote database.

13.2.2 Installation requirements

When installing PureMessage on nodes in a cluster, make sure that you meet the following requirements:

- The path to the installation folder must be identical on each node.
- The IIS websites present on each node of the cluster must be identical. In particular, the allocated port numbers of each site must be the same across nodes.

13.3 Installation procedure on DAGs

Database Availability Groups (DAGs) are used for implementing high availability in Exchange 2013.

- For DAGs, PureMessage uses DFS Replication (DFSR) to copy quarantine files between nodes. If you are using DAGs with Exchange 2013 in a high availability environment with multiple Transport Servers, these servers must be part of a Microsoft cluster. This allows PureMessage to replicate quarantine files using DFSR.
- Do not install on different DAG members concurrently. The PureMessage service should be installed on each DAG member one after another, but not simultaneously.
- If a DAG member has PureMessage installed and if it is added or removed from the DAG, then PureMessage must be reinstalled on that server. This is required so that the replication settings on the server are updated.

  To maintain Exchange availability during the re-install of PureMessage, the mailbox databases hosted on the server should be moved to an alternative server in the DAG.
- If you have separated Mailbox and Client Access servers, then install PureMessage first to the Mailbox server and then to the Client Access server.

13.4 Uninstalling PureMessage from a cluster

All PureMessage administration consoles (if running) need to be closed from all servers before uninstalltion. Follow instructions in *Uninstalling PureMessage* (section 12).

13.5 Administering PureMessage on a cluster

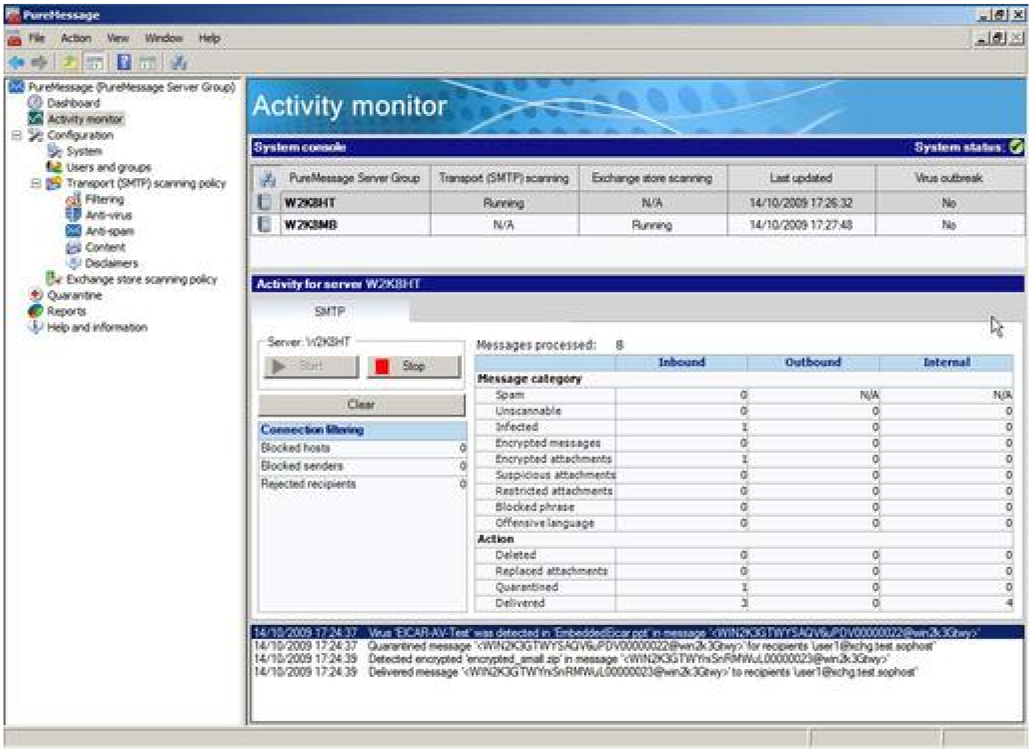
Several PureMessage servers may be arranged into a group and administered together from a single PureMessage console. All PureMessage servers in a group have the same policy settings applied to them, that is, when a policy change is made it is automatically applied to all the servers in the group.

13.5.1 Requirements and limitations

- The number of PureMessage servers in a group is limited by users' network bandwidth, and by SQL Server database resource limits.
- All group members need to also be members of the same domain.
- The ability to administer PureMessage servers from the remote console is directly dependant on the reliability of user network and database server connections.

13.5.2 Using the PureMessage administration console

In order to manage a group of PureMessage servers, the PureMessage console should connect to any server in the group. When policy changes are made, they will be automatically applied to all services in the group. Additionally, the activity monitor and dashboard screens will display status information for all the servers in the group:



PureMessage Server Group	Transport (SMTP) scanning	Exchange store scanning	Last updated	Virus outbreak
W2K8HT	Running	N/A	14/10/2009 17:26:32	No
W2K8MB	N/A	Running	14/10/2009 17:27:48	No

Connection filtering	
Blocked hosts	0
Blocked senders	0
Rejected recipients	0

Messages processed: 8

	Inbound	Outbound	Internal
Message category			
Spam	0	N/A	N/A
Unscannable	0	0	0
Infected	1	0	0
Encrypted messages	0	0	0
Encrypted attachments	1	0	0
Suspicious attachments	0	0	0
Restricted attachments	0	0	0
Blocked phrase	0	0	0
Offensive language	0	0	0
Action			
Deleted	0	0	0
Replaced attachments	0	0	0
Quarantined	1	0	0
Delivered	3	0	4

```
14/10/2009 17:24:37   Virus 'EICAR-AV-Test' was detected in 'EmbeddedEicar.ppt' in message '<WIN2K3GTWYSAGV6uPDV00000022@win2k3Gtwy>'
14/10/2009 17:24:37   Quarantined message '<WIN2K3GTWYSAGV6uPDV00000022@win2k3Gtwy>' for recipients 'user1@xchg.test.sophost'
14/10/2009 17:24:39   Detected encrypted 'encrypted_small.zip' in message '<WIN2K3GTWYnSnRMWuL00000023@win2k3Gtwy>'
14/10/2009 17:24:39   Delivered message '<WIN2K3GTWYnSnRMWuL00000023@win2k3Gtwy>' to recipients 'user1@xchg.test.sophost'
```

In order to manage a different group of PureMessage servers from the same console, it is necessary to disconnect from the current group and reconnect to a server from the new group.

To do this, on the PureMessage toolbar, click on the **Select server** icon.

14 Appendix B: How to configure upstream (trusted) relays

You should configure any upstream (trusted) relays to improve your email scanning speed and spam detection.

By default, PureMessage will run a reputation check on each email server address specified in an email. When a server is added to the upstream (trusted) relay list, the reputation check for that server is skipped. Because a lower volume of reputation checks has to be carried out, this improves the email scanning speed.

Upstream (trusted) relays also enable the spam engine to match an email server's address against the known list of spamming email servers with more precision. A higher spam score can therefore be allocated to the email when a match is found.

14.1 Which upstream relays should be defined as trusted?

You should define as an upstream (trusted) relay any email relay that sends or forward emails to PureMessage and that meets one of the following criteria (as in Figure 3):

- Your ISP's SMTP server.
- Any email relays located on your network which are upstream to your PureMessage server(s).
- A server which delivers mail to other servers in a cluster.

For more information see, *Set up a mail domain and upstream trusted relay* (section 4.2).

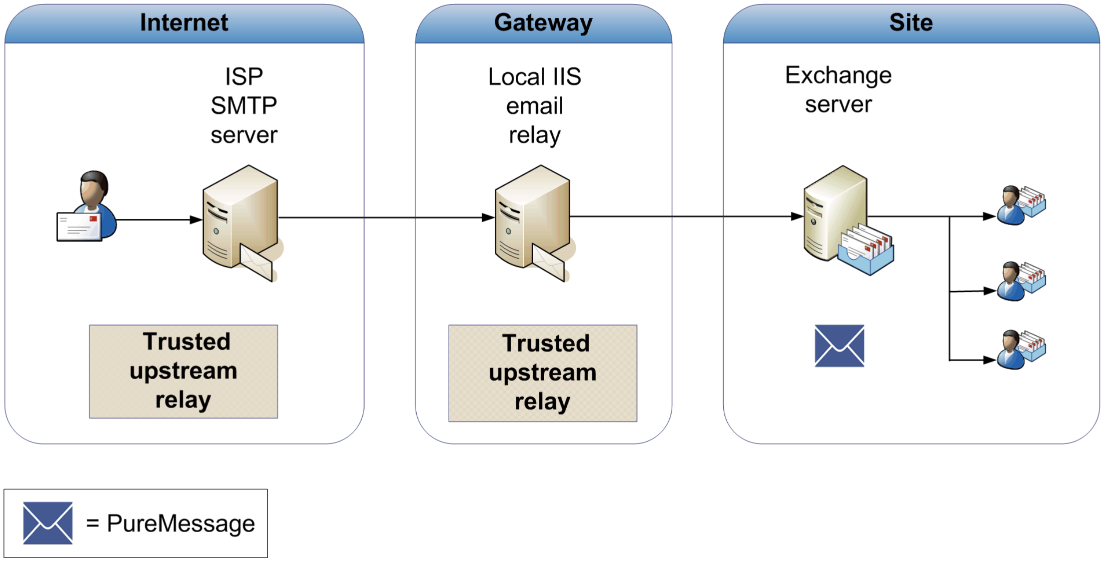


Figure 2: Trusted upstream relays

15 Appendix C: How does PureMessage route mail?

PureMessage uses the configured mail domains, trusted upstream relays, and IP address of the connecting host to distinguish between inbound, outbound and internal mail.

1. Is the recipient domain on the configured mail domain list?

   No: the message is *outbound*.

   Yes: go to step 2.

2. Is the sender's IP address external?

   Yes: the message is *inbound*.

   No: go to step 3.

3. Is the sender's IP address internal or unavailable?

   Internal: go to step 4.

   Unavailable: the message is *internal*.

4. Is the internal IP address on the list of trusted relays?

   Yes: the message is *inbound*.

   No: the message is *internal*.

16 Appendix D: About PureMessage mail scanning

PureMessage scans all SMTP inbound, outbound, and internal email messages and Exchange store emails and includes threat reduction technology to protect against new or unknown email-borne threats.

16.1 SMTP scanning

16.1.1 SMTP filtering

The SMTP filtering options in PureMessage perform recipient validation and use custom block lists to block hosts and messages in order to reduce the processing overhead on the server and save bandwidth.

Recipient validation

Organisations receive a lot of spam messages that are addressed to non-existent users. Recipient validation allows you to discard messages addressed to non-existent users.

This option requires a connection to a directory server or custom users and groups to provide the email addresses which are used to validate recipients. Typically this will be an Active Directory server.

Block lists

Block lists allow you to specify hosts and senders from whom PureMessage should not accept any messages.

Note: For information on enabling recipient validation and creating block lists, see the *PureMessage for Microsoft Exchange user manual*.

16.1.2 Anti-virus policies

You can define separate anti-virus policies for inbound, outbound and internal mail.

For information on configuring anti-virus scanning, see *Ensuring anti-virus scanning is enabled* (section 6).

16.1.3 Anti-spam policy

If your license permits, you can define an anti-spam policy.

PureMessage applies the anti-spam policy only to inbound messages. The anti-spam policy is On by default and applies to all users, but you can configure exceptions.

For information on defining an anti-spam policy, see *Blocking spam* (section 8).

16.1.4 Content filtering policies

PureMessage scans inbound, outbound and internal mail and filters unwanted content such as administrator-defined phrases and offensive language. You can define policies to filter content in a message header, subject, body, and/or attachment.

Note: For information on defining content filtering policies, see *Appendix E: Filtering attachments containing unwanted content* (section 17).

16.1.5 Attachment blocking

PureMessage can block suspicious or unwanted attachments and PUAs according to user-defined attachment types.

For information on blocking attachments and PUAs, see *Blocking files which may contain threats* (section 7).

16.2 Exchange Store scanning

PureMessage provides background scanning of Exchange private and public information stores using the Exchange Web Services API (EWS API).

Each time an item is scanned, it is stamped with an ID which indicates the virus signature version number at the time of scanning. An item will be rescanned *only* if a more up-to-date virus signature has been released by Sophos.

16.2.1 Background scanning

Exchange server background scanning continuously navigates the entire Exchange Store. As items that have not been scanned are encountered, they are submitted to PureMessage for scanning.

Background scanning is **disabled** by default for both private and public information stores.

As background scanning has a performance impact on the Exchange server, we recommend that you schedule it to run during periods of low server activity. Background scanning schedules can be defined in the Exchange store scan settings dialog.

Note: The scanning process will be reset if a virus signature update is received from Sophos. For large message stores, this can mean that background scanning will not complete a full scan of the store.

For information on defining background scanning periods and enabling background scanning, see *Configure scanning of Exchange stores* (section 9.2).

17 Appendix E: Filtering attachments containing unwanted content

PureMessage can analyse content within common document types. This enables you to search for phrases within those documents when they are attached to messages as files and apply policy rules accordingly.

PureMessage can extract content from the following file types:

- Plain text (TXT)
- HTML
- Rich text (RTF)
- PDF
- Microsoft Office documents (DOC, DOCX, PPT, PPTX, XLS, XLSX, etc)
- Microsoft Project
- Microsoft Visio

17.1 Filtering blocked phrases within attachments

This section contains two examples of how you can define policies to filter attachments which contain blocked phrases.

1. Identify attachments containing the word "Confidential". You do this by defining a *string of text* as a blocked phrase.
2. Identify attachments containing credit card numbers in the format "1234 1234 1234 1234" or "1234123412341234". You do this by defining a *regular expression* as a blocked phrase.

17.1.1 Filtering blocked phrases - strings of text

To define a string of text as a blocked phrase:

1. In the console tree, click **Configuration | Transport (SMTP) Scanning Policy**, and then click **Content**.
2. In the **Content filtering** dialog box, ensure that the status icons for inbound, outbound and internal messages title bars are Green and display **ON**.
3. Under **Outbound messages**, select the **On blocked phrase** check box.
4. Under **Outbound messages | On blocked phrase**, click **Define**.
5. On the **String (wildcards supported)** tab, click **Add**.
6. Click in the **Phrase** box and type `Confidential`.

7. Make sure that the **Attachment** check box is selected.
8. Click **OK** to save your changes and return to the **Content filtering** dialog box.
9. Under **Outbound messages**, click the **On blocked phrase** drop-down list and select **Quarantine message and deliver**.
10. In the **Manage changes** menu, click **Save changes**.

17.1.2 Filtering blocked phrases - regular expressions

To define a regular expression as a blocked phrase:

1. In the console tree, click **Configuration | Transport** (**SMTP**) **Scanning Policy**, and then click **Content**.
2. In the **Content filtering** dialog box, ensure that the status icons for inbound, outbound and internal messages title bars are Green and display **ON**.
3. Under **Internal messages**, select the **On blocked phrase** check box.
4. Under **Internal messages | On blocked phrase**, click **Define**.
5. On the **Regular expression** tab, click **Add**.
6. Click in the **Phrase** box and type the following regular expression:

   ```
   [0-9]{4} ?[0-9]{4} ?[0-9]{4} ?[0-9]{4}
   ```

   This expression will match credit card numbers in both "1234 1234 1234 1234" and "1234123412341234" formats.

7. Make sure that the **Attachment** check box is selected.
8. Click **OK** to save your changes and return to the **Content filtering** dialog box.
9. Under **Internal messages | On blocked phrase**, click **Alert**.
10. In the **Alert configuration** dialog box, select one or more check boxes to specify who will be notified in the event of PureMessage quarantining a suspicious attachment.
11. Click **OK** to save your changes and return to the **Content filtering** dialog box.
12. In the **Manage changes** menu, click **Save changes**.

You can find more information about creating regular expressions at *http://www.regular-expressions.info/*.

18 Appendix F: Database Mirroring

Database mirroring is a feature of SQL Server (available only in the Standard and Enterprise editions of SQL Server since SQL Server 2005 SP1) that provides high-availability without the need for a single-copy cluster.

To use mirrored databases with PureMessage, you must perform the following:

- *Prepare SQL Server instances* (section 18.1)
- *Install PureMessage with database mirroring* (section 18.2)
- *Configure PureMessage for database mirroring* (section 18.3)

18.1 Prepare SQL Server instances

Before installing PureMessage, you must prepare the SQL Server instances that will be used. A mirrored SQL database requires two or three SQL Server instances:

1. A principal server instance (data source).
2. A mirror server instance (failover partner).
3. Optionally, a witness server instance.

For information on SQL Server preparation for mirroring, see:

http://www.microsoft.com/technet/prodtechnol/sql/2005/dbmirror.mspx

http://msdn.microsoft.com/en-us/library/ms190941.aspx

Note:

- Ensure that the SQL Server instances are authenticated to access each other. This means that the accounts under which a SQL Server instances run must be granted access to the other SQL Server instances used in the mirror set, and that remote connections (e.g. over the TCP/IP protocol) must be enabled.
- The principal and mirror server instances should host the same edition of SQL Server, and it should be an edition that supports mirroring.
- For automatic failover, a witness server is required.
- For high-availability, the SQL Server instances must be installed on different physical servers and use synchronous mode.
- If any firewalls exist between the SQL Servers, they must be configured to allow the SQL servers to communicate over the TCP port chosen for mirroring.
- It is recommended that SQL installations use the same SQL instance name and file paths on all servers.

18.2 Install PureMessage with database mirroring

Database mirroring is enabled in PureMessage by selecting the **Remote** database option and supplying the names of both the principal and mirror server instances during installation. The names should be entered in the PureMessage Database settings dialog box, separated with a semi-colon.

Example: Server1\Instance1;Server2\Instance1

If PureMessage has already been installed without mirroring then these changes can be made retrospectively. For information, contact Sophos Technical Support.

18.3 Configure PureMessage for database mirroring

Once the PureMessage installation is completed, the databases and PureMessage login will have been created on the principal server instance.

The PureMessage login is named <domain>\SophosPureMessage, where <domain> is the domain of the PureMessage Server (or the machine name for a server that is in a workgroup).

The following steps can all be performed from the SQL Server Management Studio application, or by issuing the SQL commands provided:

For more information on using SQL Server Management Studio see, *http://technet.microsoft.com/en-us/library/ms175134.aspx*.

1. Create the PureMessage login on the mirror server instance:

   ```
   [Mirror]> CREATE LOGIN [<domain name>\SophosPureMessage] FROM
   WINDOWS
   ```

   `<domain name>` must be replaced with the actual domain of your PureMessage server, or with the machine name if in a Workgroup.

   For more information on setting up login accounts, see *http://technet.microsoft.com/en-us/library/ms366346.aspx*.

2. Perform a full backup for each of the four PureMessage databases from the principal server:

```
[Principal]> BACKUP DATABASE [SavexCnfg] TO DISK =
'<path>\SavexCnfg.bak'
[Principal]> BACKUP DATABASE [SavexDir] TO DISK =
'<path>\SavexDir.bak'
[Principal]> BACKUP DATABASE [SavexQuar] TO DISK =
'<path>\SavexQuar.bak'
[Principal]> BACKUP DATABASE [SavexRprt] TO DISK =
'<path>\SavexRprt.bak'
```

   `<path>` must be replaced with a path to a folder where the backup is to be stored.

   For more information on preparing a mirror database for mirroring, see *http://technet.microsoft.com/en-us/library/ms189047.aspx*.

3. Make the database backup available on the mirror server and restore each database to the mirror server instance. This will set the mirrored databases to **Mirror, Synchronized/Restoring** state.

```
[Mirror]> RESTORE DATABASE [SavexCnfg] FROM DISK =
'<path>\SavexCnfg.bak' WITH NORECOVERY
[Mirror]> RESTORE DATABASE [SavexDir] FROM DISK =
'<path>\SavexDir.bak' WITH NORECOVERY
[Mirror]> RESTORE DATABASE [SavexQuar] FROM DISK =
'<path>\SavexQuar.bak' WITH NORECOVERY
[Mirror]> RESTORE DATABASE [SavexRprt] FROM DISK =
'<path>\SavexRprt.bak' WITH NORECOVERY
```

   `<path>` must be replaced with a path to a folder where the backup is held.

   If the path names of the principal and mirror databases differ then it will be necessary to use the MOVE option of the RESTORE command, e.g.

```
[Mirror]> RESTORE DATABASE [SavexCnfg] FROM DISK =
<path>\SavexCnfg.bak' WITH NORECOVERY,
MOVE 'SavexCnfg' TO 'C:\Program Files\Microsoft SQL
Server\MSSQL.1\MSSQL\DATA\SavexCnfg.mdf',
MOVE 'SavexCnfg_log' TO 'C:\Program Files\Microsoft SQL
Server\MSSQL.1\MSSQL\DATA\SavexCnfg_1.LDF'
```

   For more information on preparing a mirror database for mirroring, see *http://technet.microsoft.com/en-us/library/ms189047.aspx*.

4. Create a mirroring endpoint on the principal server instance:

```
[Principal]> CREATE ENDPOINT [Mirroring]
STATE=STARTED
AS TCP (LISTENER_PORT = <port>)
FOR DATA_MIRRORING (ROLE = PARTNER)
```

   `<port>` must be replaced with a TCP port number to be used for the endpoint (e.g. 7022).

5. Create an endpoint on the mirror server instance:

   ```
   [Mirror]> CREATE ENDPOINT [Mirroring]
   STATE=STARTED
   AS TCP (LISTENER_PORT = <port>)
   FOR DATA_MIRRORING (ROLE = ALL)
   ```

6. Point the mirror server instance's partner to the principal server instance:

   ```
   [Mirror]> ALTER DATABASE [SavexCnfg] SET PARTNER =
   'TCP://<hostname>:<port>'
   [Mirror]> ALTER DATABASE [SavexDir] SET PARTNER =
   'TCP://<hostname>:<port>'
   [Mirror]> ALTER DATABASE [SavexQuar] SET PARTNER =
   'TCP://<hostname>:<port>'
   [Mirror]> ALTER DATABASE [SavexRprt] SET PARTNER =
   'TCP://<hostname>:<port>'
   ```

   `<hostname>` must be replaced with the fully-qualified, DNS hostname of the principal server.

   `<port>` must be replaced with a TCP port number to be used for the endpoint (e.g. 7022).

7. Point the principal server instance's partner to the mirror server instance:

   ```
   [Principal]> ALTER DATABASE [SavexCnfg] SET PARTNER =
   'TCP://<hostname>:<port>'
   [Principal]> ALTER DATABASE [SavexDir] SET PARTNER =
   'TCP://<hostname>:<port>'
   [Principal]> ALTER DATABASE [SavexQuar] SET PARTNER =
   'TCP://<hostname>:<port>'
   [Principal]> ALTER DATABASE [SavexRprt] SET PARTNER =
   'TCP://<hostname>:<port>'
   ```

   `<hostname>` must be replaced with the fully-qualified, DNS hostname of the mirror server.

   `<port>` must be replaced with a TCP port number to be used for the endpoint (e.g. 7022).

   For more information on setting up database mirroring using Windows authentication, see *http://technet.microsoft.com/en-us/library/ms179306.aspx*.

8. If a witness server is required then it can be configured as follows:

   ```
   [Witness]> CREATE ENDPOINT [Mirroring]
   STATE=STARTED
   AS TCP (LISTENER_PORT = <port>)
   FOR DATA_MIRRORING (ROLE = WITNESS)
   ```

   `<port>` must be replaced with a TCP port number to be used for the endpoint (e.g. 7022).

9. If a witness server is required on the principal server, set the witness for each database:

   ```
   [Principal]> ALTER DATABASE [SavexCnfg] SET WITNESS =
   'TCP://<hostname>:<port>'
   [Principal]> ALTER DATABASE [SavexDir] SET WITNESS =
   'TCP://<hostname>:<port>'
   [Principal]> ALTER DATABASE [SavexQuar] SET WITNESS =
   'TCP://<hostname>:<port>'
   [Principal]> ALTER DATABASE [SavexRprt] SET WITNESS =
   'TCP://<hostname>:<port>'
   ```

   <hostname> must be replaced with the fully-qualified, DNS hostname of the witness server.

   <port> must be replaced with a TCP port number to be used for the endpoint (e.g. 7022).

   For more information on adding a database mirroring witness using Windows authentication, see *http://technet.microsoft.com/en-us/library/ms190430.aspx*.

10. Depending on the permissions of the accounts running the SQL servers it may be necessary to explicitly grant permissions to the accounts for accessing the endpoints as follows:

    ```
    [Principal]> GRANT CONNECT ON ENDPOINT::[Mirroring] TO [<user>]
    [Mirror]> GRANT CONNECT ON ENDPOINT::[Mirroring] TO [<user>]
    [Witness]> GRANT CONNECT ON ENDPOINT::[Mirroring] TO [<user>]
    ```

    <user> must be replaced with the SAM name of account running the accessing SQL Server.

11. If necessary, e.g. if the servers are under heavy load, increase the ping timeout for the connections as follows:

    ```
    [Principal]> ALTER DATABASE [SavexCnfg] SET PARTNER TIMEOUT
    <integer>
    [Principal]> ALTER DATABASE [SavexDir] SET PARTNER TIMEOUT
    <integer>
    [Principal]> ALTER DATABASE [SavexQuar] SET PARTNER TIMEOUT
    <integer>
    [Principal]> ALTER DATABASE [SavexRprt] SET PARTNER TIMEOUT
    <integer>
    ```

    <integer> must be replaced with the required timeout (in seconds). The default time out used by SQL Server is 10 seconds.

19 Glossary

Active Directory synchronization A one-way synchronization of Active Directory users and groups with the PureMessage cache.

Active/Passive cluster A two-node cluster where the Active node owns the services and the Passive node remains inoperative.

adware and PUAs Adware displays advertising, for example, pop-up messages, which affects user productivity and system efficiency. A potentially unwanted application (PUA) is an application that is not inherently malicious but is generally considered unsuitable for the majority of business networks.

background scanning A form of scanning in which the Exchange Store is scanned when the Exchange server has periods of low activity.

dashboard An at-a-glance view of the status of the PureMessage servers.

demilitarized zone (DMZ) A network area protected by firewalls that sits between an organization's internal network and an external network, usually the internet.

downstream A transmission from an information server toward an end user.

email relay A type of server used to pass email from one point of the internet to another. Every email contains a list of the email relays it passes through on the internet, including the relay that was used to send the email.

Exchange Store The mailbox and public folders stored on an Exchange server.

failover In an Active/Passive cluster, the capability to switch services automatically to the Passive node upon the failure or abnormal termination of the Active node.

information store See Exchange store.

malware Short for malicious software. Software designed specifically to damage or disrupt a system, such as a virus, worm, or Trojan.

node A server that is part of a cluster.

non-delivery report (NDR) An automated electronic mail message from a mail system to a sender indicating failed message delivery.

private store A database (usually a mailbox) on an Exchange server that is only accessible to a single user.

public store A database on an Exchange server that is accessible to multiple users.

real-time scanning Automatic interception and scanning of email attachments as they are sent or received.

scheduled scan A scan that is scheduled to take place automatically at a particular time.

Simple Mail Transfer Protocol (SMTP) An internet standard for email transmission across IP networks. Email server software uses SMTP to send and receive mail messages.

spyware A program that installs itself onto a user's computer by stealth, subterfuge, or social engineering, and sends information from that computer to a third party without the user's permission or knowledge.

upstream A transmission from an end user toward the server.

upstream trusted relay A known email server that sends or forward emails to the server on which PureMessage is installed.

20 Technical support

You can find technical support for Sophos products in any of these ways:

- Visit the SophosTalk community at *community.sophos.com/* and search for other users who are experiencing the same problem.
- Visit the Sophos support knowledgebase at *www.sophos.com/en-us/support.aspx*.
- Download the product documentation at *www.sophos.com/en-us/support/documentation/*.
- Send an email to *support@sophos.com*, including your Sophos software version number(s), operating system(s) and patch level(s), and the text of any error messages.

21 Legal notices

XPExplorerBar

OpenSSL cryptographic toolkit

The OpenSSL toolkit stays under a dual license, i.e. both the conditions of the OpenSSL License and the original SSLeay license apply to the toolkit. See below for the actual license texts. Actually both licenses are BSD-style Open Source licenses. In case of any license issues related to OpenSSL please contact openssl-core@openssl.org.

OpenSSL license

Copyright © 1998–2011 The OpenSSL Project. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgment:

   "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (http://www.openssl.org/)"
4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.
5. Products derived from this software may not be called "OpenSSL" nor may "OpenSSL" appear in their names without prior written permission of the OpenSSL Project.
6. Redistributions of any form whatsoever must retain the following acknowledgment:

   "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)"

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT "AS IS" AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

Original SSLeay license

Copyright © 1995–1998 Eric Young (eay@cryptsoft.com) All rights reserved.

This package is an SSL implementation written by Eric Young (eay@cryptsoft.com). The implementation was written so as to conform with Netscape's SSL.