SOPHOS

Security made simple.

PureMessage for Microsoft Exchange

Help

Product version: 4.0

Document date: June 2015

Contents

1 About PureMessage for Microsoft Exchange

Sophos PureMessage 4.0 for Microsoft Exchange 2013 is software that provides integrated gateway and messaging protection from viruses, spam and unwanted email content.

It scans all internal, inbound, and outbound email messages and Exchange server stores. It also includes threat reduction technology to protect against new or unknown email-borne threats.

You can use PureMessage for Microsoft Exchange to ensure the hygiene of messages on your server or servers.

Main features

- **Filtering** at the SMTP transport level involves checking that inbound mail is addressed to valid recipients and is not from senders or servers you wish to block.
- **Anti-virus scanning** is done at the SMTP transport level on inbound, outbound, and internal mail and also within the Exchange store (for example, mailboxes and public folders). It involves scanning the message for viruses and taking appropriate action, such as quarantining email or deleting infected attachments.
- **Anti-spam scanning** relates to incoming mail only, and involves checking whether a message needs to be categorised as spam or suspected spam (depending on the spam rating of the message) and taking appropriate action. A spam digest email and web based spam quarantine enables end users to manage their quarantined spam email.
- **Content filtering** relates to incoming, outgoing and internal messages, and involves filtering out inappropriate content or monitoring email communications as defined by your organization's acceptable use policy.
- The **Dashboard** provides a real-time overview of the status of all the servers. The screen displays server status and mail volume, as well as quarantine information.
- **Active Directory integration** enables the use of existing users and groups within the email policy.
- **Separate policies** can be applied to inbound, outbound and internal mail flows.
- **Management reports** can be generated in graphical or tabular format, enabling administrators to track trends and email policy enforcement.

2 Key concepts

2.1 Key concepts overview

PureMessage offers connection filtering, anti-virus scanning, anti-spam scanning, and content filtering.

You can set up policies, specifying which mail to allow, block, quarantine or monitor. You can also customize policies for particular users or groups.

This section introduces key concepts you need when using PureMessage.

- Inbound, outbound and internal mail (page 5)
- Mail domains (page 5)
- Trusted relays (page 6)
- Filtering order (page 6)
- Policies (page 6)
- Updating (page 7)

2.2 Inbound, outbound, and internal mail

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

Inbound mail

The message is **inbound** if either of the following criteria is met:

- The recipient domain is on the configured domain list and the sender IP address is external.
- The recipient domain is on the configured domain list and the message comes from an internal IP address that is on the list of upstream (trusted) relays.

Outbound mail

The message is **outbound** if the recipient domain is not on the configured domain list.

Internal mail

The message is **internal** if the recipient domain is on the configured mail domain list and the sender IP address is internal or unavailable (in the case of internal MAPI message submission by MS Outlook).

2.3 Mail domains

Mail domains (for example mycompany.com) are required by PureMessage to classify inbound, outbound, and internal messages correctly.

Mail domains are recorded or collected during installation, but you can also add them at a later date.

For information on specifying the mail domains that PureMessage will use, see Routing (page 16).

For more information on mail direction, see Inbound, outbound and internal mail (page 5).

2.4 Trusted relays

An email relay is a server used to pass email from one point on the internet to another. Each email contains a list of the email relays it passes, including the email server used to send the email.

A trusted relay is a known email server that sends or forward emails to PureMessage.

Examples of trusted relays include your ISP's SMTP server and any email relays located on your network which are upstream to your PureMessage server(s). These can be trusted because they are highly unlikely to be the source of spam email. Servers on the trusted relay list will still relay spam email but are unlikely to be its original source.

By default PureMessage will run a reputation check on each email server address specified in an email. When a server is added to the trusted relay list the reputation check for that server is skipped, because the server is "trusted". This improves the email scanning speed and enables PureMessage to identify spam with greater confidence.

For information on specifying trusted relays, see Trusted relays (page 16).

2.5 Filtering order

PureMessage filters messages in a particular order. The default order is shown below.

This order assumes that your PureMessage server receives mail at the SMTP transport level and that the mail is then routed to your Exchange store.

1. **Filtering**. This is done at the SMTP transport level and involves recipient validation and use of custom block lists. This rejects a significant amount of mail at the SMTP transport level.
2. **Anti-virus scanning**. This relates to inbound, outbound, and internal mail.
3. **Anti-spam scanning**. This relates to inbound mail only.
4. **Content filtering**. This relates to inbound, outbound and internal mail.
5. **Exchange store scanning**. This relates to mail in the Exchange store (such as mailboxes and public folders).

The "action" that you assign to a policy also affects the filtering order. For example, if you configure content filtering so that the action to be taken is "delete", and configure anti-virus scanning so that the action is "quarantine", the content filtering is carried out first.

2.6 Policies

A policy is a group of settings that specifies how PureMessage will scan email and what action it will take against threats, spam or unwanted content.

You can set a policy for each type of email scanning. For example, you can set different policies for anti-virus, anti-spam and content filtering.

Within a policy, you can typically specify:

- which types of email are scanned (e.g. inbound, outbound)
- what action is taken for each event (e.g. infected mail)
- whether some users or groups are excepted from the action you set
- whether alerts are sent.

For an example of how to set a policy, see Setting a policy (page 27).

2.7 Updating

PureMessage requires frequent updating of the anti-virus data and anti-spam rules that it uses to filter email.

Updating is carried out automatically by the **Sophos AutoUpdate** feature supplied with PureMessage. You can view updating status or configure updating via the Sophos AutoUpdate icon (a blue shield) displayed in the task bar.

Sophos AutoUpdate can fetch updates as follows:

- anti-virus updates can be fetched direct from Sophos via the internet, or from a "central installation directory" on your network which is maintained by Sophos Enterprise Console or incase of Small Business Edition the Sophos Control Center.
- anti-spam updates can only be fetched direct from Sophos.

If you use anti-spam filtering, the computer running PureMessage will therefore need access to the internet.

Note:

- For information on creating central installation directories, see Sophos Endpoint Security and Control network startup guide.
- For information on configuring Sophos AutoUpdate, see the help files in Sophos AutoUpdate.

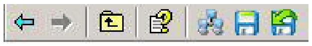
3 Administration console

3.1 Administration console overview

From the **administration console** you can view mail flow activity and administer PureMessage on all servers.

- PureMessage toolbar (page 8)
- PureMessage menu tree (page 8)

3.2 PureMessage toolbar



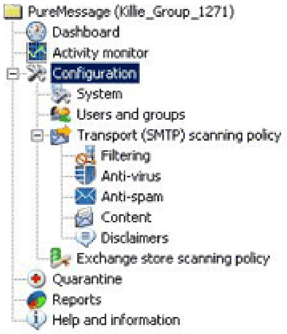
The **PureMessage toolbar** is displayed on the administration console and is an extension to the standard menu and tool bar. The main PureMessage buttons are described below.

Click this button to connect you to another group of servers. You will need to specify one of the servers within the group that you want to connect to.

Click the left button to save your configuration changes or the right button to undo your changes.

3.3 PureMessage menu tree

The **PureMessage menu tree** is displayed in the left (tree) panel of the screen. The Server Group (root node) displays the name of whichever server group the administration console is connected to. Click on a menu node to access the menu option.



The **Dashboard** provides general information and displays a list of all servers in the server group currently being administered. The dashboard provides statistics and graphs for the selected server.

You can see which services are running on a server, and whether updating is working correctly. Also displayed is information about email throughput, e.g. message volume and top viruses, and quarantine database size.

The **Activity monitor** provides a detailed breakdown of email classification as it is scanned by PureMessage. This section also enables the administrator to stop and start the PureMessage scanning service for each server.

The **Configuration** node provides access to the System, Users and groups, Transport (SMTP) scanning policy, and Exchange store scanning policy nodes.

The **System** node provides a number of system settings that are common to both SMTP and Exchange store scanning, including routing, virus outbreak settings, quarantine settings, log settings, alert configuration, email tagging and report settings.

The **Users and groups** node allows you to synchronize with Active Directory users and groups. You can also create custom users and groups.

The **Transport (SMTP) scanning policy** node relates to inbound, outbound, and internal mail. This menu node provides shortcuts to the Filtering, Anti-virus, Anti-spam, Content, and Disclaimers nodes, described below. Each node allows you to define and enable relevant policies. You can specify both overall policies and individual policies to exempt users and groups.

The **Filtering** node provides access to the recipient validation and block list menu options.

The **Anti-Virus** node enables you to set anti-virus policies for inbound, outbound, and internal mail.

The **Anti-Spam** node enables you to set policies for spam and suspected spam.

The **Content** node enables you to set content filtering policies for inbound, outbound, and internal mail.

The **Disclaimers** node enables you to define a disclaimer that is added to outbound messages.

The **Exchange store scanning policy** node enables you to specify anti-virus policies for mail in your mailboxes and public folders.

The **Quarantine** node displays a list of messages quarantined by PureMessage. You can search for quarantined messages using various search criteria and can take action on selected messages.

The **Reports** node enables you to generate reports on all incoming, outgoing and internal mail, including reports on viruses, spam, content such as offensive words or blocked phrases and connection filtering.

The **Help and Information** node provides access to the help file and the Sophos web site. It also displays system information about each server in the PureMessage server group.

4 Monitoring

4.1 Monitoring overview

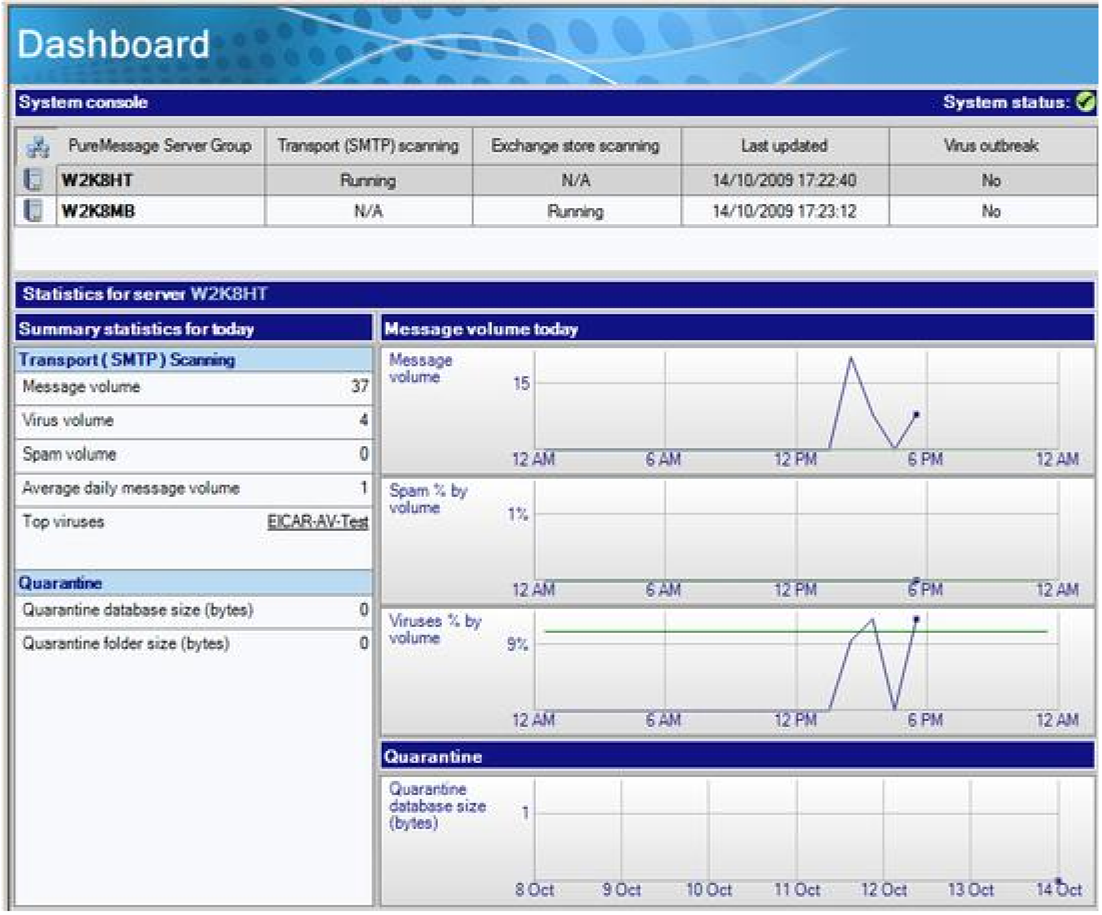
From the **administration console** you can get an overview of server status and mail flow activity on all servers.

- Overview of the Dashboard (page 10)
- Overview of the Activity monitor (page 12)

4.2 Overview of the Dashboard

The **Dashboard** provides general information and displays a list of all servers in the server group currently being administered, as well as statistics and graphs for the selected server. You can see which services are running on a server, and whether updating is working correctly. Also displayed is information about email throughput, e.g. message volume and top viruses, and quarantine database size. The information on the dashboard is refreshed automatically every 2 minutes.

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 first server in the list is selected and 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.

System console

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

- Whether transport scanning is **Running**, **Stopped** (by user) or **Unavailable**. If the scanning is unavailable, an alert is displayed.
- Whether Exchange store scanning is **Running**, **Stopped** (by user) or **Unavailable**. If the scanning 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 in progress, and if so, in which area of the server.

Summary statistics for today

Summary statistics for the selected server for the current day (since midnight) are displayed in the **Summary statistics for today** panel. It covers transport (SMTP) scanning, Exchange store scanning, and information about the quarantine database.

Transport (SMTP) scanning

The current day's transport scanning statistics are displayed as follows:

- Message volume
- Virus volume
- Spam volume
- Average daily message volume
- Top viruses.

Exchange store scanning statistics

The current day's Exchange store scanning statistics are displayed as follows:

- Attachments processed
- Viruses detected

Quarantine database statistics

The current day's quarantine database statistics are displayed as follows:

- Quarantine database size
- Quarantine folder size

Data flow graphs

The graphs for message volume, percentages of spam by volume, percentages of viruses by volume, and quarantined data show the data flow since mid-night. There are two lines; the blue line shows the mail flow since mid-night and the green line shows the average per hour data, for all data held in the database. If, for instance, you configured PureMessage to keep data for reporting purposes for 30 days, the green line will show the average data flow per hour over the last 30 days.

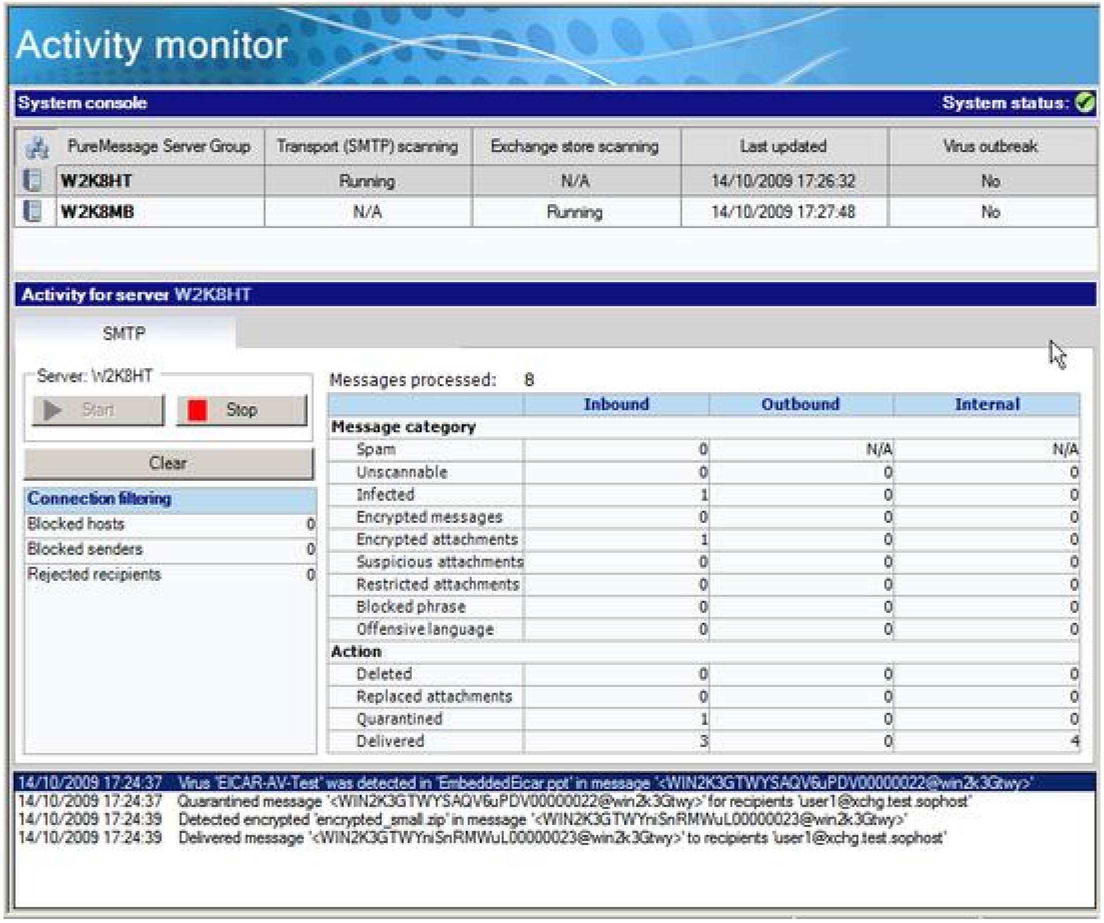
Note:

- If you have just installed PureMessage, and an update has not yet taken place, then the **Last updated** time is shown as unknown. To force an update, right-click on the shield icon on the task bar and choose the **Update now** option.
- If you have an Exchange 2007 or Exchange 2010 Edge Transport server installed in the perimeter network in an Exchange 2013 environment, the Attachment Filter agent is available on the Edge Transport server by default. The agent filters out email messages based on file name and email content type. As a consequence, emails containing certain attachments may not reach PureMessage (and their intended recipients) in their original form. This could affect the detected viruses, content or spam score that PureMessage detects for that message. For more information, see Appendix A: Using an Exchange Edge Transport server for attachment filtering (page 57).

4.3 Overview of the Activity monitor

The **Activity monitor** displays message statistics and a live log in real time for the selected server.

Click **Activity monitor**.



	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 '<WIN2K3GTWYSAQV6uPDV00000022@win2k3Gtwy>'
14/10/2009 17:24:37   Quarantined message '<WIN2K3GTWYSAQV6uPDV00000022@win2k3Gtwy>' for recipients 'user1@xchg.test.sophost'
14/10/2009 17:24:39   Detected encrypted 'encrypted_small.zip' in message '<WIN2K3GTWYniSnRMWuL00000023@win2k3Gtwy>'
14/10/2009 17:24:39   Delivered message '<WIN2K3GTWYniSnRMWuL00000023@win2k3Gtwy>' to recipients 'user1@xchg.test.sophost'
```

By default, the servers are listed in alphabetical order, and the first in the list is selected. For a selected server, the screen displays counters, as listed below.

For each server, the monitor displays server group, the status of transport (SMTP) scanning, Exchange store scanning, when the server last had an update, and whether there is a virus outbreak in progress.

Click the **SMTP** tab or the **Exchange store** tab as appropriate.

Click the **Start** button to start SMTP or Exchange store scanning job for the selected server.

Click the **Stop** button to stop the SMTP or Exchange store scanning job for the selected server.

Click **Clear** to reset the counters and clear the screen logs.

The main **SMTP** panel displays counters for the following:

- Messages received
- Connection filtering details (listed by category)
- Inbound mail (listed by category or action taken)
- Outbound mail (listed by category or action taken)
- Internal mail (listed by category or action taken)

The main **Exchange store** panel displays the following:

- Attachments scanned
- Attachments infected
- Attachments quarantined
- Attachments encrypted
- Attachments replaced
- Attachments unscannable

You can also click **Force rescan** to force a rescan of the Exchange store.

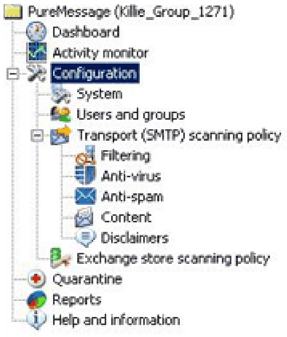
Note:

- If you have just installed PureMessage, and an update has not yet taken place, then the **Last updated** time is shown as unknown. To force an update, right click on the shield icon on the task bar and choose the **Update now** option.
- PureMessage transport (SMTP) scanning counts one email with one or more attachments as one message. If you get one email with 5 encrypted attachments, the Activity monitor displays this as one message.
- The **Delivered** figure in the inbound, outbound, and internal columns may differ from the total number of messages received. A message may be categorized, or acted upon in different ways, dependent upon the different types of content it contains and the different policies that apply to it. A scanned message may be deleted, quarantined or delivered, or even be delivered multiple times if sent to a group of people to which different policies apply.
- If you have an Exchange 2007 or Exchange 2010 Edge Transport server installed in the perimeter network in an Exchange 2013 environment, the Attachment Filter agent is available on the Edge Transport server by default. The agent filters out email messages based on file name and email content type. As a consequence, emails containing certain attachments may not reach PureMessage (and their intended recipients) in their original form. This could affect the detected viruses, content or spam score that PureMessage detects for that message. For more information, see Appendix A: Using an Exchange Edge Transport server for attachment filtering (page 57).

5 Configuration

5.1 Configuration overview

The **Configuration** node allows you to configure policies and settings in PureMessage.



- System configuration (page 15)
- Users and groups (page 24)
- Transport (SMTP) scanning policy (page 32)
- Exchange store scanning policy (page 47)

5.2 System configuration

5.2.1 System configuration overview

The **System** configuration node provides a number of system settings that are common to both SMTP and Exchange store scanning, including routing, virus outbreak settings, quarantine settings, log settings, alert configuration, email tagging and report settings.

Click **Configuration** and then click **System**.

- Routing (page 16)
- Trusted relays (page 16)
- Email tagging (page 17)
- Alert configuration (page 18)
- Virus outbreak settings (page 21)
- Quarantine settings (page 22)
- Report settings (page 22)
- Log settings (page 22)

- Backup and restore configuration (page 23)

5.2.2 Routing

The **Routing** dialog enables you to specify your mail domains and trusted relays.

Mail domains (e.g. mycompany.com) are required by PureMessage to classify inbound, outbound, and internal messages correctly. Mail domains are recorded or collected during installation, but you can also add them at a later date.

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

Upstream (trusted) relays are servers that deliver mail to PureMessage. They are used to determine mail direction and are exempt from reputation checks. For additional information on trusted relays, see Trusted relays (page 6) in the key concepts section.

For more information on mail direction, see Inbound, outbound and internal mail (page 5).

Click **Configuration | System** and then click **Routing**.

Click **Add** to add a new domain to the list.

Click **Edit** to edit an existing domain.

Click **Remove** to remove a highlighted domain.

Click **Upstream (trusted) relays** to configure upstream mail servers between the Internet and PureMessage. See Trusted relays (page 16).

Note: From the **Manage changes** menu, click **Save changes** to save your configuration.

5.2.3 Trusted relays

5.2.3.1 Trusted relays overview

The **Upstream (trusted) relays** dialog box is used to specify IP addresses of trusted relays that deliver mail to PureMessage. For more information on trusted relays, see Trusted relays (page 6) under *Key concepts*. PureMessage uses trusted relays to determine mail direction (page 5). Trusted relays are also exempt from reputation checks by PureMessage.

Click **Configuration | System** and then click **Routing**. From the **Routing** dialog box, click **Upstream (trusted) relays**.

Click **Add** to add an IP address or IP address range and a comment for administrative purposes. See Specify host IP addresses (page 17).

Click **Edit** to edit the highlighted entry.

Click **Remove** to remove the highlighted entry.

Click **OK** to save your changes.

5.2.3.2 Specify host IP addresses

You can add a host, a range of hosts, or a sender to the block list (if you accessed this screen from the **Block List** dialog box) or to the allow list (if you accessed this screen from the **Allow List** dialog box.

Specify an IP address or IP address range

Enter a single IP address or a range of addresses.

Comments (optional)

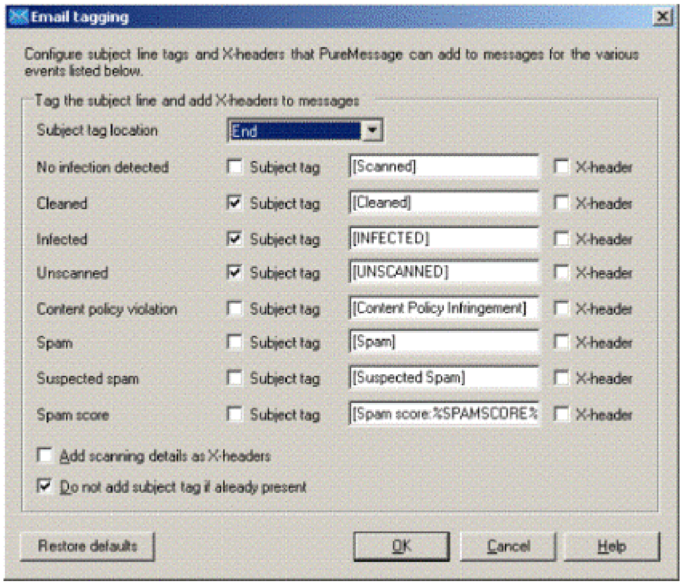
Enter a comment here. This is for administrative purposes.

Note: From the **Manage changes** menu, click **Save changes** to save your configuration.

5.2.4 Email tagging

You can specify tags (comments), which will be appended to the subject line of scanned mail.

Click **Configuration | System** and then click **Email tagging**.



Email tagging

Configure subject line tags and X-headers that PureMessage can add to messages for the various events listed below.

Tag the subject line and add X-headers to messages

Subject tag location: End

No infection detected	☐ Subject tag	[Scanned]	☐ X-header
Cleaned	☑ Subject tag	[Cleaned]	☐ X-header
Infected	☑ Subject tag	[INFECTED]	☐ X-header
Unscanned	☑ Subject tag	[UNSCANNED]	☐ X-header
Content policy violation	☐ Subject tag	[Content Policy Infringement]	☐ X-header
Spam	☐ Subject tag	[Spam]	☐ X-header
Suspected spam	☐ Subject tag	[Suspected Spam]	☐ X-header
Spam score	☐ Subject tag	[Spam score:%SPAMSCORE%	☐ X-header

☐ Add scanning details as X-headers

☑ Do not add subject tag if already present

Tag the subject line and add X-headers to messages

From this screen you can add tags (comments) to the subject line and an X-header for various events.

Select an option from the **Subject tag location** list to specify where to put the tag in the subject line.

Check the subject tag and/or X-header checkbox(es) to add a subject tag and/or X-header. You can also add the spam score to the subject line.

Add scanning details as X-headers

Select this check box to add the scanning details as X-headers. Scanning details include information such as, version of anti-virus, anti-spam engine, and so on used to scan the message.

Do not add subject tag if already present

Ensure this check box is checked to avoid duplication of subject tags as the mail goes through different PureMessage servers. Also avoids duplication of tags when a mail is forwarded or replied to by end users several times.

Restore defaults

Click this to restore the default settings.

Note: From the **Manage changes** menu, click **Save changes** to save your configuration.

5.2.5 Alert configuration

5.2.5.1 Alert configuration overview

You can set up a template for alerts and configure recipients for the administrator alert messages.

- Creating a template for alerts (page 18)
- Addresses for alerts (page 18)

5.2.5.2 Creating a template for alerts

The template enables the administrator to provide additional information to the alert recipients on the reason for the alert being sent.

Click **Configuration | System | Alert Configuration** and then click the **Alert Template** tab.

Alert subject

Enter the subject line of the alert. Right-click within the text field to view available substitution symbols (page 19).

Alert body text

In the **Alert body text** panel, enter the main text of your alert. Right-click within the text field to view available substitution symbols (page 19).

Text for each incident

In the **Text for each incident** panel, create text you want to display specific to each incident.

Click **Restore Defaults** to restore the default settings.

Note: From the **Manage changes** menu, click **Save changes** to save your configuration.

5.2.5.3 Addresses for alerts

This screen enables you to configure two alert related settings:

- Specify the email accounts to which administrator alerts will be sent.
- Specify an email account from which alerts will appear to have been sent from. This enables alert recipients to respond to an alert.

Click **Configuration | System**, and then click **Alert configuration**. By default, the **Email addresses** tab is selected.

- **Send administrator alerts to**

  The **Send administrator alerts to** panel lists the email addresses that will receive administrator alert messages.

  Click **Add** to enter a new email address.

  Click **Edit** to edit a highlighted address.

  Click **Remove** to remove a highlighted address.

- **Sender email address**

  In the **Sender email address** field, specify an email address to use when sending out alerts and other PureMessage-generated messages.

Note: From the **Manage changes** menu, click **Save changes** to save your configuration.

Click the Alert Template (page 18) tab to create a template for the alert.

5.2.5.4 Substitution symbols for alerts

To ensure that PureMessage includes specific details about an event (such as the date or the action that has been carried out) in an alert subject line or message, use the substitution symbols below.

Message body and subject substitution symbols	Description
%MESSAGE_EVENTS%	Events that were encountered; for example, Infected mail processed.
%MESSAGE_ACTION%	Action that has been carried out on the message.
%DATE%	Date when event occurred.
%TIME%	Time when event occurred.
%MESSAGE_ID%	Message identifier.
%SERVER%	Name of the server that encountered the event.
%SUBJECT%	Message subject.
%SENDER%	Sender of the message.
%RECIPIENTS%	Message recipients.
%JOB%	Job name, such as Transport (SMTP) scanning or Exchange store scanning.

Per incident substitution symbol	Description
%EVENT%	Incident event; for example, Infection detected.
%LOCATION%	Location where the event occurred, e.g. Body Text or Subject or Name of the attachment.
%REPLACED%	Specifies whether the location was replaced or not.
%DETAILS_TYPE%	Type of additional information, e.g. Virus name(s).
%DETAILS%	Additional information itself, e.g. "W32/Trojman".

Substitution symbols for replacement text

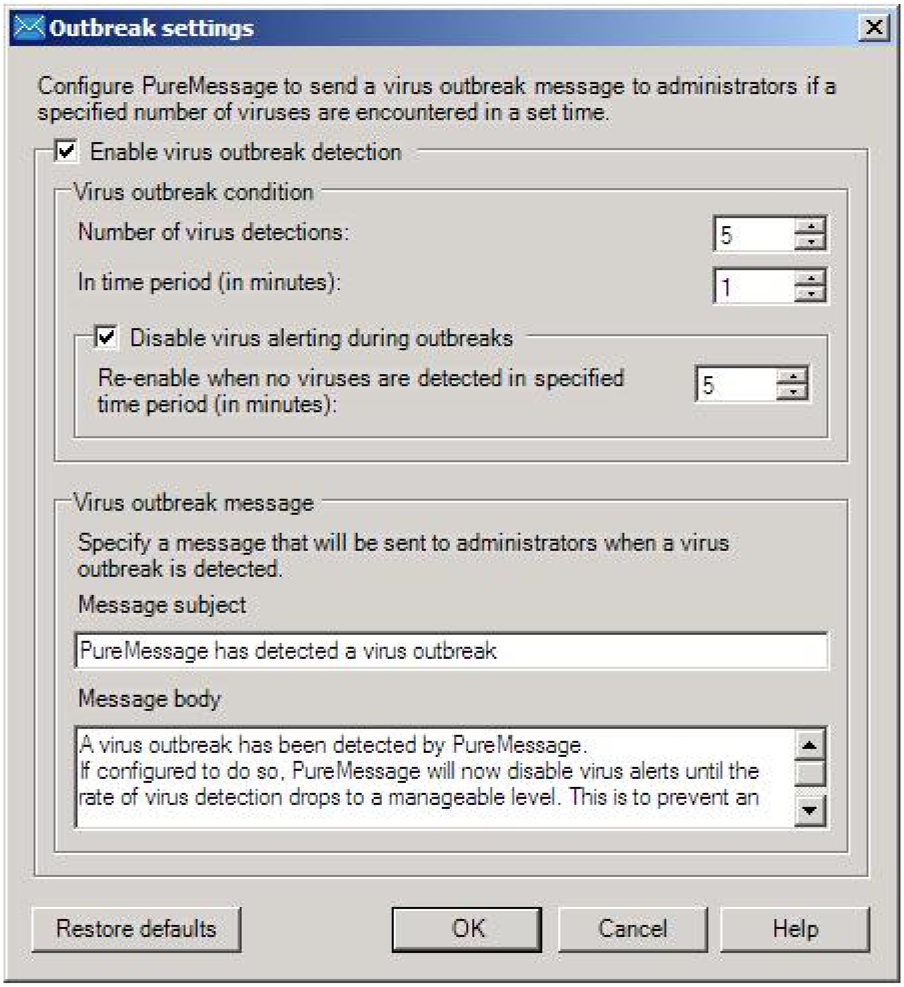
To ensure that PureMessage includes specific details of a virus or error event (for example, the date or the action that has been carried out) in the replacement text, use the substitution symbols below.

Symbol	Description
%EVENT%	Infected, encrypted or unscannable.
%LOCATION%	Location where the event occurred, e.g. Body Text or Subject or Name of the attachment.
%MESSAGEID%	Message identifier.
%DATE%	Date when attachment was replaced.
%TIME%	Time when attachment was replaced.
%SERVER%	Name of the server that added the replacement text.
%JOB%	The job name; Transport (SMTP) scanning or Exchange store scanning.
%DETAILS TYPE%	Type of additional information, e.g. Virus name(s).
%DETAILS%	Additional information itself, e.g. "W32/Trojman".

5.2.6 Virus outbreak settings

If a specified number of viruses are discovered in a set time PureMessage can send an **outbreak alert** to administrators. You can use this screen to configure the definition of an outbreak and specify the contents of an alert.

Click **Configuration | System** and click **Virus outbreak settings**.



Configure PureMessage to send a virus outbreak message to administrators if a specified number of viruses are encountered in a set time.

☑ Enable virus outbreak detection

Virus outbreak condition

Number of virus detections: 5

In time period (in minutes): 1

☑ Disable virus alerting during outbreaks

Re-enable when no viruses are detected in specified time period (in minutes): 5

Virus outbreak message

Specify a message that will be sent to administrators when a virus outbreak is detected.

Message subject

PureMessage has detected a virus outbreak

Message body

A virus outbreak has been detected by PureMessage.
If configured to do so, PureMessage will now disable virus alerts until the rate of virus detection drops to a manageable level. This is to prevent an

Ensure the **Enable virus outbreak detection** checkbox is checked. If this is not checked no outbreak will be detected and no alert sent.

Virus outbreak condition

By default PureMessage warns administrators when an outbreak has occurred. You can change the settings for this option.

Disable virus alerting during outbreaks

Click **Disable virus alerting during outbreaks** to prevent the administrator from receiving an excess number of alerts during an outbreak. You can then enter a number (time period) in the box **Re-enable when no viruses are detected in specified time period (in minutes).**

Virus outbreak message

Enter text in the **Message subject** panel. This will appear in the subject line of the alert message to the administrator.

Enter text in the **Message body** panel. This will be used as the body of the message.

Note: From the **Manage changes** menu, click **Save changes** to save your configuration.

5.2.7 Quarantine settings

The **Quarantine settings** page lets you specify the number of days to keep mail in the quarantine database before deleting the mail.

Click **Configuration | System** and click **Quarantine settings**.

Enter the number of days you want to keep mail messages before deletion.

Click **Purge old mails now** to delete items older than the specified number.

Click **Restore defaults** to restore the defaults.

Note: From the **Manage changes** menu, click **Save changes** to save your configuration.

5.2.8 Report settings

The **Report settings** page lets you specify the number of days to keep reporting data before deleting it.

Click **Configuration | System** and click **Report settings**.

Check the **Enable data collection for reports** checkbox.

Enter the number of days you want to keep report data before deletion.

Click **Purge now** to delete any reporting data older than the specified number of days.

Click **Restore defaults** to restore the defaults.

Note: From the **Manage changes** menu, click **Save changes** to save your configuration.

5.2.9 Log settings

You can specify the kind of messages to be logged and you can optionally set the maximum log file size. There are three levels of logging. You can log all errors, warnings and information. Alternatively, you can log warnings and errors or errors only, or you can disable logging completely.

Click **Configuration | System | Log settings**.

Transport (SMTP) scanning logging level

Select a level of logging from the **Windows event logging** list or accept the default.

Select a level of logging from the **File logging** list or accept the default.

Optionally, check the **Limit log file size to** checkbox and enter a number in the **MB** box. If the log file reaches its maximum size, the file is renamed by adding a time-stamp onto its name, and a new log-file is created.

Exchange store scanning logging level

Select a level of logging from the **Windows Event logging** list or accept the default.

Select a level of logging from the **File logging** list or accept the default.

Optionally, check the **Limit log file size to** checkbox and enter a number in the **MB** box. If the log file reaches its maximum size, the file is renamed by adding a time-stamp onto its name, and a new log-file is created.

Click **Restore defaults** to restore the factory defaults.

Note: From the **Manage changes** menu, click **Save changes** to save your configuration.

The log files for SMTP and Exchange store scanning (SMTPScan.log and ExchangeStoreScan.log) are located in the **Logs** folder under the PureMessage installation directory. If Windows Event logging is enabled, PureMessage writes logs to the Windows application event log.

5.2.10 Backup and restore configuration

You can backup a PureMessage configuration to a specified folder. You can then restore it at a later date, if required.

Note:

- Restoring a configuration will overwrite the existing configuration. If you wish to save your current configuration, ensure you backup before applying a new one.
- Before you restore a configuration across PureMessage server groups ensure any user-specific policies, Active Directory configuration, and recipient validation configurations are valid in the new group as well.

In the **PureMessage menu tree**, click **Configuration** and click **System**. On the right pane of the **Configuration** menu, you have the options **Backup configuration** and **Restore configuration**.

To backup the current configuration:

1. In the **Configuration** menu, click **Backup configuration**.
2. Choose a folder.
3. Click **OK.** The configuration files are saved to the chosen directory.

To restore a configuration:

1. In the **Configuration** menu, click **Restore a configuration**.
2. In the **Browse for folder** screen, select the folder with your target configuration.
3. Click **OK**.
4. In the popup box, click **Yes** to confirm that you want to restore the configuration and overwrite your existing configuration.

Note: From the **Manage changes** menu, click **Save changes** to save your configuration.

5.3 Users and groups

5.3.1 Users and groups overview

The **Users and groups** node allows you to configure and synchronize with Active Directory. You can also specify custom users and groups, and configure end user spam digest settings.

Click **Configuration** and then click **Users and groups**.

- Active Directory (page 24)
- End user spam digest email (page 25)
- Custom users and groups (page 25)

5.3.2 Active Directory

You can configure PureMessage to integrate with Microsoft Active Directory to create message policies based on users and groups already configured in the directory server. Active Directory can also be used for recipient validation, for example to filter messages addressed to users not present in the directory server.

Click **Configuration | Users and groups**, and then click **Active Directory**.

To connect to Active Directory, click **Detect Active Directory**. The fields in the **Active Directory Settings** panel are filled in automatically.

Enter your user name and password in the **Logon Credentials** pane if you are synchronizing with an instance of AD LDS or if you are synchronizing with the Active Directory Global Catalog Server. Otherwise, PureMessage will log on using the SophosPureMessage service account.

Click **Verify settings** to connect to Active Directory. PureMessage will attempt to log on using the credentials you supplied. If the credentials are correct, a popup appears confirming this. Click **OK** to continue.

Synchronize with Active Directory

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

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

A popup may appear saying that the configuration changes need to be saved. Click **OK** to continue.

Note: 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.

To configure directory server settings when using AD LDS, refer to Appendix B: Configuring PureMessage with AD LDS (using AdamSync) (page 58).

5.3.3 End user spam digest email

You can let end users know that they have spam email in the quarantine and enable them to access it.

Note: This section tells you how set up spam digests. For information on how end users can deal with quarantined spam and how they can access the quarantined spam anytime directly via a web browser, see the Enabling end users to access quarantined spam (page 51) section.

Click **Configuration | Users and groups** and then click **End user spam digest email**.

1. Check the **Enable spam digest emails to be sent to end users** checkbox.
2. Enter a subject in the **Digest subject** text box.
3. Enter the body of the digest text in the **Digest body text** panel. Right-click to view available substitution symbols.
4. Enter the time(s) and day(s) you want to send digests out. You can send digests out up to twice a day.

Note: From the **Manage changes** menu, click **Save changes** to save your configuration.

5.3.4 Custom users and groups

5.3.4.1 Custom users and groups overview

By default, the transport (SMTP) policies are applicable to all users. You can set up an exception with a different action to be applied within an existing policy, and apply that to custom users or groups. You can set up custom users and groups independent of Active Directory, for instance you could create temporary custom users for guests.

Click **Configuration | Users and groups** and then click **Custom users and groups**.

Custom users and groups

The main panel displays basic details about the custom user or groups. That is, type, name, email, and description.

Click **New group** to add a custom group. The **Custom group (page 25)** dialog box appears. Create a new group, which is then displayed as an entry on the Custom users and groups screen.

Click **New User** to add a custom user. The **Custom user (page 26)** dialog box appears. Specify user details, which are then displayed as an entry on the Custom users and groups screen.

Click **Edit** to edit the highlighted custom user or group.

Click **Remove** to delete the highlighted custom user or group.

Note: From the **Manage changes** menu, click **Save changes** to save your configuration.

5.3.4.2 Custom groups overview

The **Custom group** dialog box allows you to create a custom group for administrative purposes, for example you can apply a unique action within a policy to a custom group.

Click **Configuration | Users and groups | Custom users and groups** and then click **New group**.

Group details

Enter details in the **Group name** and, optionally, in the **Description (optional):** fields.

Group Members

The main panel displays custom group members in alphabetical order when the dialog box is opened. When new entries are added, they are added to the end of the list.

Click **Add** to add new members to a custom group. The **Find users and groups (page 26)** dialog box appears. In the **Find users and groups** dialog box, search and choose relevant users or groups and return it to the **Custom groups** dialog box.

Click **Remove** to remove the highlighted custom group.

Note: From the **Manage changes** menu, click **Save changes** to save your configuration.

5.3.4.3 Find users and groups

The **Find users and groups** dialog box allows you to find and select users and groups from Active Directory or the custom users and groups list.

Click **Configuration | Users and groups | Custom users and groups | New group** and then click **Add**.

1. In the **Search users and groups in:** field, select either **Active Directory** or **Custom users and groups** from the drop-down menu.
2. In the **Name** field, enter the name of the person or group to search for. You can use the wildcards '*' and '?'.
3. Optionally, in the **Description** field, enter a description to search for. You can use the wildcards '*' and '?'.
4. Click **Find now**. A list of groups and users appears in alphabetical order.
5. Highlight one or more entries and click **Add**. The selected entries are added to the specified group in the **Group members** panel of the **Custom group** dialog box.

5.3.4.4 Custom users

The **Custom user** dialog box allows you to create new users.

Click **Configuration | Users and groups | Custom users and groups** and then click **New user**.

User Details

Enter data into the **Display name:** and **Primary email address:** fields to specify user details. Optionally, enter a note for administrative details in the **Description (optional):** field.

Alias email addresses (optional)

The **Display name** and **Primary email address** fields are mandatory, all other fields are optional.

When you click **Add**, a new entry appears in the **Alias email addresses** panel at the bottom of the list. Type the new address.

Click **Edit** to edit a highlighted address. (If you select multiple entries, **Edit** option will be disabled).

Click **Remove** to remove a highlighted address.

Note: From the **Manage changes** menu, click **Save changes** to save your configuration.

5.4 Policies

5.4.1 Policies overview

A policy is a group of settings that specifies how PureMessage will scan email and what action it will take against threats, spam or unwanted content.

You can set a policy for each type of email scanning. For example, you can set different policies for anti-virus, anti-spam and content filtering.

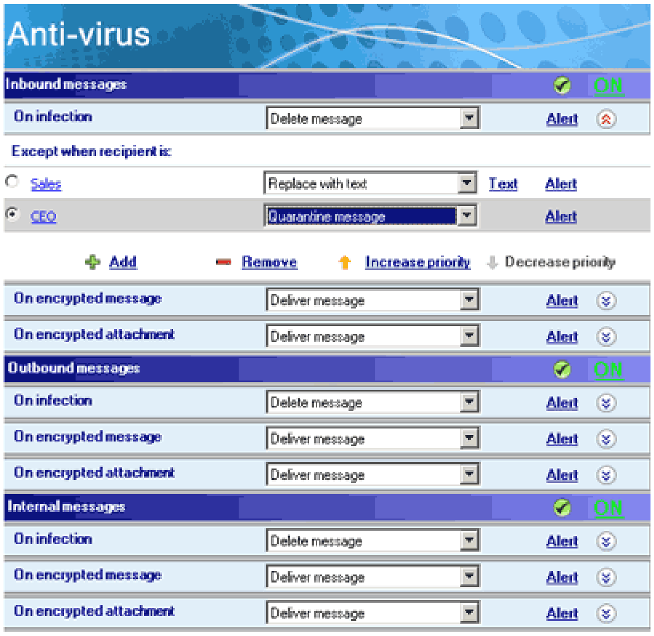
- Setting a policy (page 27)
- Setting up actions (page 28)
- Setting replacement text (page 29)
- Setting up alerts (page 29)
- Setting up exceptions (page 31)

5.4.2 Setting a policy

Here is an example of how to set a policy.

Setting an anti-virus policy

Click **Configuration | Transport (SMTP) scanning policy** and then click **Anti-virus**.



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

Enabling scanning

The screen displays three different types of email scanning: inbound mail, outbound mail and internal mail.

By default, scanning is enabled for all.The menu bar for each kind of mail will be blue, and the associated icon will display a checkmark and the word **ON**.

Note: If any menu bar is red, scanning for that direction of mail is disabled. Click the associated **OFF** text or circled alert icon to enable scanning.

Setting actions

There are three types of event. Infected mail, an encrypted attachment (e.g. password protected file), or an encrypted message.

For each event, you can select an action from the drop-down menu, e.g. Delete message, Quarantine message or Replace with text. For information, see Setting up actions (page 28).

If you select **Replace with text**, the **Text** link appears. Follow the link to specify the replacement text that will be used. For information on how to set replacement text, see Setting replacement text (page 29).

Setting up alerts

If you configure PureMessage to perform an action, the **Alert** link appears. Follow the link to specify alerts. For information on setting up alerts, see Setting up alerts (page 29).

Setting up exceptions

You can also exempt some users or groups or apply different actions to them for a particular event. For more information, see Setting up exceptions (page 31).

5.4.3 Setting up actions

Select an action from the policy panel **Action** list. You can choose from the following options:

Note: Depending on the policy type, certain options might not be available.

- **No Action** No action is taken. No alert message is generated and no subject tagging is performed.
- **Deliver message** No action is taken, but alert message is generated and subject tagging is performed.
- **Replace with text** Replaces the entire attachment with plain text. The text to be replaced is configurable. For information on how to set replacement text, see Setting replacement text (page 29).
- **Quarantine and Replace with text** Quaranties the original attachment and replaces it with plain text. The text to be replaced is configurable. This is option is only available for Exchange Store Scanning policy. For information on how to set replacement text, see Setting replacement text (page 29).

- **Delete message** Deletes the entire message.
- **Quarantine message** Quarantines the original message and does not deliver it.
- **Quarantine message and deliver** Quarantine the original but also delivers a copy of the message to the original intended recipients.

5.4.4 Setting replacement text

When PureMessage takes an action to replace an attachment with text, for example when an inbound message has an infected attachment, you may wish to give the intended recipient information about the replaced attachment such as the event that caused the action, names of detected viruses and so on.

You specify the text of this message when editing a policy.

For example, click **Configuration | Transport (SMTP) scanning policy**, and then click **Anti-virus**. In the **Anti-virus** dialog box, for one of the events listed, select **Replace attachment with text** from the drop-down menu. Then click the **Text** link that is displayed.

In the **Replacement text** dialog box, right-click within the text box to view available substitution symbols (page 19).

Click **Restore defaults** to restore the default settings.

Note: From the **Manage changes** menu, click **Save changes** to save your configuration.

5.4.5 Setting up alerts

For every event relating to Transport (SMTP) or Exchange store scanning, you can configure whether **alerts** should be sent to administrators, senders, and recipients. When exceptions are added, the alert configuration is copied from the default (top level) event.

The **Alert configuration** dialog box is accessed from a number of different screens.

In the **Alert configuration** dialog box, make your selection by choosing the appropriate check boxes to send alerts for senders, recipients or administrators.

Note: From the **Manage changes** menu, click **Save changes** to save your configuration.

5.4.6 Substitution symbols for alerts

To ensure that PureMessage includes specific details about an event (such as the date or the action that has been carried out) in an alert subject line or message, use the substitution symbols below.

Message body and subject substitution symbols	Description
%MESSAGE_EVENTS%	Events that were encountered; for example, Infected mail processed.
%MESSAGE_ACTION%	Action that has been carried out on the message.

Message body and subject substitution symbols	Description
%DATE%	Date when event occurred.
%TIME%	Time when event occurred.
%MESSAGE_ID%	Message identifier.
%SERVER%	Name of the server that encountered the event.
%SUBJECT%	Message subject.
%SENDER%	Sender of the message.
%RECIPIENTS%	Message recipients.
%JOB%	Job name, such as Transport (SMTP) scanning or Exchange store scanning.

Per incident substitution symbol	Description
%EVENT%	Incident event; for example, Infection detected.
%LOCATION%	Location where the event occurred, e.g. Body Text or Subject or Name of the attachment.
%REPLACED%	Specifies whether the location was replaced or not.
%DETAILS_TYPE%	Type of additional information, e.g. Virus name(s).
%DETAILS%	Additional information itself, e.g. "W32/Trojman".

Substitution symbols for replacement text

To ensure that PureMessage includes specific details of a virus or error event (for example, the date or the action that has been carried out) in the replacement text, use the substitution symbols below.

Symbol	Description
%EVENT%	Infected, encrypted or unscannable.

Symbol	Description
%LOCATION%	Location where the event occurred, e.g. Body Text or Subject or Name of the attachment.
%MESSAGEID%	Message identifier.
%DATE%	Date when attachment was replaced.
%TIME%	Time when attachment was replaced.
%SERVER%	Name of the server that added the replacement text.
%JOB%	The job name; Transport (SMTP) scanning or Exchange store scanning.
%DETAILS TYPE%	Type of additional information, e.g. Virus name(s).
%DETAILS%	Additional information itself, e.g. "W32/Trojman".

5.4.7 Setting up exceptions

5.4.7.1 Setting up exceptions overview

When you configure PureMessage to take action against certain kinds of mail or content, you can specify "exceptions". This means that you can exempt particular users or groups from the action, or apply a different action to them.

Sample exceptions

Here is an example of exceptions set in the anti-spam part of the Transport (SMTP) scanning policy. Imagine that you want to delete all mail identified as spam, unless it is for:

- the sales department, who need to be able to check that it is not a misidentified order.
- the CEO, whose assistant will screen all email.

To achieve this, do as follows:

1. Set the action for **On spam** to **Delete message**.
2. Click the double-arrow at the end of the On spam bar to display more options. In **Except when recipient is:** click **Add** and then click **Select users or groups**. Select the group you want. Set the action to **Quarantine message**.
3. Click **Add** again and add the CEO. Set the action to **Deliver message**.

You can also specify the order in which PureMessage deals with these exceptions. You do this by selecting the exception and clicking **Decrease priority** or **Increase priority**. The highest priority exception, i.e the one that will be applied first, is at the top of the exception list.

For more information on selecting users and groups, see Add users and groups to set up exceptions (page 32).

Note: If a message is addressed to users with different policy configurations, the message will be split and the appropriate policy will be applied to each message. For example, if a message was outbound and disclaimers were applicable to some recipient domains but not others, the message would be split into domains that take disclaimers and domains that don't.

5.4.7.2 Add users and groups to set up exceptions

When you create an exception to a policy, you need to specify the users or groups that the exception will apply to.

From the **Anti-virus**, **Anti-spam**, or **Content** screen, click the double arrow on the right side of your selected bar to create an exception policy. Click **Add**. Then click **Select users and groups**.

Click **Add** to add a user or group. The **Find users and groups (page 32)** dialog box appears. Find your user or group, and return the data to the **Users and groups** dialog box.

Click **Remove** to remove a highlighted user or group.

Note: From the **Manage changes** menu, click **Save changes** to save your configuration.

5.4.7.3 Find users and groups to set up exeptions

When you create an exception to a policy, you must specify the users or groups that the exception will apply to.

To create the exception:

From the **Anti-virus**, **Anti-spam**, or **Content** screen, click the double arrow on the right side of your selected bar to create an exception policy. Click **Add**. Then click **Select users and groups**. In the **Users and groups** dialog box, click **Add**. You are now prompted to search for users and groups.

1. In the **Search users and groups in:** list, select either **Active Directory** or **Custom users and groups**.
2. In the **Name:** field, enter the name of the person or group to search for. You can use the wildcards '*' and '?'.
3. Optionally, in the **Description:** field, enter a description to search for. You can use the wildcards '*' and '?'.
4. Click **Find Now**. A list of groups and users matching your search criteria appears in alphabetical order.
5. Highlight one or more entries and click **Add**. The selected entries are displayed in the **Users and groups** dialog box. Click **OK**.

5.5 Transport (SMTP) scanning configuration

5.5.1 Transport (SMTP) scanning configuration overview

Transport (SMTP) traffic relates to inbound, outbound, and internal mail. See inbound, outbound, and internal mail (page 5).

PureMessage offers filtering, anti-virus scanning, anti-spam scanning, and content filtering. You can set up customized policies, specifying what mail to allow, what to block, and what to manage (quarantine, delete, and so forth). You can also add a disclaimer to outbound mail.

- Filtering (page 33)
- Anti-virus (page 35)
- Anti-spam (page 36)
- Content (page 39)
- Disclaimers (page 45)

5.5.2 Filtering

5.5.2.1 Filtering overview

The **Filtering** options in PureMessage allow you to block specific senders and hosts. It also allows you to enable recipient validation which deletes mail addressed to invalid users.

Click **Configuration | Transport (SMTP) scanning** and then click **Filtering**.

- Block list (page 33)
- Recipient validation (page 34)

5.5.2.2 Block list overview

You can create and edit a customized block list of IP addresses and known bad senders. PureMessage will then block or delete messages from those hosts or senders at the SMTP transport level.

Click **Configuration | Transport (SMTP) scanning policy | Filtering** and then click **Block list**.

Host/Sender and comments display

The main panel shows a column for **Host/Sender**, which displays data that you have added. The **Comments** column is a notes field for general use.

Click **Add** to add a host or sender you want to block. The Specify host IP address or IP range or sender (page 34) dialog box appears.

Click **Remove** to remove a highlighted entry.

Click **Import** to import a list of bad hosts or senders. This list should be in CSV (comma-separated) or plain text format. A warning appears, and you can choose to replace the existing list or merge the new list with the existing list.

Click **Export** to export the block list in CSV (comma-separated) or plain text format.

Click **Advanced**. The Block list - Advanced (page 34) dialog box appears. You can decide how PureMessage rejects messages from blocked IP addresses and, optionally, specify the SMTP response string for rejected mail.

Note: From the **Manage changes** menu, click **Save changes** to save your configuration.

5.5.2.3 Specify an IP address or IP range or sender in block list

You can specify a single IP address, a range of IP addresses, or a single address to add to the block list.

Click **Configuration | Transport (SMTP) scanning policy | Filtering | Block list** and then click **Add**.

Specify an IP address or IP address range

Click **Specify an IP address or IP address range**. Enter an IP address or a range of IP addresses.

Specify sender

Click **Specify Sender**. Enter a sender address. You can use wildcards, such as '*' and '?'. E.g. *@company.com

Comment (Optional)

You can enter a comment for administrative purposes.

Note: From the **Manage changes** menu, click **Save changes** to save your configuration.

5.5.2.4 Block list - Advanced settings

You can specify how PureMessage will deal with mail from a blocked host and you can enter a response string to return at the protocol level.

Click **Configuration | Transport (SMTP) scanning policy | Filtering | Block list** and click **Advanced**.

When a blocked host connects

If a message comes from a blocked host, you can either drop the connection and return a response or drop the connection without returning a response. Returning a response with alternate contact details is recommended, so that a legitimate host if blocked by mistake can contact you.

Restore defaults

Click this button to restore the default settings.

Note: From the **Manage changes** menu, click **Save changes** to save your configuration.

5.5.2.5 Recipient validation

Recipient validation gets rid of inbound messages sent to invalid users. These messages are often spam, but occasionally they could be valid mail with a misspelled address.

Click **Configuration | Transport (SMTP) scanning policy | Filtering** and then click **Recipient validation**.

Enable Recipient Validation

If you enable recipient validation, PureMessage will only accept messages for users and groups that are present in your Active Directory or custom users/groups. Make sure you have configured your Active Directory or custom users/groups before enabling recipient validation.

Click **Restore Defaults** to revert to default settings.

Note: From the **Manage changes** menu, click **Save changes** to save your configuration.

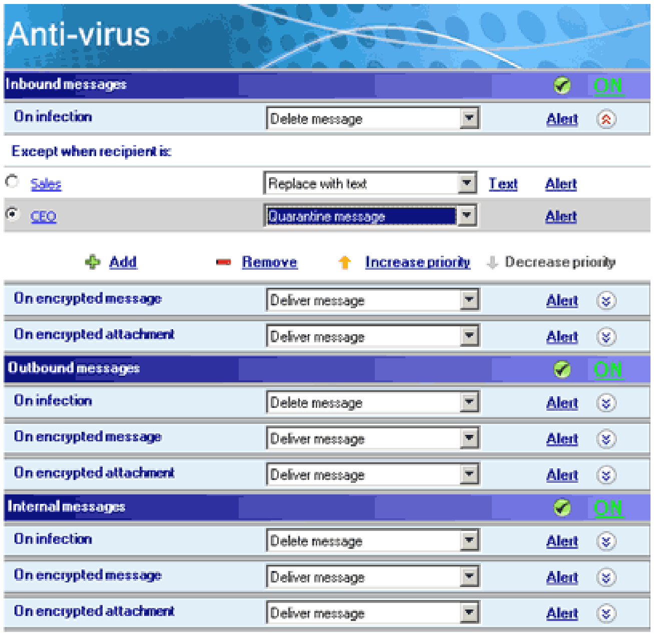
5.5.3 Anti-virus

5.5.3.1 Anti-virus overview

You can define separate **anti-virus** policies for inbound, outbound, and internal mail. See Inbound, outbound, and internal mail (page 5) in the **Key concepts** section.

You can specify what action is to be taken when PureMessage encounters infected mail or mail that is encrypted (e.g. S/MIME or PGP encrypted message) or an encrypted attachment (e.g. Password protected file). You can also specify exceptions from that rule, which have a policy of their own.

Click **Configuration | Transport (SMTP) scanning policy** and then click **Anti-virus**.



Anti-virus

Inbound messages			✓ ON
On infection	Delete message	Alert	
Except when recipient is:			
○ Sales	Replace with text	Text	Alert
● CEO	Quarantine message		Alert
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	

The screen displays types of event and the associated actions.

There are three types of events:

- Infected mail which includes mail with a virus or other malware.
- Encrypted message. Example, S/MIME or PGP encrypted.
- Encrypted attachment. Example, a password protected file.

All events have the following actions: no action, delete message, quarantine message, quarantine message and deliver, and deliver message. The events On infection, and On encrypted attachment also have the action Replace attachment with text.

By default, anti-virus scanning for inbound, outbound, and internal mail is enabled. The menu bar for each direction of mail will be blue, and the associated icon will display a checkmark and the word **ON**. If any menu bar is red, scanning for that direction of mail is disabled. Click the associated **OFF** text or circled alert icon to enable scanning.

For details of other anti-virus settings, see Change Anti-Virus settings (page 36).

5.5.3.2 Change anti-virus settings

In this dialog you can configure anti-virus settings for Transport (SMTP) scanning.

Click **Configuration | Transport (SMTP) scanning policy | Anti-virus**, and then click **Change anti-virus settings**.

Scanning level

Click **Normal (recommended)** to scan only those parts of a file that are likely to contain viruses.

Click **Extensive** to scan the complete contents of a file. Extensive scanning is usually not required and should be turned on only if recommended by Sophos technical support.

Scanning options

By default, PureMessage scans for viruses inside archive files, including ZIP, ARJ, RAR, GZIP, TAR, CMZ, and so on.

Automatic disinfection

Click **Disinfect messages that contain a virus** to attempt cleaning of infected items. Note that not all viruses can be cleaned. If PureMessage fails to clean a virus then the **On Infection** event is triggered.

Scanning Actions

Select an action from the **On unscannable** panel's **Action** list.

Optionally, check the **Alert administrator** checkbox.

Select an action from the **On application error** panel's **Action** list. The default is **Deliver message**. If you change the default action, PureMessage displays a warning. This is because if the action is set to quarantine and if PureMessage is malfunctioning then it may end up quarantining all mails that it receives. Optionally, check the **Alert administrator** checkbox.

Click **Restore defaults** to restore defaults.

Note: From the **Manage changes** menu, click **Save changes** to save your configuration.

5.5.4 Anti-spam

5.5.4.1 Anti-spam overview

The **anti-spam** options in PureMessage enable you to set policies for spam and suspected spam. You can set a global policy for each category of spam and you can also specify exceptions to that policy. These exceptions may have different actions specified for them.

Click **Configuration | Transport (SMTP) Scanning policy**, and then click **Anti-spam**.

By default, anti-spam scanning for inbound messages is enabled. The **Inbound Messages** bar is blue, and the associated icon displays a checkmark and the word **ON**. If the menu bar is red, spam scanning for inbound mail is disabled. Click the **OFF** icon or circled alert icon to enable scanning. The inbound messages bar becomes blue and the icon displays **ON**.

For details of other settings, see Change Anti-spam settings (page 37)

5.5.4.2 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. We recommend you set your ratings above 50 to avoid legitimate mail being classed as spam or suspected spam. You have the option to add the spam score as a Microsoft Spam Confidence Level (SCL) rating to the message.

Click **Configuration | Transport (SMTP) scanning policy | Anti-spam**, and then click **Change anti-spam settings**.

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.

Check the **Check reputation of message relays against external DNS block lists** checkbox. If you want to exclude certain relays from reputation checks, click **Upstream trusted relay**. See the Key concepts (page 5) section for more information. Check the **Check reputation of first external relay only** checkbox after configuring the trusted relays correctly.

To add the spam score as a SCL rating, check the **Add spam score to message as Microsoft Spam Confidence Level (SCL) rating** checkbox. Message delivered to end users with a SCL rating higher than a particular value are diverted into the users Junk mail folder in Microsoft Outlook.

Note: From the **Manage changes** menu, click **Save changes** to save your configuration.

5.5.4.3 Allow specific senders overview

Messages from allowed senders or hosts will not be scanned for spam.

Click **Configuration | Transport (SMTP) scanning policy | Anti-spam** and then click **Allow specific senders**.

Click **Add**. The **Specify an IP address or IP range or sender (page 37)** dialog box appears. In the **Specify an IP address or IP range or sender** dialog box, you can specify an IP address or IP address range, or you can enter an individual email address. The information appears in the **Host/Sender** column and, optionally, in the **Comments** column of the main panel.

Click **Edit** to edit a highlighted host or sender.

Click **Remove** to remove a highlighted host or sender.

Click **Import** to import data in plain text or CSV (comma-separated) format.

Click **Export** to export data to a file in plain text or CSV (comma-separated) format.

Note: From the **Manage changes** menu, click **Save changes** to save your configuration.

5.5.4.4 Allow specific IP address or sender

You can specify a single IP address, a range of IP addresses, or a single address to add to the allow list.

Click **Configuration | Transport (SMTP) scanning policy | Filtering | Allow list** and then click **Add**.

Specify an IP address or IP address range

Click **Specify an IP address or IP address range**. Enter an IP address or a range of IP addresses.

Specify sender

Click **Specify Sender**. Enter a sender address. You can use wildcards, such as '*' and '?'. E.g. *@company.com

Comment (Optional)

You can enter a comment for administrative purposes.

Note: From the **Manage changes** menu, click **Save changes** to save your configuration.

5.5.4.5 Block specific senders overview

You can create and edit a customized block list of IP addresses and known bad senders. PureMessage will then block or delete messages from those hosts or senders at the SMTP transport level.

Click **Configuration | Transport (SMTP) scanning policy | Anti-spam** and then click **Block specific senders**.

Host/Sender and comments display

The main panel shows a column for **Host/Sender**, which displays data that you have added. The **Comments** column is a notes field for general use.

Click **Add** to add a host or sender you want to block. The **Specify host IP address or IP range or sender (page 38)** dialog box appears.

Click **Remove** to remove a highlighted entry.

Click **Import** to import a list of bad hosts or senders. This list should be in CSV (comma-separated) or plain text format. A warning appears, and you can choose to replace the existing list or merge the new list with the existing list.

Click **Export** to export the block list in CSV (comma-separated) or plain text format.

Click **Advanced**. The **Block list - Advanced (page 39)** dialog box appears. You can decide how PureMessage rejects messages from blocked IP addresses and, optionally, specify the SMTP response string for rejected mail.

Note: From the **Manage changes** menu, click **Save changes** to save your configuration.

5.5.4.6 Block specific IP address or sender

You can specify a single IP address, a range of IP addresses, or a single address to add to the block list.

Click **Configuration | Transport (SMTP) scanning policy | Anti-spam | Block specific senders**. From the **Block list** dialog box, click **Add**.

Specify an IP address or IP address range

Click **Specify an IP address or IP address range**. Enter an IP address or a range of IP addresses.

Specify sender

Click **Specify Sender**. Enter a sender address. You can use wildcards, such as '*' and '?'. E.g. *@company.com

Comment (Optional)

You can enter a comment for administrative purposes.

Note: From the **Manage changes** menu, click **Save changes** to save your configuration.

5.5.4.7 Block specific senders - Advanced settings

You can specify how PureMessage will deal with mail from a blocked host and you can enter a response string to return at the protocol level.

Click **Configuration | Transport (SMTP) scanning policy | Anti-spam | Block specific senders** and click **Advanced**.

When a blocked host connects

If a message comes from a blocked host, you can either drop the connection and return a response or drop the connection without returning a response. Returning a response with alternate contact details is recommended, so that a legitimate host if blocked by mistake can contact you.

Restore defaults

Click this button to restore the default settings.

Note: From the **Manage changes** menu, click **Save changes** to save your configuration.

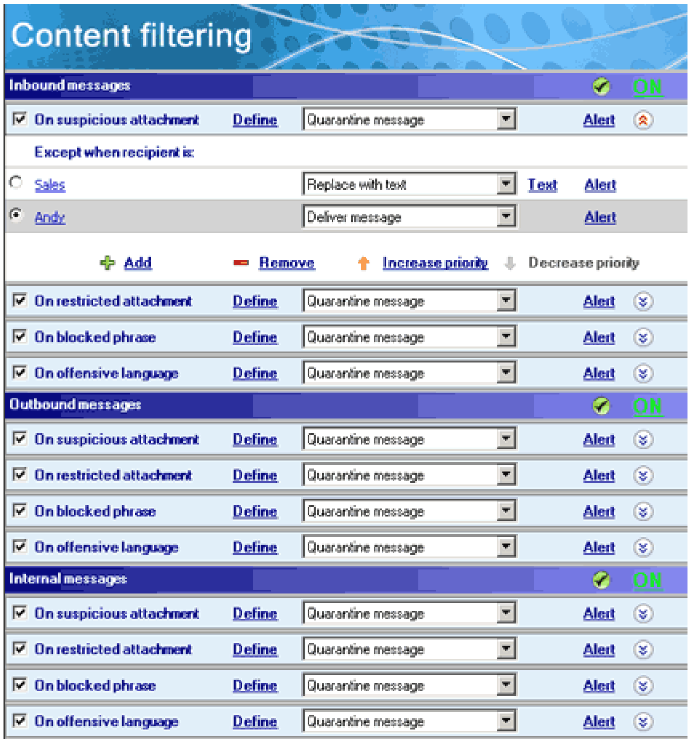
5.5.5 Content

5.5.5.1 Content overview

You can define separate **content filtering policies** for inbound, outbound, and internal mail. You can also block content based on four different events: suspicious attachment, restricted attachment, blocked phrase, or offensive language.

You need to both enable and configure content filtering. For instance, if you want to block incoming PUAs (potentially unwanted applications), you need to enable content scanning for inbound mail and configure a policy to block incoming PUAs.

Click **Configuration | Transport (SMTP) scanning policy**, and then click **Content**.



Content filtering

Inbound messages				✓ ON
☑ On suspicious attachment	Define	Quarantine message		Alert
Except when recipient is:				
○ Sales		Replace with text	Text	Alert
● Andy		Deliver message		Alert
Add	Remove	Increase priority	Decrease priority	
☑ On restricted attachment	Define	Quarantine message		Alert
☑ On blocked phrase	Define	Quarantine message		Alert
☑ On offensive language	Define	Quarantine message		Alert
Outbound messages				✓ ON
☑ On suspicious attachment	Define	Quarantine message		Alert
☑ On restricted attachment	Define	Quarantine message		Alert
☑ On blocked phrase	Define	Quarantine message		Alert
☑ On offensive language	Define	Quarantine message		Alert
Internal messages				✓ ON
☑ On suspicious attachment	Define	Quarantine message		Alert
☑ On restricted attachment	Define	Quarantine message		Alert
☑ On blocked phrase	Define	Quarantine message		Alert
☑ On offensive language	Define	Quarantine message		Alert

Enable content scanning for inbound, outbound, or internal mail as required. The menu bar for each direction of mail is blue when scanning is enabled, and the associated icon displays a checkmark and the word **ON**. If any menu bar is red, scanning for that direction of mail is disabled. Click the associated **OFF** text or circled alert icon to enable scanning.

For details of other content configuration settings, see Change content filtering settings (page 45).

5.5.5.2 On suspicious attachment name

You can add an attachment name that you consider suspicious to be blocked. These attachments would typically be used to send malicious code. By default file names with double extensions and file types listed under the **Executable** and **Object Code** sections on the **Attachment types** tab are considered suspicious. You can optionally specify a size limit (if an attachment with the relevant name exceeds the size limit, the attachment is blocked). You can also block all files with multiple extensions, and specify exceptions to that rule.

Note: This function will check the attachment name only. If the sender has altered an otherwise suspicious attachment name, PureMessage will not detect it, unless that attachment type is selected on the **Attachment types** tab.

Click **Configuration | Transport (SMTP) Scanning Policy | Content**. On the **Content filtering** screen, in the **On suspicious attachment** bar, click **Define**. In the **Suspicious attachment type** dialog box, click the **Attachment names** tab.

Click **Add** and enter an **Attachment name** that you want to block. You can use the wildcards '*' and '?', for example *.pdf. Optionally, enter a size limit in MB.

Click **Remove** to remove a highlighted attachment name and size.

Check the **Block all files with multiple extensions except** check box, click the **Add** to enter one or more exceptions if required.

Click **Edit** to edit a highlighted exception.

Click **Remove** to remove a highlighted exception.

Click **Restore defaults** to restore default settings.

Click **OK** to save your changes, and return to the **Content filtering** screen.

Note: From the **Manage changes** menu, click **Save changes** to save your configuration.

If you want to allow certain attachments from the suspicious attachments list, follow the steps in Exclude suspicious attachments from filtering (page 42).

5.5.5.3 On suspicious attachment type

You can select attachment types that you consider suspicious to be blocked. By default file names with double extensions and file types listed under the **Executable** and **Object Code** sections on the **Attachment types** tab are considered suspicious. You can optionally specify a size limit (if an attachment of the relevant type exceeds the limit, the attachment is blocked). You can also block potentially unwanted applications, and you can enter exceptions to that rule.

Note: PureMessage detects the True File Type (TFT) of the attached file and therefore even if the attachment is renamed, PureMessage will still detect the original file type.

Click **Configuration | Transport (SMTP) Scanning Policy | Content.** On the **Content filtering** screen, in the **On suspicious attachment** bar, click **Define**. In the **Suspicious attachment type** dialog box, click the **Attachment types** tab.

In the **Select attachment group** drop-down, choose an attachment category.

PureMessage is preconfigured with a list of file types that are currently used to carry threats. Check the relevant attachment type(s) to block. You can select or clear all the options by using check box on the title bar. Optionally, enter a file size limit in MB.

Optionally, select the **Block adware/potentially unwanted applications (PUAs)** check box to block adware and PUAs.

If you want to allow an application that may otherwise be blocked as an adware or PUA, click **Add** and enter the name of an application that you want to allow. For more information about adware and PUAs that Sophos detects, go to http://www.sophos.com/en-us/threat-center/threat-analyses/adware-and-puas.aspx.

Click **Edit** to edit a highlighted allowed adware/PUA.

Click **Remove**, to remove a highlighted adware/PUA from the list of allowed applications.

Click **OK** to save your changes and return to the **Content filtering** screen.

Note: From the **Manage changes** menu, click **Save changes** to save your configuration.

If you want to allow certain attachments from the suspicious attachments list, follow the steps in Exclude suspicious attachments from filtering (page 42).

5.5.5.4 Exclude suspicious attachments from filtering

If you want to allow certain attachments that would otherwise be identified as suspicious and blocked, you can exclude them from content filtering as follows.

1. Click **Configuration | Transport (SMTP) Scanning Policy | Content.** On the **Content filtering** screen, in the **On suspicious attachment** bar, click **Define**. In the **Suspicious attachment type** dialog box, click the **Excluded attachment names** tab.
2. To add or remove an attachment, or to restore default settings:
   - Click **Add** and enter an attachment name that you want to exclude from filtering. You can use the wildcards '*' and '?', for example *.pdf or abcd.*
   - Click **Remove** to remove a highlighted attachment name.
   - Click **Restore defaults** to restore default settings.
3. Click **OK** to save your changes, and return to the **Content filtering** screen.

   Note: From the **Manage changes** menu, click **Save changes** to save your configuration.

5.5.5.5 On restricted attachment name

You can add an attachment name to be blocked. These attachments could be media (music or movies) sent within an organisation, and you may have a policy of restricting or monitoring them, rather than automatically deleting them. You can optionally specify a size limit (if an attachment with the relevant name exceeds the size limit, the attachment is blocked). You can also block all files with multiple extensions, and specify exceptions to that rule.

Note: This function will check the attachment name only. If the sender has altered an otherwise restricted attachment name, PureMessage will not detect it, unless that attachment type is selected on the **Attachment types** tab.

Click **Configuration | Transport (SMTP) scanning policy | Content**. On the **Content filtering** screen, in the **On restricted attachment** bar, click **Define**. In the **Restricted attachment type** dialog box, click the **Attachment names** tab.

Click **Add** to enter an **Attachment name** to block. You can use the wildcards '*' and '?', for example *.pdf. Optionally, enter a size limit in MB.

Click **Remove** to remove a highlighted attachment name and size.

Check the **Block all files with multiple extensions except** check box,click **Add** to enter one or more exceptions if required.

Click **Edit** to edit a highlighted exception.

Click **Remove** to remove a highlighted exception.

Click **Restore defaults** to restore default settings.

Click **OK** to save your changes, and return to the **Content filtering** screen.

Note: From the **Manage changes** menu, click **Save changes** to save your configuration.

If you want to allow certain restricted attachments, follow the steps in Exclude restricted attachments from filtering (page 43).

5.5.5.6 On restricted attachment type

You can select attachment types to be blocked. You can optionally specify a size limit (if an attachment of the relevant type exceeds the limit, the attachment is blocked). You can also block potentially unwanted applications, and you can enter exceptions to that rule.

Note: PureMessage detects the True File Type (TFT) of the attached file and therefore even if the attachment is renamed, PureMessage will still detect the original file type.

Click **Configuration | Transport (SMTP) Scanning Policy | Content**. On the **Content filtering** screen, in the **On restricted attachment** bar, click **Define**. In the **Restricted attachment type** dialog box, click the **Attachment types** tab.

In the **Select an attachment group** drop-down, choose an attachment category.

PureMessage is preconfigured with a list of file types that are currently used to carry threats. Check the relevant attachment type(s) to block. You can select or clear all the options by using check box on the title bar. Optionally, enter a file size limit in MB.

Optionally, select the **Block adware/potentially unwanted applications (PUAs)** check box to block adware and PUAs.

If you want to allow an application that may otherwise be blocked as an adware or PUA, click **Add** and enter the name of an application that you want to allow. For more information about adware and PUAs that Sophos detects, go to http://www.sophos.com/en-us/threat-center/threat-analyses/adware-and-puas.aspx.

Click **Edit** to edit a highlighted allowed adware/PUA.

Click **Remove**, to remove a highlighted adware/PUA from the list of allowed applications.

Click **OK** to save your changes and return to the **Content filtering** screen.

Note: From the **Manage changes** menu, click **Save changes** to save your configuration.

If you want to allow certain restricted attachments, follow the steps in Exclude restricted attachments from filtering (page 43).

5.5.5.7 Exclude restricted attachments from filtering

If you want to allow certain restricted attachments, you can exclude them from content filtering as follows.

1. Click **Configuration | Transport (SMTP) Scanning Policy | Content**. On the **Content filtering** screen, in the **On restricted attachment** bar, click **Define**. In the **Restricted attachment type** dialog box, click the **Excluded attachment names** tab.
2. To add or remove an attachment, or to restore default settings:
   - Click **Add** and enter an attachment name that you want to exclude from filtering. You can use the wildcards '*' and '?', for example *.pdf or abcd.*
   - Click **Remove** to remove a highlighted attachment name.
   - Click **Restore defaults** to restore default settings.
3. Click **OK** to save your changes, and return to the **Content filtering** screen.

   Note: From the **Manage changes** menu, click **Save changes** to save your configuration.

5.5.5.8 On blocked phrase

You can enter or import specific phrases to be blocked. You can also search within the subject line, body text, and attachments and choose to take action only when a specified number of phrases are detected. On the **String** tab you can enter phrases that use wildcards such as '*' and '?'. On the **Regular expression** tab you can enter search strings using regular expressions. When PureMessage checks mail for blocked phrases, it will use both lists.

Click **Configuration | Transport (SMTP) scanning policy | Content**. On the **Content filtering** screen, in the **On blocked phrase** bar click **Define**.

Note: If you have configured the action to be **Replace with text**, none of the original mail text is displayed.

Phrase type

Click the **String (wildcards supported)** tab and enter a string, optionally using the wildcards "*" and "?". Select which areas of mail you want PureMessage to search.

Click the **Regular expression** tab if you want to enter a regular expression.

Click **Add**, enter the phrase on a single line, and check the relevant check box(es) to specify where PureMessage is to search for that phrase.

Click **Remove** to remove a highlighted phrase.

Click **Import** to import phrases from a plain text or CSV file.

Click **Export** to export phrases to a plain text or CSV file.

Optionally, check the **Take action only when specified number of phrases are detected** check box, and enter the number in the accompanying box.

Click **OK** to save your changes and return to the **Content filtering** screen.

Note: From the **Manage changes** menu, click **Save changes** to save your configuration.

5.5.5.9 On offensive language

You can enter or import specific phrases that you consider offensive to be blocked. You can also search within attachments and choose to take action only when a specified number of phrases are detected.

Note: PureMessage comes with a suggested list of offensive terms, entered as regular expressions.

Click **Configuration | Transport (SMTP) scanning policy**, and then click **Content**. On the **Content filtering** screen, in the **On offensive language** bar, click **Define**.

Note: If you have configured the action to be **Replace with text**, none of the original mail text is displayed.

Phrase type

Click the **String (wildcards supported)** tab and enter a string, optionally using the wildcards "*" and "?". Select which areas of mail you want PureMessage to search.

Click the **Regular expression** tab if you want to enter a regular expression.

Click **Add**, enter the phrase on a single line, and check the relevant check box(es) to specify where PureMessage is to search for that phrase.

Click **Remove** to remove a highlighted phrase.

Click **Import** to import phrases from a plain text or CSV file.

Click **Export** to export phrases to a plain text or CSV file.

Optionally, check the **Take action only when specified number of phrases are detected** check box, and enter the number in the accompanying box.

Click **OK** to save your changes and return to the **Content filtering** screen.

Note: From the **Manage changes** menu, click **Save changes** to save your configuration.

5.5.5.10 Change content filtering settings

The **Change content filtering settings** option allows you to enable searching of phrases within archive files.

Click **Configuration | Transport (SMTP) scanning policy | Content**, and then click **Change content filtering settings**.

In the **Content filtering settings** dialog box, check the **Search phrases within archive files** check box.

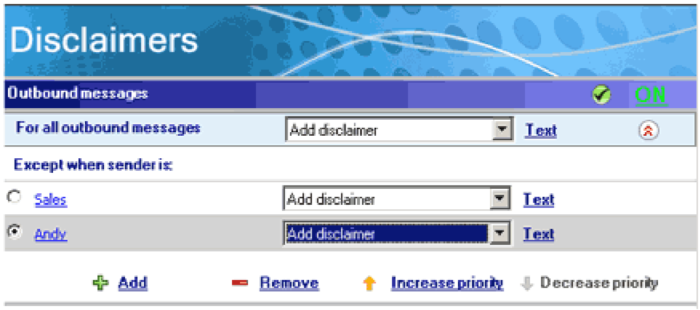
Note: From the **Manage changes** menu, click **Save changes** to save your configuration.

5.5.6 Disclaimers

5.5.6.1 Disclaimers overview

The **Disclaimers** option in PureMessage enables you to add specified disclaimer text to outgoing messages. Moreover, you can set up different disclaimers for specific groups within your company.

Click **Configuration | Transport (SMTP) Scanning Policy**, and then click **Disclaimers**.



For all outbound messages: Add disclaimer — Text

○ Sales: Add disclaimer — Text

● Andy: Add disclaimer — Text

Outbound Messages

On the Outbound messages bar, click the **ON/OFF** button so that **ON** is displayed.

For all Outbound Messages

Select an option from the **For all Outbound Messages** list. This option is then the overall policy for outbound mail. You can choose between **Add disclaimer** and **Do not add disclaimer**. For this example, select **Add disclaimer**.

Click **Text** to access the Disclaimer (page 46) dialog box, from which you can edit your disclaimer.

Except when sender is

The **Except when sender is** panel allows you to exempt select users/groups from the actions in the overall disclaimer policy and give them actions of their own.

Click the double arrow to the right of the **For all Outbound Messages** bar to display the **Except when sender is** panel. The panel displays any exception policies you have created.

Add and **Remove** buttons

Click **Add** to add a new exception rule to the **Except when sender is** panel. Click **Remove** to remove the highlighted exception from the list.

Increase priority and **Decrease priority** buttons

You can also specify the order in which PureMessage deals with these exceptions. You do this by selecting the exception and clicking Decrease priority or Increase priority. The highest priority exception, i.e the one that will be applied first, is at the top of the exception list.

You can also Change Disclaimer Settings (page 46).

5.5.6.2 Add a disclaimer

You can write or edit a **disclaimer** and specify whether to put it on the top or bottom of outgoing mail.

Click **Configuration | Transport (SMTP) Scanning Policy**, and then click **Disclaimers**. In the **Disclaimers** screen, select **Add disclaimer** in the event bar, and click **Text**.

Disclaimer location

Select an option from the **Disclaimer location** list to select **Top** or **Bottom**.

Text Version

Enter your disclaimer in plain text.

HTML Version

Enter your disclaimer using HTML. Click **Preview** to view your HTML disclaimer.

When specifying HTML disclaimer text, do not specify the <HTML> or <BODY> tags.

Note: From the **Manage changes** menu, click **Save changes** to save your configuration.

5.5.6.3 Change disclaimer settings

You can configure a list of external domains to which disclaimers should not be added.

Click **Configuration | Transport (SMTP) Scanning Policy**, and then click **Disclaimers**. On the **Disclaimers** screen, select **Change disclaimer settings**.

Click **Add** to add a new domain name. You can use the wildcards '*' and '?'. E.g. ***.company.com**.

Click **Edit** to edit a highlighted domain name.

Click **Remove** to remove a highlighted domain name.

Note: From the **Manage changes** menu, click **Save changes** to save your configuration.

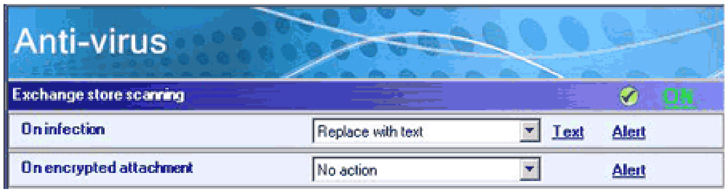
5.6 Exchange store scanning configuration

5.6.1 Exchange store scanning configuration overview

Exchange store scanning scans mail in your mailboxes and public folders and allows you to run background store scanning.

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

Click **Configuration**, and then click **Exchange store scanning policy**.



On infection: Replace with text

On encrypted attachment: No action

By default, Exchange store scanning is enabled. The **Exchange store scanning** bar is blue, the associated icon displays a checkmark and the word **ON**. If the menu bar is red, Exchange store scanning is disabled. Click the **OFF** icon or circled alert icon to enable scanning. The Exchange store scanning bar becomes blue, and the icon displays **ON**

On infection

Select an action from the **On infection** list. This action becomes the policy for infected mail.

If you select **Replace attachment with text** as your action, the **Text** link appears. Click **Text** to access the **Replacement text** dialog box. Edit the replacement text and return to the **Exchange store scanning** dialog box. See Replacement Text (page 29).

Optionally, click **Alert** to specify whether to send an alert if a policy rule is applied. For more information, see Setting up alerts (page 29).

On encrypted attachment

Select an action from the **On encrypted attachment** list. This action becomes the policy when PureMessage encounters mail with an encrypted attachment such as a password protected file.

From the **Actions** menu, click **Change Exchange store scan settings (page 47)** to configure scanning level and options.

5.6.2 Enable scanning of Exchange stores

You can configure PureMessage on Exchange Server 2013 to run background scans at scheduled times on both the private and public stores. Background scanning checks all items in the store.

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

Click **Configuration | Exchange store scanning policy | Change Exchange store scan settings** and then click the **Stores** tab.

Exchange private store

Select the **Enable background scanning** check box to enable background scanning of Exchange private store.

Exchange public store

Select the **Enable background scanning** check box to enable background scanning of Exchange public store.

Enable background scanning only for out of working hours

Select the **Enable background scanning only for out of working hours** check box and enter your company's working days and times. PureMessage will run background scanning outside of these hours.

Note: From the **Manage changes** menu, click **Save changes** to save your configuration.

To set the Exchange store scanning level, click the **Scan** tab. For information, see Change Exchange store scanning options (page 48).

Note: Do not schedule scans for times when backups of the Exchange server are being made. If you do, it may impact the performance of your server when backup operations are in progress.

5.6.3 Change Exchange store scanning options

You can use the **Scan** page to specify a level of scanning, set automatic disinfection, and configure actions for certain events.

Click **Configuration | Exchange Store Scanning Policy | Change Exchange store scan settings**, and then click the **Scan** tab.

Scanning level

Select **Normal (Recommended)** or **Extensive**. Normal scanning checks only those parts of a file that are likely to contain viruses whereas extensive scanning checks the complete contents of the file. Extensive scanning is usually not required and should be turned on only if recommended by Sophos technical support.

Scanning options

By default, **Scan inside archive files** is enabled.

Automatic disinfection

Click **Disinfect messages that contain a virus** to attempt cleaning of infected items. Note that not all viruses can be cleaned. If PureMessage fais to clean a virus then the **On Infection** event is trigerred.

Scanning actions

On unscannable

Select an action from the **Action:** list, and optionally, check the **Alert Administrator** checkbox.

By default, **Alert administrator on application error** is enabled; however if the number of application errors exceeds a certain number in a particular period, application error alerts will be disabled briefly, until the rate falls to a more manageable level.

Note: From the **Manage changes** menu, click **Save changes** to save your configuration.

6 Quarantine

6.1 Quarantine overview

The **Quarantine** screen displays quarantined messages, offers a sophisticated search engine to enable you to view and sort your data, and also offers an **Actions** menu to manage selected data.

You can view, sort, and manage your quarantined mail and tell users about quarantined spam and suspected spam.

- Managing quarantined items (page 49)
- Delivering quarantined items (page 50)
- Submit an item to Sophos for analysis (page 50)
- Enabling users to access quarantined spam (page 51)

6.2 Managing quarantined items

The **Quarantine** screen displays quarantined messages, offers a sophisticated search engine to enable you to view and sort your data, and offers an **Actions** menu to manage selected data.

Click **Quarantine**.

Message view

The main panel (**Message view**) displays the quarantined mail, which meets the criteria specified in the **Search Quarantine** panel.

Double-click a message to view further details about why PureMessage quarantined it. The **Message details** dialog box displays the reason for quarantine, email properties and source. (This feature is not available if you have selected more than one message).

You can re-order the columns and PureMessage will retain this order, even when the administration console is closed and re-opened. The columns include server name, message identifier, time, sender, recipients, subject, spam score etc. By default, when you visit the Message view for the first time, messages from all servers are displayed for the current day and are sorted according to time (latest first).

Search quarantine

You can search for messages based on subject, sender, recipients, message ID, and reason for quarantine, or any combination of these parameters. The text fields support wildcards "*****" and "**?**".

Enter dates in the **To** and **From** fields to filter messages within a particular date range. If you only enter a date in the **From** field, messages are displayed from this date onwards.

Select a **Server** from the list or accept the default **All servers**. Each server listed will be in the PureMessage group.

Select a **Sort by** option from the list to sort your data.

Actions

In the **Actions** panel, select an option from the **What would you like to do with the selected message?** list. You can view email details, delete mail, delete any viral attachments, disinfect, deliver, or submit the email to Sophos for analysis.

Note: In the event of the SQL database being unavailable, you may not see all the quarantined items in the message view. If the SQL database fails, quarantined items are queued as files. Once the database becomes available, these queued files will be entered into the quarantine database by a scheduled task (Sophos-PureMessage-QuarResubmitTask). You can run this scheduled task manually or you can wait for it to re-enter data at a scheduled time each day.

6.3 Delivering quarantined items

You can specify whether to deliver a quarantined message to its original intended recipients and/or deliver it to a user-specified list of email recipients.

Click **Quarantine**, search and select the required messages and in the **Actions** panel, select **Deliver/Forward** from the **What would you like to do with the selected message?** list.

Release from quarantine

Check the **Deliver message(s) to intended recipients** checkbox. The mail will be delivered as originally intended.

Alternatively, check the **Deliver message(s) to specified recipients (comma separated multiple addresses)** checkbox. Enter the recipients in the text box underneath.

Optionally you can check the **Automatically delete message(s) from quarantine after delivery** checkbox.

Check the **Add sender to allowed list (skip spam scanning for this sender)** checkbox, if you trust the sender.

Note: From the **Manage changes** menu, click **Save changes** to save your configuration.

6.4 Submitting a quarantined item to Sophos

When you submit a quarantined item to Sophos for analysis, please state your reason.

Click **Quarantine**, search and select the required messages and in the **Actions** panel, select **Submit to Sophos** from the **What would you like to do with the selected message?** list.

Reason for submission

Select a reason for submission. The file may be suspicious, or it may be mail that you believe the PureMessage spam filter has wrongly classified.

Enter additional comments if appropriate.

6.5 Enabling end users to access quarantined spam

6.5.1 Enabling end users to access quarantined spam overview

You can let end users know that they have spam email in the quarantine and enable them to access it.

- Setting up spam digest emails (page 51)
- End-user access to the web-based spam quarantine (page 51)
- How does a user deal with quarantined spam? (page 52)

6.5.2 Setting up spam digest emails

You can let end users know that they have spam email in the quarantine.

This is achieved by configuring PureMessage to send end users a spam digest email at a regular time each day. PureMessage sends the spam digest only if an end user has an item of spam in quarantine.

The spam digest email provides a direct link to the end-user spam quarantine website. End-users can also access the website directly at anytime by visiting the quarantine digest web page. See Direct end user access to the web based spam quarantine (page 51).

To set up spam digest emails and specify when they are sent, do as follows.

Click **Configuration|Users and Groups** and then click **End user spam digest Email**.

Enter a subject in the **Digest Subject** box.

Enter the body of the digest text in the **Digest Body Text** panel. Right-click to view available substitution symbols.

Send digests on

Enter the time(s) and days(s) you want to send digests out. You can send digests out up to twice a day.

Click **Restore Defaults** to restore default settings.

Note: From the **Manage changes** menu, click **Save changes** to save your configuration.

6.5.3 End-user access to the web-based spam quarantine

If you use Active Directory, the users can visit the spam quarantine web page directly, using a web browser, 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 spam quarantine website. By default this is set to port 8081.

When the user accesses the page, Internet Information Services (IIS) will authenticate them using Windows Authentication. If the users are requested to enter their Active Directory credentials, they should enter their username in the format domain\username.

If the user's Active Directory account owns multiple email addresses, the quarantine for that account will show email messages from all the corresponding addresses.

6.5.4 How does a user deal with quarantined spam?

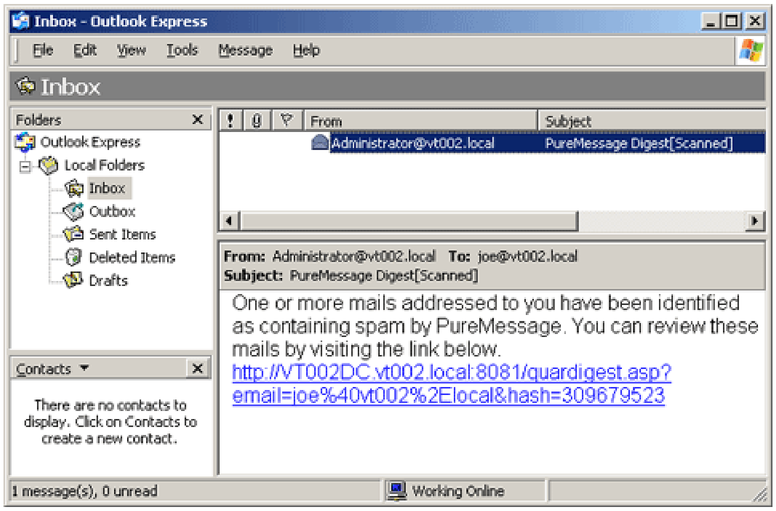
Note: This section is intended for end users. You can distribute the contents within your organisation as instructions.

This section tells you how to view your quarantined email via the PureMessage quarantine website. From this site, you can delete email you consider to be spam or retrieve email you consider to be genuine.

Viewing your quarantined email

You can access the PureMessage quarantine website either by following the link in a quarantine digest email or, if your organisation uses Active Directory, you can access the website directly from your web browser (such as Internet Explorer).

When you are sent email which qualifies as spam or suspected spam, it is held on the PureMessage server and available to view via the quarantine website. Your System Administrator sends you notification that this has happened, in the form of a digest email (example shown below).

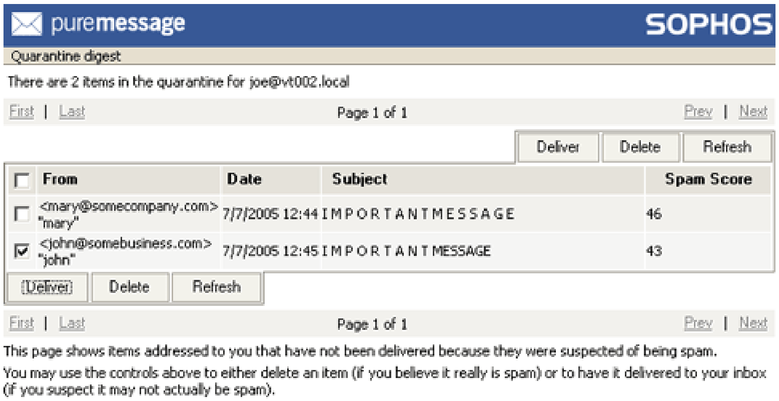


There are no contacts to display. Click on Contacts to create a new contact.

From: Administrator@vt002.local **To:** joe@vt002.local
Subject: PureMessage Digest[Scanned]

One or more mails addressed to you have been identified as containing spam by PureMessage. You can review these mails by visiting the link below.
http://VT002DC.vt002.local:8081/quardigest.asp?email=joe%40vt002%2Elocal&hash=309679523

Click on the link in the email to access the PureMessage quarantine website and view your quarantined email.



There are 2 items in the quarantine for joe@vt002.local

☐	From	Date	Subject	Spam Score
☐	<mary@somecompany.com> "mary"	7/7/2005 12:44	IMPORTANTMESSAGE	46
☑	<john@somebusiness.com> "john"	7/7/2005 12:45	IMPORTANT MESSAGE	43

This page shows items addressed to you that have not been delivered because they were suspected of being spam.

You may use the controls above to either delete an item (if you believe it really is spam) or to have it delivered to your inbox (if you suspect it may not actually be spam).

Alternatively, if your organisation uses Active Directory, you can access the quarantine website from your web browser. In the **Address** bar, enter the quarantine website address, which can be provided by your System Administrator, in the format

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 (the port is usually 8081).

You may be requested to enter your Active Directory credentials. Enter your username in the format domain\username. If you aren't sure of your Active Directory credentials, ask your System Administrator for help.

If your Active Directory account owns multiple email addresses, the quarantine digest for your account will show email messages from all the corresponding addresses.

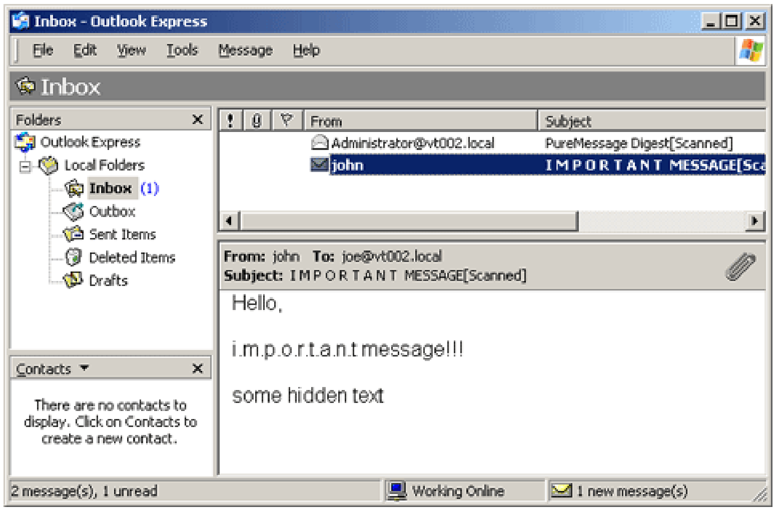
For assistance, contact your System Administrator.

Retrieving or deleting your quarantined email

If you have many pages of quarantined items, then you can use the **First** and **Last** links to quickly go to the first and last pages of your items. Click **Prev** to go to the previous page, or **Next** to access the next page.

Select the email(s) shown on the PureMessage quarantine website and click **Delete** or **Deliver** as appropriate. Click **Refresh** to refresh the screen.

If you deliver an email then it will arrive in your inbox as shown below.



From	Subject
Administrator@vt002.local	PureMessage Digest[Scanned]
john	I M P O R T A N T MESSAGE[Sca

From: john **To:** joe@vt002.local
Subject: I M P O R T A N T MESSAGE[Scanned]

Hello,

i.m.p.o.r.t.a.n.t message!!!

some hidden text

2 message(s), 1 unread

7 Reporting

7.1 Reporting overview

The **Reporting** options in PureMessage allow you to configure and generate a number of different types of report.

- Generating reports (page 55)
- Setting up reports (page 56)

7.2 Generating reports

You can configure and generate a variety of reports in a number of formats.

Click **Reports**.

The reports are grouped by category, so for example within the category filtering you will find the reports for Top blocked hosts and Top blocked senders. You can then add other criteria to specify the server(s) involved, the type and direction of the data, the output format, and configure the report schedule.

Generate report

To generate a report, follow these steps.

1. Select a category from the **Category** list. These include message trends, filtering, anti-virus, anti-spam, content, and quarantine.
2. Select a report from the **Report** list. The report options vary depending on the category selected.
3. Select or enter a number between 1 and 100 from the **Top** list, indicating how many results you want. If you were to run a report on blocked senders and you enter "25" in the **Top** list, you would be creating a report on the top 25 blocked senders.
4. From the **Server** list, select a single server, each server, or all servers.
5. Select a job from the **Job** list, such as SMTP, Exchange store, or all jobs.
6. Select a direction from the **Direction** list, such as inbound, outbound, internal or all.
7. Select a format from the **Format** list, such as pie, bar, line, ribbon or table. The report will be displayed in the selected format.
8. Select a time scale from the **Reporting Period** list, or select a range of dates from the **From** and **To** lists.
9. Click **Generate Report**.

Click **Export** to export the report to disk as a .csv or .html file.

Click **Print** to print the report.

Note: CSV (short for "comma-separated values," another name for the comma-delimited format) is a type of data format in which each piece of data is separated by a comma. This is a popular format for transferring data from one application to another, because most database systems are able to import and export comma-delimited data. For example, a .csv file can be imported into Microsoft Excel for further analysis.

7.3 Configuring collection of report data

Click **Reports**.

In the right side **Configuration** pane, click **Change report settings**.

In the **Report Settings** dialog box, ensure the **Enable data collection for reports** checkbox is checked.

Enter the number of days to keep the reporting data in the database.

Click **Purge now** to delete any reporting data older than the specified number of days.

Click **Restore Defaults** to restore the default settings.

Note: From the **Manage changes** menu, click **Save changes** to save your configuration.

8 Appendixes

8.1 Appendix A: Using an Exchange Edge Transport server for attachment filtering

If you don't want to expose your Mailbox servers directly to the internet, you can use an Edge Transport server in your perimeter network. The Edge Transport server role is available in Microsoft Exchange Server 2013 Service Pack 1 (SP1) or later, Exchange Server 2010, and Exchange Server 2007. You can continue to use an existing or install a new Exchange Server 2007, Exchange Server 2010, or Exchange Server 2013 (SP1 or later) Edge Transport server. For more information, see Use an Exchange 2010 or 2007 Edge Transport server in Exchange 2013 or Install the Exchange 2013 Edge Transport role using the Setup wizard.

In an Exchange Edge Transport server, the Attachment Filtering agent is available by default. The agent filters out email messages based on file name and email content type. As a consequence, emails containing certain attachments may not reach PureMessage (and their intended recipients) in their original form. This could affect the detected viruses, content or spam score that PureMessage detects for that message.

The Exchange Attachment Filtering agent also performs searches inside archive files. The default list of attachment content types and file names affected is:

Content types

- application/x-msdownload
- message/partial
- text/scriptlet
- application/prg
- application/msaccess
- text/javascript
- application/x-javascript
- application/javascript
- x-internet-signup
- application/hta

File names

*.xnk *.wsh *.wsf *.wsc

*.vbs *.vbe *.vb *.url

*.shs *.shb *.sct *.scr

*.scf *.reg *.prg *.prf

*.pif *.pcd *.ops *.mst

*.msp *.msi *.psc2 *.psc1

*.ps2 *.ps11 *.mdb *.ps11xml

*.ps1 *.msc *.mdz *.ps1xml

*.mdw *.mdt *.mde *.ps2xml

*.mda *.lnk *.ksh *.jse

*.js *.isp *.ins *.inf

*.hta *.hlp *.fxp *.exe

*.csh *.crt *.cpl *.com

*.cmd *.chm *.bat *.bas

*.asx *.app *.adp *.ade

The Exchange Attachment Filtering agent can be configured using the Exchange Management Shell.

To view the Attachment Filtering agent configuration, use:

```
Get-AttachmentFilterListConfig
```

To view a complete list of all file name extensions and content types affected, run the following command:

```
Get-AttachmentFilterEntry | FL
```

To disable the Exchange Attachment Filtering agent, use the following command:

```
Disable-TransportAgent "Attachment Filtering Agent"
```

For more information about Attachment Filtering agent cmdlets, see Anti-spam and anti-malware cmdlets (Anti-Spam cmdlets > Attachment Filtering cmdlets on Edge Transport servers).

For more information about attachment filtering, see Attachment filtering on Edge Transport servers.

8.2 Appendix B: Configuring PureMessage with AD LDS (using AdamSync)

AdamSync is a tool that allows an instance of Active Directory Lightweight Directory Services (AD LDS) to be synchronized with Active Directory (AD). It is intended primarily to be used to copy recipient information from AD to an instance of AD LDS that has been installed with an Exchange server in an Edge Transport server role. Such a server will usually be in a perimeter network (DMZ), where direct access to AD is blocked by the firewall. AdamSync is run from inside the firewall, where it has access to AD, and pushes data to AD LDS through a port that has been opened in the firewall.

The complete set of steps required to set up AdamSync manually are as follows:

1. Install AD LDS.
2. From the desktop, click **Start | All programs | Administrative Tools | Active Directory Lightweight Directory Services** to create an AD LDS instance.
   a. In the **Welcome** dialog box, click **Next**.

b. In the **Setup Options** dialog box, select **A unique instance** and click **Next**.
c. In the **Instance Name** dialog box, select the default name **Instance 1** and click **Next**.
d. In the **Ports** dialog box, select the default ports for LDAP (389) and SSL (636) and click **Next**.
e. In the **Application Directory Partition** dialog box, select **Yes create an application directory partition** and enter the name of the partition. To avoid confusion, keep the partition name the same as the partition name in Active Directory, e.g. dc=jazz,dc=sophos,dc=com
f. In the **File Locations** dialog box, accept the default locations and click **Next**.
g. In the **Service Account Selection** dialog box, select the option **This account** and specify the administrator account name and password.
h. In the **Active Directory Lightweight Directory Services Setup Wizard** dialog box, select **Yes** to add permission for the selected account to run as a service.
i. In the **AD LDS Administrators** dialog box, add the currently logged in user (the default) and click **Next**.
j. In the **Importing LDIF Files** dialog box, add the **MS-InetOrgPerson.LDF, MS-User.LDF** and **MS-UserProxy.LDF** as schemas to be imported and click **Next**.
k. Verify the settings and click **Next** to create an instance of AD LDS.
l. After the instance is created, click **Finish** to exit the wizard.

3. The schema of the AD LDS instance must be extended to allow synchronization information to be stored. From the command prompt, go to the folder **C:\Windows\ADAM** and use the command:

```
ldifde -i -f ms-AdamSyncMetaData.ldf -s localhost:389 -c
"cn=configuration, dc=x" #configurationNamingContext
```

The schema must also be extended to accept the attributes present on the AD objects being synchronized. The above command should be repeated using the file **MS-AdamSchemaW2K3.ldf**.

4. Make a copy of the file **MS-AdamSyncConf.xml** called **Conf.xml** and open it for editing in Notepad.exe.

a. The **<source-ad-name>** element value should be set to the AD server name
b. The **<source-ad-partition>** element value must be set to the AD partition name, e.g. dc=jazz,d=sophos,dc=com
c. The **<base-dn>** element value must be modified so that it points to the users container with AD E.g. cn=users,dc=jazz,dc=sophos,dc=com
d. The **<target-dn>** element value must be set to the name of the partition created in step 2.
e. Change the **<object-filter>** element value to the following string **(|(objectclass=user) (objectclass=group) (objectclass=contact))**
f. By default, several attributes are excluded from synchronization by the <exclude> elements. Add the following attributes to the list:

```
<exclude>homeMTA</exclude>
<exclude>homeMDB</exclude>
<exclude>mDBUseDefaults</exclude>
<exclude>mailNickname</exclude>
<exclude>msExchHomeServerName</exclude>
<exclude>msExchMailboxSecurityDescriptor</exclude>
<exclude>msExchUserAccountControl</exclude>
```

```
<exclude>msExchMailboxGuid</exclude>
<exclude>msExchPoliciesIncluded</exclude>
<exclude>msExchRecipientDisplayType</exclude>
<exclude>msExchVersion</exclude>
<exclude>msExchRecipientTypeDetails</exclude>
<exclude>legacyExchangeDN</exclude>
<exclude>showInAddressBook</exclude>
<exclude>msNPAllowDialin</exclude>
<exclude>msExchUserCulture</exclude>
```

5. Install the configuration file by using the following command:

   ```
   adamsync /i localhost:389 Conf.xml
   ```

6. Perform synchronization by using the following command:

   ```
   adamsync /sync localhost:389 "dc=jazz,dc=sophos,dc=com" /log log.txt
   ```

   Important: Check the log.txt file to see if there were any errors.

   If the operation was successful then at the end of the log file you will notice text similar to:

   ```
   Finished (successful) synchronization run

   Number of entries processed via dirSync: 46

   Number of entries processed via ldap: 0

   Processing took 0 seconds (0,0).

   Beginning again run

   Aging requested every 0 runs. We last aged 1 runs ago.

   Saving Configuration File on dc=jazz,dc=sophos,dc=com

   Saved configuration file
   ```

   If you notice an error such as "ldap_add_sw: No such attribute" or "ldap_add_sw: Object class violation" then exclude the offending attributes listed in the log file one by one in conf.xml (as described in step 4.6). Each time you add an attribute for exclusion, reinstall the configuration by running:

   ```
   adamsync /d localhost:389 "dc=jazz,dc=sophos,dc=com"
   ```

   Repeat steps 5 and 6.

   Synchronization can be performed from any computer on the network, provided it has access to AD and to AD LDS through the configured LDAP port. Synchronization is incremental, and will only include changes made since the last synchronization was performed.

7. Connect to AD LDS using ADSIEdit and check if all objects have been imported correctly. Note that this synchronization was a one time operation and step 6 needs to be repeated whenever changes are made to Active Directory so that the changes get synchronized with AD LDS.
8. To configure PureMessage with AD LDS, open the PureMessage administration console and go to **Configuration | Users and groups | Active Directory**.

   a. Enter the name of the server where AD LDS is installed and specify the port number as 389.

b. The BaseDN for users and groups should be set to the name of the AD LDS partition created in step 2.
c. The Name attribute should be **name**, the Email attribute should be **mail**, the Email alias attribute should be **proxyaddresses** and the Description attribute should be **description**.
d. Specify the logon credentials and click **Verify settings**.
e. Click **Synchronize now** to synchronize data between AD LDS and PureMessage, and click **OK**.

9 Help and information

The **Help and information** screen displays information about each server in the PureMessage group. You can also access the help file and visit the Sophos web site for more information and technical support.

Click **Help and information**.

Help topics

Click **Help topics** to launch the PureMessage help file in a separate window.

Sophos online

Click **Visit Sophos website** to open your default browser and access the home page of the Sophos website.

Click **Go to Sophos threat library** to open your default browser and access the Sophos threat library, where you can browse for general information and find specific information about hoaxes, scams, viruses, and other threats, all catalogued by name.

Click **Sophos technical support** to open your default browser and access the Sophos support page, where you can download the latest products and documentation and search the knowledgebase (further help articles).

Product information

When you contact support, you will need to supply them with sufficient information to identify yourself, such as your company name, Sophos license number, Sophos username supplied to you when you bought the product, as well as product information. The product information required is displayed in the **Product information** panel.

Click **Copy** to copy the product information to the clipboard.

Click **Print** to print the product information.

Click **Export** to export the product information onto your disk in plain text format (TXT).

10 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.aspx.
- Open a ticket with our support team at https://secure2.sophos.com/support/contact-support/support-query.aspx.

11 Legal notices

Common Public License

The Sophos software that is referenced in this document includes or may include some software programs that are licensed (or sublicensed) to the user under the Common Public License (CPL), which, among other rights, permits the user to have access to the source code. The CPL requires for any software licensed under the terms of the CPL, which is distributed in object code form, that the source code for such software also be made available to the users of the object code form. For any such software covered under the CPL, the source code is available via mail order by submitting a request to Sophos; via email to support@sophos.com or via the web at http://www.sophos.com/en-us/support/contact-support/contact-information.aspx. A copy of the license agreement for any such included software can be found at http://opensource.org/licenses/cpl1.0.php

crt

$FreeBSD$
@(#)COPYRIGHT 8.2 (Berkeley) 3/21/94

The compilation of software known as FreeBSD is distributed under the following terms:

Copyright (c) 1992-2013 The FreeBSD 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.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR AND CONTRIBUTORS "AS IS" AND ANY EXPRESS 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 AUTHOR OR 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)

The developmental work of Programming Language C was completed by the X3J11 Technical Committee.

The views and conclusions contained in the software and documentation are those of the authors and should not be interpreted as representing official policies, either expressed or implied, of the Regents of the University of California.

NOTE: The copyright of UC Berkeley's Berkeley Software Distribution ("BSD") source has been updated. The copyright addendum may be found at fttp://ftp.cs.berkeley.edu/pub/4bsd/README.Impt.License. Change and is included below.

July 22, 1999

To All Licensees, Distributors of Any Version of BSD:

As you know, certain of the Berkeley Software Distribution ("BSD") source code files require that further distributions of products containing all or portions of the software, acknowledge within their advertising materials that such products contain software developed by UC Berkeley and its contributors.

Specifically, the provision reads:

"3. All advertising materials mentioning features or use of this software must display the following acknowledgement: This product includes software developed by the University of California, Berkeley and its contributors."

Effective immediately, licensees and distributors are no longer required to include the acknowledgement within advertising materials. Accordingly, the foregoing paragraph of those BSD Unix files containing it is hereby deleted in its entirety.

William Hoskins
Director, Office of Technology Licensing
University of California, Berkeley

dtoa.c

The author of this software is David M. Gay.

Copyright © 1991, 2000 by Lucent Technologies.

Permission to use, copy, modify, and distribute this software for any purpose without fee is hereby granted, provided that this entire notice is included in all copies of any software which is or includes a copy or modification of this software and in all copies of the supporting documentation for such software.

THIS SOFTWARE IS BEING PROVIDED "AS IS", WITHOUT ANY EXPRESS OR IMPLIED WARRANTY. IN PARTICULAR, NEITHER THE AUTHOR NOR LUCENT MAKES ANY REPRESENTATION OR WARRANTY OF ANY KIND CONCERNING THE MERCHANTABILITY OF THIS SOFTWARE OR ITS FITNESS FOR ANY PARTICULAR PURPOSE.

IEEE Software Taggant Library

This software was developed by The Institute of Electrical and Electronics Engineers, Incorporated (IEEE), through the Industry Connections Security Group (ICSG) of its Standards Association. Portions of it include software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/), and those portions are governed by the OpenSSL Toolkit License.

IEEE License

Copyright (c) 2012 IEEE. 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 IEEE Industry Connections Security Group (ICSG)".

4. The name "IEEE" must not be used to endorse or promote products derived from this software without prior written permission from the IEEE Standards Association (stds.ipr@ieee.org).
5. Products derived from this software may not contain "IEEE" in their names without prior written permission from the IEEE Standards Association (stds.ipr@ieee.org).
6. Redistributions of any form whatsoever must retain the following acknowledgment:

   "This product includes software developed by the IEEE Industry Connections Security Group (ICSG)".

THIS SOFTWARE IS PROVIDED "AS IS" AND "WITH ALL FAULTS." IEEE AND ITS CONTRIBUTORS EXPRESSLY DISCLAIM ALL WARRANTIES AND REPRESENTATIONS, EXPRESS OR IMPLIED, INCLUDING, WITHOUT LIMITATION: (A) THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE; (B) ANY WARRANTY OF NON-INFRINGEMENT; AND (C) ANY WARRANTY WITH RESPECT TO THE QUALITY, ACCURACY, EFFECTIVENESS, CURRENCY OR COMPLETENESS OF THE SOFTWARE.

IN NO EVENT SHALL IEEE 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 AND REGARDLESS OF WHETHER SUCH DAMAGE WAS FORESEEABLE.

THIS SOFTWARE USES STRONG CRYPTOGRAPHY, WHICH MAY BE SUBJECT TO LAWS AND REGULATIONS GOVERNING ITS USE, EXPORTATION OR IMPORTATION. YOU ARE SOLELY RESPONSIBLE FOR COMPLYING WITH ALL APPLICABLE LAWS AND REGULATIONS, INCLUDING, BUT NOT LIMITED TO, ANY THAT GOVERN YOUR USE, EXPORTATION OR IMPORTATION OF THIS SOFTWARE. IEEE AND ITS CONTRIBUTORS DISCLAIM ALL LIABILITY ARISING FROM YOUR USE OF THE SOFTWARE IN VIOLATION OF ANY APPLICABLE LAWS OR REGULATIONS.

Info-ZIP

Copyright © 1990–2007 Info-ZIP. All rights reserved.

For the purposes of this copyright and license, “Info-ZIP” is defined as the following set of individuals:

Mark Adler, John Bush, Karl Davis, Harald Denker, Jean-Michel Dubois, Jean-loup Gailly, Hunter Goatley, Ed Gordon, Ian Gorman, Chris Herborth, Dirk Haase, Greg Hartwig, Robert Heath, Jonathan Hudson, Paul Kienitz, David Kirschbaum, Johnny Lee, Onno van der Linden, Igor Mandrichenko, Steve P. Miller, Sergio Monesi, Keith Owens, George Petrov, Greg Roelofs, Kai Uwe Rommel, Steve Salisbury, Dave Smith, Steven M. Schweda, Christian Spieler, Cosmin Truta, Antoine Verheijen, Paul von Behren, Rich Wales, Mike White

This software is provided “as is,” without warranty of any kind, express or implied. In no event shall Info-ZIP or its contributors be held liable for any direct, indirect, incidental, special or consequential damages arising out of the use of or inability to use this software.

Permission is granted to anyone to use this software for any purpose, including commercial applications, and to alter it and redistribute it freely, subject to the following restrictions:

1. Redistributions of source code must retain the above copyright notice, definition, disclaimer, and this list of conditions.
2. Redistributions in binary form (compiled executables and libraries) must reproduce the above copyright notice, definition, disclaimer, and this list of conditions in documentation and/or other materials provided with the distribution. The sole exception to this condition is redistribution of a standard UnZipSFX binary (including SFXWiz) as part of a self-extracting archive; that is permitted without inclusion of this license, as long as the normal SFX banner has not been removed from the binary or disabled.
3. Altered versions—including, but not limited to, ports to new operating systems, existing ports with new graphical interfaces, versions with modified or added functionality, and dynamic, shared, or static library versions not from Info-ZIP—must be plainly marked as such and must not be misrepresented as being the original source or, if binaries, compiled from the original source. Such altered versions also must not be misrepresented as being Info-ZIP releases--including, but not limited to, labeling of the altered versions with the names "Info-ZIP" (or any variation thereof, including, but not limited to, different capitalizations), "Pocket UnZip," "WiZ" or "MacZip" without the explicit permission of Info-ZIP. Such altered versions are further prohibited from misrepresentative use of the Zip-Bugs or Info-ZIP e-mail addresses or the Info-ZIP URL(s), such as to imply Info-ZIP will provide support for the altered versions.
4. Info-ZIP retains the right to use the names “Info-ZIP,” “Zip,” “UnZip,” “UnZipSFX,” “WiZ,” “Pocket UnZip,” “Pocket Zip,” and “MacZip” for its own source and binary releases.

Lua

The Sophos software that is described in this document may include some software programs that are licensed (or sublicensed) to the user under the Lua License. A copy of the license agreement for any such included software can be found at http://www.lua.org/copyright.html

Microsoft software

This Sophos product may include certain Microsoft software, licensed to Sophos for inclusion and use herein.

Mersenne Twister (mt19937ar.c)

Copyright (c) 1997–2002 Makoto Matsumoto and Takuji Nishimura. 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. The names of its contributors may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS 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 COPYRIGHT OWNER OR 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.

OpenSSL Cryptography and SSL/TLS 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.

This library is free for commercial and non-commercial use as long as the following conditions are adhered to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com).

Copyright remains Eric Young’s, and as such any Copyright notices in the code are not to be removed. If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

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 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 acknowledgement:

   “This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)”

   The word “cryptographic” can be left out if the routines from the library being used are not cryptographic related :-).

4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement:

   “This product includes software written by Tim Hudson (tjh@cryptsoft.com)”

Protocol Buffers (libprotobuf)

pstdint

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. The name of the author may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR "AS IS" AND ANY EXPRESS 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 AUTHOR 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.

Simple ECMAScript Engine (SEE)

Copyright © 2003, 2004, 2005, 2006, 2007 David Leonard. 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. Neither the name of David Leonard nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS “AS IS” AND ANY EXPRESS 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 COPYRIGHT OWNER OR 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.

SQLCipher

Copyright © 2008-2012 Zetetic LLC

strcasestr.c

Udis86

UnRAR

Alexander L. Roshal

XPExplorerBar

Index