

SOPHOS

Sophos for Microsoft SharePoint Help

Product version: 2.0

Document date: March 2011



Contents

1 About Sophos for Microsoft SharePoint.....	3
2 Dashboard.....	4
3 Configuration.....	5
4 Reports.....	27
5 Search.....	28
6 System status.....	31
7 Technical support.....	32
8 Legal notices.....	33

1 About Sophos for Microsoft SharePoint

Sophos for Microsoft SharePoint is a security solution for Microsoft SharePoint. Sophos for Microsoft SharePoint includes the following features for your SharePoint store:

- Detects and deals with malware, Potentially Unwanted Applications (PUAs), and suspicious files.
- Blocks access to offensive content or files that can be malicious by setting content filtering policies based on file name, file type, or a phrase.
- Performs on-access scanning.
- Performs on-demand and scheduled scanning for all or part of the SharePoint store.
- Quarantines and cleans items if they are: infected, considered adware/PUA or suspicious, contain a blocked file name, file type, or phrase.
- Generates reports based on several categories, such as anti-virus, content filtering, and quarantine items.
- Sends alerts when a virus, malware, adware/PUA or suspicious file is detected or blocked.
- Maintains a log of activities.

2 Dashboard

The **Dashboard** tab displays the status of the scans and statistics that provide information about the SharePoint store. It has four sections:

Select server

The **Select server** section has a drop-down list of available servers in the configuration group. Based on the server that is selected information is displayed in the other sections of the **Dashboard** tab.

Summary statistics today

The **Summary statistics today** section displays threat statistics for the current day. The information displayed is for the selected server.

Quarantine

The **Quarantine** section provides the following information for the selected server:

■ **Items in quarantine**

Displays the number of files stored in quarantine.

■ **Quarantine folder size**

Displays the actual size of quarantined items.

System console

The **System console** section displays the status of each server in the group. A green icon indicates the system is healthy. A red icon is displayed when an error occurs, such as failure to download updates.

This section also displays the time of the last update and the status of scans for the selected server. The status is always displayed for an on-access scan, but for an on-demand or scheduled scan the status is only displayed when it is running.

3 Configuration

The **Configuration** tab lets you manage and configure Sophos for Microsoft SharePoint.

In a farm, in order to manage several Sophos for Microsoft SharePoint servers together, you should have selected the same SQL Server instance and Sophos for Microsoft SharePoint configuration group during the installation. Configuration changes made to any of the servers in a configuration group will be applied to all the servers in that configuration group.

By default, the on-access scan control page is displayed. The left pane of the tab displays options to configure Sophos for Microsoft SharePoint. You can click on any of the items to expand the menu. The **Configuration** tab lets you:

- View and control the current state of a scan.
- Configure each scan individually.
- Authorize files to exclude from scanning.
- Manage system settings such as, alert, quarantine, report, log, and backup and restore configuration.

3.1 On-access scan

The on-access scan lets you intercept files as they are accessed, and grants access to only those files that do not pose a threat to your computer or are authorized for use.

You can configure the following settings for an on-access scan:

- [Scan control](#) (page 6)
- [Anti-virus policy](#) (page 8)
- [Anti-virus settings](#) (page 10)
- [Content filtering policy](#) (page 12)
- [Content filtering settings](#) (page 19)

3.2 On-demand scan

The on-demand scan lets you perform a scan of the SharePoint store, or parts of the SharePoint store, that you can run immediately.

You can scan whole or only a part of the SharePoint store during an on-demand scan by editing **Scan target settings** in the **On-demand scan** menu.

You can configure the following settings for an on-demand scan:

- [Scan control](#) (page 6)
- [Anti-virus policy](#) (page 8)

- [Anti-virus settings](#) (page 10)
- [Content filtering policy](#) (page 12)
- [Content filtering settings](#) (page 19)
- [Scan target settings](#) (page 19)

3.3 Scheduled scan

The scheduled scan lets you perform a scan of the SharePoint store, or parts of the SharePoint store, that runs at a set time.

You can scan whole or only a part of the SharePoint store during a scheduled scan by editing **Scan target settings** in the **Scheduled scan** menu.

You can configure the following settings for a scheduled scan:

- [Scan control](#) (page 6)
- [Anti-virus policy](#) (page 8)
- [Anti-virus settings](#) (page 10)
- [Content filtering policy](#) (page 12)
- [Content filtering settings](#) (page 19)
- [Scan target settings](#) (page 19)
- [Schedule settings](#) (page 21)

3.4 Scan control

The **Scan control** page lets you start or stop a scan. The page displays information about the items that have been scanned based on their categories, and the actions that have been taken during the scan.

Scan control page varies depending upon the scan:

- [Scan control: on-access scan](#) (page 6)
- [Scan control: on-demand scan](#) (page 7)
- [Scan control: scheduled scan](#) (page 7)

The information in **Scan control** page is refreshed automatically every 2 minutes. Alternatively, you can click **Refresh** to update the information immediately.

3.4.1 Scan control: on-access scan

For on-access scan, the **Scan control** page displays the status for all servers.

The scan status will change only when the scan is started/stopped.

- A green icon and the text **Running** is displayed when the on-access scan is running on all servers.
- A yellow status icon and the text **Stopped** is displayed when the on-access scan is not running on any one of the servers.

The **Activity for** drop-down list lets you view information about other servers in the group.

Click **Reset** to reset the counters to zero in the **Category** and **Actions** sections of the page.

3.4.2 Scan control: on-demand scan

For an on-demand scan, the **Scan control** page displays a link **Configured to run on server** indicating which server the scan is configured to run on. You can click on this link to change the server on which the scan will run.

In a farm, the data in the SharePoint store is stored by SQL Server and is accessible by each server in the farm. For on-demand scan you can select any one of the servers in a configuration group that performs the scan. The configured server can scan all or configured parts of the SharePoint store.

- A green icon and the text **Running** is displayed when the on-demand scan is running.
- A yellow status icon and the text **Stopped** is displayed when the on-demand scan is not running.

The **Summary for** drop-down list lets you view information about other servers in the group.

Click **Reset** to reset the counters to zero in the **Category** and **Actions** sections of the page.

3.4.3 Scan control: scheduled scan

For scheduled scan, the **Scan control** page displays a link **Configured to run on server** indicating which server the scan is configured to run on. You can click on this link to change the server on which the scan will run.

In a farm, the data in the SharePoint store is stored by SQL Server and is accessible by each server in the farm. For scheduled scan you can select any one of the servers in a configuration group that performs the scan. The configured server can scan all or configured parts of the SharePoint store.

Note: You must configure a scheduled scan to ensure all the existing items in the SharePoint store are scanned based on your configuration and new identities that are downloaded from Sophos.

The scan status automatically changes based on the schedule.

- A green icon and the text **Running** is displayed when the scheduled scan is running.
- A yellow status icon and the text **Stopped** is displayed when the scan is waiting for the scheduled time.

The **Summary for** drop-down list lets you view information about other servers in the group.

Click **Reset** to reset the counters to zero in the **Category** and **Actions** sections of the page.

For information on how to schedule a scan, see [Schedule settings](#) (page 21).

3.5 Anti-virus policy

The **Anti-virus policy** page lets you specify actions that are to be taken when the product finds malware, adware/PUAs, encrypted items, or suspicious files during an upload or download action. The following anti-virus policies are available:

Rule name	Rule description	Default action	Default alert	Default enabled
On infection	Specifies action for known malware, such as, viruses, Trojans, and spyware.	Replace with text.	On	Yes
On adware/PUA	Specifies action for known adware and potentially unwanted applications, such as Netmon.	For on-access scan, block access. For on-demand scan, continue.	On	No
On suspicious file (HIPS)	Specifies action for items that are not known to be malware but have suspicious behavior and are likely to be malware.	Continue.	On	No
On encrypted	Specifies action for files that are encrypted, such as password-protected files.	Continue.	On	Yes

Click on a policy to view a wizard that lets you modify the properties.

3.5.1 Modify anti-virus policy

The anti-virus policies lets you define actions to be performed based on the items that are detected.

Note: You cannot create a new anti-virus policy or modify the rule type, rule configuration, or rule description for anti-virus policies.

To modify a policy:

1. Click on a policy that you want to edit.
The **Edit policy rule** window is displayed.

2. In **Rule Type**, an option is selected based on the chosen policy. Click **Next**.
3. In **Rule Action**, set a desired action:

Note: You can choose a different option for the **Upload** and **Download** actions for an on-access scan if you are using a SharePoint 2010 server.

Ensure the upload action is the same or more restrictive than the download action.

Option	Description
Continue	Indicates no action will be taken on the files but the event is logged and alerts will be sent if configured.
Quarantine and continue	Quarantines the file and but lets you continue to use it.
Replace with text	Replaces the file in SharePoint store with a text file using the same file name and extension. The text to be replaced is configurable.
Quarantine and replace with text	Quarantines the original file and replaces the file in the SharePoint store with a text file using the same file name and extension.
Block	Blocks access to files categorized under the event, this option is only available for on-access scan. Note: This option is only available for the anti-virus policy of on-access scans.
Quarantine and block	Quarantines the file and blocks it from being accessed. Note: This option is only available for the anti-virus policy of on-access scans.

Select **Enable** to enable the rule and select **Alert** if you want to be notified via email every time an action is performed. For information on how to set alerts, see [Alert and Email settings](#) (page 22).

4. If you had chosen **Replace with text** as an option, in **Replacement Text**, configure the content that should be in the text file that will be replaced in the SharePoint store using the same file name and extension. For information, see [Configure replacement text for anti-virus policy](#) (page 9). Click **Finish**.

Note: SharePoint caches the scan result, hence a file might not be scanned if it is downloaded soon after upload.

3.5.2 Configure replacement text for anti-virus policy

You can customize the text file that a detected file is to be replaced with when you choose the **Replace with text** or **Quarantine and replace with text** option for a policy.

The following substitution symbols are supported for replacement text:

Substitution symbol	Description
%DATE%	Date when the event occurred.
%DETAILS%	Additional information. For example, w32/trojman.
%DETAILS_TYPE%	Type of the additional information. For example, malware name(s).
%DIRECTION%	Direction of the data flow: upload or download. Note: This option is supported only for on-access scan on SharePoint 2010.
%EVENT%	Incident event. For example, malware detected.
%FILE_NAME%	Name of the item.
%LAST_MODIFIED_USER%	User who last modified the item (if available).
%LOCATION%	Location of the item (if available). Note: Location refers to the item's internal SharePoint folder path.
%ORIGINAL_AUTHOR%	User who originally added the item (if available).
%RULE_NAME%	Name of the rule that triggered the event. For example, on infection.
%SCAN_NAME%	Scan name. For example, on-access scan.
%SERVER%	Name of the server that encountered the event.
%TIME%	Time when the event occurred.

Note: If the content of a file is replaced during an on-access scan, the values for location, last modified user, and original author are not displayed in the replaced text of a file.

3.6 Anti-virus settings

The **Anti-virus settings** page lets you change the following scanning options:

Scanning level

You choose between **Normal** and **Extensive** scanning levels.

Note: Sophos does not recommend selecting the **Extensive** option, except on the advice of Sophos technical support.

Scanning options

You can select any of the following scanning options:

- **Scan inside archives**

Performs a scan inside compressed files, such as ZIP and RAR.

- **Alert administrator on errors**

Sophos for Microsoft SharePoint sends alert emails to the addresses configured in the alert settings. Alerts are sent on a per-event basis for on-access scan; for on-demand and scheduled scans a consolidated email is sent listing all the events.

- **Attempt to clean infected documents**

Attempts to disinfect the files.

Note: For on-access scan, the option **Attempt to clean infected documents** is available under Microsoft SharePoint anti-virus settings.

Microsoft SharePoint anti-virus settings

Note: These Microsoft SharePoint anti-virus settings are available only for on-access scan.

Microsoft SharePoint provides anti-virus settings which can be used when a compatible anti-virus scanner is installed. Installing Sophos for Microsoft SharePoint will set the following default options to the Microsoft SharePoint anti-virus settings:

Option	Default state / value
Scan documents on upload	Enabled
Scan documents on download	Enabled
Allow users to download infected documents	Disabled
Attempt to clean infected documents	Enabled
Time out duration (in seconds)	900
Number of threads	5

Sophos for Microsoft SharePoint lets you configure these settings from the **Anti-virus settings** page by mirroring them from the SharePoint administration web site. These settings are available only for on-access scan.

Note: For on-access scan, the options **Replace with text** and **Quarantine and replace with text** will work only if the option **Attempt to clean infected documents** is selected in the scanning options.

It is recommended that changes to the Microsoft SharePoint anti-virus settings are made from the Sophos for Microsoft SharePoint anti-virus settings page rather than the Microsoft SharePoint administration web site.

3.7 Content filtering policy

The **Content filtering policy** page lets you block access to offensive content and to unwanted file types. You can create, modify, and delete content filtering rules.

Important: We strongly recommend that the content filtering rules are tested on a sample of files before applying to the complete SharePoint store. If you set a rule with replacement action for a common file name, file type, or phrase (for example, Replace with text or Quarantine and replace with text) all or many of the files in the SharePoint store will be replaced and cannot be restored. Alternatively, for a new rule you can initially set the action to **Continue** and run it. You can view the logs later to check the files that are affected by the rule and then change the action as desired.

By default, the following rules are available:

Rule name	Rule description	Default action	Default alert	Default enabled
On restricted file types	Blocks access to common virus carrier file types.	For on-access scan, block access. For on-demand and scheduled scan, continue.	On	No
On offensive language	Blocks access to common offensive phrases using regular expressions.	For on-access scan, block access. For on-demand and scheduled scan, continue.	On	No

You can choose to enable or disable any of these policies. Click on a policy to view a wizard that lets you modify the properties.

3.7.1 Modify content filtering policy

Content filtering policies let you view and create and content filtering rules. Content filtering rules are not enabled by default.

To modify a policy:

1. Click on a policy that you want to edit.
The **Edit policy rule** window is displayed.

- In **Rule Type**, an option is displayed based on the chosen policy. Click **Next**.
- In **Rule Action**, set a desired action:

Note: You can choose a different option for the **Upload** and **Download** actions for an on-access scan if you are using a SharePoint 2010 server.

Ensure the upload action is the same or more restrictive than the download action.

Option	Description
Continue	Indicates no action will be taken on the files but the event is logged and alerts will be sent if configured.
Quarantine and continue	Quarantines the file and but lets you continue to use it.
Replace with text	Replaces the file in SharePoint store with a text file using the same file name and extension. The text to be replaced is configurable.
Quarantine and replace with text	Quarantines the original file and replaces the file in the SharePoint store with a text file using the same file name and extension. The text to be replaced is configurable.

Select **Enable** to enable the rule and select **Alert** if you want to be notified via email every time an action is performed. For information on how to set alerts, see [Alert and Email settings](#) (page 22).

- If you had chosen Replace with text as an option, in **Replacement Text**, configure the content that should be in the text file that will be replaced in the SharePoint store using the same file name and extension. For information, see [Configure replacement text for anti-virus policy](#) (page 9). Click **Finish**.

Note: SharePoint caches the scan result, hence a file might not be scanned if it is downloaded soon after upload.

3.7.2 Add Rule

You can choose to create and define new content filtering rules.

Important: We strongly recommend that the content filtering rules are tested on a sample of files before applying to the entire SharePoint store. If you set a rule with replacement action for a common file name, file type, or phrase (for example, Replace with text or Quarantine and replace with text) all or many of the files in the SharePoint store will be replaced and cannot be restored. Alternatively, for a new rule you can initially set the action to **Continue** and run it. You can view the logs later to check the files that are affected by the rule and then change the action as desired.

To define a rule:

- In the **Configuration** tab, select a scan, and click **Content filtering policy**.

The Content filtering policy page is displayed with the existing rules.

2. On the upper-right corner of the page, click **Add Rule**.

The **Add policy rule** window is displayed.

3. You can choose from the following options and then click **Next**.

- **Block file names**, for more information, see [Configure file name blocking](#) (page 14).
- **Block file types**, for more information, see [Configure file type blocking](#) (page 15).
- **Block phrases**, for more information, see [Configure phrase blocking](#) (page 17).

Based on the rule type, a configuration dialog is displayed to configure settings related to the rule type.

3.7.2.1 Configure file name blocking

You can choose to block files with a particular file name.

Important: We strongly recommend that you test the content filtering rules on a sample of files before applying to the complete SharePoint store. For example, if you set a rule that quarantines a common file name (like a*), all the files that start with 'a' in the SharePoint store will be quarantined and cannot be restored.

1. In **Rule Type**, select **Blocked file name** and click **Next**.
2. In **Rule Configuration**, under the **File name** tab, specify file names that must be blocked (one per line).
3. In the **Exceptions** tab, specify file names that must be excluded from blocking (one per line).
4. Set the **Take action only if file size exceeds (in MB)** to set a value for file size, if required. Click **Next**.

- In **Rule Action**, set a desired action:

Note: You can choose a different option for the **Upload** and **Download** actions for an on-access scan if you are using a SharePoint 2010 server.

Ensure the upload action is the same or more restrictive than the download action.

Option	Description
Continue	Indicates no action will be taken on the files but the event is logged and alerts will be sent if configured.
Quarantine and continue	Quarantines the file and but lets you continue to use it.
Replace with text	Replaces the file in SharePoint store with a text file using the same file name and extension. The text to be replaced is configurable.
Quarantine and replace with text	Quarantines the original file and replaces the file in the SharePoint store with a text file using the same file name and extension. The text to be replaced is configurable.

Select **Enable** to enable the rule and select **Alert** if you want to be notified via email every time an action is performed. For information on how to set alerts, see [Alert and Email settings](#) (page 22).

- If you had chosen Replace with text as an option, in **Replacement Text**, configure the content that should be in the text file that will be replaced in the SharePoint store using the same file name and extension. For information, see [Configure replacement text for anti-virus policy](#) (page 9). Click **Next**.
- In **Rule Name**, enter a rule name and click Finish.

Note: SharePoint caches the scan result, hence a file might not be scanned if it is downloaded soon after upload.

3.7.2.2 Configure file type blocking

You can choose to block specific files types.

Important: We strongly recommend that you test the content filtering rules on a sample of files before applying to the complete SharePoint store. For example, if you create a rule that quarantines a common file type (like PDF), all the PDF files in the SharePoint store will be quarantined and cannot be restored.

- In **Rule Type**, select **Blocked file type** and click **Next**.
- In **Rule Configuration**, under the **File types** tab, select from **Choose the file types to block** drop-down list.

A full list of the applications included in that group is displayed.

- To block a file type, select it and click "Add".



- To remove a file type, select it and click "Remove".



- To remove all existing file types from blocked list, click "Remove all".



3. In the **Exceptions** tab, specify file types that must be excluded from blocking (one per line) and click **Next**.

Set **Take action only if file size exceeds (in MB)** to set a value for file size, if required.

4. In **Rule Action**, set a desired action:

Note: You can choose a different option for the **Upload** and **Download** actions for an on-access scan if you are using a SharePoint 2010 server.

Ensure the upload action is the same or more restrictive than the download action.

Option	Description
Continue	Indicates no action will be taken on the files but the event is logged and alerts will be sent if configured.
Quarantine and continue	Quarantines the file and but lets you continue to use it.
Replace with text	Replaces the file in SharePoint store with a text file using the same file name and extension. The text to be replaced is configurable.
Quarantine and replace with text	Quarantines the original file and replaces the file in the SharePoint store with a text file using the same file name and extension.

Select **Enable** to enable the rule and select **Alert** if you want to be notified via email every time an action is performed. For information on how to set alerts, see [Alert and Email settings](#) (page 22).

5. If you had chosen **Replace with text** as an action, in **Replacement Text**, configure the content that should be in the text file that will be replaced in the SharePoint store using the same file name and extension. For information, see [Configure replacement text for anti-virus policy](#) (page 9). Click **Next**.
6. In **Rule Name**, enter a rule name and click **Finish**.

Note: SharePoint caches the scan result, hence a file might not be scanned if it is downloaded soon after upload.

3.7.2.3 Configure phrase blocking

You can choose to block files with specific phrases. You can use wildcards '*' and '?' to specify phrases. Phrases are not case sensitive.

Important: We strongly recommend that you test the content filtering rules on a sample of files before applying to the complete SharePoint store. For example, if you set a rule that quarantines a common phrase (like 'the'), all files containing the word 'the' in the SharePoint store will be quarantined and cannot be restored.

1. In **Rule Type**, select **Blocked phrase** and then click **Next**.
2. In **Rule Configuration**, in the **Strings** tab, enter a phrase that you want to block (one per line).
3. In the **Regular expressions** tab, enter a regular expression phrase that you want to block (one per line).
4. In the **Exceptions** tab, specify the file names that must be excluded from phrase blocking (one per line).
5. Optionally, select **Take action only when a minimum number of phrases are detected**. The value entered must be between 2 and 10 occurrences.
6. In **Rule Action**, set a desired action:

Note: You can choose a different option for the **Upload** and **Download** actions for an on-access scan if you are using a SharePoint 2010 server.

Ensure the upload action is the same or more restrictive than the download action.

Option	Description
Continue	Indicates no action will be taken on the files but the event is logged and alerts will be sent if configured.
Quarantine and continue	Quarantines the file and but lets you continue to use it.
Replace with text	Replaces the file in SharePoint store with a text file using the same file name and extension. The text to be replaced is configurable.
Quarantine and replace with text	Quarantines the original file and replaces the file in the SharePoint store with a text file using the same file name and extension. The text to be replaced is configurable.

Select **Enable** to enable the rule and select **Alert** if you want to be notified via email every time an action is performed. For information on how to set alerts, see [Alert and Email settings](#) (page 22).

7. If you had chosen **Replace with text** as an action, in **Replacement Text**, configure the content that should be in the text file that will be replaced in the SharePoint store using the same file name and extension. For information, see [Configure replacement text for anti-virus policy](#) (page 9). Click **Next**.

8. In **Rule Name**, enter a rule name and click **Finish**.

For information on the file types that are blocked, see [File types supported for blocking phrases](#) (page 18).

Note: SharePoint caches the scan result, hence a file might not be scanned if it is downloaded soon after upload.

3.7.2.4 File types supported for blocking phrases

Sophos for Microsoft SharePoint can analyse content within common document types. This enables you to search for phrases within those documents. By default, Sophos for Microsoft SharePoint scans content from the following files based on a combination of file type and extension:

Sophos for Microsoft SharePoint can extract content from the following common file types, such as:

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

The list of common file types that are supported will be updated by Sophos during an update.

3.7.2.5 Configure replacement text for content filtering policy

You can customize the text file that a detected file is to be replaced with when you choose the **Replace with text** or **Quarantine and replace with text** option for a policy.

Note: You cannot configure the replacement text when you choose to block by file names.

The following substitution symbols are supported for replacement text:

Substitution symbol	Description
%DATE%	Date when the event occurred.
%DETAILS%	Additional information. For example, w32/trojman.
%DETAILS_TYPE%	Type of the additional information. For example, malware name(s).

Substitution symbol	Description
%DIRECTION%	Direction of the data flow: upload or download. Note: This option is supported only for on-access scan on SharePoint 2010.
%EVENT%	Incident event. For example, malware detected.
%FILE_NAME%	Name of the item.
%LAST_MODIFIED_USER%	User who last modified the item (if available).
%LOCATION%	Location of the item (if available). Note: Location refers to the item's internal SharePoint folder path.
%ORIGINAL_AUTHOR%	User who originally added the item (if available).
%RULE_NAME%	Name of the rule that triggered the event. For example, on infection.
%SCAN_NAME%	Scan name. For example, on-access scan.
%SERVER%	Name of the server that encountered the event.
%TIME%	Time when the event occurred.

Note: If the content of a file is replaced during an on-access scan, the values for location, last modified user, and original author are not displayed in the replaced text of a file.

3.8 Content filtering settings

The **Content filtering settings** page lets you configure scanning inside archive files. By default, the **Search for phrases within archive files** option is not enabled.

3.9 Scan target settings

The **Scan target settings** page lets you choose areas and files within the SharePoint store that must be scanned when an on-demand or scheduled scan becomes active. The page has two tabs:

- [Scan locations](#) (page 20)
- [Scan files](#) (page 20)

3.9.1 Scan locations

The **Scan locations** tab lets you specify the parts of the data store you want to scan during an on-demand scan or scheduled scan.

Note: The list displaying the SharePoint data store structure displays only folders and not individual files.

To set a scan location:

1. In the **Configuration** tab, select a scan, and click **Scan target settings**.

The scan target settings page is displayed.

2. Click the **Scan Location** tab and choose a location from the drop-down menu:

- **Scan all locations** (selected by default)
- **Scan all locations selected below**
- **Scan all locations except those selected below**

3. Select the locations that you want to scan from the SharePoint data store structure displayed.

- To add a location, select it and click "Add".



- To remove a location, select it and click "Remove".



- To remove all location, click "Remove all".



4. Click **Apply** to save the settings.

If you modify and save settings when an on-demand or scheduled scan is active, the changes will take effect the next time the scan is started.

3.9.2 Scan files

The **Scan files** tab lets you choose the files that you want to scan during an on-demand or scheduled scan.

1. In the **Configuration** tab, select a scan, and click **Scan target settings**.

The scan target settings page is displayed.

2. Click the **Scan files** tab and choose a filter to scan the files:

- **Scan all files**

- Scan all files that match the filter selected below
- Scan all files except that match the filter below

3. If you select a filter, in the text box, enter the files names one per line.

The file names are not case sensitive and can contain wildcards '*' and '?'.

4. Click **Apply** to save the settings.

If you modify and save settings when an on-demand or scheduled scan is active, the changes will take effect the next time the scan is started.

3.10 Schedule settings

The **Schedule settings** page lets you schedule a scan at a particular day and time.

Note: You must configure a scheduled scan to ensure all the existing items in the SharePoint store are scanned based on your configuration and new identities that are downloaded from Sophos.

To schedule a scan, select **Schedule this scan**, set the **Days when the scan will run**, and **Scan start time** fields to specify when you want to perform the scan.

You can set the **Number of minutes after which scan should be aborted**, if the scan is not yet complete.

3.11 Authorization

The **Authorization** menu lets you exclude files from checking while performing a scan. The exceptions will apply to all scans.

Adware/PUAs

The **Adware/PUAs** page lets you add adware/PUA names, one per line, which must be excluded from the check.

Note: The adware/PUA name is the identity name but not the file name. You can locate the identity name for an adware/PUA from the logs. Alternatively, if you authorize an adware/PUA from the quarantine list, the file will be included in the authorization list.

Suspicious Files

The **Suspicious files** page lets you add files that must be excluded from the "On suspicious file (HIPS)" check. You can use wildcards '?' and '*' and the file names are not case sensitive.

3.12 System

The **System** menu of the configuration tab lets you configure the following settings for Sophos for Microsoft SharePoint:

- [Alert and Email settings](#) (page 22)
- [Quarantine settings](#) (page 24)
- [Report settings](#) (page 25)
- [Log settings](#) (page 25)
- [Backup and restore](#) (page 26)

Note: If you are using SharePoint 2007 or earlier, the location, direction and username fields will not be available for on-access scan in Logs, Quarantine, Alerts, and Reporting sections.

3.12.1 Alert and Email settings

The **Alert and Email settings** page lets you configure the content for email alerts, and the addresses to which alert messages are sent. If alerting is enabled for an event, messages are sent as follows:

- On-access scanning sends a message for each incident.

Note: If you are using SharePoint 2007 or earlier, the following information is not available for on-access scan in logs, quarantine, and alerts and reporting: Location, Direction and Username.

- On-demand or scheduled scanning sends a single consolidated message for all events at the end of the scan.

This page has two sections:

- [Template](#) (page 22)
- [Address](#) (page 24)

3.12.1.1 Template

You can modify the email content by customizing the template for email alerts.

1. In the **Configuration** tab, click **System**, and then click **Alert settings**.

The **Alert Settings** page is displayed.

2. Under the **Template** section, in the **Alert subject** field, enter the subject line of the alert. Click **Insert substitution symbols** to insert desired information. The following options are available for the alert subject:

Substitution symbol	Description
%SCAN_NAME%	Name of the scan. For example, on-access scan.
%SERVER%	Name of the server that encountered the event.

3. In the **Alert body** text panel, create the main content of your alert. Click **Insert substitution symbols** to insert desired information. The following options are available for the alert body:

Substitution symbol	Description
%ACTION%	Action that has been carried out on the item. For example, Replace with text.
%DATE%	Date when event occurred.
%EVENTS%	Events that were encountered while processing the item. For example, malware detected.
%FILE_NAME%	Name of the item.
%LAST_MODIFIED_USER%	User who last modified the item (if available).
%LOCATION%	Location of the item (if available). Note: Location refers to the item's internal SharePoint folder path.
%ORIGINAL_AUTHOR%	User who originally added the item (if available).
%SCAN_NAME%	Name of scan name. For example, on-access scan.
%SERVER%	Name of the server that encountered the event.
%TIME%	Time when event occurred.

4. In the **Text for each incident** panel, enter any unique per-incident text you want to display. Click **Insert substitution symbols** to insert desired information. The following options are available:

Substitution symbol	Description
%DETAILS%	Additional information. For example, w32/trojman.
%DETAILS_TYPE%	Type of the additional information. For example, malware name(s).
%EVENT%	Incident event. For example, malware detected.
%RULE_NAME%	Name of the rule that triggered the event. For example, on infection.

5. Click **Apply** to save the changes.

3.12.1.2 Address

You can add or modify recipients to whom the alerts are sent provided their SMTP server accepts the email.

1. In the **Configuration** tab, click **System**, and then click **Alert settings**.

The **Alert Settings** page is displayed.

2. Under the **Address** section, enter the email addresses that will receive administrator alert messages, one per line.

The list can be empty in which case no alert messages are sent.

3. Enter the **Sender email address**. This will appear as the sender of the alert messages.

Note: The sender email address cannot be empty.

4. Enter the **SMTP mail server** address.

5. Enter the **SMTP port**, this field cannot be empty and should be a number between 1 and 65536.

Default: 25

6. Click **Apply** to save the settings.

Make sure that the SMTP mail server accepts anonymous (non-authenticated) emails sent from the Sophos for Microsoft SharePoint computer. It should also accept, and be able to relay, emails sent to stats@vista.sophos.com and any recipients specified under the **Address** section.

3.12.2 Quarantine settings

The **Quarantine settings** page lets you configure quarantine housekeeping settings.

You can choose to purge the quarantine data immediately, or specify the number of days to keep the quarantine data before deleting it. Click **Purge now** to immediately delete quarantine data that is older than the specified number of days.

3.12.3 Report settings

The **Report settings** page lets you configure reporting settings.

Data collection

By default, data collection for reports is enabled. If **Enable data collection for reports** is not selected, no data is collected from the database for reports. You may disable data collection for reports while troubleshooting database performance problems.

Housekeeping

You can choose to purge report data immediately, or specify the number of days to keep quarantine data before deleting. Click **Purge now** to immediately delete report data that is older than the specified number of days.

3.12.4 Log settings

The **Log settings** page lets you specify the kind of messages to be logged. The logging options can be set individually for each of the following categories:

Windows event logging

Logs application events in Windows Event Viewer for Sophos for Microsoft SharePoint based on the specified logging level.

File logging

Logs events in the 'Logs' folder located in the Sophos for Microsoft SharePoint install location. Logs are recorded based on the specified logging level. You can limit the log file size by setting a value.

Note: If the log file reaches its maximum size, as specified in the Log Settings, the file is renamed by adding a time-stamp onto its name, and a new log-file is created.

Database logging

Logs events in the database to enable search for logs based on the specified logging level. Click **Purge now** to immediately delete logs that are older than the specified number of days.

Note: You will not be able to search for logs from Sophos for Microsoft SharePoint, if you set the database logging level to **None**.

You can specify the kind of messages to be logged for each category using the following logging options:

- **None** indicates logging is off.

- **Errors only** logs application errors like failing to quarantine, initialization failures, unexpected errors.
- **Error and warnings** log includes error messages and application warnings along with warnings about malware detection and disinfection, content policy rules infringement, actions taken, encrypted and unscannable items.
- **Errors, warnings and information** log includes error and warnings along with informational messages related to general product status.

3.12.5 Backup and restore

The **Backup and restore** page lets you make a back up of the Sophos for Microsoft SharePoint configuration to a specific location. You can then store, move, or restore it on a later date.

Note: During installation, Sophos for Microsoft SharePoint creates a backup of the default configuration (SophosSharepointDefaultConfig.xml) in the installation directory. The configuration file can be used to restore Sophos for Microsoft SharePoint to factory defaults.

Backup

Lets you download the product configuration as an XML file.

Restore

Lets you restore the product configuration from an XML file that has been backed up.

4 Reports

The **Reports** tab lets you generate and export reporting data from the database. If an error occurs while inserting the data into the database then an error is logged and the data is stored on disk. Later when the database is available, the data is inserted.

4.1 Generate Reports

You can generate and export reports based on categories.

To generate a report:

1. Click the **Reports** tab.

The **Generate report** pane is displayed on the left-hand side of the page.

2. Select a **Category** of the scan from the drop-down menu. You can choose from **Anti-virus**, **Content filtering**, and **Quarantine**.
3. Based on the category of the scan, select a **Report** from the drop-down menu.
4. Enter a value for the number of entries that you want to be displayed in the **Top** field.
Note: You can specify a value up to 10000.
5. Select a **Server** for which the report is to be generated from the drop-down list.
6. Select a **Scan name** from the drop-down list. You can choose from **on-access**, **on-demand**, or **scheduled**.
7. Select a **Reporting Period** for which the report must be generated, or set the **From** and **To** fields to filter messages within a particular date range.
8. Click **Generate**.

A report is generated based on the selection criteria.

You can click **Export** to save the report as a CSV file.

5 Search

The **Search** tab lets you manage quarantine items and search logs. The search pane on the left hand side of the search page has the following options:

- [Quarantine](#) (page 28)
- [Logs](#) (page 29)

Note: If you are using SharePoint 2007 or earlier, the location, direction and username fields will not be available for on-access scan in Logs, Quarantine, Alerts, and Reporting sections.

5.1 Quarantine

Sophos for Microsoft SharePoint can be configured to quarantine an item that:

- is infected.
- is adware/PUA.
- is suspicious (HIPS).
- is encrypted.
- contains a blocked file name, file type, or phrase.

Quarantined items are isolated in a secured format on the disk. You can choose to disinfect or delete any files that are quarantined. You can also authorize items that are classified as PUA or suspicious.

5.1.1 Search quarantine

You can search for items that are quarantined based on a particular date range, server, file characteristic such as file name, location, author, last modified user, reason for quarantine, or any combination of these parameters. The text fields support use of wildcards "*" and "?".

By default, items from the server you are connected to are displayed for the current day, and are sorted according to time (latest first). Click **Reset** to clear the options and modify.

To search quarantined items:

1. Click the **Search** tab.

The Search pane is displayed on the left-hand side of the page.

2. In search parameters, select **Quarantine** from the drop-down menu.
3. Enter dates in the **From** and **To** fields to filter items within a particular date range.

If you only enter a date in the **From** field, items are displayed from the selected date onwards.

4. Enter the **File name**, **Location**, **Original Author**, and **Last modified user** to include any of these options in the search.
5. Select a **Reason**, **Server**, **Scan name**, and **Sort by** from the drop-down lists and then click **Search**.


A list of items is displayed based on the criteria.

5.1.2 Actions for quarantine

Sophos for Microsoft SharePoint lets you perform specific actions on the quarantine items after the search results are displayed. To take action on quarantined items:

1. Search for quarantined items.

For information on how to search for quarantine items, see [Search quarantine](#) (page 28).

2. Select an item and click on the  sign to view details about the item such as, malware names, content policy.

You can click on a malware name to view its description from the Sophos website in a new browser window.

3. Select the files and choose any of the following actions:

- **Delete**

Deletes the selected item from the database.

- **Disinfect**

Disinfects the selected item. A summary is displayed if disinfection fails for any item when multiple files are selected.

- **Authorize**

Authorizes the item so that it is not quarantined by subsequent scans by adding it to the appropriate authorized list.

Note: The **Authorize** button is enabled only if a selected file is categorized as an adware/PUA or suspicious file.

4. You can retrieve a file and save it to disk by clicking the disk icon , or email it by clicking on the email icon .

For information on email settings, see [Alert and Email settings](#) (page 22).

5.2 Logs

Sophos for Microsoft SharePoint lets you search and review log messages.

5.2.1 Search logs

You can search for messages that are logged based on a date range, server, scan name, log string, log type, or any combination of these parameters. The text fields support use of wildcards such as *, ? and are not case sensitive.

By default when you open the panel, logs from all servers are displayed for the current day and are sorted according to time (latest first). Click **Reset** to clear the options and modify as required.

To search for logs:

1. Click the **Search** tab.

A list of available options is displayed in the left hand pane.

2. Under Search parameters, select **Logs** from the drop-down menu.
3. Enter dates in the **From** and **To** fields to filter messages within a particular date range.

If you only enter a date in the **From** field, messages are displayed from the selected date onwards.

4. Select a **Server** and **Scan name** from the drop-down lists.
5. Enter text or a value in the **Contains String** to search for a particular value.
6. Choose **Log Types**. You can choose from **Errors**, **Warnings**, **Information**, or any combination.
7. Select a **Sort by** option from the drop-down list and then click **Search**.

Logs are displayed based on the search criteria.

You can click **Export** to save the search results as a CSV file.

6 System status

The **System status** tab displays information about the product version, threat detection engine version and other details related to all the servers in the configuration group. You can click on a server name to view additional information.

Click **Export** on the lower-right corner of the page to save the system information that is displayed.

7 Technical support

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

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

8 Legal notices

Copyright © 2011 Sophos Limited. All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording or otherwise unless you are either a valid licensee where the documentation can be reproduced in accordance with the licence terms or you otherwise have the prior permission in writing of the copyright owner.

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