SOPHOS

# Sophos for Microsoft SharePoint
## startup guide

Product version: 2.0
Document date: March 2011

# Contents

# 1 About this guide

This guide tells you how you can protect Microsoft Windows SharePoint Services (WSS) 3.0 and Microsoft Office SharePoint Server 2007 and 2010 by installing and setting up Sophos for Microsoft SharePoint version 2.0.

If you are installing Sophos for Microsoft SharePoint for the first time, read this guide.

If you are upgrading, see the *Sophos for Microsoft SharePoint upgrade guide*, instead of this guide.

You can find details of all configuration options of Sophos for Microsoft SharePoint in the *Sophos for Microsoft SharePoint Help*.

For information on configuring Sophos Anti-Virus, refer to the Sophos Anti-Virus documentation.

# 2 About Sophos for Microsoft SharePoint

Sophos for Microsoft SharePoint is a security solution for Microsoft SharePoint. The key features of Sophos for Microsoft SharePoint include:

- On-access scanning of the SharePoint store for malware, Potentially Unwanted Applications (PUAs), suspicious files with Host Intrusion Protection System (HIPS), and exceptions to your corporate content by applying content filtering policies.
- On-demand and scheduled scanning for selected portions of the SharePoint store. The scan includes detection for malware, PUAs, suspicious files (HIPS), and exceptions to your corporate content by applying content filtering policies.
- A web-based user interface that allows administrators to configure settings, monitor status, perform routine quarantine management tasks, and generate reports.

# 3 System requirements

For system requirements, see the system requirements page of the Sophos website *http://www.sophos.com/products/all-sysreqs.html*.

# 4 Planning your installation

You can deploy Sophos for Microsoft SharePoint to a stand-alone computer or in a server farm environment.

## 4.1 Deploying on a stand-alone computer

In a stand-alone computer scenario, one server runs all the SharePoint server components and the SQL Server data store used by the SharePoint. In this scenario install Sophos for Microsoft SharePoint on the same computer.

## 4.2 Deploying to a server farm environment

In a server farm environment, there may be one or more servers in the farm running the SharePoint server components and SQL Server. In this scenario, install Sophos for Microsoft SharePoint on all the servers that have the SharePoint server components installed.

In a farm, in order to manage several Sophos for Microsoft SharePoint servers together, you must select the same SQL Server instance and Sophos for Microsoft SharePoint configuration group during the installation. The servers belonging to the same Sophos for Microsoft SharePoint configuration group will share the same configuration and can be monitored from any of the servers in the configuration group.

When installing on the first server choose a remote SQL Server and create a new configuration group. For subsequent installations, choose the same SQL Server and join the existing (newly created) configuration group.

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 and scheduled scans 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.

# 5 Installing Sophos for Microsoft SharePoint

## 5.1 Preparing for installation

When you run the Sophos for Microsoft SharePoint installer, you may be prompted to restart the SharePoint server several times before the installation of the Sophos for Microsoft SharePoint software begins. This depends on the components that are installed as prerequisites.

## 5.2 Install Sophos for Microsoft SharePoint

To install Sophos for Microsoft SharePoint:

1. Log on to the SharePoint server with local administrator rights. If you are in a domain, you must also be a domain user.

   For a complete list of permissions that are required for installation, see *http://www.sophos.com/support/knowledgebase/article/58866.html*.

2. Find the Sophos for Microsoft SharePoint installer that you downloaded earlier and double-click on it.
3. In the **Welcome** page, click **Next**.
4. In the **License Agreement** page, read the agreement. If you agree with the terms, click **I accept the terms of the license agreement** and click **Next**.
5. In the **Choose Destination Location** page, you see the default folder where Sophos for Microsoft SharePoint will be installed. If you want to install it in a different folder, click **Browse** and select a folder. Click **Next**.
6. In the **Sophos Download Credentials** dialog box, enter the **User name** and **Password** that were supplied by Sophos.

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

7. In the **Database Settings** page, select one of the following options:

   - **Local**

     Select this option if you want to use an SQL Server instance that is present on this server. If no database instance is found, the installer installs a local SQL Server Express 2008 instance on this server.

   - **Remote**

     Select this option if you have an SQL Server instance installed on another computer.

     In the remote SQL database, multiple installations of Sophos for Microsoft SharePoint can use the same database instance, but the database content will not be shared.

8. In the **Configuration Group** page, select a group you want to join or create a new group.

   Sophos for SharePoint installations can be grouped together to share the same policy configuration and be managed from a single management console. For more information, see *Deploying to a server farm environment* (page 4).

9. In the **Service Credentials** page, enter the credentials for the account that will be used for Sophos for Microsoft SharePoint services.

   The account must have local administrator rights and full access to the SharePoint store content. Sophos for Microsoft SharePoint uses these credentials to scan and clean items in the SharePoint store.

   Read *http://www.sophos.com/support/knowledgebase/article/58866.html* for more information on which accounts you can use.

   **Note:** If you have Windows User Account Control (UAC) enabled, you will be prompted for local administrative privileges with full access rights to the entire SharePoint store. Ensure the account has the necessary privileges and then click **Yes** to continue.

   If your computers are in a workgroup, continue to step 13.

10. In the **Administrators group** page, accept the default group name or provide a different group name.

    If the installer cannot create the group or if the group does not exist, a message is displayed **The group does not exist. Please ask a Domain Administrator to create the group**. In this case, contact the domain administrator to create the group and add the installing user and the service user as members to the group.

11. In the **Email Alerts** page, enter an administrator email address, SMTP server name and port number.

    The SMTP server must be able to accept anonymous (non-authenticated) emails sent from the Sophos for Microsoft SharePoint server. It must also be able to accept and relay emails sent to stats@vista.sophos.com and the administrator email address.

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

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

15. When installation is complete, the InstallShield Wizard **Complete** page is displayed. Click **Finish**.

## 5.3 Configure firewall

If Sophos for Microsoft SharePoint is installed on a server that has a firewall installed, ensure that the firewall is configured to allow incoming TCP connections to the Sophos for Microsoft SharePoint website port.

The link to Sophos for Microsoft SharePoint in the start menu contains the URL and port number for the administrative web site. For information, see *Open the Sophos for Microsoft SharePoint administration web site* (page 7).

**Note:** If you are using Windows Server 2008 or later with the default Windows Firewall, the firewall is automatically configured during installation.

## 5.4 Open the Sophos for Microsoft SharePoint administration web site

To open the Sophos for Microsoft SharePoint administration web site from the server on which Sophos for Microsoft SharePoint is installed, click **Start** > **Programs** > **Sophos** > **Sophos for Microsoft SharePoint**.

The shortcut is the URL containing the address and port number of the administration web site.

To open the Sophos for Microsoft SharePoint administration web site from another computer, use a web browser to open the appropriate web address.

For example, this might be http://192.0.2.0:8081, where 192.0.2.0 is the IP address of the server on which Sophos for Microsoft SharePoint is installed.

If you cannot open the Sophos for Microsoft SharePoint administration web site, try the following:

- Make sure that Javascript is enabled in your web browser.
- Add the Sophos for Microsoft SharePoint administration web site to the list of trusted sites in your web browser.
- If you are opening the administration web site from another computer, make sure that access is not blocked by a firewall.
- If your web browser is configured to use a proxy server, you might need to configure it to (a) either not use a proxy or (b) bypass the proxy server for local addresses.

**Note:** By default, Sophos for Microsoft SharePoint is not configured to use the SSL secured communication. If you want to secure it manually, use the Internet Information Services (IIS) Manager MMC console and configure the 'Sophos for Microsoft SharePoint' website. For more information see the IIS Manager Help.

## 5.5 Allow a user to manage Sophos for Microsoft SharePoint

If you are a domain administrator or a member of the Windows Administrators group, you can allow a user to manage Sophos for Microsoft SharePoint.

To do this, you add the user as a member of the Sophos for Microsoft SharePoint Administrators group that was mentioned during installation.

# 6 Scan types

Sophos for Microsoft SharePoint lets you perform three types of scans:

### On-access scan

A scan that intercepts files as they are accessed, and grants access to only those that do not pose a threat to your computer or are authorized for use.

### On-demand scan

A scan of the SharePoint store, or parts of the SharePoint store, that you can run immediately.

### Scheduled scan

A scan of the SharePoint store, or parts of the SharePoint store, that runs at a set time.

You can manage each of these scans individually by selecting it from the left pane on the **Configuration** tab. By default, the configuration tab displays the on-access scan control page.

# 7 Ensure on-access scan is enabled

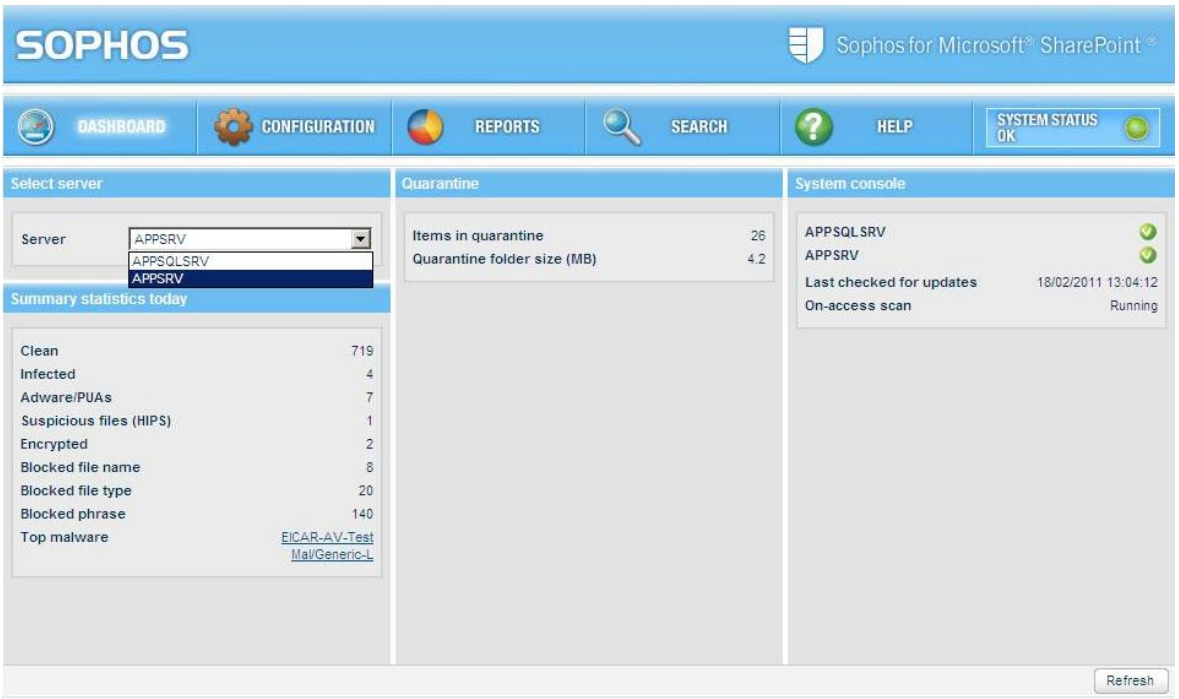
By default, on-access scanning is enabled for Sophos for Microsoft SharePoint.

**Note:** Microsoft SharePoint or Microsoft Office products may provide incorrect warning messages when the on-access scan blocks files. For information on the messages that are displayed, see *http://www.sophos.com/support/knowledgebase/article/55263.html*.

To ensure that on-access scanning is enabled:

- Open Sophos for Microsoft SharePoint. On the navigation bar, the **System status** tab should display **OK** with a green icon.

  In the **Dashboard** tab, under **System Console** section, all the servers in the configuration group should have the text **Running** against on-access scan.



# 8 Scan a specific location

You can choose to scan only specific areas and files within the SharePoint store when you perform an on-demand or scheduled scan.

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.

To scan a specific location:

1. Open Sophos for Microsoft SharePoint. On the navigation bar, click the **Configuration** tab.

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

2. Click **On-demand scan** and then click **Scan target settings**.

   The scan target settings page is displayed.

3. In the **Scan Location** tab, select one of the options:

   - **Scan all locations**
   - **Scan all locations selected below**
   - **Scan all locations except those selected below**

4. Choose the locations that you want to scan from the SharePoint data store structure displayed.

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

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

   - To remove all locations, click "Remove all" button.

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

5. In the **Scan files** tab, specify the file names to be scanned within the selected location(s).

   You must specify each filter on a new line. The file names can contain the wildcard '*' and '?'. The file names specified are **not** case-sensitive.

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

7. To start the scan, under on-demand scan, click **Scan control** and click **Start**.

**Note:** If you modify and save settings while an on-demand scan is active, the changes will take effect the next time the scan is started.

# 9 Schedule a scan

You can schedule a scan to run on a particular day and time. You can also choose to scan the whole or only a part of the SharePoint store during a scheduled scan by editing **Scan target settings** in the **Scheduled scan** menu.

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.

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:

1. Open Sophos for Microsoft SharePoint, on the navigation bar click **Configuration** tab.

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

2. Click **Scheduled scan** and then click **Schedule settings**.

   The schedule settings page is displayed.

3. Select **Schedule this scan**.
4. Select the **Days when the scan will run**.
5. Specify the **Scan start time**.
6. You can set the **Number of minutes after which scan should be aborted**, to specify the number of minutes after which the scan is stopped, if it is not yet complete.
7. Click **Apply** to save the settings.

**Note:** If you modify and save settings while a scheduled scan is active, the changes will take effect the next time the scan is started.

# 10 Configure anti-virus

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

To configure anti-virus policies:

1. Open Sophos for Microsoft SharePoint. On the navigation bar, click the **Configuration** tab.

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

2. Select a scan and click **Anti-virus policy**.

   The **Anti-virus policy** page displays the following rules:

   - **On infection**

     Specifies action for known malware, such as, viruses, Trojans, and spyware. The default action is set to **Replace with text**. This replaces the file in SharePoint store with a text file using the same file name. The text to be replaced is configurable.

   - **On adware/PUA**

     Specifies action for known adware and potentially unwanted applications. The default action for on-access scan is set to **Block**, for on-demand and scheduled scan no action is specified. By default this rule is disabled.

   - **On suspicious file (HIPS)**

     Specifies action for items that are not known to be malware but contents appear to be suspicious and could most likely be malware. By default no action is specified and this rule is disabled.

   - **On encrypted**

     Specifies action for files that are encrypted, such as, password protected files. By default no action is specified.

3. You can click on a policy to modify it. For information on how to edit an anti-virus policy, see *Modify an existing policy* (page 12).

For information on supported actions and configuring the anti-virus settings, see the Sophos for Microsoft SharePoint help.

# 11 Configure content filtering

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

**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.

To change content filtering rules:

1. Open Sophos for Microsoft SharePoint. On the navigation bar, click the **Configuration** tab.

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

2. Select a scan and click **Content filtering policy**.

   The following default rules are available:

   - **On restricted file types**

     These files include common virus carrier file types.

   - **On offensive language**

     This includes regular expressions for blocking offensive phrases.

   **Note:** You can click on a rule name to view or edit details for an existing rule.

3. You can click on a policy to modify it. For information on how to edit a content filtering policy, see *Modify an existing policy* (page 12).

For information on how to create a new rule, block content based on file names, file types, and phrases, or modify an existing content filtering policy, see the *Sophos for Microsoft SharePoint user manual.*

# 12 Modify an existing policy

You can modify an existing anti-virus policy or content filtering policy.

To modify a policy:

1. Open Sophos for Microsoft SharePoint. On the navigation bar, click the **Configuration** tab.

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

2. Select a scan and click on the **Anti-virus policy** or **Content filtering policy** that you want to modify.
3. The **Edit policy rule** window is displayed. Click **Next**.

   **Note:** Some of the options described below cannot be modified based on the policy that is chosen.

4. In **Rule Type**, an option is displayed based on the chosen policy. Click **Next**.

5. 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 but lets you continue to use it. |
| **Replace with text** | Replaces the file in the SharePoint store with a text file using the same file name and extension. The replacement text 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.<br>**Note:** This option is only available for on-access scan. |
| **Quarantine and block** | Quarantines the file and blocks it from being used.<br>**Note:** This option is only available for on-access scan. |

   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 *Set up alerts* (page 13).

6. 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. Click **Finish**.

   For information on configuring the replacement text, see Sophos for Microsoft SharePoint Help.

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

# 13 Set up alerts

Sophos for Microsoft SharePoint sends alerts to the administrator email address specified during installation with a default email template. You can customize the content of the email that is received, and modify the email addresses.

To configure alerts:

1. In the Sophos for Microsoft SharePoint window. On the navigation bar, click the **Configuration** tab.

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

2. Click **System** and then click **Alert and Email settings**.

   The **Alert and Email settings** page is displayed.

3. To modify the content of email, under the **Template** section:

   a) Enter the **Alert subject**, this appears as the subject of the alert.

   b) Enter the **Alert body**, this appears as the main body of the alert.

   c) Enter the **Text for each incident**, this can be any unique per-incident text you want to display.

   For a list of substitution symbols and their values, see the *Sophos for Microsoft SharePoint Help.*

4. To add or modify email addresses, under the **Address** section:

   a) Enter the email address to which the alert messages must be sent, one per line.

   The list can be empty in which case no alert message is sent.

   b) Enter the **Sender email address**, this appears as the sender of the alert messages.

   The sender email address cannot be empty.

   c) Enter the **SMTP mail server** address.

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

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

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.

# 14 Quarantine items

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 disk. You can choose to disinfect, delete, or authorize the items that are classified as PUA or suspicious.

For information on how to search for quarantine items and the actions that can be performed on quarantined items, see the *Sophos for Microsoft SharePoint user manual.*

# 15 Back up and restore configuration

Sophos for Microsoft SharePoint lets you export and import configuration as an XML file. This lets you save and apply the configuration to multiple SharePoint servers.

**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.

To back up and restore configuration:

1. In the Sophos for Microsoft SharePoint window. On the navigation bar, click the **Configuration** tab.

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

2. Click **System**, and then click **Back up/Restore**.

   The Back up/ Restore option page is displayed.

3. To back up the existing configuration, click **Download**.

   A dialog box appears to save the configuration file.

4. To restore the configuration, or apply the configuration on another server, click **Browse** to open the saved configuration file and then click **Upload**.

A message appears indicating the settings have been successfully restored from the uploaded file.

# 16 Uninstalling Sophos for Microsoft SharePoint

## 16.1 Uninstall sequence

The Sophos for Microsoft SharePoint uninstallation process will only remove Sophos for Microsoft SharePoint from the computer. If you want to remove Sophos Anti-Virus and Sophos AutoUpdate also, you must uninstall them individually in the following order:

1. Sophos for Microsoft SharePoint
2. Sophos Anti-Virus
3. Sophos AutoUpdate

## 16.2 Uninstall Sophos for Microsoft SharePoint

To uninstall Sophos for Microsoft SharePoint:

1. If the Sophos for Microsoft SharePoint window is open at any location, close it.
2. Open **Control Panel** and double-click **Add/Remove Programs**.
3. In the **Add/Remove Programs** dialog box, select Sophos for Microsoft SharePoint and click **Remove**.
4. In the **Confirm Uninstall** message box, click **Yes**.

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

# 17 Appendix: Database Mirroring

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

To use mirrored databases with Sophos for Microsoft SharePoint, you must perform the following:

- *Prepare SQL Server instances* (page 16)
- *Install Sophos for Microsoft SharePoint with database mirroring* (page 17)
- *Configure Sophos for Microsoft SharePoint for database mirroring* (page 17)

## 17.1 Prepare SQL Server instances

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

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

For information on SQL Server preparation for mirroring, see:

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

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

**Note:**

- Ensure that the SQL Server instances are authenticated to access each other. This means that the accounts under which a SQL Server instances run must be granted access to the other SQL Server instances used in the mirror set, and that remote connections (for example, over the TCP/IP protocol) must be enabled.

- The principal and mirror server instances should host the same edition of SQL Server, and it should be an edition that supports mirroring.
- For automatic failover, a witness server is required.
- For high-availability, the SQL Server instances must be installed on different physical servers and use synchronous mode.
- If any firewalls exist between the SQL Servers, they must be configured to allow the SQL servers to communicate over the TCP port chosen for mirroring.
- It is recommended that SQL installations use the same SQL instance name and file paths on all servers.

## 17.2 Install Sophos for Microsoft SharePoint with database mirroring

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

**Example:** Server1\Instance1;Server2\Instance1

**Note:** Do not include the name of any witness server in the list of instance names.

When the instance names are specified separated with a semi-colon, the Sophos for Microsoft SharePoint installer will install the SQL Server Native Client, if it is not already present on the system. If an earlier version of SQL Native Client is available, Sophos for Microsoft SharePoint will upgrade it to SQL Native Client for SQL Server 2008 SP1.

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

## 17.3 Configure Sophos for Microsoft SharePoint for database mirroring

Once the Sophos for Microsoft SharePoint installation is completed, the databases and Sophos for Microsoft SharePoint login will have been created on the principal server instance.

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

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

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

1. Create the Sophos for Microsoft SharePoint login on the mirror server instance:

   **[Mirror]> CREATE LOGIN [<domain name>\SophosSharePoint] FROM WINDOWS**

   **<domain name>** must be replaced with the actual domain of your Sophos for Microsoft SharePoint server, or with the machine name if in a Workgroup.

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

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

   **[Principal]> BACKUP DATABASE [SavspCnfg] TO DISK = '<path>\SavspCnfg.bak'**
   **[Principal]> BACKUP DATABASE [SavspDir] TO DISK = '<path>\SavspDir.bak'**
   **[Principal]> BACKUP DATABASE [SavspQuar] TO DISK = '<path>\SavspQuar.bak'**
   **[Principal]> BACKUP DATABASE [SavspRprt] TO DISK = '<path>\SavspRprt.bak'**

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

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

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

   **[Mirror]> RESTORE DATABASE [SavspCnfg] FROM DISK = '<path>\SavspCnfg.bak' WITH NORECOVERY**
   **[Mirror]> RESTORE DATABASE [SavspDir] FROM DISK = '<path>\SavspDir.bak' WITH NORECOVERY**
   **[Mirror]> RESTORE DATABASE [SavspQuar] FROM DISK = '<path>\SavspQuar.bak' WITH NORECOVERY**
   **[Mirror]> RESTORE DATABASE [SavspRprt] FROM DISK = '<path>\SavspRprt.bak' WITH NORECOVERY**

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

   If the path names of the principal and mirror databases differ then it will be necessary to use the MOVE option of the RESTORE command. For example:

   **[Mirror]> RESTORE DATABASE [SavspCnfg] FROM DISK = <path>\SavspCnfg.bak' WITH NORECOVERY,**
   **MOVE 'SavspCnfg' TO 'C:\Program Files\Microsoft SQL Server\MSSQL.1\MSSQL\DATA\Savspcnfg.mdf',**
   **MOVE 'SavspCnfg_log' TO 'C:\Program Files\Microsoft SQL Server\MSSQL.1\MSSQL\DATA\SavspCnfg_1.LDF'**

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

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

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

   **<port>** must be replaced with a TCP port number to be used for the endpoint. For example, 7022.

5. Create an endpoint on the mirror server instance:

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

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

   **[Mirror]> ALTER DATABASE [SavspCnfg] SET PARTNER = 'TCP://<hostname>:<port>'**
   **[Mirror]> ALTER DATABASE [SavspDir] SET PARTNER = 'TCP://<hostname>:<port>'**
   **[Mirror]> ALTER DATABASE [SavspQuar] SET PARTNER = 'TCP://<hostname>:<port>'**
   **[Mirror]> ALTER DATABASE [SavspRprt] SET PARTNER = 'TCP://<hostname>:<port>'**

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

   **<port>** must be replaced with a TCP port number to be used for the endpoint. For example, 7022.

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

   **[Principal]> ALTER DATABASE [SavspCnfg] SET PARTNER = 'TCP://<hostname>:<port>'**
   **[Principal]> ALTER DATABASE [SavspDir] SET PARTNER = 'TCP://<hostname>:<port>'**
   **[Principal]> ALTER DATABASE [SavspQuar] SET PARTNER = 'TCP://<hostname>:<port>'**
   **[Principal]> ALTER DATABASE [SavspRprt] SET PARTNER = 'TCP://<hostname>:<port>'**

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

   **<port>** must be replaced with a TCP port number to be used for the endpoint. For example, 7022.

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

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

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

   **<port>** must be replaced with a TCP port number to be used for the endpoint. For example, 7022.

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

   **[Principal]> ALTER DATABASE [SavspCnfg] SET WITNESS = 'TCP://<hostname>:<port>'**
   **[Principal]> ALTER DATABASE [SavspDir] SET WITNESS = 'TCP://<hostname>:<port>'**
   **[Principal]> ALTER DATABASE [SavspQuar] SET WITNESS = 'TCP://<hostname>:<port>'**
   **[Principal]> ALTER DATABASE [SavspRprt] SET WITNESS = 'TCP://<hostname>:<port>'**

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

   **<port>** must be replaced with a TCP port number to be used for the endpoint. For example, 7022.

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

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

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

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

11. If necessary, increase the ping timeout for the connections as follows:

    **[Principal]> ALTER DATABASE [SavspCnfg] SET PARTNER TIMEOUT <integer>**
    **[Principal]> ALTER DATABASE [SavspDir] SET PARTNER TIMEOUT <integer>**
    **[Principal]> ALTER DATABASE [SavspQuar] SET PARTNER TIMEOUT <integer>**
    **[Principal]> ALTER DATABASE [SavspRprt] SET PARTNER TIMEOUT <integer>**

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

# 18 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.

# 19 Legal notices