

Preventing Symantec AntiVirus Corporate Edition 9.x and 10.x from scanning the Brightmail directory structure

Situation:

This document describes how to prevent Symantec AntiVirus Corporate Edition 9.x and 10.x from scanning the Brightmail directory structure.

Solution:

On any mail server, certain folders must be excluded from scanning by Symantec AntiVirus. Although Brightmail is not a mail server, the way that it processes mail messages requires that its file structure must be excluded for similar reasons. If Auto-Protect scans the Brightmail directory structure, it can cause false positive virus detections, unexpected behavior on the server, or damage to the Brightmail databases. This is true of all antivirus programs that run on mail servers.



The folders to exclude depend on the version of Brightmail that you use.

Brightmail 5.5.x and Brightmail 6.0

- <Drive>:\mysql\data\
Exclude this folder only if the Brightmail Quarantine component is installed.
- <Drive>:\Program Files\Brightmail

Brightmail 6.0.x

- <Drive>:\mysql\data\
Exclude this folder only if the Brightmail Quarantine component is installed.
- <Drive>:\Program Files\Symantec\sbas\Scanner

To create the exclusions, follow the steps outlined in the sections below. Click an icon to either expand () or collapse () each section. (If you cannot expand a section, then read the document [Cannot expand sections in a Symantec Knowledge Base document.](#))

Servers

When Symantec AntiVirus 9.x server is on a server running Brightmail, configure exclusions for Auto-Protect through the Symantec System Center. Manual scans should still be run from within Symantec AntiVirus, so that the exclusions can be created.

To configure exclusions for Auto-Protect from the Symantec System Center

1. Start the Symantec System Center, and unlock the server group.
2. Right-click the server that runs Brightmail, and then click **All Tasks > Symantec AntiVirus > Server Auto-Protect Options**.
3. Check **Exclude selected files and folders**.
4. Click **Exclusions**.
5. Click **Files/Folders** to create the exclusions.
6. Exclude all necessary Brightmail folders by clicking once in the empty box to the left of each folder.

To configure exclusions for a scheduled scan from the Symantec System Center

1. Start Symantec System Center, and unlock the server group.
2. Right-click the server group, and then click **All Tasks > Symantec AntiVirus > Scheduled Scans**.

3. Create a scheduled scan, or edit an existing one.
4. Click **Scan Settings**.
5. Select the drives, folders, or files to scan.
6. Click **Options**.
7. Check **Exclude files and folders**, and then click **Exclusions**.
8. Click **Files/Folders** to create the exclusions.
9. Exclude all necessary Brightmail folders by clicking once in the empty box to the left of each directory.

To start a manual scan with the appropriate exclusions from within Symantec AntiVirus

1. Start Symantec AntiVirus.
2. Click **Scan > Scan Computer**.
3. Select the drives, folders, or files to scan.
4. In the lower-right corner, click **Options**.
5. Check **Exclude files and folders**.
6. Click **Exclusions**.
7. Click **Files/Folders** to create the exclusions.
8. Exclude all necessary Brightmail folders by clicking once in the empty box to the left of each directory.



Unmanaged clients

If the server running Brightmail is configured as an unmanaged client, you must configure all exclusions from within Symantec AntiVirus, and you must not install the Email Tools.

To configure exclusions for Auto-Protect from within Symantec AntiVirus

1. Start Symantec AntiVirus.
2. Click **Configure**, and then click **File System Auto-Protect**.
3. Click **Exclude selected files and folders**.
4. Click **Exclusions**.
5. Click **Files/Folders** to create the exclusions.
6. Exclude all necessary Brightmail folders by clicking once in the empty box to the left of each directory.

To configure exclusions for a scheduled scan from within Symantec AntiVirus

1. Start Symantec AntiVirus.
2. Click **Scheduled Scans**.
3. Create a new scan, or select the scan you wish to configure, and click **Next** twice.
4. Select the drives, folders, or files to scan.
5. In the lower-right corner, click **Options**.
6. Click **Exclude files and folders**.
7. Click **Exclusions**.
8. Click **Files/Folders** to create the exclusions.
9. Exclude all necessary Brightmail folders by clicking once in the empty box to the left of each directory.

To start a manual scan with the appropriate exclusions from within Symantec AntiVirus

1. Start Symantec AntiVirus.
2. Click **Scan**, and then click **Scan Computer**.
3. Select the drives, folders, or files to scan.
4. In the lower-right corner, click **Options**.

5. Click **Exclude files and folders**.
6. Click **Exclusions**.
7. Click **Files/Folders** to create the exclusions.
8. Exclude all necessary Brightmail folders by clicking once in the empty box to the left of each directory.



Managed clients

If the server running Brightmail is configured as a managed client in a client group that you have created specifically for Brightmail, configure the exclusions through the Symantec System Center. Manual scans should be run from within Symantec AntiVirus, and should be configured there.

Notes:

- The server running Brightmail should not be configured as a managed client unless it is in a client group specifically for Brightmail.
- If Symantec AntiVirus is installed as a client, you must not install the Email Tools.

To configure exclusions for Auto-Protect from the Symantec System Center

1. Start the Symantec System Center, and unlock the server group.
2. Under Groups, right-click the client group, and then click **All Tasks > Symantec AntiVirus > Client Auto-Protect Options**.
3. Check **Exclude selected files and folders**, and click the lock icon so that it appears as locked.
4. Click **Exclusions**.
5. Click **Files/Folders** to create the exclusions.
6. Exclude all necessary Brightmail folders by entering the full paths of each folder, one on each line.

To configure exclusions for a scheduled scan from the Symantec System Center

1. Start the Symantec System Center, and unlock the server group.
2. Under Groups, right-click the client group, and then click **All Tasks > Symantec AntiVirus > Scheduled Scans**.
3. Create a scheduled scan, or edit an existing one.
4. Click **Scan Settings**.
5. Click **Options**.
6. Check **Exclude files and folders**, and then click **Exclusions**.
7. Click **Folders** to create the exclusions.
8. Exclude all necessary Brightmail folders by entering the full paths of each folder, one on each line.

To start a manual scan with the appropriate exclusions from within Symantec AntiVirus

1. Start Symantec AntiVirus.
2. Click **Scan**, and then click **Scan Computer**.
3. Select the drives, folders, or files to scan.
4. In the lower-right corner, click **Options**.
5. Click **Exclude files and folders**.
6. Click **Exclusions**.
7. Click **Files/Folders** to create the exclusions.

8. Exclude all necessary Brightmail folders by clicking once in the empty box to the left of each directory.

Translations of this Document:

Given the time needed to translate documents into other languages, the translated versions of this document may vary in content if the English document was updated with new information during the translation process. The English document always contains the most up-to-date information.