# File-Level Antivirus Scanning on Exchange 2007

***Applies to:*** *Exchange Server 2007 SP2, Exchange Server 2007 SP1, Exchange Server 2007* ***Topic Last Modified:*** *2009-07-22*

This topic describes the effects of file-level antivirus programs on computers that are running Microsoft Exchange Server 2007. If you implement the recommendations described in this topic, you can enhance the security and health of your Exchange organization.

File-level scanners are frequently used. However, if they are configured incorrectly, they can cause problems in Exchange 2007.

There are two types of file-level scanners:

- *Memory-resident file-level scanning* refers to a part of file-level antivirus software that is loaded in memory at all times. It checks all the files that are used on the hard disk and in computer memory.
- *On-demand file-level scanning* refers to a part of file-level antivirus software that you can configure to scan files on the hard disk manually or on a schedule. Some versions of antivirus software start the on-demand scan automatically after virus signatures are updated to make sure that all files are scanned with the latest signatures.

The following problems may occur when you use file-level scanners with Exchange 2007:

- File-level scanners may scan a file when the file is being used or at a scheduled interval. This can cause the scanners to lock or quarantine an Exchange log or a database file while Microsoft Exchange tries to use the file. This behavior may cause a severe failure in Microsoft Exchange and may also cause -1018 errors.
- File-level scanners do not provide protection against e-mail viruses, such as the Melissa virus.

**Note:**

The Melissa virus was a Trojan horse macro virus that propagated itself through e-mail messages in 1999. The virus sent e-mail messages that had malicious attachments to addresses that it found in the personal address books on Microsoft Outlook mail clients. Such viruses can cause data destruction.

## Exchange 2007 Recommendations

If you are deploying file-level scanners on Exchange 2007 servers, make sure that the appropriate exclusions, such as directory exclusions, process exclusions, and file name extension exclusions, are in place for both scheduled and real-time scanning. This section describes directory exclusions, process exclusions, and file name extension exclusions for each server or server role.

### Directory Exclusions

You must exclude specific directories for each Exchange server or server role on which you run a file-level antivirus scanner. This section describes the directories that you should exclude from file-level scanning for each server or server role.

Mailbox server role

- Exchange databases, checkpoint files, and log files across all storage groups. By default, these are located in sub-folders under the %Program Files%\Microsoft\Exchange Server\Mailbox folder. You can obtain the directory location by running the following commands in the Exchange Management Shell:
  - To determine the location of a transaction log and checkpoint file, run the following command:

    ```
    Get-StorageGroup -server <servername>| fl *path*
    ```

  - To determine the location of a mailbox database, run the following command:

    ```
    Get-MailboxDatabase -server <servername>| fl *path*
    ```

  - To determine the location of a public folder database, run the following command:

```
Get-PublicFolderDatabase -server <servername>| fl *path*
```

- Database content indexes. By default, these are located in storage group sub-folders under the %Program Files%\Microsoft\Exchange Server\Mailbox folder.
- General log files, such as message tracking log files. These files are located in subfolders under the %Program Files%\Microsoft\Exchange Server\TransportRoles\Logs folder and %Program Files%\Microsoft\Exchange Server\Logging folder. To determine the log paths being used, run the following command in the Exchange Management Shell:

```
Get-MailboxServer <servername>| fl *path*
```

- The Offline Address Book files that are located in subfolders under the %Program Files%\Microsoft\Exchange Server\ExchangeOAB folder
- IIS system files in the %SystemRoot%\System32\Inetsrv folder
- The temporary folder that is used with offline maintenance utilities, such as Eseutil.exe. By default, this folder is the location where the .exe file is run from. However, you can configure where you perform the operation from when you run the utility.
- The temporary folders that are used to perform conversions:
    - Content conversions are performed in the server's TMP folder.
    - OLE conversions are performed in %Program Files%\Microsoft\Exchange Server \Working\OleConvertor folder.
    - The Mailbox database temporary folder: %Program Files%\Microsoft \Exchange Server\Mailbox\MDBTEMP
- Any Exchange-aware antivirus program folders

Clustered Mailbox server
All the items listed in the Mailbox server role list, and the following:

- The quorum disk and the %Winnt%\Cluster folder
- The file share witness. This is located on another server in the environment, typically a Hub Transport server.
- The ExchangeOAB directory on a shared drive. The location is specified by the registry key SYSTEM\CurrentControlSet\Services\MSExchangeSA\Parameters\<CMS-name>\OabDropFolderLocation

> **Note:**
>
> By default, the ExchangeOAB directory is at the following location: %Program Files%\Microsoft\Exchange Server\ExchangeOAB

Hub Transport server role

- General log files, for example, message tracking. These files are located in subfolders under the %Program Files%\Microsoft\Exchange Server\TransportRoles\Logs folder. To determine the log paths being used, run the following command in the Exchange Management Shell:

```
Get-TransportServer <servername>| fl *logpath*,*tracingpath*
```

- The message folders that are located under the %Program Files%\Microsoft \Exchange Server\TransportRoles folder. To determine the paths being used, run the following command in the Exchange Management Shell:

```
Get-TransportServer <servername>| fl *dir*path*
```

- The transport server role queue database, checkpoint, and log files that are located in the %Program Files%\Microsoft\Exchange Server\TransportRoles\Data\Queue folder. For more information about how to obtain the directory location if the queue database files have been moved from the default location, see Working with the Queue Database on Transport Servers [ http://technet.microsoft.com/en-us/library/bb124343(EXCHG.80).aspx ] .
- The transport server role Sender Reputation database, checkpoint, and log files that are located in the %Program Files%\Microsoft\Exchange Server\TransportRoles \Data\SenderReputation folder
- The transport server role IP filter database, checkpoint, and log files that are located in the %Program Files%\Microsoft\Exchange Server\TransportRoles\Data\IpFilter folder
- The temporary folders that are used to perform conversions:
    - Content conversions are performed in the server's TMP folder.
    - OLE conversions are performed in %Program Files%\Microsoft\Exchange Server

\Working\OleConvertor folder.

- Any Exchange-aware antivirus program folders

Edge Transport server role

- The Active Directory Application Mode (ADAM) database and log files that are located in the %Program Files%\Microsoft\Exchange Server\TransportRoles\Data\Adam folder. For more information about how to obtain the directory location if the ADAM database files have been moved from the default location, see How to Modify ADAM Configuration [ http://technet.microsoft.com/en-us/library/aa997269(EXCHG.80).aspx ] .
- General log files, for example message tracking. These files are located in subfolders under the %Program Files%\Microsoft\Exchange Server\TransportRoles\Logs folder. To determine the log paths being used, run the following command in the Exchange Management Shell:

```
Get-TransportServer <servername>| fl *logpath*,*tracingpath*
```

- The message folders that are located under the %Program Files%\Microsoft \Exchange Server\TransportRoles folder. To determine the log paths being used, run the following command in the Exchange Management Shell:

```
Get-TransportServer <servername>| fl *dir*path*
```

- The transport server role queue database, checkpoint, and log files that are located in the %Program Files%\Microsoft\Exchange Server\TransportRoles\Data\Queue folder. For more information about how to obtain the directory location if the queue database files have been moved from the default location, see Working with the Queue Database on Transport Servers [ http://technet.microsoft.com/en-us/library/bb124343(EXCHG.80).aspx ] .
- The transport server role Sender Reputation database, checkpoint, and log files that are located in the %Program Files%\Microsoft\Exchange Server\TransportRoles \Data\SenderReputation folder
- The transport server role IP filter database, checkpoint, and log files that are located in the %Program Files%\Microsoft\Exchange Server\TransportRoles\Data\IpFilter folder
- The temporary folders that are used to perform conversions:
    - Content conversions are performed in the server's TMP folder.
    - OLE conversions are performed in %Program Files%\Microsoft\Exchange Server \Working\OleConvertor folder.
- Any Exchange-aware antivirus program folders

Client Access server role

- The Internet Information Services (IIS) 6.0 compression folder that is used with Microsoft Outlook Web Access. By default, the compression folder in IIS 6.0 is located at %systemroot%\IIS Temporary Compressed Files.
  For more information, see the Microsoft Knowledge Base article 817442, A 0-byte file may be returned when compression is enabled on a server that is running IIS [ http://go.microsoft.com/fwlink/?LinkId=3052&kbid=817442 ] .
- IIS system files in the %SystemRoot%\System32\Inetsrv folder
- The Internet-related files that are stored in the sub-folders of the %Program Files%\Microsoft\Exchange Server\ClientAccess folder
- The temporary folder that is used to perform content conversion. By default, this is the server's TMP folder.

Unified Messaging server role

- The grammar files that are stored in the subfolders in the %Program Files%\Microsoft \Exchange Server\UnifiedMessaging\grammars folder
- The voice prompts that are stored in the subfolders in the %Program Files%\Microsoft \Exchange Server\UnifiedMessaging\Prompts folder
- The voicemail files that are stored in the %Program Files%\Microsoft\Exchange Server \UnifiedMessaging\voicemail folder
- The bad voicemail files that are stored in the %Program Files%\Microsoft\Exchange Server \UnifiedMessaging\badvoicemail folder

Microsoft ForeFront Security for Exchange Server

- The archived messages that are stored in the %Program Files%\Microsoft ForeFront Security\Exchange Server\Data\Archive folder
- The quarantined files that are stored in the %Program Files%\Microsoft ForeFront Security \Exchange Server\Data\Quarantine folder
- The antivirus engine files that are stored in the subfolders of

%Program Files%\Microsoft ForeFront Security\Exchange Server\Data\Engines\x86 folder
- The configuration files that are stored in the %Program Files%\Microsoft ForeFront Security \Exchange Server\Data folder

Microsoft ForeFront Security For Exchange Server on Single Copy Clusters (SCC)
In addition to the directories that contain antivirus engine and configuration files, exclude the directory on the shared storage used for ForeFront data.

To determine the path that ForeFront uses on an SCC, check the value of the following registry key:

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Forefront Server Security\Exchange Server\DatabasePath

Incorrectly editing the registry can cause serious problems that may require you to reinstall your operating system. Problems resulting from editing the registry incorrectly may not be able to be resolved. Before editing the registry, back up any valuable data.

### Process Exclusions

Many file-level scanners now support the scanning of processes. This too can adversely affect Microsoft Exchange if the incorrect processes are scanned. Therefore, you should exclude the following processes from file-level scanners.

| | |
|---|---|
| Cdb.exe | Microsoft.Exchange.Search.Exsearch.exe |
| Cidaemon.exe | Microsoft.Exchange.Servicehost.exe |
| Cluster.exe | Msexchangeadtopologyservice.exe |
| Dsamain.exe | Msexchangefds.exe |
| Edgecredentialsvc.exe | Msexchangemailboxassistants.exe |
| Edgetransport.exe | Msexchangemailsubmission.exe |
| Galgrammargenerator.exe | Msexchangetransport.exe |
| Inetinfo.exe | Msexchangetransportlogsearch.exe |
| Mad.exe | Msftefd.exe |
| Microsoft.Exchange.Antispamupdatesvc.exe | Msftesql.exe |
| Microsoft.Exchange.Contentfilter.Wrapper.exe | Oleconverter.exe |
| Microsoft.Exchange.Cluster.Replayservice.exe | Powershell.exe |
| Microsoft.Exchange.Edgesyncsvc.exe | Sesworker.exe |
| Microsoft.Exchange.Imap4.exe | Speechservice.exe |
| Microsoft.Exchange.Imap4service.exe | Store.exe |
| Microsoft.Exchange.Infoworker.Assistants.exe | Transcodingservice.exe |
| Microsoft.Exchange.Monitoring.exe | Umservice.exe |
| Microsoft.Exchange.Pop3.exe | Umworkerprocess.exe |
| Microsoft.Exchange.Pop3service.exe | W3wp.exe |

If you are also deploying ForeFront Security for Exchange Server, exclude the following processes.

| | |
|---|---|
| Adonavsvc.exe | Fscstatsserv.exe |
| Fsccontroller.exe | Fsctransportscanner.exe |
| Fscdiag.exe | Fscutility.exe |
| Fscexec.exe | Fsemailpickup.exe |
| Fscimc.exe | Fssaclient.exe |
| Fscmanualscanner.exe | Getenginefiles.exe |
| Fscmonitor.exe | Perfmonitorsetup.exe |
| Fscrealtimescanner.exe | Scanenginetest.exe |
| Fscstarter.exe | Semsetup.exe |

### File Name Extension Exclusions

In addition to excluding specific directories and processes, as a secondary measure, in case directory exclusions fail or files are moved, you should exclude the following Exchange-specific file name extensions.

Application-related extensions

- .config
- .dia
- .wsb

Database-related extensions

- .chk
- .log
- .edb
- .jrs
- .que

Offline Address Book-related extensions:

- .lzx

Content Index-related extensions

| | | |
|---|---|---|
| .ci | .wid | .001 |
| .dir | .000 | .002 |

Unified Messaging-related extensions

- .cfg
- .grxml

ForeFront Security for Exchange Server–related extensions

| | | |
|---|---|---|
| .avc | .dt | .lst |
| .cab | .fdb | .mdb |
| .cfg | .fdm | .ppl |
| .config | .ide | .set |
| .da1 | .key | .v3d |
| .dat | .klb | .vdb |

| | | |
|---|---|---|
| .def | .kli | .vdm |

The file name extensions listed for ForeFront Security for Exchange Server are the signature files from various antivirus directory engines. In most cases, these file name extensions do not change, but file name extensions may be added in the future as third-party antivirus vendors update their antivirus signature files.

**Tags:** av exclusions

## Community Content

**This list of Exchange AV exclusions is crazy!** Last Edit 3:10 AM by Anthony Maw

The list of exclusions here is enough to be bewildering to even experienced Exchange administrators and the probability of error is HIGH. Does anybody at Microsoft actually recommend that users actually try to exclude all these hundreds of this-and-that items?

**Tags:**

**IIS 7 Temporary Compressed files folder** Last Edit 8:32 AM by Lasse Pettersson -

When running IIS7 the "Temporary Compressed files" folder is located in **C:\Inetpub\temp**

**Tags:**

**All these exclusions leave HUGE security holes...** Last Edit 4:51 AM by MIDAC

Well, if I was a virus I would certainly try to hide in any of the folders discussed here... and there are many to choose from! I cannot believe the recommendation is to exclude the server's TMP folder too?

**Tags:**

**Trying to find the TMP folder for "content conversion" ?** Last Edit 9:54 PM by evilution13B

· The temporary folder that is used to perform content conversion. By default, this is the server's TMP folder. --> I'm probably reading more into this but wanted to validate the correct folder (running Win2008 64BIT). Is the "TMP" folder actaully "C:\Windows\Temp" or another folder? There is a "TMP" folder under documents and settings for each local user profile but that doesn't make sense. I'm sure this is simple but wanted to validate 100% for the exclusion list. Thanks

**Tags:** folder location tmp

**What is the Alternative ?** Last Edit 4:02 PM by Frank Rowland

it is complicated to run Anti-virus on exchange, but the alternative to all of these exclusions is to run NO ANTI-VIRUS at all.
Which is worse?

**Tags:**

**You can use exchange aware anti virus solutions.** Last Edit 8:43 PM by Dr. RPC

If you think that the above steps mentioned in the technet article are cubresome and complex , you are right.

As an alternative you can use exchange aware anti virus solutions.

**Tags:**