WINDOWS ANTIVIRUS EXCLUSION RECOMMENDATIONS

Servers, Clients, and Role-Specific

Abstract

This document will provide a baseline for the proper file, directory, and process antivirus exclusions to be applied to Windows servers and clients with special attention to specific roles.

Brian Helmick

Premier Field Engineer - Microsoft

Version	Revised By	Date	Comments
1.0	Brian Helmick	5/15/2013	Original Draft
1.1	Brian Helmick	8/1/2013	Added Lync Exclusions
1.2	Brian Helmick	12/18/2013	Updated Lync Exclusions
1.3	Brian Helmick	1/16/2014	Updated SCOM Exclusions
1.4	Brian Helmick	11/8/2017	Updated Exchange, Skype, SCCM, TFS

TABLE OF CONTENTS

PURPOSE AND USE

The information in this document is for the purpose of setting proper file, directory, and process exclusions on Windows servers and clients. In addition to generic exclusions which should be put in place across all servers and clients, role- and application-specific exclusions are addressed as well. Specific files and processes are noted whenever possible however, in their absence, it is implied to exclude the full directory path given. The information in this document has been gathered from numerous published sources, many of which are cited and can be accessed via the links included in the attached Appendix. This guide is intended to be used as a baseline for establishing exclusion policies, however, it is always recommended to follow up with specific product documentation and guidance in the event any recommendations have been changed or added. Please be sure to review the links specific to each product that is listed in the appendix. The collection of information in this document is a summary of the information contained within those links and more detailed information, descriptions, and specifics can often be found at those sources.

Keep in mind when using this document that these exclusion lists are cumulative. For instance, when defining exclusions for an Exchange Server that is clustered, the cumulative set of files, directories, and processes that should be excluded would include those listed under General Exclusions, Exchange, Cluster, and in some cases IIS.

Important: This document contains information that shows how to help lower security settings or how to temporarily turn off security features on a computer. Before you make these changes, it is recommended that you evaluate the risks that are associated with implementing these workarounds in your particular environment. If these workarounds are applied it is also recommended that you take any appropriate additional steps to help protect the computer. It is recommended that you temporarily apply these procedures to evaluate a system. If your system performance or stability is improved by the recommendations made here, contact your antivirus software vendor for instructions or for an updated version of the antivirus software.

The information contained within this document is current up to the point of the most recent revision date.

GENERAL EXCLUSIONS – APPLIES TO ALL CURRENTLY SUPPORTED VERSIONS OF WINDOWS CLIENT OPERATING SYSTEMS

Important: When a directory that is to be excluded has a directory name greater than 8 characters long, add both the short and long directory names of the directory to the exclusion list. These names are required by some AV programs to traverse the subdirectories.

MICROSOFT FOREFRONT FILES

- %windir%\SoftwareDistribution\Datastore
  - Tmp.edb
- %ProgramData%\Microsoft\Search\Data\Applications\Windows
  - Log files

WINDOWS UPDATE OR AUTOMATIC UPDATE RELATED FILES

- %windir%\SoftwareDistribution\Datastore
  - Datastore.edb
- %windir%\SoftwareDistribution\Datastore\Logs
  - Res*.log
  - Edb*.jrs
  - Edb.chk
  - Tmp.edb

WINDOWS SECURITY FILES

- %windir%\Security\Database
  - *.edb
  - *.sdb

  - *.log
  - *.chk
  - *.jrs

GROUP POLICY RELATED FILES

- %allusersprofile%
  - NTUser.pol
- %Systemroot%\System32\GroupPolicy
  - Registry.pol

Note: Do not exclude any one of these files based on the file name extension. For example, do not exclude all files that have a .chk extension. Microsoft has no control over other files that may use the same extensions as the files that are described above.

Note: All the files and folders that are noted above are protected by default permissions to allow only SYSTEM and administrator access, and they contain only operating system components. Excluding an entire folder may be simpler but may not provide as much protection as excluding specific files based on file names.

DOMAIN CONTROLLERS - APPLIES TO ALL CURRENTLY SUPPORTED VERSIONS OF WINDOWS SERVER

ACTIVE DIRECTORY AND ACTIVE DIRECTORY-RELATED FILES

- NTDS database files - The location of these files is specified in the following registry key:

  HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\NTDS\Parameters\DSA Database File. The default location is %windir%\Ntds.
  - Ntds.dit
- Active Directory transaction log files - The location of these files is specified in the following registry key: HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\NTDS\Parameters\Database Log Files Path. The default location is %windir%\Ntds.
  - EDB*.log
  - Res*.log
  - Edb*.jrs
  - Ntds.pat
- NTDS Working folder – The location of this folder is specified in the following registry key:

  HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\NTDS\Parameters\DSA Working Directory
  - Temp.edb
  - Edb.chk

SYSVOL FILES

- File Replication Service (FRS) Working folder files – The location of this folder is specified in the following registry key: HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\NtFrs\Parameters\Working Directory. The default location is %windir%\Ntfrs
  - edb.chk in the %windir%\Ntfrs\jet\sys folder
  - Ntfrs.jdb in the %windir%\Ntfrs\jet folder
  - *.log in the %windir%\Ntfrs\jet\log folder
- FRS Database Log files – The location of this folder is specified in the following registry key: HKEY_LOCAL_MACHINE\System\Currentcontrolset\Services\Ntfrs\Parameters\DB Log File Directory. The default location is %windir%\Ntfrs.
  - Edb*.log (if the registry key is not set).
  - FRS Working Dir\Jet\Log\Edb*.jrs (Windows Server 2008 and Windows Server 2008 R2).
- Staging folder files – The location of this folder is specified in the following registry key.

    - HKEY_LOCAL_MACHINE\System\Currentcontrolset\Services\NtFrs\Parameters\Replica Sets\GUID\Replica Set Stage. By default, staging uses the following location: %systemroot%\Sysvol\Staging areas
        - Nntfrs_cmp*.*
- Sysvol\Sysvol files - The current location of the Sysvol\Sysvol folder and all its subfolders is the file system reparse target of the replica set root. The Sysvol\Sysvol folder uses the following location: %systemroot%\Sysvol\Domain
    - *.adm
    - *.admx
    - *.adml
    - Registry.pol
    - *.aas
    - *.inf
    - Fdeploy.inf
    - Scripts.ini
    - *.ins
    - Oscfilter.ini
- FRS Preinstall folder files – Replica_root\DO_NOT_REMOVE_NtFrs_PreInstall_Directory
    - Ntfrs*.*
- DFSR database and working folder files - The location is specified by the following registry key: HKEY_LOCAL_MACHINE\System\Currentcontrolset\Services\DFSR\Parameters\Replication Groups\GUID\Replica Set Configuration File=Path >. In this registry key, "Path" is the path of an XML file that states the name of the Replication Group. In this example, the path would contain "Domain System Volume." The default location is the following hidden folder: %systemdrive%\System Volume Information\DFSR
    - db_normal
    - FileIDTable_*
    - SimilarityTable_*
    - *.xml
    - db_dirty
    - db_lost
    - Dfsr.db
    - Fsr.chk
    - *.frx
    - *.log
    - Fsr*.jrs
    - Tmp.edb

If any one of these folders or files is moved or is put in a different location, scan or exclude the equivalent element.

DFS FILES

The same resources that are excluded for a SYSVOL replica set must also be excluded when FRS or DFSR is used to replicate shares that are mapped to the DFS root and link targets on Windows Server 2008 R2-based, Windows Server 2008-based, Windows Server 2003-based, or Windows 2000-based member computers or domain controllers.

DHCP FILES

- The location of DHCP files is specified in the following registry key: HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\DHCPServer\Parameters. The DatabasePath, DhcpLogFilePath, and BackupDatabasePath parameters are the paths to focus on. The default location for these files is %systemroot%\System32\DHCP
    - *.mdb
    - *.pat
    - *.log
    - *.chk
    - *.edb

DNS FILES

- By default, DNS uses the following folder: %systemroot%\System32\Dns
  - *.log
  - *.dns
  - BOOT

WINS FILES

- By default, WINS uses the following folder: %systemroot%\System32\Wins
  - *.chk
  - *.log
  - *.mdb

Note: Use a version of antivirus software that is designed to work with Active Directory domain controllers and that uses the correct Application Programming Interfaces (APIs) to access files on the server. Older versions of most vendor software inappropriately change a file's metadata as the file is scanned. This causes the File Replication Service engine to recognize a file change and therefore schedule the file for replication. Newer versions prevent this problem.

Note: Do not put Active Directory or FRS database and log files on NTFS file system compressed volumes.

EXCHANGE SERVER 2003

FILE AND DIRECTORY EXCLUSIONS

- Exchange databases and log files across all storage groups. By default, these are located in the Exchsrvr\Mdbdata folder.
- Exchange MTA files in the Exchsrvr\Mtadata folder.
- Additional log files such as the Exchsrvr\server_name.log directory.
- The Exchsrvr\Mailroot virtual server folder.
- The working folder that is used to store streaming .tmp files that are used for message conversion. By default, this folder is Exchsrvr\Mdbdata, but the location is configurable.
- The Exchsrvr\Conndata folder.

Note: You may want to exclude the whole Exchsrvr folder from both on-demand file-level scanners and memory-resident file-level scanners.

- The temporary folder that is used in conjunction with offline maintenance utilities such as Eseutil.exe. By default, this folder is the location where the .exe file is run from, but you can configure where you run the file from when you run the utility.
- Site Replication Service (SRS) files in the Exchsrvr\Srsdata folder.
- Microsoft Internet Information Services (IIS) system files in the %SystemRoot%\System32\Inetsrv folder.
- Any messaging antivirus program folders.
- Exclude the folder that contains the checkpoint (.chk) file

Note: Even if you move the Exchange databases and log files to new locations and exclude those folders, the .chk file may still be scanned.

PROCESS EXCLUSIONS

- Cdb.exe
- Cidaemon.exe
- Store.exe
- Emsmta.exe
- Mad.exe
- Mssearch.exe
- Inetinfo.exe
- W3wp.exe

EXCHANGE SERVER 2007

FILE AND DIRECTORY EXCLUSIONS

MAILBOX SERVER ROLE

- Mailbox Databases
  - 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 (in addition to those listed above)
  - 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
    - 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.
    - 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.
    - 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.
    - 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.
    - 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

PROCESS EXCLUSIONS

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

ADDITIONAL PROCESS EXCLUSIONS (IF DEPLOYING FOREFRONT SECURITY FOR EXCHANGE SERVER)

Adonavsvc.exe	Fsccontroller.exe	Fscdiag.exe
Fscexec.exe	Fscimc.exe	Fscmanualscanner.exe
Fscmonitor.exe	Fscrealtimescanner.exe	Fscstarter.exe

Fscstatsserv.exe	Fsctransportscanner.exe	Fscutility.exe
Fsemailpickup.exe	Fssaclient.exe	Getenginefiles.exe
Perfmonitorsetup.exe	Scanenginetest.exe	Semsetup.exe

FILE NAME EXTENSION EXCLUSIONS

- 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
    - *.dir
    - *.wid
    - *.000
    - *.001
    - *.002
- Unified Messaging-related extensions
    - *.cfg
    - *.grxml
- ForeFront Security for Exchange Server–related extensions
    - *.avc
    - *.cab
    - *.cfg
    - *.config
    - *.da1
    - *.dat
    - *.def
    - *.dt
    - *.fdb
    - *.fdm
    - *.ide
    - *.key
    - *.klb
    - *.kli
    - *.lst
    - *.mdb
    - *.ppl
    - *.set
    - *.v3d
    - *.vdb
    - *.vdm

EXCHANGE SERVER 2010 AND EXCHANGE SERVER 2013

You must exclude specific directories for each Exchange server on which you run an antivirus scanner. This section describes the directories that you should exclude from file-level scanning and memory-resident scanning.

FILE AND DIRECTORY EXCLUSIONS

MAILBOX SERVERS

- Mailbox Databases
  - Exchange databases, checkpoint files, and log files. By default, these are located in sub-folders under the %ExchangeInstallPath%Mailbox folder. To determine the location of a mailbox database, transaction log, and checkpoint file, run the following command: Get-MailboxDatabase -Server <servername>| Format-List *path*
  - Database content indexes. By default, these are located in the same folder as the database file.
  - Group Metrics files. By default, these files are located in the %ExchangeInstallPath%GroupMetrics folder.
  - General log files, such as message tracking and calendar repair log files. By default, these files are located in subfolders under the %ExchangeInstallPath%TransportRoles\Logs folder and %ExchangeInstallPath%Logging folder. To determine the log paths being used, run the following command in the Exchange Management Shell: Get-MailboxServer <servername> | Format-List *path*
  - The Offline Address Book files. By default, these are located in subfolders under the %ExchangeInstallPath%ClientAccess\OAB folder.
  - IIS system files in the %SystemRoot%\System32\Inetsrv folder.
  - The Mailbox database temporary folder: %ExchangeInstallPath%Mailbox\MDBTEMP
- Members of Database Availability Groups
  - All the items listed in the Mailbox databases list, and the cluster quorum database that exists at %Windir%\Cluster.
  - The witness directory files. These files are located on another server in the environment, typically a Client Access server that isn't installed on the same computer as a Mailbox server. By default, the witness directory files are located in %SystemDrive%:\DAGFileShareWitnesses\<DAGFQDN>.
- Transport service
  - Log files, for example, message tracking and connectivity logs. By default, these files are located in subfolders under the %ExchangeInstallPath%TransportRoles\Logs folder. To determine the log paths being used, run the following command in the Exchange Management Shell: Get-TransportService <servername> | Format-List *logpath*,*tracingpath*
  - Pickup and Replay message directory folders. By default, these folders are located under the %ExchangeInstallPath%TransportRoles folder. To determine the paths being used, run the following command in the Exchange Management Shell: Get-TransportService <servername>| fl *dir*path*
  - The queue databases, checkpoints, and log files. By default, these are located in the %ExchangeInstallPath%TransportRoles\Data\Queue folder.
  - The Sender Reputation database, checkpoint, and log files. By default, these are located in the %ExchangeInstallPath%TransportRoles\Data\SenderReputation folder.
  - The temporary folders that are used to perform conversions:
    - By default, content conversions are performed in the Exchange server's %TMP% folder.
    - By default, OLE conversions are performed in %ExchangeInstallPath%Working\OleConverter folder.
  - The content scanning component is used by the Malware agent and data loss prevention (DLP). By default, these files are located in the %ExchangeInstallPath%FIP-FS folder.
- Mailbox Transport service
  - Log files, for example, connectivity logs. By default, these files are located in subfolders under the %ExchangeInstallPath%TransportRoles\Logs\Mailbox folder. To determine the log paths being used, run the following command in the Exchange Management Shell: Get-MailboxTransportService <servername> | Format-List *logpath*

- Unified Messaging
    - The grammar files for different locales, for example en-EN or es-ES. By default, these are stored in the subfolders in the %ExchangeInstallPath%UnifiedMessaging\grammars folder.
    - The voice prompts, greetings and informational message files. By default, these are stored in the subfolders in the %ExchangeInstallPath%UnifiedMessaging\Prompts folder
    - The voicemail files that are temporarily stored in the %ExchangeInstallPath%UnifiedMessaging\voicemail folder.
    - The temporary files generated by Unified Messaging. By default, these are stored in the %ExchangeInstallPath%UnifiedMessaging\temp folder.

CLIENT ACCESS SERVERS

- Web components
    - For servers using Internet Information Services (IIS) 7.0, the compression folder that is used with Microsoft Outlook Web App. By default, the compression folder for IIS 7.0 is located at %SystemDrive%\inetpub\temp\IIS Temporary Compressed Files.
    - IIS system files in the %SystemRoot%\System32\Inetsrv folder
    - Inetpub\logs\logfiles\w3svc
- POP3 and IMAP4 protocol logging
    - POP3 folder: %ExchangeInstallPath%Logging\POP3
    - IMAP4 folder: %ExchangeInstallPath%Logging\IMAP4
- Front End Transport service
    - Log files, for example, connectivity logs and protocol logs. By default, these files are located in subfolders under the %ExchangeInstallPath%TransportRoles\Logs\FrontEnd folder. To determine the log paths being used, run the following command in the Exchange Management Shell: Get-FrontEndTransportService <servername> | Format-List *logpath*

PROCESS EXCLUSIONS

Cdb.exe	Cidaemon.exe	Clussvc.exe
Dsamain.exe	EdgeCredentialSvc.exe	EdgeTransport.exe
ExFBA.exe	Inetinfo.exe	MSExchangeSubmission.exe
MSExchangeTransport.exe	MSExchangeTransportLogSearch.exe	MSExchangeThrottling.exe
Msftefd.exe	Msftesql.exe	OleConverter.exe
Powershell.exe	ScanEngineTest.exe	ScanningProcess.exe
TranscodingService.exe	UmService.exe	Microsoft.Exchange.Pop3service.exe
Microsoft.Exchange.ProtectedServiceHost.exe	Microsoft.Exchange.RPCClientAccess.Service.exe	Microsoft.Exchange.Search.Service.exe
Microsoft.Exchange..Servicehost.exe	Microsoft.Exchange.Store.Service.exe	Microsoft.Exchange.Store.Worker.exe
Microsoft.Exchange.TransportSyncManagerSvc.exe	Microsoft.Exchange.AntispamUpdateSvc.exe	Microsoft.Exchange.UM.CallRouter.exe
Microsoft.Exchange.ContentFilter.Wrapper.exe	MSExchangeDelivery.exe	Microsoft.Exchange.Diagnostics.Service.exe
MSExchangeFrontendTransport.exe	Microsoft.Exchange.Directory.TopologyService.exe	MSExchangeHMHost.exe
Microsoft.Exchange.EdgeSyncSvc.exe	MSExchangeHMWorker.exe	Microsoft.Exchange.Imap4.exe
Microsoft.Exchange.Imap4service.exe	Microsoft.Exchange.Monitoring.exe	Microsoft.Exchange.Pop3.exe
MSExchangeLESearchWorker.exe	MSExchangeMailboxAssistants.exe	MSExchangeMailboxReplication.exe
MSExchangeRepl.exe	UmWorkerProcess.exe	UpdateService.exe
W3wp.exe		

FILE NAME EXTENSION EXCLUSIONS

- Application-related extensions:
  - *.config
  - *.dia
  - *.wsb
- Database-related extensions:
  - *.chk
  - *.edb
  - *.jrs
  - *.jsl
  - *.log
  - *.que
- Offline address book-related extensions:
  - *.lzx
- Content Index-related extensions:
  - *.ci
  - *.dir
  - *.wid
  - *.000
  - *.001
  - *.002
- Unified Messaging-related extensions:
  - *.cfg
  - *.grxml
- Group Metrics-related extensions:
  - *.dsc
  - *.txt

EXCHANGE SERVER 2016

You must exclude specific directories for each Exchange server on which you run an antivirus scanner. This section describes the directories that you should exclude from file-level scanning as well as memory-resident scanning.

FOLDER EXCLUSIONS

Folder	Category	Description	Servers
%SystemRoot%\Cluster	DAGs	The cluster quorum database and other files for database availability groups (DAGs).	Mailbox Servers
%SystemDrive%\DAGFileShareWitnesses\<DAGFQDN>	DAGs	The witness directory on the witness server that's configured for the DAG. The witness server can be virtually any Microsoft Windows server in the local Active Directory forest that isn't already a member of the DAG. To see the actual location, run the following command: Get-DatabaseAvailabilityGroup *<DAGName>*| Format-List *Witness*	Any
%ExchangeInstallPath%ClientAccess\OAB	Offline Address Books	Offline Address Book files.	Mailbox Servers
%ExchangeInstallPath%FIP-FS	Antimalware and DLP	Content scanning that's used by the Malware agent and data loss prevention (DLP).	Mailbox Servers

%ExchangeInstallPath%GroupMetrics	MailTips	Group Metrics files that are used to calculate values for the Large Audience and External Recipients MailTips.	Mailbox Servers
%ExchangeInstallPath%Logging	Exchange process logs	This folder contains many different types of Exchange logs in subfolders. For example: • Calendar Repair Assistant logs • Managed Folder Assistant logs • IMAP4 protocol logs • POP3 protocol logs To see the actual locations, run the following commands: • Get-MailboxServer -Server <*ServerName*> | Format-List *LogPath* • Get-PopSettings <*ServerName*> | Format-List LogFileLocation Get-ImapSettings <*ServerName*> | Format-List LogFileLocation	
%ExchangeInstallPath%Mailbox	Mailbox databases	Exchange databases, checkpoint files, and log files. By default, these files are located in subfolders based on the name of the database. To see the actual locations, run the following command: Get-MailboxDatabase -Server <*ServerName*> | Format-List EdbFilePath,LogFolderPath By default, database context index files are located in the same folder as the database files in a subfolder that's named after the GUID of the database.	Mailbox Servers
%ExchangeInstallPath%TransportRoles\Data\Adam	EdgeSync	Active Directory Lightweight Directory Services (AD LDS) and log files.	Edge Transport Servers
%ExchangeInstallPath%TransportRoles\Data\IpFilter	Connection filtering	IP filter database, checkpoint, and log files.	Edge Transport Servers
%ExchangeInstallPath%TransportRoles\Data\Queue	Queues	Queue database, checkpoint, and log files.	Mailbox Servers, Edge Transport Servers
%ExchangeInstallPath%TransportRoles\Data\SenderReputation	Sender reputation	Sender Reputation database, checkpoint, and log files.	Mailbox Servers, Edge Transport Servers
%ExchangeInstallPath%TransportRoles\Data\Temp	Content conversion	Content conversion that's done in the transport pipeline.	Mailbox Servers, Edge Transport Servers
%ExchangeInstallPath%TransportRoles\Logs	Transport logs	Mail flow and transport pipeline logs are located in subfolders, for example: • Agent logging • Connectivity logging • Message tracking • Pipeline tracing	Mailbox Servers, Edge Transport Servers (Transport service only)

		• Send and Receive connector protocol logging To see the actual locations, run the following commands: • Get-TransportService *<ServerName>* | Format-List *LogPath,*TracingPath • Get-FrontEndTransportService *<ServerName>* | Format-List *LogPath Get-MailboxTransportService *<ServerName>* | Format-List *LogPath,*TracingPath	
%ExchangeInstallPath%TransportRoles\Pickup	Pickup directory	The Pickup directory is used by administrators for mail flow testing or by applications that need to create and submit their own message files. To see the actual location, run the following command: Get-TransportService *<ServerName>*| Format-List PickupDirectoryPath	Mailbox Servers, Edge Transport Servers
%ExchangeInstallPath%TransportRoles\Replay	Replay directory	The Replay directory receives messages from foreign gateway servers and can also be used to resubmit messages that administrators export from the queues of Exchange servers. To see the actual location, run the following command: Get-TransportService *<ServerName>*| Format-List ReplayDirectoryPath	Mailbox Servers, Edge Transport Servers
%ExchangeInstallPath%UnifiedMessaging\Grammars	Unified Messaging	Grammar files for different locales, for example en-EN or es-ES.	Mailbox servers
%ExchangeInstallPath%UnifiedMessaging\Prompts	Unified Messaging	Voice prompts, greetings, and informational message files.	Mailbox servers
%ExchangeInstallPath%UnifiedMessaging\Temp	Unified Messaging	Temporary files generated by Unified Messaging.	Mailbox servers
%ExchangeInstallPath%UnifiedMessaging\Voicemail	Unified Messaging	Voice mail files that are temporarily stored.	Mailbox servers
%ExchangeInstallPath%Working\OleConverter	Content conversion	Transport Neutral Encoding Format (TNEF), also known as Rich Text Format (RTF), to MIME/HTML conversions.	Mailbox Servers, Edge Transport Servers
%SystemDrive%\inetpub\temp\IIS Temporary Compressed Files	Web components	Internet Information Services (IIS) compression folder that's used with Outlook on the web.	Mailbox servers
%SystemRoot%\Microsoft.NET\Framework64\v4.0.30319\Temporary ASP.NET Files	Web components	Temporary files that are used with Exchange services. These files are located in the following subfolders: • autodiscover • ecp • ews • mapi • mapi_emsmdb • microsoft-server-activesync • oab • owa • owa_calendar • powershell • root rpc	Mailbox servers

%SystemRoot%\System32\Inetsrv	Web components	IIS system files.	Mailbox servers
%SystemRoot%\Temp\OICE_*<GUID>*\	Exchange Search	Temporary files used by the Exchange Search service and Microsoft Filter Pack to perform file conversion in a sandboxed environment.	Mailbox servers

PROCESS EXCLUSIONS

Process	Path	Description	Server
ComplianceAuditService.exe	%ExchangeInstallPath%Bin	Microsoft Exchange Compliance Audit service (MSComplianceAudit)	Mailbox servers
Dsamain.exe	%SystemRoot%\System32	Microsoft Exchange ADAM service (ADAM_MSExchange) (Active Directory Lightweight Directory Services (AD LDS) on subscribed Edge Transport servers)	Edge Transport servers
EdgeTransport.exe	%ExchangeInstallPath%Bin	Microsoft Exchange Transport service worker process	Mailbox servers Edge Transport servers
fms.exe	%ExchangeInstallPath%FIP-FS\Bin	Content scanning component that's used by the Malware agent and DLP.	Mailbox servers
hostcontrollerservice.exe	%ExchangeInstallPath%Bin\Search\Ceres\Host Controller	Microsoft Exchange Search Host Controller service (HostControllerService)	Mailbox servers
inetinfo.exe	%SystemRoot%\System32\inetsrv	Internet Information Services (IIS)	Mailbox servers
Microsoft.Exchange.AntispamUpdateSvc.exe	%ExchangeInstallPath%Bin	Microsoft Exchange Antispam Update service (MSExchangeAntispamUpdate)	Mailbox servers Edge Transport servers
Microsoft.Exchange.ContentFilter.Wrapper.exe	%ExchangeInstallPath%TransportRoles\agents\Hygiene	Content Filter agent	Mailbox servers Edge Transport servers
Microsoft.Exchange.Diagnostics.Service.exe	%ExchangeInstallPath%Bin	Microsoft Exchange Diagnostics service (MSExchangeDiagnostics)	Mailbox servers Edge Transport servers
Microsoft.Exchange.Directory.TopologyService.exe	%ExchangeInstallPath%Bin	Microsoft Exchange Active Directory Topology service (MSExchangeADTopology)	Mailbox servers
Microsoft.Exchange.EdgeCredentialSvc.exe	%ExchangeInstallPath%Bin	Microsoft Exchange Credential service (MSExchangeEdgeCredential)	Edge Transport servers
Microsoft.Exchange.EdgeSyncSvc.exe	%ExchangeInstallPath%Bin	Microsoft Exchange EdgeSync service (MSExchangeEdgeSync)	Mailbox servers
Microsoft.Exchange.Imap4.exe	ExchangeInstallPath%FrontEnd\PopImap	Microsoft Exchange IMAP4 service (MSExchangeImap4)	Mailbox servers

Microsoft.Exchange.Imap4service.exe	%ExchangeInstallPath%ClientAccess\PopImap	Microsoft Exchange IMAP4 Backend service (MSExchangeIMAP4BE)	Mailbox servers
Microsoft.Exchange.Notifications.Broker.exe	%ExchangeInstallPath%Bin	Microsoft Exchange Notifications Broker service (MSExchangeNotificationsBroker)	Mailbox servers
Microsoft.Exchange.Pop3.exe	%ExchangeInstallPath%FrontEnd\PopImap	Microsoft Exchange POP3 service (MSExchangePop3)	Mailbox servers
Microsoft.Exchange.Pop3service.exe	%ExchangeInstallPath%ClientAccess\PopImap	Microsoft Exchange POP3 Backend service (MSExchangePOP3BE)	Mailbox servers
Microsoft.Exchange.ProtectedServiceHost.exe	%ExchangeInstallPath%Bin	Microsoft Exchange Service Host service (MSExchangeServiceHost)	Mailbox servers Edge Transport servers
Microsoft.Exchange.RPCClientAccess.Service.exe	%ExchangeInstallPath%Bin	Microsoft Exchange RPC Client Access service (MSExchangeRPC)	Mailbox servers
Microsoft.Exchange.Search.Service.exe	%ExchangeInstallPath%Bin	Microsoft Exchange Search service (MSExchangeFastSearch)	Mailbox servers
Microsoft.Exchange.Servicehost.exe	%ExchangeInstallPath%Bin	Microsoft Exchange Service Host service (MSExchangeServiceHost)	Mailbox servers Edge Transport servers
Microsoft.Exchange.Store.Service.exe	%ExchangeInstallPath%Bin	Microsoft Exchange Information Store service (MSExchangeIS)	Mailbox servers
Microsoft.Exchange.Store.Worker.exe	%ExchangeInstallPath%Bin	Microsoft Exchange Information Store service worker process	Mailbox servers
Microsoft.Exchange.UM.CallRouter.exe	%ExchangeInstallPath%FrontEnd\CallRouter	Microsoft Exchange Unified Messaging Call Router service (MSExchangeUMCR)	Mailbox servers
MSExchangeCompliance.exe	%ExchangeInstallPath%Bin	Microsoft Exchange Compliance Service (MSExchangeCompliance)	Mailbox servers
MSExchangeDagMgmt.exe	%ExchangeInstallPath%Bin	Microsoft Exchange DAG Management service (MSExchangeDagMgmt)	Mailbox servers
MSExchangeDelivery.exe	%ExchangeInstallPath%Bin	Microsoft Exchange Mailbox Transport Delivery service (MSExchangeDelivery)	Mailbox servers
MSExchangeFrontendTransport.exe	%ExchangeInstallPath%Bin	Microsoft Exchange Frontend Transport service (MSExchangeFrontEndTransport)	Mailbox servers
MSExchangeHMHost.exe	%ExchangeInstallPath%Bin	Microsoft Exchange Health Manager service (MSExchangeHM)	Mailbox servers Mailbox servers Edge Transport servers
MSExchangeHMWorker.exe	%ExchangeInstallPath%Bin	Microsoft Exchange Health Manager service worker process	Mailbox servers

			Mailbox servers Edge Transport servers
MSExchangeMailboxAssistants.exe	%ExchangeInstallPath%Bin	Microsoft Exchange Mailbox Assistants service (MSExchangeMailboxAssistants)	Mailbox servers
MSExchangeMailboxReplication.exe	%ExchangeInstallPath%Bin	Microsoft Exchange Mailbox Replication service (MSExchangeMailboxReplication)	Mailbox servers
MSExchangeRepl.exe	%ExchangeInstallPath%Bin	Microsoft Exchange Replication service (MSExchangeRepl)	Mailbox servers
MSExchangeSubmission.exe	%ExchangeInstallPath%Bin	Microsoft Exchange Mailbox Transport Submission service (MSExchangeSubmission)	Mailbox servers
MSExchangeTransport.exe	%ExchangeInstallPath%Bin	Microsoft Exchange Transport service (MSExchangeTransport)	Mailbox servers Edge Transport servers
MSExchangeTransportLogSearch.exe	%ExchangeInstallPath%Bin	Microsoft Exchange Transport Log Search service (MSExchangeTransportLogSearch)	Mailbox servers Edge Transport servers
MSExchangeThrottling.exe	%ExchangeInstallPath%Bin	Microsoft Exchange Throttling service (MSExchangeThrottling)	Mailbox servers
Noderunner.exe	%ExchangeInstallPath%Bin\Search\Ceres\Runtime\1.0	Microsoft Exchange Search service (MSExchangeFastSearch)	Mailbox servers
OleConverter.exe	%ExchangeInstallPath%Bin	Converts rich text format (RTF) messages to MIME/HTML for external recipients.	Mailbox servers
ParserServer.exe	%ExchangeInstallPath%Bin\Search\Ceres\ParserServer	Microsoft Exchange Search service (MSExchangeFastSearch)	Mailbox servers
Powershell.exe	C:\Windows\System32\WindowsPowerShell\v1.0	Exchange Management Shell	Mailbox servers Edge Transport servers
ScanEngineTest.exe	%ExchangeInstallPath%FIP-FS\Bin	Content scanning component that's used by the Malware agent and DLP	Mailbox servers
ScanningProcess.exe	%ExchangeInstallPath%FIP-FS\Bin	Content scanning component that's used by the Malware agent and DLP	Mailbox servers
UmService.exe	%ExchangeInstallPath%Bin	Microsoft Exchange Unified Messaging service (MSExchangeUM)	Mailbox servers
UmWorkerProcess.exe	%ExchangeInstallPath%Bin	Microsoft Exchange Unified Messaging service worker process	Mailbox servers

UpdateService.exe	%ExchangeInstallPath%FIP-FS\Bin	Content scanning component that's used by the Malware agent and DLP	Mailbox servers
W3wp.exe	%SystemRoot%\System32\inetsrv	Internet Information Services (IIS)	Mailbox servers
wsbexchange.exe	%ExchangeInstallPath%Bin	Microsoft Exchange Server Extension for Windows Server Backup (wsbexchange	Mailbox servers

FILE NAME EXTENSION EXCLUSIONS

Extensions	Description	Servers
• .config	Application-related extensions	Mailbox servers Edge Transport servers
• .chk • .edb • .jfm • .jrs • .log • .que	Database-related extensions	Mailbox servers Edge Transport servers
• .dsc • .txt	Group Metrics-related extensions	Mailbox servers
• .cfg • .grxml	Unified Messaging-related extensions	Mailbox servers
• .lzx	Offline address book-related extensions	Mailbox servers

LYNC 2013

FILE AND DIRECTORY EXCLUSIONS

Folder and file locations listed below are the default locations for Lync Server 2013. For any locations for which you did not use the default, exclude the locations you specified for your organization instead of the default locations specified in this topic.

- %systemroot%\System32\LogFiles
- %systemroot%\SysWow64\LogFiles
- %systemroot%\Windows\Assembly\GAC_MSIL
- %programfiles%\Microsoft Lync Server 2013
- %programfiles%\commonfiles\Microsoft Lync Server 2013
- %SystemDrive%\RtcReplicaRoot
- File share store (specified in Topology Builder). File stores are specified in Topology Builder.
- SQL Server data and log files, including those for the back-end database, user store, archiving store, monitoring store, and application store. Database and log files can be specified in Topology Builder.
- SQL Server data and log files, including those for the Front-end database, Lync store, and RtcDatabase store. They are normally under %localdrive%\CSData.

PROCESS EXCLUSIONS

ABServer.exe	ComplianceService.exe	MasterReplicatorAgent.exe	ReplicationApp.exe	**Fabric Host Svc Processes**

AcpMcuSvc.exe	DataMCUSvc.exe	MediaRelaySvc.exe	RtcHost.exe	Fabric.exe
ASMCUSvc.exe	DataProxy.exe	MediationServerSvc.exe	RTCSrv.exe	FabricDCA.exe
AVMCUSvc.exe	FileTransferAgent.exe	MRASSvc.exe	XmppProxy.exe	FabricHost.exe
ChannelService.exe	IMMCUSvc.exe	OcsAppServerHost.exe	XmppTGW.exe	
ClsAgent.exe	LysSvc.exe	ReplicaReplicatorAgent.exe		

LYNC 2010

FILE AND DIRECTORY EXCLUSIONS

Folder and file locations listed below are the default locations for Lync Server 2010. For any locations for which you did not use the default, exclude the locations you specified for your organization instead of the default locations specified in this topic.

- %systemroot%\System32\LogFiles
- %systemroot%\SysWow64\LogFiles
- %systemroot%\Windows\Assembly\GAC_MSIL
- %programfiles%\Microsoft Lync Server 2010
- %programfiles%\commonfiles\Microsoft Lync Server 2010
- %SystemDrive%\RtcReplicaRoot
- File share store (specified in Topology Builder). File stores are specified in Topology Builder.
- SQL Server data and log files, including those for the back-end database, user store, archiving store, monitoring store, and application store. Database and log files can be specified in Topology Builder.

PROCESS EXCLUSIONS

ASMCUSvc.exe	DataProxy.exe	MasterReplicatorAgent.exe	MeetingMCUSvc.exe	QmsSvc.exe
AVMCUSvc.exe	FileTransferAgent.exe	MediaRelaySvc.exe	MRASSvc.exe	ReplicaReplicatorAgent.exe
DataMCUSvc.exe	IMMCUSvc.exe	MediationServerSvc.exe	OcsAppServerHost.exe	RTCArch.exe
RtcCdr.exe	RTCSrv.exe			

MICROSOFT CLUSTER SERVERS

FILE AND DIRECTORY EXCLUSIONS

- Quorum Drive (for instance Q:)
- C:\Windows\Cluster
- The path of the \mscs folder on the quorum hard disk. For example, exclude the Q:\mscs folder from virus scanning.
- The temp folder for the Cluster Service account. For example, exclude the \clusterserviceaccount\Local Settings\Temp folder from virus scanning.

Note: The temp folder exclusion does not apply to clusters on Server 2008 or above as a specific service account is no longer used.

MICROSOFT HYPER-V SERVERS, SYSTEM CENTER VIRTUAL MACHINE MANAGER

FILE AND DIRECTORY EXCLUSIONS

- Default virtual machine configuration directory

    - C:\ProgramData\Microsoft\Windows\Hyper-V
- Custom virtual machine configuration directories
- Default virtual hard disk drive directory
    - C:\Users\Public\Documents\Hyper-V\Virtual Hard Disks
- Custom virtual hard disk drive directories
- Custom replication data directories, if you are using Hyper-V Replica
- Snapshot directories
- C:\Clusterstorage and all subdirectories (if using Live Migration together with Cluster Shared Volumes)
- All VHD, VHDX, AVHD, VSV and ISO files
    - *.vhd
    - *.vhdx
    - *.avhd
    - *.vsv
    - *.iso

PROCESS EXCLUSIONS

- Vmms.exe
- Vmwp.exe

SKYPE FOR BUSINESS 2015

FILES AND DIRECTORY EXCLUSIONS

- %systemroot%\System32\LogFiles
- %systemroot%\SysWow64\LogFiles
- %systemroot%\Microsoft.NET\assembly\GAC_MSIL
- %programfiles%\Skype for Business Server 2015
- %programfiles%\Common Files\Skype for Business Server 2015\Watcher Node
- %programfiles%\Common Files\Skype for Business Server 2015
- %programfiles%\Common Files\Skype for Business Online
- %SystemDrive%\RtcReplicaRoot
- File share store (specified in Topology Builder). File stores are specified in Topology Builder.

PROCESS EXCLUSIONS

ABServer.exe	DataProxy.exe	MediationServerSvc.exe	XmppProxy.exe	**Fab Host Processes**
ASMCUSvc.exe	FileTransferAgent.exe	MRASSvc.exe	XmppTGW.exe	Fabric.exe
AVMCUSvc.exe	HealthAgent.exe	OcsAppServerHost.exe		FabricDCA.exe
ChannelService.exe	IMMCUSvc.exe	ReplicaReplicatorAgent.exe		FabricHost.exe
ClsAgent.exe	LysSvc.exe	ReplicationApp.exe		
ComplianceService.exe	MasterReplicatorAgent.exe	RtcHost.exe		
DataMCUSvc.exe	MediaRelaySvc.exe	RTCSrv.exe		

SQL SERVER

FILES AND DIRECTORY EXCLUSIONS

- SQL Server data files
    - *.mdf
    - *.ldf
    - *.ndf
- SQL Server backup files
    - *.bak
    - *.trn
- Full-Text catalog files
    - Default instance: Program Files\Microsoft SQL Server\MSSQL\FTDATA
    - Named instance: Program Files\Microsoft SQL Server\MSSQL$instancename\FTDATA
- Trace files
    - *.trc - these files can be generated either when you configure profiler tracing manually or when you enable C2 auditing for the server.
- SQL audit files (for SQL Server 2008 or later versions)
    - *.sqlaudit
- SQL query files
    - *.sql
- The directory that holds Analysis Services data – default is C:\Program Files\Microsoft SQL Server\MSSQL.X\OLAP\Data. You can view and change the data directory by using Analysis Manager. To do this, follow these steps:
    1. In Analysis Manager, right-click the server, and then click Properties.
    2. In the Properties dialog box, click the General tab. The directory appears under Data folder.
- The directory that holds Analysis Services temporary files that are used during Analysis Services processing – default is C:\Program Files\Microsoft SQL Server\MSSQL.X\OLAP\Data. You can view and change the directory that holds temporary files in Analysis Manager. To do this, follow these steps:
    1. In Analysis Manager, right-click the server, and then click Properties.
    2. In the Properties dialog box, click the General tab.
    3. On the General tab, notice the directory under Temporary file folder.

Note : Optionally, you can add a second temporary directory for Analysis Services 2000 by using the TempDirectory2 registry entry. If you use this registry entry, consider excluding from virus scanning the directory to which this registry entry points

- Analysis Services backup files – default is C:\Program Files\Microsoft SQL Server\MSSQL.X\OLAP\Backup
- The directory that holds Analysis Services log files – default is C:\Program Files\Microsoft SQL Server\MSSQL.X\OLAP\Log
- Directories for any Analysis Services 2005 and later-version partitions that are not stored in the default data directory
- Note When you create the partitions, these locations are defined in the Storage location section of the Processing and Storage Locations page of the Partition Wizard.
- Filestream data files (SQL 2008 and later versions)
- Remote Blob Storage files (SQL 2008 and later versions)
- The directory that holds Reporting Services temporary files and Logs (RSTempFiles and LogFiles)

PROCESS EXCLUSIONS

SQL SERVER 2012

- %ProgramFiles%\Microsoft SQL Server\MSSQL11.<Instance Name>\MSSQL\Binn\SQLServr.exe
- %ProgramFiles%\Microsoft SQL Server\MSRS11.<Instance Name>\Reporting Services\ReportServer\Bin\ReportingServicesService.exe
- %ProgramFiles%\Microsoft SQL Server\MSAS11.<Instance Name>\OLAP\Bin\MSMDSrv.exe

SQL SERVER 2008 R2

- %ProgramFiles%\Microsoft SQL Server\MSSQL10_50.<Instance Name>\MSSQL\Binn\SQLServr.exe
- %ProgramFiles%\Microsoft SQL Server\MSSQL10_50.<Instance Name>\Reporting Services\ReportServer\Bin\ReportingServicesService.exe
- %ProgramFiles%\Microsoft SQL Server\MSSQL10_50.<Instance Name>\OLAP\Bin\MSMDSrv.exe
- SQL Server 2008
- %ProgramFiles%\Microsoft SQL Server\MSSQL10.<Instance Name>\MSSQL\Binn\SQLServr.exe
- %ProgramFiles%\Microsoft SQL Server\MSSQL10.<Instance Name>\Reporting Services\ReportServer\Bin\ReportingServicesService.exe
- %ProgramFiles%\Microsoft SQL Server\MSSQL10.<Instance Name>\OLAP\Bin\MSMDSrv.exe

SQL SERVER 2005

- %ProgramFiles%\Microsoft SQL Server\MSSQL.1\MSSQL\Binn\SQLServr.exe
- %ProgramFiles%\Microsoft SQL Server\MSSQL.3\Reporting Services\ReportServer\Bin\ReportingServicesService.exe
- %ProgramFiles%\Microsoft SQL Server\MSSQL.2\OLAP\Bin\MSMDSrv.exe

SYSTEM CENTER CONFIGURATION MANAGER 2007, SYSTEM CENTER 2012 CONFIGURATION MANAGER

FILE AND DIRECTORY EXCLUSIONS – SITE SERVERS

- Drive:\<Config Mgr Install Folder>\Inboxes\
- Drive:\<Config Mgr Install Folder>\Logs
- Drive:\<Config Mgr Install Folder>\EasySetupPayload

Note: If you exclude the <DriveLetter):\<ConfigMgr install folder>\Inboxes directory from virus scanning or remove the antivirus software, you may make the site server and all clients vulnerable to potential virus risks. The client base component files reside in the <DriveLetter):\<ConfigMgr install folder>\Inboxes directory, therefore use these options only as a short-term troubleshooting step.

FILE AND DIRECTORY EXCLUSIONS – SITE SYSTEMS

- Management Points
  - Drive:\Program Files\SMS_CCM\ServiceData or C:\Windows\CCM\ServiceData
- Distribution Points
  - Drive:\Program Files\SMS_CCM\ServiceData or C:\Windows\CCM\ServiceData
  - ContentLib_Drive\SMS_DP$ ($=driveletter)
  - ContentLib_Drive\SMSPKG$ ($=driveletter)
  - ContentLib_Drive\SMSPKG
  - ContentLib_Drive\SMSPKGSIG
  - ContentLib_Drive\SMSSIG$

FILE AND DIRECTORY EXCLUSIONS – CLIENTS

- All SDF files under C:\Windows\CCM
- C:\Windows\CCM\ServiceData
- C:\Windows\CCMCache
- C:\Windows\CCMSetup
- C:\Windows\CCM\Logs

PROCESS EXCLUSIONS

- Smsexec.exe
- Ccmexec.exe

- CmRcService.exe
- Sitecomp.exe
- Smswriter.exe
- Smssqlbbkup.exe
- Cmupdate.exe
- Ccmrepair.exe (client side)
- Ccmsetup.exe (client side)

SYSTEM CENTER OPERATIONS MANAGER 2007, SYSTEM CENTER 2012 OPERATIONS MANAGER

FILE AND DIRECTORY EXCLUSIONS

The following file name extension-specific exclusions for Operations Manager includes real-time scans, scheduled scans, and local scans.

SQL DATABASE SERVERS

These exclusions include the SQL Server database files that are used by Operations Manager components and the system database files for the master database and for the tempdb database.

For example:

- *.mdf
- *.ldf

OPERATIONS MANAGER (MANAGEMENT SERVERS, GATEWAYS AND AGENTS)

These exclusions include the Health Service cache, together with its queue and log files that are used by Operations Manager.

For Operations Manager 2007 or Operations Manager 2007 R2

Example - C:\Program Files\System Center Operations Manager <*version*>\Health Service State*

Note The placeholder <*version*> represents "2007" for Operations Manager 2007 or Operations Manager 2007 R2.

For Operations Manager 2012

Example - C:\Program Files\System Center Operations Manager\<*component*>\Health Service State\Health Service Store*

Note The placeholder <*component*> represents "Agent" or "Server" for Operations Manager 2012.

For Operations Manager 2012 R2
For a management server:
Example - C:\Program Files\Microsoft System Center 2012 R2\Server\Health Service State*

For a gateway server:
Example - C:\Program Files\System Center Operations Manager\Gateway\Health Service State*

For an agent:
Example - C:\Program Files\Microsoft Monitoring Agent\Agent\Health Service State*

These exclusions include the queue and log files that are used by Operations Manager.

For Example:

- *.edb
- *.chk
- *.log

Note: Page files should also be excluded from any real-time scans.

PROCESS EXCLUSIONS

- Monitoringhost.exe
- HealthService.exe
- Microsoft.Mom.ConfigServiceHost.exe

SHAREPOINT

SHAREPOINT FOUNDATION 2013

FILE AND DIRECTORY EXCLUSIONS

- Drive:\Program Files\Common Files\Microsoft Shared\Web Server Extensions

  If you do not want to exclude the whole Web Server Extensions folder from antivirus scanning, you can exclude only the following two folders:

- Drive:\Program Files\Common Files\Microsoft Shared\Web Server Extensions\15\Logs
- Drive:\Program Files\Common Files\Microsoft Shared\Web Server Extensions\15\Data\Applications

Note: The Applications folder must be excluded only if the computer is running the SharePoint Foundation Search service. If the folder that contains the index file is located elsewhere, you must also exclude that folder.

- Drive:\Windows\Microsoft.NET\Framework64\v4.0.30319\Temporary ASP.NET Files
- Drive: \Users\ServiceAccount\AppData\Local\Temp\WebTempDir

Note: The WebTempDir folder is a replacement for the FrontPageTempDir folder.

- Drive:\ProgramData\Microsoft\SharePoint
- Drive:\Users\account that the search service is running as\AppData\Local\Temp

Note: The search account creates a folder in the Gthrsvc_spsearch4 Temp folder to which it periodically has to write.

- Drive:\WINDOWS\System32\LogFiles
- Drive:\Windows\Syswow64\LogFiles

Note: If you use a specific account for SharePoint services or application pools identities, you may also have to exclude the following folders:

- Drive:\Users\ServiceAccount\AppData\Local\Temp
- Drive:\Users\Default\AppData\Local\Temp

SHAREPOINT SERVER 2013

FILE AND DIRECTORY EXCLUSIONS

- Drive:\Program Files\Microsoft Office Servers

Note: If you do not want to exclude the whole Microsoft Office Servers folder from antivirus scanning, you can exclude only the following folders:

- Drive:\Program Files\Microsoft Office Servers\15.0\Data

Note: This folder is used for the indexing process. If the index files are configured to be located in a different folder, you also have to exclude that location.

- Drive:\Program Files\Microsoft Office Servers\15.0\Logs
- Drive:\Program Files\Microsoft Office Servers\15.0\Bin
- Drive:\Program Files\Microsoft Office Servers\15.0\Synchronization Service
- Any location in which you decided to store the disk-based binary large object (BLOB) cache (for example, C:\Blobcache).

Note: If you have SharePoint Server 2013, these folders should be excluded in addition to the folders that are listed in the "SharePoint Foundation 2013" section.

SHAREPOINT FOUNDATION 2010

FILE AND DIRECTORY EXCLUSIONS

- Drive:\Program Files\Common Files\Microsoft Shared\Web Server Extensions

Note: If you do not want to exclude the whole Web Server Extensions folder from antivirus scanning, you can exclude only the following two folders:

- Drive:\Program Files\Common Files\Microsoft Shared\Web Server Extensions\14\Logs
- Drive:\Program Files\Common Files\Microsoft Shared\Web Server Extensions\14\Data\Applications

Note: The Applications folder must be excluded only if the computer is running the SharePoint Foundation Search service. If the folder that contains the index file is located elsewhere, you must also exclude that folder.

- Drive:\Windows\Microsoft.NET\Framework64\v2.0.50727\Temporary ASP.NET Files
- Drive: \Users\ServiceAccount\AppData\Local\Temp\WebTempDir

Note: The WebTempDir folder is a replacement for the FrontPageTempDir folder.

- Drive:\ProgramData\Microsoft\SharePoint
- Drive:\Users\account that the search service is running as\AppData\Local\Temp

Note: The search account creates a folder in the Gthrsvc_spsearch4 Temp folder to which it periodically has to write.

- Drive:\WINDOWS\system32\LogFiles
- Drive:\Windows\Syswow64\LogFiles

Note: If you use a specific account for SharePoint services or application pools identities, you may also have to exclude the following folders:

- Drive:\Users\ServiceAccount\AppData\Local\Temp
- Drive:\Users\Default\AppData\Local\Temp

SHAREPOINT SERVER 2010

FILE AND DIRECTORY EXCLUSIONS

- Drive:\Program Files\Microsoft Office Servers

Note: If you do not want to exclude the whole Microsoft Office Servers folder from antivirus scanning, you can exclude only the following folders:

- Drive:\Program Files\Microsoft Office Servers\14.0\Data

Note: This folder is used for the indexing process. If the Index files are configured to be located in a different folder, you also have to exclude that location.

- Drive:\Program Files\Microsoft Office Servers\14.0\Logs
- Drive:\Program Files\Microsoft Office Servers\14.0\Bin
- Drive:\Program Files\Microsoft Office Servers\14.0\Synchronization Service
- Any location in which you decided to store the disk-based binary large object (BLOB) cache (for example, C:\Blobcache)

Note: If you have SharePoint Server 2010, these folders should be excluded in addition to the folders that are listed in the "SharePoint Foundation 2010" section.

WINDOWS SHAREPOINT SERVICES 3.0

FILE AND DIRECTORY EXCLUSIONS

- Drive:\Program Files\Common Files\Microsoft Shared\Web Server Extensions

Note: If you do not want to exclude the whole Web Server Extensions folder from antivirus scanning, you can exclude only the following two folders:

- Drive:\Program Files\Common Files\Microsoft Shared\Web Server Extensions\12\Logs
- Drive:\Program Files\Common Files\Microsoft Shared\Web Server Extensions\12\Data\Applications

Note: The Applications folder must be excluded only if the computer is running the Windows SharePoint Services Search service. If the folder that contains the index file is located elsewhere, you must also exclude that folder.

- Drive:\Windows\Microsoft.NET\Framework\v2.0.50727\Temporary ASP.NET Files

Note: If you are running a 64-bit version of Windows, you should also include the following directory:

- Drive:\Windows\Microsoft.NET\Framework64\v2.0.50727\Temporary ASP.NET Files
- Drive:\Documents and Settings\All Users\Application Data\Microsoft\SharePoint\Config
- Drive:\Windows\Temp\WebTempDir

Note: The WebTempDir folder is a replacement for the FrontPageTempDir folder.

- Drive:\Documents and Settings\account that the search service is running as\Local Settings\Temp\
- Drive:\Users\the account the search service is running as\Local\Temp\

Note: The search account creates a folder in the "gthrsvc Temp" folder to which it periodically has to write.

- Drive:\WINDOWS\system32\LogFiles
- Drive:\Windows\Syswow64\LogFiles

Note: If you use a specific account for SharePoint services or application pools identities, you may also have to exclude the following folders:

- Drive:\Documents and Settings\ServiceAccount\Local Settings\Application Data
- Drive:\Users\ServiceAccount\Local
- Drive:\Documents and Settings\ServiceAccount\Local Settings\Temp
- Drive:\Users\ServiceAccount\Local\Temp
- Drive:\Documents and Settings\Default User\Local Settings\Temp
- Drive:\Users\Default\AppData\Local\Temp

SHAREPOINT SERVER 2007

FILE AND DIRECTORY EXCLUSIONS

- Drive:\Program Files\Microsoft Office Servers

Note: If you do not want to exclude the whole Microsoft Office Servers folder from antivirus scanning, you can exclude only the following folders:

- Drive:\Program Files\Microsoft Office Servers\12.0\Data.

Note: This folder is used for the indexing process. If the index files are configured to be located in a different folder, you also have to exclude that location.

- Drive:\Program Files\Microsoft Office Servers\12.0\Logs
- Drive:\Program Files\Microsoft Office Servers\12.0\Bin
- Any location in which you decide to store the disk-based binary large object (BLOB) cache (for example, C:\Blobcache)

Note: If you have SharePoint Server 2007, these folders should be excluded in addition to the folders that are listed in the "Windows SharePoint Services 3.0" section.

Note: When you install SharePoint Server 2007 or apply a hotfix to an existing installation of SharePoint Server 2007, you may have to disable the real-time option of the antivirus software. Or, you may have to exclude the Drive:\Windows\Temp folder from antivirus scanning if this is required.

SHAREPOINT PORTAL SERVER 2003

- Drive:\Program Files\SharePoint Portal Server
- Drive:\Program Files\Common Files\Microsoft Shared\Web Storage System

Note: Drive: is the drive letter where you installed SharePoint Portal Server.

- If drive M is mounted, you must exclude this drive from the scan.
- If any data was placed in another location throughout the installation process you must exclude that location also.
- If you are using Microsoft SharePoint Portal Server 2003 and you apply Service Pack 1 (SP1), you must exclude the following folder from Anti Virus scans:
    - Drive:\Windows\Temp\Frontpagetempdir

TEAM FOUNDATION SERVER

FILES AND DIRECTORY EXCLUSIONS

- %ProgramFiles%\Microsoft Team Foundation Server 12.0\Application Tier\Web Services\bin

PROCESS EXCLUSIONS

- w3wp.exe

IIS SERVER

Exclude the IIS compression directory from the antivirus software's scan list.

The default compression directory in IIS 6.0 is %systemroot%\IIS Temporary Compressed Files. This directory may have been changed to another location. In IIS 7.0, the default location of the compressed file cache is %SystemDrive%\inetpub\temp\IIS Temporary Compressed Files.

To verify the compression directory:

1. Click Start, point to Programs, point to Administrative Tools, and then click Internet Information Services (IIS) Manager.
2. In IIS Manager, right-click the Web Sites folder, and then click Properties.
3. Click the Service tab.

Under HTTP Compression, make sure that Compress static files is selected, and then locate the path to the temporary directory.

PROCESS EXCLUSIONS

- %systemroot%\system32\inetsrv\w3wp.exe
- %systemroot%\SysWOW64\inetsrv\w3wp.exe

WINDOWS SERVER UPDATE SERVICES (WSUS)

FILE AND DIRECTORY EXCLUSIONS

- \WSUS\WSUSContent
- \WSUS\UpdateServicesDBFiles
- \SoftwareDistribution\Datastore
- \SoftwareDistribution\Download

CAB FILES - METHOD 1

- Wsusscan.cab file and the Wsusscn2.cab file

Note: Because the Wsusscan.cab file and the Wsusscn2.cab file contain several nested cabinet files, excluding only these files is not typically sufficient to reduce unusually high CPU usage. To significantly reduce CPU usage, also exclude nested cabinet files that are within the Wsusscan.cab file and the Wsusscn2.cab file.

Note: If a virus is present in a .cab file, the virus should be detected when the file is uncompressed. Therefore, there is almost no increased risk in using this method.

CAB FILES - METHOD 2

- Exclude all .cab files from the antivirus scan.

Note: If a virus is present in a .cab file, the virus should be detected when the file is uncompressed. Therefore, there is almost no increased risk in using this method.

ORCHESTRATOR

FILE AND DIRECTORY EXCLUSIONS

For a Management Server:

- C:\Program Files (x86)\Microsoft System Center 2012 R2\Orchestrator\Management Server

For a Runbook Server:

- C:\Program Files (x86)\Microsoft System Center 2012 R2\Orchestrator\Runbook Server

PROCESS EXCLUSIONS

- Management Service - ManagementService.exe
- Remoting Service - OrchestratorRemotingService.exe
- Run Program Service - OrchestratorRunProgramService.exe
- Runbook Server Monitor Service - RunbookServerMonitorService.exe
- Runbook Service - RunbookService.exe

APPLICATION VIRTUALIZATION (APP-V) CLIENTS

FILE AND DIRECTORY EXCLUSIONS

- %USERPROFILE%\AppData\Local\SoftGrid Client
- %USERPROFILE%\AppData\Roaming\SoftGrid Client
- %PROGRAMDATA%\Microsoft\Application Virtualization Client\SoftGrid Client

ENTERPRISE DESKTOP VIRTUALIZATION (MED-V)

FILE AND DIRECTORY EXCLUSIONS

- Virtual Hard Disk Image files
  - *.vhd
- Virtual PC Undo Disk Files
  - *.vud
- Virtual PC saved state files
  - *.vsv
- Packed image format used by MED-V (Kidaro Compressed Machine.) These will be present on MED-V Servers, Image Distribution Servers, locally packed images on MED-V Administration workstations, and as pre-staged images on clients
  - *.ckm
- Base virtual machine settings files
  - *.vmc
- Index files used by TrimTransfer feature
  - *.index
- Encrypted virtual hard disk files
  - *.evhd

SYSTEM CENTER DATA PROTECTION MANAGER (DPM) SERVER

FILE AND DIRECTORY EXCLUSIONS

- Drive:\Program Files\Microsoft DPM\DPM\XSD
- Drive:\Program Files\Microsoft DPM\DPM\Temp\MTA

Note: Delete infected files on protected servers and the DPM server. To prevent data corruption of replicas and recovery points, configure the antivirus software to delete infected files rather than automatically cleaning or quarantining them. Automatic cleaning and quarantining can result in data corruption because these processes cause the antivirus software to modify files, making changes that DPM cannot detect. Whenever DPM attempts to synchronize a replica that has been modified by another program, data corruption of the replica and recovery points can result. Configuring the antivirus software to delete infected files resolves this problem. For information about configuring your antivirus software to delete infected files, see the documentation for your antivirus software.

PROCESS EXCLUSIONS

- Drive:\Program Files\Microsoft Data Protection Manager\DPM\bin
  - dpmra.exe
- C:\Windows\Microsoft.net\Framework\v2.0.50727
  - csc.exe

INTERNET SECURITY AND ACCELERATION (ISA) SERVER 2004, INTERNET SECURITY AND ACCELERATION (ISA) SERVER 2006

FILES AND DIRECTORY EXCLUSIONS

- ISA Server installation folder – default is %ProgramFiles%\Microsoft ISA Server
- SQL MSDE folders - %ProgramFiles%\Microsoft SQL Server
- ISA Server Web cache (ISA Server administrator must define this)

PROCESS EXCLUSIONS

- ISA Server Report Summary Generator - %ProgramFiles%\Microsoft ISA Server\dailysum.exe
- ISA Server Report Generator - %ProgramFiles%\Microsoft ISA Server\isarepgen.exe
- ISA Server Diagnostic Logging Viewer - %ProgramFiles%\Microsoft ISA Server\isadlviewer.exe
- ISA Server Storage Service - %ProgramFiles%\Microsoft ISA Server\isastg.exe
- ISA Server Control Service - %ProgramFiles%\Microsoft ISA Server\mspadmin.exe
- ISA Server Web Content Download Service - %ProgramFiles%\Microsoft ISA Server\w3prefch.exe
- ISA Server Firewall Service - %ProgramFiles%\Microsoft ISA Server\wspsrv.exe
- SQL 2003 MSDE
  - %ProgramFiles%\Microsoft SQL Server\80\Tools\Binn\sqlmangr.exe;
  - %ProgramFiles%\Microsoft SQL Server\MSSQL$MSFW\sqlservr.exe
- Active Directory Lightweight Directory Services (Enterprise Edition only)
  - %WinDir%\System32\dsamain.exe

FOREFRONT THREAT MONITORING GATEWAY (TMG) 2010

FILES AND DIRECTORY EXCLUSIONS

- TMG installation folder (may be changed during installation):
  - %ProgramFiles%\Microsoft Forefront Threat Management Gateway
- TMG SQL Express and SRS installation folders (not changeable)
  - %ProgramFiles%\Microsoft SQL Server\MSSQL10.ISARS%ProgramFiles%\Microsoft SQL Server\MSSQL10.MSFW
- TMG Malware scanning cache (may be changed by TMG administrator)
  - %SystemRoot%\Temp\ScanStorage
- TMG Log Queue (may be changed by the TMG administrator)
  - %ProgramFiles%\Microsoft Forefront Threat Management Gateway\Logs
- Web cache—(TMG administrator must define this)

PROCESS EXCLUSIONS

- TMG Report Summary Generator
  - %ProgramFiles%\Microsoft Forefront Threat Management Gateway\dailysum.exe
- TMG Report Generator
  - %ProgramFiles%\Microsoft Forefront Threat Management Gateway\isarepgen.exe
- TMG Diagnostic Logging Viewer
  - %ProgramFiles%\Microsoft Forefront Threat Management Gateway\isadlviewer.exe
- TMG Managed Control Service
  - %ProgramFiles%\Microsoft Forefront Threat Management Gateway\IsaManagedCtrl.exe
- TMG Storage Service
  - %ProgramFiles%\Microsoft Forefront Threat Management Gateway\isastg.exe
- TMG Administration Component
  - %ProgramFiles%\Microsoft Forefront Threat Management Gateway\mspadmin.exe
- TMG Firewall Service
  - %ProgramFiles%\Microsoft Forefront Threat Management Gateway\wspsrv.exe
- TMG Web Content Download Service
  - %ProgramFiles%\Microsoft Forefront Threat Management Gateway\w3prefch.exe
- SQL 2008 Express and SQL 2008 Reporting Services

    - %ProgramFiles%\Microsoft SQL Server\MSSQL10.ISARS\MSSQL\Binn\sqlservr.exe
    - %ProgramFiles%\Microsoft SQL Server\MSSQL10.ISARS\MSSQL\Binn\ReportingServicesService.exe
    - %ProgramFiles%\Microsoft SQL Server\MSSQL10.MSFW\MSSQL\Binn\sqlservr.exe
- Active Directory Lightweight Directory Services
    - %WinDir%\System32\dsamain.exe

FOREFRONT UNIFIED ACCESS GATEWAY (UAG) 2010

FILES AND DIRECTORY EXCLUSIONS

- UAG installation folder (may be changed during installation):
    - %ProgramFiles%\Microsoft Forefront Unified Access Gateway
- UAG SQL Express and SRS installation folders (not changeable)
    - %ProgramFiles%\Microsoft SQL Server\MSSQL10.ISARS%ProgramFiles%\Microsoft SQL Server\MSSQL10.MSFW
- UAG Malware scanning cache (may be changed by UAG administrator)
    - %SystemRoot%\Temp\ScanStorage
- UAG Log Queue (may be changed by the UAG administrator)
    - %ProgramFiles%\Microsoft Forefront Unified Access Gateway\Logs
- Web cache—(UAG administrator must define this)

PROCESS EXCLUSIONS

- UAG Report Summary Generator
    - %ProgramFiles%\Microsoft Forefront Unified Access Gateway\dailysum.exe
- UAG Report Generator
    - %ProgramFiles%\Microsoft Forefront Unified Access Gateway\isarepgen.exe
- UAG Diagnostic Logging Viewer
    - %ProgramFiles%\Microsoft Forefront Unified Access Gateway\isadlviewer.exe
- UAG Managed Control Service
    - %ProgramFiles%\Microsoft Forefront Unified Access Gateway\IsaManagedCtrl.exe
- UAG Storage Service
    - %ProgramFiles%\Microsoft Forefront Unified Access Gateway\isastg.exe
- UAG Administration Component
    - %ProgramFiles%\Microsoft Forefront Unified Access Gateway\mspadmin.exe
- UAG Firewall Service
    - %ProgramFiles%\Microsoft Forefront Unified Access Gateway\wspsrv.exe
- UAG Web Content Download Service
    - %ProgramFiles%\Microsoft Forefront Unified Access Gateway\w3prefch.exe
- SQL 2008 Express and SQL 2008 Reporting Services
    - %ProgramFiles%\Microsoft SQL Server\MSSQL10.ISARS\MSSQL\Binn\sqlservr.exe
    - %ProgramFiles%\Microsoft SQL Server\MSSQL10.ISARS\MSSQL\Binn\ReportingServicesService.exe
    - %ProgramFiles%\Microsoft SQL Server\MSSQL10.MSFW\MSSQL\Binn\sqlservr.exe
- Active Directory Lightweight Directory Services
    - %WinDir%\System32\dsamain.exe
- Forefront UAG DNS-ALG Service
    - %ProgramFiles%\Microsoft Forefront Unified Access Gateway\DnsAlgSrv.exe
- Forefront UAG Monitoring Manager
    - %ProgramFiles%\Microsoft Forefront Unified Access Gateway\MonitorMgrCom.exe
- Forefront UAG Session Manager
    - %ProgramFiles%\Microsoft Forefront Unified Access Gateway\SessionMgrCom.exe
- Forefront UAG File Sharing

    - %ProgramFiles%\Microsoft Forefront Unified Access Gateway\ShareAccess.exe
- Forefront UAG Quarantine Enforcement Server
    - %ProgramFiles%\Microsoft Forefront Unified Access Gateway\uagqessvc.exe
- Forefront UAG Terminal Services RDP Data
    - %ProgramFiles%\Microsoft Forefront Unified Access Gateway\uagrdpsvc.exe
- Forefront UAG User Manager
    - %ProgramFiles%\Microsoft Forefront Unified Access Gateway\UserMgrCom.exe
- Forefront UAG Watch Dog Service
    - %ProgramFiles%\Microsoft Forefront Unified Access Gateway\WatchDogSrv.exe
- Forefront UAG Log Server
    - %ProgramFiles%\Microsoft Forefront Unified Access Gateway\whlerrsrv.exe
- Forefront UAG SSL Network Tunneling Server
    - %ProgramFiles%\Microsoft Forefront Unified Access Gateway\whlios.exe

APPENDIX A – SOURCES

PRIOR ANTIVIRUS EXCLUSION COMPILATIONS

http://social.technet.microsoft.com/wiki/contents/articles/953.microsoft-anti-virus-exclusion-list.aspx
http://blogs.technet.com/b/jeff_stokes/archive/2010/05/19/anti-virus-exclusions-and-you.aspx

GENERAL EXCLUSIONS

http://support.microsoft.com/kb/822158

DOMAIN CONTROLLERS

http://support.microsoft.com/kb/822158

EXCHANGE SERVER

http://technet.microsoft.com/en-us/library/bb332342.aspx

http://technet.microsoft.com/en-us/library/bb332342%28EXCHG.80%29.aspx

http://support.microsoft.com/kb/328841

https://technet.microsoft.com/EN-US/library/bb332342(v=exchg.160).aspx

LYNC

http://technet.microsoft.com/en-us/library/gg195736(v=ocs.14).aspx

CLUSTER SERVERS

http://support.microsoft.com/kb/250355

HYPER-V AND SYSTEM CENTER VIRTUAL MACHINE MANAGER (SCVMM)

http://support.microsoft.com/kb/961804/en-us

http://support.microsoft.com/kb/2628135

SKYPE FOR BUSINESS 2015

https://technet.microsoft.com/EN-US/library/mt629173.aspx

SQL SERVER

http://support.microsoft.com/kb/309422

CONFIGURATION MANAGER

http://blogs.technet.com/b/configurationmgr/archive/2010/11/30/configmgr-2007-antivirus-scan-and-exclusion-recommendations.aspx

http://blogs.technet.com/b/systemcenterpfe/archive/2013/01/11/updated-system-center-2012-configuration-manager-antivirus-exclusions-with-more-details.aspx

http://www.systemcenterblog.nl/2012/05/09/anti-virus-scan-exclusions-for-configuration-manager-2012/

https://support.microsoft.com/en-us/help/327453/recommended-antivirus-exclusions-for-configuration-manager-2012-and-cu

SYSTEM CENTER OPERATIONS MANAGER (SCOM)

http://support.microsoft.com/kb/975931

http://social.technet.microsoft.com/wiki/contents/articles/637.recommendations-for-antivirus-exclusions-in-mom-2005-and-operations-manager-2007.aspx

SHAREPOINT

http://support.microsoft.com/kb/952167

TEAM FOUNDATION SERVER

https://support.microsoft.com/en-us/help/2636507/antivirus-exclusions-for-microsoft-team-foundation-server

INTERNET INFORMATION SERVICES (IIS) SERVER

http://support.microsoft.com/kb/817442

WINDOWS SERVER UPDATE SERVICES (WSUS)

http://technet.microsoft.com/en-us/library/dd939908(WS.10).aspx#av

ORCHESTRATOR

https://social.technet.microsoft.com/wiki/contents/articles/26665.system-center-orchestrator-antivirus-exclusions.aspx

MICROSOFT APPLICATION VIRTUALIZATION (APP-V) CLIENTS

http://support.microsoft.com/kb/2576031

MICROSOFT ENTERPRISE DESKTOP VIRTUALIZATION (MED-V)

http://social.technet.microsoft.com/wiki/contents/articles/566.aspx

SYSTEM CENTER DATA PROTECTOIN MANAGER (DPM) SERVER

http://technet.microsoft.com/en-us/library/ff399439.aspx

INTERNET SECURITY AND ACCELERATION (ISA) SERVER

http://technet.microsoft.com/en-us/library/cc707727.aspx

FOREFRONT THREAT MANAGEMENT GATEWAY (TMG)

http://technet.microsoft.com/en-us/library/cc707727.aspx

FOREFRONT UNIFIED ACCESS GATEWAY (UAG)

http://technet.microsoft.com/en-us/library/cc707727.aspx