BitDefender Security for File Servers

RECOMMENDED CONFIGURATION

bitdefender
secure your every bit

Summary

Computers running Windows Server 2003, Windows 2000 or Windows XP

The following files and folders must be excluded from both **real time** and **on-demand** scanning!

> ***Note:*** *%SystemRoot%, %SystemDrive%, %ProgramFiles% are system variables dependent on the operation system and computer configuration. They can be determined using the command SET.*

1. Exclude Microsoft Windows Update or Automatic Update related files:

1.1. The Windows Update or Automatic Update database file:

%SystemRoot%\ SoftwareDistribution\Datastore\Datastore.edb

1.2. The transaction log files, located in the following folder:

%SystemRoot%\ SoftwareDistribution\Datastore\Logs

Edb*.log (wildcard character indicated that there may be several files)

Res1.log

Res2.log

Edb.chk

Tmp.edb

Computers Running Windows Server 2003 and Windows 2000 Domain Controllers

The following files and folders must be excluded from both **real time** and **on-demand** scanning!

> ***Note:*** *%SystemRoot%, %SystemDrive%, %ProgramFiles% are system variables dependent on the operation system and computer configuration. They can be determined using the command SET.*

> ***Warning:*** *Serious problems might occur if you modify registers incorrectly by using Registry Editor or another method! These problems might require reinstallation of the operating system! Registry keys are given here for the sole purpose of informing you about the location of some files and not to modify them.*

2. Exclude Active Directory and Active Directory-related files:

1.3. Main 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:

  %SystemRoot%\ntds

- Exclude the following files:

  Ntds.dit

  Ntds.pat

1.4. 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:

%SystemRoot%\ntds

- Exclude the following files:

  EDB*.log (the wildcard character indicates that there may be several files)
  Res1.log
  Res2.log
  Ntds.pat (Microsoft Windows Server 2003 no longer uses the Ntds.pat file)

1.5. The 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

- Exclude the following files:

  Temp.edb

  Edb.chk

3. SYSVOL files:

3.1. The File Replication Service (FRS) Working folder

- The location of this folder is specified in the following registry key:

  HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\NtFrs\Parameters\Working Directory

- Exclude the following files:

  FRS Working Dir\jet\sys\edb.chk

  FRS Working Dir\jet\ntfrs.jdb

  FRS Working Dir\jet\log*.log

3.2. The FRS Database Log files

- The location of those files is specified in the following registry key:

  HKEY_LOCAL_MACHINE\system\currentcontrolset\services\NtFrs\Parameters\DB Log File Directory

- The default location is:

  %SystemRoot%\ntfrs

- Exclude the following files:

  FRS Working Dir\jet\log*.log (if registry key is not set)

DB Log File Directory\log*.log (if registry key is set)

3.3. The Staging folder

- 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

- The current location of the Staging folder and all of its sub-folders is the file system reparse target of the replica set staging folders. Staging defaults to the following location:

  %SystemRoot%\sysvol\staging areas

- The current location of the SYSVOL\SYSVOL folder and all of its sub-folders is the file system reparse target of the replica set root. The SYSVOL\SYSVOL folder defaults to the following location:

  %SystemRoot%\sysvol\sysvol

3.4. The FRS Preinstall folder

- The location of this folder is specified in the following registry key:

  Replica_root\DO_NOT_REMOVE_NtFrs_PreInstall_Directory

- The Preinstall folder is always open when FRS is running.

***In summary**, the targeted and excluded list of folders for a SYSVOL tree that is placed in its default location would look similar to the following:*

1.	*%systemroot%\sysvol*	*Exclude*
2.	*%systemroot%\sysvol\domain*	*Scan*
3.	*%systemroot%\sysvol\domain\DO_NOT_REMOVE_NtFrs_PreInstall_Directory*	*Exclude*
4.	*%systemroot%\sysvol\domain\Policies*	*Scan*
5.	*%systemroot%\sysvol\domain\Scripts*	*Scan*
6.	*%systemroot%\sysvol\staging*	*Exclude*
7.	*%systemroot%\sysvol\staging areas*	*Exclude*
8.	*%systemroot%\sysvol\sysvol*	*Exclude*

If any one of these folder or files have been moved or placed in a different location, scan or exclude the equivalent element.

4. DFS

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

For more information, see Microsoft KB article: http://support.microsoft.com/kb/822158/.

Mail Servers Running BitDefender Security for File Servers or/and BitDefender Security for Mail Servers

The following files and folders must be excluded from both **real time** and **on-demand** scanning!

> ***Note:*** *%SystemRoot%, %SystemDrive%, %ProgramFiles% are system variables dependent on the operation system and computer configuration. They can be determined using the command SET.*

1. If BitDefender for File Servers is installed on a mail server

- Exclude the following folders:

  the folder where the mail server is installed

  the folder where the mailboxes and mail queues are stored

2. If BitDefender Security for File Servers is installed on the same machine as BitDefender Security for Mail Servers

- Exclude the folder where BitDefender creates its temporary files:

  %SystemRoot%\Temp\BDNP

Computers Running Microsoft Exchange Server and BitDefender Security for File Servers

The following files and folders must be excluded from both **real time** and **on-demand** scanning!

> ***Note:*** *%SystemRoot%, %SystemDrive%, %ProgramFiles% are system variables dependent on the operation system and computer configuration. They can be determined using the command SET.*

1. If BitDefender Security for File Servers is installed on the same machine as BitDefender Security for Exchange
   - Exclude the folder where BitDefender creates its temporary files:

     %ProgramFiles%\Softwin\Temp

     %SystemRoot%\Temp\BDNP\ (BitDefender for MS Exchange 2003 and 2000 only)
2. Exclude Exchange databases and log files across all storage groups.
   - The default location is:

     \Exchsrvr\Mdbdata
3. Exclude Exchange .mta files.
   - The default location is:

     \Exchsrvr\Mtadata
4. Exclude the additional log files such as the

   \Exchsrvr\Server_name.log
5. Exclude virtual server folder.
   - The default location is:

     \Exchsrvr\Mailroot
6. Exclude the working folder that is used to store streaming .tmp files that are used for message conversion.
   - The location is configurable. The default location is:

     \Exchsrvr\Mdbdata

7. Exclude the temporary folder that is used in conjunction with offline maintenance utilities 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 when you run the utility.

8. Exclude Site Replication Service (SRS) files in the folder:

   \Exchsrvr\Srsdata

9. Exclude Internet Mail Connector files.
   - The default location is:

   \Exchsrvr\IMCData

10. Exclude Microsoft Internet Information Service (IIS) system files. The default location is:

    %SystemRoot%\System32\Inetsrv

11. Exclude the folder that contains the Checkpoint (.chk) files.

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

12. For Exchange 5.5 only:

    12.1. Exclude the following file types:

    .edb

    .log

13. For Exchange 2000 only:

    13.1. Exclude drive M:

    13.2. Exclude the following file types:

    .edb

    .stm

    .log

    13.3. If you use Microsoft BackOffice POP3 Connector to pull emails from and external POP3 account, exclude the incoming folder.
    - The default location is:

    %ProgramFiles%\Microsoft BackOffice\Connectiviry\POP3 Connector\Incoming

14. For Exchange 2003 only:

14.1. If you use Microsoft BackOffice POP3 Connector to pull emails from an external POP3 account, exclude the **incoming folder**.

- The default location is:

  %ProgramFiles%\Microsoft Windows Small Business Server\Networking\POP3\Incoming Mail

14.2. The Internet Information Services (IIS) 6.0 compression folder that is used with Outlook Web Access 2003.

- The default location is the following folder:

  %SystemRoot%\IIS Temporary Compressed Files

14.3. For clusters

- Exclude

  Quorum disk

  %Winnt%\Cluster folder

  \Exchsrvr\Conndata folder

14.4. If the antivirus supports scanning processes feature, exclude the following processes from scanning:

Cdb.exe

Cidaemon.exe

Store.exe

Emsmta.exe

Mad.exe

Mssearch.exe

Inetinfo.exe

W3wp.exe

Note: *You may want to exclude the whole Exchsrvr folder from scanning.*

Note: *Microsoft strongly recommends that you* ***temporarily disable*** *file-based scanning software* ***during operating system and Exchange upgrades****; this includes upgrading to new versions of Exchange and the operating system, and applying any Exchange or operating system fixes or service packs.*

For more information see the following Microsoft KB articles:

http://support.microsoft.com/kb/823166

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

http://support.microsoft.com/kb/245822/

Computers Running Microsoft ISA Servers and BitDefender Security for File Servers

The following files and folders must be excluded from both **real time** and **on-demand** scanning!

> ***Note:*** *%SystemRoot%, %SystemDrive%, %ProgramFiles% are system variables dependent on the operation system and computer configuration. They can be determined using the command SET.*

1. If BitDefender Security for File Servers is installed on the same machine as BitDefender Security for ISA Servers

- Exclude the folder where BitDefender creates its temporary files:

  \%SystemRoot%\Temp\BDNP

  %SystemRoot% is:
  - On Windows 2000 :

    \Winnt

  - On Windows 2003 and ISA 2000

    \Windows

  - On Windows 2003 and ISA 2004, 2006,

    the Network Service profile, which is usually on %SystemDrive%\Documents and Settings\NetworkService\Local Settings

Computers Running Microsoft SharePoint Server and BitDefender Security for File Servers

The following files and folders must be excluded from both **real time** and **on-demand** scanning!

> ***Note:*** *%SystemRoot%, %SystemDrive%, %ProgramFiles% are system variables dependent on the operation system and computer configuration. They can be determined using the command SET.*

1. If BitDefender for File Servers is installed on the same machine as BitDefender for MS SharePoint
   - Exclude the folder where BitDefender creates its temporary files:

     %SystemRoot%\Temp\BDTemp
2. To increase server performance, you should exclude the SharePoint databases.
   - They are usually located in a path of form:

     %ProgramFiles%\Microsoft SQL Server

Computers Running BitDefender Security for File Servers and BitDefender Enterprise Manager

The following files and folders must be excluded from both **real time** and **on-demand** scanning!

> ***Note:*** *%SystemRoot%, %SystemDrive%, %ProgramFiles% are system variables dependent on the operation system and computer configuration. They can be determined using the command SET.*

1. To increase server performance, exclude the Enterprise Manager working folder:

%ProgramFiles%\Softwin\BitDefender Enterprise Manager\BitDefender Server