Need to Know

Etrust Server Exclusions

Etrust Antivirus software monitors files on the server for viruses. This scanning may cause issues with certain files, processes and directories. The following outlines what exemptions from scanning should be made on the server machine.

1. Should always exclude the following files and folders from file-level scanners:

- .EML, .EDB, .STM, .LOG, .DAT and .CHK files.

- The Exchange Server drive represented by the IFS. By default, this is drive M. This is normally specific to Exchange 2000 and SBS 2000.

- Exchange databases and log files. 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 file.

- The Exchsrvr\Mailroot virtual server folder.

- The working folder that is used to store streaming temporary files that are used for message conversion. By default, this folder is located at \Exchsrvr\MDBData, but you can configure the location.

- The temporary folder that is used with offline maintenance tools such as Eseutil.exe. By default, this folder is the location where the .exe file is run from, but you can configure the location when you run the tool.

- Site Replication Service (SRS) files in the Exchsrvr\Srsdata folder.

- Microsoft Internet Information Service (IIS) system files in the %SystemRoot%\System32\Inetsrv folder.

- IIS working files in the %SystemRoot%\IIS Temporary Compressed Files folder.

- DHCP Folder in %SystemRoot%\System32\DHCP

2. Should also exclude the following processes from all scanning :

store.exe
isinteg.exe
eseutil.exe

mtacheck.exe
exmgmt.exe
srsmain.exe
emsmta.exe