Does antivirus software work with EFT Server?

THE INFORMATION IN THIS ARTICLE APPLIES TO:

- EFT (All Versions)

QUESTION

Does antivirus software work with EFT?

ANSWER

EFT writes files to disk in plaintext by default, which any antivirus agent should be able to examine. EFT has the option to create folders with Microsoft Encrypting File System enabled. These should also be open to antivirus agents to examine. If a file is sent to EFT and the file is already encrypted, the antivirus client will likely be unable to detect a virus in the encrypted file.

Are you able to provide a list of file exclusions so we can work through these internally?

Due to the large number of AV programs on the market and differences in how those programs operate, Globalscape is unable to provide a definitive list of files to be excluded from AV scans, as that list could change depending on the AV vendor.

For fail safe compatibility, Globalscape recommends excluding the installation directory where the EFT program files are installed, along with its configuration and cluster config paths, listed below.

If full exclusion is not an option, the following two methods could be applied:

- The first is to not add any exclusions, and then add in exclusions if/when errors are encountered by EFT in its normal course of operations. This maximizes AV coverage at the risk of operational failures within EFT.
- The second is to exclude known file types that are typically managed by file locks, such as configuration files, log files, and dependencies loaded by EFT. This can be determined via tools such as Microsoft's Process Explorer (https://docs.microsoft.com/en-us/sysinternals/downloads/process-explorer) and following EFT's process tree. This increases AV coverage but at the expense of upfront efforts required to try to identify which files to exclude. There is also residual risk associated with missing certain file or path exclusions that may result in operational

failures.

Executables:

Running these with a service account with the proper permissions is recommended.

EFT Server/EFT Server Enterprise specific:

- Cftpstes.exe - EFT Server Service
- Cftpsai.exe - EFT Administration Console
- Amtb.exe - AWE Task Builder
- Awe.exe - AWE Engine

DMZ Gateway Server specific:

- DMZGatewayAdmin.exe - DMZ Gateway console
- DMZGatewayServerService.exe - DMZ Server Service

DMZ runs off of java so you will need to make sure that java is allowed to run on the box. The default path that it calls from is here:

"C:\Program Files\GlobalSCAPE\DMZ Gateway\bin\DMZGatewayServerService.exe" -s "C:\Program Files\GlobalSCAPE\DMZ Gateway\conf\DMZGatewayServerService.conf"

If you have the latest version of DMZ Gateway Server (3.5.0 build 16), it uses jre1.8.0_162(Java).

Folder paths:

Full-control permission is recommended for the service account.

EFT Server/EFT Server Enterprise specific:

- <Installation path> - Default location (C:\Program Files (x86)\Globalscape\EFT Server Enterprise or C:\Program Files\Globalscape\EFT Server)
- <Local config path> - Default location (C:\ProgramData\Globalscape\EFT Server Enterprise)

High Availability specific:

- <Shared config path> - Determined by the installation
- <Site root paths> - Default location (C:\InetPub\EFTRoot)

DMZ Gateway Server specific:

- <DMZ installation directory> - Default location (C:\Program Files\GlobalSCAPE\DMZ Gateway)