Passport: 4000 Antivirus Software

SUMMARY

Antivirus software, if used, should be carefully configured to avoid performance issues.

MORE INFORMATION

Some Passport systems are capable of receiving messages from external sources, via SMTP or various API's. Therefore, it is conceivable that these messages could contain viruses. To provide protection against passing on these viruses, it may be worthwhile to use antivirus (AV) software.

The only folder in the Passport system that should be checked for viruses is the MSG folder. The content of all messages pass through this folder. For performance purposes, the AV software should be set to perform its real-time checks only when files are written to this folder. There should be no need to perform any real-time checks when files are read from this folder, and doing so will impair performance needlessly.

Note that this folder might reside on a separate file server. In this case, the AV software on that file server should be used for any such real-time checks. You should not configure any AV software on the Passport computer itself to perform any checks on any network folder.

All other folders in the Passport system should be excluded from any AV checks or scans.

The typical action for AV software, upon detecting a virus, is to move the file to some quarantine area. The Passport will therefore regard any inability to read a file that it has just written to the MSG folder to be an indication that the associated message contains a virus. Such messages will be exceptioned with the notice that a possible virus was detected.

Antivirus Exclusions:

- *C:\Program Files (X86)\Passport4000\
- C:\Users\Public\LaneTelecommunications\
- C:\Users\(Passport Service Account)\
- C:\Program Files (x86)\Common Files\Passport4000 Shared\
- C:\Program Files (x86)\Common Files\ImageMaker\
- C:\Program Files (x86)\Common Files\Brooktrout\

Firewall Rules For Any Port These EXE's Can Talk In and Out:

- *C:\program files (x86)\passport4000\exe\cmon.exe
- *C:\program files (x86)\passport4000\exe\pccmail.exe
- *C:\program files (x86)\passport4000\exe\smtp.exe

*C:\ above is used as reference to the installed drive, could be D:\, etc.

Port Exclusions:

- Named Pipes, FileApi & HSBFile TCP port 445
- Comm. Server, LFaxService to Message Servers: TCP Port 700/701
- Passport Client Applications to Message Server: DCOM
- Message Server to DocConvert Servers: DCOM
- Passport WebService to Message Server: DCOM
- Passport Message Objects API: DCOM

DCOM:

- Protocol used: TCP, UDP
- Port used: TCP-135, UDP-135, and UDP 1024-65535
- SQL Server ODBC: TCP default port 1433, UDP default port 1434 and DCOM for Windows Management Instrumentation (WMI) for SQL Server Configuration Manager

SMTP:

- TCP default port 25 (outgoing) & 587

HTTP:

- Passport Web Client, WebService: HTTP TCP default port 80 & 443

FoIP Using SR140 or TR1034 SIP and T.38 Requirements:

- Port 5060 – SIP signaling port – UDP (UDP remains the default. Starting with SDK 6.6, SIP over TCP can be used to communicate between SR-140 and a SIP gateway as long as the gateway supports TCP)
- Port 8080 – TCP port for HTTP (license activation - required for automatic registration via Internet; otherwise, manual registration via Dialogic Website is required)
- Ports 56000 to 57000 – UDP ports for FoIP traffic