Onyx Anti-virus and Firewall Guidelines

ONYX does not recommend any specific antivirus software or running without security software in place, but some firewall and antivirus software must configured with exceptions for ONYX applications and printer ports to allow proper functioning and maximum performance. This example assumes ONYX software is installed at C:\Onyx21\

- None of the executable files within the ONYX directories should be blocked by antivirus
    - Change the antivirus settings to add exceptions for individual program files or the whole installation directory
    - Typical antivirus settings to allow programs are called “low risk” or “safe” processes.
    - The most important program are:
        - RIP-Queue – C:\Onyx21\server\postershop.exe
        - Media Manager – C:\Onyx21\MediaManager\bin\MediaManager.exe
        - Job Editor – C:\Onyx21\Preflight\preflightLauncher.exe
    - RIP processing EXE files should also have no restrictions:
        - Thrive: appeui.exe, appenormalizer.exe
        - RIP: jawsqt.exe, jawspap.exe
    - Licensing program files must also be allowed with no restrictions:
        - C:\Windows\System32\hasplms.exe

- Folders that ONYX uses should have antivirus scanning/monitoring disabled
    - All folders in the ONYX installation (C:\Onyx21 and all subdirectories)
    - Printer specific “work” folders may need to be added as a separate exceptions if the work folder for a printer has been configured to be outside of the main installation path (C:\Onyx21 in our example)
- Network communication cannot be blocked by antivirus or firewall
    - TCP/IP needs to be allowed on ports 80, 515, 1947, 8889, 9100 and 10000
    - For HP printers, ports 8085, 8086 and 8090 may also need to be allowed