

# ONYX Antivirus & Firewall Guidelines

ONYX does not recommend any specific antivirus software or running without security software in place, but some firewall and antivirus software must be 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:\Onyx22\

- Licensing program files and servers must also be allowed with no restrictions:
  - Physical Key Licensing
    - C:\Program Files (x86)\Common Files\Aladdin Shared\HASP
  - Soft Key Licensing
    - C:\ProgramData\Onyx\NetLicense
    - Onyx License Verification Server <https://api-prod-ogfx.azure-api.net>
    - The Following URL can be used to test the connection to the License Verification Server. This should return the following: "Valid connection found"  
*<https://api-prod-ogfx.azure-api.net/licensing/connection/test>*
- 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:\Onyx22\server\postershop.exe
    - Media Manager – C:\Onyx22\MediaManager\bin\MediaManager.exe
    - Job Editor – C:\Onyx22\Preflight\preflightLauncher.exe
  - RIP processing EXE files should also have no restrictions:
    - Thrive: appeui.exe, appenormalizer.exe
    - RIP: jawsqt.exe, jawspap.exe
- Folders that ONYX uses should have antivirus scanning/monitoring disabled.
  - All folders in the ONYX installation (C:\Onyx22 and all subdirectories)
  - Printer specific "work" folders may need to be added as a separate exception if the work folder for a printer that has been configured to be outside of the main installation path (C:\Onyx22 in our example)
- Network communication cannot be blocked by antivirus or firewall.
  - TCP/IP needs to be allowed on ports 80, 515, 1947, 5093, 8889, 9100, 27017 and 10000
  - For HP printers, ports 8085, 8086, and 8090 also need to be allowed.
  - For Epson printers, port 30561 also needs to be allowed.
  - For Mimaki printers, ports 8002, 11110, and 11111 also need to be allowed.