XPression Anti-Virus Best Practices

Introduction

Ross Video has many years of experience developing networked production equipment, enabling us to deliver field validated solutions that are proven to meet today's changing work-flow requirements. Ross Video products leverage the same high speed networking technologies and interoperability pioneered by the IT industry.

Standard IT platforms provide proven flexibility and workflow advantages, but they are more susceptible to virus infection than custom hardware solutions. Ross Video recognizes that you cannot afford to have your on-air equipment or content exposed to these viruses and risk taking your programming off-air.

This document offers recommendations on how to best protect your Ross Video products from virus infection.

Compatible Products

The following products are compatible with the instructions and guidelines in this document:

- XPression Studio, Studio Flex, Studio SCE, & GO!
- XPression BlueBox, BlueBox Flex, BlueBox SCE, BlueBox OFL, & GO!
- XPression Prime & GO!
- XPression Clips
- XPression Clip Store
- XPression Player & Player SCE
- XPression Developer
- XPression Designer
- XPression DataLinq Server
- XPression Gateway
- XPression Project Server
- XPression Asset Cache Server
- XPression Template Builder
- XPression INcoder
- XPression Remote Sequencer
- XPression Tessera

Antivirus Products

Ross Video uses ESET for our corporate and product verification initiatives. It is not possible for Ross Video to qualify each and every anti-virus software product on the market, yet we feel that the products are similar enough in nature and function to make a general statement about the utilization of them, including “best practices” for real-time scanning and scheduled scanning.

Phone: +1 613-686-1557 • Technical Support: +1-833-859-0499 (North America) • +800 3540 3545 (Int'l) • 1 300 007 677 (Australia) • 3500DR-500-03 Rev 3 • February 2026

Exclusion of Certain File Types

Real-time anti-virus scanners have an effect on the overall performance of the host PC. Ross Video recommends leaving real-time scanning enabled, but disabling real-time scanning of certain low-infection risk file types to reduce the impact on playback performance.

The following file types can be excluded from real-time scanning (Ross Video recommends that these file types are still included in scheduled scans):

Video Clip Files

- .AVI, .MPG, .MOV, and .MP4

Image Files

- .BMP, .JPG, .PSD, .PCT, .PCX, .PIC, .PNG, .TGA, and .TIF

Audio Files

- .MP3 and .WAV

3D Models

- .3DS, .FBX, .FBM, .OBJ, and .C4D

Network Setup and Configuration

The following guidelines are outlined for your IT department to use in setting up the networking of Ross Video on-air equipment in a broadcast facility. While it is understood that all of these guidelines may not be practical, following them will provide the best level of protection against system infection.

- Never share a folder or drive to “Everyone” with full-access.
- Always assign a local Administrator password on every machine. Not assigning a local Administrator password can introduce a serious security risk.
- Do not store files with .EXE extensions in directories with write permissions.
- If possible, keep all Ross Video production equipment on a separate network that is isolated from other machines in the facility.
- Disable Internet access on all Ross Video production machines that do not require it.
- Install and run anti-virus software on all Ross Video PC-based equipment.

Institution of Policies

While following the previous guidelines is critical to protect your broadcast network from infection, some of the responsibility must be passed on to users to keep the system free from infection. Ross Video recommends that the following policies are enforced by your IT department and followed by all users of Ross Video products:

- Perform a complete system scan of any machine before attaching it to the same network as any Ross Video production equipment.
- Perform a complete scan of any material on CD, Pen- or USB drive or other external media before copying it to any on-air Ross Video product.
- Exercise extreme caution when copying material to a Ross Video product that is used in 24/7 operation and, if possible, only during maintenance periods.
- Avoid downloading files directly from the Internet to any Ross Video on-air product whenever possible.

Scheduled Scans

Ross Video recommends that regular scheduled system scans are performed during periods where the system is under light use. These scans should be performed on a daily basis and will complement the Network Setup and Configuration guidelines outlined in this document.