Windows and General Security

Windows 10/11 and associated server operating systems have the ability to setup various levels of permissions/security for users who will be logging onto the machines and the network.

These permissions and security settings are often the source of system-level problems when running a networked program such as Anthology. Various anti-virus and firewall products you may have running on your system can also make simple tasks difficult if these products are not properly set up. Finally, upgrading programs (including Anthology) on a system can cause complications when Windows or antivirus or firewall products reapply their default settings to the new version.

Problems with improper or insufficient security settings usually manifests through Anthology with random error messages or problems with doing electronic ordering via FTP, with processing credit cards, or with not being able to print or save changes; or with “File access denied” messages.

This document is intended to give some general guidance on permissions and security issues that may need to be addressed in a network installation of Anthology. However, please note that the details of network troubleshooting and configuration are not covered under the free support period or Anthology Maintenance Agreement available at the Customer Zone of our web site.

You may prefer to get a local technician who specializes in network applications to help with these issues, or Anthology Consulting Services offers a number of affordable ways to help.

Every user of Visual Anthology on the network must have full control both permissions and security on the entire Anthology directory tree (i.e., the Anthology home directory and all its subdirectories).

To share the Anthology folder on the file server, you must turn off “Simple File Sharing” so that you can apply full permissions. (Please refer to Microsoft Windows document).

After an Anthology upgrade or a Windows update, Windows Firewall may recognize a change and may start blocking any internet connection attempts from upgraded software. The permissions and security for Anthology’s VAL.EXE file in Windows Firewall may need to be reset after an upgrade.

Please take the time to learn how to turn off auto and live updates and set up the scheduling for “updates” and “scanning” as it is important that all updates are controlled updates with your full knowledge rather than auto updates where you have no knowledge when it is applied to your computers.

Anti-Virus Exclusions and Exceptions

There are many software applications that are designed to protect your computer from a virus, malware / spy-ware, and other forms of damaging or malicious code. We strongly suggest that you consider purchasing one of these available packages and keep it up to date and scan your systems at least once a week (before or after business hours). **Please make sure your program is scheduled to update and scan at a time before or after regular business hours. This should also include "Auto-Updates" for Windows updates. Schedule ALL program updates "before or after" regular business hours.**

Once installed, each of these pieces of software essentially keeps an "eye out" for anything coming into the system that might cause a problem. They safeguard your computer in the event something tries to attack your operating system and damage its files.

For instance Norton Anti-Virus calls their active scan "Auto-protect" and AVG calls their active scanning the "Resident Shied". The premise is exactly the same: they are constantly active. Every file that passes through the system is examined by these programs for malicious code.

While we encourage and recommend the use of these vital pieces of software, we also would like you to familiarize yourself with how to properly configure them.

When you run Anthology in a networked environment, there are many files that are viewed, opened, and appended across the network. The performance of the file server can be greatly reduced (or increasingly problematic) if every file that needs to be viewed, opened, or appended to through the network is temporarily stopped by "Auto-protect" or "Resident Shield" as they try to verify that this is a good or bad program.

That's why each of these software applications allows you to exclude or make exceptions to the constant scanning rule. It is your responsibility to learn how to create exclusion or exceptions list within the Anti-Virus software you choose. To learn how to do this, start with the help files available in the program you have chosen.

Configuring Windows Firewall Exclusions in Windows 7, 10 and 11

Windows Firewall and other security programs need to be told to leave VAL.EXE alone

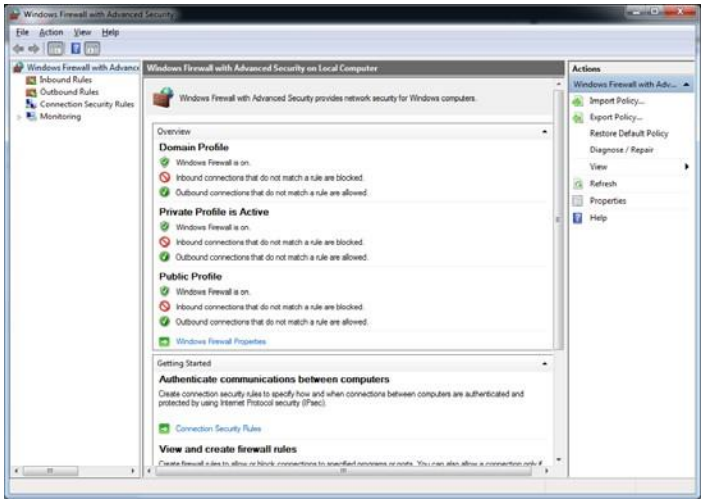
(Exception/Exclusion) on every workstation taking credit cards. Note that in Windows 7 this means going into the Control Panel, Windows Firewall, Advanced Configuration, and adding an "InBound Rule" and an "OutBound Rule". If you just use the wizard tool you'll only get an Inbound rule.

- Go to Start | Control Panel
- Click on “System and Security”

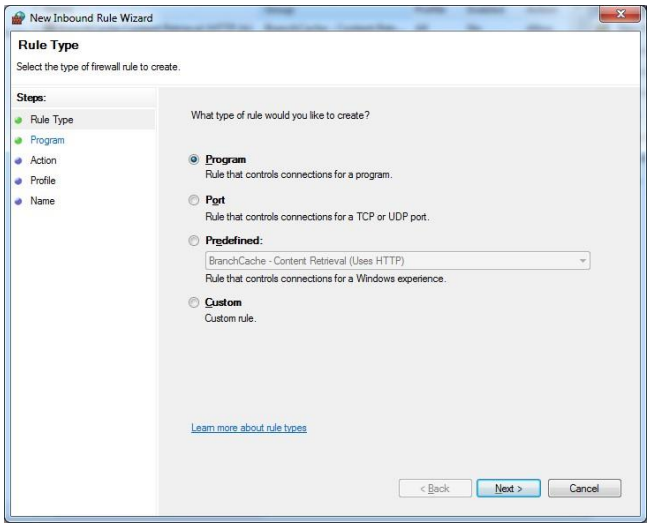
- Click on “Windows Firewall”

- Click on the “Advanced Settings” link on the far left side

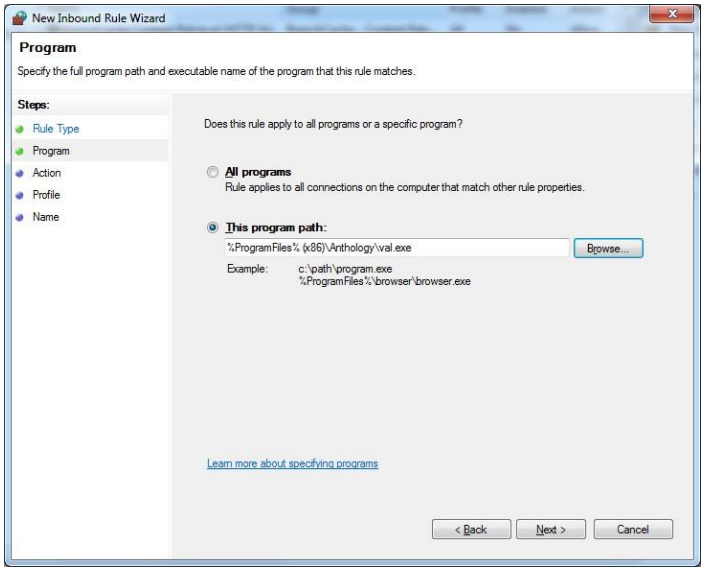
- Regardless if the Windows Firewall is turned on or off, the exclusions should still be put in place in case the Firewall gets turned on later by accident.
- The Windows Firewall config screen comes up



- Click on the InBound Rules, right click, “New Rule”
- Choose “Program” for the rule, Next

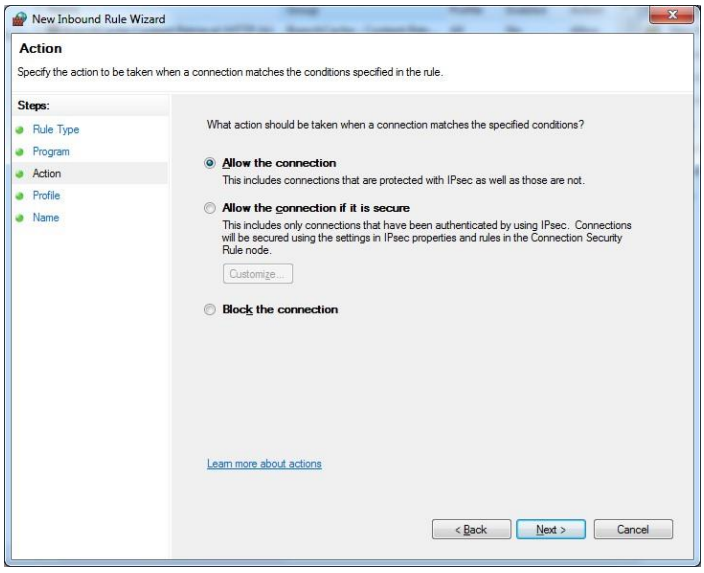
- 

  Browse to VAL.EXE on the server via local or mapped network drive, Next

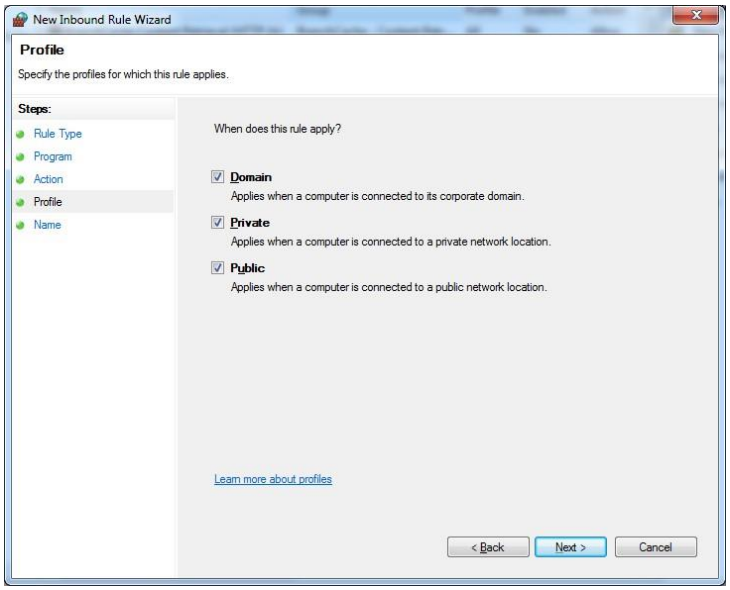


- Choose to Allow the Connection, Next

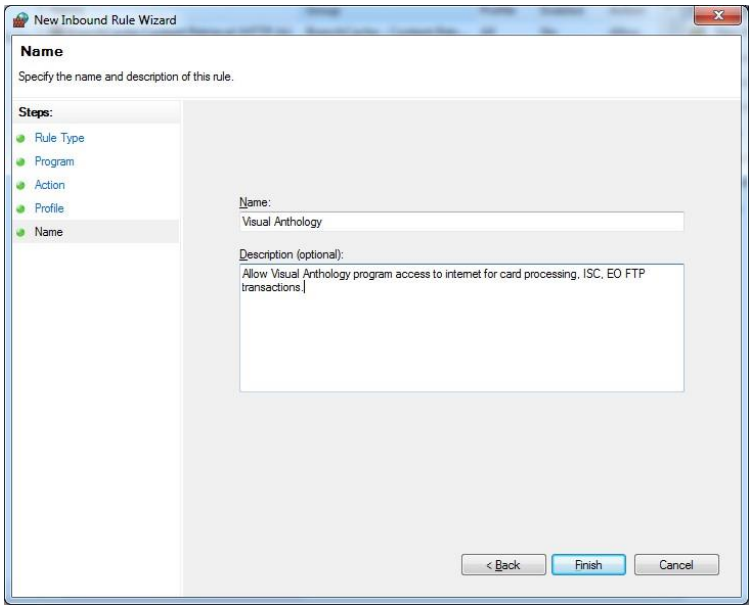
•



Allow rule to apply to all three, Domain, Private, and Public. Next. (Note this area might have settings that are optional, start with wide open first)



- Give the rule a name and description, Finish

- 

- Go back to Firewall Advanced window and add another Rule for the Outbound side repeating steps above. Note that the Action area by default will set the connection to Blocked, be sure to change to Allow. You may need to do a Restart on the machine after making these changes for them to take effect.