Windows and General Security

Windows XP, Windows 7 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).

The 'Simple File Sharing' that is Windows XP's default setting designed for a simple networks or even read/write permission does not grant enough permissions to run a complex application like Anthology. 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).

Windows XP Service Pack 2 has changed the way permissions and security is handled on directories and files. These changes may not take effect immediately after Service Pack 2 is installed because your existing programs already have these properties set. When you upgrade a program Windows XP sees the upgrade as a new program installation and applies permissions anew according to its new rules, often applying the lowest level, most stringent permissions. Windows 7 may also change some behaviors as the new service packs come out.

Further, Windows Firewall will also recognize the change and may start blocking any internet connection attempts from upgraded software. The permissions and security for Anthology's VAL.EXE and credit card program PCCharge ACTIVE-CHARGE.EXE files 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, mal-ware / 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.**

The big four in the industry right now are:

- **Windows Firewall**
- **AVG Professional version**
- **Norton Anti-Virus (Not Norton 360 or other bundled offers)**
- **MacAfee Professional version**
- **Panda AV**
- **Kaspersky**

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.

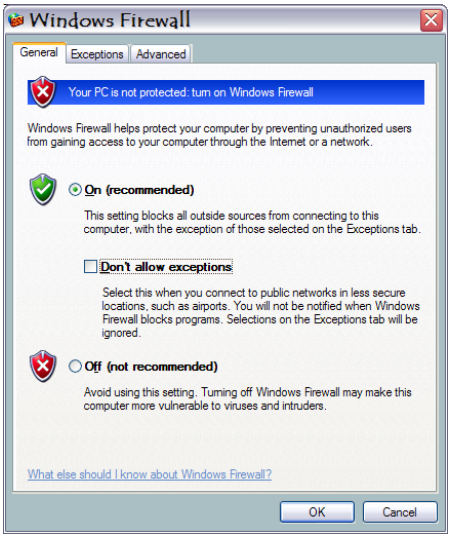
When you run Anthology in a networked environment, there are many files that are viewed, opened, and appended across the network. The performance of the file server can be greatly reduced (or increasingly problematic) if every file that needs to be viewed, opened, or appended to through the network is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

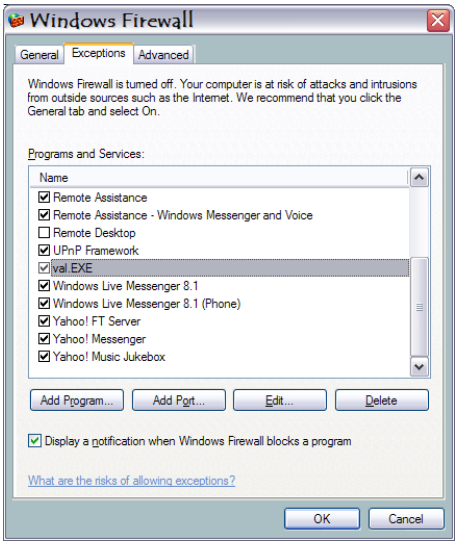
That's why each of these software applications allows you to exclude or make exceptions to the constant scanning rule. It is your responsibility to learn how to create exclusion or exceptions list within

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 XP

Windows XP and Vista both have this firewall functionality loaded by default. It is best to setup these exclusions regardless if you have the function enabled or not as doing some windows updates could turn the function back on with no warning to you. Go to Start menu, Control Panel, Windows Firewall. Click on the Exceptions tab, click on “Add Program”. Browse to the Anthology or Active-Charge directories on your server. For Visual Anthology select the file named “Val.exe”, and for Pccharge look for the file marked “Active-Charge.exe”. Click OK to save changes.

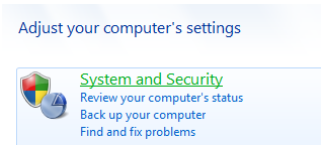




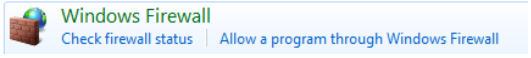
Configuring Windows Firewall Exclusions in Windows 7

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

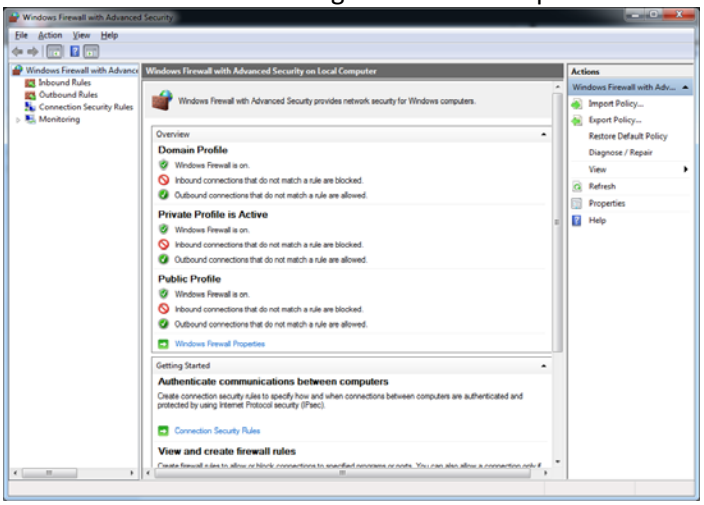


- Click on “System and Security”
- Click on “Windows Firewall”

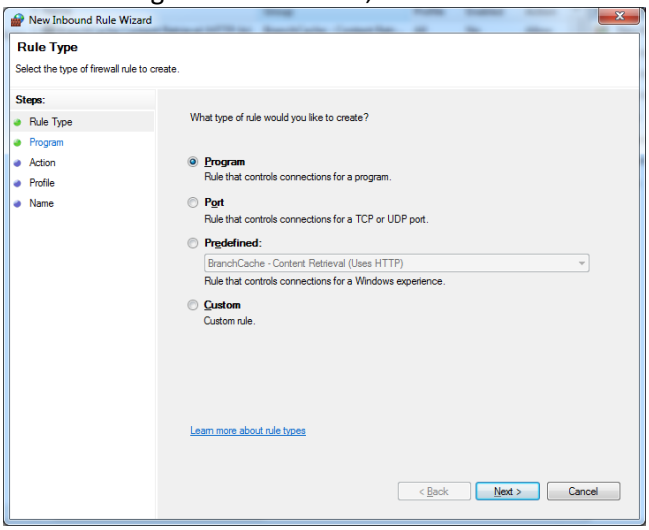


- Click on the “Advanced Settings” link on the far left side

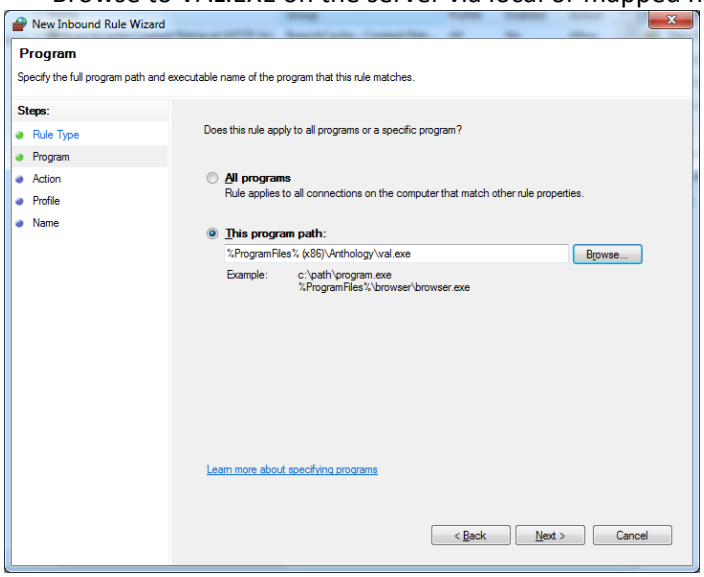
- Regardless if the Windows Firewall is turned on or off, the exclusions should still be put in place in case the Firewall gets turned on later by accident.
- The Windows Firewall config screen comes up



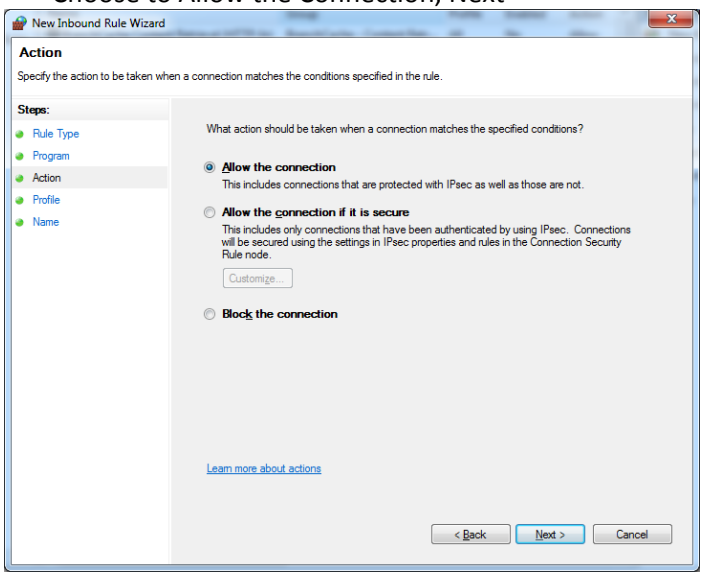
- Click on the InBound Rules, right click, “New Rule”
- Choose “Program” for the rule, Next



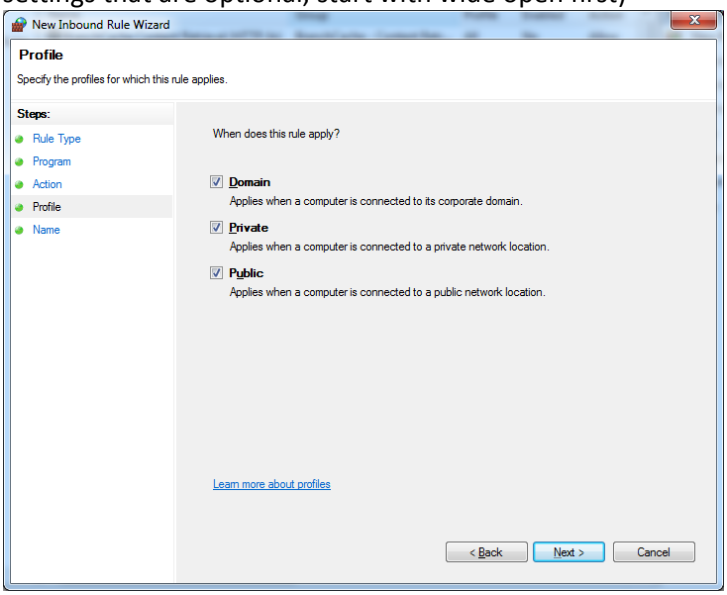
- Browse to VAL.EXE on the server via local or mapped network drive, Next



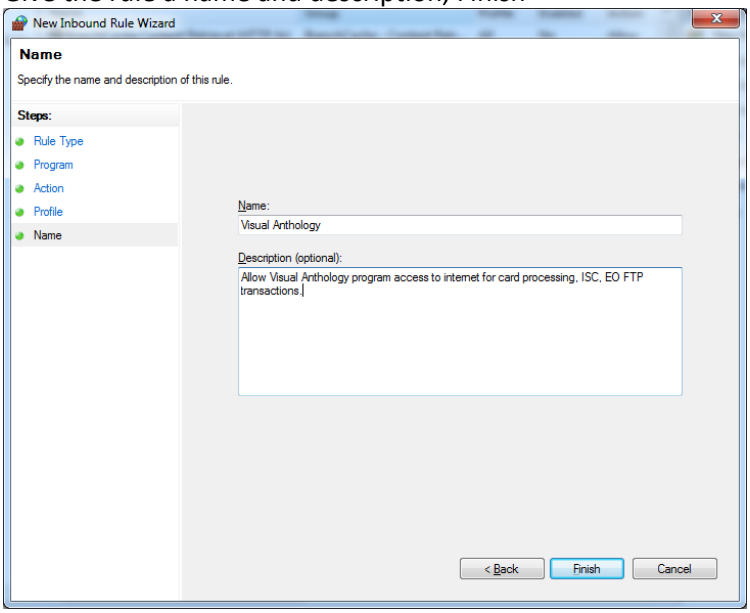
- Choose to Allow the Connection, Next



- 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.

Configuring AVG Exclusions

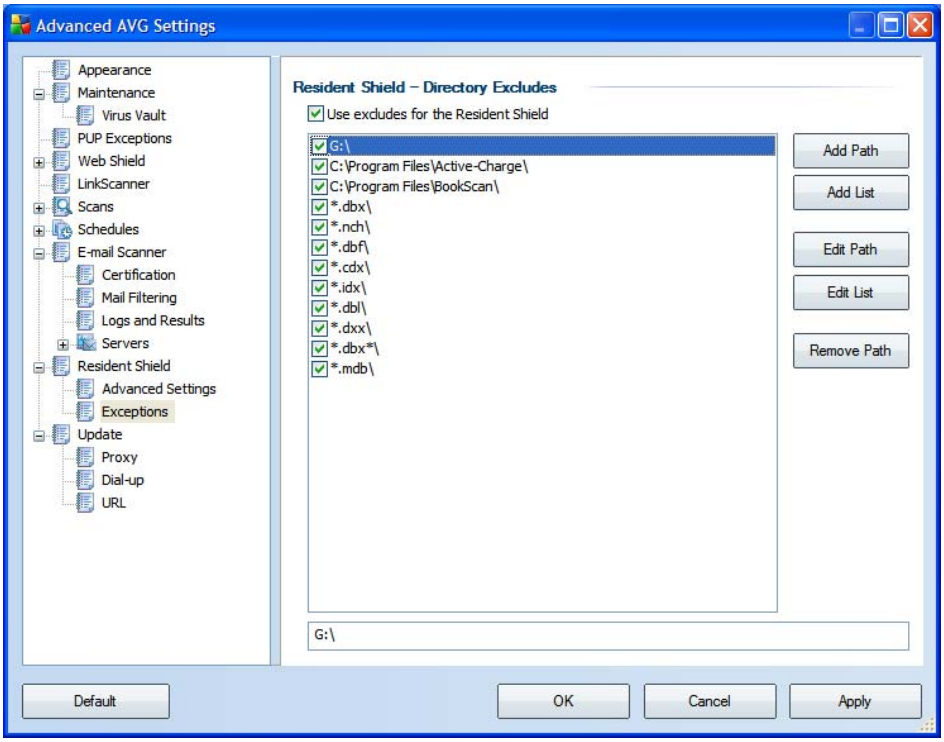
Anthology currently recommends and installs AVG Professional version 8.0 when we build turnkey systems. The screen shots below show how we configure the exceptions within the AVG program. We are providing this as an example. Different programs and different versions of the program might look

different from our example. Once again, it will be your responsibility to learn how to configure the exclusions or exceptions to the constant scanning rules in the anti-virus software you choose.

Here's how we configure the Exclusions in AVG 8.0 when we build a turnkey system. This particular example is from a Workstation machine (Pos1):

1. Double click the AVG icon in the task bar (located by the time clock in the lower right hand corner). This will launch the main AVG interface displayed in the first screen shot.
2. Click Tools at the top then click "Advanced Settings".

3. This will bring up the "Advanced AVG Settings" window.



4. Click and highlight “Exceptions” in the list on the left hand side as per the screen shot.
5. Put a check in the “Use excludes for the Resident Shield” check box and click “Add Path”.
6. Here is a list of everything we recommend you exclude:
    - **Any directories or paths related to your Anthology, BookScan, PCCharge, or database of books installations**. **Examples**:
        - C:\program files\Anthology (this the default Anthology directory)
        - C:\program files\Bookscan (this is the default BookScan directory)
        - C:\program files\active-charge (this is the default PCCharge directory)
        - C:\TITLE_SOURCE (this is an example of a locally installed database of books)
    - **Any network mapped drives referring to these same locations:**
        - G:\ (this is the default map drive letter we use for the main Anthology folder from a workstation)
        - K:\ (this is the default map drive letter we use for a database of books)
        - H:\ (this is the default map drive letter we use for the Active-Charge directory)
    - After you have added all of your paths then click “Add List”.
    - **Here is a list of file types we exclude:**
    - *.dbx
    - *.dbf
    - *.cdx
    - *.idx
    - *.fp*
    - *.mbd

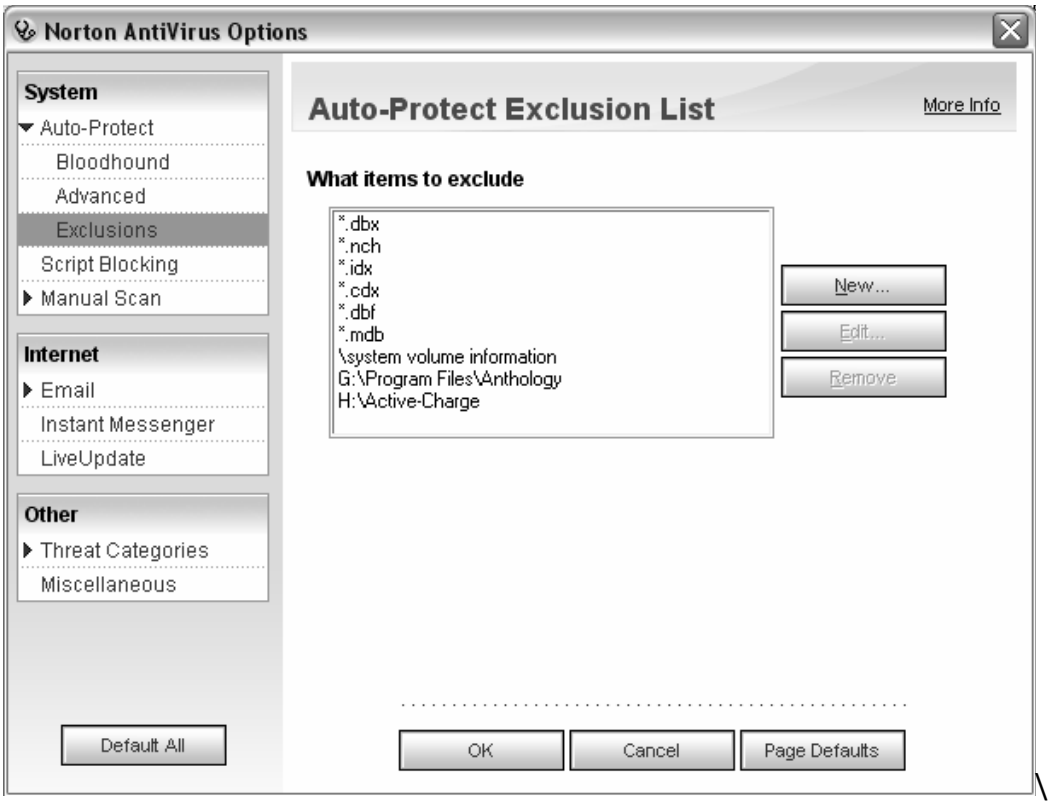
We are providing this list as of May, 5th 2008. This is just an example of how we configure these exceptions. AVG 8.0 is a third-party application and Anthology Technical Support cannot provide technical support for its use. If you have questions regarding configuring exclusions and exceptions in the software that you have chosen, please refer to the help files and technical support provided with that application.

Norton Anti-Virus 2006 Example:

Important! When users upgrade their Norton products from one version to the next (i.e., 2005 to 2006) any exclusions previously set up may be lost.

Following is a brief list of Auto-Protect exclusions you may wish to set up in your Norton program if performance is an issue. Open your Norton program to edit your exclusion list to allow *.dbf, *.cdx, *.idx and *.fpt files, as well as the Anthology directory on the server. Go to the Norton Anti-Virus screen and choose Options. If you are presented with a choice for Norton Antivirus choose that. The new Options screen should have a field on the top left for "Auto-Protect", click once on this to bring up the Exclusions menu item. If you use PCCharge you should also exclude *.mdb and the Active-Charge directory on the payment server. If you use CD Fetch from a database of books you should add their program directories to the list as well.

These entries will prevent the constant scanning of Anthology and PCCharge files traveling across the network and on the local station. You should make sure as well that a full system scan is being performed regularly. The Norton default is a full scan scheduled to run at 8pm on Friday night. For more information on configuring Norton please visit www.symantec.com

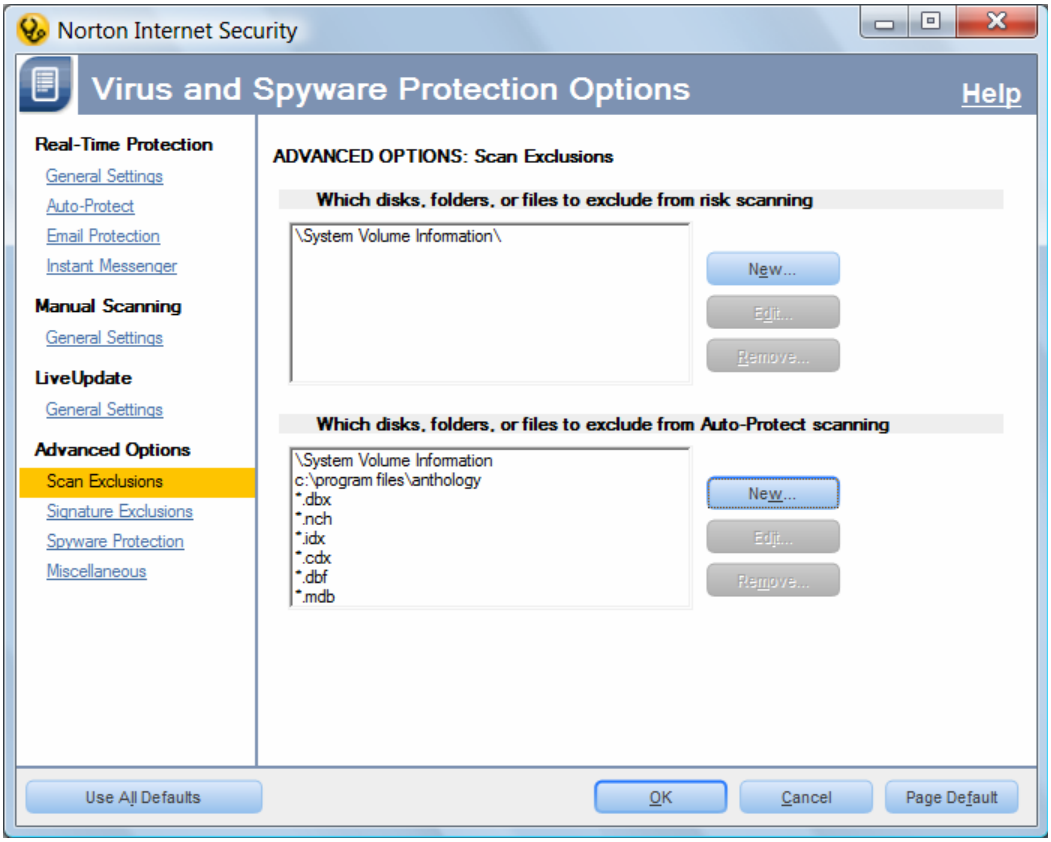


For Norton versions 2006 and older:

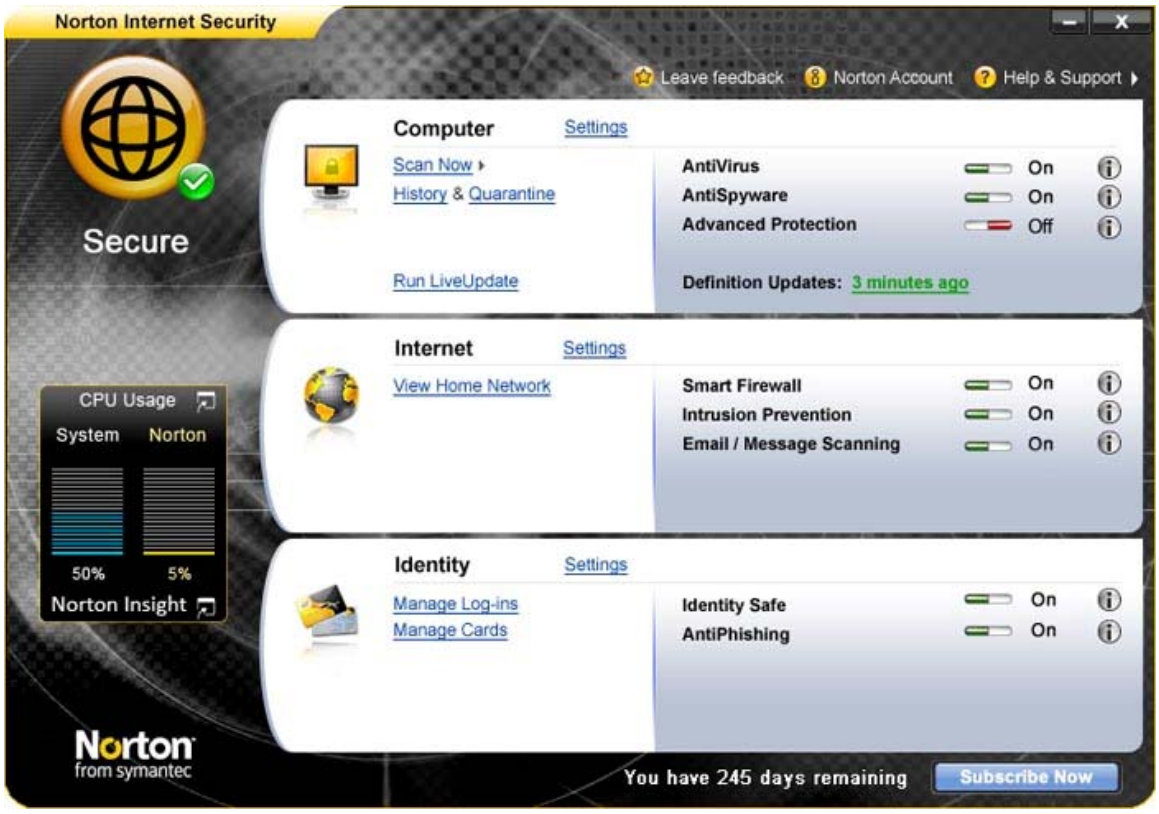
1. Double click on the Norton icon in the system tray (near the time)
2. Click on Tools | Options
3. Go to Norton Anti-virus
4. Click on “Auto-Protect” on the top left
5. Click on Exclusions
6. Click on New; begin adding the items shown above. The drive letters of G and H above May not match yours exactly. You should add the paths to your Anthology folder on the Server, using the same path found in the icon properties.

For Norton version 2007

1. Double click on the Norton icon in the system tray (near the time)
2. Click on the 2nd tab, marked “Norton Internet Security”
3. Click on Settings
4. Click on “Auto-Protect” under Basic Security
5. Click on Configure
6. Click on “Scan Exclusions” beneath Advanced Options
7. Click on New; begin adding the items shown above. The drive letters of G and H shown below may not match yours exactly. You should add the paths to your Anthology folder on the server, using the same path found in the icon properties.



For Norton Internet Security 2009



Symantec lists some detailed steps on how to enable web-based applications to access the internet:

http://www.symantec.com/norton/support/productdetail/index.jsp?pvid=nis_2009

Symantec also lists detailed steps on how to configure their network security map. A security map allows you to specify which computers on your local network may communicate with one another. In some cases installing or upgrading to a new version of Norton you must re-specify which computers on your network are 'trusted'.

http://www.symantec.com/norton/support/kb/web_view.jsp?wv_type=public_web&docurl=20080610160029EN&ln=en_US

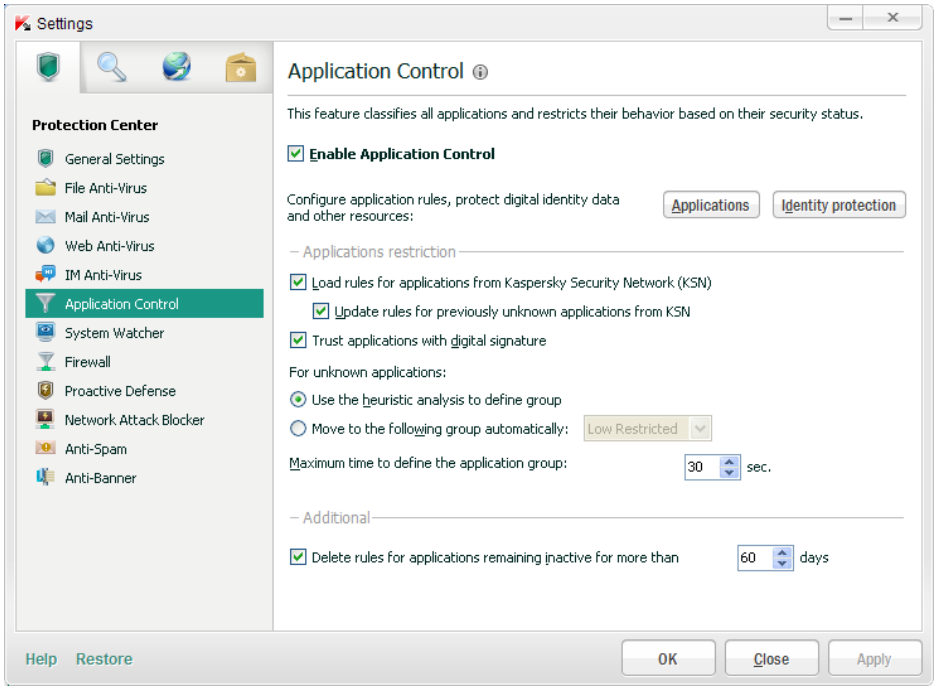
We are providing this list as of January 2012. This is just a sample of how we configure these Exceptions. Norton Anti-Virus is a third party application and Anthology Technical Support does not support it. If you have questions regarding configuring exclusions and exceptions in the software that you have chosen, please refer to the help files and technical support provided for in that application.

Configuring Kaspersky exclusions

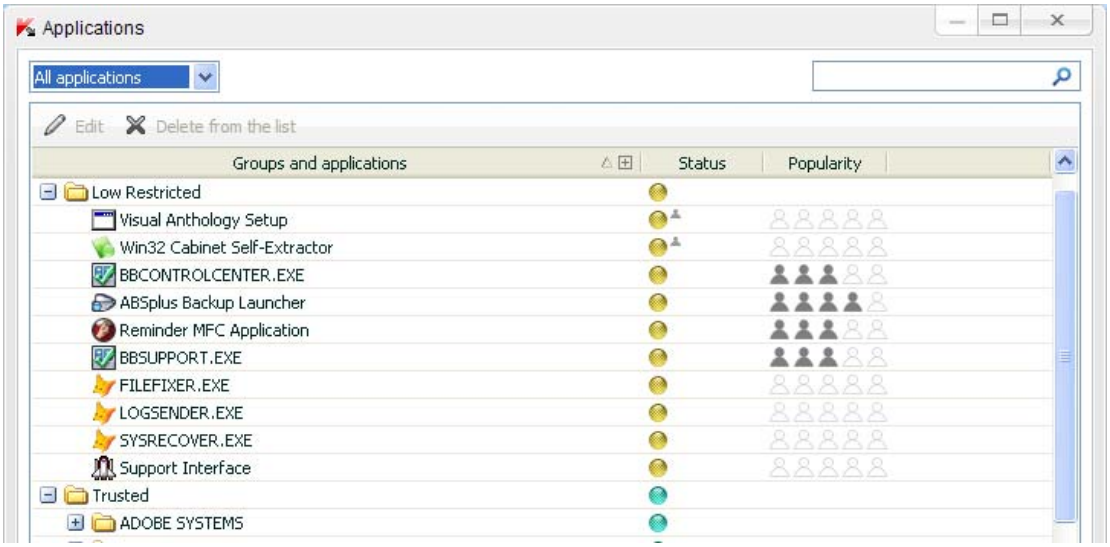
These settings must be done at the server and on any workstation.

To set exclusions in Kaspersky Internet Security 2012, open the main interface window and choose “Settings”.

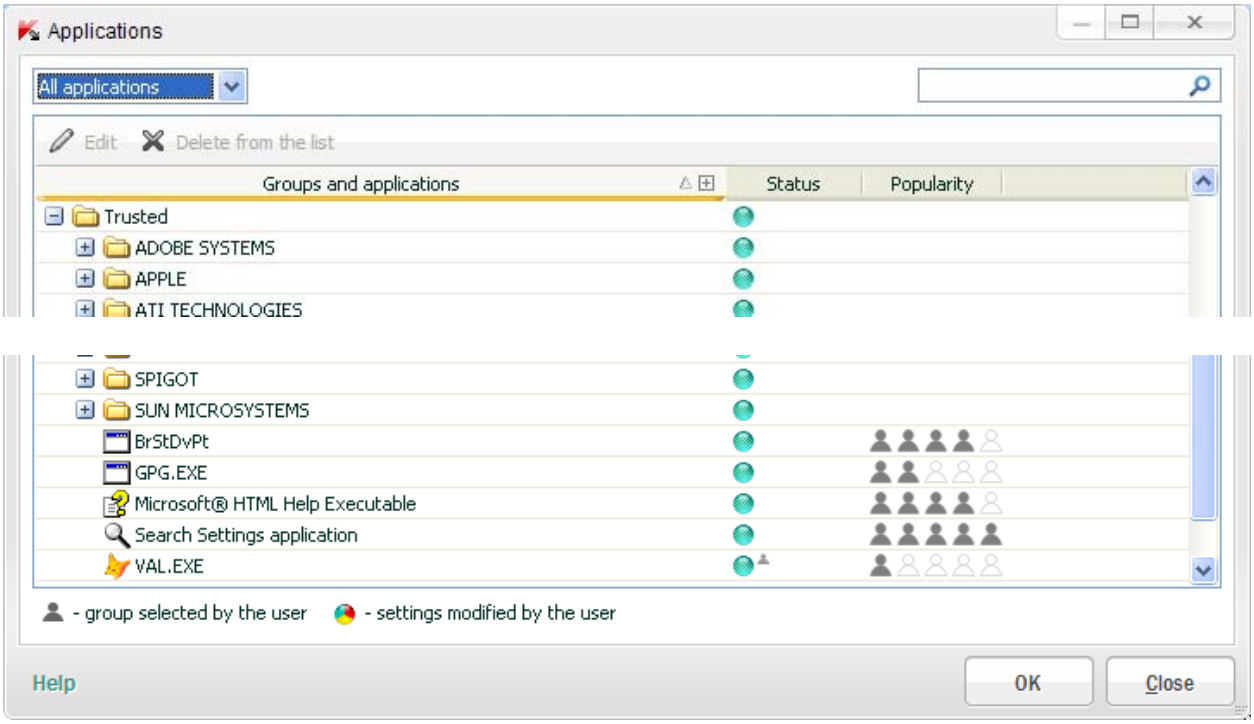
In the Settings window, under “Protection Center” choose “Application Control”



On the right side of the Application Control window, click the “Applications” button.
Scroll through the list of applications and locate the val.exe entry, it may be located under the “Low Restricted” group.

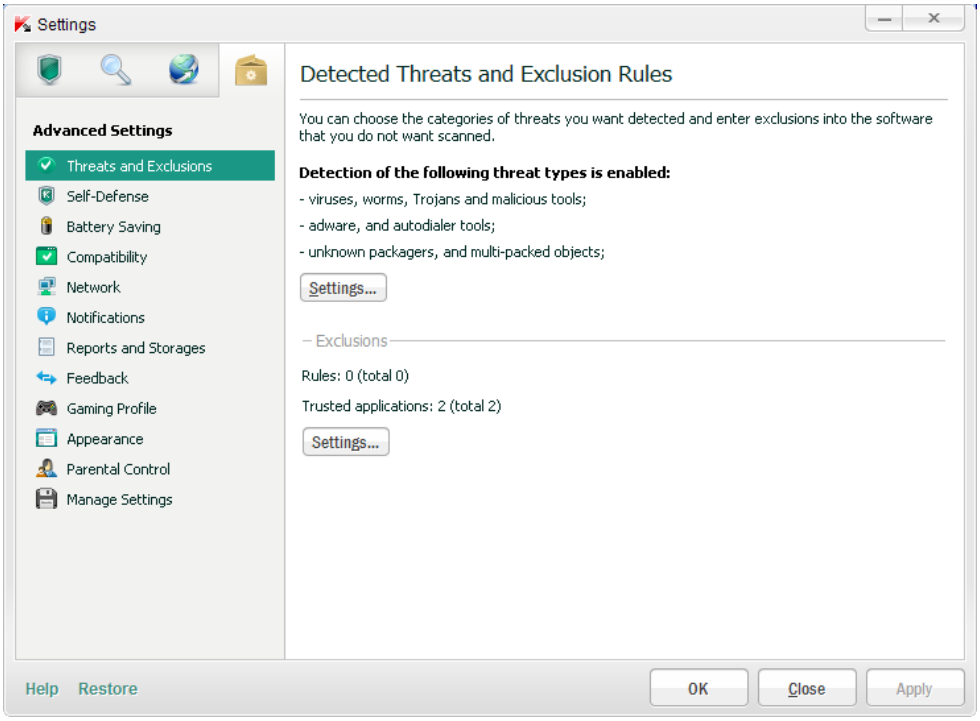


Right click on the Val.exe entry, choose to add it to the “Trusted” group.



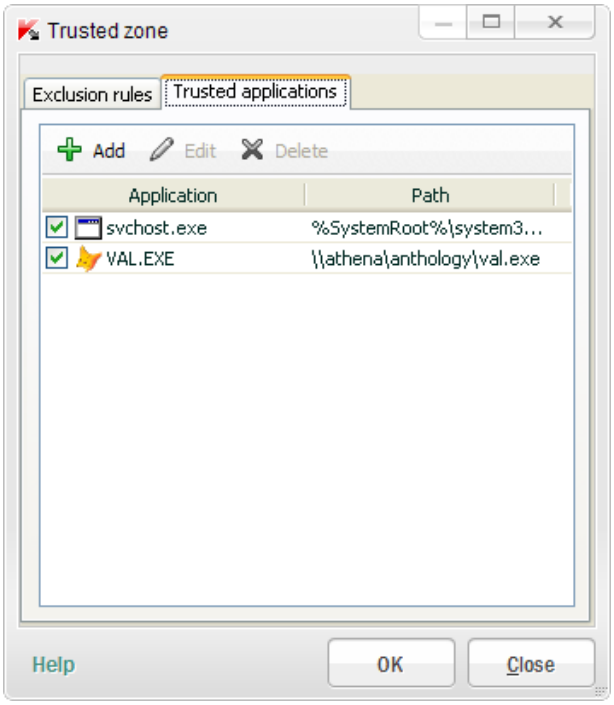
Click Ok to complete the change, continue on to Advanced Settings for additional settings.

On the main Settings window, click on the “Advanced Settings” tab (tan icon, far right)

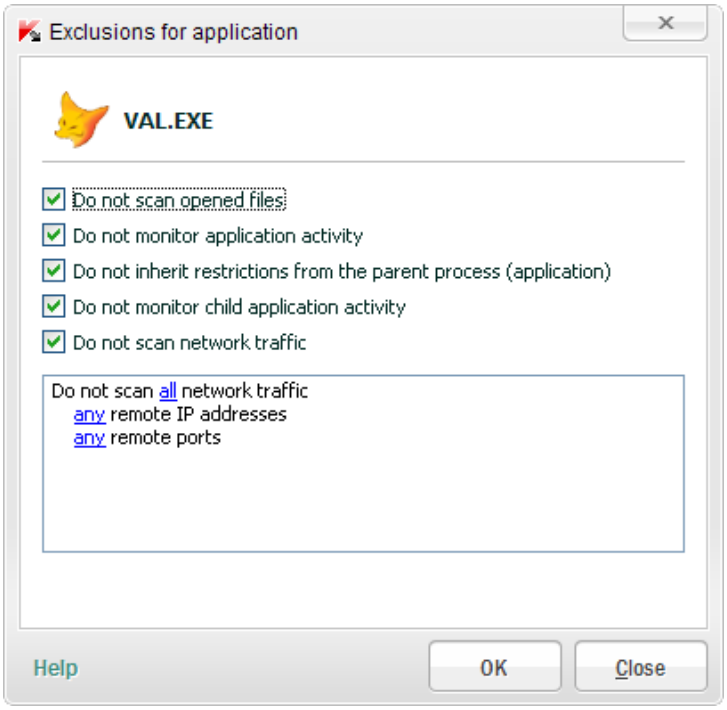


Select “Threats and Exclusions” on the left, then the Exlusion “Settings” button on the bottom half.

The “Trusted Zone” window appears, in the “Trusted Applications” tab, add the “VAL.EXE” app by clicking the “+ Add” and selecting it from the presented list of applications:



Highlight the “VAL.EXE” application from the list, and click “Edit” above.



Add a checkmark to each of the boxes, so Kaspersky does not interfere with VAL’s processing.

Click “OK” to save changes and “OK” again to close the Settings window. Restart computer.