Internet Security and Anti-Virus Applications Impacts on CimPro

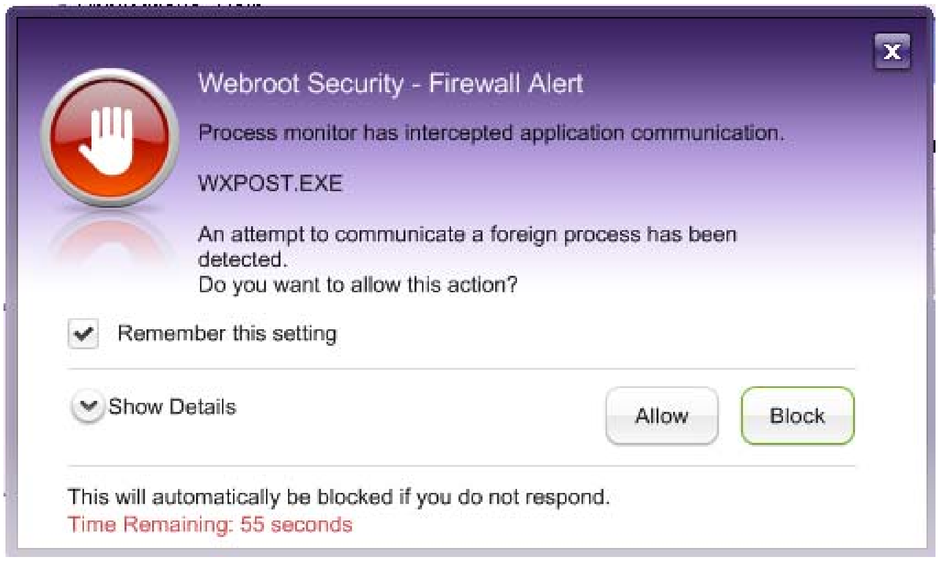
(January 2011)

Some of the latest generation of Internet Security and Anti-Virus applications are causing problems with various Austin NC applications and executables. These security applications are not determining that these Austin NC applications are infected, but are considering them as “unknowns”; thus they are being flagged as potential threats. Depending on the application (e.g., Norton Internet Security, Webroot Internet Security, McAfee, etc.) the security application's response may be nothing, flagging it as a potential hazard and asking the user to “Allow” or “Block” the application, quarantining the application, or even deleting the application. **NOTE:** Austin NC, Inc. has checked all its applications for viruses using several different anti-virus applications and our code is “virus free”.

It is not possible for Austin NC to know what type of security software each user is using to protect their computer or the settings that each user has specified for their security application. Thus, we cannot give exact fixes for each and every situation. Below are some generic helpful hints based on a few security applications we know about.

<u>The Security Application Flags an Austin NC Application as a Potential Hazard</u>

Figure 1 is a screen shot of a dialog from *Webroot Internet Security Complete 2011*. This security application identified one of the processing executables used by CimPro as a potential hazard. It asks the user to “Allow” or “Block” this executable (in this case WXPOST.EXE). To ensure CimPro works correctly, the user should “Allow” all CimPro related executables. In this case, there is a check box stating “Remember this setting”. If this is an option on your security application, ensure that the check box is checked; otherwise this dialog may reappear each time CimPro is run. The same would apply to any Option File Generator executables.



Webroot Security - Firewall Alert

Process monitor has intercepted application communication.

WXPOST.EXE

An attempt to communicate a foreign process has been detected.
Do you want to allow this action?

☑ Remember this setting

This will automatically be blocked if you do not respond.
Time Remaining: 55 seconds

Figure 1: Sample Dialog from Webroot Internet Security Complete 2011

The Security Application Quarantines or Deletes Application

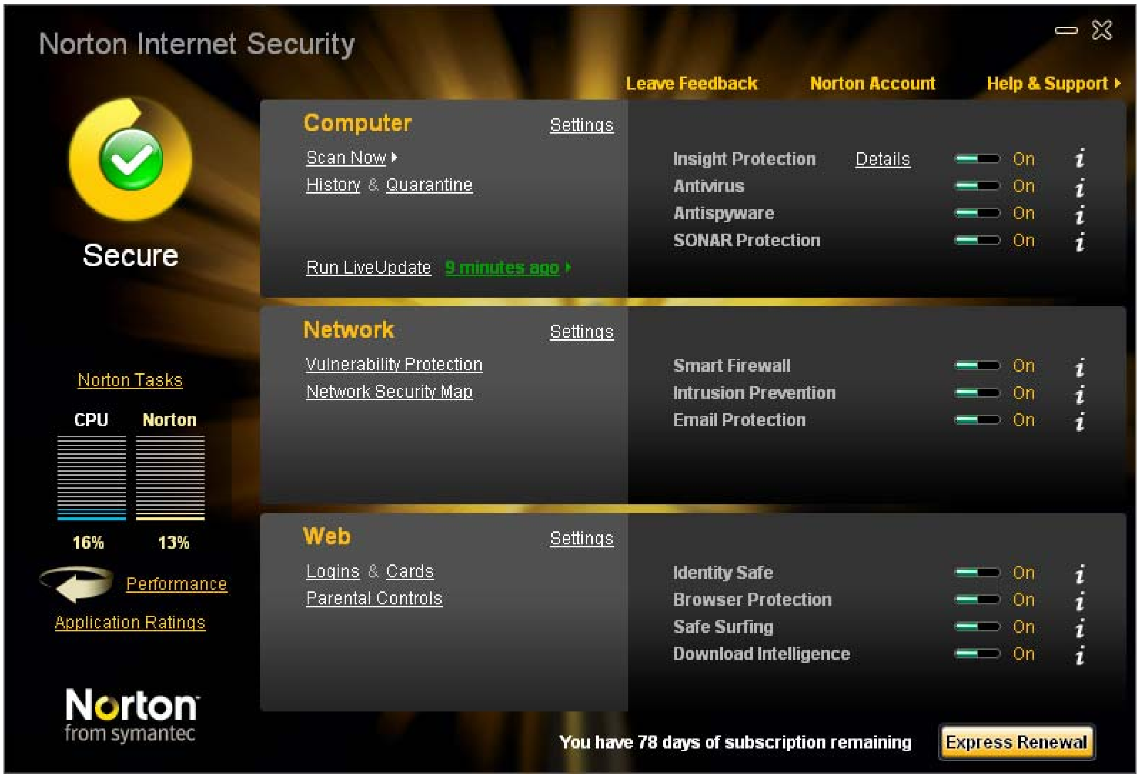
Some security applications (such as Norton Internet Security 2010) may inform you that one or more of the executables being used by CimPro (or the Option File Generator) may pose a risk and either automatically quarantine or remove the offending executable. The notification may be through a dialog or a pop-up indicator on the lower portion (generally lower right) part of the screen. It does not give the user the option to accept or deny the application. Thus, there are two ways to solve this:

1) Re-install or un-quarantine the deleted executable in the proper location and then tell the security application that this executable is acceptable.
2) Proactively tell the security application to allow all applications / executables from a specified directory (e.g., C:\camsys\anc\).

Restore Deleted or Quarantined Applications

Certain anti-virus applications may automatically quarantine or delete CimPro or Option File Generator related executables. One example of this is *Norton Internet Security (NIS) 2010*. Some security applications are now using heuristic programs during runtime to detect suspicious applications. As an example, NIS 2010 uses a runtime heuristic called SONAR to detect unknown or suspicious files. When it detects file that match is detection criteria, it deletes them automatically. The following shows how to restore a deleted (or quarantined) in NIS 2010. Similar procedures would be required for other security applications.

1. Open up NIS 2010 and click on the **Quarantine** link as shown in Figure 2.

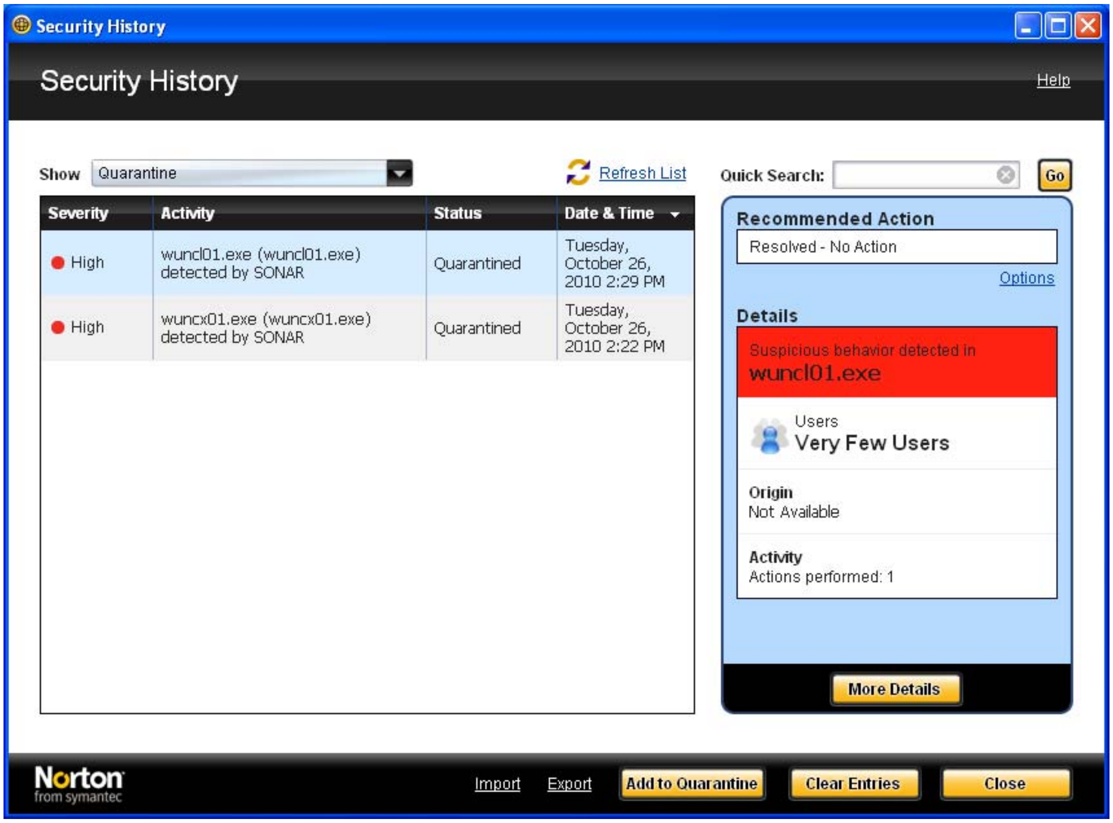


Insight Protection On
Antivirus On
Antispyware On
SONAR Protection On
Smart Firewall On
Intrusion Prevention On
Email Protection On
Identity Safe On
Browser Protection On
Safe Surfing On
Download Intelligence On

You have 78 days of subscription remaining

Figure 2: Main NIS 2010 Screen

2. This will bring up a list of quarantined files as shown in Figure 3.



Security History

Show: Quarantine

Severity	Activity	Status	Date & Time
● High	wuncl01.exe (wuncl01.exe) detected by SONAR	Quarantined	Tuesday, October 26, 2010 2:29 PM
● High	wuncx01.exe (wuncx01.exe) detected by SONAR	Quarantined	Tuesday, October 26, 2010 2:22 PM

Recommended Action: Resolved - No Action

Details

Suspicious behavior detected in wuncl01.exe

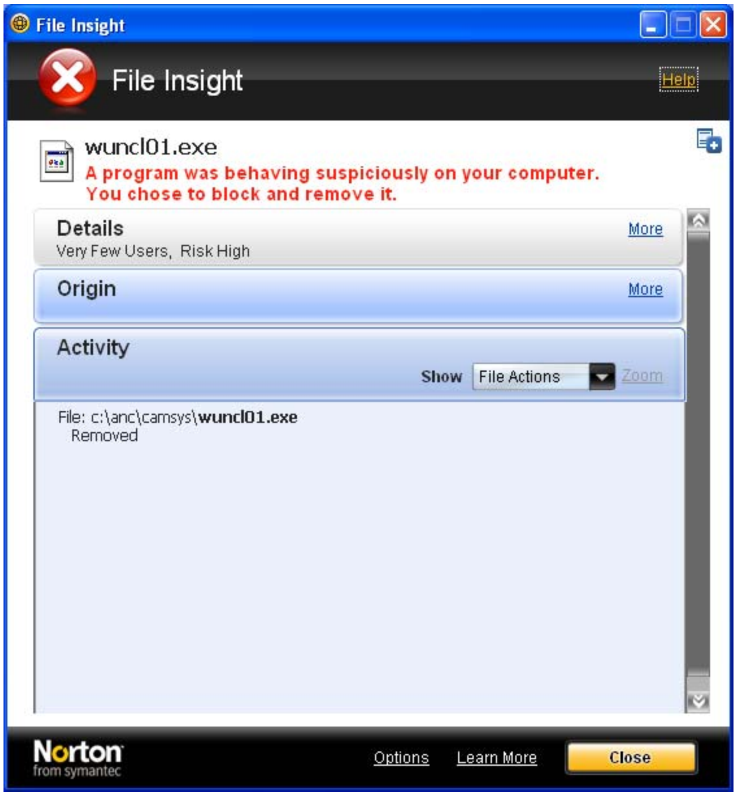
Users: Very Few Users

Origin: Not Available

Activity: Actions performed: 1

Figure 3: Quarantined Security History

3. Select the desired file (i.e., wuncl01.exe is selected above)
4. Click the **More Details** button on the right side of the dialog which will bring up the dialog shown in Figure 4.



wuncl01.exe

A program was behaving suspiciously on your computer.
You chose to block and remove it.

Details

Very Few Users, Risk High

Origin

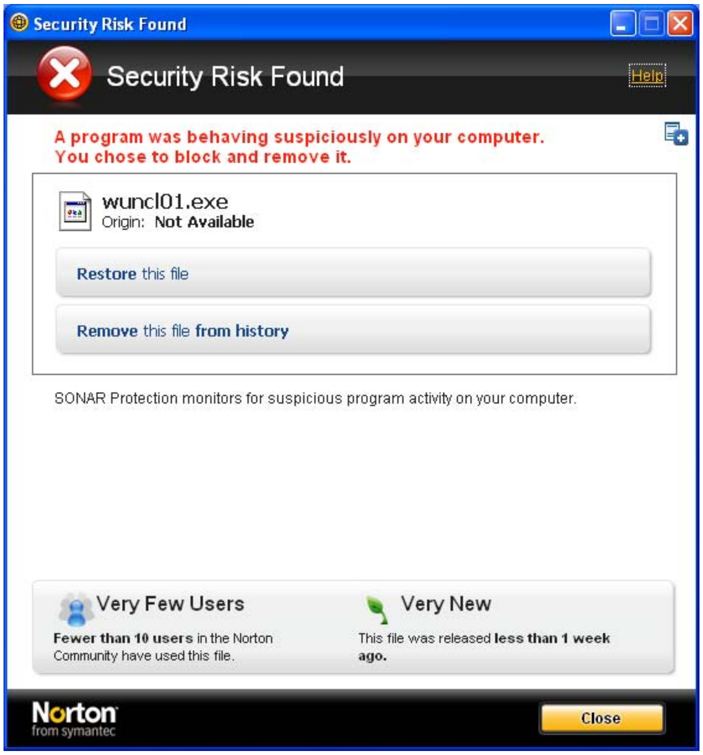
Activity

Show File Actions

File: c:\anc\camsys\wuncl01.exe
Removed

Figure 4: File Insight Dialog

5. Click the **Options** link at the bottom of the dialog which will bring up the dialog shown in Figure 5.



A program was behaving suspiciously on your computer.
You chose to block and remove it.

wuncl01.exe
Origin: Not Available

Restore this file

Remove this file from history

SONAR Protection monitors for suspicious program activity on your computer.

Very Few Users

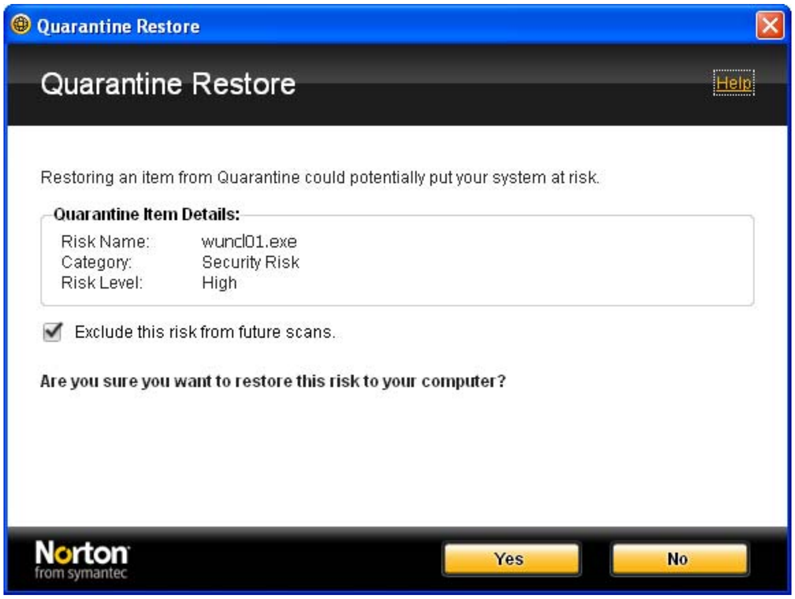
Fewer than 10 users in the Norton Community have used this file.

Very New

This file was released less than 1 week ago.

Figure 5: Security Risk Found Dialog

6. Click the **Restore this file** link which will bring up the dialog shown in Figure 6.



Restoring an item from Quarantine could potentially put your system at risk.

Quarantine Item Details:

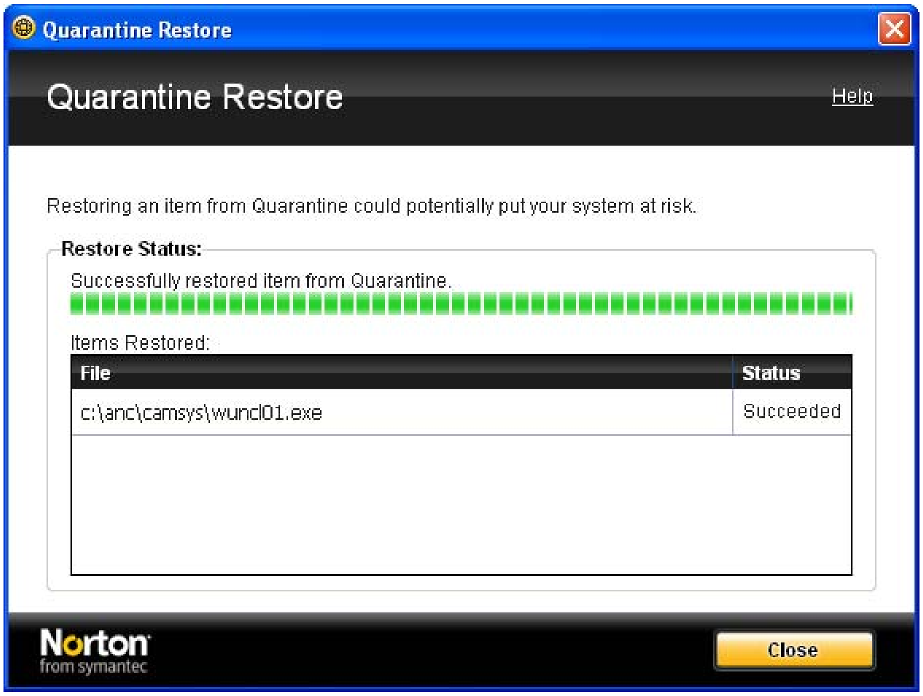
Risk Name:	wuncl01.exe
Category:	Security Risk
Risk Level:	High

☑ Exclude this risk from future scans.

Are you sure you want to restore this risk to your computer?

Figure 6: Quarantine Restore Dialog

7. In this dialog make sure the "Exclude this risk from future scans" check box is checked and then click the **Yes** button. The dialog shown in Figure 8 will show verification that the file has been restored. Click the **Close** button to end the process.
8. Exit out of the remainder of the NIS dialogs.



Restoring an item from Quarantine could potentially put your system at risk.

Restore Status:

Successfully restored item from Quarantine.

Items Restored:

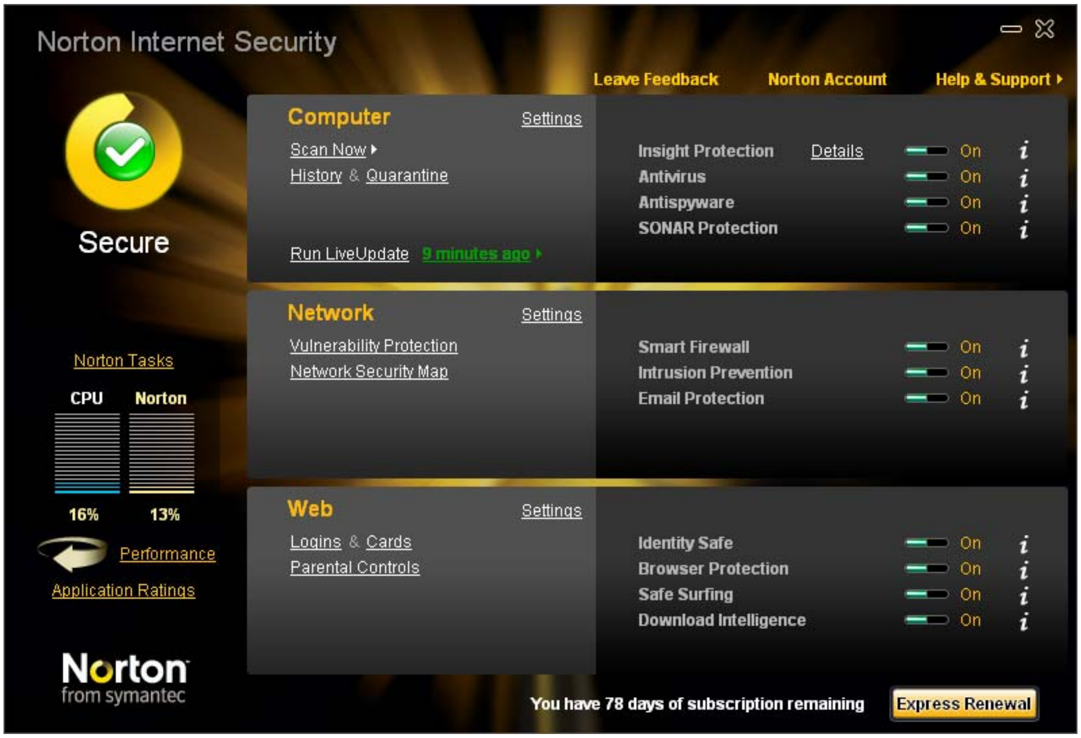
File	Status
c:\anc\camsys\wuncl01.exe	Succeeded

Figure 8: Quarantine Restore – Verification Dialog

Proactively Preventing a Security Application From Quarantining a File

The following steps show how to proactively prevent *Norton Internet Security (NIS) 2010* from deleting or quarantining CimPro or Option File Generator executables. Procedures for other security applications would be similar.

1. Open up NIS 2010 and click the **Settings** link in the “Computer” section (see Figure 9):

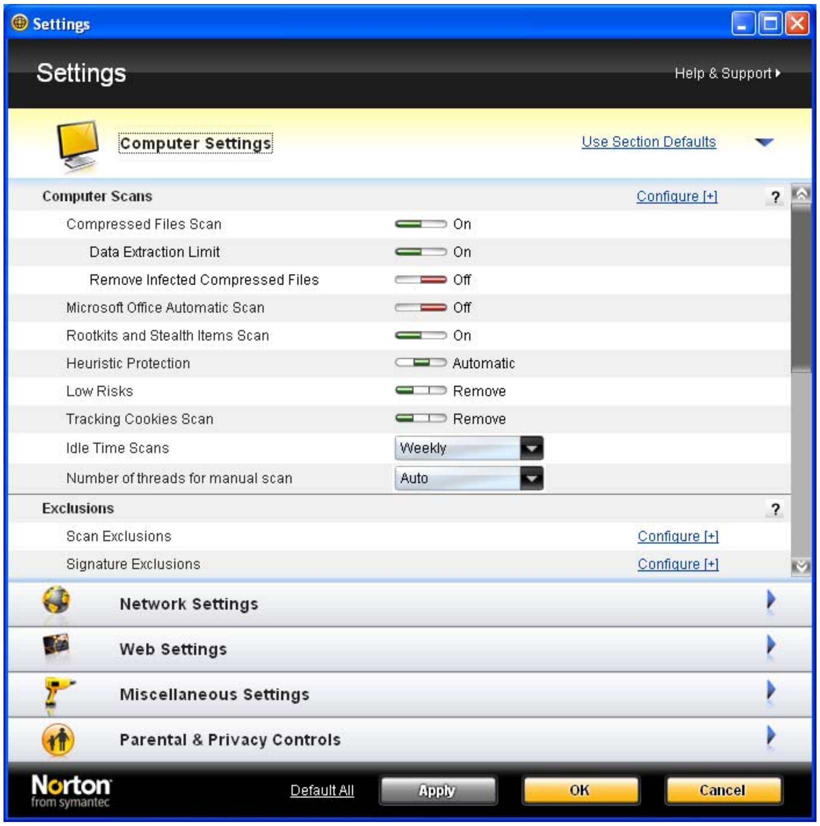


Insight Protection On
Antivirus On
Antispyware On
SONAR Protection On
Smart Firewall On
Intrusion Prevention On
Email Protection On
Identity Safe On
Browser Protection On
Safe Surfing On
Download Intelligence On

You have 78 days of subscription remaining

Figure 8: Main NIS Screen

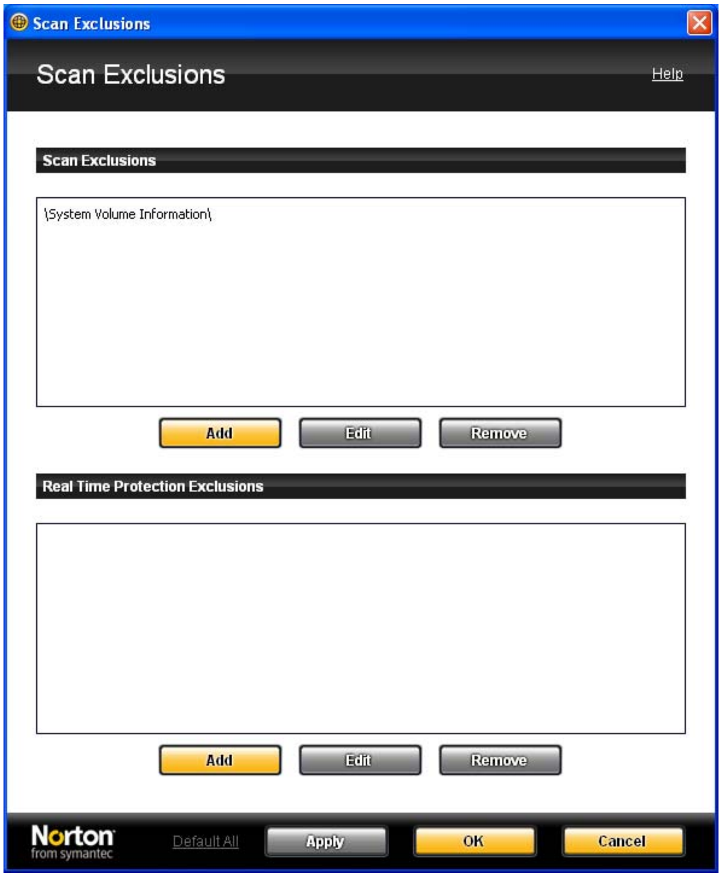
2. This should open up the setting screen as show in Figure 9 below.



Computer Scans	Configure [+]
Compressed Files Scan	On
Data Extraction Limit	On
Remove Infected Compressed Files	Off
Microsoft Office Automatic Scan	Off
Rootkits and Stealth Items Scan	On
Heuristic Protection	Automatic
Low Risks	Remove
Tracking Cookies Scan	Remove
Idle Time Scans	Weekly
Number of threads for manual scan	Auto
Exclusions	
Scan Exclusions	Configure [+]
Signature Exclusions	Configure [+]

Figure 9: Settings Dialog

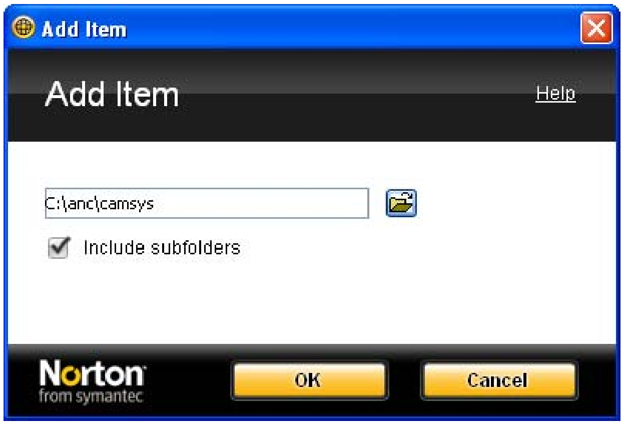
3. With the “Computer Scans” section expanded (as shown above), find the “Exclusions” sub-section and click on the **Configure [+]** link adjacent to **Scan Exclusions**. This will open the dialog shown in Figure 10.



\System Volume Information\

Figure 10: Scan Exclusions Dialog

4. In the “Real Time Protection Exclusions” section (the lower part of the dialog), click the **Add** button which will bring up the dialog shown in Figure 11.



C:\anc\camsys

☑ Include subfolders

Figure 11: Add Item Dialog

5. In this dialog either type or use the browse button to select the Camsys (or folder where the CimPro files are located) folder as shown above. Ensure the “Include subfolders” check box is selected. Click the **OK** button. This will return you the dialog shown in Figure 10 and will

now display the directory path you specified (e.g., C:\anc\camsys) in the list box in the lower portion of Figure 10. Click the **OK** button in Figure 10.

6. Exit out of all NIS 2010 dialogs and close NIS 2010.
7. This should prevent NIS 2010 from quarantining any CimPro related files.

As discussed, the above “scenarios” are based on Webroot Internet Security Complete 2011 and Norton Internet Security 2010. Other security applications may cause similar problems with the Austin N.C. suite of products. The steps to solve problems with other security applications should be similar. For assistance, please feel free to contact Austin N.C. at support@austinnc.com or check the website (www.austinnc.com)