Using Deep Freeze Enterprise with Sophos Antivirus

Author: Anthony Rizzoto
Supported by: Denise Erdman and Randy Brodhead

Last modified: November 12, 2008

Using Deep Freeze Enterprise with Sophos Antivirus

Introduction

This white paper explains the configuration for using Deep Freeze Enterprise with Sophos Antivirus. The content for this white paper has been provided by the Northampton Community College.

The process of updating virus definitions on workstations protected by Deep Freeze Enterprise involves three fundamental steps:

1. Rebooting the workstations into a *Thawed* state so the updates are kept upon restart
2. Updating the virus definitions
3. Shutting down or restarting the workstation into a *Frozen* state

This white paper provides technical information on how to perform these steps with Sophos Anti-Virus.

> ⚠️ *Deep Freeze is not marketed as an antivirus product. However, Deep Freeze will protect workstations from any virus—just restart the Frozen workstation and the virus is gone. Many viruses require a fundamental change to be made to the core files and only become active on restart. With Deep Freeze installed and activated, these viruses are deleted upon restart and therefore never become active.*
>
> *Ensure the BIOS is set to boot directly to the C: drive and that the BIOS is protected with a password; failure to do so can result in boot sector viruses being transferred to the hard disk drives via infected floppy disks.*

Creating a ThawSpace

ThawSpace is a virtual partition on a workstation that can be used to store programs, save files, or make permanent changes. All files stored in the ThawSpace are retained after a restart, even if the workstation is Frozen. To create a ThawSpace using the Configuration Administrator, complete the following steps:

1. In Deep Freeze, go to *Configuration>Drives*. In the *ThawSpace* pane, select *Create*.
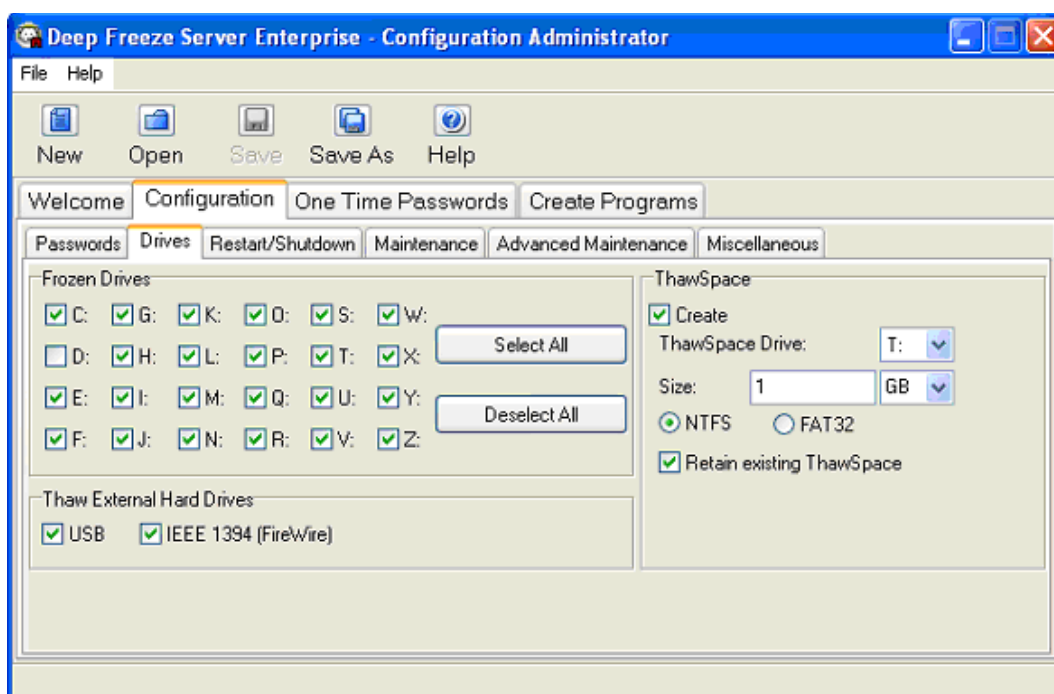
2. The *ThawSpace Drive* option is used to select the drive letter assigned to the ThawSpace. The default letter is *T:*, It can be changed to any available letter. The next available letter is used if the selected drive letter already exists on a workstation when Deep Freeze is installed.

3. The Size option reflects the size of the ThawSpace; the default size is 1 GB and the minimum size is 16MB. Workstations running Windows 95/98/Me can host a maximum ThawSpace of up to 2GB. Workstations running Windows 2000/XP/Vista can host a maximum ThawSpace of up to 1 TB when using the NTFS file system or 4GB when using the FAT32 file system. If the workstation does not have enough free space to accommodate the selected ThawSpace size, the size of the ThawSpace is adjusted downward to ensure proper operation of the workstation.

> ⚠️ *A dialog is always displayed asking if the ThawSpace should be retained or deleted during an Attended Uninstall, regardless of whether the Retain Existing ThawSpace option has been selected. This option is not displayed if the uninstall is performed through the Console.*

Configuring the Computer for Installing Sophos

The following options are used by the Northampton Community College. The following settings may not be applicable for all users:

1. Make sure *File and Printer Sharing* is selected in the *Windows Firewall* dialog of your operating system.
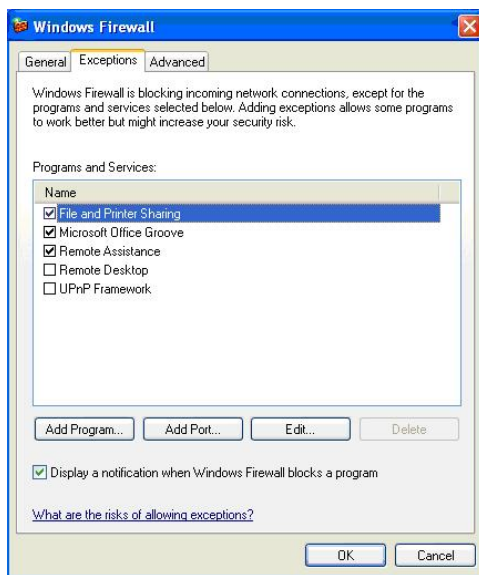

2. Open *Windows Explorer* and choose *Tools > Folder Options >View*. Clear the *Use simple file sharing* check box.

3. Click *Next* through the remainder of the tabs, setting the options required for your environment.

4. After the package is created, expand the *Package Node* under the *Software Distribution > Packages* node to display the Programs node. Select the *Programs* node and click on *New > Program* in the *Actions* to display the *New Program Wizard*.
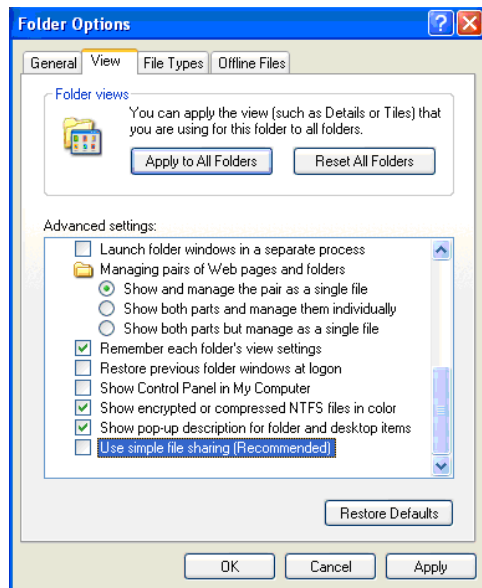
Installing and Configuring the Winbolic Link

Complete the following steps to install and configure the Winbolic Link:

1. Download the Winbolic Link from http://www.pearlmagik.com/winbolic/.

2. Install and run the Winbolic Link.

3. Highlight the drive letter that represents the ThawSpace. In this example, it is the *S:* drive.

4. In the *Name of link* field, enter *Sophos*.

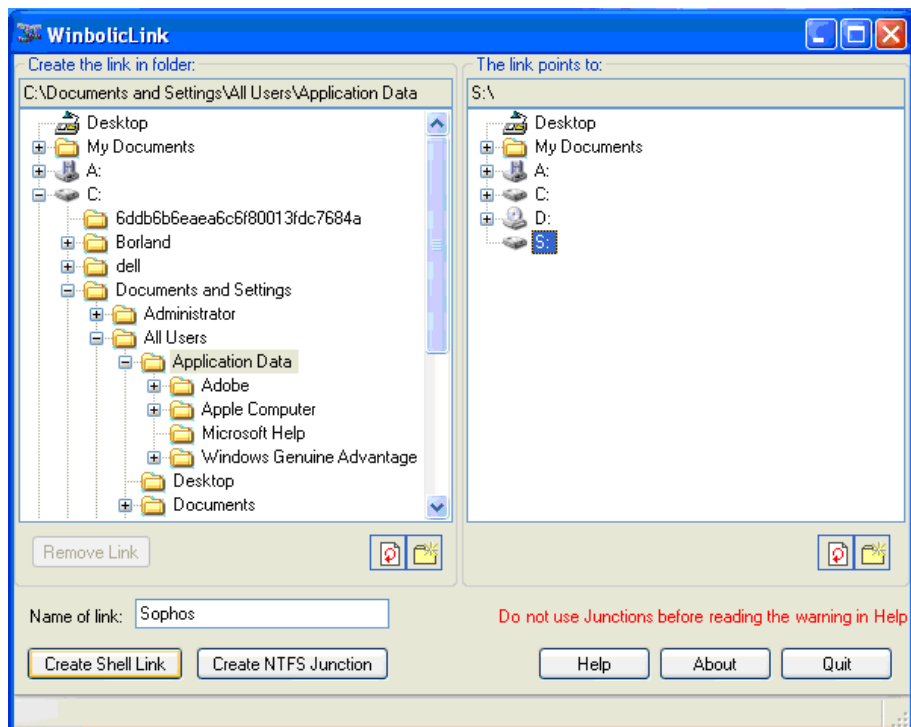5. Navigate to *C:\Program Files* and click *Create Shell Link*.
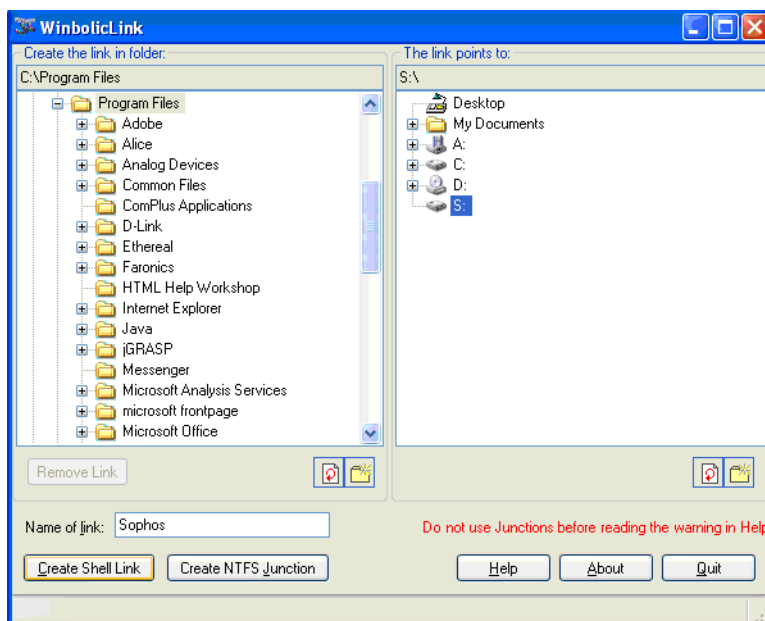
6.   If the Shell Link is successfully created, the following screen is displayed:
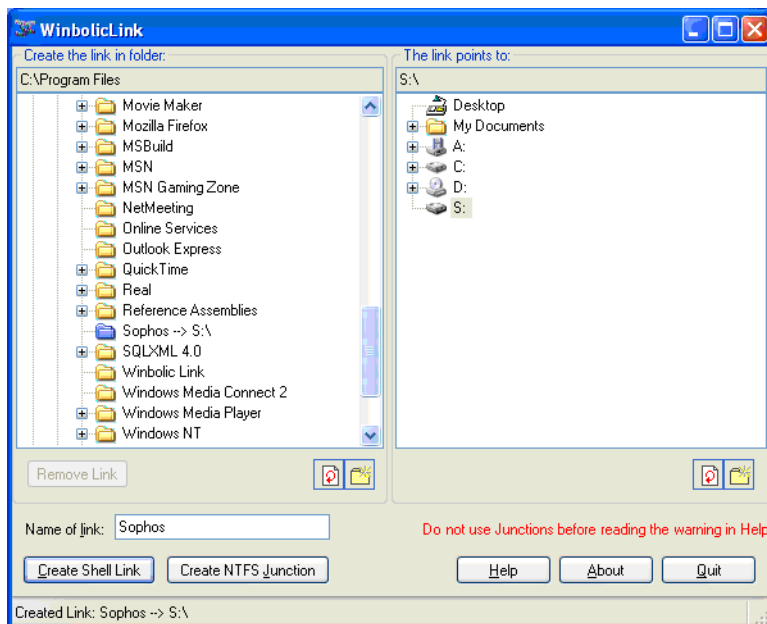

7.   The Sophos folder is now visible in the left pane. Unhide the *All Users\Application Data* folder. Clear the *Hidden* check box in the *Application Data Properties* dialog.
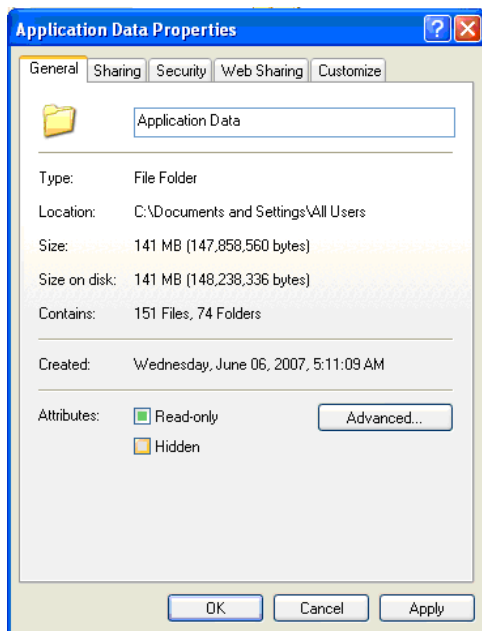

8.   Repeat steps 1 to 7 navigating to *C:\Documents and Settings\All Users\Application Data*.

9.   Highlight the *S:* drive (ThawSpace) and enter *Sophos* in the *Name of link* field.

10.   If the Shell Link is successfully created, the following screen is displayed.
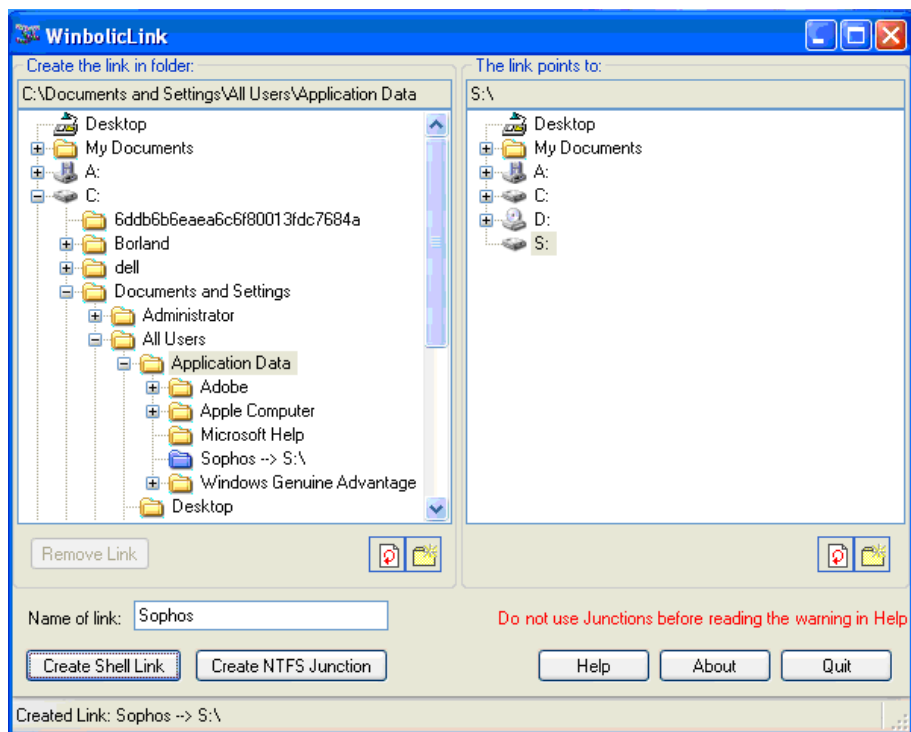
11.   Close the *Winbolic Link* and navigate to the newly created folders via Windows Explorer. The folders appear as a *Mounted Volume* as displayed in the following screens.
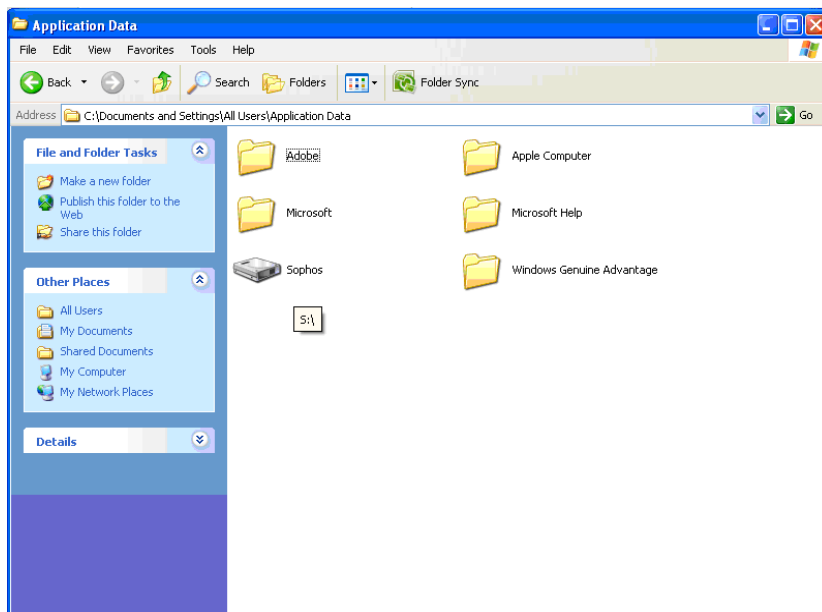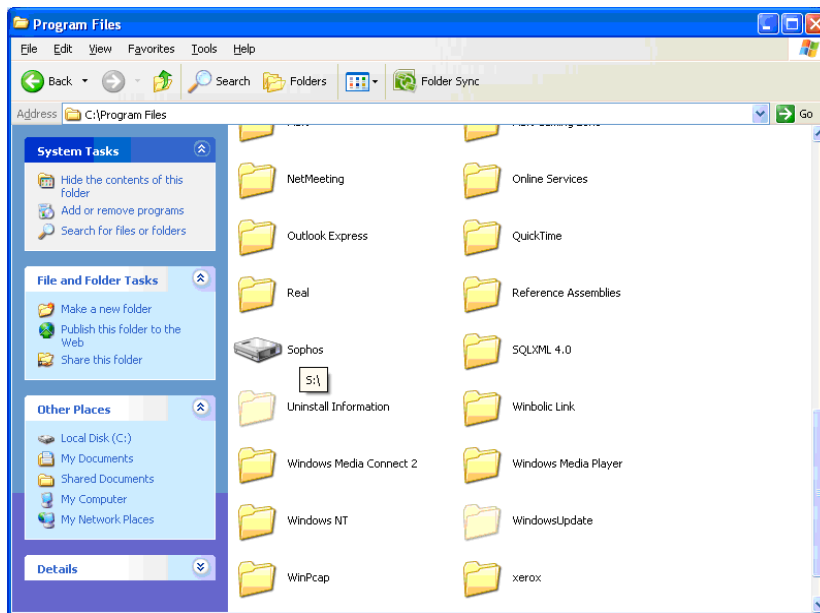
12. Install Sophos on the mounted volume *Sophos*. For security, you can remove all permissions from the *Sophos* folder. However, you must provide *Write Permissions* to the system user.