Faronics
DEEP FREEZE™
ABSOLUTE Workstation Integrity

Deep Freeze Enterprise - Panda BusinessSecure Antivirus

TECHNICAL WHITEPAPER

Last modified: June 13, 2005

Faronics
Toll Free Tel: 800-943-6422
Toll Free Fax: 800-943-6488
International Tel: +1 604-637-3333
International Fax: +1 604-637-8188

www.faronics.com

Faronics™

Introduction

The process of updating the 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 Signature File.
3. Shutting down or restarting the workstation into a *Frozen* state.

This white paper provides technical information on how to perform these steps with Panda's BusinesSecure Antivirus.

Deep Freeze is not marketed as an antivirus product. However, Deep Freeze protects 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.

Setting the Workstations to a Thawed state

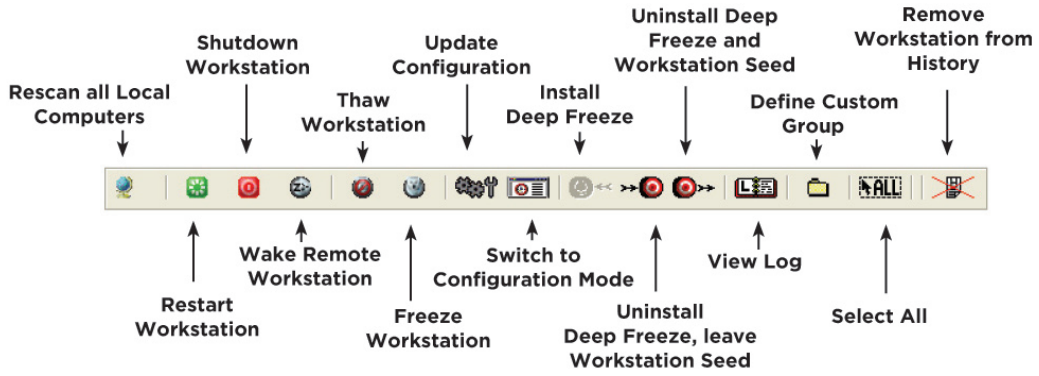
In order to make any permanent changes, the workstations protected by Deep Freeze have to be set in a *Thawed* state. Those permanent changes can include antivirus updates; therefore, the workstations must be rebooted into a *Thawed* state before applying these updates.

There are basically three ways to remotely set workstations into a *Thawed* state:

- By manually using the Deep Freeze Enterprise Console
- By setting up an Scheduled Maintenance Period
- By using the Command Line Control

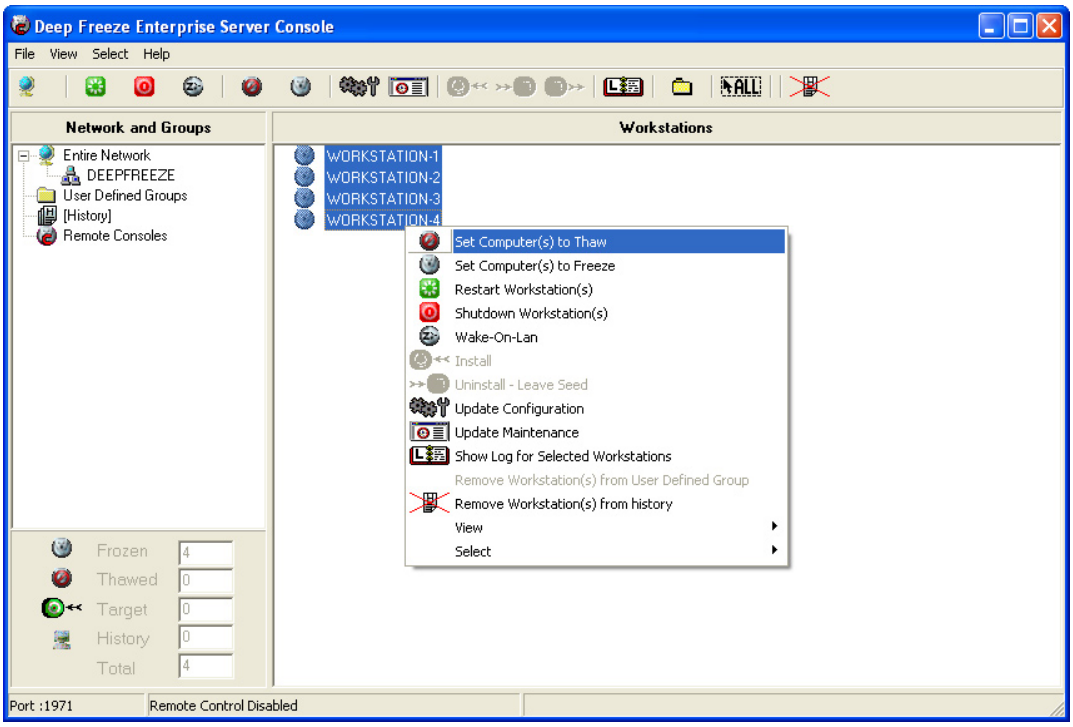
Manually Using the Deep Freeze Enterprise Console

The Enterprise Console contains a toolbar at the top of the screen that allows quick access to the functions of the Console.



To boot a workstation into the *Thawed* state, select the workstation and click the *Thaw Workstation* icon on the toolbar.

Alternatively, right-click and select the *Set Computer(s) to Thaw* option in the context menu.



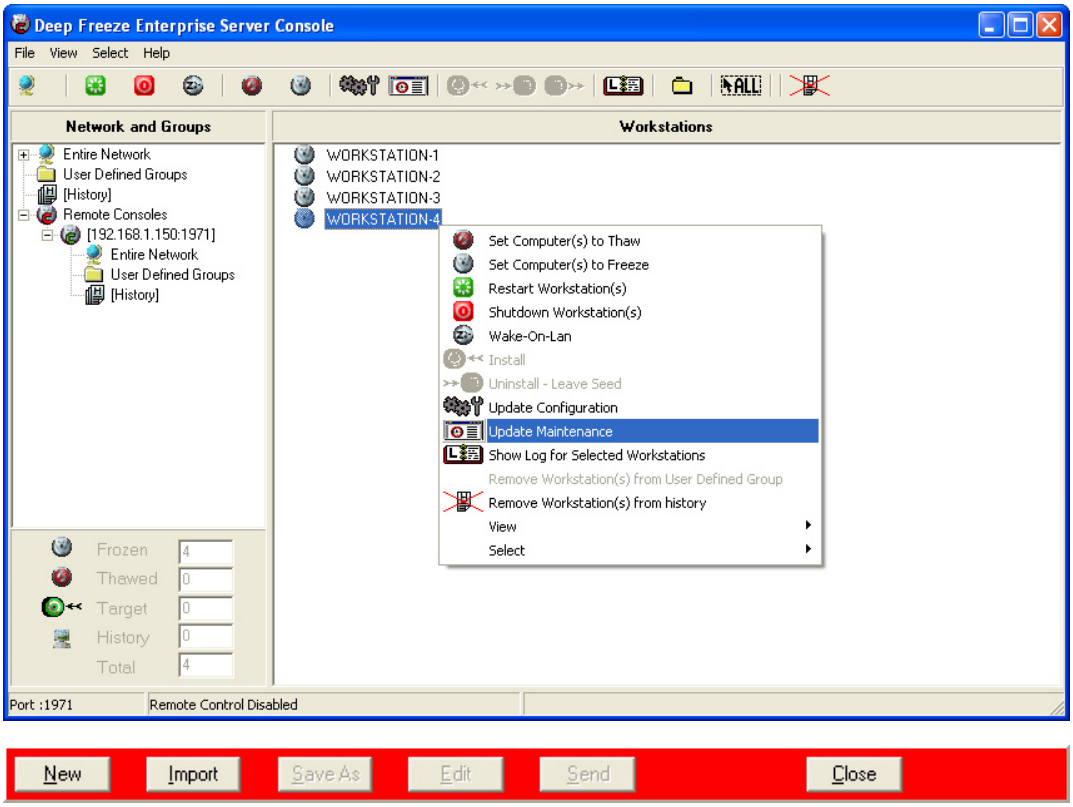
Click *OK* in the confirmation window.

The selected workstations restart in the *Thawed* state.

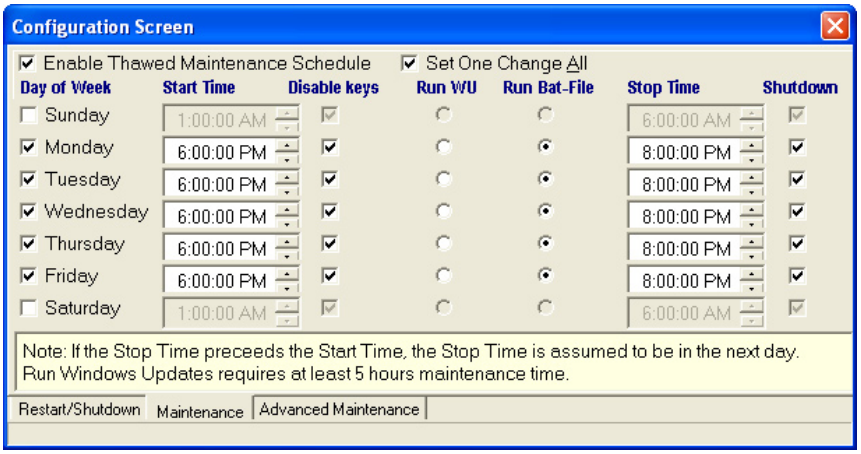
Setting up a Scheduled Maintenance Period

There are two ways to set up a Scheduled Maintenance Period. The first way is to set it up when configuring the Deep Freeze Enterprise installation files with the Configuration Administrator (best method for new deployments). The second way is to create or update the Maintenance Period using the Enterprise Console. Assuming you have already deployed Deep Freeze throughout your network, the following instructions elaborate on how to create/update the Maintenance Period with the Enterprise Console.

1. Open the Enterprise Console, select any workstation, and right-click on it.
2. Select *Update Maintenance Period*. A red bar appears at the bottom of the screen.



3. Click *New*. The *Configuration Screen* appears. It only contains the *Restart/Shutdown*, *Maintenance*, and *Advanced Maintenance* options.



4. Click the *Maintenance* tab and place a check in the *Enable Thawed Maintenance Schedule* check box. Also place a check beside each day you want the Maintenance Schedule to run.
5. Once the days are checked, set the Maintenance start time for each day in the *Start Time* column, and the end time in the *Stop Time* column.
6. It is recommended that the *Disable keys* option is checked so the keyboard and mouse are disabled while the workstations are in the *Thawed* state.

   It is also important to check the *Shutdown* box so Deep Freeze shuts the workstations down at the end of the Maintenance Period. Otherwise the workstations are restarted after the Maintenance Period is complete.
7. Close the *Configuration Screen*. A pop-up message appears requesting the administrator to select the workstations to send the new configuration to.
8. Select the workstations to be updated and click *Send*.

   This action updates all the selected workstations' configuration on the fly. This means the workstations don't have to be in the *Thawed* state for the configuration updates to take place.

Controlling Deep Freeze Through the Command Line Control - DFC

The Deep Freeze *Command Line Control* (*DFC*) offers network administrators increased flexibility in managing Deep Freeze workstations. DFC works in combination with third party enterprise management tools and/or central management solutions. This combination allows administrators to update workstations on the fly and on demand.

It is important to note that DFC is not a stand-alone application. DFC integrates seamlessly with any solution that can run script files, including standard run-once login scripts.

The DFC executable is installed in the same directory as the Configuration Administrator:
C:\Program Files\Faronics\Deep Freeze Enterprise\Dfc.exe

DFC commands require a password with command line rights. One Time Passwords (OTPs) cannot be used.

DFC Boot Control

Syntax	Description
`DFC password /BOOTTHAWED`	Restarts workstation into a Thawed state; only works on Frozen workstations.
`DFC password /THAWNEXTBOOT`	Sets up workstation to restart Thawed the next time it restarts; only works on Frozen workstations and does not force workstation to restart.
`DFC password /BOOTFROZEN`	Restarts workstation into a Frozen state; only works on Thawed workstations.
`DFC password /FREEZENEXTBOOT`	Sets up workstation to restart Frozen the next time it restarts; only works on Thawed workstations and does not force workstation to restart.

DFC Status Query

Syntax	Description
`DFC get /ISFROZEN`	Queries workstation if it is Frozen. Returns 0 if Thawed. Returns 1 if Frozen.

Configuration Update

Syntax	Description
`DFC password /CFG=[path] depfrz.rdx`	Replaces Deep Freeze configuration information. Works on Thawed or Frozen workstations. Password changes are effective immediately. Other changes require restart.

Example Batch File

Below is a sample batch file that can be modified for use with any antivirus software that supports updating through a command line.

```
@ECHO OFF
\\SERVER\SHARE\FOLDER\DFC.EXE get /isfrozen
IF ERRORLEVEL 1 GOTO FROZEN
IF ERRORLEVEL 0 GOTO THAWED
ECHO Errors where encountered running the command line control on this
workstation.
:FROZEN
\\SERVER\SHARE\FOLDER\DFC.EXE password /bootthawed
GOTO END
:THAWED
REM ************************************************************************
REM * Insert the command to update the antivirus software here.  *
REM ************************************************************************
\\SERVER\SHARE\FOLDER\DFC.EXE password /freezenextboot
REM Send commands to reboot the system.
REM For Windows 95/98/ME
RUNDLL32 SHELL32.DLL,SHExitWindowsEx 2
REM For Windows 2000 (may need to be called 2x)
RUNDLL32 USER32.DLL,ExitWindowsEx 2
RUNDLL32 USER32.DLL,ExitWindowsEx 2
REM For Windows XP
SHUTDOWN -s -t 01
GOTO END
:END
```

Updating the Virus Signature File

This document provides three different ways to approach Virus Signature File updates for the Panda BusinesSecure Antivirus.

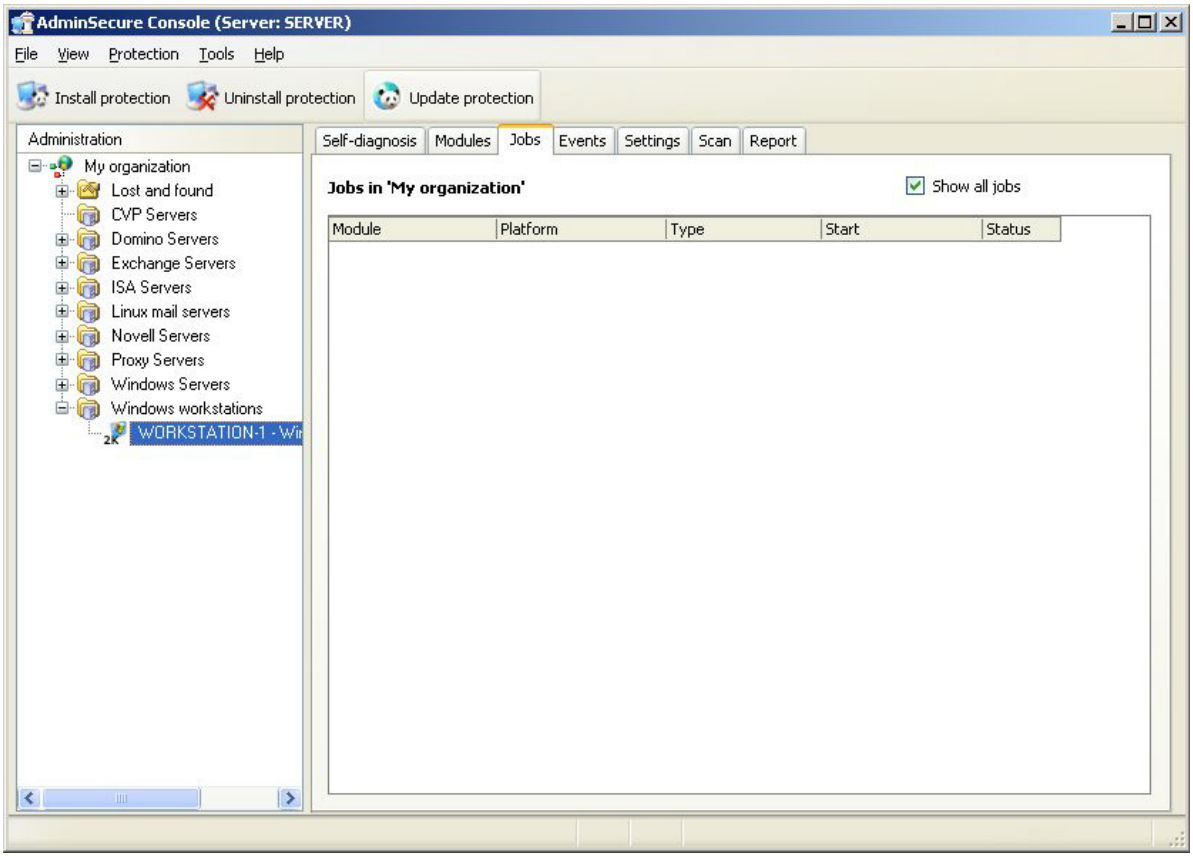
1) Do Nothing

The Virus Signature File keeps getting updated every time the workstations are restarted, but the changes are lost upon reboots. On fast switched networks, this has a negligible impact on the boot-up time.

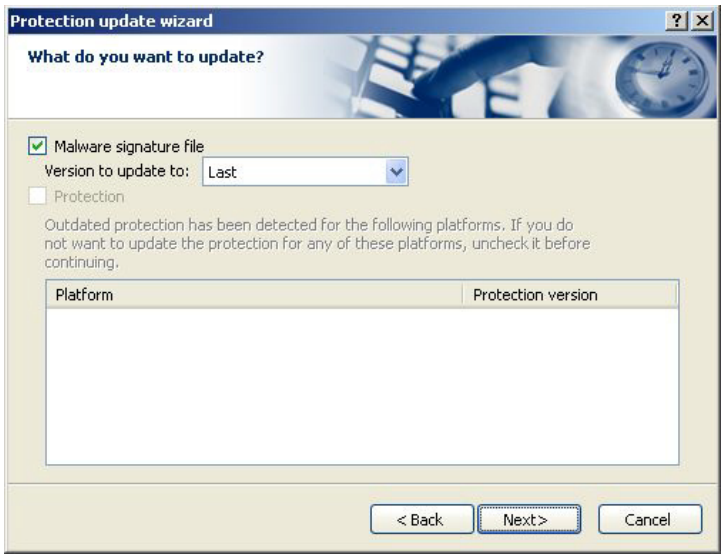
The workstations then have the latest Signature File at all times; the only down side of this method is that, with time, the Signature File keeps growing bigger. Therefore, it is recommended to schedule a *Thawed* Maintenance Period at least twice a year to make the updates permanent.

2) Manually Update the New Virus Definitions.

1. Using the Enterprise Console, set the workstations to reboot into the *Thawed* state. Once the computers are back on, open the *Panda AdminSecure Console* on your antivirus server.
2. Expand the Windows Workstations by clicking on the plus (+) sign, then select the Workstations you want to update.
3. Click *Update Protection,* located at the top of the screen



The *Protection Update Wizard* appears.



4. After clicking *Next*, a screen appears, asking what Virus Signature File you want to use to update the workstations.

   By default this option is set to *Last*.

5. Click *Next*. Then click *Finish* on the next screen.

6. The new job is created (to verify job, click on *Jobs* tab) and the updating process begins.

3) Mounted Hard Disks

This method does not involve setting the workstations into a Thawed state before making the updates but rather mounting *Thawed* partitions so the virus definition updates can take place while the workstations are in the *Frozen* state.

Windows 2000 introduced the ability to mount a hard disk drive or partition to an empty folder on an existing hard disk drive instead of assigning a drive letter to that partition. This allows a drive to be accessed using a standard Windows path, as opposed to the traditional drive letter. This allows users to expand the storage available in a specific directory by adding another hard disk, without having to change the directory structure of the hard disk or the location of saved data.

For example, if a user's workstation contains a large number of documents in the user profiles and the hard disk drive is filled, an administrator can add a second hard disk and move the user's data to that drive. The drive can be mounted with the user's data in the same location after the data has been moved, making the process transparent to the user.

Steps to Ensure a Successful Deployment

Ensure that the Windows 2000/XP system drive is using the NTFS file system. The ability to mount partitions as paths is not available with the FAT32 file system.

Ensure that adequate free space is available on the workstation's hard disk drive to accommodate the newly created partitions. The complete workstation image should be evaluated to determine what folders need to be recreated as drives on the workstation to allow the applications to function as required. Any application that is mounted as a drive can be damaged, uninstalled, or changed because the files located on the secondary partition are not protected by Deep Freeze.

Only directories that require being *Thawed* should be opened and only enough space for the applications to run properly should be freed. Leaving a large amount of free data space open could allow users to load files into the workstation or install applications that are unauthorized or unwanted. Steps can be taken to ensure that only administrators or authorized personnel can have access to modify the files contained in these partitions.

A combination of proper application of the Windows security policy and the use of NTFS file access rights can effectively protect the Thawed directory. For more information on Windows 2000/XP system and security policies, refer to the link below:

How to maintain Windows security: http://www.microsoft.com/windows/security/

Refer to your imaging solution documentation for information regarding imaging with mounted drives. Workstations should be imaged either in RAW format or in a sector-by-sector mode. (For example: using the -ID switch in Symantec Ghost).

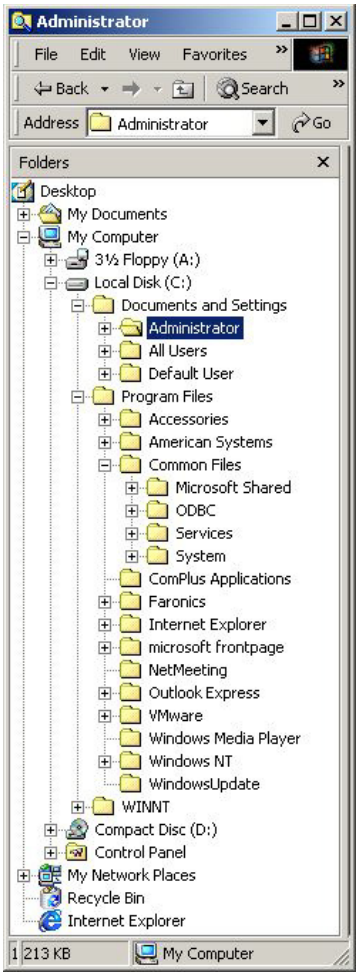
After all concerns have been addressed, the folders that need replacement are documented, and the size requirements of the partitions have been determined, a new master image can be created or an existing image can be modified.

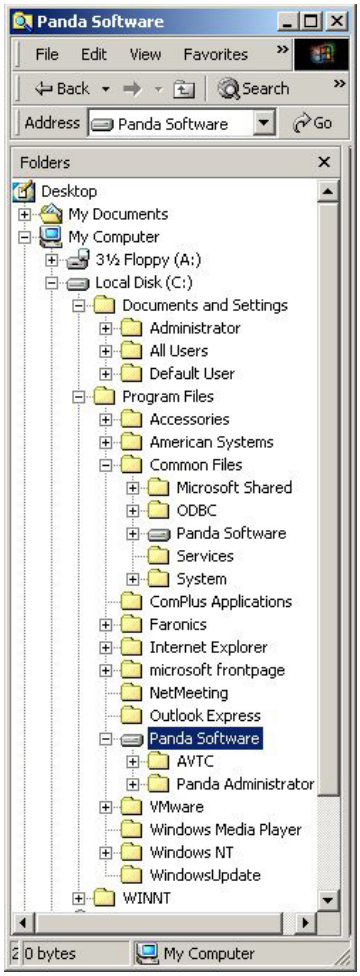
Preparing the Windows 2000 / XP Workstations for BusinesSecure Antivirus Installation on Mounted Partitions

Some Panda's BusinesSecure Antivirus scan engine updates make modifications to the Windows Registry and, since this is protected by Deep Freeze, we strongly recommend that the following method be used just for virus definitions updates.

The following steps detail the procedure for installing Panda's BusinesSecure Antivirus client software on the workstations in a manner that allows automatic updates to proceed correctly.

Below are before and after screen shots of the installation of Panda BusinesSecure Antivirus using the default options:





The installation of Panda BusinesSecure Antivirus creates two new directories on the workstation:

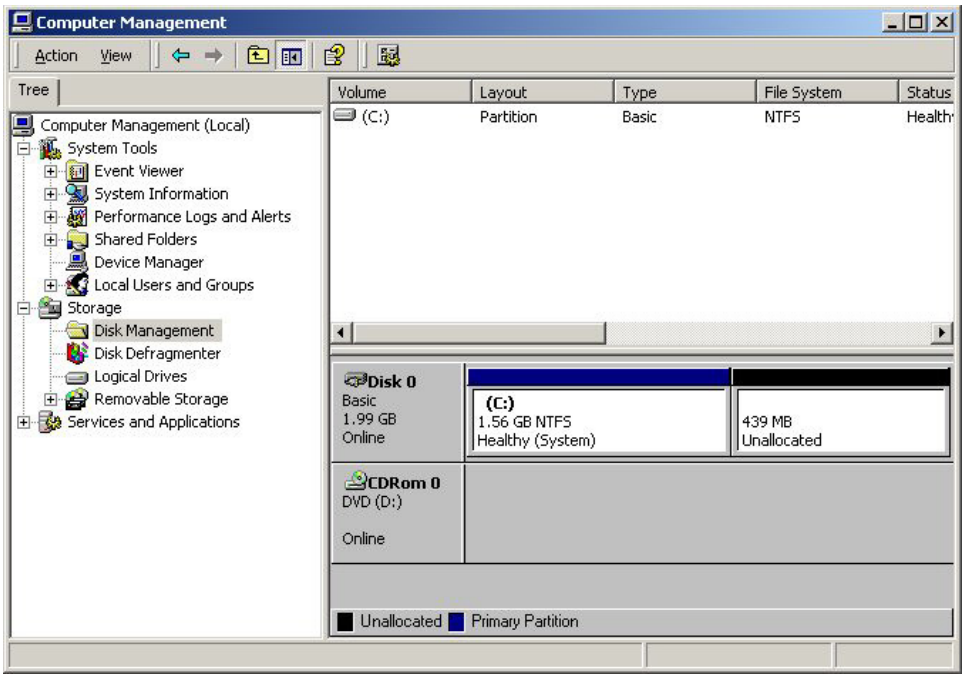
C:\Program Files\Panda Software
C:\Program Files\Common Files\Panda Software

To ensure that the application has the ability to apply full updates to the virus definitions and the scanning engine, the new folders must be recreated as partitions.

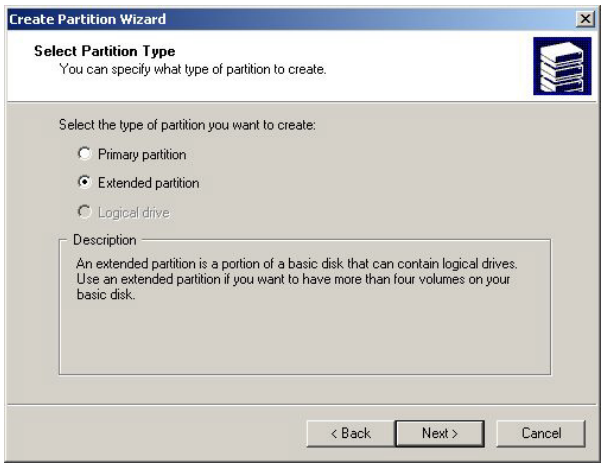
Partition #	Name of Folder the Partition Replaces	Drive Size
1	C:\Program Files\Panda Software	100MB
2	C:\Program Files\Common Files\Panda Software	50MB

The size of the partitions has been selected to allow Panda BusinesSecure enough room to enable it to update the files it uses. Because these are going to be moved to new drives, the size limit of 100MB and 50MB respectively are always enforced, regardless of how much free space remains on the C:\ drive.

The first step in creating the additional partitions required is to create an extended partition to store the additional partitions using the *Disk Management* feature of the Computer Management console. When the console is opened, the following image appears:



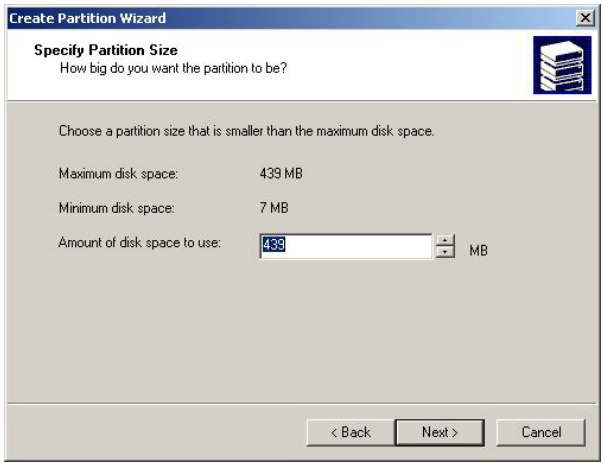
To create an extended partition, right-click on the unallocated space shown in the bottom of the screen and select *Create Partition*. The following Wizard appears to assist in creating the partition.



The first screen of the wizard prompts for the type of partition required.

Extended partition should be checked because we are creating multiple small partitions and do not want to limit the number of partitions that can be created.

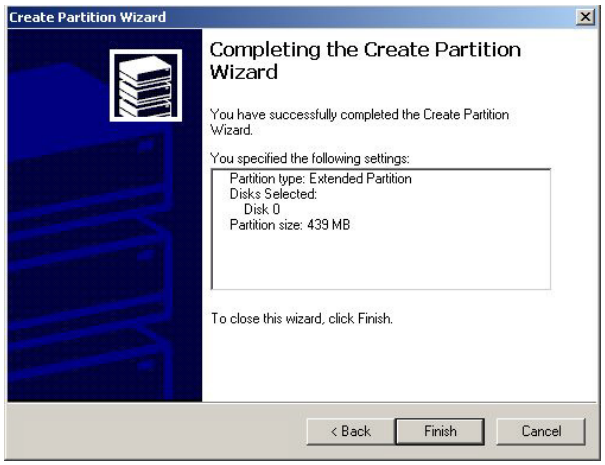
Click *Next*.



The next screen prompts for the size of partition to be created.

It is recommended that you configure all the disk space remaining on the drive at this time.

Click *Next*.

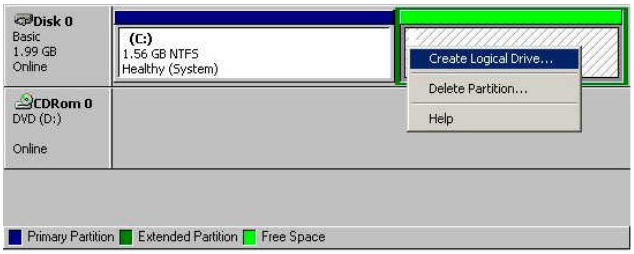


The last screen shows confirmation of the partition type and size once the partition has been successfully created.

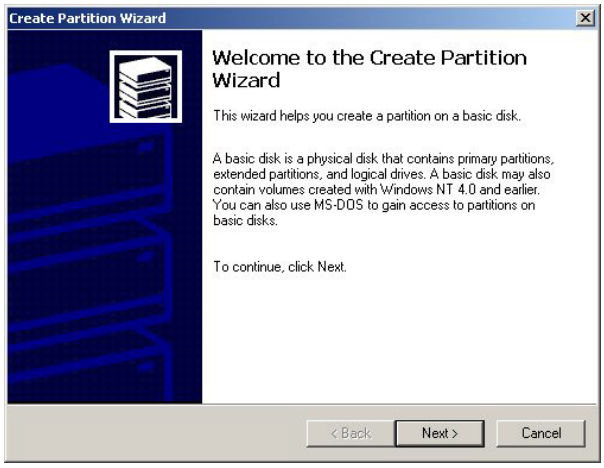
Click *Finish*.

Once the extended partition is created, the logical drives can be created and mounted on the empty folders that need to be created.

This can be done by right-clicking on the free space now present on the drive (as shown below) and selecting *Create Logical Drive*.

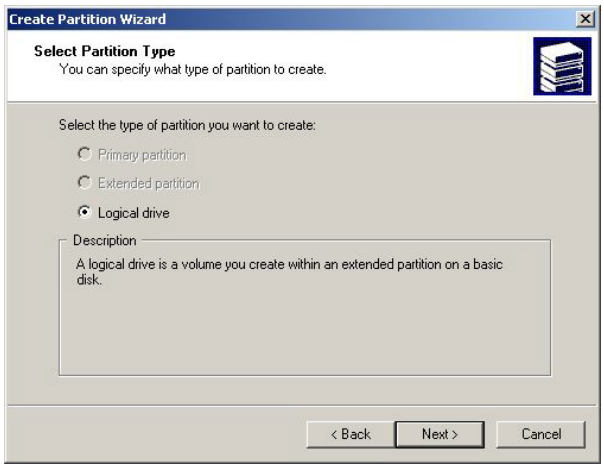


The following wizard appears. This wizard allows you to set the size and folder name of the partition.



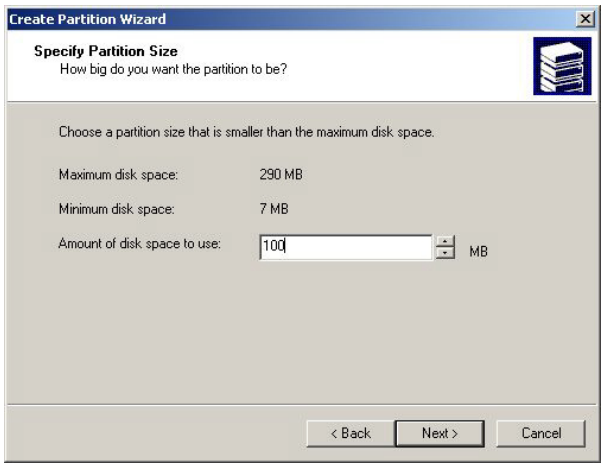
This is the first introduction screen.

Click *Next*.



The second screen should have the option to create a *Logical drive* selected as a default.

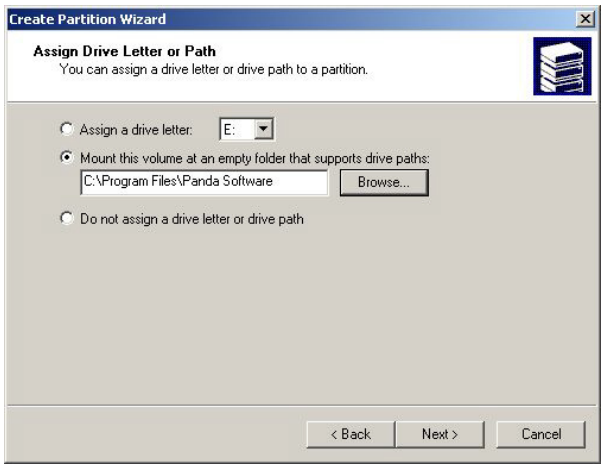
Click *Next*.



The next screen prompts for the size of partition to be created.

Specify enough size to allow for updates to the application to be applied, but not enough for the space to be used to install additional applications. In this example, a 100MB partition size is selected.

Click *Next*.

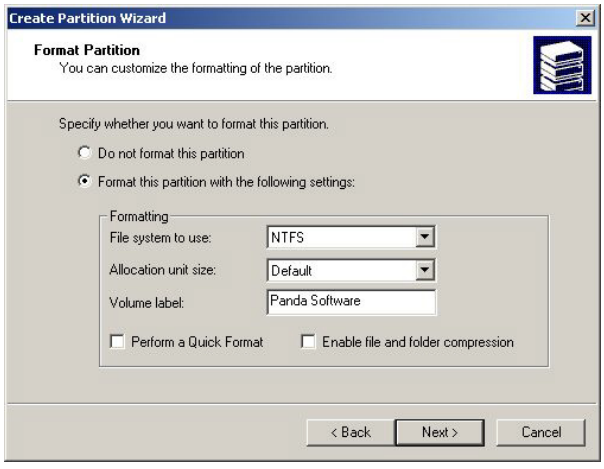


The next screen prompts for the drive letter or path of the new partition.

The option *Mount this volume at an empty folder that supports drive paths* should be selected.

The path the drive will be mounted to should be entered in the text field. In this case, the path is *C:\Program Files\Panda Software*.

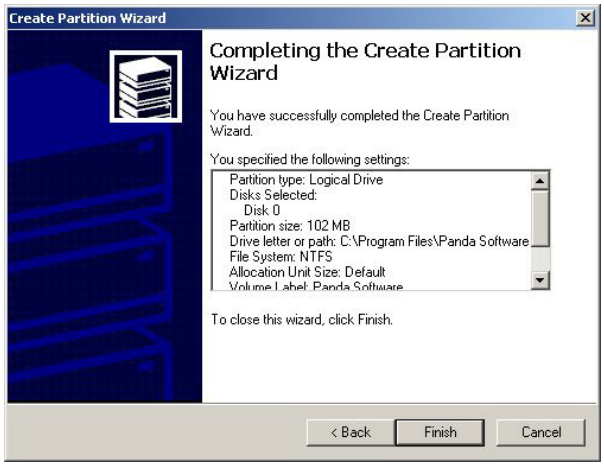
Click *Next*.



The next screen is used to specify the formatting options for the partition.

It is recommended to format the partition using the NTFS file system and to include a descriptive volume label to distinguish the partition from others that may exist.

Click *Next*.

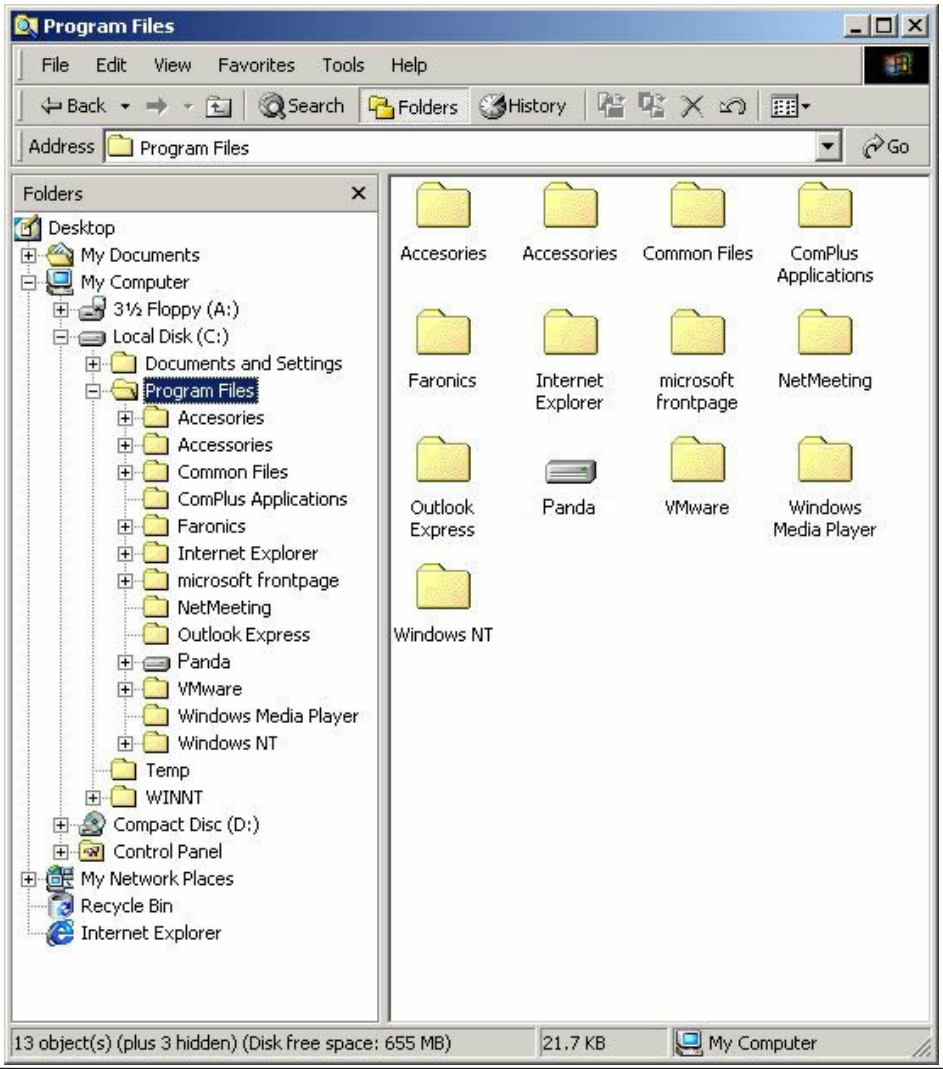


The last screen shows confirmation of the selected options once the partition has been successfully created.

Click *Finish* to exit the wizard and begin formatting the new drive.

The previous steps should be repeated for each directory that the application requires to be Thawed, substituting the appropriate names and volume sizes for each drive. After a drive has been successfully mounted as a path, a new icon appears that represents the folder as a hard disk drive.

In the example below, the Panda Software folder is displayed as a small hard disk drive.



After all the appropriate drives have been created, Panda BusinesSecure Antivirus should be installed normally using the manufacturer's installation program.

Refer to your imaging solution documentation for information regarding imaging with mounted drives. Workstations should be imaged either in RAW format or in a sector by sector mode. (For example: using the -ID switch in Symantec Ghost).