

FARONICS

DEEPFREEZE™

ABSOLUTE Workstation Integrity



Deep Freeze Enterprise - Trend Micro OfficeScan

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

©1999-2006 Faronics Corporation. All rights reserved.
Deep Freeze, Anti-Executable, and WINSelect are trademarks
and/or registered trademarks of Faronics Corporation.
All other company and product names are trademarks of their respective owners.

Introduction

The process of updating virus pattern files 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 pattern file
3. Shutting down or restarting the workstation into a Frozen state

This white paper provides technical information on how to approach these steps with Trend Micro OfficeScan.



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 will be 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

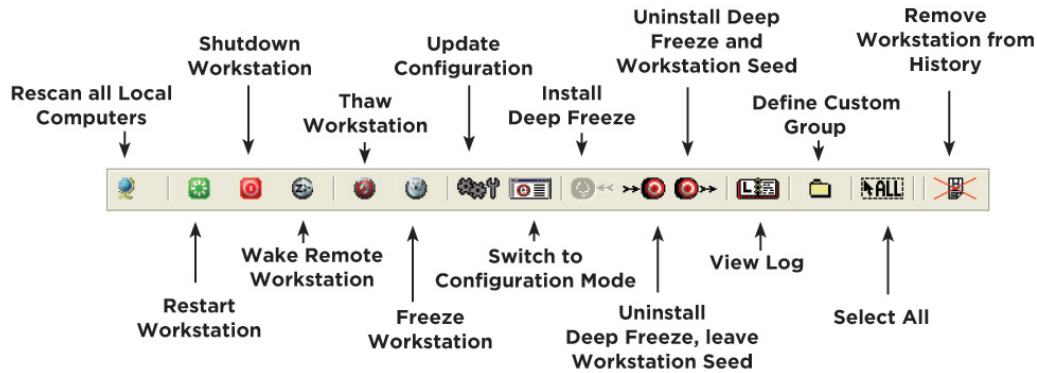
In order to make any permanent changes, the workstations protected by Deep Freeze have to be set into a *Thawed* state. Those permanent changes include antivirus updates; therefore, the workstations must be rebooted into a *Thawed* state before applying these updates.

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

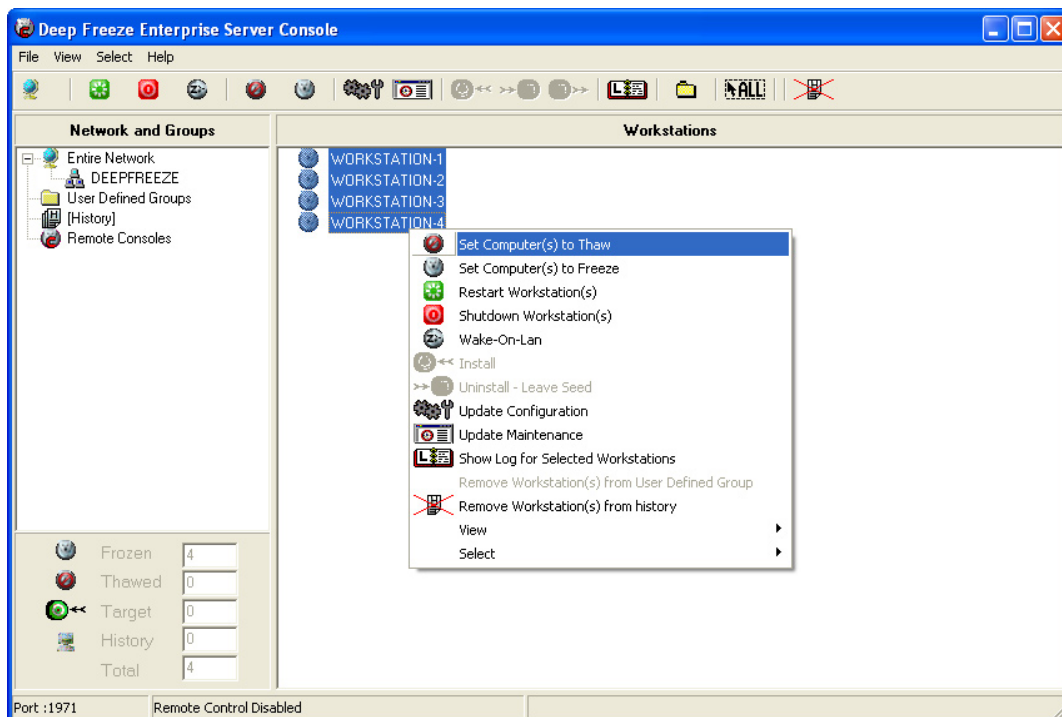
Manually Using the Deep Freeze Enterprise Console

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



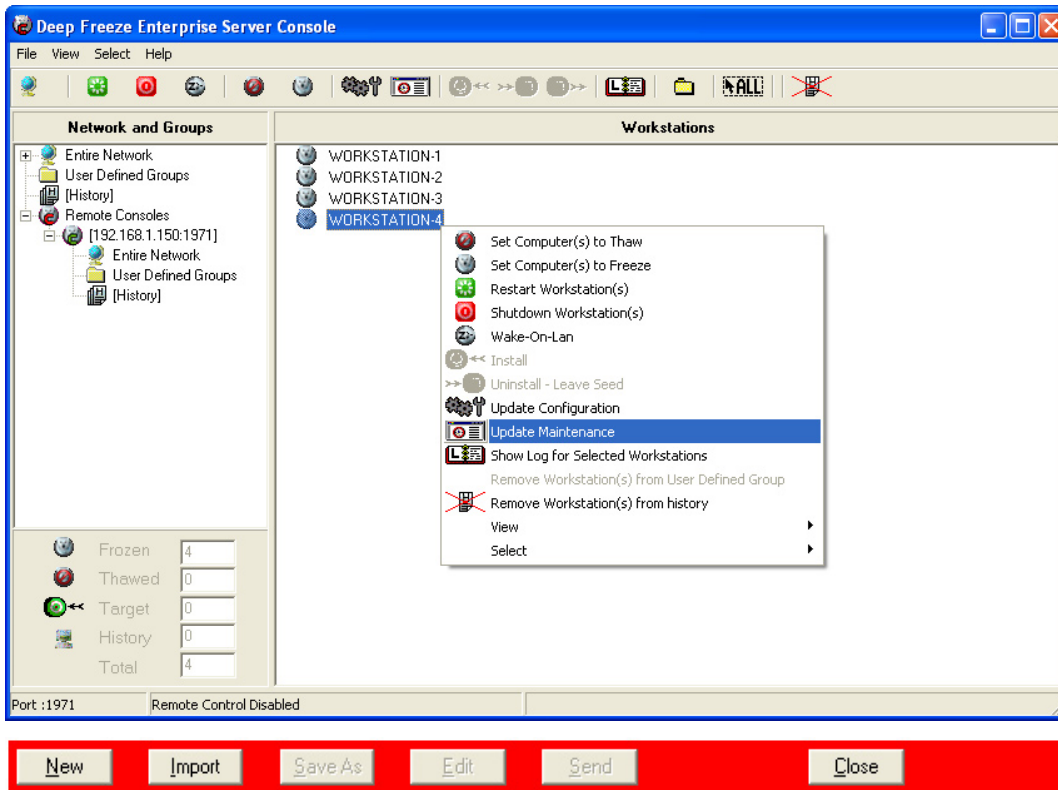
Click *OK* in the confirmation window.

The selected workstations restart in the *Thawed* state.

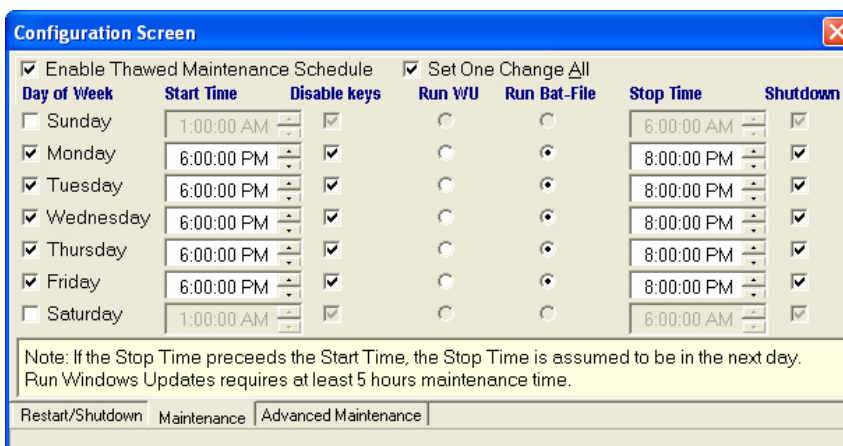
Setting up a Scheduled Maintenance Period

There are two ways to set up a Scheduled Maintenance Period. One is to set it up when configuring the Deep Freeze Enterprise installation files with the Configuration Administrator (best method for new deployments). The other way is to create or update the Maintenance Period using the Enterprise Console. Assuming Deep Freeze is already deployed 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*. 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.

Also, it is 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 that 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. 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. 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 Definitions

This document provides six different ways to approach virus patterns updates for the Trend Micro OfficeScan.

1) Do Nothing

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

The workstations have the latest pattern at all times; the only down side of this method is that, with time, the patterns will keep 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 Patterns

Using the Enterprise Console, set the workstations to reboot into the *Thawed* state. Once the computers are back on, access the OfficeScan Management Console.

On the left menu, click *Updates*, select *Client Deployment > Manual Deployment*. Click *Notify*.

The screenshot shows the Trend Micro OfficeScan Management Console interface. The left sidebar contains a navigation menu with the following items: Scan Now, Update Now, Cleanup Now, Summary, Outbreak Prevention, Virus Outbreak Monitor, Clients, Cisco NAC, Administration, Updates (expanded), Server Update, Client Deployment, Update Source, Automatic Deployment, Manual Deployment, Update Agent, Rollback, Logs, and Tools. The main content area is titled "Manual Deployment" and includes the following text: "You can manually update all components to clients. Components will be updated according to the list below." Below this text is a table with the following data:

Component	Version Available	Last Update
Antivirus		
Virus pattern	2.400.00	2/10/2005 13:48:04
Client program for Windows NT/2000/XP/Server 2003	6.5	1/21/2005 13:07:26
Scan engine for Windows NT/2000/XP/Server 2003	7.500.1001	2/10/2005 13:32:39
Client program for Windows 95/98/Me	6.5	1/21/2005 13:07:26
Scan engine for Windows 95/98/Me	7.500.1001	2/10/2005 13:48:13
Server program	6.5	1/21/2005 13:07:26
Additional Threat pattern	0.227.00	2/10/2005 13:33:06
Damage Cleanup Service		
Damage Cleanup template	515	2/10/2005 13:32:49
Damage Cleanup engine	3.9.1020	2/10/2005 13:32:57
Cisco NAC		
Cisco Trust Agent	1.0.53	1/21/2005 13:07:26

Below the table, there is an "Update Target" section with the following options:

- Select clients with out-of-date components
 - Include roaming client(s)
- Manually select clients

Click **Notify** to inform target clients to download the latest components.

A "Notify" button is located at the bottom of the page.

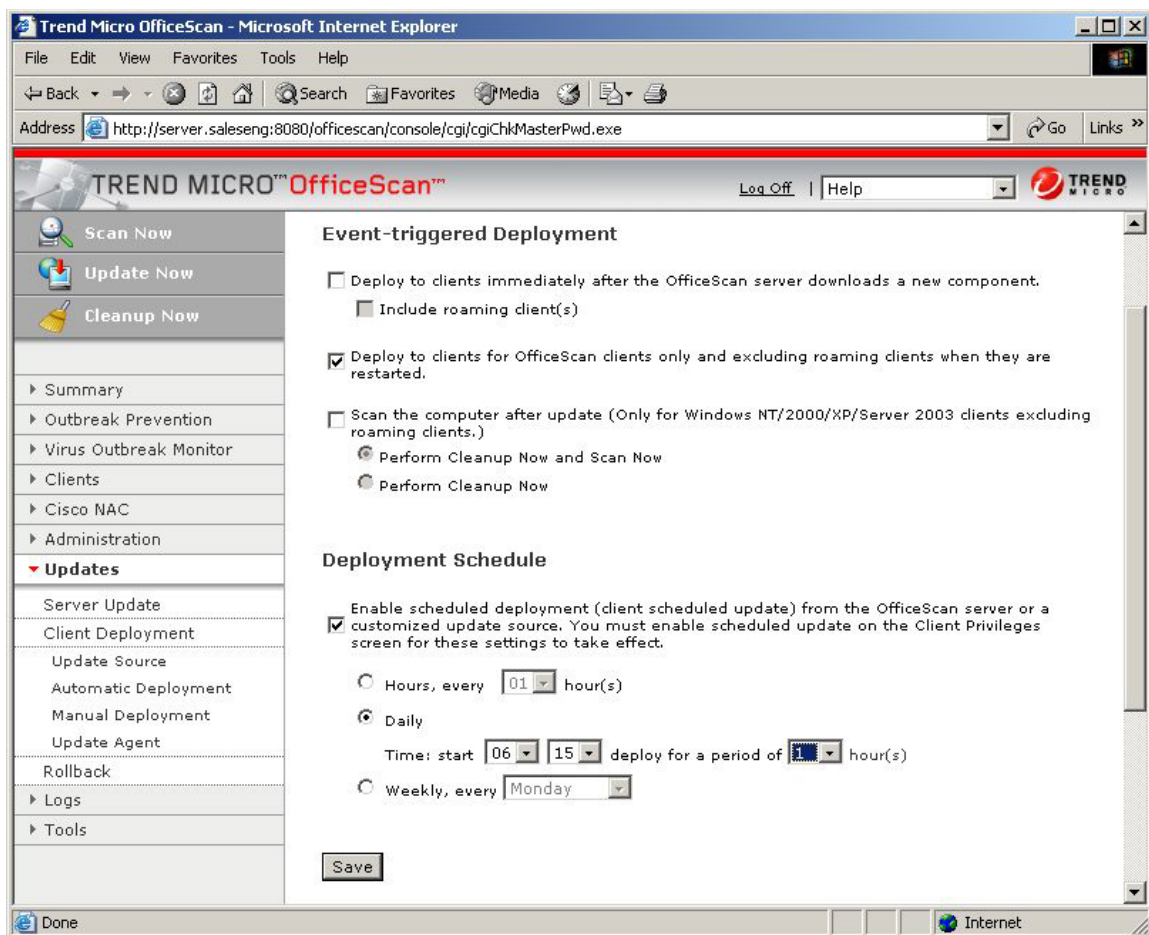
Follow the steps as prompted. The server and the workstations are updated with the latest virus pattern.

3) Scheduling Virus Pattern Files Updates

1. Using the Deep Freeze Enterprise Console, schedule a Maintenance Period as per instructions on p. 4-5.
2. Open the OfficeScan Management Console. On the left menu click *Updates*.
3. Select *Client Deployment > Automatic Deployment*.

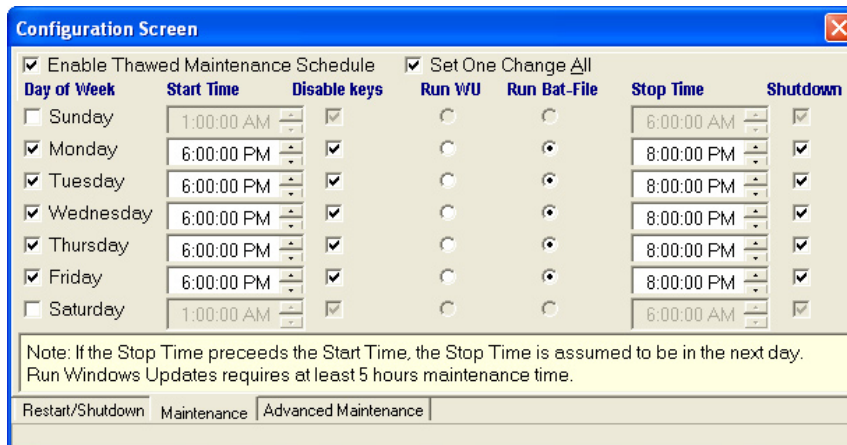
Under the Deployment Schedule section check *Enable scheduled deployment*.

4. In our example, we set Deep Freeze Enterprise to have a maintenance window Monday through Friday from 18:00 to 20:00. It is important to give the workstations enough time to reboot into the *Thawed* state. Fifteen minutes is sufficient.
5. Click the *Daily* radio button, set the starting time at 18:15, and leave the deployment period in one hour. Click *Save* to update the settings.



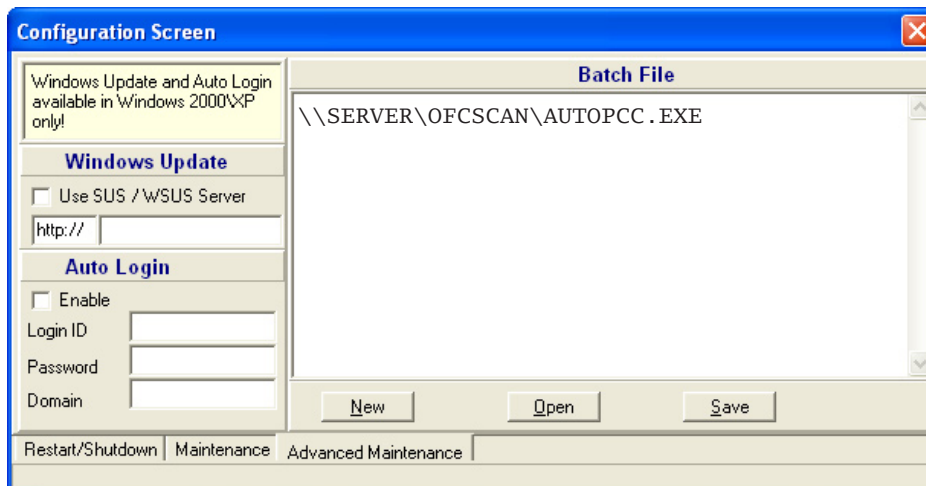
4) Configure Deep Freeze Enterprise to Run a Batch File that Updates the Virus Pattern File

1. Open the Deep Freeze Enterprise Console and follow the steps on p. 4 to set up a Scheduled Maintenance Period.
2. Check the *Run Bat* radio button to allow the workstations to run a batch file automatically during the Maintenance period.



3. Click the *Advanced Maintenance* tab and enter the following line in the Batch File window.

```
\\SERVER\OFCSKAN\AUTOPCC.EXE
```



This command triggers the update and the virus pattern file downloads from the server.

5) Updating Virus Patterns via a Batch File in a Third-Party Desktop Management Solution

Virus pattern files can be also updated running a batch file from a Desktop Management software such as Novell ZenWorks, Altiris, Microsoft SMS, BigFix, etc. You can add a task that runs the following batch file.

```
@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 *****
\\SERVER\OFCSCAN\AUTOPCC.EXE
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
```

6) 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 definitions 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 simply 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.

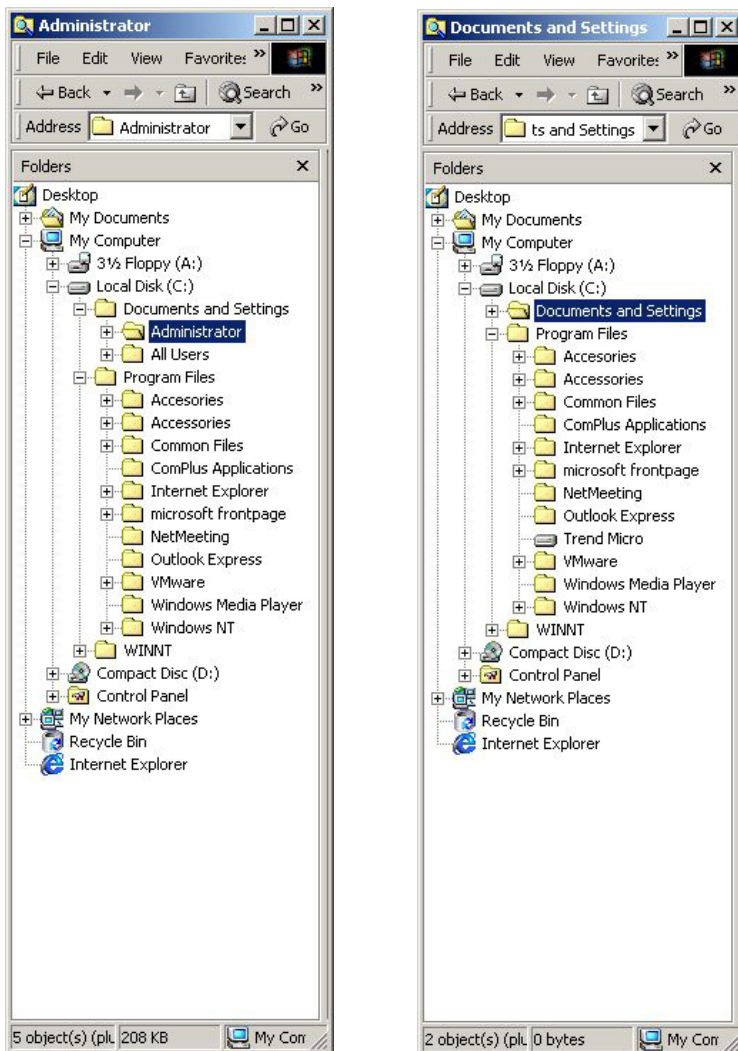
Preparing the Windows 2000 / XP Workstations for OfficeScan Installation on Mounted Partitions



Some OfficeScan 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 common antivirus 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 Trend Micro OfficeScan using the default options:



The installation of Trend Micro OfficeScan creates one new directory on the workstation:

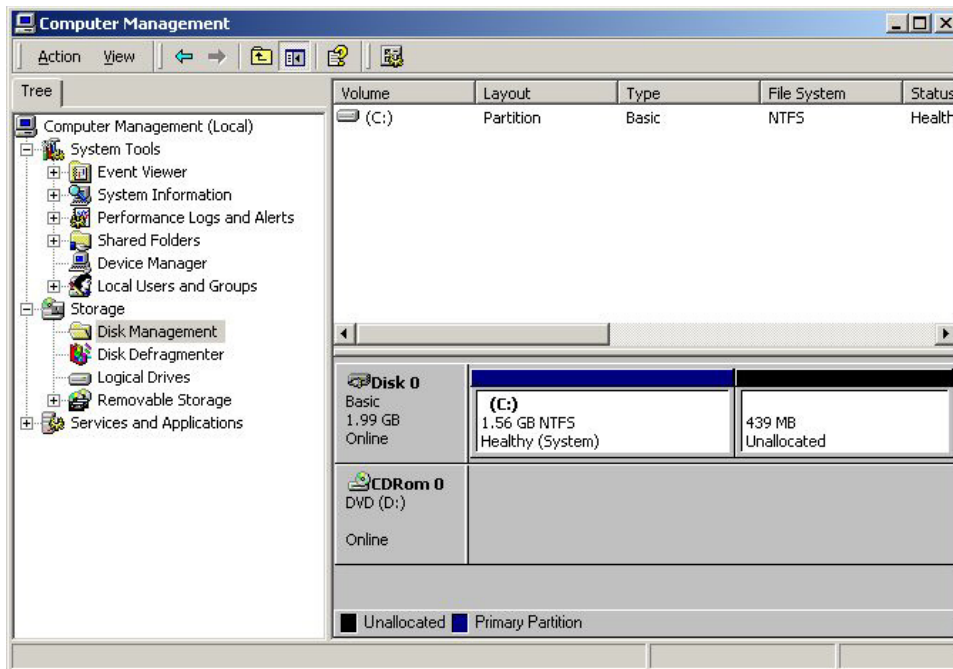
C:\Program Files\Trend Micro

To ensure that the application has the ability to apply full updates to the virus definitions, the *C:\Program Files\Trend Micro* folder must be recreated as a partition.

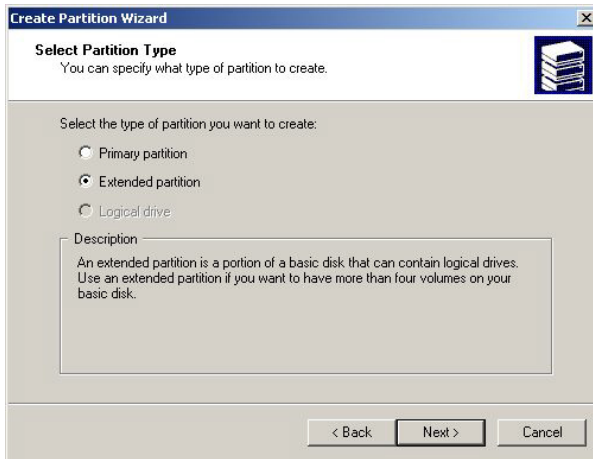
Partition #	Name of Folder the Partition Replaces	Drive Size
1	C:\Program Files\Trend Micro	120MB

The partition size has been selected to allow Trend Micro OfficeScan enough room to be able to update the files that it uses. Because these are going to be moved to a new drive, the size limit of 120 MB is 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 that stores the additional partitions using the Disk Management feature of the Computer Management console. When the console is opened, the following image appears:



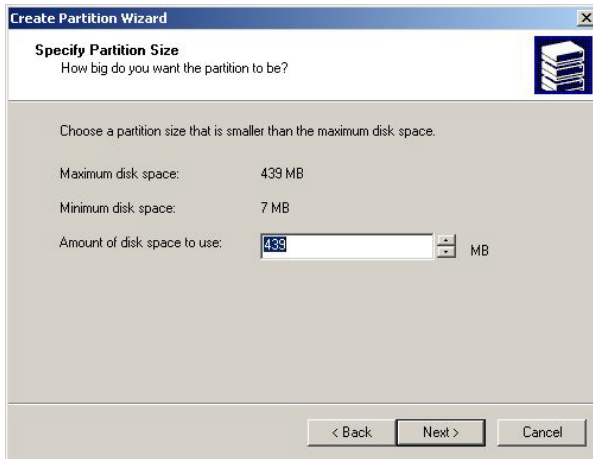
To create an extended partition, right-click on the unallocated space shown in the bottom of the screen and select *Create Partition*. The following Wizard appears to assist in creating the partition.



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.

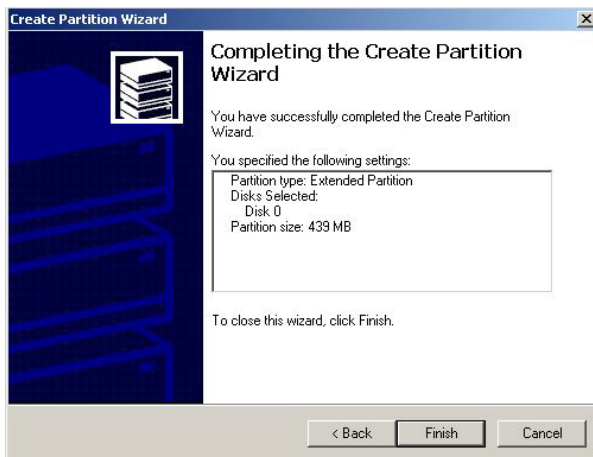
Click *Next*.



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.

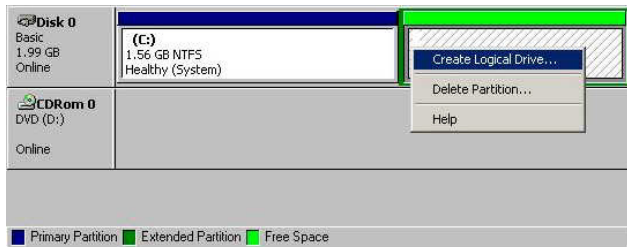
Click *Next*.



The last screen shows confirmation of the partition size and type 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*.

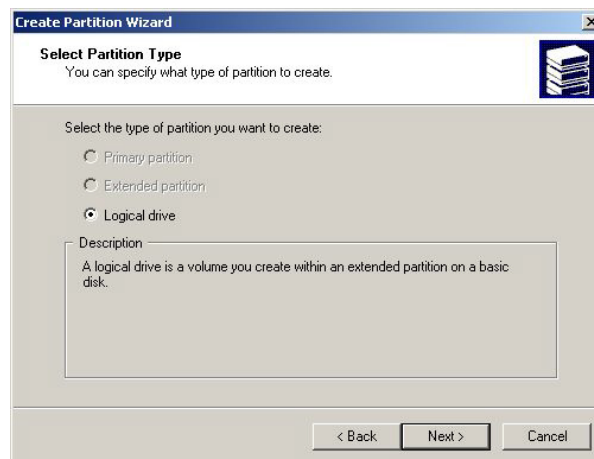


A wizard appears to set the size and folder name of the new partition.



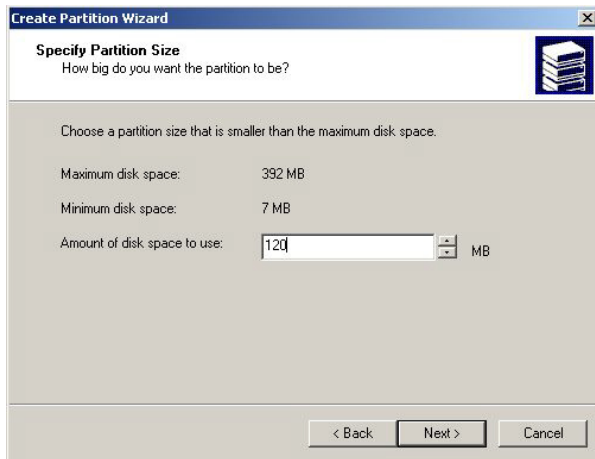
This is the first introduction screen.

Click *Next*.



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

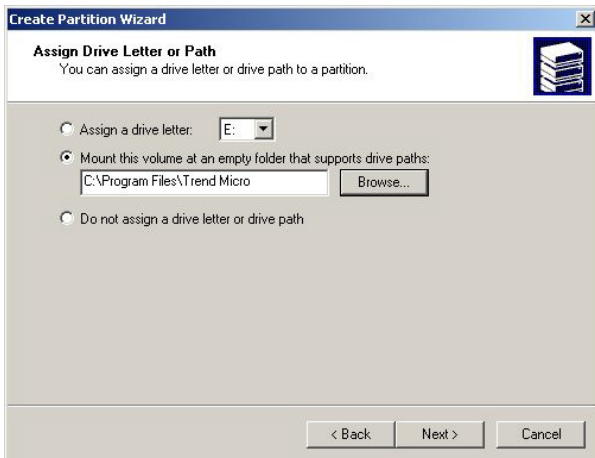
Click *Next*.



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 120 MB partition size is selected.

Click *Next*.

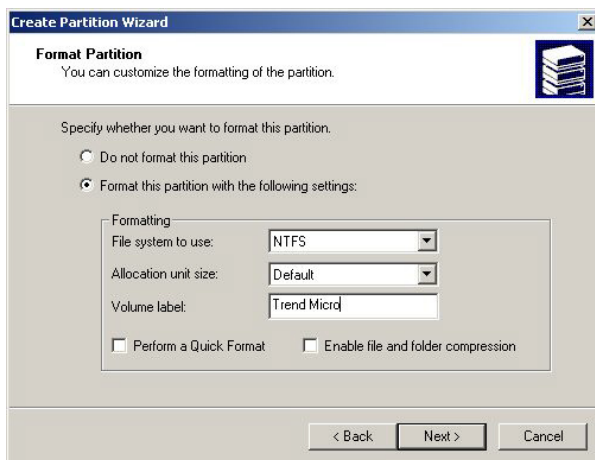


The next screen prompts for the drive letter or path of the new partition.

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\Trend Micro*.

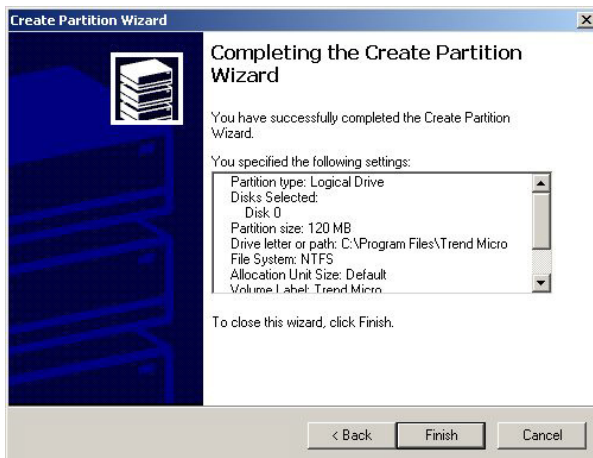
Click *Next* to continue.



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* to continue.

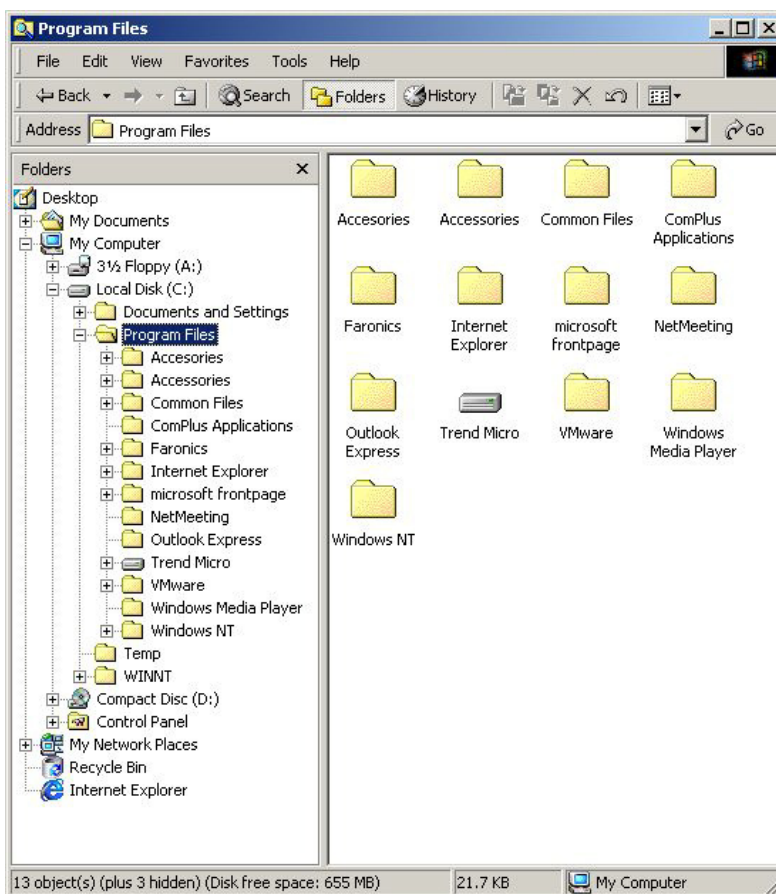


The last screen shows confirmation of the selected options once the partition has been successfully created.

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

After the drive has been successfully mounted as a path, a new icon appears representing the folder as a hard disk drive.

In the example below, the Trend Micro folder is displayed as a small hard disk drive.



Now you are ready to deploy the OfficeScan clients as per the manufacturer's installation instructions.



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).