Faronics

DEEPFREEZE™

ABSOLUTE Workstation Integrity

Deep Freeze Enterprise - Best Practices

TECHNICAL WHITEPAPER

Last modified: June 25, 2009

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

This document was created to give administrators a set of guidelines to follow to ensure Deep Freeze is set up and deployed in the most ideal way. This document describes the best way to set up a client machine to use Deep Freeze. It also describes some different methods to administer Deep Freeze for patches and updates.

Implementation

This section explains the recommended methods to initially configure your Deep Freeze environment and deploy it to your clients. This section also explains additional configuration settings recommended by Faronics to secure the machines.

Selecting a Customization Code

When configuring a Customization Code, it is good to use a combination of letters and numbers. It is also recommended to write this code down and store it in a safe place. Unlike a password, a Customization Code is not easy to change after deployment. Changing the Customization Code results in having to re-deploy the entire installation of Deep Freeze.

Installation Configuration

When creating a workstation install file, there are many settings that can be configured. It is recommended to create a password for the workstation that can be used locally at the client machine. This allows the administrator to Thaw the client machine when changes need to be made. It also allows for the possibility that the client machine will not be seen in the Enterprise Console, in which case this would be the only way to turn off Deep Freeze.

Installation Deployment

Any deployment solution can be used to push an image with Deep Freeze to your clients. Faronics does not recommend any specific deployment solutions. They should all work with an image that has Deep Freeze installed. In order to successfully deploy an image with Deep Freeze installed, Deep Freeze must be in a Thawed state with the *Clone* flag set. For more information about deploying with Deep Freeze, please refer to the white paper entitled: *Deep Freeze - Rapid Deployment* at the following location:

http://www.faronics.com/whitepapers/DF_RapidDeployment.pdf

Securing the System

The CMOS should be configured to prevent booting from the floppy drive or CD-ROM drive (i.e. set to boot to the hard drive) and the CMOS must be password protected. This is a normal precaution for most public access computers. The Windows Registry, the computer CMOS, and the boot sector are protected by Deep Freeze from within Windows.

Retaining User Data

In an environment where the user data needs to be stored on the local machine, it is possible to set up an area where the user data can be stored. This involves redirecting data to a Thawed location. For more information about setting up a Thawed area, refer to the document titled, *Retaining User Data* at the following location:

http://www.faronics.com/whitepapers/DF_RetainUserData.pdf

Installation Order With Other Faronics Products

In order to properly install an environment that contains both Deep Freeze and Anti-Executable, it is suggested to install Deep Freeze first, followed by Anti-Executable. This ensures that Deep Freeze is properly added to Anti-Exectuable's list of authorized executables.

Network Architecture

Complex networking environments are described in detail in the Deep Freeze Enterprise user guide, in Appendix B:

http://www.faronics.com/doc/DF6Ent_Manual.pdf

Maintenance

Now that Deep Freeze has been deployed, the following information provides recommendations to managing a Deep Freeze deployment.

To Patch or Not to Patch

This debate has gone on for quite some time. There is no specific recommendation whether to keep machines up to date or to never patch the machines. Both methods have their advantages. This may come down to the policy that has been implemented in the organization.

Antivirus Requirements

With Deep Freeze installed and computers Frozen, it is not possible for harmful files to remain on the Frozen partition after a reboot. This leads many people to ask whether an antivirus solution is required.

It is true that after a reboot any files modified on the Frozen partition are reverted back to their correct state. However, Deep Freeze does not prevent the harmful files from executing. This can cause the machine to become a *Typhoid Mary*, meaning the harmful files could propagate from a Deep Freeze machine to other machines on the network. As well, there is nothing preventing the harmful file from propagating back to the Deep Freeze machine immediately after a reboot.

Patch Management

Several methods can be used to update machines protected by Deep Freeze:

1. Use the Scheduled Maintenance feature to set up an automatic Thawed period during which time updates can be sent to the workstations.

   During the Scheduled Maintenance, an option can be set so that the keyboard and mouse are disabled at the workstation, allowing for updates to only take place via the network.

2. Use Deep Freeze Command Line Control (DFC) to control the Frozen and Thawed states via secure command lines issued over the network. DFC can be integrated into your existing imaging or management solution or you can use run-once login scripts. For more information on the Command Line Control, please refer to the white paper entitled: *Deep Freeze - Remote Administration with Secure Command Line Control* at the following location:

   http://www.faronics.com/whitepapers/DF_RemoteAdministration.pdf

3. Use the Enterprise Console to centrally Thaw workstations and make them available for updating. The Console can then be used to Freeze the workstations when the updates are complete.