Faronics
Simplifying Computer Management



Deep Freeze

ADVANCED System Integrity

User Guide

Last modified: 2026

© 1999 – 2026 Faronics Corporation. All rights reserved. Faronics, Deep Freeze, Deep Freeze Cloud, Faronics Core Console, Faronics Anti-Executable, Faronics Anti-Virus, Faronics Device Filter, Faronics Data Igloo, Faronics Power Save, Faronics Insight, Faronics System Profiler, and WINSelect are trademarks and/or registered trademarks of Faronics Corporation. All other company and product names are trademarks of their respective owners.
Protected by patents: US 7,539,828 | US 7,917,717 | US 9,152,824 | US 9,785,370

Contents

Preface 9
Important Information 10
About Faronics 10
Product Documentation 10
Technical Support 11
Contact Information 11

Introduction 13
Deep Freeze Overview 14
System Requirements 15
Deep Freeze Enterprise Files 16

Installing Deep Freeze 17
Installation Overview 18
Installing Deep Freeze Enterprise Configuration Administrator and Enterprise Console 18
Customization Code 21
Re-Initializing the Customization Code 21
Update Mode 21
One Time Passwords 23

Using Deep Freeze Enterprise Configuration Administrator 25
Accessing the Configuration Administrator 26
Toolbar and Menus 26
Passwords Tab 28
Drives Tab 29
Frozen Drives 29
ThawSpace 30
Existing ThawSpace 32
Always Thaw External Hard Drives 33
Workstation Tasks Tab 34
Windows Update 35
Restart 39
Shutdown 40
Idle Time 42
Batch File 43
Thawed Period 45
Windows Update Tab 48
Batch File Tab 50
Advanced Options Tab 52
Network 52

Advanced Options 53
Stealth Mode 56
License 56
Creating Workstation Install Program and Workstation Seed 58

Using Deep Freeze Enterprise Console 61

Deep Freeze Configuration 62
Applying Deep Freeze Configuration 62
Editing Deep Freeze Configuration 63
Deleting Deep Freeze Configuration 63
Exporting Deep Freeze Configuration 63
Configuration Generator 64
Using Configuration Generator from Command Line 65
Configuration File Parameters 65
Deep Freeze Enterprise Console 70
Launching the Enterprise Console 70
Activating the Enterprise Console 71
Status Icons 71
View Columns 73
Status Based Selection 74
Managing Communication Between the Console and Workstations 75
Configuring the Local Service 75
Editing or Removing a Local Service Connection 77
Configuring Proxy Server Connection 77
Remote Consoles 79
Setting up Remote Control Enabled Connections 79
Connecting to a Remote Console 80
Managing Deep Freeze with the Console 81
Reboot Thawed/Reboot Thawed Locked for an Assigned Number of Times 82
Login User 82
Sending Messages to Computers 83
Updating a Deep Freeze Configuration File 84
Run Windows Update 84
Remote Launch 85
Push and Launch 86
Format ThawSpace 87
Delete ThawSpace 87
Viewing the Console Log File 88
Target Installing Deep Freeze 89
Updating Deep Freeze Software 89
Thawed Alerts 89
Licensing 90
Manual Activation 91
License Icon 92
Reports 93

Customize the Grid 94
Tags 96
Create/Assign Tags 96
Remove/Unassign Tags 96
Delete Tags 97
Notes 98
Add Notes 98
Scheduling Deep Freeze Tasks 99
Editing Scheduled Tasks 103
Assigning Computers to Scheduled Tasks 104
Adding a Task 104
Editing a Task 104
Pausing a Task 104
Resuming a Task 104
Deleting a Task 105
Executing a Task Immediately 105
Scheduled Task Properties 105
Managing Network and Groups 106
Adding a Group 106
Building a User-Defined Group Structure 109
Importing Groups from Active Directory 109
History 110
Adding Computers to a Group 111
Configure Custom Actions 112
Control with RDC 112
Remote Execute with PsExec 113
Push and Install MSI file with PsExec 114
Push and Launch 115
Remote Launch 116
Deleting, Importing and Exporting Custom Actions 117
Console Customizer 118
Deep Freeze Enterprise Console Shutdown 119
Installing Deep Freeze on the Workstation 120
Attended Install or Uninstall 120
Uninstalling Deep Freeze on the Workstation via the Console 122
Silent Install or Uninstall 123
Example Command Line 123
Silent Install or Uninstall Using a Shortcut 124
Network Install on Multiple computers 124
Installing Over Existing Deep Freeze Versions 125
Installing Using Imaging 125
Target Install 126
Check for Updates 127

Managing Deep Freeze Computers 129

Login Screen 130

Launching Deep Freeze on Touchscreen Devices 130
Status Tab 131
Status on Next Boot 131
Clone 131
License 132
Password Tab 134
Network Tab 135
ThawSpace Tab 136
Permanent Software Installations, Changes, or Removals 137

Managing Anti-Virus 139
Anti-Virus Overview 140
Anti-Virus Reports 141
Migrating to the New Anti-Virus 142
Enable Anti-Virus on Enterprise Console 143
Install Anti-Virus Client on the workstation 144
Anti-Virus Configuration 145
Creating Anti-Virus Configuration 145
Applying Anti-Virus Configuration 164
Editing Anti-Virus Configuration 164
Deleting Anti-Virus Configuration 164
Using Faronics Anti-Virus from the Enterprise Console 165
Anti-Virus Commands 165
Scheduling Anti-Virus Tasks 169
Using Anti-Virus on the Workstation 170
Launching Anti-Virus on the Workstation 170
Scanning the Workstation 171
Scanning a File or a Folder via Right-Click 172
View Scanning History 172
View and Take Action on Quarantined Files 173
Updating Anti-Virus Definitions on the Workstation 174
Managing Anti-Virus on the Workstation via the System Tray 175
Check for Anti-Virus Updates 177
Update Faronics Anti-Virus 178
Updating Anti-Virus Definitions 179
Uninstall Anti-Virus Client from the Enterprise Console 180
Disable Faronics Anti-Virus from the Enterprise Console 181

Deep Freeze Command Line Control 183
Deep Freeze Command Line Control (DFC.EXE) 184
DFC Return Values 184
Deep Freeze Command Line Syntax 185
Faronics Anti-Virus Command Line Syntax 188

Appendix A Ports and Protocols 189

Appendix B Network Examples 191
Example 1: Single Subnet 192
Example 2: Multiple Subnets, One Local Service 193
Example 3: Multiple Ports, Console Accessed Remotely 194
Example 4: Multiple Subnets, Multiple Local Services 195

Appendix C Troubleshooting a Remote Console Connection 197
No Clients In the Console 197
Port is in Use Error When Starting the Console 198

Appendix D Creating a Customized Deep Freeze Enterprise Console 199

Appendix E Deep Freeze Action Files (RDC Example) 201
Deep Freeze Action Files 201
Action File Example 201
Deep Freeze Action File Structure 202
Console Parameters 204



Preface

This user guide explains how to install, configure and use Deep Freeze Enterprise.

Topics

Important Information
Technical Support

Important Information

This section contains important information about your Faronics Product.

About Faronics

Faronics delivers market-leading solutions that help manage, simplify, and secure complex IT environments. Our products ensure 100% machine availability, and have dramatically impacted the day-to-day lives of thousands of information technology professionals. Fueled by a market-centric focus, Faronics' technology innovations benefit educational institutions, health care facilities, libraries, government organizations, and corporations.

Product Documentation

The following documents form the Deep Freeze Enterprise documentation set:

- Deep Freeze Enterprise User Guide – This is the document you are reading. This document guides you how to use the product.
- Deep Freeze Enterprise Release Notes – This document lists the new features and known issues and closed issues.

Technical Support

Every effort has been made to design this software for ease of use and to be problem free. If problems are encountered, contact Technical Support.

Email: support@faronics.com

Phone: 800-943-6422 or +1-604-637-3333

Hours: 7:00am to 5:00pm (Pacific Time)

Contact Information

- Web: www.faronics.com
- Email: sales@faronics.com
- Phone: 800-943-6422 or +1-604-637-3333
- Fax: 800-943-6488 or +1-604-637-8188
- Hours: 7:00am to 5:00pm (Pacific Time)
- Address:

Faronics Technologies USA Inc.
5506 Sunol Blvd, Suite 202
Pleasanton, CA, 94566 USA

Faronics Corporation (Headquarters)
609 Granville Street, Suite 1400
Vancouver, BC V7Y 1G5
Canada

Faronics EMEA
8, The Courtyard, Eastern Road
Bracknell, Berkshire
RG12 2XB, United Kingdom

Faronics Pte Ltd
160 Robinson Road
#05-05 SBF Center
Singapore 068914



Introduction



Deep Freeze protects the computers that are set to boot from the hard drive. Configure the CMOS to boot from the hard drive only. The CMOS must be password protected to prevent unauthorized changes. Deep Freeze protects the Master Boot Record (MBR) when the computer is Frozen.

Topics

Deep Freeze Overview
System Requirements
Deep Freeze Enterprise Files

Deep Freeze Overview

Faronics Deep Freeze helps eliminate computer damage and downtime by making computer configurations indestructible. Once Deep Freeze is installed on a computer, any changes made to the computer—regardless of whether they are accidental or malicious—are never permanent. Deep Freeze provides immediate immunity from many of the problems that plague computers today—inevitable configuration drift, accidental system misconfiguration, malicious software activity, and incidental system degradation.

Faronics Anti-Virus can now be managed using Deep Freeze Enterprise (a separate license is required for Faronics Anti-Virus). Faronics Anti-Virus provides protection from security threats without slowing down computers due to slow scan times and large footprints. Built with next-generation technology, Faronics Anti-Virus gives you powerful anti-virus, anti-rootkit and anti-spyware software in-one. This protects you against today's highly complex malware threats while providing seamless integration with Deep Freeze.

Deep Freeze integration with Faronics Anti-Virus ensures your protection is up-to-date in the simplest way possible, providing deployment and management capabilities through Deep Freeze Enterprise Console. Designed to work together seamlessly, Faronics Anti-Virus is updated even while workstations are Frozen, offering the most comprehensive protection system.

System Requirements

Desktop edition

Deep Freeze client and Faronics Anti-Virus client:

- Windows 7 and 8.1 (32 and 64-bit)
- Windows 10 up to version 22H2 (32 and 64-bit)
- Windows 11 up to version 26H2
- Windows Embedded 7 and 8

Deep Freeze Enterprise Configuration Administrator and Enterprise Console:

- Windows 7 and 8.1 (32 and 64-bit)
- Windows 10 up to version 22H2 (32 and 64-bit)
- Windows 11 up to version 26H2
- Windows Server 2008 R2 (32 and 64-bit)
- Windows Server 2012, 2016, 2019, 2022, 2025

Server edition

Deep Freeze client:

- Windows Server 2008 R2 (32 and 64-bit)
- Windows Server 2012, 2016, 2019, 2022, 2025

Deep Freeze Enterprise Configuration Administrator and Enterprise Console:

- Windows 7 and 8.1 (32 and 64-bit)
- Windows 10 up to version 22H2 (32 and 64-bit)
- Windows 11 up to version 26H2
- Windows Server 2008 R2 (32 and 64-bit)
- Windows Server 2012, 2016, 2019, 2022, 2025

Deep Freeze requires 10% of the hard drive to be left as free space.



Deep Freeze is compatible with the Core Isolation feature of Windows.

For more information, contact Technical Support at support@faronics.com.

Deep Freeze Enterprise Files

Deep Freeze uses different colored icons to represent its components. Files identified by a red icon should generally only be installed on an administrative computer.

Icon	Definition
	Deep Freeze Enterprise Configuration Administrator and Enterprise Console installation file.
	The Configuration Administrator application is used to create customized, pre-configured, computer installation program files and Workstation Seeds.
	The Enterprise Console application is used to centrally deploy, monitor, manage, and maintain Deep Freeze installations.
	A customized Deep Freeze workstation installation file is created in the Configuration Administrator and deployed to workstations within the enterprise. This file includes the Workstation Seed. If the Deep Freeze workstation installation file is installed, the Workstation Seed is not required to be installed separately.
	A Workstation Seed enables seamless communication between the Enterprise Console and computers on a network. When the Workstation Seed is installed on a computer, the computer becomes visible on the Enterprise Console. Once a computer is visible on the Enterprise Console, various actions such as Restart, Shutdown and Wake-on-LAN can be performed on the computer remotely. Deep Freeze can also be installed remotely on visible computer thereby allowing Deep Freeze related actions on remote computers.

Installing Deep Freeze

This chapter describes the installation process of Deep Freeze.

Topics

Installation Overview
Customization Code
One Time Passwords

Installation Overview

Installing Deep Freeze Enterprise Configuration Administrator and Enterprise Console

The Configuration Administrator is intended to be installed only on the computer used to administrate Deep Freeze. The Configuration Administrator is used to create customized Deep Freeze installation files and Workstation Seeds. The Deep Freeze Enterprise Console installs automatically with the Deep Freeze Enterprise Configuration Administrator.



If you are using Deep Freeze 6.5 (or higher), you have the option to automatically upgrade the Enterprise Console, Configuration Administrator, and Deep Freeze install/configuration files (under the Install Programs folder) during installation while installing Deep Freeze 8.1 (or higher). The Customization Code is not required while upgrading Deep Freeze.

Complete the following steps to install the Configuration Administrator:

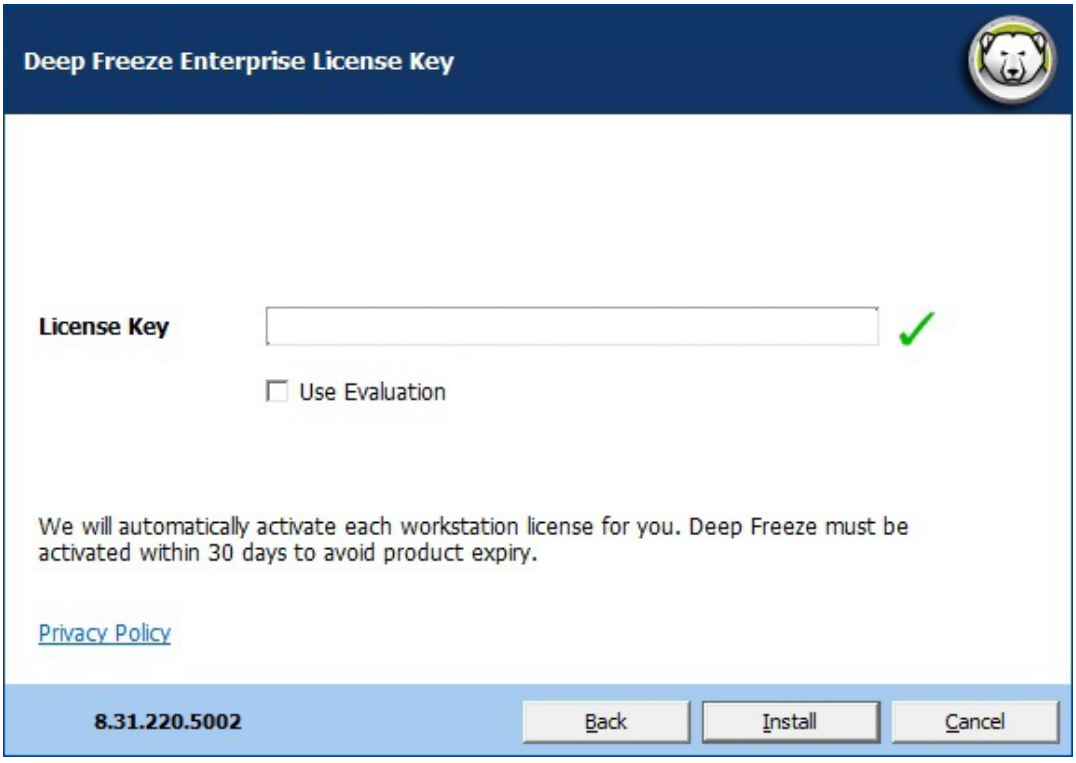
1. Double-click the file *DFEnt.exe* to begin the installation process. The following screen appears:



2. Click *Next*. Read and accept the license agreement. Click *Next*.



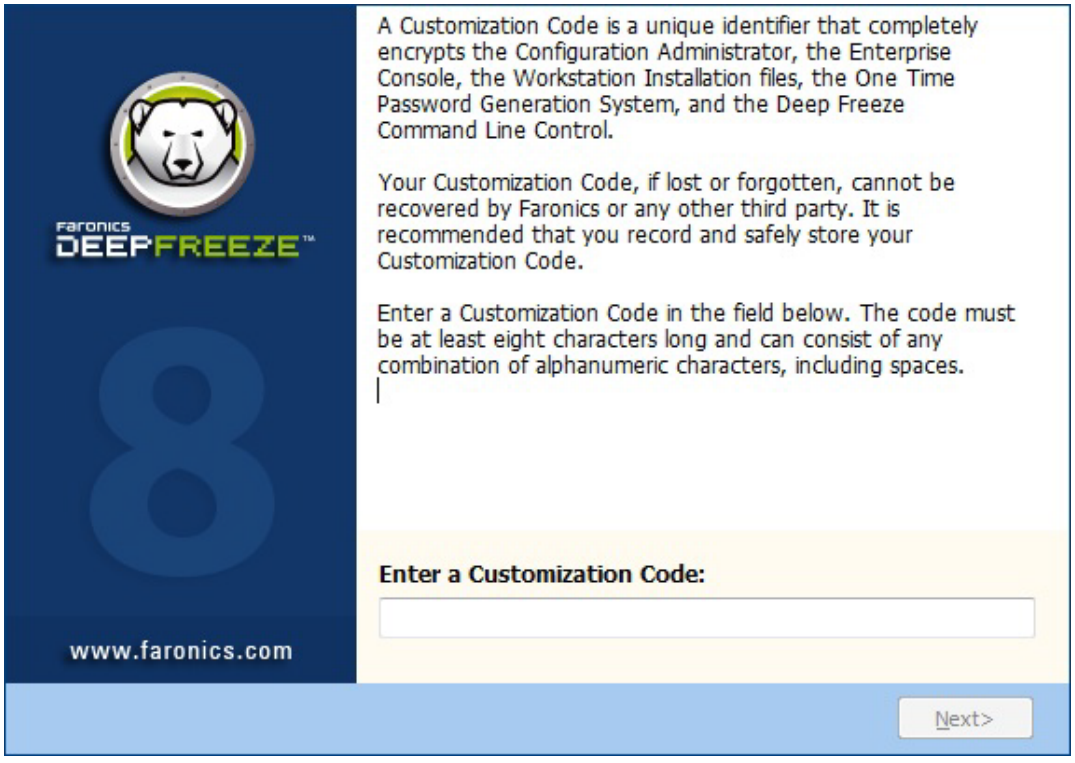
3. Enter the License Key in the *License Key* field or select the *Use Evaluation* checkbox to install in Evaluation mode. Click *Next*. (Deep Freeze will automatically activate the workstation licenses. Deep Freeze must be activated within 30 days to avoid expiry.)



4. Enter the License Key in the *License Key* field or select the *Use Evaluation* checkbox to install in Evaluation mode. Click *Install*.



5. The Customization Code screen appears.



6. Specify the *Customization Code* and click *Next*. The *Customization Code* must be a minimum of eight characters.

Customization Code

The Customization Code is a unique identifier that encrypts the Configuration Administrator, the Enterprise Console, the computer installation files, the One Time Password Generation System, and Deep Freeze Command Line Control. This code is not a password that can be used to access Deep Freeze.

The Customization Code ensures that unauthorized administrators are prevented from accessing or controlling a computer. Multiple Deep Freeze administrators controlling the same group of computers must use a matching Customization Code.



The Customization Code must be recorded and guarded with care. Faronics is unable to recover a lost or forgotten Customization Code.

Re-Initializing the Customization Code

If another administrator wants to create installation files with the same Configuration Administrator using a different Customization Code, complete the following steps:

1. Run *DFInit.exe*.

   This resets the existing Customization Code for the Configuration Administrator and Enterprise Console.

2. Enter a new Customization Code.
3. Click *OK* for the new Customization Code to become active.

Update Mode

Update Mode can be used to automatically create updated versions of existing files of Deep Freeze Enterprise by executing a special *Update* command. This command completes two tasks:

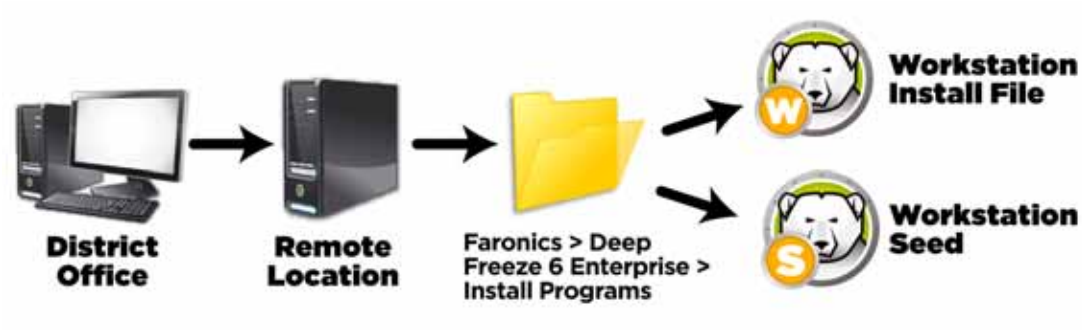
- Updates previous versions of the Deep Freeze Enterprise Console and the Deep Freeze Enterprise Configuration Administrator. (Found in *Faronics* > *Deep Freeze Enterprise*.)
- Updates any user created files stored in the *Faronics* > *Deep Freeze Enterprise* > *Install Programs* folder.

The benefit of these updates is that a number of files can be updated to the latest version while retaining their configuration data (created with an older version of Deep Freeze Enterprise).

The command automatically updates files created by an administrator (.exe, .rdx) that are present in the *Faronics* > *Deep Freeze Enterprise* > *Install Programs* directory, including the following sub-directories:

- Workstation install files
- Workstation Seed files

In the example below, the district office has received a new version of Deep Freeze Enterprise Configuration Administrator and can automatically update any existing Deep Freeze Workstation Install files and Workstation Seeds at a remote location.



The update command does not require a password, but does require a Customization Code. Use the following command syntax:

```
\PathToFile\DFEnt.exe /update="Customization Code" C:\dfupdate.log
```

- *PathToFile* must be replaced with the actual path to the installation file (*DFEnt.exe*)
- *DFEnt.exe* must be the actual name of the installation file (it may differ if it was downloaded)
- Customization Code must be in quotes if there is a space in it
- Customization Code must match the old installation files' Customization Code

The log file provides full details of exactly which files were updated.

The update process may take a few minutes to complete.

Update Mode does not update the existing version of Deep Freeze on computers. Computers must be updated using the Enterprise Console.

One Time Passwords

The One Time Passwords Generation System is used to generate temporary passwords for Deep Freeze that expire at midnight on the day they were generated.

One Time Passwords dialog can be accessed from:

- *Tools* > *One Time Passwords* in the Enterprise Console. For more information refer to Using Deep Freeze Enterprise Console.
- *File* > *One Time Passwords* in the Configuration Administrator. For more information refer to Using Deep Freeze Enterprise Configuration Administrator.

A One Time Password (OTP) can be useful if, for example, a Deep Freeze password is forgotten or if a configuration file was created without any passwords defined. An OTP can also be used to provide access to a computer for an individual performing maintenance duties without requiring that individual to know the permanent Deep Freeze password.

To create an OTP, complete the following steps:

1. Select either *Password valid for one use only* or *Password valid for multiple uses*. All OTPs expire at midnight on the day they were created, regardless of type.
2. Enter the OTP Token from the computer that requires the OTP into the *Token* field. The OTP Token for the computer is located in the logon dialog, as shown below.



3. Click *Generate*.

The Deep Freeze Command Line interface does not support the use of One Time Passwords.



Using Deep Freeze Enterprise Configuration Administrator

Topics

Accessing the Configuration Administrator
Passwords Tab
Drives Tab
Workstation Tasks Tab
Windows Update Tab
Batch File Tab
Advanced Options Tab
Creating Workstation Install Program and Workstation Seed

Accessing the Configuration Administrator

Open the Configuration Administrator by selecting the following path from the Start menu:

Start > All Programs > Faronics > Deep Freeze Enterprise > Deep Freeze Administrator

The Configuration Administrator provides various tabs to configure passwords, Frozen drives, Workstation Tasks, Windows Updates, Batch Files, and Advanced Options. Once the settings have been configured, a Workstation Install file can be created. The Workstation Install file can be installed on the computers that need to be protected by Deep Freeze. Deep Freeze Enterprise Configuration Administrator can also be accessed from within the Deep Freeze Enterprise Console.

Toolbar and Menus

Toolbar

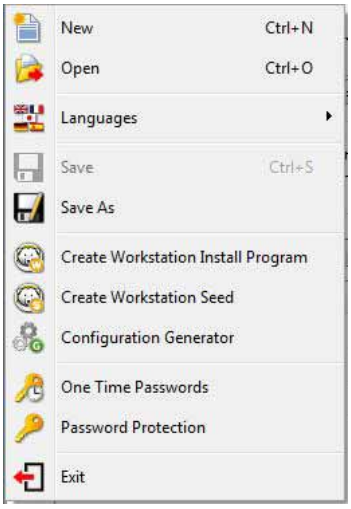
The Toolbar is available at the top of every tab in the Configuration Administrator.



Icon	Function
New	Blanks out all existing configuration settings. Opens with default configuration settings.
Open	Open any saved .rdx, Workstation Installation file or Workstation Seed file.
Save	Save a .rdx, Workstation Installation file or Workstation Seed file. File name and path is listed at the bottom of the Configuration Administrator in the status section.
Save As	Save the configuration settings as a .rdx file.
Help	Access the Deep Freeze Help file.
Create	*Create Workstation Installation File* creates a customized installer for installing on workstations. The workstations can then be managed from the Deep Freeze Enterprise Console. *Create Workstation Seed File* creates a seed that allows Deep Freeze Console to communicate with workstations across the network. Once the seed is installed on workstations, Deep Freeze Workstation Installation File can then be deployed remotely.

File Menu

The *File* menu contains the same options as those available on the Toolbar, with the additions of the option to choose from the available languages and *Password Protection*.



Password Protection

Password Protection offers an additional layer of security for the administrator.

To password protect access to the Configuration Administrator, complete the following steps:

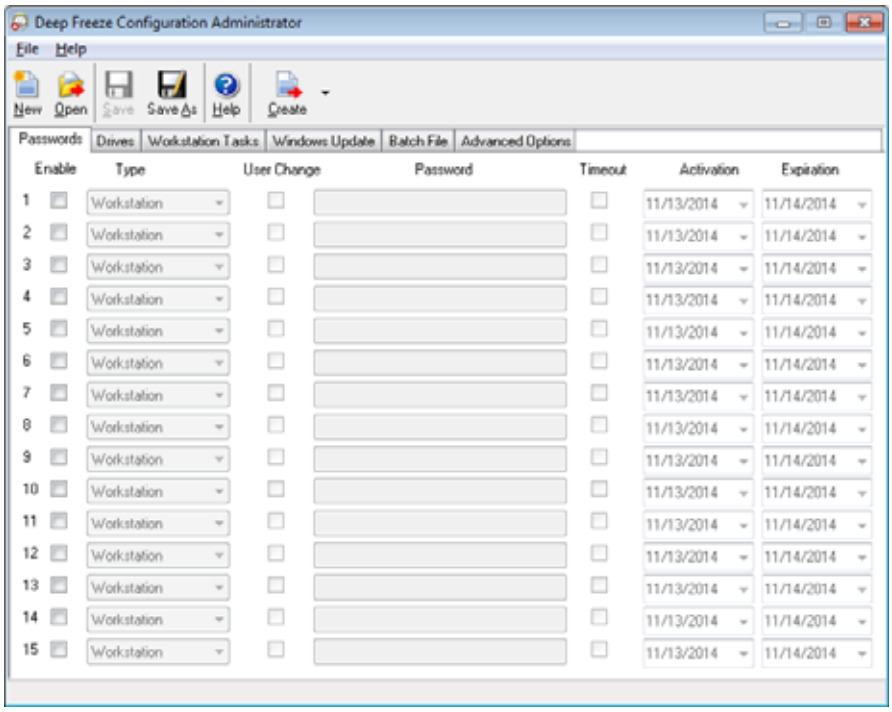
1. Open the *File* menu and select *Password Protection*.
2. Select the *Protect with password* checkbox.
3. Enter and confirm the password.
4. Click *OK* to set the password or *Cancel* to exit the dialog without setting a password.



Store the password in a safe location. If the password is lost, you cannot recover it. You will have to reinstall Deep Freeze.

Passwords Tab

Deep Freeze Enterprise allows the administrator to choose up to 15 fixed passwords.



To create a password, complete the following steps:

1. Select *Enable* on the appropriate row.
2. From the *Type* drop-down list, choose the preferred kind of password. The following options are available:
   > Workstation – Designated for use at the workstation when the Login Screen is launched.
   > Command Line – For use with Command Line Controls. The Command Line Control tool (DFC.exe) does not function unless at least one Command Line password is defined.
3. Optional – For passwords, select the *User Change* checkbox to allow a user to change the password at the computer.
4. Enter the password.



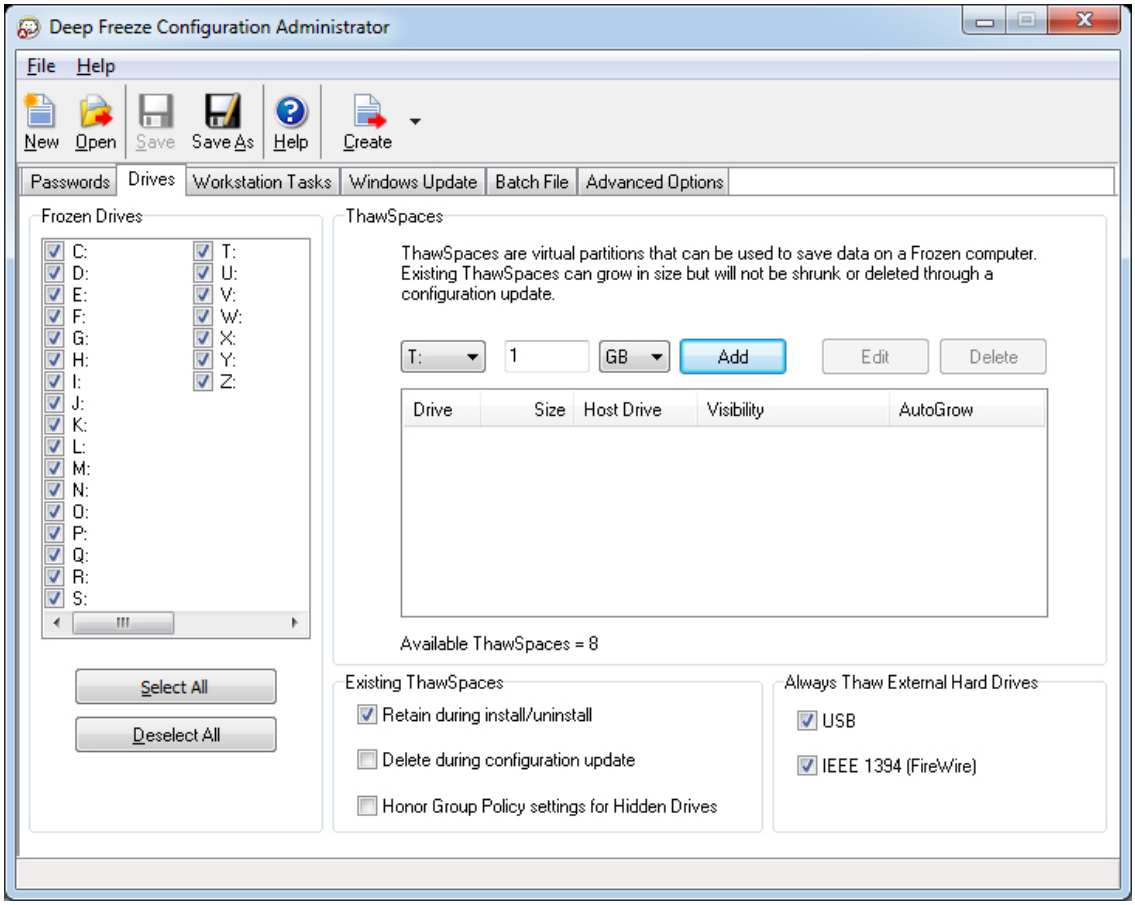
The password entered in the *Password* field is not hidden.

Do not use the same password for Command Line and the GUI.

5. To set a password to become active and expire on specified dates, select the *Timeout* checkbox and use the drop-down calendars to specify an *Activation date* and *Expiration date*.

Drives Tab

The Drives tab is used to select which drives are to be Frozen (protected by Deep Freeze) or Thawed (unprotected). You can also create a ThawSpace — a virtual partition hosted on a local Frozen or Thawed drive where data can be saved permanently without being deleted by Deep Freeze during a reboot.



Frozen Drives

By default, all drives are Frozen. To put a drive in a Thawed state, clear the checkbox of the preferred drive.

While only local drives (partitions or physical drives) can be Frozen, all drive letters are shown because the pre-configured installation file may be installed on many computers with various hardware and software setups.

Example

In the above screen, the D: is not selected from the Frozen Drives list. Therefore, all drives except D: are Frozen.

ThawSpace

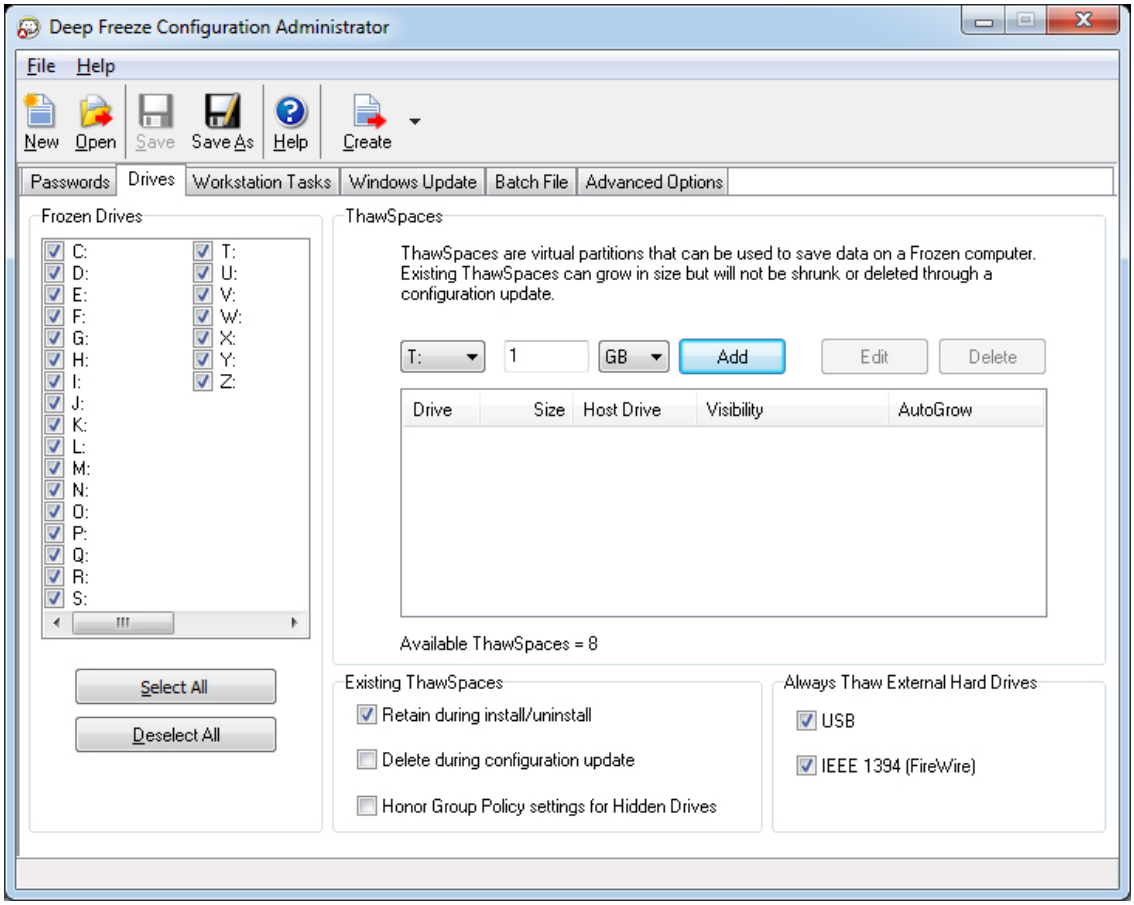
ThawSpace is a virtual partition that can be used to store programs, save files, or make permanent changes. All files stored in the ThawSpace are retained after a restart, even if the computer is Frozen. A ThawSpace can be created on a drive that is configured to be Frozen or Thawed.

A ThawSpace can be set to automatically expand through the *Automatically Grow* option to prevent running out of space. The ThawSpace will automatically expand by 25% of its current size after reaching 25% free space or less. It will expand up to the maximum size defined in ThawSpace configuration.



The ThawSpace will expand only in Thawed state.

Once the ThawSpace is expanded it will not be shrunk even when there is more than 25% of free space or when updating workstation configuration with smaller size for the given ThawSpace drive letter.



To create a single ThawSpace or multiple ThawSpaces using the Configuration Administrator, complete the following steps:

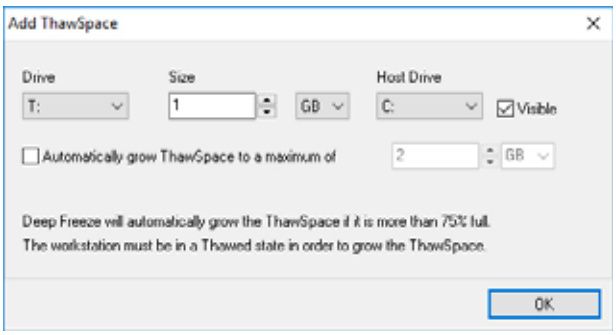
1. Select the *Drive Letter*. The default letter is *T:*. However, it can be changed to any available letter. The next available letter is automatically used if the selected drive letter already exists on a computer when Deep Freeze is installed.

> When a *Drive Letter* is selected from the drop-down and used to create a ThawSpace, it is removed from the drop-down.

> When a ThawSpace is removed, the corresponding *Drive Letter* is added back to the drop-down.

> The *Drive Letter* cannot be same as the *Host Drive*.

2. Click *Add*. The *Add ThawSpace* dialog is shown:



3. Enter the *Size*. This is the size of the ThawSpace. The maximum size is 1024 GB and the minimum size is 16 MB.

> If the computer 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 computer.

> If you select the Size less than 16 MB, the ThawSpace is set to 16 MB.

> If you select the Size more than 1024 GB (1 TB), the ThawSpace is set to 1024 GB (1 TB).

4. Select the ThawSpace storage unit in MB or GB.
5. Select the *Host Drive*.

> The *Host Drive* is the drive where the ThawSpace is created.

> The storage required for the ThawSpace is used from the total storage available on the *Host Drive*.

6. Select *Visible* or *Hidden* from the *Visibility* drop-down.

> If you select *Visible*, the drive will be visible in Windows Explorer.

> If you select *Hidden*, the drive will not be visible in Windows Explorer.

> However, the hidden drive can be accessed by typing the drive letter in *Start* > *Run*.

7. Check the *Automatically grow ThawSpace to a maximum* checkbox and configure the maximum size of the ThawSpace.
8. Click *Add* to add the ThawSpace.

Removing a ThawSpace

To remove a ThawSpace, select the ThawSpace and click *Remove*. The ThawSpace is removed and the drive letter is now added back to the *Drive Letter* drop-down. Click *Remove All* to remove all the ThawSpaces.





When a ThawSpace is removed in the Configuration Administrator, it will not take effect until the configuration is applied on the workstation.

Before removing a ThawSpace, remove any profile redirections or Symbolic Links.

Removing a ThawSpace will also remove the data stored in it.

A ThawSpace is not protected by Deep Freeze. Deploy standard data protection options such as, Anti-Virus and backup procedures.

Example

In the above screen, a ThawSpace of 16 MB is created on the *Host Drive* C: and the ThawSpace is designated with the drive letter T:. The ThawSpace T: is set to *Visible* and can be accessed via the Windows Explorer.



It is recommended to assign Drive Letters towards the end of the alphabet (X, Y, Z) in order to avoid automatic reassignment when a removable drive is unplugged.

Existing ThawSpace

The *Retain during install/uninstall* checkbox is selected by default to prevent ThawSpaces created during previous installations from being deleted. A dialog is always displayed asking if the ThawSpace should be retained or deleted during an Attended Uninstall, regardless of whether *Retain during install/uninstall* has been selected. This option is not displayed if the uninstall is performed through the Enterprise Console.

Select *Delete during configuration update* to delete all the existing ThawSpaces on the workstation and re-create while applying the configuration. The existing ThawSpaces and the data in the ThawSpaces will be deleted and the new ThawSpaces as per the settings will be created when the configuration is applied.

The *Honor Group Policy settings for Hidden Drives* ensures that the Group Policy settings for hidden drives do not conflict with the Deep Freeze settings for hidden drives.

Hidden drive settings for Group Policies are user-specific. Hidden drive settings for Deep Freeze are global if the *Honor Group Policy settings for Hidden Drives* option is disabled.



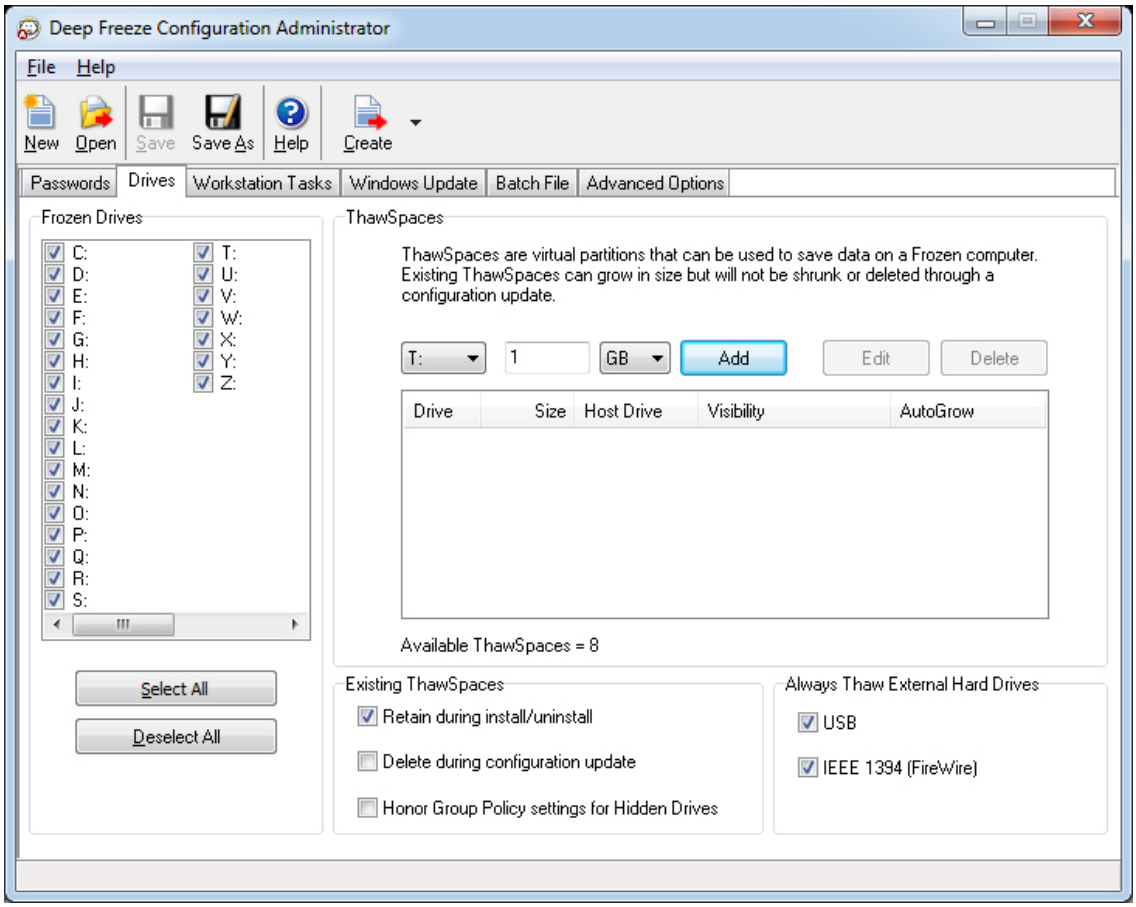
If there are no Group Policies for hidden drives, it is recommended to disable this option.

Always Thaw External Hard Drives

The *Always Thaw External Hard Drives* pane has two checkboxes, *USB* and *IEEE 1394 (FireWire)* and both checkboxes are selected by default. This ensures that the USB or IEEE 1394 (FireWire) hard drives are always Thawed.

If the USB and/or IEEE 1394 (FireWire) external hard drives checkboxes are cleared, the drive is *Frozen* or *Thawed* according to the letter each drive mounts to in the Frozen Drives section.

Network drives and removable media drives (floppy, memory keys, CD-RW, etc.) are not affected by Deep Freeze and therefore cannot be Frozen.



Example

In the above screen, drives E: and F: are selected in the *Frozen Drives* pane.

Let us assume that E: corresponds to a USB hard drive and F: corresponds to an IEEE 1394 (FireWire) hard drive.

The *USB* and *IEEE 1394 (FireWire)* checkboxes are selected in the *Always Thaw External Hard Drives* pane, the external hard drives would be *Thawed*.

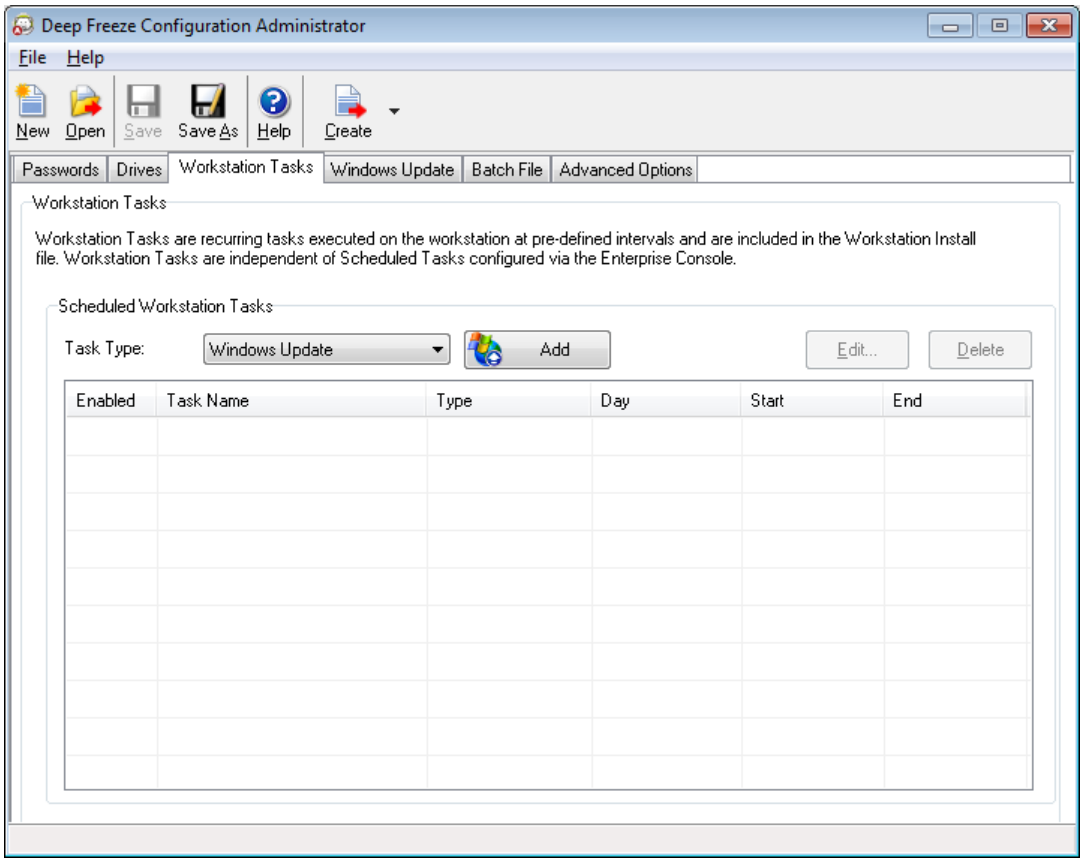
The USB checkbox is selected. The *IEEE 1394 (FireWire)* checkbox is cleared. In this example, the *USB* drive (*D:*) would be Thawed and the *IEEE 1394 (FireWire)* drive (*F:*) would be Frozen.

Workstation Tasks Tab

The Workstation Tasks tab allows you to schedule various tasks that run at the workstation. The Workstation Tasks reside at the workstation and will run even if the workstations lose their network connectivity or if they are unable to communicate with the Deep Freeze Console. The Workstation Tasks are part of the Workstation Install File or Deep Freeze Configuration (.rdx) file. The following Workstation Tasks are available:

- Windows Update – Schedule Windows updates. You can configure additional settings in the Windows Update tab.
- Restart – Periodically restart workstations to bring them to the original configuration or erase unwanted data.
- Shutdown – Shut down the workstations at a specified time every day to save power.
- Idle Time – Shut down or restart the workstations if they are idle for a specified period of time.
- Batch File – Run a batch file on the target workstation. You can configure additional settings in the Batch File tab.
- Thawed Period – Reboot Thawed for a specified period to perform manual software installs, automated software installs via third-party tools or other permanent configuration changes.

Each task is covered in detail in the following sections.



Workstation Tasks vs. Scheduled Tasks: If communication between the Enterprise Console and the target computer fails, the Workstation Tasks are still executed since they exist on the target computer.



Tasks scheduled through the Scheduled Tasks Wizard in the Deep Freeze Enterprise Console exist on the Console and not on the target computers. Therefore, a continuous connectivity between the Console and the target computer is required for the Scheduled Tasks to be executed. For more information, refer to the Scheduling Deep Freeze Tasks section.



Overlapping tasks cannot be created in the Workstation Tasks tab. If a newly created task overlaps with an existing task, a message is displayed.



A message can be displayed to the user for a maximum of 5 minutes. There must be a gap of a minimum of 5 minutes between any two tasks.



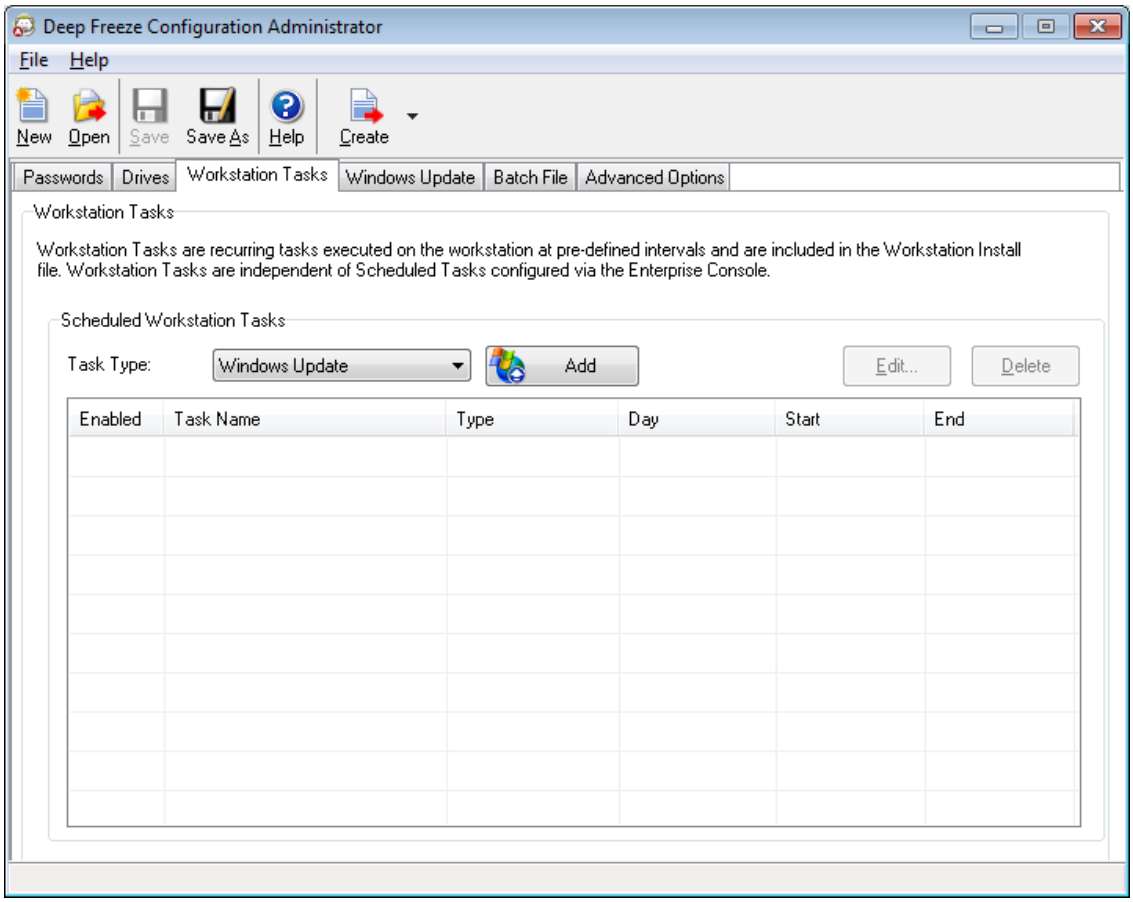
A Workstation Task is triggered only when Deep Freeze is in a Frozen state.

Windows Update

Windows Update tasks are scheduled for downloading Windows Updates on the workstation. Windows Updates can be downloaded even when the workstation is in a Frozen state. A Windows Update task has a Start Time and an End Time. After downloading Windows Updates, the workstation reboots in a Thawed state to apply.

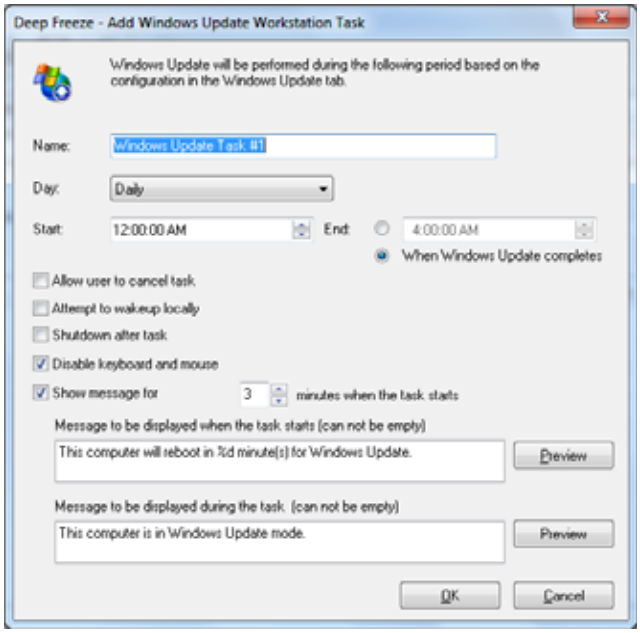


Windows Updates can also be applied manually on the workstation by selecting the workstation and via the command *Run Windows Update* from the context-menu in the Deep Freeze Console. For more information, refer to Managing Deep Freeze with the Console.



The Windows Update task can be scheduled by completing the following steps:

1. Select *Windows Update* from the *Task Type* drop-down and click *Add*.
2. The following options are displayed:



> Name – Specify a name for the task.

> Day – Select the day, or specify if the task will occur on Weekdays or Weekends.

> Start – Select the Start Time.

> End – Select the End Time. The minimum interval is 15 minutes. Alternatively, you can select *When Windows Update completes*. If the Windows Update Task is not completed in 6 hours, Deep Freeze will end the task gracefully.



If a Windows Update task is set to end *When Windows Update Completes*, and the computer is turned off at the scheduled start time of the task, the Windows Update task will be triggered for the computer if the computer is powered on within 15 minutes after the scheduled start time.

For example, a computer is turned off when the Windows Update task is set to start at 11:40 pm. If the computer is powered on between 11:40 pm to 11:55 pm, the Windows Update task will automatically execute on the computer.

> Allow user to cancel task – Select the checkbox if the user is allowed to cancel the task before it starts.

> Attempt to wake up locally – Select this checkbox to wake up the workstation locally without requiring any communication from the Enterprise Console.



Waking up the workstation locally depends on the hardware specifications of your workstation. This option will work only if it is supported by your hardware.

> Shutdown after task – Select the checkbox to shutdown the computer after the task.

> Disable Keyboard and Mouse – Select the checkbox to disable keyboard and mouse during the task.

> Show message – Select the checkbox to display a message on the computer *Before* and *During* the task. Specify the time interval in minutes and enter a brief message to be displayed before the task starts.

3. Click *OK*. You will be taken to the Windows Update Tab to configure additional settings if it has not been configured earlier.



The message *This computer will reboot in %d for Windows Update* is displayed in the *Message to be displayed before the task* field. This message can be edited. Add the word *minutes* in the message after *%d* to include the word minutes as part of the message.



When scheduling the Windows Update task select the *When Windows Update completes* option or ensure that you allow a sufficient time frame to permit all required update activities. Review of Microsoft Security Bulletins from the Technet web site (http://technet.microsoft.com/en-us/security/bulletin) to consider the appropriate time frame based upon the Critical and Security updates being released.

If you are not using WSUS, Deep Freeze Windows Update process will only apply non-user-intervention Critical and Security updates, as well as Feature updates for Windows 10 and above. If you are using WSUS, all WSUS approved updates will be applied.

If you are not using WSUS, Windows Update task will always try to install Feature updates whenever available starting from Windows 10. You can defer installing Feature updates by selecting *Choose when updates are installing* under Advanced Options of Windows Updates system settings, or enabling local computer policy *Select when Preview Builds and Feature Updates are received* located in *Computer Configuration* > *Administrative Templates* > *Windows Components* > *Windows Update* > *Windows Update for Business*.

Alternatively, to apply other available updates, visit the Microsoft Update Catalog site (http://catalog.update.microsoft.com) to obtain KB downloads which can then be applied using a Deep Freeze Batch File Workstation Task. Batch File tasks can also be used to apply other third-party software updates.

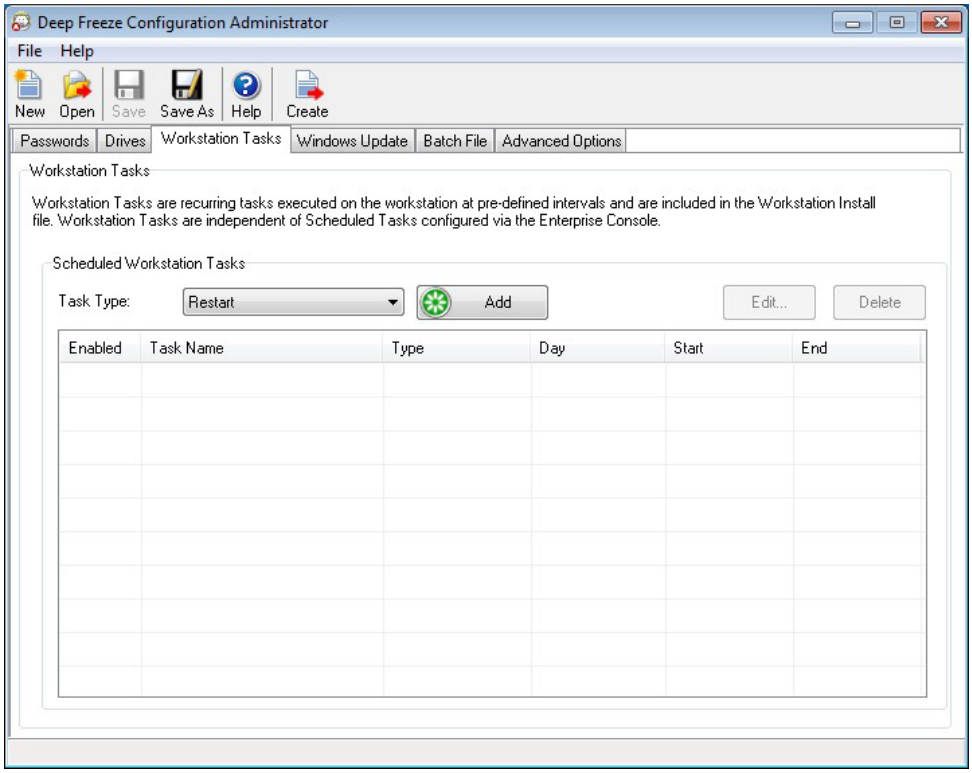
The Deep Freeze Windows Update tab settings override the Windows Update settings on the workstation.

Example

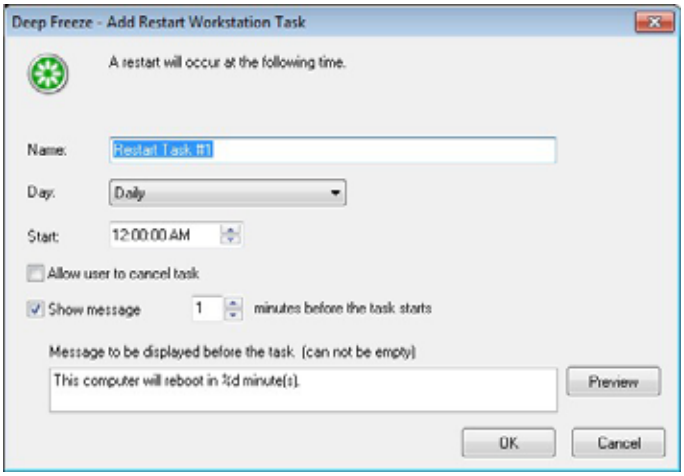
In the above screen, a Windows Update task has been created to perform Windows Updates at the computer daily at 12:00 AM and end when *Windows Update* completes. The task is configured to display a message to the user before Windows Update. The keyboard and mouse are disabled.

Restart

The Restart task can be scheduled by completing the following steps:



1. Select *Restart* from the *Task Type* drop-down and click *Add*.
2. The following options are displayed:



> Name – Specify a name for the task.

> Day – Select the day, or specify if the task will occur on Weekdays or Weekends.

> Start – Select the Start Time.

> Allow user to cancel the task – Select the checkbox if the user is allowed to cancel the task before it starts.

> Show message – Select the checkbox to display a message on the computer before the task starts. Specify the time interval in minutes and enter a brief message to be displayed before the task starts.

3. Click *OK*.

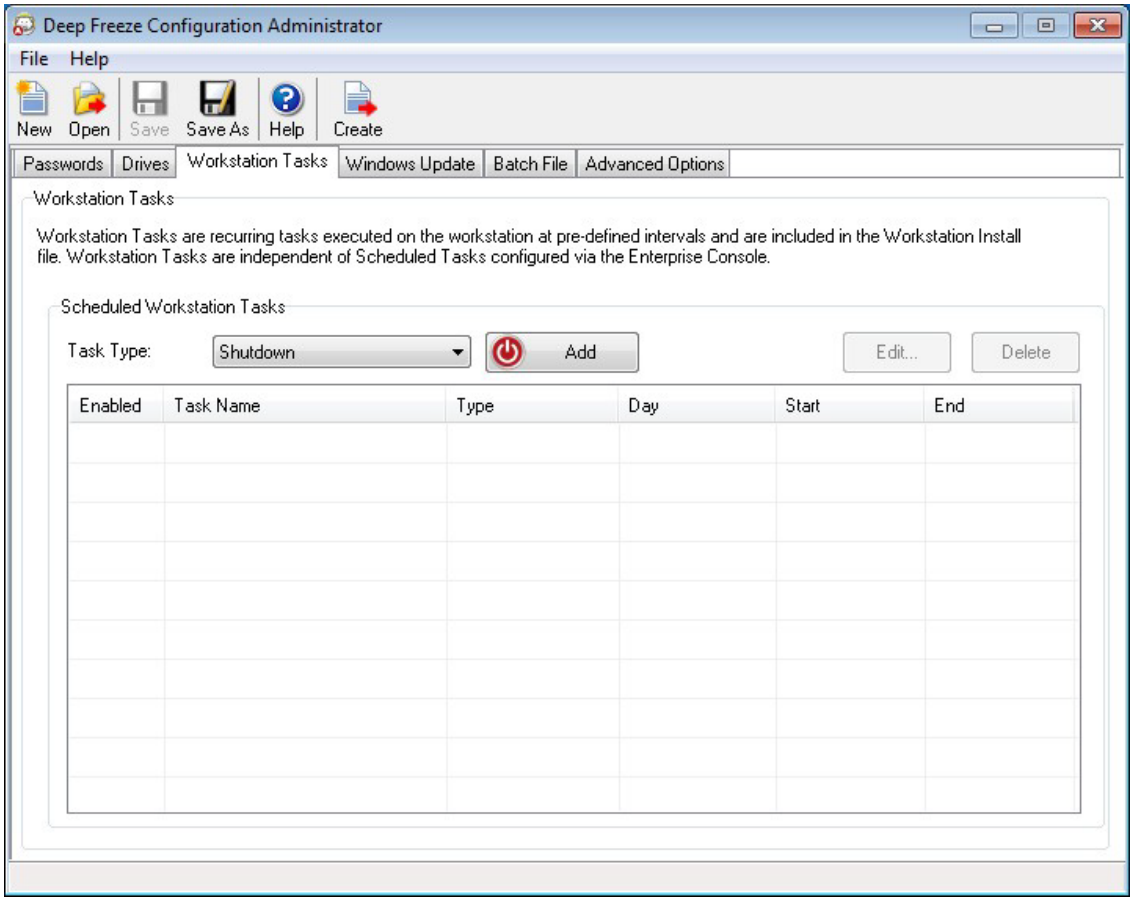
The message *This computer will reboot in %d seconds* is displayed in the *Message to be displayed before the task* field. This message can be edited. Add the word *minutes* in the message after *%d* to include the word minutes as part of the message.

Example

In the above screen, a Workstation Task has been created to restart the computer daily at 12:00 AM. The task is configured to display a message to the user 1 minute before the Restart.

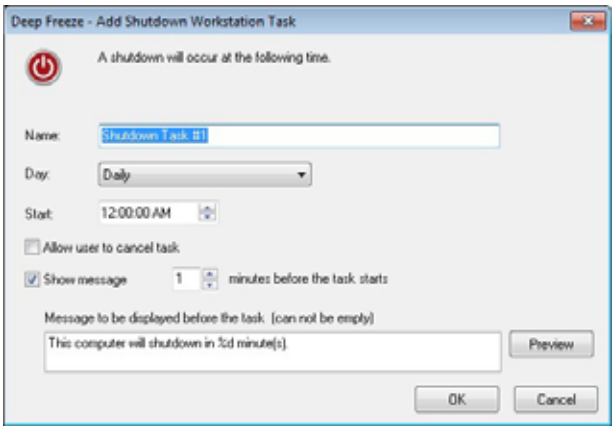
Shutdown

The Shutdown task can be scheduled by completing the following steps:



1. Select *Shutdown* from the *Task Type* drop-down and click *Add*.

2. The following options are displayed:



> Name – Specify a name for the task.

> Day – Select the day, or specify if the task will occur on Weekdays or Weekends.

> Start – Select the Start Time.

> Allow user to cancel the task – Select the checkbox if the user is allowed to cancel the task before it starts.

> Show message – Select the checkbox to display a message on the computer before the task starts. Specify the time interval in minutes and enter a brief message to be displayed before the task occurs.

3. Click *OK*.

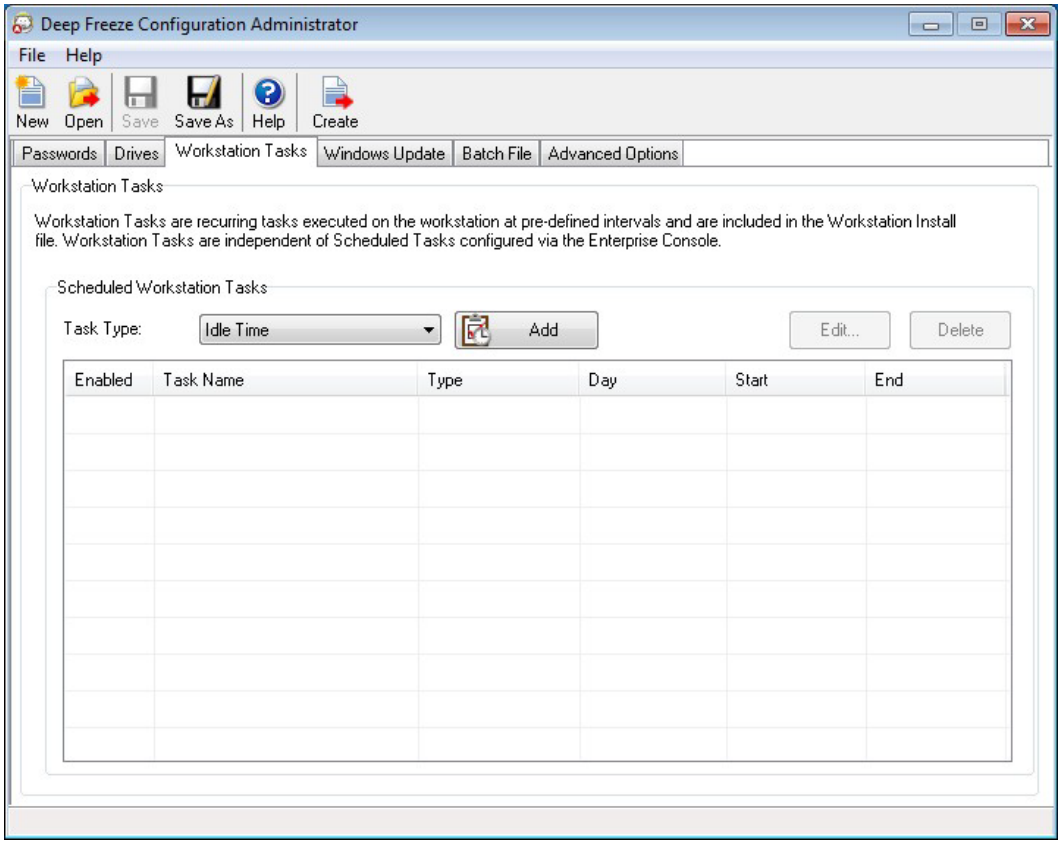
The message *This computer will shutdown in %d seconds* is displayed in the *Message to be displayed before the task* field. This message can be edited. Add the word *minutes* in the message after *%d* to include the word minutes as part of the message.

Example

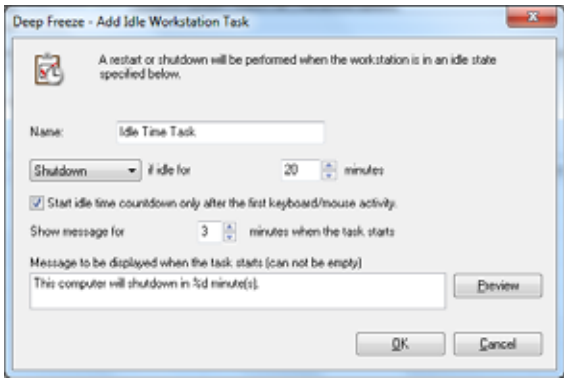
In the above screen, a Shutdown task has been created to shutdown the computer daily at 12:00 AM. The task is configured to display a message to the user 1 minute before the Shutdown task.

Idle Time

The Idle Time task can be scheduled by completing the following steps:



1. Select *Idle Time* from the *Task Type* drop-down and click *Add*.
2. The following options are displayed:



> Name – Specify a name for the task.

> Restart or Shutdown – Select Restart or Shutdown and specify the idle time in minutes after which the task must take place.

> Start idle time countdown only after the first keyboard/mouse activity – This option is only for the Shutdown task. Select this checkbox for the timer to start counting only after the first keyboard or mouse activity. For example, if the idle time is specified as 20 minutes, and this option is selected, the workstation task will shutdown the computer 20 minutes after the first keyboard and mouse activity.

> Show message – Select the checkbox to display a message. Specify the time interval in minutes and enter a brief message.



After the computer is started, the Idle Time counter becomes active only after the first keyboard or mouse activity has been initiated. During a Remote Desktop session, the Idle Time of the controlling computer is used to activate the task.

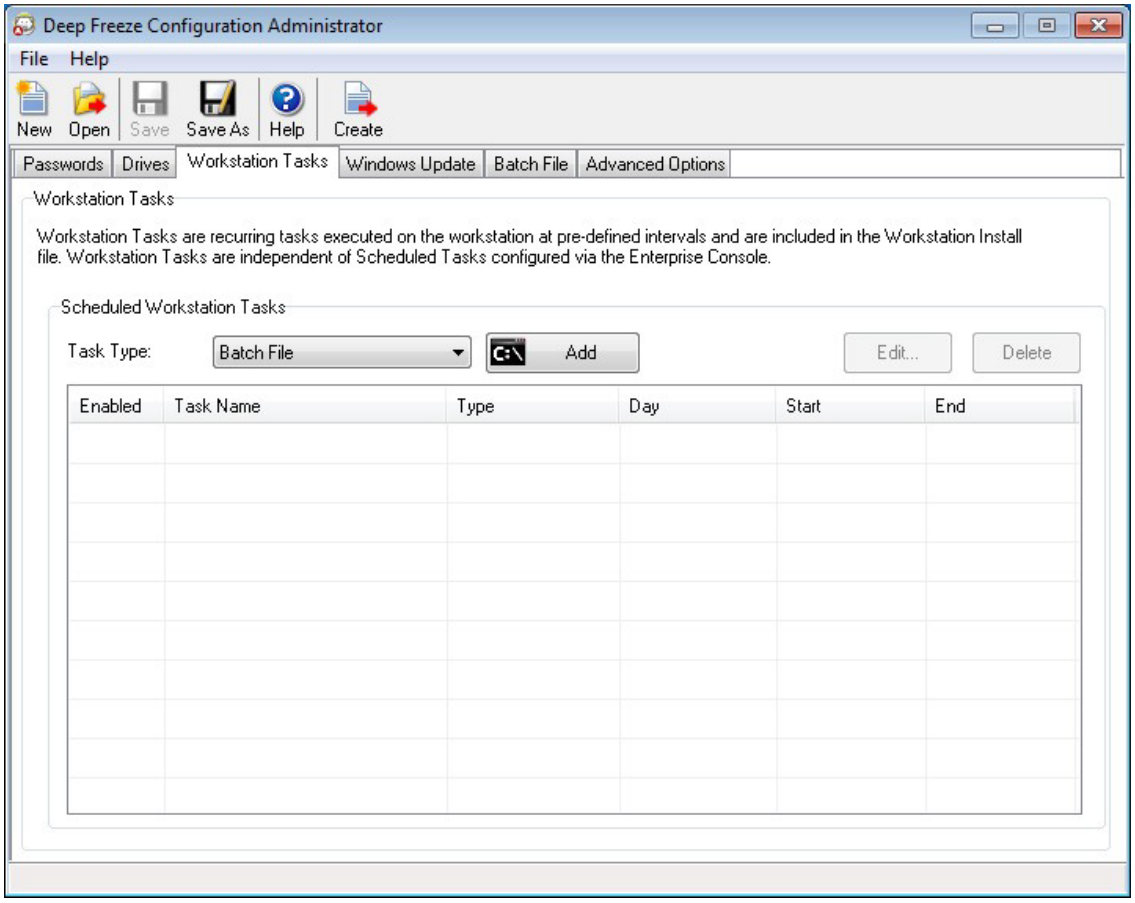
3. Click *OK*.

Example

In the above screen, the Idle Time task is set to *Restart* when the computer is idle for 1 minute. A message is displayed to the user for 1 minute after the idle time has elapsed. The computer will restart unless the user cancels the task in the message dialog displayed.

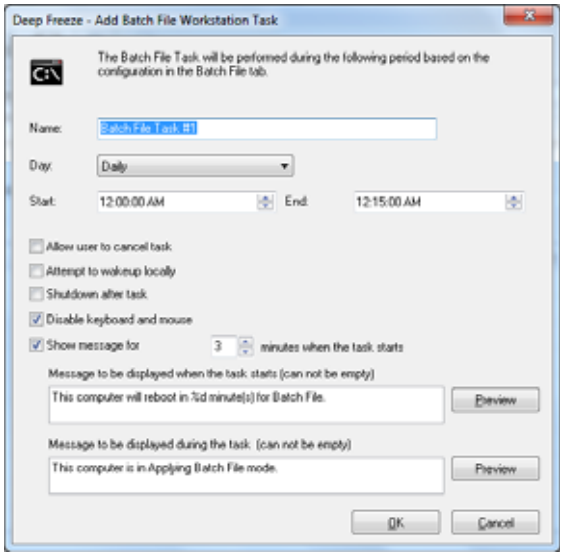
Batch File

Batch File tasks are scheduled for executing batch files on the workstation. A Batch File task has a Start Time and an End Time. During this period, the batch file is executed on the workstation. You must configure additional settings in the Batch File tab for the Batch File Task to work. You can configure to shutdown the workstation after the Batch File Task is completed. Workstations will reboot *Frozen* after the batch file has been executed.



The Batch File task can be scheduled by completing the following steps:

1. Select *Batch File* from the *Task Type* drop-down and click *Add*.
2. The following options are displayed:



> Name – Specify a name for the task.

> Day – Select the day, or specify if the task will occur on Weekdays or Weekends.

> Start – Select the Start Time.

> End – Select the End Time. The minimum interval is 15 minutes.

> Allow user to cancel the task – Select the checkbox if the user is allowed to cancel the task before it starts.

> Attempt to wake up locally – Select this checkbox to wake up the workstation locally without requiring any communication from the Enterprise Console.



Waking up the workstation locally depends on the hardware specifications of your workstation. This option will work only if it is supported by your hardware.

> Shutdown after task – Select the checkbox to shutdown the computer after the task.

> Disable Keyboard and Mouse – Select the checkbox to disable keyboard and mouse during the task.

> Show message – Select the checkbox to display a message on the computer *Before* and *During* the task. Specify the time interval in minutes and enter a brief message to be displayed before the task starts.

3. Click *OK*.

4. Go to Batch File Tab to configure additional settings.

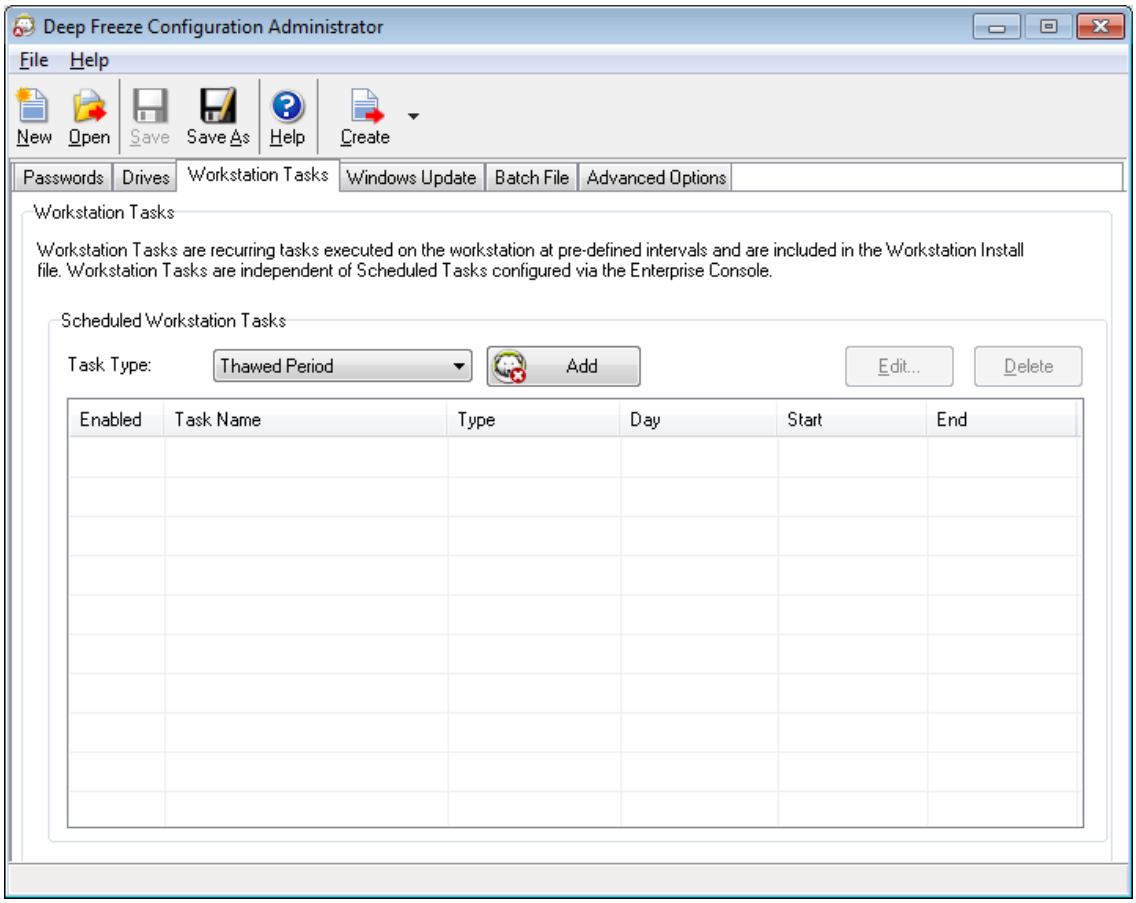
> The message *This computer will reboot in %d for Batch File* is displayed in the *Message to be displayed before the task* field. This message can be edited. Add the word *minutes* in the message after *%d* to include the word minutes as part of the message.

Example

In the above screen, a Batch File task has been created to execute a Batch File at the computer daily at 12:00 AM and end at 12:15 AM. The task is configured to display a message to the user before the Batch File is executed. The keyboard and mouse are disabled.

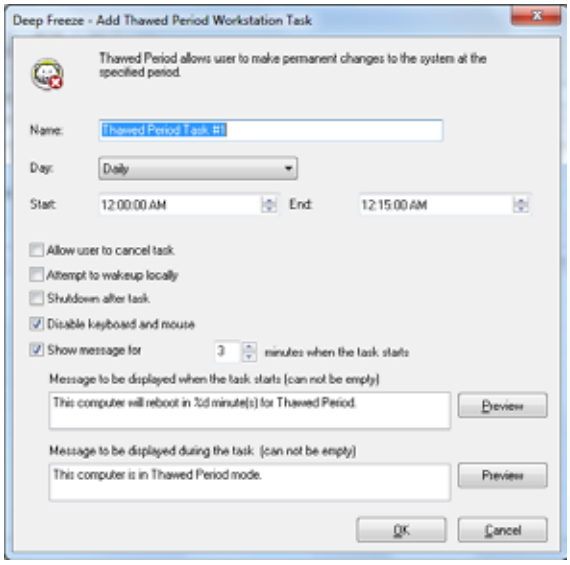
Thawed Period

Thawed Period tasks are scheduled to reboot the workstation is in a Thawed state. A Thawed Period is useful for some applications that update automatically at regular intervals. A Thawed Period is also useful for administrators to schedule maintenance and make permanent changes to the computers. This may include installing new software, updating software, configuration changes, and other maintenance functions. A Thawed Period has a Start Time and an End Time.



The Thawed Period can be scheduled by completing the following steps:

1. Select *Thawed Period* from the *Task Type* drop-down and click *Add*.
2. The following options are displayed:



> Name – Specify a name for the task.

> Day – Select the day, or specify if the task will occur on Weekdays or Weekends.

> Start – Select the Start Time.

> End – Select the End Time. The minimum interval is 15 minutes.

> Allow user to cancel task – Select the checkbox if the user is allowed to cancel the task before it starts.

> Attempt to wake up locally – Select this checkbox to wake up the workstation locally without requiring any communication from the Enterprise Console.



Waking up the workstation locally depends on the hardware specifications of your workstation. This option will work only if it is supported by your hardware.

> Shutdown after task – Select the checkbox to shutdown the computer after the task.

> Disable Keyboard and Mouse – Select the checkbox to disable keyboard and mouse during the task.

> Show message – Select the checkbox to display a message on the computer *Before* and *During* the task. Specify the time interval in minutes and enter a brief message to be displayed before the task starts.

3. Click *OK*.



The message *This computer will reboot in %d for Maintenance* is displayed in the *Message to be displayed before the task* field. This message can be edited. Add the word *minutes* in the message after *%d* to include the word minutes as part of the message.

Example

Anti-Virus programs require regular virus definition updates to protect the system. Virus definitions can be updated during a Thawed Period.

In the above screen, a Thawed Period task has been created daily between 12:00 AM and 12:15 AM. The user is not allowed to cancel the task before it starts. The computer will shut down after the maintenance period. The keyboard and mouse are disabled during the maintenance period. The task is configured to display a message to the user 5 minutes before the task starts. The following message will be displayed on the computer at 11:55 PM: *The computer will reboot in 5 minutes to enter into a Thawed Period*.

To ensure that the virus definitions are applied permanently, schedule the virus definition update for your Anti-Virus program so that it starts *after* Deep Freeze successfully starts the Thawed Period task and *ends* before Deep Freeze ends the Thawed Period task. This ensures that the virus definitions downloaded and updated by the Anti-Virus program stay permanently on the system. Hence the system is fully protected by Anti-Virus and Deep Freeze.

Faronics Anti-Virus: Faronics Anti-Virus works with Deep Freeze and does not require a Thawed Period task for updating virus definitions. Faronics Anti-Virus can update virus definitions even when the computers managed by Deep Freeze are in a *Frozen* state.

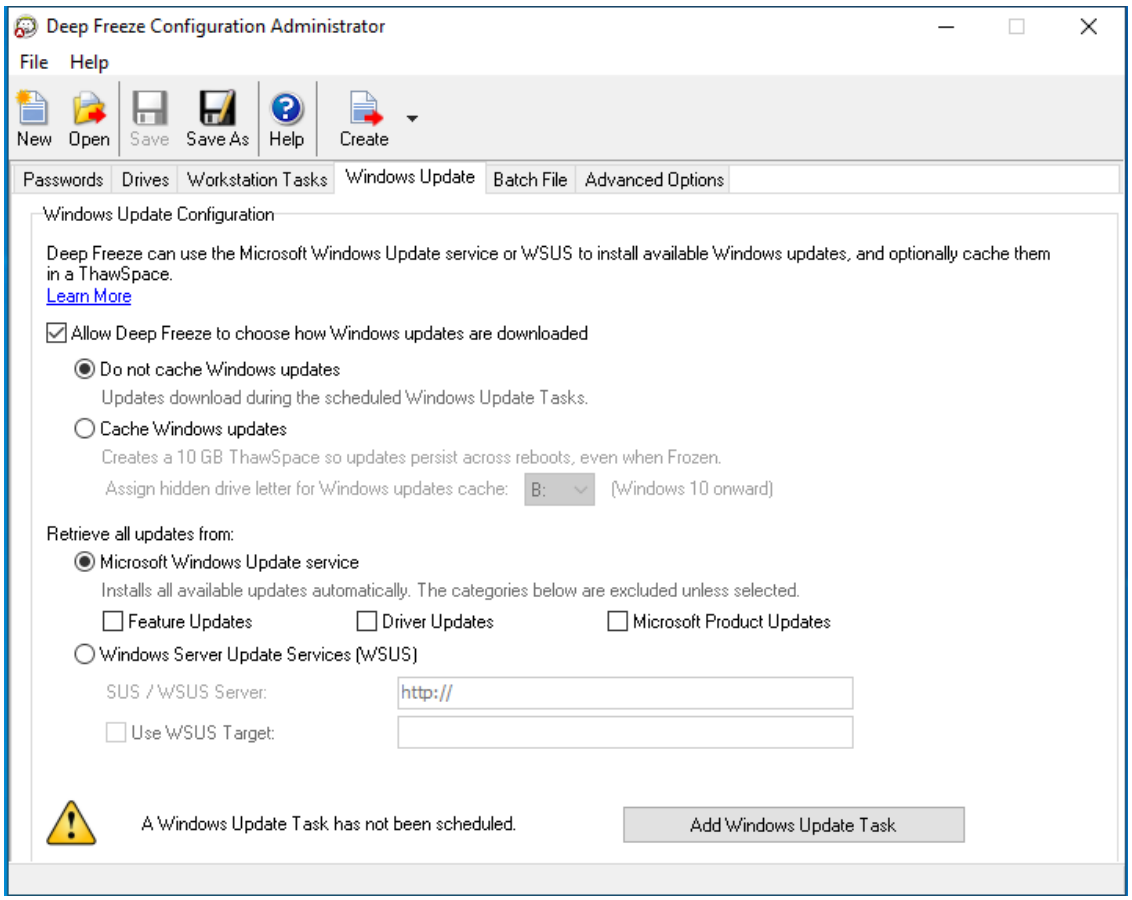


Other Anti-Virus Programs: All other Anti-Virus programs require scheduling a Thawed Period task to update virus definitions. Refer to your Anti-Virus program user guide for information on how the virus definitions are downloaded. Alternatively, virus definitions can be applied manually when the computers managed by Deep Freeze are in a *Thawed* state. You can also schedule a *no user intervention* install of your virus definitions through a Batch File Task.

Windows Update Tab

The Windows Update tab allows you to customize settings for Windows Update. When you first create a Windows Update Task, you will be given an option to modify the default settings in the Windows Update tab. Modifying the default settings is not mandatory. Windows Update will be performed even with the default settings. The settings in the Windows Update tab will apply to all Windows Update tasks.

The Deep Freeze Windows Update tab settings override the Windows Update settings on the workstation.



The settings in the Windows Update tab can be customized as follows:

Allow Deep Freeze to choose how Windows updates are downloaded: – Select this checkbox to allow Deep Freeze to choose how Windows updates are downloaded. The following options are available:

- Select the Windows Updates download options:

> Do not cache Windows updates – Select this option to download Windows updates only during the Windows Update task.

> Cache Windows updates – Select this option to download when the workstation is in a Frozen or Thawed state and install during the Windows Update Task. This option creates a 10 GB ThawSpace and the Windows Updates are stored in the ThawSpace to ensure that Windows Update files are persistent across multiple reboots.

For Windows 10 and above – When Cache Windows updates is selected, the drive letter drop-down list is enabled. Select a drive letter from the drop-down list to assign as the hidden drive letter for storing Windows Updates cache. The assigned hidden Windows Updates cache drive letter will not be visible in Windows Explorer.



The hidden drive letter is not visible on the workstations and is only available for Windows 10 and above.

- Always retrieve updates from:

> Microsoft Windows Update website – Select this option to download updates directly from the Microsoft Windows Update website.

Selecting this option will download and install all updates automatically except *Feature Updates, Driver Updates*, and *Microsoft Product Updates*. These update types will be installed only if they are selected separately.

> Windows Server Update Services (WSUS) – Select this option to download from WSUS server. Specify the *SUS/WSUS Server*. Optionally, select *Use WSUS Target* and specify the target. Microsoft SUS client and SUS/WSUS server can be downloaded at: http://www.microsoft.com/wsus.



A log file is created for each individual workstation and is stored locally on the workstation.

The default name for the Deep Freeze Windows Update Log file is *DFWuLogfile.log* and can be found at:

C:\Program Files\Faronics\Deep Freeze\Install C-[X]\DFWuLogfile.log (32-bit systems) and C:\Program Files (x86)\Faronics\Deep Freeze\Install C-[X]\DFWuLogfile.log (64-bit systems).

- You cannot change the name or location of the log file.
- The Deep Freeze Log file and the Windows Update log file (at C:\windows\windowsupdate.log) are very useful for troubleshooting your Windows updates.
- X is an incremental value depending on how many times you have installed Deep Freeze on the workstation.

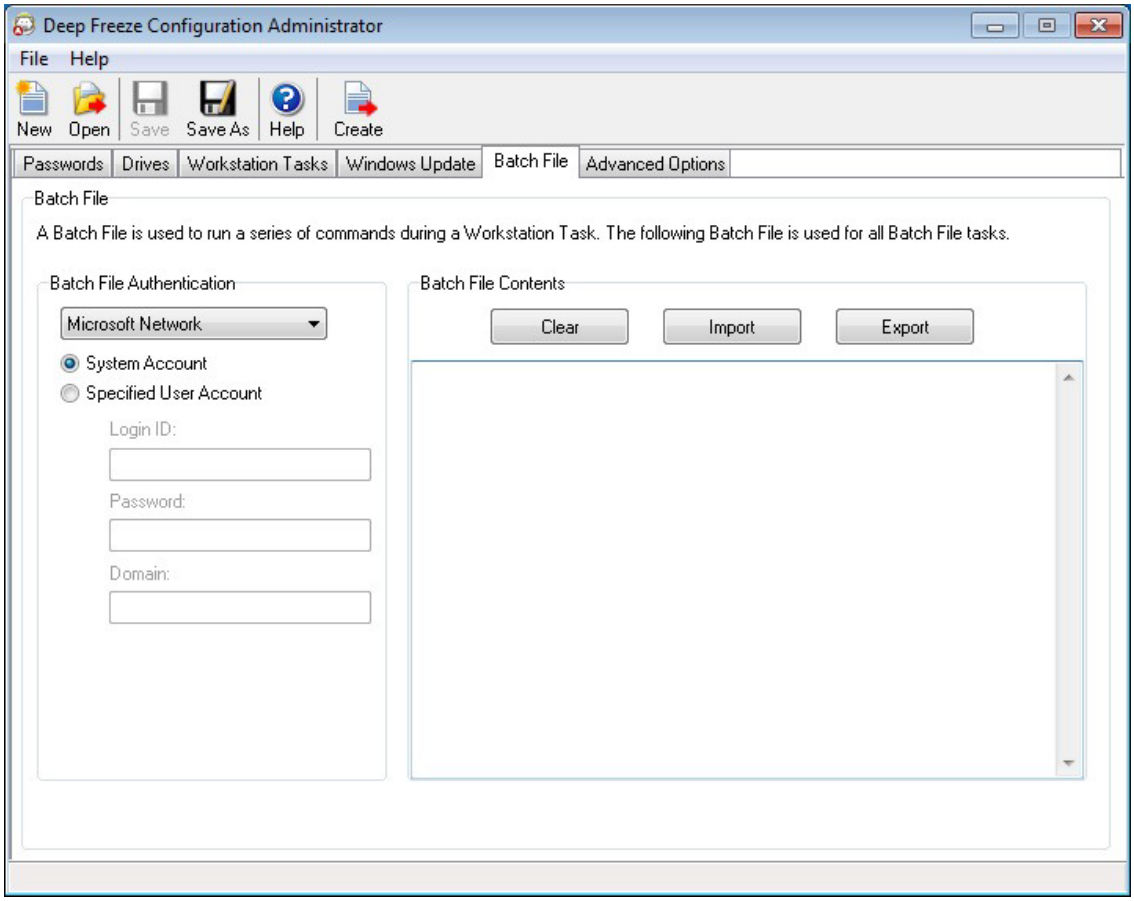
Contact Faronics Support for help troubleshooting the DFWuLogfile.log (at http://support.faronics.com).

Contact Microsoft Support for troubleshooting Windows Update Errors. (See http://support.microsoft.com/kb/906602)

Also see Microsoft KB 902093 *How to read the Windows Update log file* found at: http://support.microsoft.com/kb/902093/ or visit http://support.microsoft.com.

Batch File Tab

The Batch File tab allows you to customize settings for the Batch File task. When you schedule a Batch File task from the Workstation Tasks tab, you must configure the settings in the Batch File tab.



Configure the following options:

- Batch File Authentication

  Select Microsoft Network and select if the account to be used is a System account or a Specified user account. If you select Specified user account, specify the Login ID, Password, and Domain. For Novell Network, select Novell, specify the Login ID, Password, Tree, Context, and Server.



The default configuration using the Microsoft Network/System Account authentication must be tested prior to using alternative credentials. Using this machine level account often is sufficient to complete the task.

Use of a specified user account may be required if the batch file requires network access to secure resources.

- Batch File Contents

  Enter a custom batch file to run during the Batch File task. The same batch file applies to all Batch File tasks. The following options are available when running custom batch files:

  > To clear the current batch file, click *Clear.*

  > To load an existing file, click *Import* and browse to the location of the file.

  > To save the contents of the field, click *Export* and browse to the preferred save location.

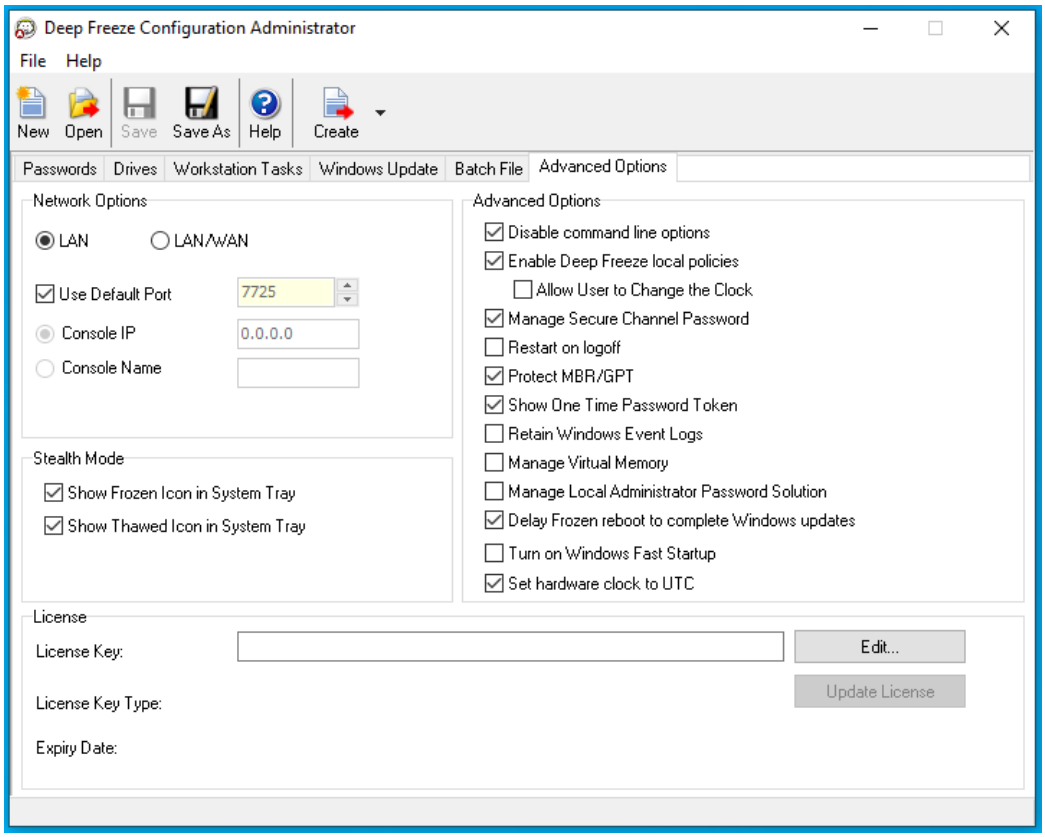
  The batch file can be any command or series of commands that the command processor can run. You can run custom scripts that require the use of a third-party scripting engine by calling the script from the batch file as if it was being run from the command line.



Batch Files allow you to use VB Scripts, PowerShell scripts, Ninite and other third-party solutions. Contact your software vendor or refer to your third-party solution user guide to know more about scripting solutions that include *no user intervention* options.

Advanced Options Tab

The Advanced Options tab is used to configure the network settings used by the computers to communicate with the Console, configure various security options, and administer License Keys.



Network

Communication between the Deep Freeze Enterprise Console and computers with Deep Freeze installed can use two different modes: LAN Mode or LAN/WAN Mode.

- LAN – Select LAN to configure Deep Freeze to communicate within a Local Area Network (LAN). LAN mode is a self-configuring mode that requires only a port number. The default port is 7725. The port number can be changed if it is in conflict with other programs on the LAN. In LAN mode, the Deep Freeze target computer and the Enterprise Console find each other through UDP broadcasts. These broadcasts only occur when computer or the Enterprise Console is started, ensuring that there is little network traffic associated with target computer and Console communication.
- LAN/WAN – Select LAN/WAN to configure Deep Freeze to communicate in both a LAN and a WAN (wide area network). LAN/WAN can be used in either a LAN or WAN environment and over the Internet. This mode uses an IP address or the computer

name, along with a port number, to allow communication between the Enterprise Console and the managed computers.

The following two methods are available to identify the Console:

- Specify the Console IP, which must be static
- Specify the Console Name, in which case the IP can be dynamic (if valid DNS name resolution is available as part of the domain infrastructure).

When the Enterprise Console is behind a firewall or a NAT (network address translation) router, the firewall or router must be configured to allow traffic to pass through to the Enterprise Console. Depending on the firewall or router, computers may need to be configured with the IP address of the firewall so that traffic can be forwarded.



Deep Freeze automatically configures the required exceptions in the Windows Firewall. It is not required to configure the Windows Firewall manually.

For more information on configuring and using Deep Freeze in a specific network environment, refer to Appendix B or contact Technical Support.

If a port number other than the default of 7725 (registered to Deep Freeze) is used, care should be taken to ensure that there are no conflicts with applications already running on the network. Well-known ports (0–1023) should be avoided and any Registered Ports (1024–49151) should be checked for conflicts before deployment.



It is recommended to use ports in the unallocated range above 49152. Using Port Segmentation, you can isolate a lab or building by port number by configuring the Port Number on the workstations and in the Deep Freeze Enterprise Console. Using this method, you can provide management functions for a specific set of workstations and not your entire organization. UDP and TCP port exceptions for these ports will be required. For more information, refer to Example 3: Multiple Ports, Console Accessed Remotely.

A complete listing of the ports assigned to various applications can be found on the Internet Assigned Numbers Authority web site at http://www.iana.org/assignments/port-numbers.

Advanced Options

- Disable Command Line options – This option is selected by default. Clearing this checkbox allows for further customization of the Deep Freeze installation program when using the Silent Install System. Selecting this option prevents the pre-existing configuration choices from being changed during installation.
- Enable Deep Freeze local policies – For enhanced security, Deep Freeze removes the following local privileges: debugging programs, modifying firmware, and changing the system time; clear this option to use existing privileges.

- Allow user to change the clock – Select this option to allow Frozen users to adjust the system clock. Enable this feature during Daylight Savings to allow Windows to update the time automatically each season.
- Manage Secure Channel Password – Secure Channel Password is a feature of all Windows operating systems and only applicable if the system is running in Windows Server Domain Environment. Secure Channel Password is used for secure communication between the server and workstations. The Secure Channel Password is automatically changed based on the operating system settings. While using Deep Freeze, the newly changed Secure Channel Password is lost on reboot. The *Manage Secure Channel Password* option avoids this situation. The Manage Secure Channel Password feature of Deep Freeze changes the value of the Group Policy *Maximum machine account password age* based on the Deep Freeze state (*Frozen* or *Thawed*).

  > Select the *Manage Secure Channel Password* option if you want Deep Freeze to manage Secure Channel Password.

    When the workstation is Frozen – The workstation will not change the Secure Channel Password. This ensures that the secure communication between the server and the workstation is always maintained.

    When the workstation is Thawed – The workstation will change the Secure Channel Password and sync the password with the server.

  > Do not select the *Manage Secure Channel Password* option if you do not want Deep Freeze to manage the Secure Channel Password.

    When the workstation is Frozen – When the Secure Channel Password is changed and synced with the server, it resets to the old password on reboot.

    When the workstation is Thawed – If the workstation is *Thawed* on the day the Secure Channel Password is changed, the new password takes affect and the workstation is synced with the server.



The Manage Secure Channel Password feature of Deep Freeze always overrides the Group Policy *Maximum machine account password age* and *Disable machine account password changes*.

Set the following in the Group Policy for the Manage Secure Channel Password feature to work:

Domain Controller: Refuse machine account password changes to *Not Defined*

- Restart on Logoff – Select this checkbox to Restart the computer automatically when it is logged off. If this option is selected, the computer is restarted when a user logs off in a Frozen state.
- Protect MBR/GPT – Select this checkbox if you want Deep Freeze to protect the Master Boot Record or the GUID Partition Table. If this option is selected, changes to the Master Boot Record are reversed on reboot when the computer is in a Frozen state.
- Show One Time Password Token – When this option is selected, the OTP Token will be displayed on the password entry dialog on the Deep Freeze workstation.

  If OTP feature is not used, it is recommended to keep this option disabled.

- Retain Windows Event Logs – Select this checkbox to retain Windows Event Logs. Deep Freeze creates a 100 MB ThawSpace and stores all Windows Event Logs so they are not erased upon reboot even when the computer is in a Frozen state. The log file is recycled once it reaches 100 MB. The log files contain events related to Application, Hardware, System and Security.

  If a larger Event Log size is detected on the local workstation, the ThawSpace will automatically grow to accommodate this requirement.

- Manage Virtual Memory – Enable this for rare cases where hardware with limited RAM may experience performance issues. Selecting this option allows Deep Freeze to manage the page file size.

  This option is disabled by default. The page file size will be adjusted to match the RAM size if this option is enabled, which will allocate more hard drive space on the workstation.

- Manage Local Administrator Password Solution – Local Administrator Password Solution (LAPS) is a Windows feature that automatically manages and backs up the password of a local administrator account on Active Directory-joined or Windows Server Active Directory-joined machines.

  When this option is enabled on systems where LAPS setup is detected, Deep Freeze will disable the ability of LAPS to change the configured local admin password in Frozen state and allow to do so in Thawed state. This feature ensures that the current admin password can be rotated only in Thawed state and remain synchronized with Active Directory.

- Delay Frozen reboot to complete Windows updates – Select this option to delay reboot into a Frozen state if configuration or installation for Windows updates are pending. If you select this option and perform Windows updates (through means other than Deep Freeze), rebooting into a Frozen State will ensure that all Windows updates installation and configuration are completed before rebooting into a Frozen state.

  If you select *Delay Frozen reboot to complete Windows updates* and install Deep Freeze, the installer checks if all Windows updates are completed. If the Windows updates are not completed, Deep Freeze installation will not proceed. Complete Windows updates and try installing Deep Freeze again.

  If you disable *Delay Frozen reboot to complete Windows updates* and install Deep Freeze, ensure that all Windows updates are completed manually. Disabling this option may result in the computer being stuck in a reboot cycle due to incomplete Windows updates.

- Turn on Windows Fast Startup – Specifies whether the Windows Fast Startup (hybrid shutdown) feature is enabled on the workstation. When enabled, a shutdown hibernates the kernel session instead of closing it, and the next power-on resumes that session rather than performing a full boot, which reduces startup time. Restart operations are unaffected.

  Fast Startup bypasses the full boot cycle that Deep Freeze relies on to restore the Frozen state. After a shutdown and power-on, changes made in the Frozen state may not be discarded. Disable this option where the Frozen state must be restored on every startup.

- Set hardware clock to UTC – Select this option to allow the system to automatically adjust the time during Daylight Saving Time changes on workstations that do not synchronize with an Internet time server.

  When this option is disabled, Deep Freeze will attempt to correct the system time after the next Frozen startup. The correction may take up to 30 seconds. During this interval, the system clock may be inaccurate, which could temporarily affect applications or services that require accurate system time.

Example

On a Windows Domain Environment using Windows Server 2008 R2 that manages multiple workstations, Secure Channel Password is used for secure communication between the server and workstations.

In Deep Freeze Enterprise Configuration Administrator, go to the *Advanced Options* tab and select *Manage Secure Channel Password*. Create the Workstation Install file and deploy it to the workstation.

Set the following in the Group Policy for the Manage Secure Channel Password feature to work:

Domain Controller: Refuse machine account password changes to *Not Defined*

Domain Member: Disable machine account password changes to *Disabled*

When the workstation is Frozen, the Secure Channel Password does not change. When the workstation is Thawed, the Secure Channel Password is changed at the workstation and synced with the server.

Stealth Mode

- Show Frozen icon in system tray – Select this option to display the icon to indicate that Deep Freeze is installed and the computer is Frozen.
- Show Thawed icon in system tray – Select this option to display the icon to indicate that Deep Freeze is installed but the computer is Thawed.

If the options to show a Deep Freeze icon in the System Tray are unchecked, the keyboard shortcut CTRL+ALT+SHIFT+F6 must be used to access the logon dialog.

License

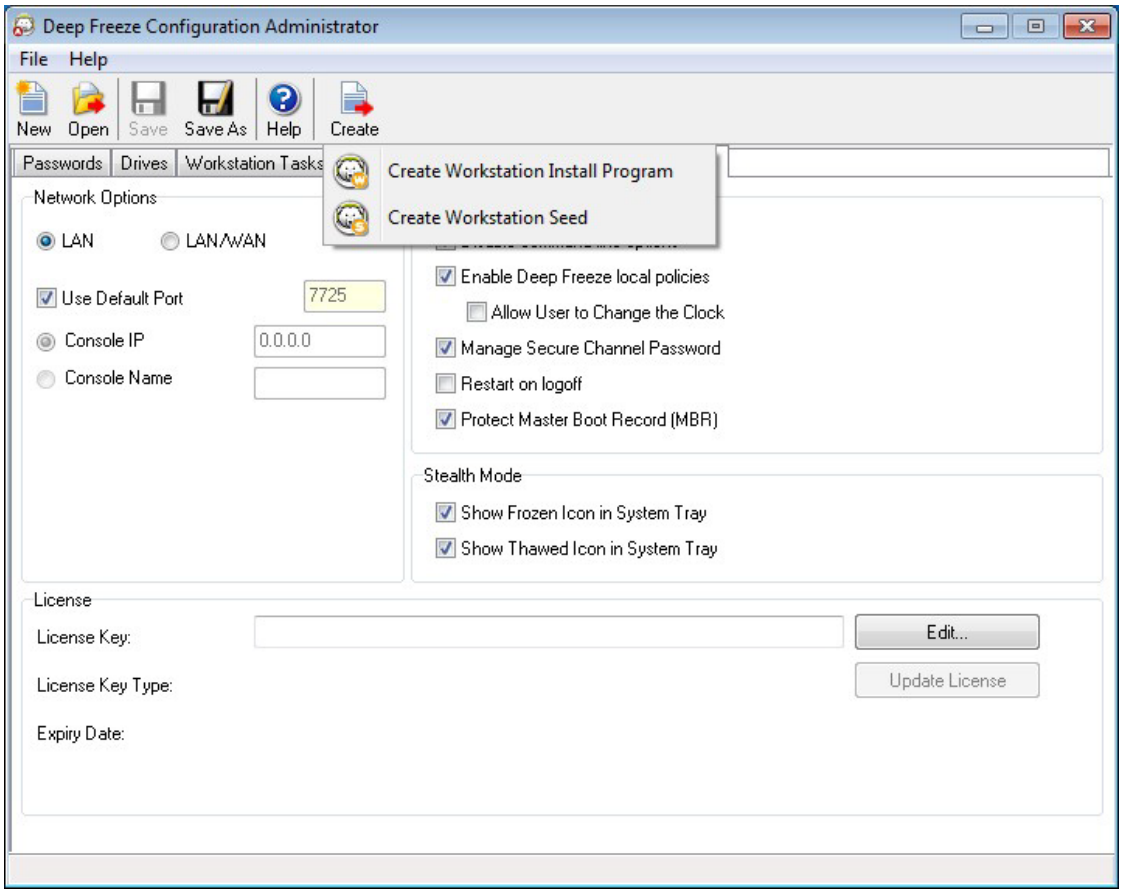
- License Key – Click *Edit* and enter the License Key. Click *Update License*.
- License Key Type – The License Key type is displayed. This field displays if this is an Evaluation version or a full version.
- Expiry Date – The *Expiry Date* for Deep Freeze is displayed.

The License Key can be updated in the following ways:

- Through the Workstation Install file – The License Key is updated in the Configuration Administrator and a Workstation Install file is created. The License Key is now part of the Workstation Install file.

- Through the Enterprise Console – The License Key can be updated directly on the Enterprise Console. When the License Key is updated in the Enterprise Console, it is automatically updated on all connected computers. For more information on updating directly through the Enterprise Console, refer to the Licensing section.
- Manually on each computer – The License Key can be updated manually on each computer. For more information, refer to the Status Tab section.

Creating Workstation Install Program and Workstation Seed



To create customized Deep Freeze installation program files with all of the options that were configured in the previous sections, click the *Create* button in the Configuration Administrator toolbar and select *Create Workstation Install Program*.



The default file name for this program is DFWks.exe. We recommend that you keep the default name, but in larger deployments you may want to suffix it with information related to its configuration such as: *DFwks_10gbThawSpace.exe* or *DFWks_NoMaintenance.exe* or *DFwks_Wed-5pmUpdates.exe* to assist in organization and identification of the installer functions. The same recommendation applies for *Deep Freeze Configuration* files (.rdx) as well.

This file can then be used to install Deep Freeze on computers using:

- Attended Install (install based on user input).
- Silent Install system – Install that does not inform user of progress or provide messages during installation). For more information on the Silent Install command, refer to Silent Install or Uninstall.
- Target Install – Through the Deep Freeze Enterprise Console for workstations that already contain a Seed or previous version of Deep Freeze that has been created with the same Customization Code.

To create a Workstation Seed, click the *Create* button in the Configuration Administrator toolbar and select *Create Workstation Seed*. The Workstation Seed is a lightweight program that allows administrators to remotely install and control computers from the Enterprise Console. The Workstation Seed can be installed as part of a master image and then deployed via imaging software. All computers on the LAN with the Workstation Seed installed are displayed in the Enterprise Console. The default file name for this program is *DFWksSeed.exe*.

All files are saved to *Deep Freeze Enterprise > Install Programs* folder by default. A different location can be chosen and the file name can be changed if required. To set up another location as the default location, select the preferred location for saving the installation programs and Workstation Seeds and click *Save*. Check the *Set this folder as the default location save location* checkbox when prompted. Click *OK*.

It is recommended that a naming convention is used if you are creating multiple customized installation files.



DFwks.exe, *DFwksseed.exe,* and *DepFrz.rdx* files can be created and deployed interchangeably to any Deep Freeze computer that uses the same Customization Code. The Deep Freeze Seed can be used as a template/place holder to ensure your basic elements such as passwords, Network Configuration or standardized workstation tasks are all consistent. The seed will not utilize any of the configuration settings but will hold them in the file. To use the file as a template simply open the *DFwksseed.exe* file using the Configuration Administrator and make any required changes. Then, to create workstation installation click *Create > Create Workstation Installation File*.



It is recommended to restrict the use of the Configuration Administrator in larger environments for security reasons. This can be done by password protecting the Deep Freeze Administrator or alternatively, making it unavailable by removing the DFadmin.exe file from the *C:\program files\faronics\Deep Freeze Enterprise* folder. This file can be moved to the Domain Administrator's workstation and deleted from the Common Deep Freeze Enterprise Console. It can be restored by copying it from another installation of the same version and authorizing using the OTP password or by reinstallation or upgrade of Deep Freeze Enterprise using the same Customization Code.



Using Deep Freeze Enterprise Console

This chapter describes using the Deep Freeze Enterprise Console.

Topics

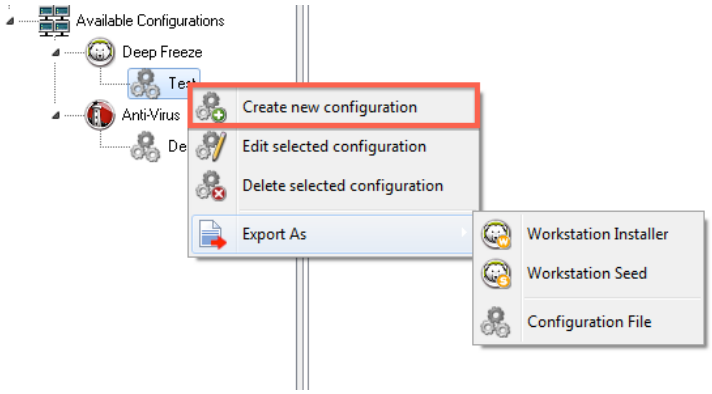
Deep Freeze Configuration
Configuration Generator
Deep Freeze Enterprise Console
View Columns
Status Based Selection
Managing Communication Between the Console and Workstations
Remote Consoles
Connecting to a Remote Console
Managing Deep Freeze with the Console
Licensing
Reports
Tags
Notes
Scheduling Deep Freeze Tasks
Assigning Computers to Scheduled Tasks
Managing Network and Groups
History
Adding Computers to a Group
Configure Custom Actions
Console Customizer
Deep Freeze Enterprise Console Shutdown
Installing Deep Freeze on the Workstation
Uninstalling Deep Freeze on the Workstation via the Console
Silent Install or Uninstall
Check for Updates

Deep Freeze Configuration

Deep Freeze Configuration is a group of settings that defines the behavior of Deep Freeze on the workstation. Deep Freeze Configurations can be created and applied through the Deep Freeze Console.

Complete the following steps to create a Deep Freeze configuration:

1. Launch Deep Freeze Console.
2. Go to *Network and Groups* > *Available Configurations* > *Deep Freeze.*
3. Right-click and select *Create New Configuration*.



4. Select or specify the settings for each tab as described in Using Deep Freeze Enterprise Configuration Administrator.
5. Specify the name of the configuration and click *OK*.
6. Optionally, select *Export As* > *Workstation Seed* or *Export As* > *Workstation Installer* from the drop-down to export the configuration.
7. Click *OK*.

Applying Deep Freeze Configuration

Once a configuration is created, it can be applied to multiple workstations.

Complete the following steps to apply the Deep Freeze configuration:

1. Go to *Workstations* pane.
2. Select one or more workstations.
3. Right-click and select *Update Configuration* > *Deep Freeze* > *[Configuration Name]*.

The configuration is applied on the selected workstation(s).

If you change the Deep Freeze Configuration for Passwords, Workstation Tasks, or Restart on Log off, and apply the configuration, the settings are applied on the fly.

If the *Delete during configuration update* option was selected when creating the install file, existing ThawSpaces and the data in the ThawSpaces will be deleted and the new ThawSpaces as per the settings will be created when the configuration is applied.

All other settings require a reboot for the settings to take effect. *Disable Command Line* changes cannot be modified by applying configuration changes.

Editing Deep Freeze Configuration

Complete the following steps to edit the Deep Freeze configuration:

1. Go to Networks and Groups Pane in Enterprise Console.
2. Select *Available Configurations* > *Deep Freeze* > *[Configuration Name]*.
3. Right-click on the selected configuration and select *Edit Selected Configuration.*
4. Edit the settings as required.
5. Click *OK*.

Deleting Deep Freeze Configuration

Complete the following steps to delete the Deep Freeze configuration:

1. Go to Networks and Groups Pane in Enterprise Console.
2. Select *Available Configurations* > *Deep Freeze* > *[Configuration Name]*.
3. Right-click on the selected configuration and select *Delete Selected Configuration.*
4. Click *OK*.

Exporting Deep Freeze Configuration

Complete the following steps to export the Deep Freeze configuration:

1. Go to Networks and Groups Pane in Enterprise Console.
2. Select *Available Configurations* > *Deep Freeze* > *[Configuration Name]*.
3. Right-click on the selected configuration and select *Export As.* There are three options:
   - > Select Workstation Installer. Specify a name and click *Save*.
   - > Select Workstation Seed. Specify a name and click *Save*.
   - > Select Configuration File. Specify a name and click *Save*.

Configuration Generator

Deep Freeze Console provides a tool called the Configuration Generator to automatically create Deep Freeze Installation or Deep Freeze Configuration files based on the parameters specified in a CSV file. A Sample CSV file is provided which can be edited to include unlimited entries. The parameters for the settings in CSV file are identical to the settings in the Deep Freeze Enterprise Configuration Administrator. The column title in the CSV file represents the particular setting and the row represents an entry for a single Deep Freeze Configuration or Deep Freeze Installation file.

Complete the following steps to generate multiple Deep Freeze Installation files using the Configuration Generator:

1. Launch Deep Freeze Console. Go to *Tools* > *Configuration Generator*. Alternatively, you can also launch it from the Deep Freeze Enterprise Configuration Administrator from *File* > *Configuration Generator*.



2. Click *Browse* in the Configuration Generator.
3. Select the configuration file (.csv) file.
4. Click *Generate*.

Deep Freeze Installation file or Deep Freeze Configuration files are created.

If you are using the Configuration Generator for the first time, click *Sample CSV* to download a template of the file. You can update the Sample CSV file with the values required for generating the Deep Freeze Installation or Deep Freeze Configuration files. It is recommended to save the file with a more descriptive name.

Using Configuration Generator from Command Line

You can also generate the Deep Freeze Installation or Deep Freeze Configuration files from the command line. Launch the command line from the Deep Freeze Installation location, provide the following parameters and press enter:

32-bit systems:

```
[System Drive]:\Program Files\Faronics\Deep Freeze
Enterprise\DFAdmin.exe import [PATH\ConfigurationFile.csv]
```

64-bit systems:

```
[System Drive]:\Program Files (x86)\Faronics\Deep Freeze
Enterprise\DFAdmin.exe import [PATH\ConfigurationFile.csv]
```

The Deep Freeze Installation or Deep Freeze Configuration files are generated and saved in the location specified in the CSV file.

If you are running the command in synchronous mode, specify the command as follows:

```
start /wait [System Drive]:\Program Files\Faronics\Deep Freeze
Enterprise\DFAdmin.exe import [PATH\ConfigurationFile.csv]
```

Configuration File Parameters

The following table explains the parameters in the Configuration File:

- Do not modify the column headings. Modifying the headings will lead to Deep Freeze ignoring the particular cell values. The default values in the Deep Freeze Enterprise Configuration Administrator will be used.
- For parameters with multiple entries, add multiple columns. For example, Passwords, ThawSpaces etc., can have multiple columns like *Password1Enable, Password2Enable*, *ThawSpace1Drive*, *ThawSpace2Drive*.
- Leaving the entry blank or deleting an entire column will use the default value in the Deep Freeze Enterprise Configuration Administrator. If the mandatory fields have no values, or if the columns representing the mandatory fields are deleted, the Deep Freeze Installation or Deep Freeze Configuration files will not be generated. An error message will be generated and stored in the log file. Click the *Review log file for failed configurations* link in the Configuration Generator to view the error log.
- Do not use a comma (,) for the name of the parameter or value.
- Parameter names and values are not case sensitive.
- Fields that require date will use the format yyyy/mm/dd.
- Fields that require time will use the format hh:mm:ss (24-hour clock).

Column/Parameter	Description
FileName	Specify the file name and path where the files will be saved.
rdx	Specify 1 for generating the Deep Freeze Configuration file. Specify 0 to not generate the Deep Freeze Configuration file.
exe	Specify 1 for generating the Deep Freeze Installation file. Specify 0 to not generate the Deep Freeze Installation file.
Password1Enable	Specify 1 for enabling the password 1. Specify 0 to disable the password 1.
Password1Type	Specify Workstation or Command Line.
Password1UserChange	Specify 1 if user is allowed to change. Specify 0 if the user is not allowed to change.
Password1	Specify the password.
Password1TimeOut	Specify 1 if password will timeout. Specify 0 if password will not timeout.
Password1Activation	Specify the password activation date.
Password1Expiration	Specify the password expiration date.
FrozenDrives	Specify the Frozen drive letters in a single line (for example CDEF).
ThawSpace1Drive	Specify the ThawSpace drive letter.
ThawSpace1Size	Specify the ThawSpace size.
ThawSpace1SizeUnit	Specify the unit whether MB or GB.
ThawSpace1HostDrive	Specify the ThawSpace host drive letter.
ThawSpace1Visibility	Specify Visible if the ThawSpace is visible. Specify Hidden if the ThawSpace is invisible.
RetainExistingThawSpace	Specify 1 for retaining the ThawSpace. Specify 0 for deleting the ThawSpace.
HonorGPSettings	Specify 1 to enable Honor Group Policy Settings. Specify 0 to disable Honor Group Policy Settings.
USB	Specify 1 to keep USB external drives Thawed. Specify 0 to keep USB external drives Frozen.

Column/Parameter	Description
FireWire	Specify 1 to keep FireWire external drives Thawed. Specify 0 to keep FireWire external drives Frozen.
LAN_WAN	Specify 1 if the communication between workstation and Deep Freeze Console is LAN/WAN mode. Specify 0 if the communication between workstation and Deep Freeze Console is not LAN/WAN mode.
UseDefaultPort	Specify 1 to use the default port 7725. Specify 0 if the default port is not to be used.
Port	Specify the port.
ConsoleIP_NAME	Specify the Console IP, which must be static or the name.
DisableCMD	Specify 1 to disable the command line. Specify 0 to enable command line.
EnableLocalPolicies	Specify 1 to enable Deep Freeze Local policies. For enhanced security, Deep Freeze removes the following local privileges: debugging programs, modifying firmware, and changing the system time. Specify 0 to disable Deep Freeze Local policies.
AllowChangeClock	Specify 1 to allow Frozen users to adjust the system clock. Specify 0 if Frozen users are not allowed to adjust the system clock.
ManageSCP	Specify 1 to manage Secure Channel Password. Specify 0 to disable Secure Channel Password.
RestartOnLogoff	Specify 1 to Restart the workstation on logoff. Specify o to disable the Restart the workstation on logoff.
ProtectMBR	Specify 1 to protect the Master Boot Record. Specify 0 if you do not want Deep Freeze to protect the Master Boot Record.
ShowFrozenIcon	Specify 1 to show Frozen icon in the system tray. Specify 0 to hide Frozen icon in the system tray.
ShowThawedIcon	Specify 1 to show Thawed icon in the system tray. Specify 0 to hide Thawed icon in the system tray.
DelayFrozenReboot	Specify 1 to Delay Frozen Reboot to complete Windows Updates. Specify 0 to disable the Delay Frozen Reboot to complete Windows Updates option.

Column/Parameter	Description
BatchAuthentication	Specify 1 for Batch Authentication. Specify 0 for no Batch Authentication.
UserAccount	Specify 1 to use a user account. Specify 0 to use a system account.
LoginID	Specify the login ID.
Password	Specify the password.
Domain	Specify the domain.
Tree	Specify the Tree.
Context	Specify the Context.
Server	Specify the Server name.
BatchFile	Specify the contents of the batch file. Only 1 line is supported.
AllowWUDownload	Specify 1 to allow Deep Freeze to choose how Windows Updates are downloaded. Specify 0 if Deep Freeze will not choose how Windows Updates are downloaded.
CacheWU	Specify 1 to Cache Windows Updates. Specify 0 if Windows Updates are not to be cached.
WSUS	Specify 1 to use WSUS for Windows Updates. Specify 0 if WSUS will not be used for Windows Updates.
UseWSUSTarget	Specify 1 to use a WSUS Target. Specify 0 if a WSUS Target will not be used.
WSUSServer	Specify the URL for WSUS.
WSUSTarget	Specify the WSUS Target.
INCLUDEFEATUREUPDATE	Specify 1 to include Feature Updates. Specify 0 if not including Feature Updates.
INCLUDEDRIVERUPDATES	Specify 1 to include Driver Updates. Specify 0 if not including Driver Updates.
INCLUDEMICROSOFTPRODUCTUPDATES	Specify 1 to include Microsoft Product Updates. Specify 0 if not including Microsoft Product Updates.

Column/Parameter	Description
FASTSTARTUP	Specify 1 to enable Fast Startup. Specify 0 to disable Fast Startup.
ENABLEUTC	Specify 1 to enable UTC. Specify 0 to disable UTC.
Task1Enabled	Specify 1 to enable a Workstation Task. Specify 0 to disable a Workstation Task.
Task1Type	Specify the type of task – Restart, Shutdown, Batch File, Windows Update or Idle Time task. The Start Time for the Idle Time task must be 0:00:00.
Task1Name	Specify the name of the task.
Task1Day	Specify the day.
Task1Start	Specify the start time.
Task1End	Specify the end time.
Task1AllowCancel	Specify 1 to allow user to cancel the task. Specify 0 if a user is not allowed to cancel the task.
Task1ShutdownAfterTask	Specify 1 to shut down the workstation after the task. Specify 0 to if Deep Freeze will not shut down the workstation after the task.
Task1DisableInput	Specify 1 to disable keyboard and mouse. Specify 0 if keyboard and mouse are not to be disabled.
Task1ShowMessageFor	Specify the number of minutes to show message.
Task1StartMessage	Specify the message when the task starts. Only 1 line is supported.
Task1DuringMessage	Specify the message during the message. Only 1 line is supported.

Deep Freeze Enterprise Console

The Deep Freeze Enterprise Console displays the status of all Frozen, Thawed, and Target computers on the network and allows the administrator to perform specific tasks on those computers. Detailed status information is available with selective or group reporting.

To search for a computer, click into the search bar shown on the upper right of the console and enter your search string. You can use wildcards when performing a search. This feature searches throughout all columns.

The Enterprise Console allows administrators to remotely perform the following tasks:

- Immediately Target Install computers
- Selectively Freeze, Thaw, or Thaw Lock one or more computers
- Lock or Unlock selected computers
- Restart or shutdown computers
- Stop scheduled maintenance
- Power on computers equipped with a Wake-on-LAN network card
- Update Deep Freeze software
- Schedule tasks directly from the Console
- Send messages to computers
- Import groups and containers from Active Directory
- Generate One Time Passwords
- Schedule Actions
- Customize the Enterprise Console
- Update the License Key
- Log in a user
- Add tags or notes to computers
- View and export reports about the computer's performance, current status and history

The Enterprise Console can only wake a computer from a powered-down state if the computer is properly configured to power on when a Wake-on-LAN packet is received.

Launching the Enterprise Console

The Enterprise Console is installed with the Deep Freeze Enterprise Configuration Administrator. Open the Console by selecting the following path from the Start menu:

Start > All Programs > Faronics > Deep Freeze Enterprise > Deep Freeze Console

Activating the Enterprise Console

As a security feature of Deep Freeze Enterprise the OTP feature prevents unauthorized Deep Freeze Enterprise Console use. When the DFConsole.exe file is copied to a new computer, the Console must be activated. When it is run for the first time on the new computer, a dialog displays with an OTP Token.

The network administrator enters this token in the Configuration Administrator's OTP Generation System. An OTP is generated. Enter it in the dialog and the Console will run.

The computer on which the Enterprise Console is installed must not have an installation of the Workstation Seed (using the same port) or a full Deep Freeze installation.

Status Icons

The Enterprise Console displays the status of the computers on the local area network with the following icons beside or above the computer name, depending on the view selected:

Classic Look	Modern Look	Definition
		Target: Computers that have the Deep Freeze Workstation Seed installed but do not have Deep Freeze installed; Deep Freeze can only be remotely installed on computers with this icon.
		Computers with Deep Freeze installed in a Frozen state.
		Computers with Deep Freeze installed in a Thawed state.
		Computers with Deep Freeze installed in a Thawed Locked state.
		Computers that are currently powered down.
		Computers that are currently in Maintenance Mode.
		Computers whose communication with the Console has been interrupted.

Classic Look	Modern Look	Definition
		Computers that are Locked.
		Computers that are Thawed for the period longer than defined in the Thawed Alert settings.
		Computers that are Thawed Locked for the period longer than defined in the Thawed Alert settings.

View Columns

Deep Freeze Enterprise Console provides the ability to specify the columns that are displayed in the Workstations pane. Complete the following steps to display the desired columns:

1. Go to *View* > *Columns*.
2. Select the following columns to display:
   - > Configuration
   - > Configuration Date
   - > Expiry Date
   - > Installation File
   - > IP Address
   - > License Status
   - > Login Name
   - > MAC Address
   - > Note
   - > Operating System
   - > Port
   - > Status
   - > Tags
   - > Thawed For
   - > ThawSpace Free (GB)
   - > Version
   - > Workgroup
   - > Workstations
   - > Anti-Virus

Status Based Selection

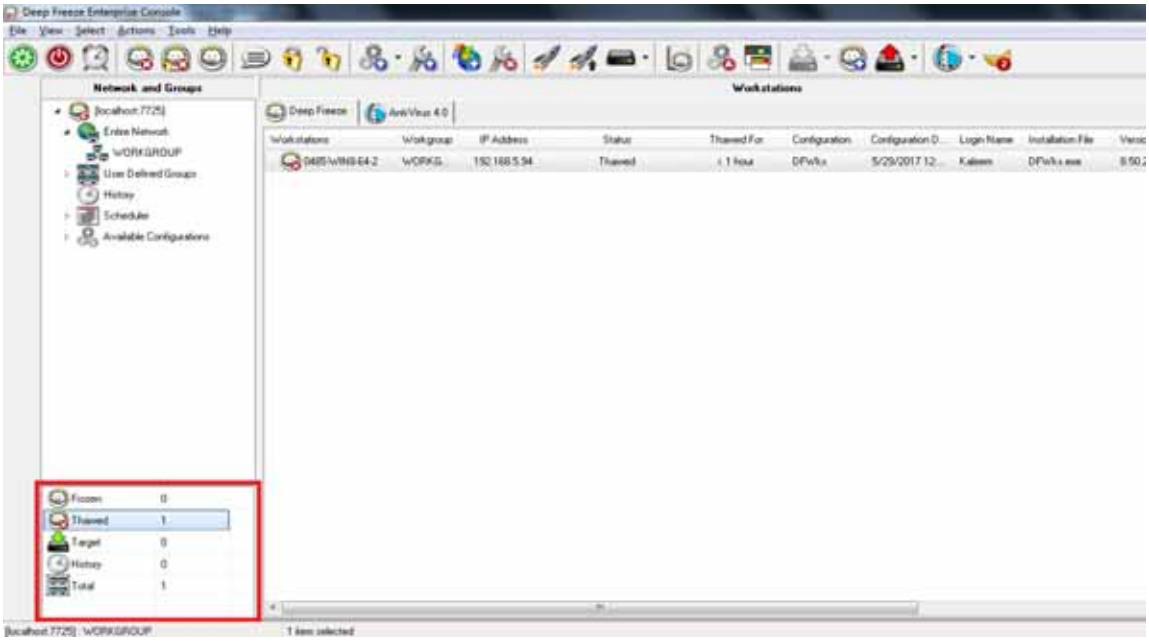
You can select the workstations based on the Deep Freeze status on the managed workstations. The status based selection can be done through the *Select* menu in the Deep Freeze Enterprise Console. The Select menu has the following options:

- Select All Frozen – Selects the workstations in Frozen state. Workstations that are Frozen and Locked are also selected.
- Select All Thawed – Selects the workstations in Thawed state. Workstations that are Thawed and Locked are also selected.
- Select All Target – Selects all the target computers where Deep Freeze can be installed.
- Select All – Selects all workstations.

The following selection options are available from the Status pane as well:

- Frozen – Selects the workstations in Frozen state. Workstations that are Frozen and Locked are also selected.
- Thawed – Selects the workstations in Thawed state. Workstations that are Thawed and Locked are also selected.
- Target – Selects all the target computers where Deep Freeze can be installed.
- History – Displays the history.
- Total – Selects all workstations.

The status pane on Deep Freeze Enterprise Console can also be used to select and display the workstation count for a particular state.



Managing Communication Between the Console and Workstations

There are two types of connections from Console to workstation and Console to Console:

1. Local connections – Connections that can only be accessed by the Enterprise Console that hosts those connections.
2. Remote control enabled connections – Connections that can be accessed by the Console that hosts as well as other Consoles connected remotely.



The Server Service for Deep Freeze 6.5 will not automatically update the Server Service for Deep Freeze 6.4 or lower. Both services can be installed on the same computer, but only one service can run at a time.

A computer can lose communication with the Console for any of the following reasons:

- The computer is powered off manually or is shut down without warning.
- The network is experiencing heavy traffic or outages.
- The computer's network settings are changed to point to a new Console.

In most cases, communication with the computer is re-established when the computer is powered on or when the conditions causing the communications breakdown are rectified. It may take several minutes for the computer to report back to the Console and re-establish communication. If communication cannot be re-established, contact Technical Support for troubleshooting steps.

Configuring the Local Service

The local service is a service that sets up and maintains connections to computers.

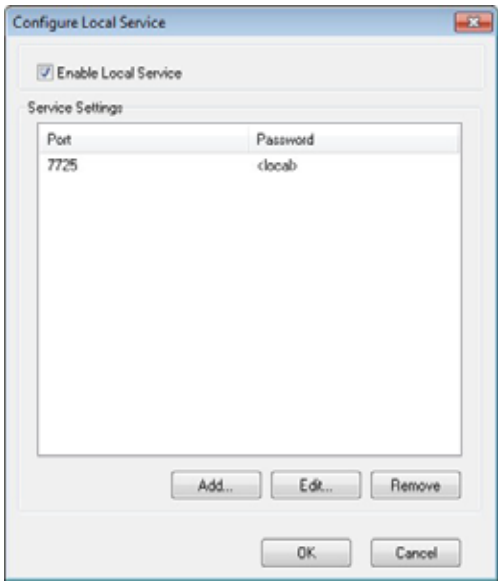
Enabling the Local Service

By default the local service will be installed and enabled when the Console is first run.

To enable the local service again if it has been disabled (and/or uninstalled)

1. Select *Tools* > *Network Configuration*.

2. Select the *Enable local service* checkbox to enable it.



Disabling the Local Service

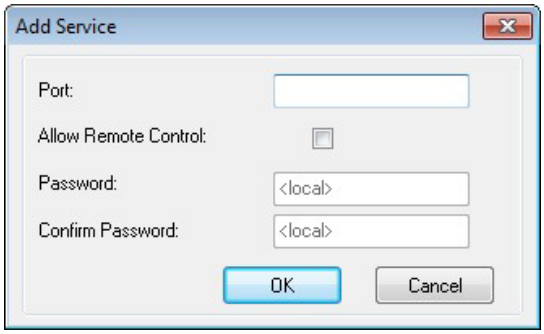
Clearing the *Enable local service* checkbox and clicking *OK* displays the option to either disable the local service or uninstall the local service.



Adding a Local Service Connection

1. To add local service connection, select *Tools >Network Configuration*.
2. To add a connection select Add and specify the port number (7725 in this case).
3. To enable the Console to be controlled remotely, select *Allow Remote Control* checkbox and specify a password.

After selecting *Add*, a connection that serves port 7725 will be created in the connections list of the local service as well as the in the network pane of the Console.



Editing or Removing a Local Service Connection

Once a Local Service connection has been added to it can be edited or removed through the *Tools > Network Configuration*.

To edit a local service connection perform the following steps:

1. Ensure the *Enable Local Service* option is selected.
2. Select a port from the Local Service connections list and click *Edit*.
3. The edit dialog appears that allows for the port to be controlled remotely and password protected.
4. To remove a port from the Local Service, highlight the port and click *Remove*. This does not delete the entry from the *Network and Groups* pane in the Enterprise Console. It simply removes it from the Local Service connections list.
5. To remove the entry form the network pane in the Console, select it and click the *Remove* icon located in the sidebar.

Configuring Proxy Server Connection

If you are using a proxy server to connect to the Internet, you must specify the proxy server settings for the following features to work correctly:

- Check for updates
- Announcements
- License Activation

Complete the following steps to specify the proxy server settings:

1. Select *Tools > Network Configuration*.
2. Go to the Proxy Server tab.
3. Select the *Enable Proxy Server* checkbox to enable it.



4. Specify the following proxy server settings:
   > Address – Specify the IP address of the proxy server.
   > Port – Specify the port number for the proxy server.
5. This step is optional. Follow this step only if your proxy server requires authentication. Select *My proxy server requires authorization (logon credentials)* checkbox and specify the values for the following fields:
   > Authentication Type – Select the authentication type.
   > User name – Specify the user name.
   > Password – Specify the password.
   > Domain – Specify the domain.
6. Click *OK*.

Remote Consoles

A Remote Console is a Console that hosts one or more connections that allow other Consoles to connect through. Existing connections must be edited to allow them to be accessed remotely.

Setting up Remote Control Enabled Connections

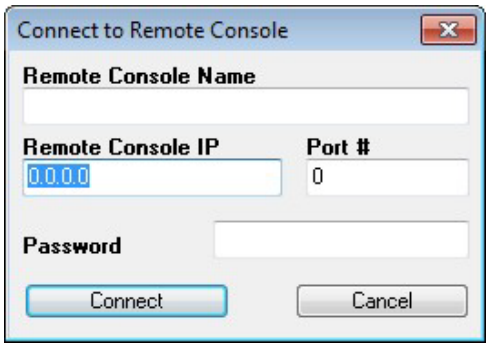
To allow a connection to be accessed remotely perform the following steps:

1. Open *Tools* > *Network Configurations*.
2. Select the *Enable local service* checkbox.
3. Select a port from the list and click *Edit*.
4. Ensure *Allow Remote Control* is selected.
5. Specify a password.
6. Click *OK*.

Connecting to a Remote Console

Once a Remote Console has been established by the hosting Console it can be accessed by other Consoles from a different machine.

1. Select the *Connect to Remote Console* icon in the side bar or by right-clicking on the network item. Upon selection the *Connect to Remote Console* dialog appears:



2. In the *Connect to Remote Console* dialog, specify the connection details such as *Remote Console Name*, *Remote Console IP*, *Port number,* and *Password*. This information is provided by the administrator of the host Console. Once entered, this information can be retrieved by right-clicking a port in the *Network and Groups Pane* and selecting *Properties*.

If the connection to a Remote Console has been severed, it can be reconnected by clicking the *Reconnect to Remote Console* icon in the sidebar or by right-clicking on an entry in the *Network and Groups* pane.

Managing Deep Freeze with the Console

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

Go to V*iew* > *Classic Look* to view the icons in Classic Windows format.

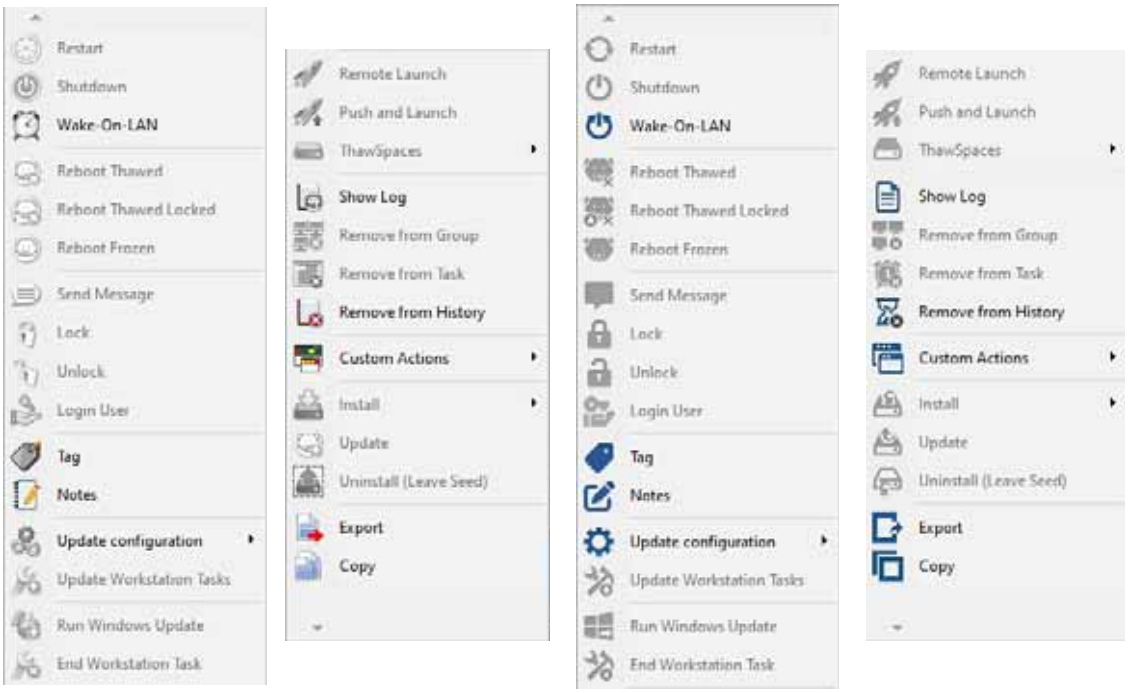


Go to *View* > *Modern Look* to view the icons in Modern Windows format.



These commands can also be accessed using the contextual menu, as shown below, that appears by right-clicking on one or more computers. When a particular action is chosen, the selected computer performs the action and the status icons update accordingly. If multiple computers are selected, the action is applied only to the applicable computers. For example, if you select computers that are Thawed and Frozen and apply the Reboot Thawed action, only the Frozen computers will be Thawed. The action will not be applied on the computers that are already Thawed.

Classic Look	Modern Look



Specific icons are disabled if the selected computer does not support that action. For example, a computer that has a *Target* icon, will not show the option to be Thawed or Frozen, because the program has not been installed yet.

Reboot Thawed/Reboot Thawed Locked for an Assigned Number of Times

You can select to reboot a workstation in Thawed or Thawed Locked state for an assigned number of times. When selected, this option will keep the workstation in a Thawed state whenever it reboots for the next assigned restarts.

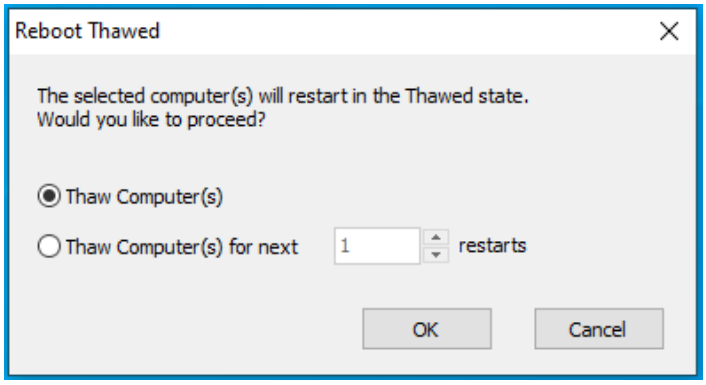
Complete the following steps:

1. Select one or multiple workstations.
2. Right-click and select *Reboot Thawed* or *Reboot Thawed Locked*.
3. Select the *Thaw Computer(s) for next X restarts* and assign the number of restarts.

   Selecting this option will reboot the workstation in Thawed or Thawed Locked state for the assigned restarts.

   For example, when you assign '3' as the number of restarts, the workstation will remain in a Thawed or Thawed Locked state after rebooting the next 3 times.

   The maximum number of times you can select to reboot the workstation in Thawed or Thawed Locked state is 99.



Login User

Administrators will be able to log in a user on selected computer(s) without having to walk up to each computer.

For this feature to work, the computers must be configured to hide the user account from the Windows logon screen and display the *User Name* and *Password* fields during logon.



This policy is mandatory for the *Login User* feature to be enabled in Deep Freeze.

To hide the last logged username on a Windows welcome screen, go to *Local Security Policy* > *Security Settings* > *Local Policies* > *Security Options* > *Interactive Logon: Don't Display Last Signed In (Username at Sign-in)* > select *Enabled*. Note that this policy is disabled by default.

If CTRL+ALT+DEL is required before a user can log on to Windows, you will need to additionally configure the following policies:

- Go to *Local Security Policy* > *Security Settings* > *Local Policies* > *Security Options* > *Interactive Logon: Do not Require CTRL+ALT+DELETE* > select *Enabled*.
- Go to *Local Computer Policy* > *Administrative Templates* > *Windows Components* > *Windows Logon Options* > *Disable/enable Software Secure Attention Sequence (or SAS)*. Select *Enabled*, then select *Services and Ease of Access Applications*.



This feature will not work if the Deep Freeze license is expired.

The last 10 user logins will be remembered, and the password needs to be entered every time a user is selected.

This feature is not available on computers that have only the Workstation Seed installed.



Sending Messages to Computers

To send a message to one or more computers, complete the following steps:

1. Select the computer(s) to send a message.
2. Right-click and select *Send Message* from the contextual menu.
3. Type the message in the dialog that appears and click *Send*. Alternatively, you can also send a previously sent message from the history drop-down. A dialog appears asking for confirmation to send the message to the selected computers.
4. Click *OK* to send or *Cancel* to close the dialog without sending the message.

Updating a Deep Freeze Configuration File

Complete the following steps to update the configuration on one or many computer(s) with the settings of an existing .rdx file. (An .rdx file is a file containing the conditions specified in the Deep Freeze Enterprise Configuration Administrator).

1. Right-click on the computer(s) and select *Update with RDX file*.
2. A message appears asking for an existing .rdx file to be located.
3. Click *OK*. A standard *Open File* dialog appears to select an .rdx file.
4. Locate a file and click *Open* to update the configuration on the selected computer(s) with the settings in the .rdx file. Click *Cancel* to cancel the configuration update.

Run Windows Update

Windows Updates can be applied on demand from the right-click context menu.

Complete the following steps to run Windows Updates on the workstation.

1. Right-click on the computer(s) and select *Run Windows Update*.
2. Click *OK*.

Windows Updates are applied on the selected workstation(s). The settings configured in the Windows Update Tab tab are used.

Apart from applying Windows Updates on demand from the right-click context menu, you can also schedule the Windows Updates task. For more information, refer to Scheduling Deep Freeze Tasks on how to schedule a Windows Updates task.



If the Network options in the new configuration have changed, the computer(s) may lose communication with the existing Enterprise Console. If communication with the computers is lost, check the Network settings on the updated computers to ensure that the port numbers and/or IP address of the Console have not been changed.



Changes to passwords take effect immediately. All other changes take effect after each computer is restarted. ThawSpace and/or Frozen Drives cannot be changed through updating the configuration file.

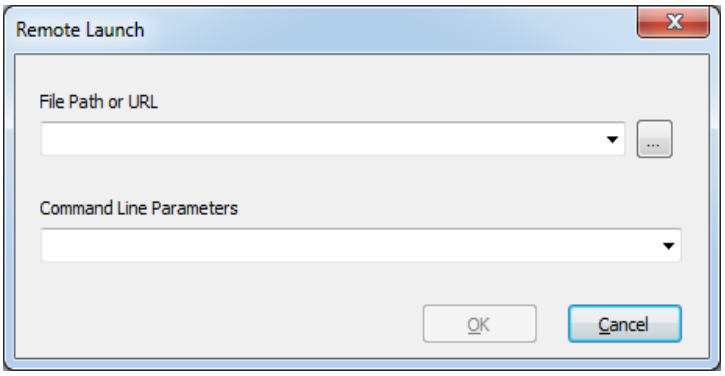
Remote Launch

This feature allows IT administrators to remotely launch executable files on managed workstations. File types supported are .exe (executables), .msi (MSI installers), .bat/.cmd (batch script), .vbs (VB script), and .ps1 (PowerShell). When an MSI installer is selected, Deep Freeze runs it using MSIEXEC.

You can also specify a web URL or FTP location for downloading and installing executable files. The file will be automatically downloaded from the specified location and launched on the workstation.

To remotely launch executables on workstations, complete the following steps:

1. An executable can be launched on workstations in one of the following ways:
   > Right-click on one or more workstations and select *Remote Launch* from the context menu.
   > Scheduled through Deep Freeze tasks.
2. Specify the values for the following fields or alternatively, select a previously specified value from the history drop-down:



   > Filename and Path – Specify the filename and path where the file is available on the target computer. Alternatively, you can browse to select the executable. Or specify a URL or FTP location. File types supported are .exe, .msi, .bat/.cmd, .vbs, and .ps1. MSI installers are run in install mode by default. For example, if the executable MyApplication.exe is available at C:/AppFolder, specify *C:/AppFolder/MyApplication*.
3. Specify the Command Line Parameters with environment variables (optional):
   > Arguments – Specify the arguments that you want to apply with this executable. For example, if the executable is run from the command prompt with the command C:\AppFolder\MyApplication -o logFile.log, specify *-o logFile.log* for arguments. For .msi files, specify the arguments that you would normally specify when launching a .msi file with MSIEXEC. If you do not specify any argument for a .msi file, Deep Freeze will automatically append "/i" (install). Deep Freeze also replaces any display options with /qn, (quiet, no UI).
4. Click *OK*.

The file is remotely launched on the selected workstations.

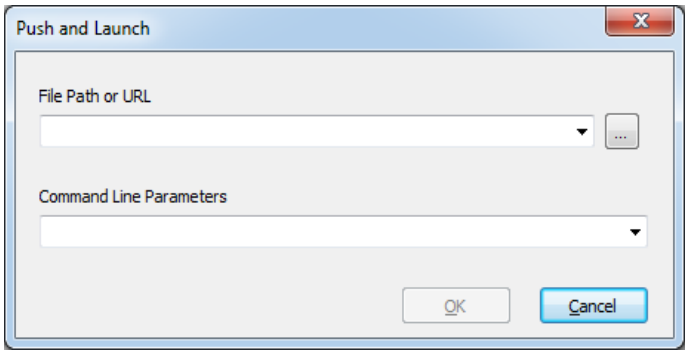
Push and Launch

This feature allows IT administrators to push and launch executable files on managed workstations.

You can also specify a web URL or FTP location for downloading and installing executable files. The file will be automatically downloaded from the specified location and launched on the workstation.

Complete the following files to push and launch files on managed workstations:

1. An executable can be launched on workstations in one of the following ways:
   > Right-click on one or more workstations and select *Push and Launch* from the context menu.
   > Scheduled through Deep Freeze tasks.
2. Browse to select the file path or specify the file path (or alternatively, select a previously specified value from the history drop-down):



   > Filename and Path – Specify the filename and path where the file is available on the console computer. Alternatively, you can browse to select the executable. Or specify a URL or FTP location. File types supported are .exe, .msi, .bat/.cmd, .vbs, and .ps1. MSI files are run in install mode by default. For example, if the executable MyApplication.exe is available at C:/AppFolder, specify *C:/AppFolder/MyApplication*.
3. Specify the Command Line Parameters with environment variables (optional):
   > Arguments – Specify the arguments that you want to apply with this executable. For example, if the executable is run from the command prompt with the command C:\AppFolder\MyApplication -o logFile.log, specify *-o logFile.log* for arguments. For .msi files, specify the arguments that you would normally specify when launching a .msi file with MSIEXEC. If you do not specify any argument for a .msi file, Deep Freeze will automatically append "/i" (install). Deep Freeze also replaces any display options with /qn, (quiet, no UI).
4. Click *OK*.

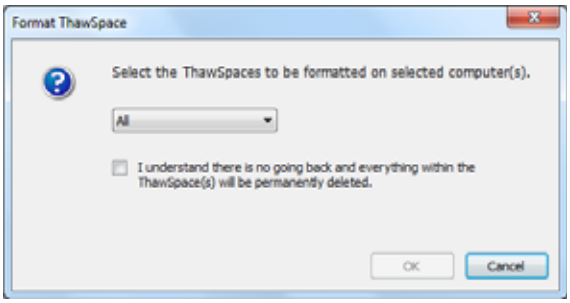
The file is pushed to the selected workstation and remotely launched on the selected workstations.

Format ThawSpace

Deep Freeze Enterprise Console provides the ability to format a specific ThawSpace or all ThawSpaces on managed workstations.

Complete the following steps to format ThawSpaces:

1. Select one or multiple workstations.
2. Right-click and select *ThawSpaces > Format ThawSpace*. Alternatively, you can click the Format ThawSpace icon in the toolbar.
3. The Format ThawSpace dialog is shown. Select *All* or select the specific drive to format.



4. Select *I understand there is no going back and everything within the ThawSpace(s) will be permanently deleted*.
5. Click *OK*.



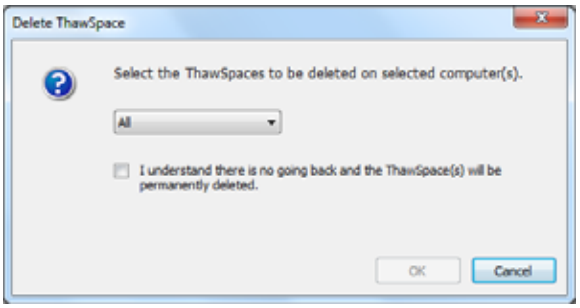
The Format ThawSpace command deletes all data on ThawSpaces. The data cannot be recovered once it is deleted. Backup important files before formatting the ThawSpace.

Delete ThawSpace

Deep Freeze Enterprise Console provides the ability to delete a specific ThawSpace or delete all the ThawSpaces on managed workstations.

Complete the following steps to delete ThawSpaces:

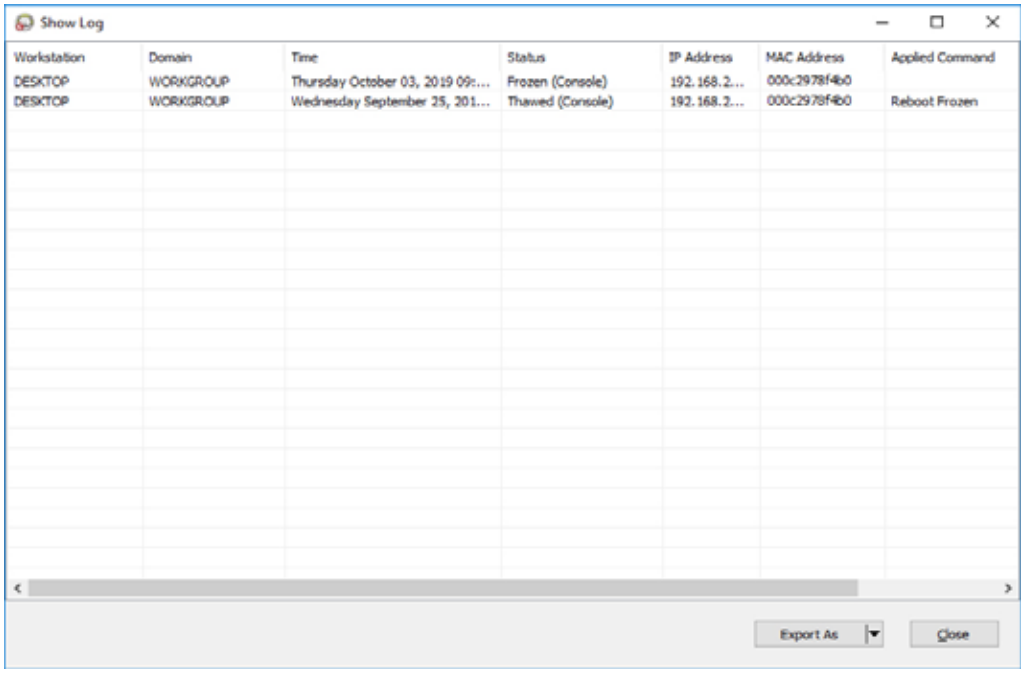
1. Select one or multiple workstations.
2. Right-click and select *ThawSpaces > Delete ThawSpace*. Alternatively, you can click the *Delete ThawSpace* icon in the toolbar.
3. The *Delete ThawSpace* dialog is shown. Select *All* or select the specific drive to delete.



4. Select *I understand there is no going back and the ThawSpace(s) will be permanently deleted*.
5. Click *OK*.

Viewing the Console Log File

The Enterprise Console keeps a log of the status and activity history of all connected computers. The log stores information for the previous 7 days. Information older than 7 days is automatically deleted from the log.



- To view the log file for one or many computers, right-click on the computer(s) and select *Show Log*.
- To sort the log file, click on a preferred heading. The following columns are available:
  - > Workstation
  - > Domain
  - > Time
  - > Status

    The Status column displays the current status of the computer and how the computer was rebooted.

    For example, if the computer was rebooted to a Thawed state through the console, the status will display as *Thawed (Console)*.
  - > IP Address
  - > MAC Address
  - > Applied Command (Frozen, Thawed, Restart, Shutdown)
  - > Installation File
- To export the log file click *Export As* and select *Text* or *CSV*. Specify the name of the file and click *OK*.

Target Installing Deep Freeze

Complete the following steps to remotely install a Full Workstation Installation on any computer that has the Workstation Seed installed.

1. Right-click on one or multiple computers and select *Install*. A dialog is displayed, asking if the installation should proceed. Click *OK*.
2. A dialog box appears to select the file to be installed on the remote computer.
3. Select the installation file to use and click *Open*.
4. The computer installs Deep Freeze and restarts.
5. Once the installation is complete, the Enterprise Console reflects the change in the computer's status, and displays it as *Frozen*.

Updating Deep Freeze Software

To update Deep Freeze computers (where Deep Freeze 7.7 or higher is installed) with a new version of Deep Freeze, complete the following steps:

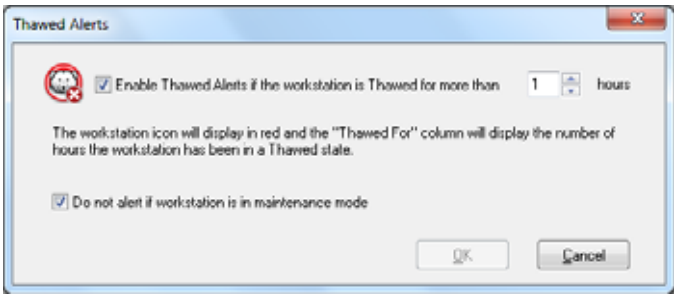
1. In the Enterprise Console, select the computers to be updated. The computers can be in either a Frozen or Thawed state.
2. Right-click, and select *Update Deep Freeze* from the contextual menu.
3. The selected computers update to the new version of Deep Freeze software, but retain all settings from the current version. The computers reboot twice to complete the update.

Thawed Alerts

Thawed Alerts notify the administrator if a computer has been left in a Thawed state for a specified period of time. Deep Freeze Enterprise Console will display the workstation icon in red and the *Thawed For* column will display the number of hours the workstation has been in a Thawed state.

Complete the following steps to set a Thawed alert:

1. Go to *Tools* > *Thawed Alerts*.
2. The *Thawed Alerts* dialog is displayed. Select *Enable Thawed Alerts if the workstation is Thawed for more than x hours*. Select the value for x.



3. Select *Do not alert if workstation is in maintenance mode* if you do not want to be alerted about workstations undergoing maintenance.
4. Click *OK*.

Licensing

The License Key can be updated via the Deep Freeze Enterprise Console and the workstation licenses can be activated either automatically or manually.

To activate the Deep Freeze workstation licenses automatically, complete the following steps:

1. Launch the *Deep Freeze Enterprise Console*.
2. Go to *Tools* > *Licensing*.
3. The *Licensing* dialog is displayed.



4. Click *Edit* and enter the License Key in the *License Key* field.
5. Click *Update License*. This converts Deep Freeze from the *Evaluation* version to a *Licensed* version. The *License Key Type* field displays the *License Key*. The *Expiry Date* displays the date and time when the license expires.

Deep Freeze automatically activates each workstation license via the Enterprise Console or by connecting directly to the Faronics License Activation Server.

Activation of your product license is necessary to authenticate your copy and avoid product expiry. Deep Freeze workstations not activated within 30 days cannot be Frozen.

The workstation will connect either via the local console or directly to the Faronics Activation server and transmit to our secure servers certain information relating to your computer (including product version, license key, machine ID, OS version, MAC address, CPU ID, and console machine ID) as and when an Internet connection is available.

Manual Activation

To activate the Deep Freeze workstation licenses manually, follow the steps outlined under Licensing. Thereafter, complete the following steps:

1. Click *Activate Now.* Two options are available:



> Select *Activate Online* to activate Deep Freeze workstation license over the Internet. The license on the workstation is activated on clicking *Next*. The computer must be connected to the Internet to Activate Online.

> Select *Activate Offline* to activate the Deep Freeze workstation license with Faronics by email or by phone. Click *Next*. The Activate Offline screen is displayed:



2. Click *Create Offline Activation Request File* and click *Save*. Send the file to activation@faronics.com to receive an Activation Response File. Browse to select the *Activation Response File* received from Faronics. Click *Apply Offline Activation Request File*.



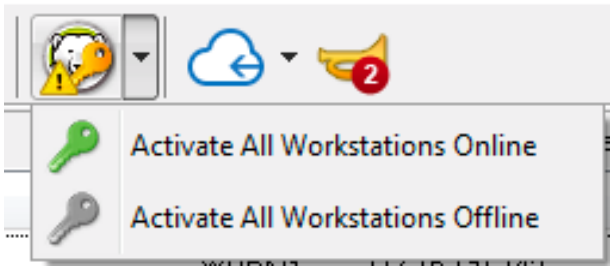
The License Key is automatically updated on all computers communicating with the Enterprise Console. If a computer is offline (shut down or disconnected from the network), the License Key is updated when the computer communicates with the Enterprise Console.

License Icon

If you have workstations whose Deep Freeze licenses are not activated by Faronics License Activation Server, an activation icon appears in the toolbar. You can activate the workstations with pending activations either online or offline.

Complete the following steps to activate the workstations using the activation icon:

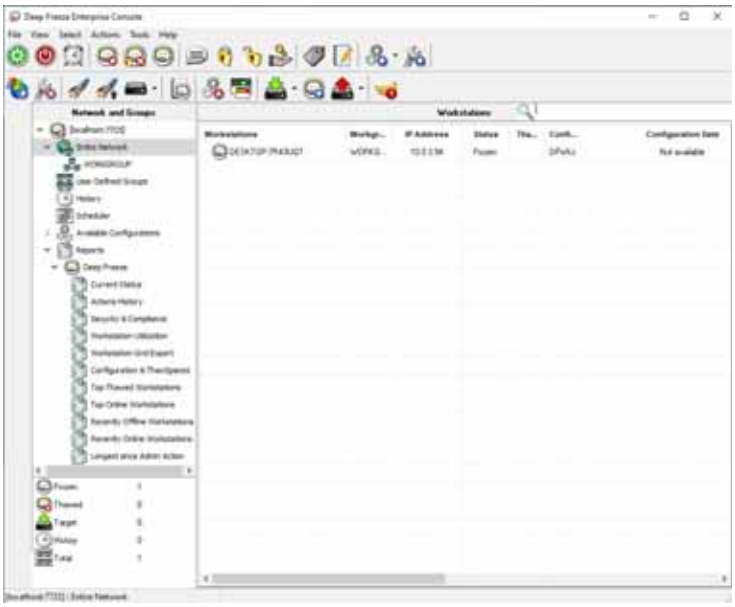
1. Click the drop-down on the activation icon.



2. Select *Activate All Workstations Online*. Deep Freeze Console contacts the Faronics Licensing Server and activates the licenses. An Internet connection is required to activate online.
3. Alternatively, select Activate All Workstations Offline. For more information about offline activation, go to Manual Activation.

Reports

Deep Freeze console compiles various reports about the workstation's performance, current status and history, as well as Anti-Virus Reports. You can access the following reports from the *Networks and Groups* panel.



You can export information to spreadsheet format by clicking *Export as XLS*.

- Current Status: Displays the status of Deep Freeze on the workstation and indicates how long the workstation has been in a Thawed state.
- Actions History: Records the actions applied on workstations, including the timing of these actions, the version of Deep Freeze after the update, configuration, and associated tags or user-defined groups.
- Security and Compliance: Displays details of the security status of Deep Freeze, indicating whether the product requires an update, activation, or has been in a Thawed state for an extensive period.
- Workstation Utilization: Displays details of each workstation's usage over a selected period.
- Workstation Grid Export: When exported, the content of the report provides an exact version of the current workstation grid, retaining the structure and format of the grid as displayed on the console, including the order of the visible columns.
- Configuration and ThawSpaces: Provides details of configuration, ThawSpaces, and scheduled tasks for workstations.
- Full Configuration Report: Presents a comprehensive report of each configuration setting in all Available Configurations, RDX, and Install files.
- Top Thawed Workstations: Identifies workstations that have been in a Thawed state the longest.
- Top Online Workstations: Identifies the workstations with the highest uptime.

- Recently Offline Workstations: Identifies workstations that have recently stopped communicating with the Deep Freeze console.
- Recently Online Workstations: Identifies workstations that have recently communicated with the Deep Freeze console.
- Longest Since Admin Action: Identifies workstations that have not received any console or workstation UI commands for the longest time, potentially highlighting neglected or low-priority machines.

Customize the Grid

View or Hide Reports

To view or hide reports, right-click on *Deep Freeze* under and select/unselect the reports you would like to view or hide.

Organizing Columns in the Grid

Customize the way information is displayed by clicking and dragging the column headers to new locations.

Search and Filter

You can select to filter the view by clicking on the filter on top right of each column and customize the filter with conditional parameters.

- Equals
- Does not equal
- Is less than
- Is less than or equal to
- Is greater than
- Is greater than or equal to
- Is like
- Is not like
- Contains
- Does not contain
- Begins with
- Ends with
- Is blank
- Is not blank
- Is between
- Is not between
- Is any of

- Is none of

Where available, you can select to filter the view by clicking on the timestamp at the bottom and selecting from the pre-defined date range, or customize your date preferences and click *Apply Filter*.

Customizing Filters

After you add a filter, you can customize the filter and add more filter combinations to create a set of filters that you save, reuse, and access later with a simple click. Click *Customize* at the bottom right and select to *Add Condition, Add Group* or *Clear All* in the *Filter Builder*.

Click *Filter > Add Condition* to add a new condition and specify the condition in this format: *Column Name, Parameter, Expression*.

For example: *Workstation Name = (Equals) Desktop*.

Alternatively, click *Press the Button to Add a New Condition*.

Click *Filter > Add Group* to add a sub-group condition and specify the parameters for this condition.

Click *Save As* to save the filter on your network.

Click *Open* and select from the saved filter to apply the filter.

Group by

You can also organize your view by groups by dragging column headers to the area that says *Drag a Column Header Here to Group by that Column*.

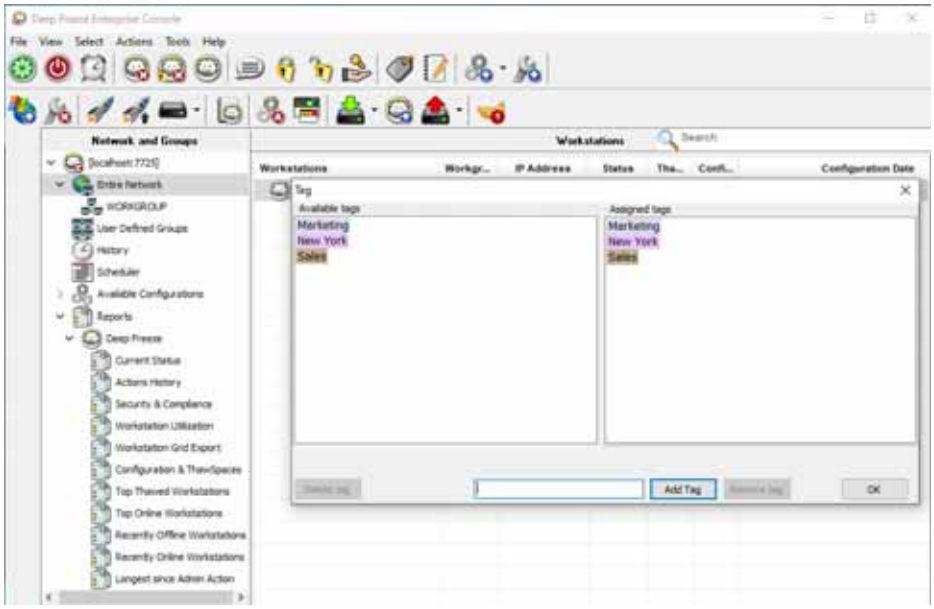
Tags

Tags are simple pieces of data, usually one-word descriptions, keywords or labels providing details about an item (such as Computers, Groups, and more) to make it easy to find related items by browsing or searching.

For example, you may want to tag the computers as per departments like Accounts, Marketing, or Sales. You can then search for the tag 'Accounts' and all items with the specified tag are displayed.

Create/Assign Tags

Tags can be applied to multiple computers.



Complete the following steps to create or assign tags:

1. Select a workstation from the grid.
2. Click the *Tag* icon from the toolbar.
3. In the Tag Computer field, start typing the first few characters and select from the list (if the tag already exists), or create an entirely new tag, and click *Add Tag*.

The new tag will be automatically assigned to the selected computer.

Alternatively, double-click on any of the available tags to assign the tag to the workstation.

Remove/Unassign Tags

Complete the following steps to remove or unassign tags:

1. Select a workstation from the grid.

2. Click the *Tag* icon from the toolbar.
3. In the *Assigned Tabs* pane, select the tags to be removed/unassigned.
4. Click *Remove Tag*.

The tag will be automatically removed/unassigned to the selected computer.



Tags that have been unassigned from computers are only removed and will not be deleted from the list of tags.

Delete Tags

Complete the following steps to delete tags:

1. Select a workstation from the grid.
2. Click the *Tag* icon from the toolbar.
3. Select a tag from the list of *Available Tags*.
4. Click *Delete Tag*.

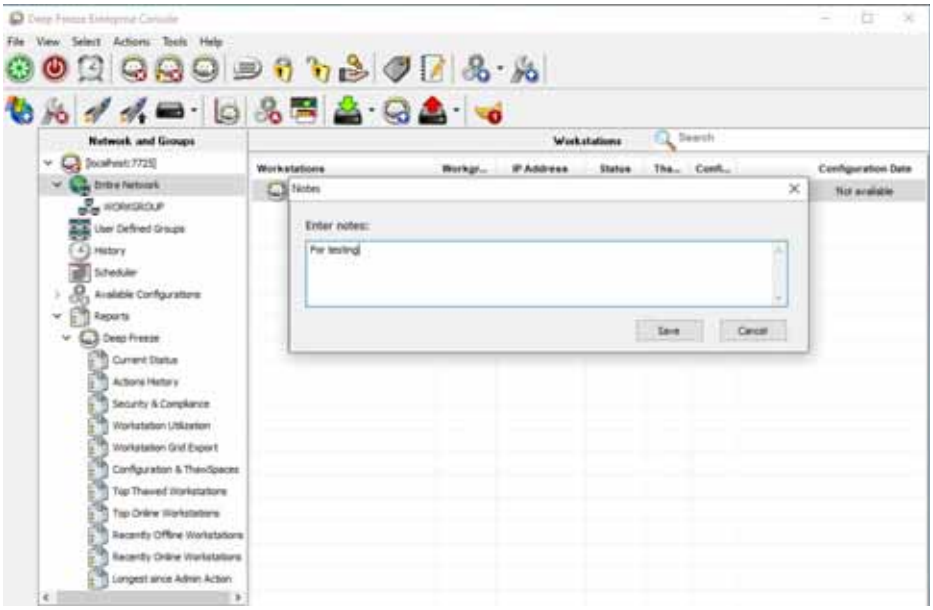


Tags that have been deleted will globally delete the tag from the list (not just from the workstation) and be automatically removed from computers which have been assigned the tags.

Notes

Notes provide additional context or description used to explain, annotate, or add information for the selected workstation.

Add Notes



Complete the following steps to add notes:

1. Select a workstation from the grid.
2. Click the *Notes* icon from the toolbar.
3. Type in your notes (Up to a maximum of 260 characters).
4. Click *Save*.

Notes will be displayed as tooltip when you hover the mouse over the note in the grid.

Notes can only be applied to a single workstation.

Scheduling Deep Freeze Tasks

Deep Freeze Enterprise offers two types of Deep Freeze Tasks:

- Single Task – Contains only one Deep Freeze task
- Combination Task – Can contain up to 5 Deep Freeze tasks for a maximum of 20 hours. A Combination Task cannot be run immediately and it can only be scheduled.

Single Task

To schedule a Deep Freeze task in the Enterprise Console using the Scheduled Task Wizard, complete the following steps:

1. Open the *Scheduled Task Wizard* in one of the following ways:
   > Click *Scheduler* in the *Network and Groups* pane and click the *Add Task* icon.
   > Right-click on *Scheduler* in the *Network and Groups* pane, and choose *Add Task.*

The following screen is displayed:



2. Double-click the preferred task or select the task and click *Next*. The following tasks are available for Deep Freeze:
   > Combination Tasks
   > Restart
   > Shutdown
   > Wake-on-LAN
   > Reboot Frozen
   > Reboot Thawed
   > Reboot Thawed Locked
   > Send Message
   > Login User
   > Run Windows Updates
   > Remote Launch

> Push and Launch

> Update

> Format ThawSpace

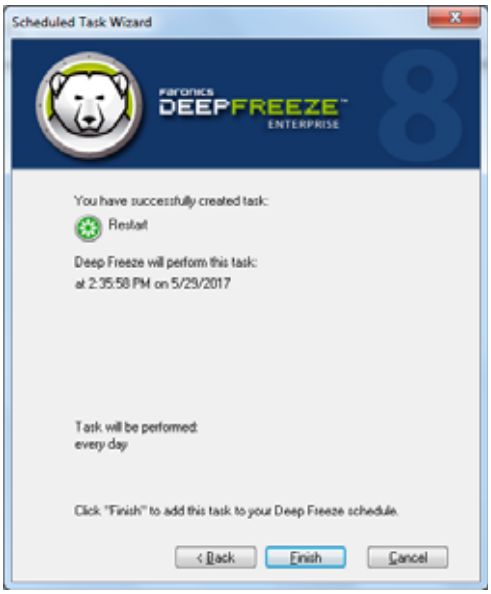
3. In the following screen, enter a name for the task and choose the preferred task execution schedule: Daily, Weekly, Monthly, or One time only. Task names must be unique. No two tasks can have the same name. Click *Next*.



4. Depending on the choice of task execution, the time and date configuration options that follow will vary. Click *Next*.



5. Click *Finish* once the configuration is completed.



The default start time for a task is five minutes from the current time.

Combination Task

To schedule a Combination Task in the Enterprise Console using the Scheduled Task Wizard, complete the following steps:

1. Open the *Scheduled Task Wizard* in one of the following ways:
   > Click *Scheduler* in the *Network and Groups* pane and click the *Add Task* icon.
   > Right-click on *Scheduler* in the *Network and Groups* pane, and choose *Add Task.*

The following screen is displayed:



2. Select *Combination Task* and click *Next*.
3. In the following screen, enter a name for the task and choose the preferred task execution schedule: Daily, Weekly, Monthly, or One time only. Task names must be unique. No two tasks can have the same name. Click *Next*.



4. Depending on the choice of task execution, the time and date configuration options that follow will vary. Click *Next*.



5. Select the task from the drop-down and specify the time. Click the + sign to add another task. Repeat the process to add up to 5 tasks for a maximum of 20 hours. Click *Next*.



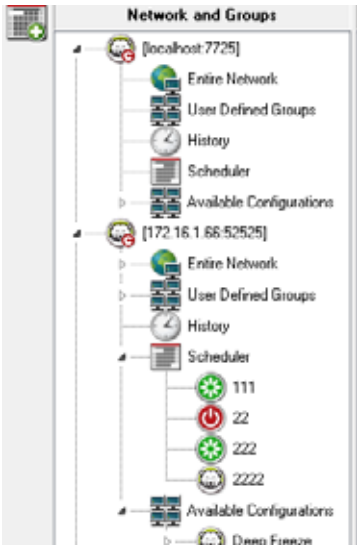
6. Review the list of tasks and click *Finish*.

Editing Scheduled Tasks

To edit Scheduled Tasks, right-click the task and select Edit Task. Follow steps 1-5 in section Scheduling Deep Freeze Tasks.

Assigning Computers to Scheduled Tasks

After a task has been scheduled, it appears under the *Scheduler* in the *Network and Groups* pane of the Console.



To assign computers to a task, select the preferred computers from the *Workstations* pane in the Console and drag them onto the preferred task. Or, drag a group onto the task.

To see which computers are assigned to a specific task, click on the task. The assigned computers appear in the *Workstations* pane.

To delete a computer from a task, right-click on the computer and select *Remove from Task*.

Adding a Task

To add a task, right-click on *Scheduler* and select *Add Task*.

Editing a Task

To edit a task, right-click on the task and select *Edit Task*.

Pausing a Task

To pause a task, right-click on the task and select *Pause Task*.

Resuming a Task

To resume a task, right click on the task and select *Resume Task*.

Deleting a Task

To delete a task, right-click on the task and select *Delete Task*.

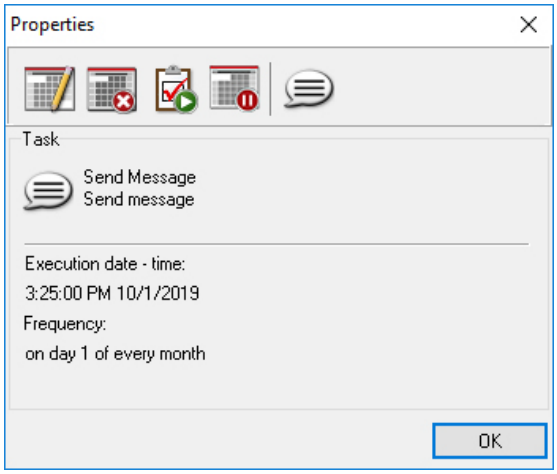
Executing a Task Immediately

To execute a task immediately, right-click on the task and select *Execute Task*.

Scheduled Task Properties

To see the properties of a task, right-click on the task name and select *View Properties*.

The following screen displays:



Scheduled tasks will still execute even if the Enterprise Console is closed provided the local service is enabled and the network connections are not shutdown upon exiting the Enterprise Console.

Managing Network and Groups

The Enterprise Console automatically arranges computers by their workgroup or domain. Click the appropriate workgroup or domain to view the computers in that workgroup or domain.

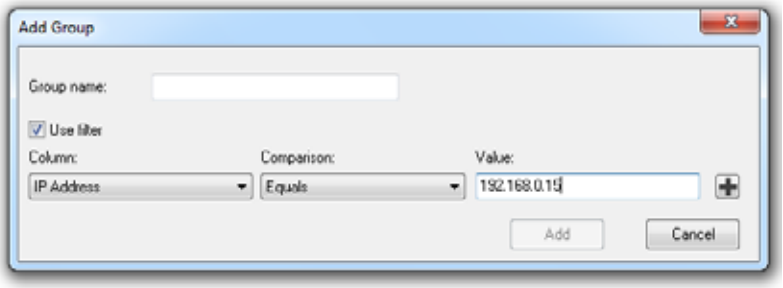
The Enterprise Console can be used to define specific groups in order to arrange computers.

Adding a Group

The Add Group dialog allows you to configure multiple filters to sort the workstations into different groups. This filter automatically updates the list of workstations based on the changes in the selected parameters.

Complete the following steps to add a group with a Filter:

1. Right-click *User Defined Groups* in *Network and Groups* pane.
2. Select *Add Group*. The Add Group dialog is displayed:



3. Specify the *Group Name*.
4. Select *Column*.
5. Select *Comparison*.
6. Select *Option* And/Or if you are adding another filter.
7. Specify *Value* or *Regular Expression*.
8. Click *Add*.

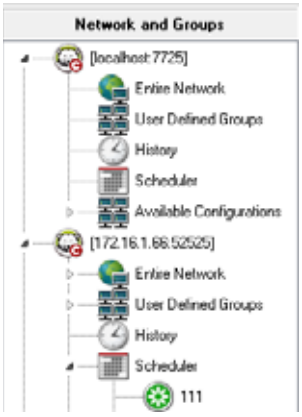
The following table shows the Column, Comparison, Option, and Values.

Select Column	Select Comparison	Select Option	Specify Value or Regular Expression
Workstations	Equals Not Equal To Regular Expression Contains	And Or	Specify the *Value* or *Regular Expression*.
Workgroup	Equals Not Equal To Regular Expression Contains	And Or	Specify the *Value* or *Regular Expression*.
IP Address	Equals Not Equal To Regular Expression Contains	And Or	Specify the *Value* or *Regular Expression*.
Status	Equals Not Equal To	And Or	Frozen Frozen and Locked Thawed Thawed and Locked Applying Windows Update Applying Batch File Thawed Period Maintenance Mode License Expired WKS Seed Offline
Tags	Equals Not Equal To	And Or	Specify the *Value* or *Regular Expression*.
Note	Contains	And Or	Specify the *Value* or *Regular Expression*.
Configuration	Equals Not Equal To Regular Expression Contains	And Or	Specify the *Value* or *Regular Expression*.

Select Column	Select Comparison	Select Option	Specify Value or Regular Expression
Configuration Date	Equals Not Equal To Greater Than Greater Than or Equal To Less Than Less Than or Equal To	And Or	Specify the *Date*.
Installation File	Equals Not Equal To Regular Expression Contains	And Or	Specify the *Value* or *Regular Expression*.
Version	Equals Not Equal To Greater Than Greater Than or Equal To Less Than Less Than or Equal To	And Or	Specify the *Value* or *Regular Expression*.
Operating System	Equals Not Equal To Regular Expression Contains	And Or	Specify the *Value* or *Regular Expression*.
MAC Address	Equals Not Equal To Regular Expression	And Or	Specify the *Value* or *Regular Expression*.
Login Name	Equals Not Equal To Regular Expression	And Or	Specify the *Value* or *Regular Expression*.
Thawed For	Greater Than Greater Than or Equal To Less Than Less Than or Equal To	And Or	Specify the *Value.*
ThawSpace Free (GB)	Equals Not Equal To Regular Expression	And Or	Specify the *Value* or *Regular Expression*.

Building a User-Defined Group Structure

After a group has been added, one or more sub-groups can be added below it, and further sub-groups can be added indefinitely as a way to differentiate between environments, as in the example shown below.



Importing Groups from Active Directory

If the group structure has already been designed within Active Directory, that structure can be imported directly into the Enterprise Console. Complete the following steps to import from the Active Directory:

1. Select *Tools* > *Import Groups from Active Directory*, or click the *LDAP* icon located in the sidebar.
2. The following dialog appears. Select either the *Microsoft* tab or the *Novell* tab.



3. Enter the LDAP server information of the import location. The option to login anonymously is also available. If this checkbox is not selected, a username and password is required.
4. Select *Secure LDAP* if your network uses Secure LDAP. (For more information on Secure LDAP go to https://support.microsoft.com/en-ca/kb/321051.)
5. Click *Connect*. The *Active Directory* hierarchy appears. Select the required entries and click *Import*.

History

The Enterprise Console stores the history of the target computers.

If a computer is disconnected from a network, shutdown or is restarting, an exclamation sign (!) appears in the Enterprise Console for the particular computer. If the computer comes back online, the exclamation sign disappears.

If the computer goes offline permanently (for example, if the computer was permanently unplugged from the network), or if the computer is shutdown, the exclamation sign stays on.

In the Enterprise Console, go to *File > Exit*. Select the option *Close and shutdown network connections option* and click *OK*. Once you reopen the Enterprise Console, the computers with the exclamation sign (!) will appear in History. If the computer is shutdown and is equipped with Wake-on-LAN hardware, right-click on the computer in History and select Wake-on-LAN to wake the computer.

Options in History:

- To view history, click *History* in the *Networks and Groups* pane.
- To delete computer(s) from History, select the computer(s), right-click and select *Remove from History* in the context menu.
- To wake the computer using Wake-on-LAN, select the computer(s), right-click and select *Wake-on-LAN* in the context menu.

Adding Computers to a Group

Computers can be added to a group by dragging them from the *Workstations* pane to the preferred group, or by using an automatic filter set during the creation of the groups.

Automatic group filtering allows computers to be added to user-defined groups automatically. The computers are added based on their computer name.

Wildcards (*, ?) can be used to add computers based on a specific segment of the name.

Example: *Lab1-** adds all computers with names starting with Lab1- .

Sorting Groups Alphabetically

To sort the Groups alphabetically, right-click *User Defined Groups* and select *Sort Groups Alphabetically*.

Removing Workstations from User Defined Group

To remove a computer from a Group, right-click on the computer in *User Defined Groups* and select *Remove from Group*.

Importing or Exporting Groups to File

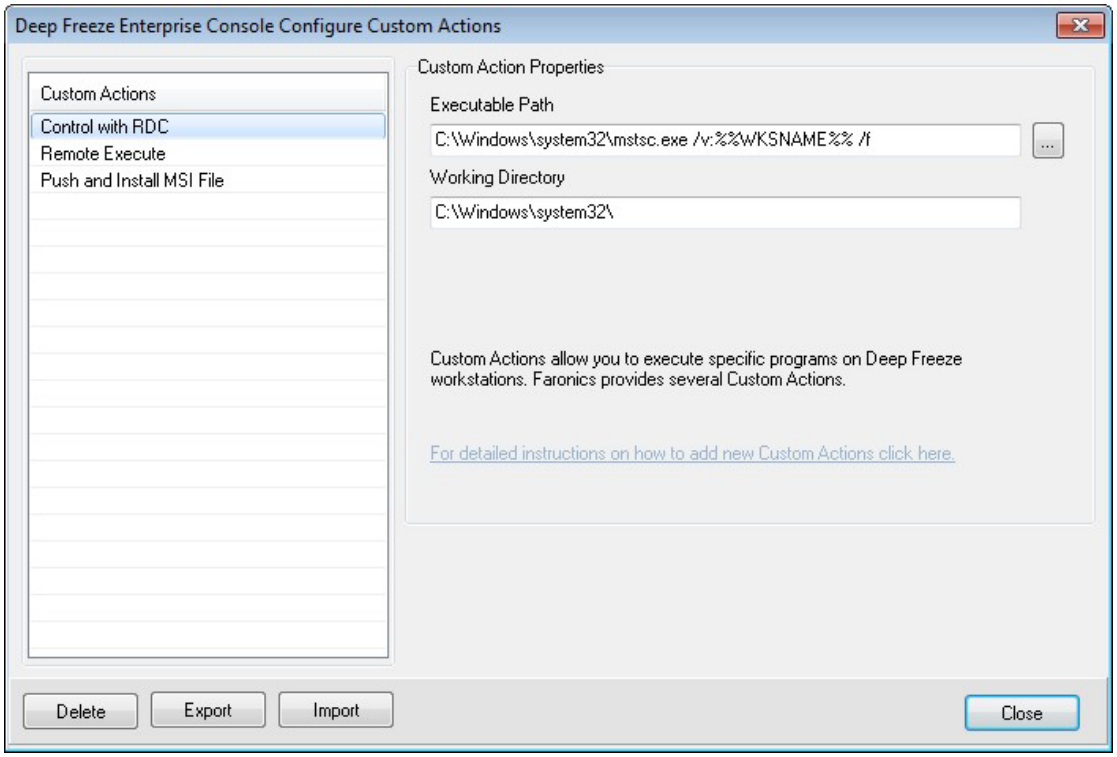
To import groups from a file or export groups to a file, choose the preferred option from the *Tools* menu.

Configure Custom Actions

Deep Freeze provides the following custom actions that can be accessed via the *Actions* menu. Additional actions can be created to suit specific needs. Deep Freeze provides three default actions. Additional Custom Actions can be configured by importing the appropriate .xml file in the Deep Freeze Console. For more information on Custom Actions, the structure of the custom action file and details about various parameters, refer to Appendix E.

Control with RDC

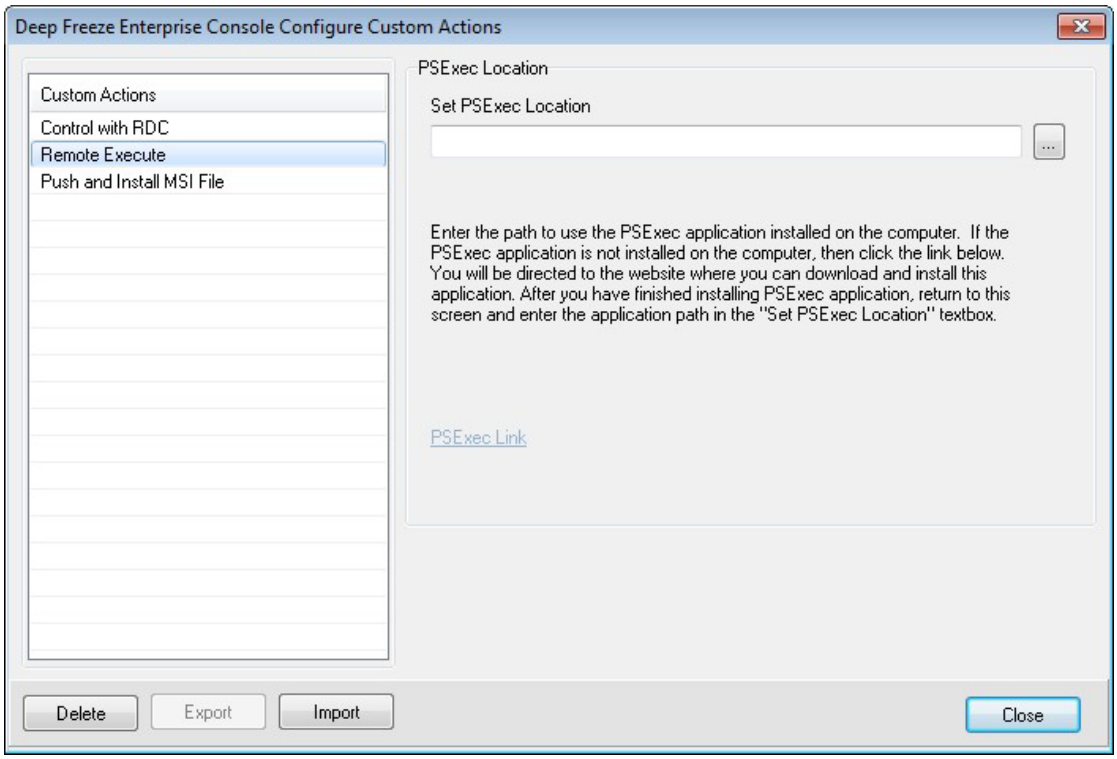
This allows connecting to the computer through Microsoft Remote Desktop Protocol. Remote Desktop Connection must already be enabled on the target machines.



1. Go to *Action* > *Custom Actions.*
2. Select *Control with RDC*.
3. Enter the *Executable Path* or browse to select the location.
4. Enter the *Working Directory*.
5. Click *Apply*.

Remote Execute with PsExec

Remote Execute allows you to remotely execute an executable file on a computer. PsExec is a tool that can be used to remotely execute an executable file on a computer. PsExec must be downloaded and installed on the computer. For more information on PsExec, visit http://www.faronics.com/pstools.



Configure

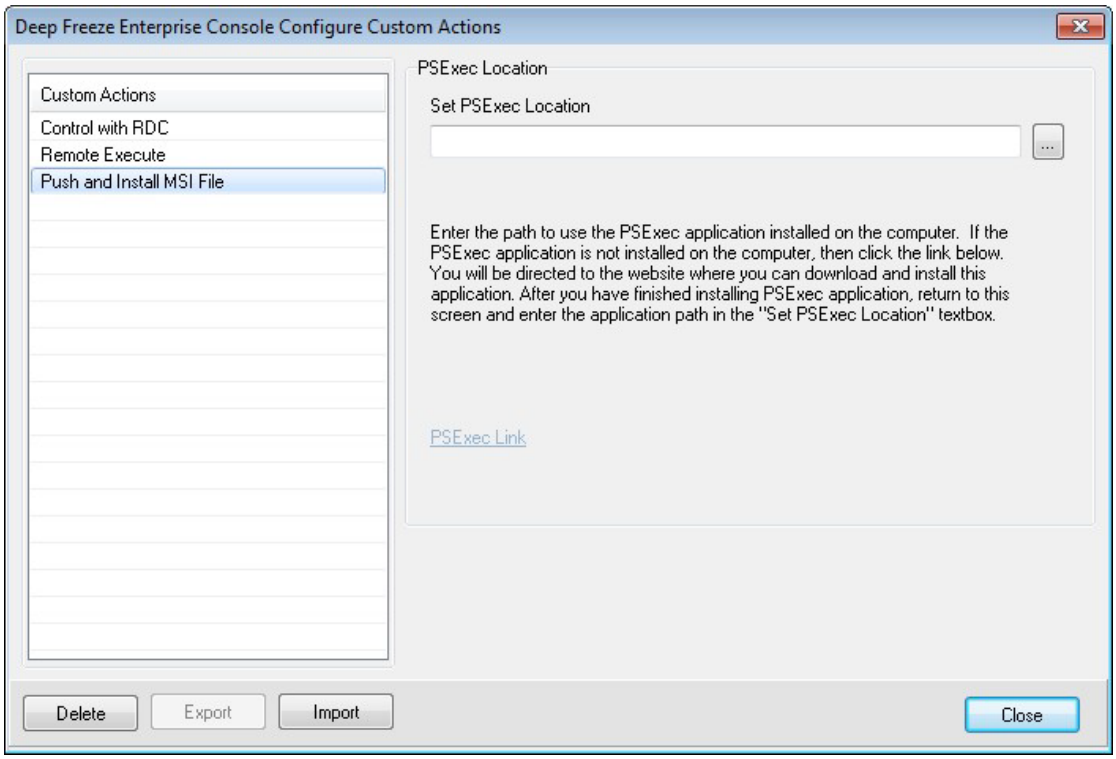
1. Go to *Action* > *Custom Actions.*
2. Select *Remote Execute*.
3. Enter the *PSExec Location* or browse to select the location.
4. The *Executable path* and the *Working Directory* are added automatically. The *Executable path* and *Working Directory* can be modified later.
5. Click *Close*.

Execute

1. Select the computers from the *Workstations* pane.
2. Select *Action* > *Remote Execute*.
3. The *Remote Execute* dialog is displayed.
4. Enter the *User Name*, *Password* and *Command*.
5. Click *OK*.

Push and Install MSI file with PsExec

The *Push and Install MSI file* option allows you to push and install a .msi file on a computer through the Enterprise Console.



Configure

1. Go to *Action > Custom Actions.*
2. Select *Push and Install MSI file*.
3. Enter the *PSExec Location* or browse to select the location.
4. The *Executable path* and the *Working Directory* are added automatically. The *Executable path* and *Working Directory* can be modified later.
5. Click *Close*.

Execute

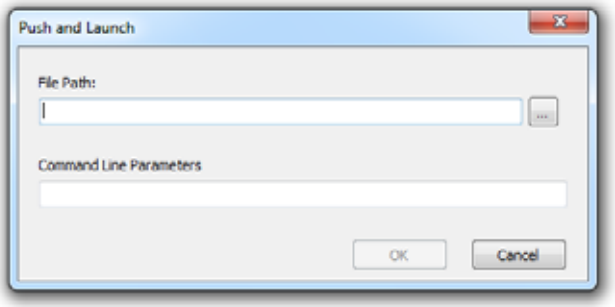
1. Select the computers from the *Workstations* pane.
2. Select *Action > Push and Install MSI file*.
3. The *Push and Install MSI file* dialog is displayed.
4. Enter the *User Name*, *Password*, *File Name* and *Drive Letter*.
5. Click *OK*.

Push and Launch

You can push and launch files on managed workstations.

Complete the following files to push and launch files on managed workstations:

1. Select one or more workstations from the Workstation pane.
2. Right-click and select *Actions* > *Push and Launch*. The Push and Launch dialog is displayed:



3. Browse to select the file path or specify the file path.
   > Filename and Path – Specify the filename and path where the file is available on the console computer. Alternatively, you can browse to select the executable. File types supported are .exe (executables) and .msi (MSI installers). MSI files are run in install mode by default. For example, if the executable MyApplication.exe is available at C:/AppFolder, specify *C:/AppFolder/MyApplication*.
4. Specify the Command Line Parameters with environment variables (optional):
   > Arguments – Specify the arguments that you want to apply with this executable. For example, if the executable is run from the command prompt with the command C:\AppFolder\MyApplication -o logFile.log, specify *-o logFile.log* for arguments. For .msi files, specify the arguments that you would normally specify when launching a .msi file with MSIEXEC. If you do not specify any argument for a .msi file, Deep Freeze will automatically append "/i" (install). Deep Freeze also replaces any display options with /qn, (quiet, no UI).
5. Click *OK*.

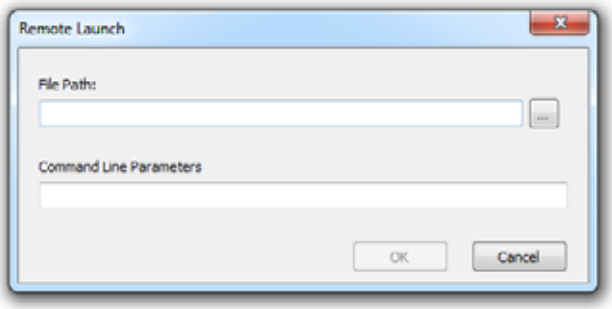
The file is pushed to the selected workstation and remotely launched on the selected workstations.

Remote Launch

You can remotely launch executable files on managed workstations.

Complete the following files to remotely launch files on managed workstations:

1. Select one or more workstations from the Workstation pane.
2. Right-click and select *Actions* > *Remote Launch*. The Remote Launch dialog is displayed:



3. Browse to select the file path or specify the file path.
   > Filename and Path – Specify the filename and path where the file is available on the target computer. Alternatively, you can browse to select the executable. File types supported are .exe (executables) and .msi (MSI installers). MSI installers are run in install mode by default. For example, if the executable MyApplication.exe is available at C:/AppFolder, specify *C:/AppFolder/MyApplication*.
4. Specify the Command Line Parameters with environment variables (optional):
   > Arguments – Specify the arguments that you want to apply with this executable. For example, if the executable is run from the command prompt with the command C:\AppFolder\MyApplication -o logFile.log, specify *-o logFile.log* for arguments. For .msi files, specify the arguments that you would normally specify when launching a .msi file with MSIEXEC. If you do not specify any argument for a .msi file, Deep Freeze will automatically append "/i" (install). Deep Freeze also replaces any display options with /qn, (quiet, no UI).
5. Click *OK*.

The file is remotely launched on the selected workstations.

Deleting, Importing and Exporting Custom Actions

Deleting Custom Actions

To delete Custom Actions, complete the following steps:

1. Go to *Action* > *Custom Actions.*
2. Select the Custom Action to be deleted.
3. Click *Delete*.

Importing Custom Actions

To import Custom Actions, complete the following steps:

1. Go to *Action* > *Custom Actions.*
2. Click *Import*.
3. Browse to select the .xml file to be imported.
4. Click *Open* to import the file.

Exporting Custom Actions

To export Custom Actions, complete the following steps:

1. Go to *Action* > *Custom Actions.*
2. Select the Custom Action to be exported.
3. Click *Export*.
4. The Export Custom Action to File dialog is displayed.
5. Specify a *File name* and click *Save*.

Console Customizer

The Console Customizer lets you specify which features and commands you want to be available in the Console, and save the result as a new Console that can be distributed in your organization.

The available settings are grouped into categories (Console functions, Workstation commands, Deep Freeze commands, Workstation install/uninstall commands, and Scheduler commands). Click on the plus (+) icon to the far left of each category to disclose the full list of settings available in that category.

Select or clear the individual checkboxes as required. Alternatively, select or clear the entire categories at once. Settings that are cleared will not be available in the new Enterprise Console you create. For an example on how to use the Console Customizer in a practical scenario, refer to Appendix D.

Complete the following steps to create Consoles with limited functionality:

1. Select *Tools* > *Console Customizer*.
2. The Console Customizer is displayed.



3. Select the features to be displayed in the new Console.
4. Click *Save As* to save the Console. Specify a name for the file.
5. When you double-click the newly created .exe file, the Console with the limited functionality is launched.

Deep Freeze Enterprise Console Shutdown

To shut down the Deep Freeze Console select *File > Exit* or click the close window button. Upon exit, you can choose to:

- Minimize the Console to the system tray.

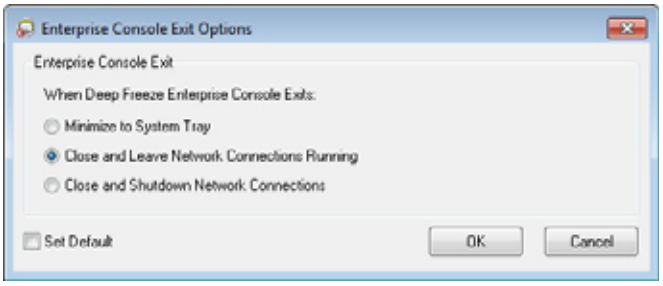
  This does not stop the Console and keeps the connections active. The Deep Freeze Console icon appears in the system tray. Scheduled tasks will still execute. To reopen the Deep Freeze Enterprise Console, right-click its icon located in the taskbar and select *Restore Deep Freeze Console*.

- Close Deep Freeze Console and leave the network connections running

  This closes the Console but keeps the connections to the computers active. Scheduled tasks will still execute.

- Close Deep Freeze Console and shut down network connections.

  This stops Console processes, closes the connections (including local service), and scheduled tasks will not start to execute. However, scheduled tasks that have started executing will continue.



The dialog will not appear on future exits once the *Set Default* option has been selected. To edit these settings select *Tools > Exit Options*.

Installing Deep Freeze on the Workstation

After a customized installation program file has been created using the Configuration Administrator, Deep Freeze can be deployed to computers using an Attended Install, a Target Install, the Silent Install System, or as part of an imaging process.



All background utilities and anti-virus software should be disabled and all applications should be closed prior to installation. These programs may interfere with the installation, which could result in Deep Freeze not functioning correctly.

The computer restarts after any type of installation is completed. Deep Freeze must be in a Thawed state for any type of uninstall to succeed.

Any existing ThawSpace will be deleted during an uninstall if:

- The option to retain existing ThawSpace was not checked in the Configuration Administrator.
- The ThawSpace was not created with Deep Freeze Enterprise Version 5 or later.

Attended Install or Uninstall

To install or uninstall Deep Freeze, complete the following steps:

1. Run the installation program file (*DFWks.exe*) on the computer. The following screen appears:
2. Click *Install* to begin the installation. Follow the steps presented, then read and accept the license agreement. Deep Freeze installs and the computer restarts.



Click *Uninstall* to uninstall Deep Freeze. Uninstall can only be clicked if Deep Freeze has previously been installed and the computer is currently Thawed. If there is an existing ThawSpace, Deep Freeze displays a dialog asking if it should be retained or deleted.



If the hard drive is too fragmented, it is not possible to create ThawSpace(s). A message is displayed prompting you to abort installation, or install Deep Freeze without ThawSpace(s).

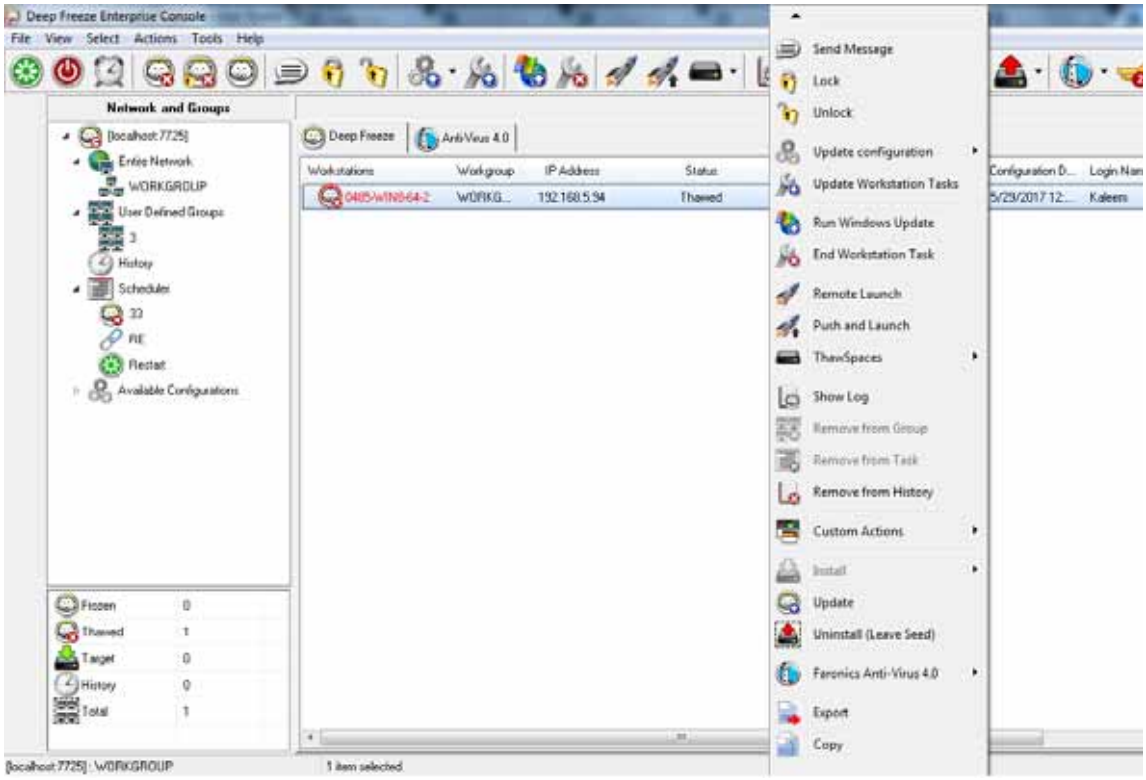


If you select *Delay Frozen reboot to complete Windows updates* (Advanced Options Tab in the Configuration Administrator) and install Deep Freeze, the installer checks if all Windows updates are completed. If the Windows updates are not completed, Deep Freeze installation will not proceed. Complete Windows updates and try installing Deep Freeze again.

If you disable *Delay Frozen reboot to complete Windows updates* and install Deep Freeze, ensure that all Windows updates are completed without using Deep Freeze. Disabling this option may result in the computer being stuck in a reboot cycle due to incomplete Windows updates.

Uninstalling Deep Freeze on the Workstation via the Console

The Enterprise Console can be used to uninstall Deep Freeze completely or to uninstall Deep Freeze but leave the Workstation Seed. A computer must be in a Thawed state in order to uninstall the program.



To uninstall Deep Freeze on a computer and leave the Workstation Seed, right-click on the Thawed workstation(s) and select *Uninstall (Leave Seed)*, as shown above. Or click the icon on the toolbar.

To completely uninstall Deep Freeze and the Workstation Seed, select the computer(s) to be uninstalled and click the *Uninstall* icon on the toolbar.

The computer must be Thawed before Deep Freeze can be uninstalled. The Enterprise Console prompts for confirmation. Once the uninstall is confirmed, Deep Freeze uninstalls and the computer restarts.

Silent Install or Uninstall

Deep Freeze can be rapidly installed to many computers over a network using the Silent Install System. Any deployment utility that allows execution of a command line on a remote computer can implement the Silent Install System. After the Silent Install is complete, the computer immediately restarts. The command line has the following options:

Syntax	Description
`[/Install]`	Install Deep Freeze using installation file
`[/Install /Seed]`	Install only the specified Workstation Seed file
`[/Install /Thawed]`	Install Deep Freeze using installation file and boot into Thawed state
`[/Uninstall]`	Uninstall Deep Freeze
`[/Uninstall /Seed]`	Uninstall Deep Freeze and leave the Workstation Seed installed
`[/PW=password]`	Set a password during installation*
`[/AllowTimeChange]`	Allow system clock to be changed*
`[/Freeze=C,D,...]`	Freeze only drives listed (Thaw all others)*
`[/Thaw=C,D,...]`	Thaw only drives listed (Freeze all others)*
`[/USB]`	Exempt external USB hard disks from protection
`[/FireWire]`	Exempt external FireWire hard disks from protection

Example Command Line

```
DFWks.exe /Install /Freeze=C /PW=password
```

In the above example, the Deep Freeze installation program file is named *DFWks.exe*. Only the C: drive will be Frozen. Any other drives on the computer will be Thawed. If the computer only has a C: drive, the [/Freeze] switch can be omitted. A password (password) will be created. After executing the command, Deep Freeze will install and the computer will restart Frozen and ready to use.

The Silent Install System does not work without the `[/Install]` or `[/Uninstall]` switch. Deep Freeze must be in a Thawed state before `[/Uninstall]` can be used.



To run the configuration command line options, Disable Command Line options on the Advanced Options tab must be cleared.





* These options are disabled by default.

Silent Install or Uninstall Using a Shortcut

Deep Freeze can be installed directly on a computer without having to use the installation dialog box by completing the following steps.

1. Locate the Deep Freeze installation program file (*DFWks.exe*) on the target computer.
2. Right-click on the icon and choose *Create Shortcut*.
3. Right-click on the shortcut and choose *Properties*.
4. Edit the path of the Target field by typing `/install` or `/uninstall` at the end of the path.

Example Shortcut Target:

```
C:\Documents and Settings\DFWks.exe /install
```

Double-clicking on the new shortcut results in the immediate installation or uninstallation of Deep Freeze, followed by a restart of the computer.

Deep Freeze must be in a Thawed state before `/uninstall` can be used.



If the hard drive is too fragmented, it is not possible to create ThawSpace(s). The installation is aborted.

Network Install on Multiple computers

The Silent Install System can also be used to install Deep Freeze on multiple computers over a network. If the workstations on the network use logon scripts, the scripts can be used to install Deep Freeze on all networked workstations automatically. All workstations will restart Frozen and ready for use after installation has completed.

Use the following command line syntaxes to create an install error report log file:

```
\\Server Name\Share Name\DFWks.exe /Install >> my.log
```

Installing Over Existing Deep Freeze Versions

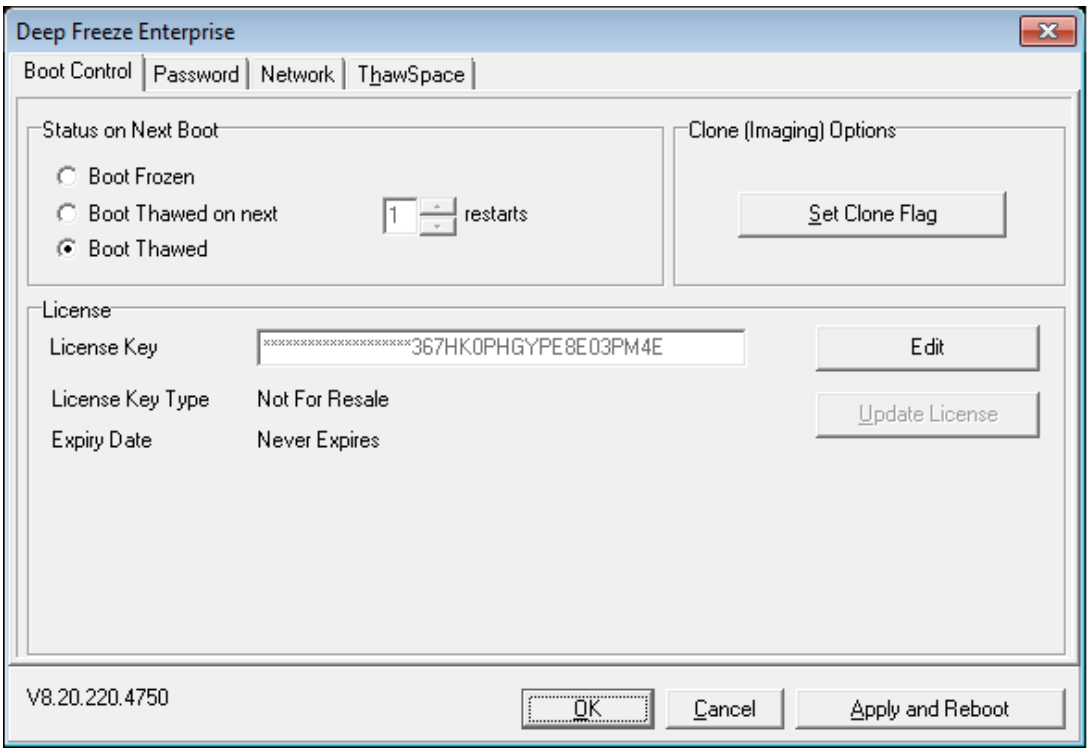
Unless the Update Deep Freeze Software feature is used (for Deep Freeze 6.5 and higher), all existing Deep Freeze versions must be uninstalled prior to performing any new Deep Freeze installation.

Installing Using Imaging

Deep Freeze has been designed to work with all major imaging and desktop management software. Use either an Attended Install or the Silent Install to install Deep Freeze on a master image.

Deep Freeze must be prepared for deployment before finalizing a master image. To prepare the master image for deployment complete the following steps:

1. Restart the computer into a *Thawed* state.
2. Launch Deep Freeze using the keyboard shortcut CTRL+SHIFT+ALT+F6. Alternatively, press *Shift* and double-click the Deep Freeze icon in the System Tray.
3. Enter the password and click *OK*.
4. Click *Set Clone Flag* in the *Boot Control tab*.
5. The message *The flag has been set successfully. Do you want to reboot your computer now?* is displayed. Click *Yes* to reboot the computer immediately. Click *No* to reboot the computer later.







The Set Clone Flag command is important during imaging since it boots the computers into a Thawed state if Deep Freeze is unable to read its configuration file after the image is successfully installed.

If the Clone Flag is not set, and if Deep Freeze is unable to read its configuration file, all drives are Frozen after the image is successfully installed.



If you are using Sysprep, make sure you set the Clone Flag after preparing the system for imaging and just before starting Sysprep.

After imaging, the computers require an additional restart for Deep Freeze to correctly detect the changes in disk configuration. If the computers are imaged in an unattended mode, steps should be taken to ensure the computers are restarted to allow the configuration to update.

To return to the Frozen state after imaging is complete, set Deep Freeze to Boot Thawed on next *n* number of restarts (in the master image) so that after *n* number of restarts, the computer is automatically Frozen. Alternatively, use Deep Freeze Command Line Control to Freeze selected computers.

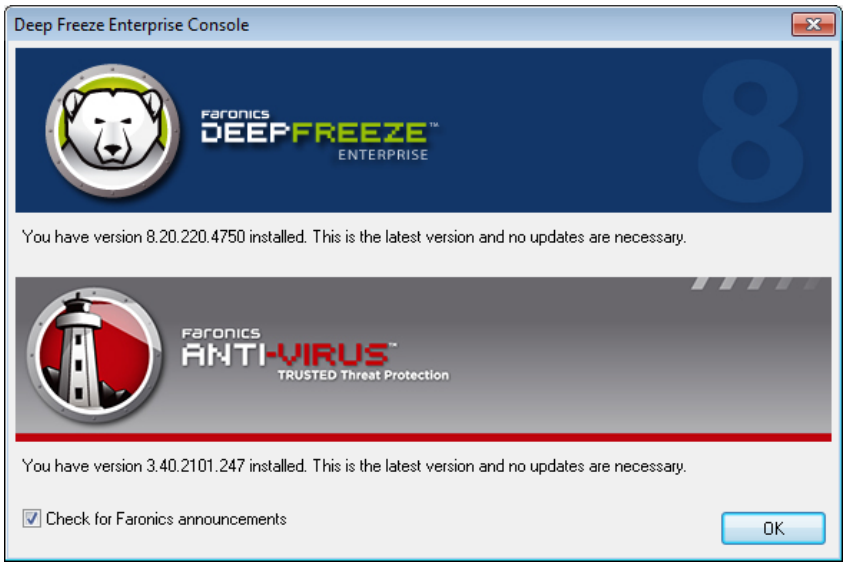
Target Install

Deep Freeze can also be deployed using a Target Install from the Enterprise Console.

Check for Updates

Deep Freeze allows you to check if there are newer versions available.

Go to *Help* > *Check for updates*. This checks if there are newer versions of Deep Freeze available.



If a new version is available, click *Download the latest version* to update Deep Freeze.



Managing Deep Freeze Computers

This chapter describes managing computers where Deep Freeze is installed.

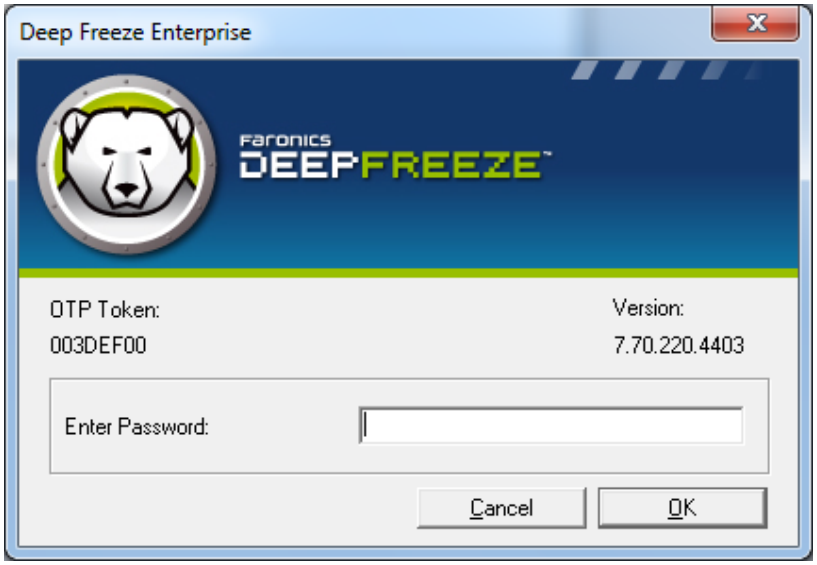
Topics

Login Screen
Status Tab
Password Tab
Network Tab
ThawSpace Tab
Permanent Software Installations, Changes, or Removals

Login Screen

Use one of the following ways to access Deep Freeze on a computer.

1. If the Deep Freeze icon is shown in the System Tray, hold down the SHIFT key and double-click the Deep Freeze icon. If the Deep Freeze is running in Stealth Mode and if the Deep Freeze icon is not displayed, the keyboard shortcut CTRL+ALT+SHIFT+F6 must be used to access the logon dialog.



2. Enter the administrator password and click *OK* to log on to Deep Freeze.

As an additional security feature, Deep Freeze prevents Brute Force attacks by automatically restarting the computer after 10 unsuccessful login attempts.

Launching Deep Freeze on Touchscreen Devices

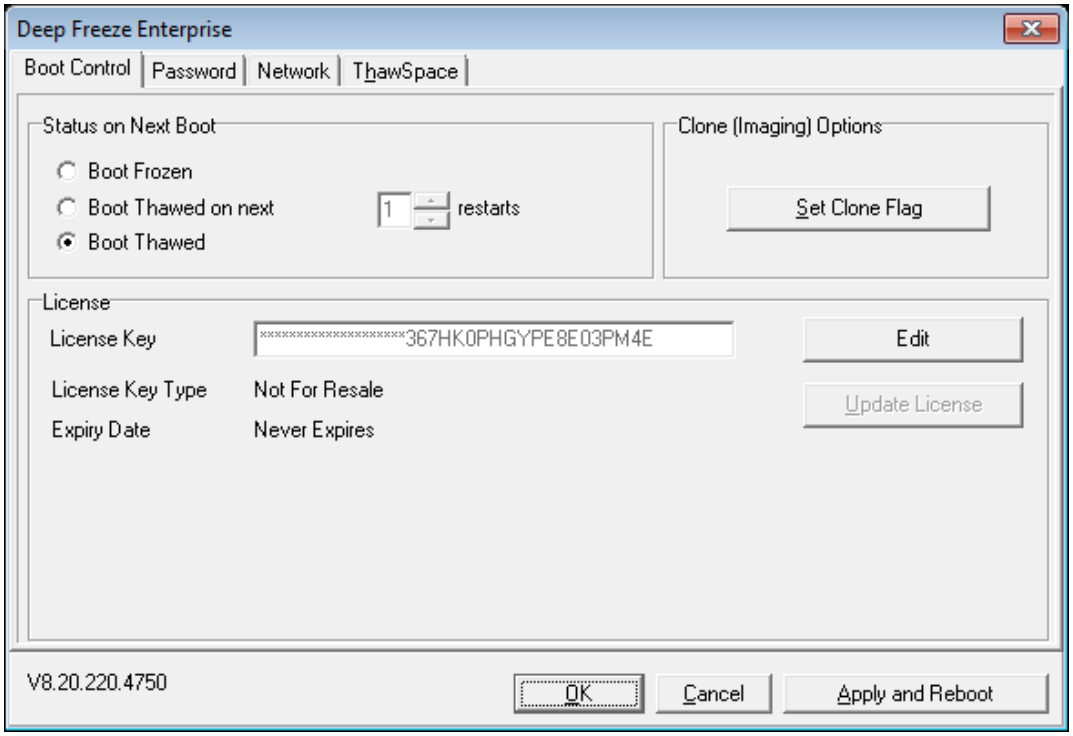
You can use CTRL+ALT+SHIFT+6 or CTRL+ALT+SHIFT+F6 to launch Deep Freeze on touchscreen devices. However, you must enable the full keyboard before using the shortcut. You can also touch and hold on the system tray to launch the Deep Freeze context-menu.

Status Tab

The *Status* tab displays the following options:

Status on Next Boot

The Status tab is used to set the mode Deep Freeze will be in after the next restart.



Choose one of the following options:

- Boot Frozen – To ensure that the computer is Frozen the next time it is restarted.
- Boot Thawed on next – To ensure that the computer is Thawed each time it is restarted for the next specified number of restarts. When that number of restarts is exceeded, the computer will boot Frozen.
- Boot Thawed – To ensure that the computer is Thawed each time it is restarted.

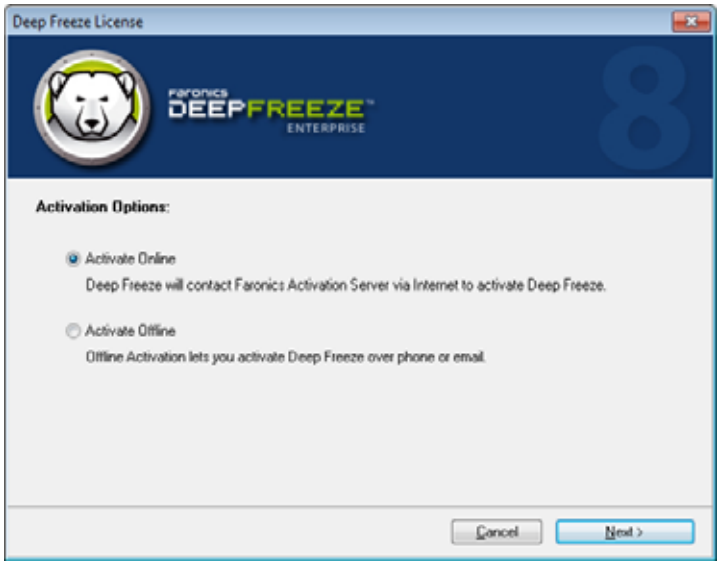
Select the radio button next to the desired choice and click *OK* to save any changes. Clicking *Apply and Reboot* will save any changes and reboot the computer immediately.

Clone

The *Clone* pane is used to prepare master images for the deployment process. For more information, refer to the Installing Using Imaging section.

License

1. To update the License Key, click *Edit* and enter the License Key in the *License Key* field.
2. Click *Update License*. This converts Deep Freeze from the *Evaluation* version to a *Licensed* version. The *License Key Type* field displays the *License Key*. The *Expiry Date* displays the date and time when the license expires.
3. Click *Activate Now*. Two options are available:



> Select *Activate Online* to activate Deep Freeze License online. This option is same as step 1. Click *Next* after selecting this option. Deep Freeze is activated online on clicking *Next*.

> Select *Activate Offline*. This option allows you to activate by phone or email. Click *Next* after activating. The Activate Offline screen is displayed:



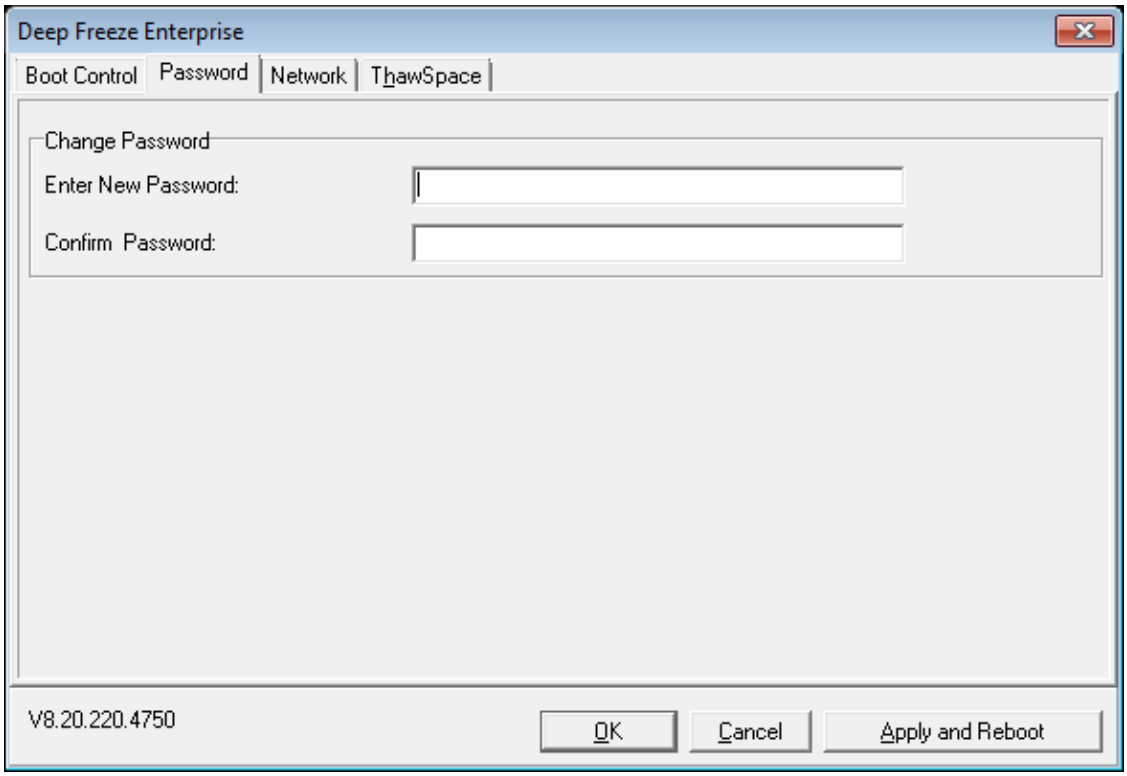
4. Click *Create Offline Activation Request File* and click *Save*. Send the file to activation@faronics.com to receive an Activation Response File. Browse to select the *Activation Response File* received from Faronics. Click *Apply Offline Activation Request File*.



The License Key is automatically updated on all computers communicating with the Enterprise Console. If a computer is offline (shut down or disconnected from the network), the License Key is updated when the computer communicates with the Enterprise Console.

Password Tab

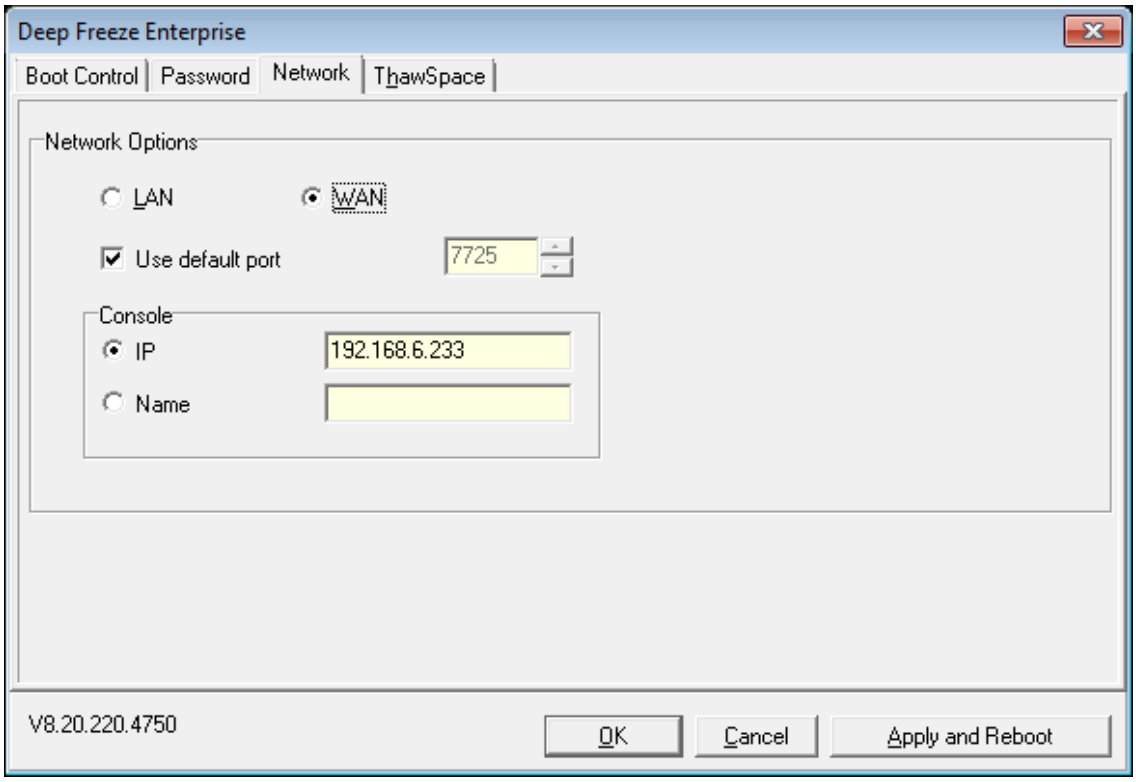
The *Password* tab allows you to change the password.



1. Specify a new password in the *Enter new password* field.
2. Confirm the new password by re-entering the same password in the *Confirm password* field.
3. Click *OK*.
4. The password is changed and a confirmation dialog is displayed.

Network Tab

The *Network* tab can be used to configure the network options on a computer.



To choose either the *LAN* or the *WAN* method of communication, click the preferred option.

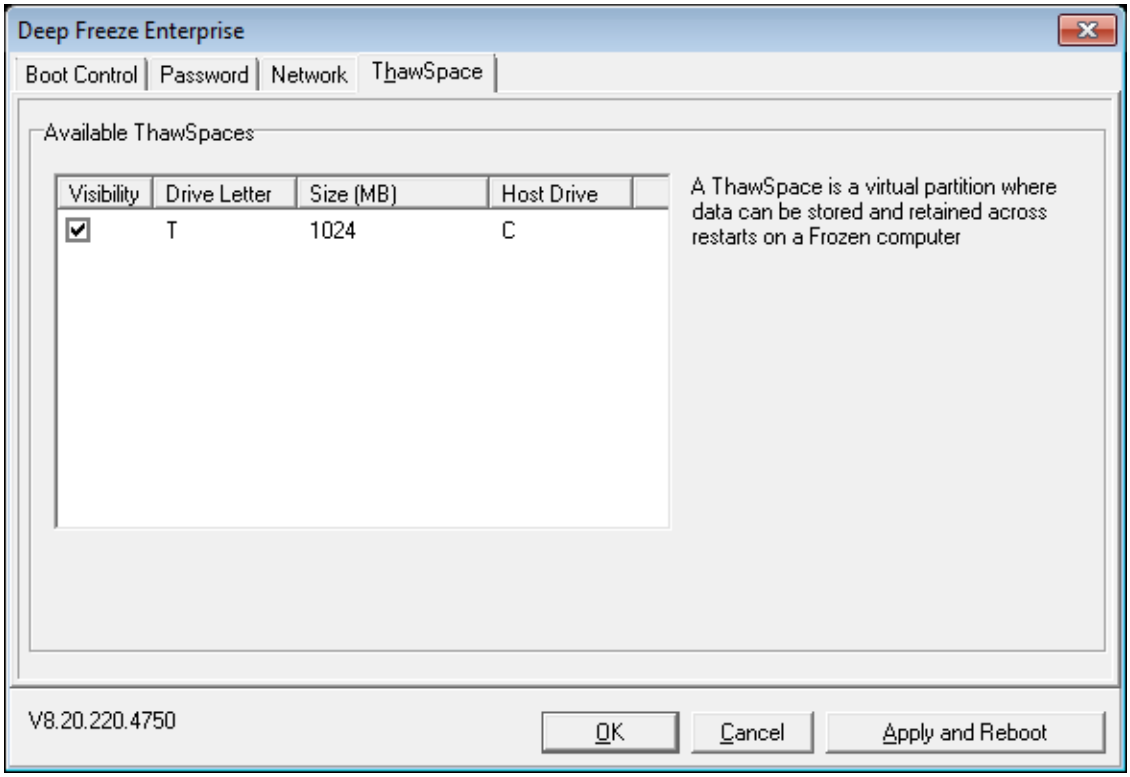
The default port number can be changed by clearing the *Use Default Port* checkbox and entering the required port number.

For more information on network configuration, refer to Appendix B.

ThawSpace Tab

ThawSpace is a virtual partition on a computer that can be used to store programs, save files, or make permanent changes. All files stored in the ThawSpace are saved after a restart, even if the computer is Frozen.

ThawSpace is only available if it was set to be created in the Deep Freeze Enterprise Configuration Administrator.



After uninstalling Deep Freeze, all the ThawSpaces become visible. When Deep Freeze is reinstalled, the ThawSpaces are *Visible* or *Hidden* as per the original settings in the ThawSpace tab.

Any existing ThawSpace is deleted during an uninstall if any of the following apply:

- The option to retain existing ThawSpace was not selected in the *Configuration Administrator.*
- The ThawSpace was not created with Deep Freeze Version 5 or higher.

Permanent Software Installations, Changes, or Removals

Computers must be Thawed for any permanent changes to take effect. Installation of software often requires one or more restarts to complete the installation.

Deep Freeze helps administrators overcome challenges with maintaining the configuration of their computers in a production environment. Deep Freeze protects computers from unauthorized changes, viruses and malware, that can leave computers in a non-functional state. Deep Freeze also provides features to retain user data while protecting the computer.

For more information on how to implement Deep Freeze and ensure that the user data is retained, refer to *Deep Freeze – Retaining User Data available* at http://www.faronics.com/library.



Managing Anti-Virus

This chapter describes installing and using Anti-Virus with Enterprise Console.

Topics

Anti-Virus Overview
Anti-Virus Reports
Migrating to the New Anti-Virus
Enable Anti-Virus on Enterprise Console
Install Anti-Virus Client on the workstation
Anti-Virus Configuration
Using Faronics Anti-Virus from the Enterprise Console
Scheduling Anti-Virus Tasks
Using Anti-Virus on the Workstation
Check for Anti-Virus Updates
Update Faronics Anti-Virus
Updating Anti-Virus Definitions
Uninstall Anti-Virus Client from the Enterprise Console
Disable Faronics Anti-Virus from the Enterprise Console

Anti-Virus Overview

Anti-Virus can be installed and used via the Enterprise Console. Using Anti-Virus is optional. Deep Freeze Enterprise can also be used independently without using Anti-Virus.

The following sections are explained:

- Enable Anti-Virus on Enterprise Console
- Install Anti-Virus Client on the workstation
- Anti-Virus Configuration
- Using Anti-Virus from the Enterprise Console
- Scheduling Anti-Virus Tasks
- Using Anti-Virus Client on the workstation
- Check for Updates
- Update Faronics Anti-Virus
- Uninstall Anti-Virus Client from the workstation
- Disable Anti-Virus on the Enterprise Console

Anti-Virus Reports

Anti-Virus Reports provides an overview of each workstation's antivirus version, protection status, Active Protection and firewall status, virus definition version, and the last update time. Also includes the last scan date and date of the last detected threat.

- Anti-Virus Definition Update Status: Displays details of Anti-Virus definition update activity on the workstations.
- Anti-Virus Status: Displays details of Anti-Virus activity on the workstations.
- Anti-Virus Compliance and Threat: Displays historical information about Threats by Number of Detections on workstations.
- Anti-Virus Scan History: Displays historical information about past scans.
- Anti-Virus Quarantine: Displays information about quarantined items on each workstation.

Migrating to the New Anti-Virus

Complete the following steps to migrate to the new Anti-Virus:

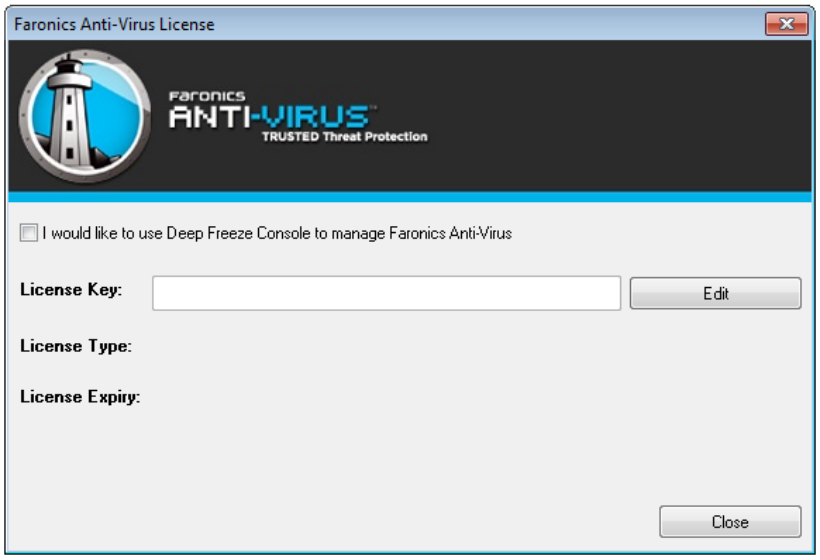
1. Uninstall Legacy Anti-Virus.
2. Configure the new Anti-Virus policy.
3. Install new Anti-Virus.

Enable Anti-Virus on Enterprise Console

Anti-Virus is now part of the Enterprise Console and can be enabled from within. You need to purchase a separate license for Anti-Virus.

Complete the following steps to enable Faronics Anti-Virus:

1. Launch the *Deep Freeze Enterprise Console*.
2. Go to *Tools* > *Licensing* > *Faronics Anti-Virus License*.



3. Select *I would like to use Deep Freeze Console to manage Faronics Anti-Virus*.
4. Click *Edit*.
5. Enter the License Key and click *Update License*.
6. Click *Close*. The Anti-Virus installer files are downloaded. The Anti-Virus columns are displayed in the Workstation pane. The Anti-Virus sub-node is added under *Available Configuration* in the Network and Groups pane.

Install Anti-Virus Client on the workstation

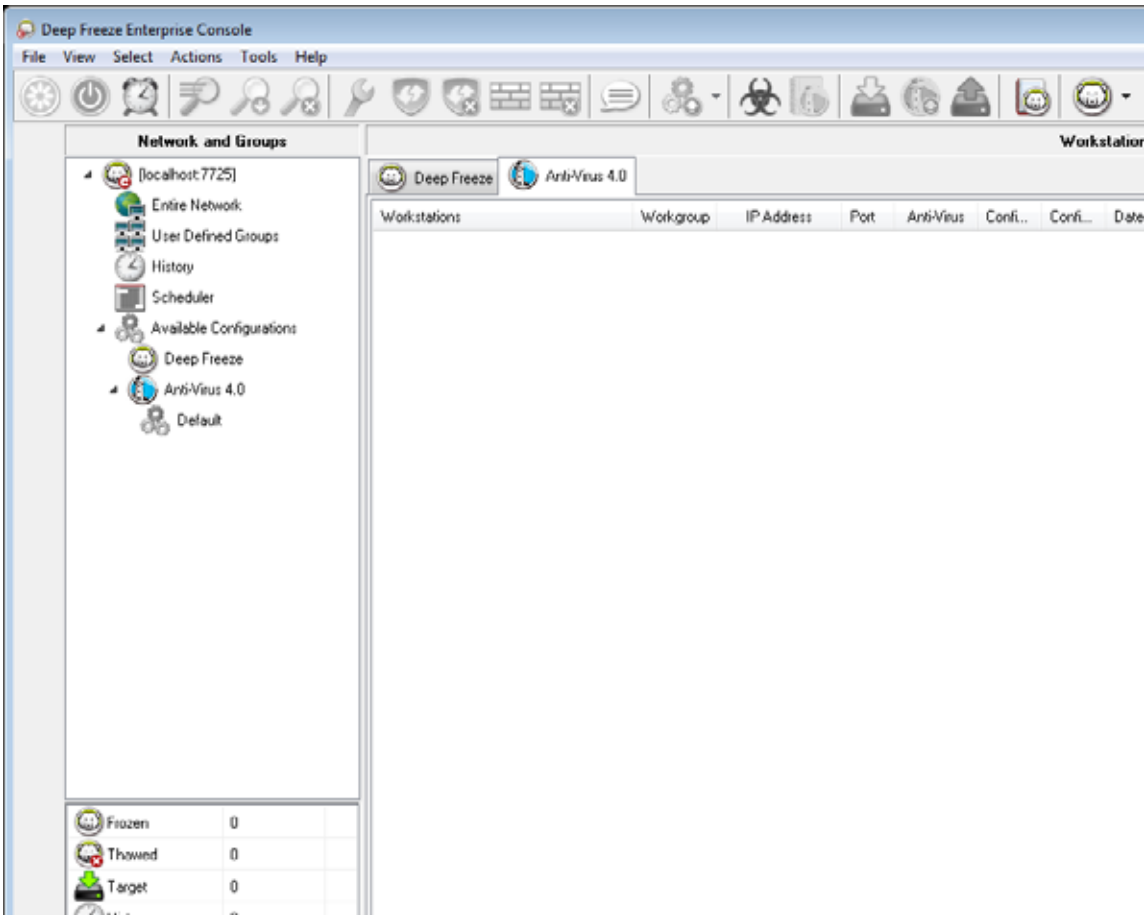
Before installing Anti-Virus on the workstation, ensure that Deep Freeze Workstation Install File or Deep Freeze Seed has been deployed to the workstation and the workstation is in a Thawed state.

Complete the following steps to install Anti-Virus onto the workstation:

1. Select a workstation (or multiple workstations) from the *Workstations* pane > *Anti-Virus* tab.
2. Click the Anti-Virus icon in the menu bar and select *Install Faronics Anti-Virus*.
3. Select the *Remove any incompatible antivirus products before installing Faronics Anti-Virus* checkbox to remove existing anti-virus programs.
4. Click *OK* to confirm the action.

The workstation reboots and Anti-Virus client is installed on the workstations.

The Anti-Virus options are enabled in the Anti-Virus tab.



Anti-Virus Configuration

An Anti-Virus configuration contains all the settings on how Anti-Virus runs on the workstation(s). A configuration contains the action taken by the program, schedule, proxy servers, error reporting and the functionality allowed to the user on the workstation(s). The following sections explain how an Anti-Virus configuration is created and applied.

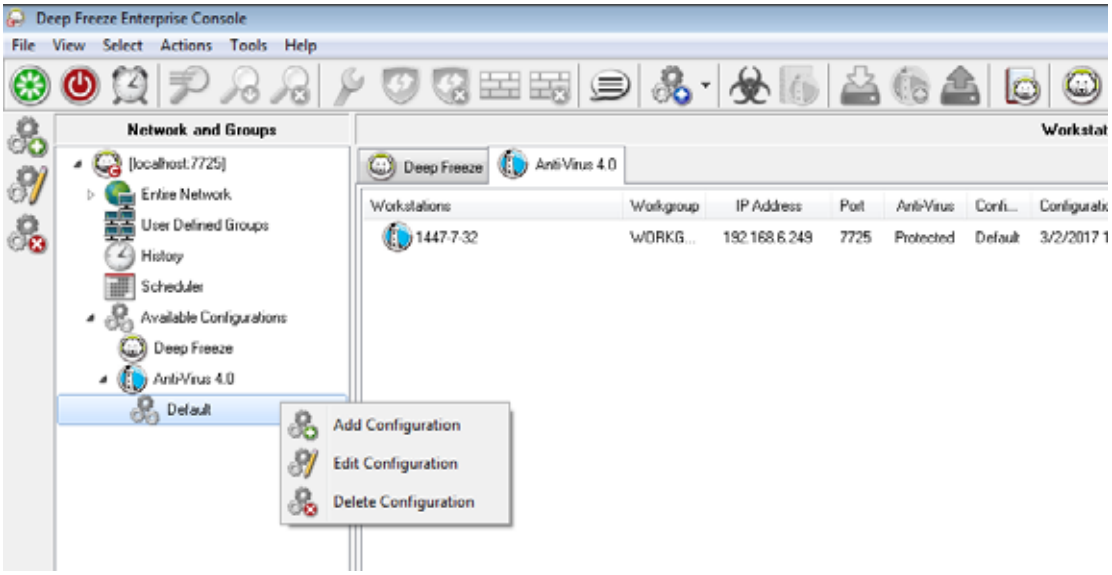


Anti-Virus contains a *Default* configuration. The Default configuration contains the most optimum configuration settings for managing Anti-Virus.

Creating Anti-Virus Configuration

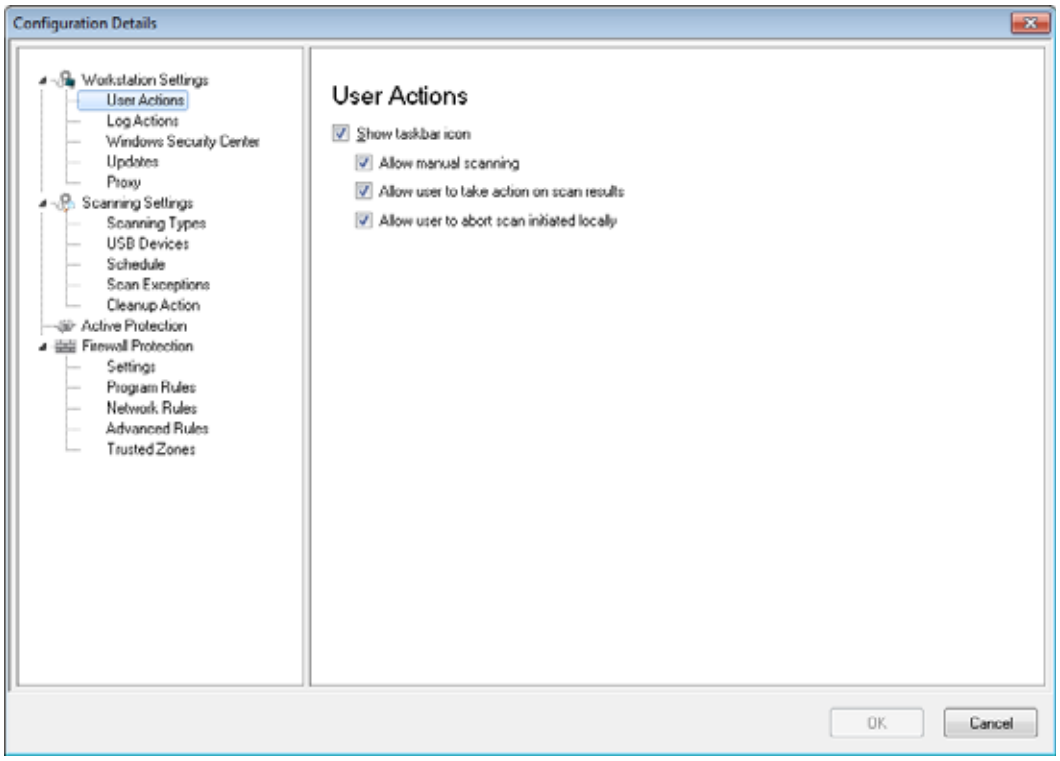
Complete the following steps create a new Anti-Virus configuration:

1. Launch the Enterprise Console.
2. In the *Network and Groups Pane*, go to *Available Configurations* > *AntiVirus*.
3. Right-click and select *Create new configuration*.



4. Specify settings in the *Workstation Settings* node:

- User Actions pane



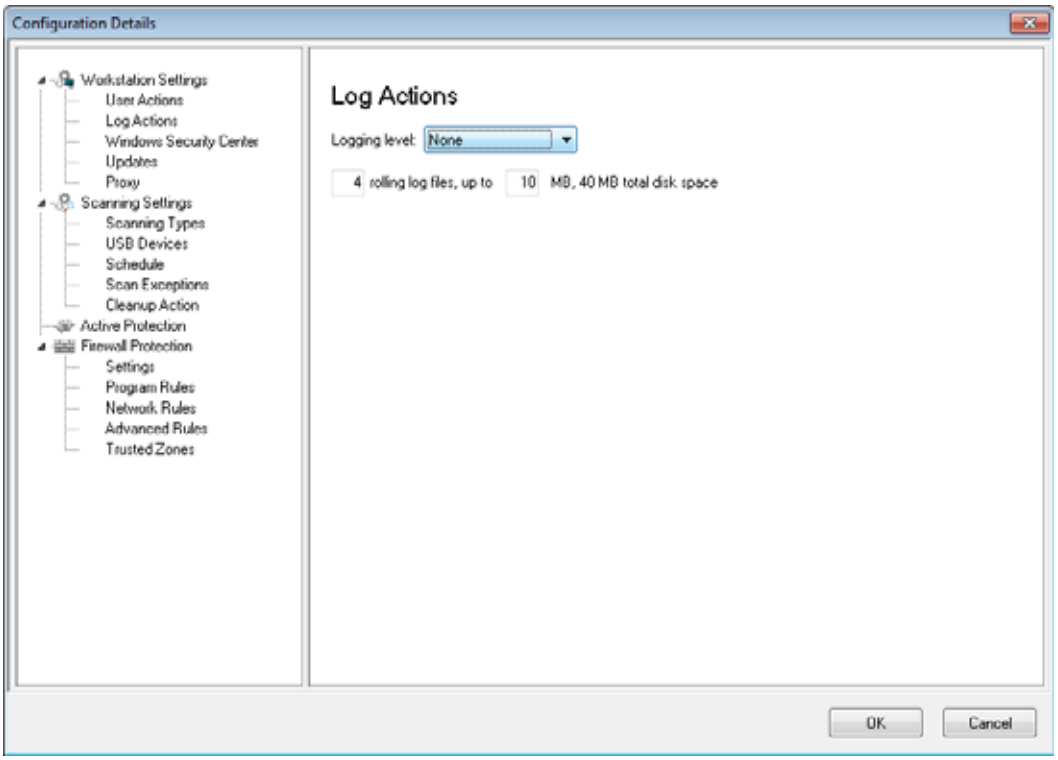
> Show taskbar icon – Select the checkbox to display Faronics Anti-Virus icon on the taskbar at the workstation(s). If this checkbox is not selected, Faronics Anti-Virus will be hidden to the user.

~ Allow manual scanning – Select the checkbox to allow users to manually initiate Faronics Anti-Virus scanning at the workstation(s).

~ Allow user to take action on scan results – Select the checkbox to allow the workstation user to take action on the scan results.

~ Allow user to abort a scan initiated locally – Select the checkbox to allow users to abort the scan initiated locally at the workstation.

- Log Actions pane

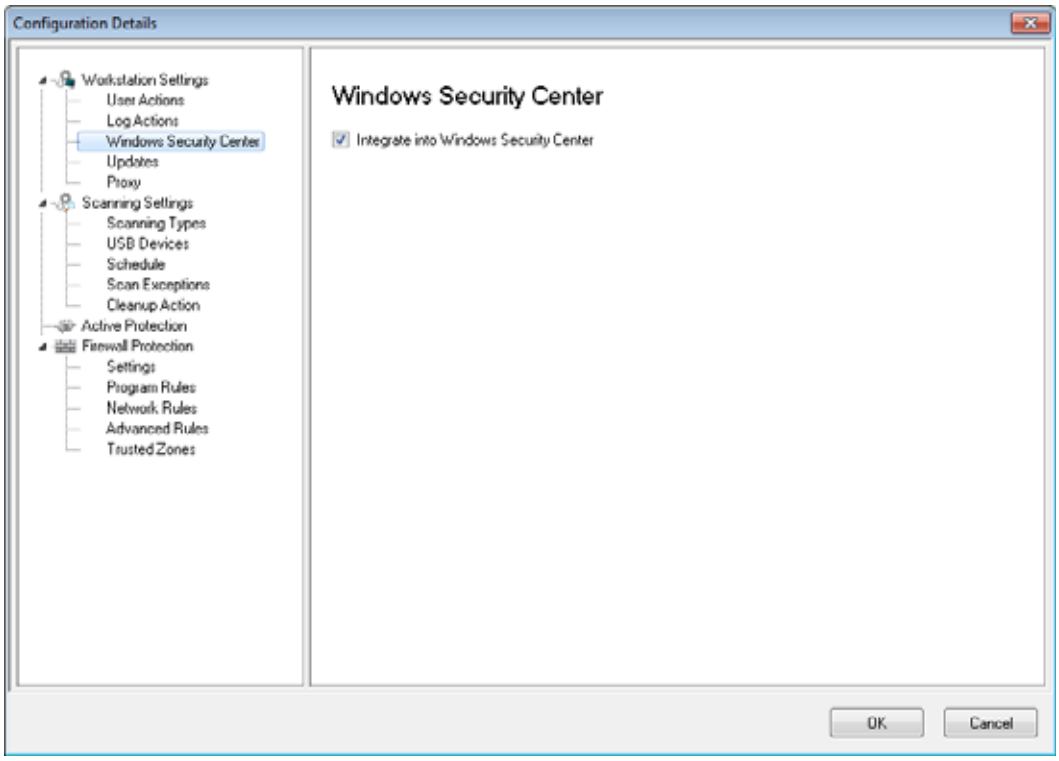


> Logging Level – Select the logging level. Select *None* for no logging. Select *Error* to log the error message. Select *Trace* for trace. Select *Verbose* for detailed logging.

> Number of logging files – Specify the number of logging files. The logging information is stored in the files serially. For example, if there are 3 files A, B and C, Faronics Anti-Virus first writes the error logs to file A. Once file A is full, it starts writing to file B and finally file C. Once file C is full, the data in file A is erased and new logging data is written to it.

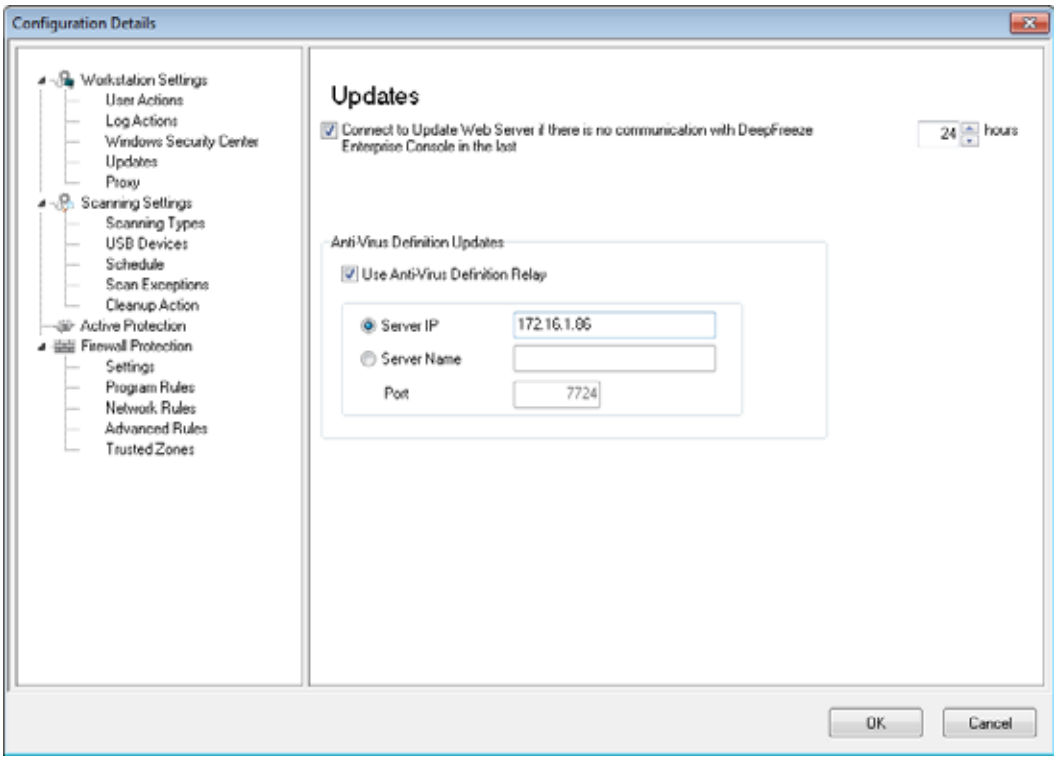
> File size – Select the size of each file in MB.

- Windows Security Center pane



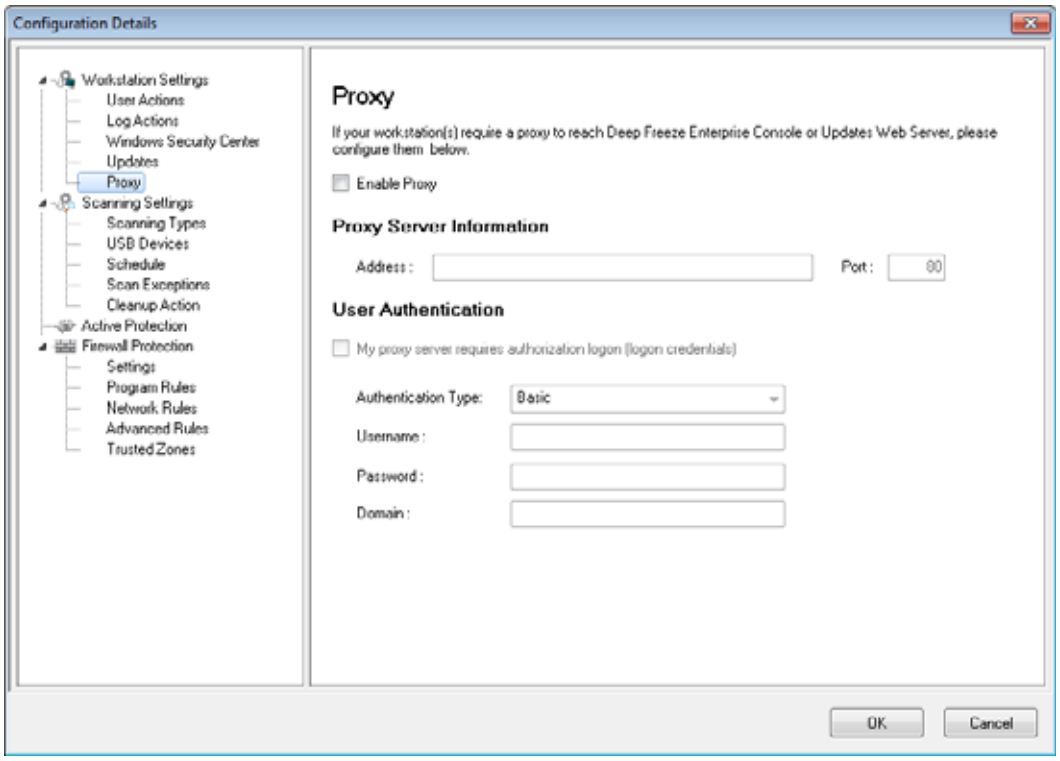
> Integrate into Windows Security Center – Select the checkbox to integrate Faronics Anti-Virus into the Windows Security Center. Windows Security Center will notify you via the System Tray if Faronics Anti-Virus is active or inactive.

- Updates pane



> Connect to Updates Web Server if there is no communication with Faronics Core Server in the last x hours – Select the checkbox to connect to the Updates Web Server and download Virus Definitions if the workstation loses contact with Faronics Core Server. If you do not select this checkbox, the Virus Definitions will not be updated if the workstation loses the connection with the Faronics Core Server.

- Proxy pane



> Enable Proxy – Select the checkbox if the workstation(s) require a proxy to reach Faronics Core Server or Updates Web Server.

> Proxy Server Information – Specify the *Address* and *Port*.

> User Authentication

My proxy server requires authorization (logon credentials) – If the server requires authentication, specify values for the following fields:

~ Authentication Type – Select the authentication type.

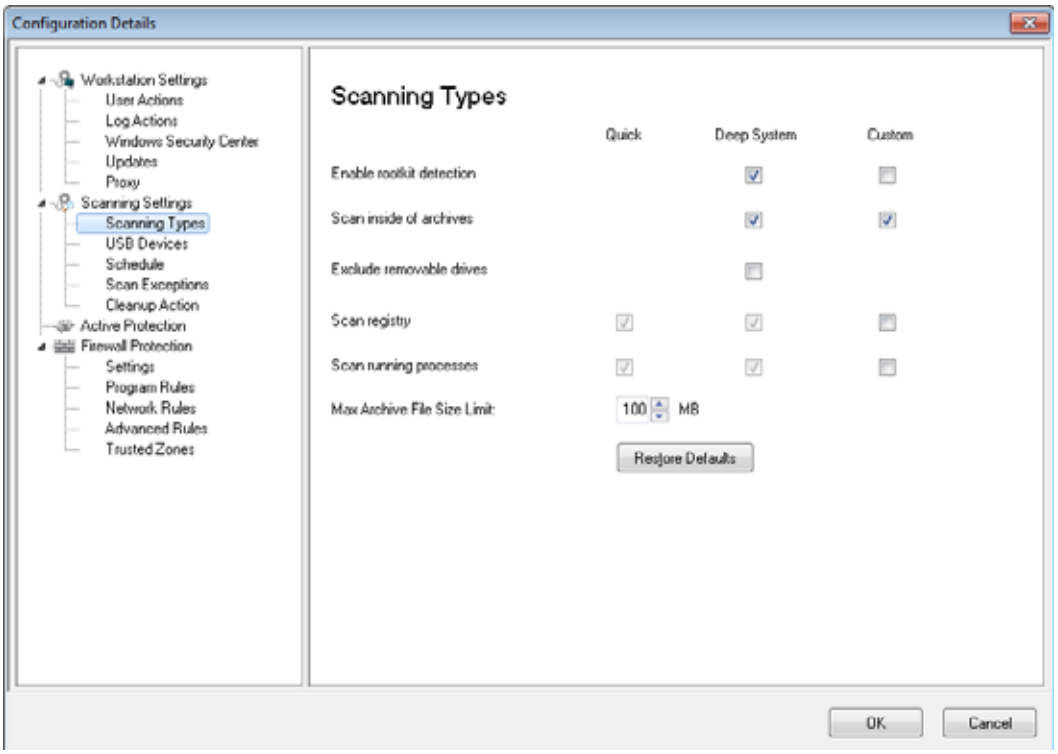
~ Username – Specify the username.

~ Password – Specify the password.

~ Domain – Specify the domain.

5. Specify settings in the *Scanning* Settings node:

- Scanning Types pane



Faronics Anti-Virus provides three types of scans:

> Quick Scan – Scans the commonly affected areas of your computer. This is shorter in duration than the Deep System Scan. Quick Scan also uses less memory than the Deep System Scan.

> Deep System Scan – Performs a through scan of all areas of the computer. The time taken for the scan depends on the size of your hard drive.

> Custom Scan – Performs a scan based on the selections made in the *Policy Details* dialog.

For each type of scan, select the following options (some options may be grayed out depending on the type of scan):

> Enable rootkit detection – Detects if the computer is infected with a rootkit.

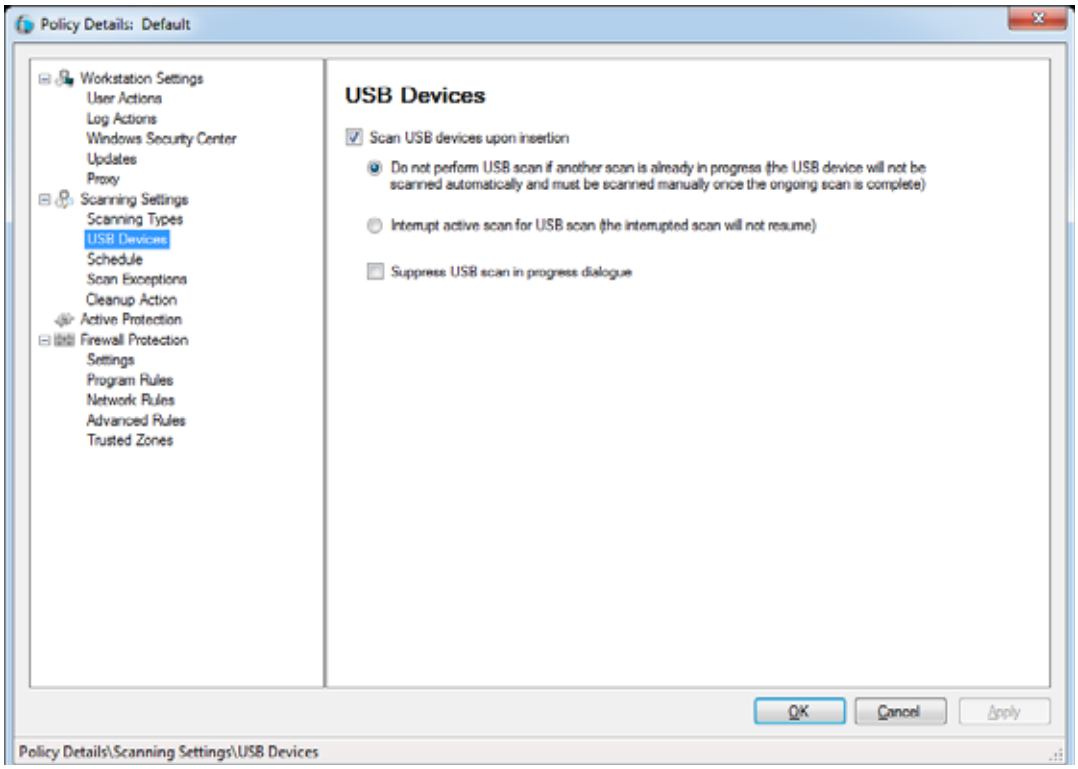
> Scan inside of archives – Scans the contents of a zip file. Select for the scan to include archive files, such as .RAR and .ZIP files. When a .RAR file is found to contain an infected file, the .RAR file will be quarantined. If a .ZIP file is found to contain an infected file, the infected file is quarantined and replaced by a .TXT file with text indicating that it was infected and that it has been quarantined. Specify the *File Size Limit.*

> Exclude removable drives (e.g USB) – Excludes the removable drives from the scan process. Any external hard disks, USB drives etc will not be scanned.

> Scan the registry – Scans the registry.

> Scan running process – Scans all running processes.

- USB Devices pane



Scan USB drives upon insertion – Select the checkbox to scan USB drives upon insertion and select one of the following options:

> Do not perform USB scan if another scan is already in progress – Select this option to ensure that an active scan is not interrupted when a USB drive is inserted. The USB drive must be manually scanned once the active scan is complete.

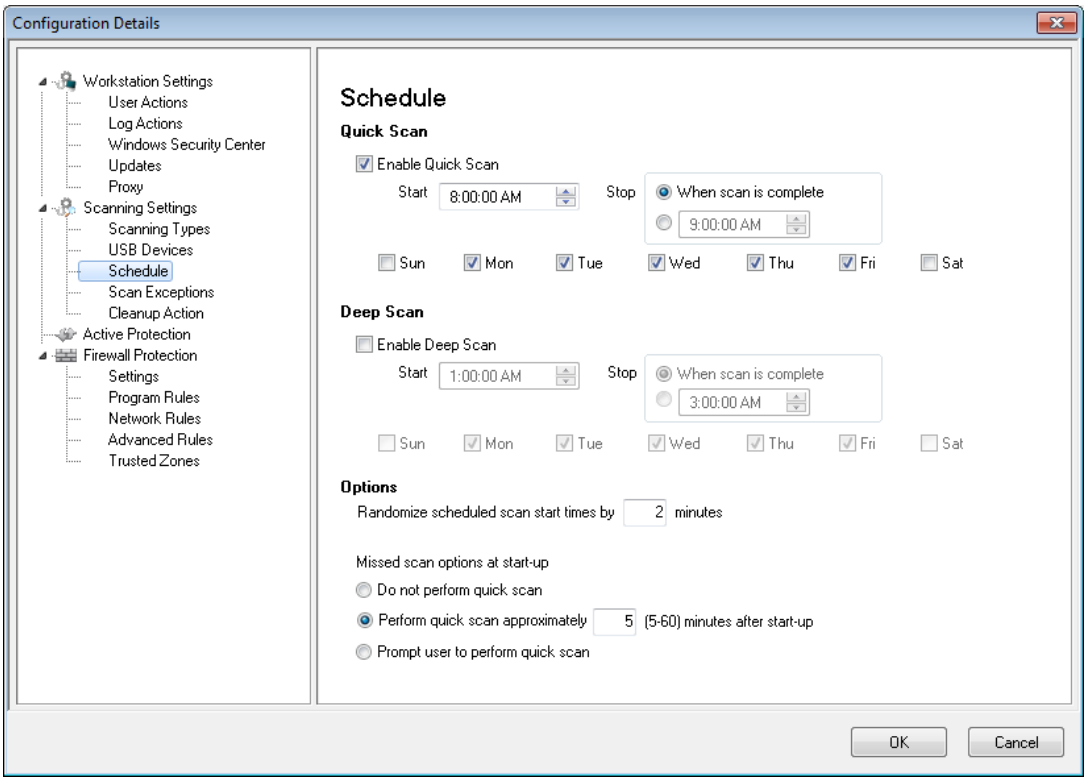
> Interrupt active scan for USB scan – Select this option to interrupt an active scan to scan the USB drive when it is inserted. Once the active scan is interrupted, it will not resume automatically and must be restarted manually.

> Suppress USB scan in progress dialogue – Select this option to hide indications that Anti-Virus is scanning USB drives when they are inserted; no Anti-Virus interface will open, and the system tray icon will not display tooltips indicating a scan in progress. Users will be notified at the end of a scan if a virus was found, but if no viruses were detected there will be no notification that the scan occurred.

Note that if the Scan USB drives upon insertion option is not selected, this option is ignored.

If the *Allow Manual Scanning* checkbox is selected in the *Workstation Settings* tab > *User Actions* pane, the USB device is scanned automatically. If the *Allow Manual Scanning* checkbox is not selected, the USB device is not scanned automatically.

- Schedule pane



Quick Scan:

> Enable Quick Scan – Select the checkbox to enable Quick Scan.

> Start – Specify the start time.

> Stop – Specify the end time. The maximum duration between the *Start* time and *Stop* time is *23.59* hours. The scan ends if all the files are scanned before the *Stop* time. If the scan is not complete before the *Stop* time, it is aborted at the *Stop* time. Alternatively, select *When scan is complete* to ensure that scan is completed.

> Days – Select the days when the scheduled Quick Scan will take place.

Deep Scan:

> Enable Deep Scan – Select the checkbox to enable Deep Scan.

> Start – Specify the start time.

> Stop – Specify the end time. The maximum duration between the *Start* time and *Stop* time is 23.59 hours. The scan ends if all the files are scanned before the *Stop* time. If the scan is not complete before the *Stop* time, it is aborted at the *Stop* time. Alternatively, select *When scan is complete* to ensure that scan is completed.

> Days – Select the days when the scheduled Deep Scan will take place.

Options:

> Randomize scheduled scan start times by x minutes – Specify the number of minutes. The scheduled scan start time is randomized to reduce the impact on network traffic. Faronics Anti-Virus reports to Faronics Core when the scanning starts. This might impact the network traffic if the scan for multiple systems start at the same time.

Missed scan options at start-up – Select one of the following options on how a scan will be performed if the workstation was not *ON* during a scheduled scan:

> Do not perform quick scan – Select this option if you do not want to perform quick scan on startup.

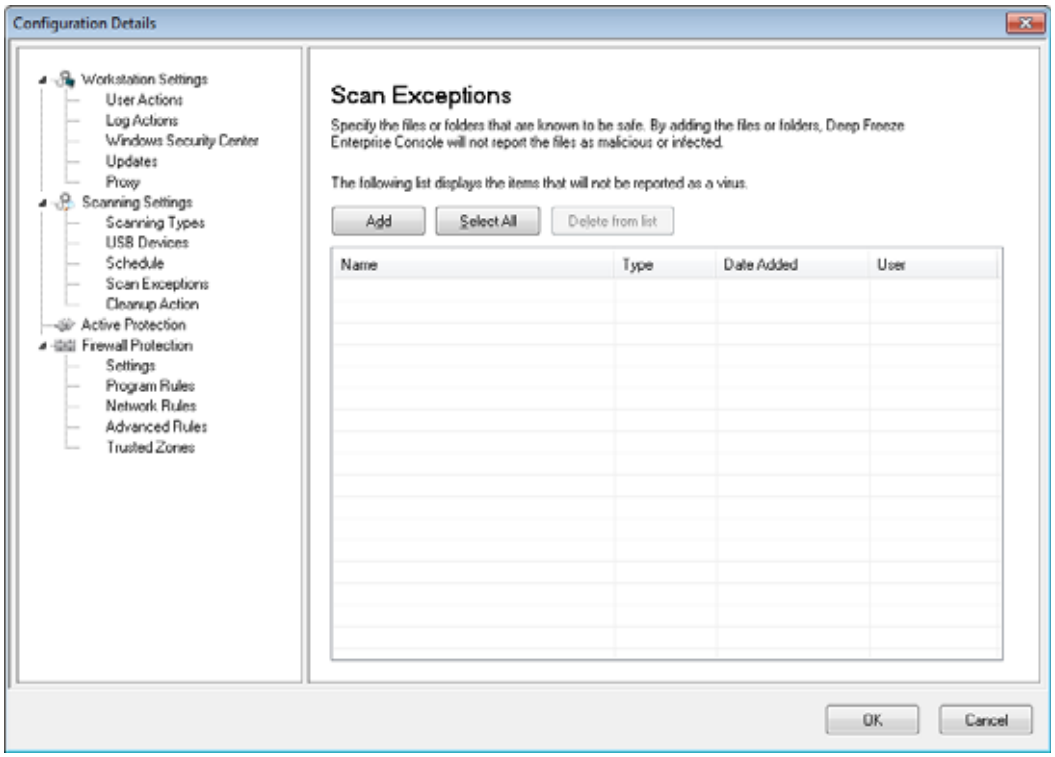
> Perform quick scan approximately x minutes after start-up – Specify the number of minutes after start-up when Faronics Anti-Virus must perform a quick scan.

> Prompt user to perform Quick Scan – Select this option to prompt the user to perform a quick scan.

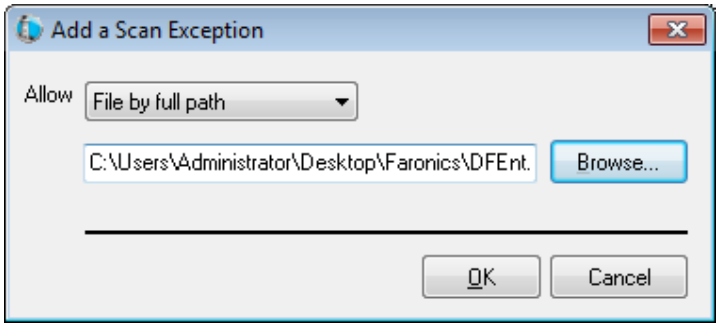
- Scan Exceptions pane

Folders or files that are known to the safe and free of infections can be added to the Scan Exceptions tab. Files added to the Scan Exceptions tab will always be scanned by Faronics Anti-Virus. However, Faronics Anti-Virus will never report the files as malicious or infected. This feature is useful since files and folders that are known to be safe by the Administrator will not be reported as malicious.

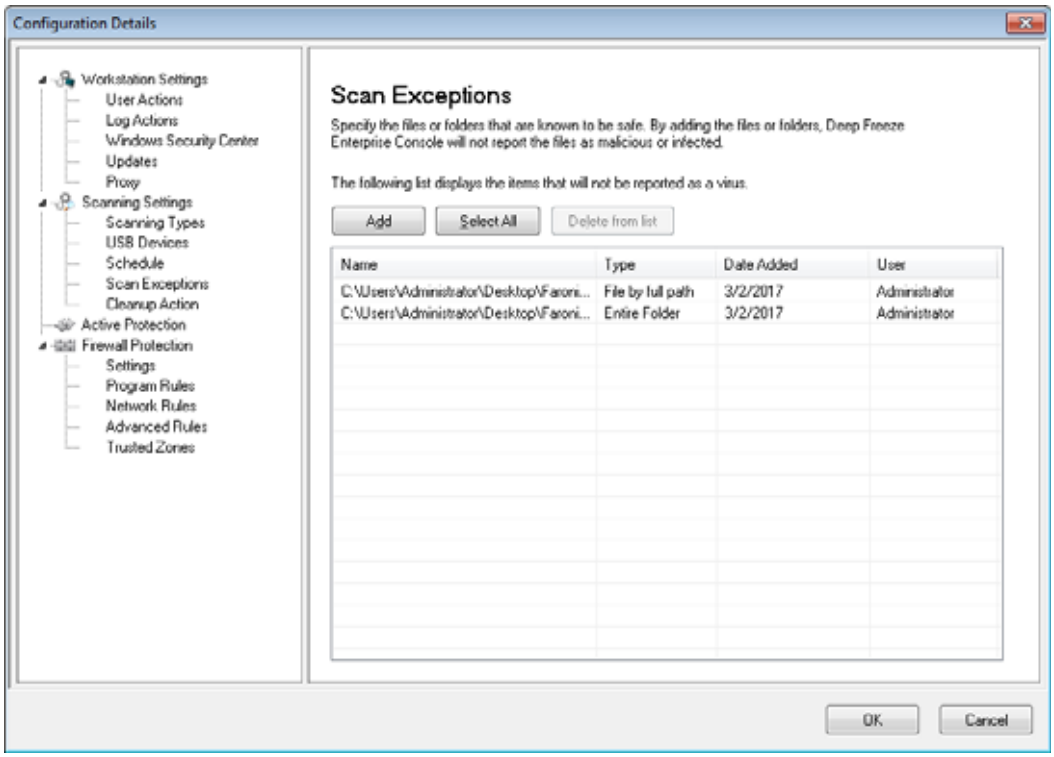
A. Click *Add*.



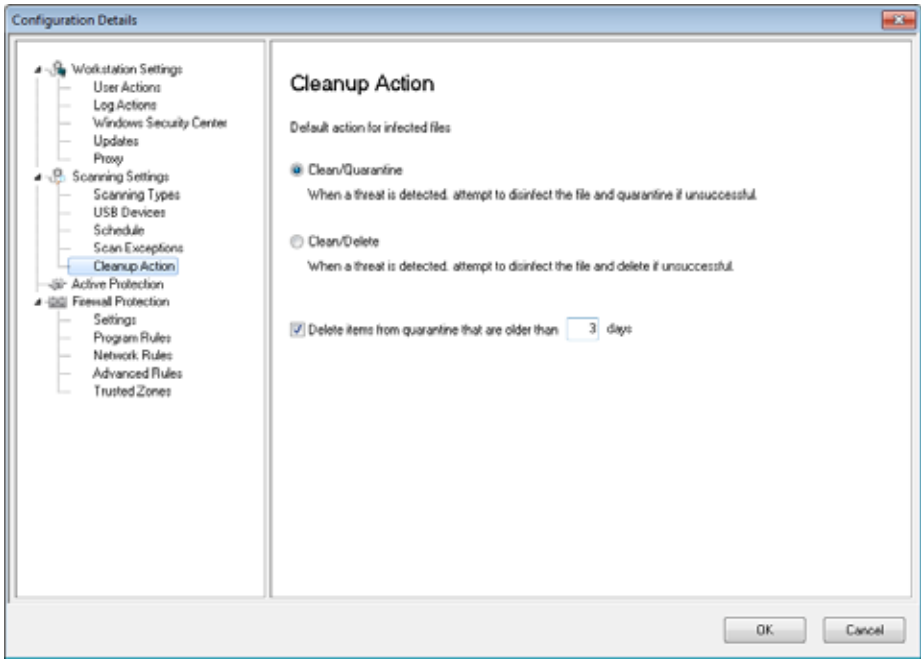
B. In the *Add* dialog, select *File by full path* or *Entire folder*. Click *Browse* to select the file or folder and click *OK*.



C. The *File by full path* is added to the Scan Exceptions pane.



- Cleanup Action pane

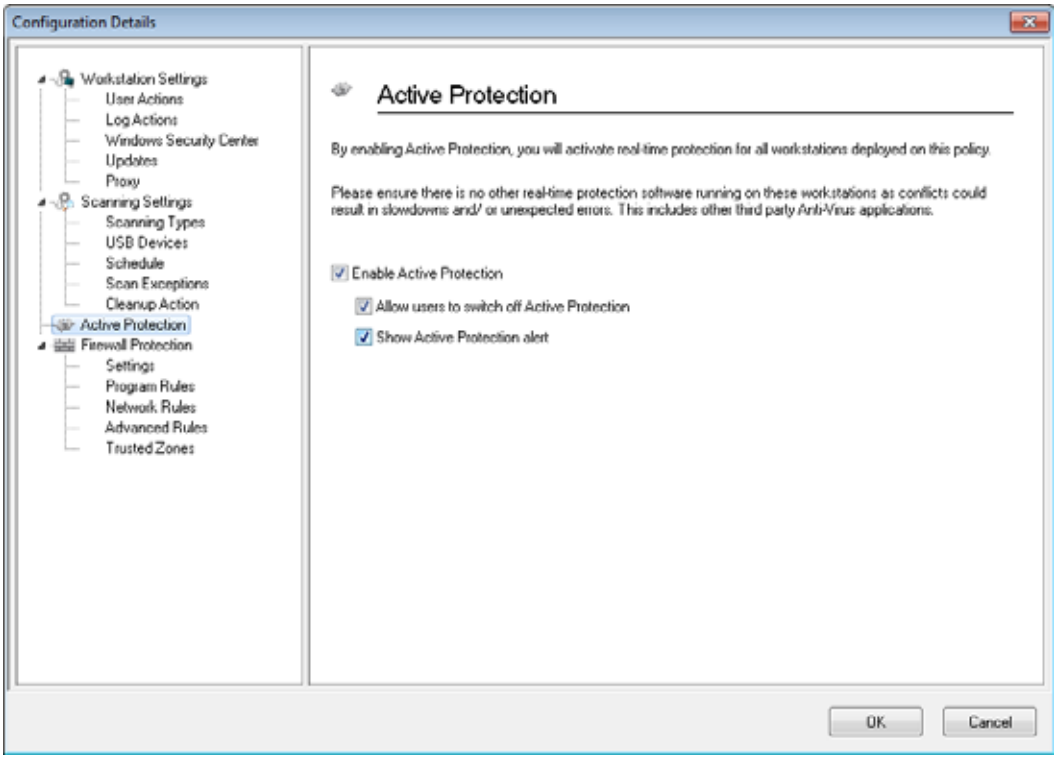


> Clean/Quarantine – When a threat is detected, attempt to disinfect the file and quarantine if unsuccessful. If the file could not be disinfected, it will be quarantined and will not be deleted.

> Clean/Delete – When a threat is detected, attempt to disinfect the file and delete if unsuccessful. If the file could not be disinfected, it will be deleted from the computer.

> Delete items from quarantine that are older than – Specify the number of days to retain items in quarantine. The default is 3 days.

6. Specify settings in the Active Protection pane:

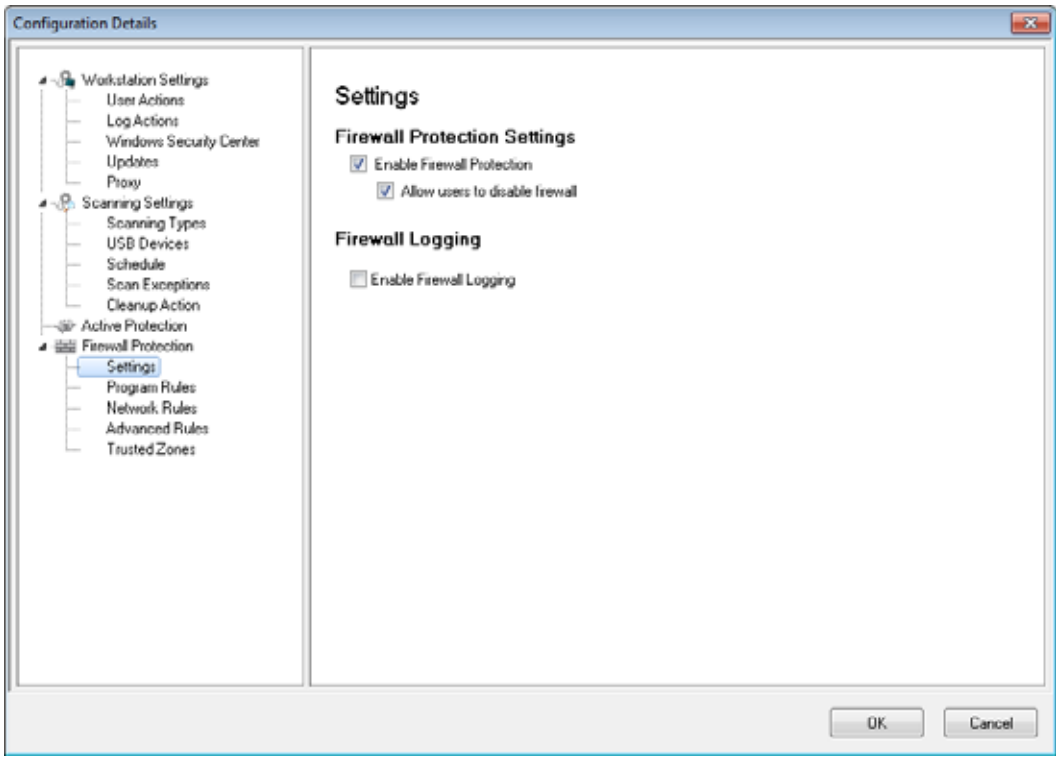


- Enable Active Protection – Select this option to enable real-time protection. Active Protection is the real-time scanning by Faronics Anti-Virus in the background without any impact on system performance. If there is a risk of real-time virus infection from the Internet, select this option.
  - > Allow users to switch off Active Protection – Select this option to allow users to switch off Active Protection. If users install or use software that might be mistaken from a virus (for example, running advanced Macros in Microsoft Office or complex batch files), select this option.
  - > Show Active Protection alert – Select this option to display an alert if a threat is detected during Active Protection. Do not select this checkbox if you do not want an alert to be displayed.

7. Specify settings in the Firewall Protection node:

   The Firewall Protection node provides bi-directional protection, protecting you from both incoming and outgoing traffic. You can create customized rules to protect your network. You can either *Allow* or *Block* the communication.

- Settings pane



Firewall Protection Settings

> Enable Firewall Protection – Select the checkbox to enable Firewall Protection. Firewall Protection prevents hackers or malicious software from gaining access to your computer through the Internet or the network.

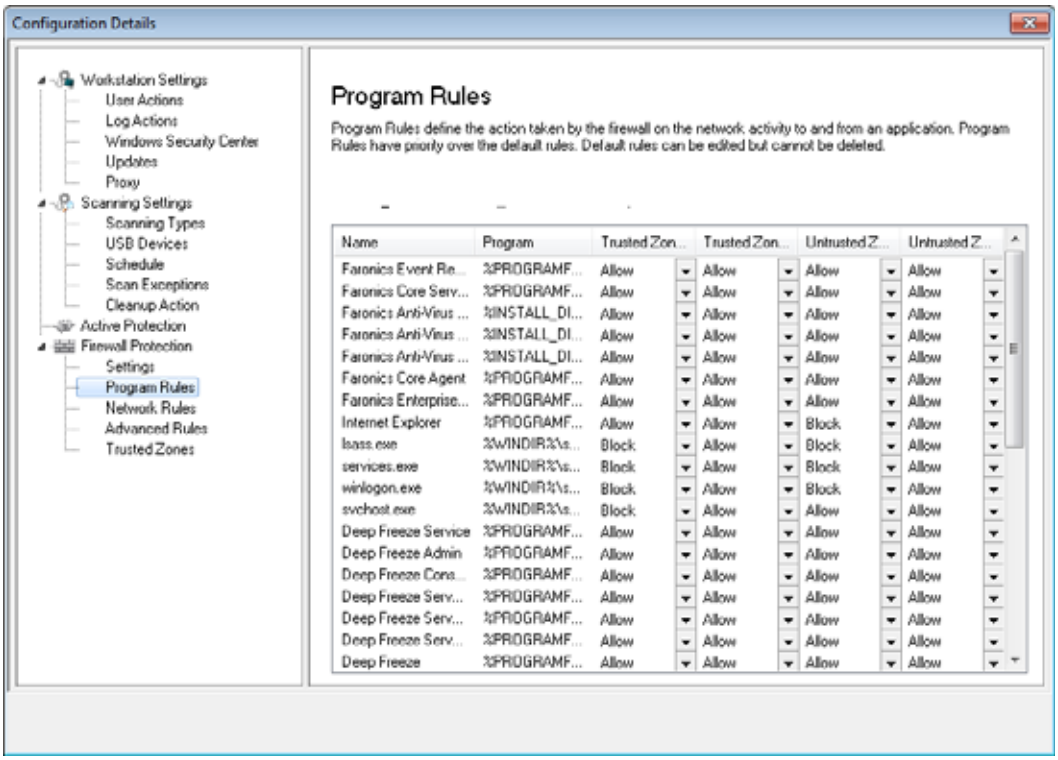
  ~ Allow users to disable firewall – Select this option to allow users to disable the firewall at the computer.

Firewall Logging

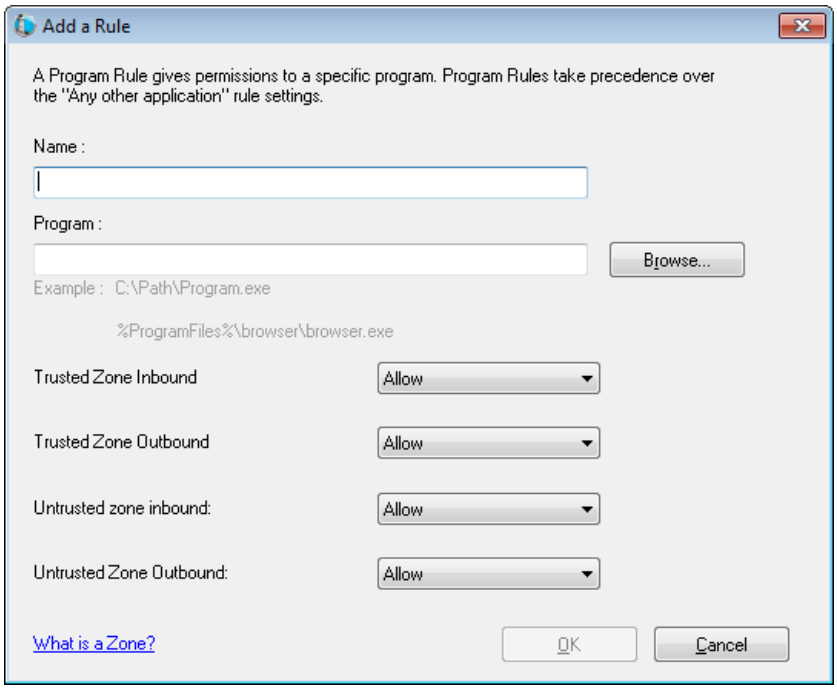
> Enable Firewall Logging – Select this option to log all actions related to the Firewall.

- Program Rules pane

  Program Rules define the action taken by the firewall on the network activity to and from an application. Program Rules have priority over the default rules. Default rules can be edited but cannot be deleted.



Click *Add* to add a new Program Rule. Specify or select the options and click *OK*. The following parameters are displayed:



> Name – Name of the rule.

> Program – Name of the program, including full path and extension.

> Trusted Zone Inbound – The action to be taken for inbound communication to the program in a Trusted Zone (*Allow* or *Block*).

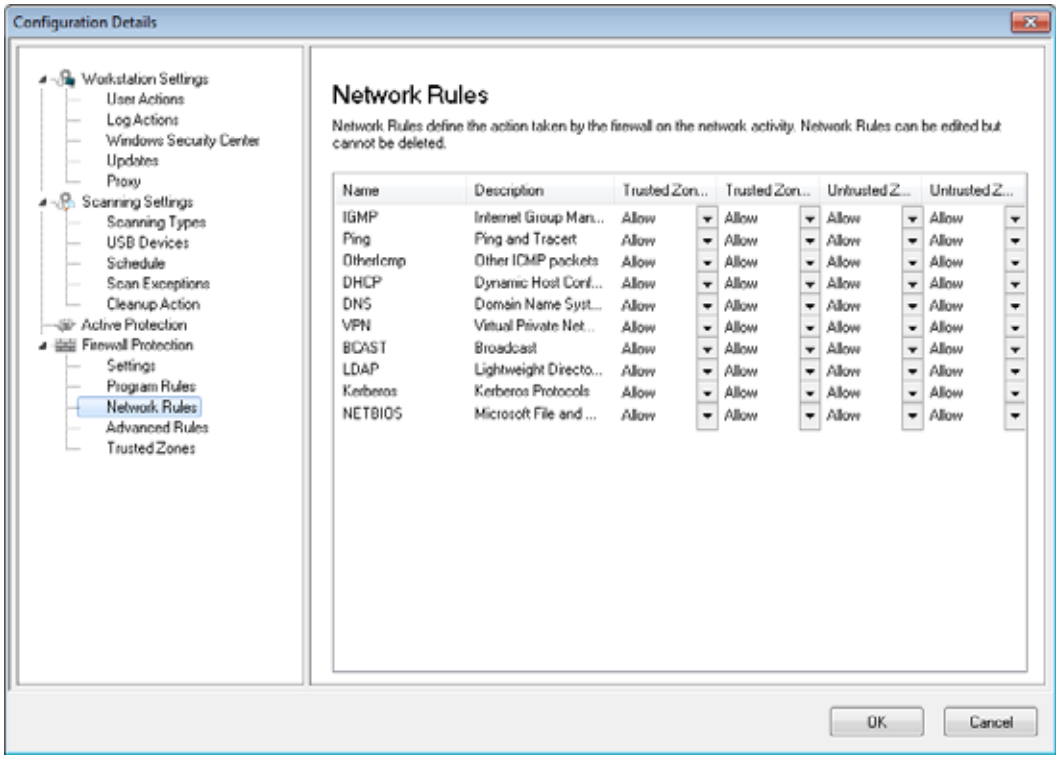
> Trusted Zone Outbound – The action to be taken for outbound communication from the program in a Trusted Zone (*Allow or Block*).

> Untrusted Zone Inbound – The action to be taken for inbound communication to the program in an Untrusted Zone (*Allow* or *Block*).

> Untrusted Zone Outbound – The action to be taken for outbound communication from the program in an Untrusted Zone (*Allow or Block*).

- Network Rule pane

Network Rules define the action taken by the firewall on the network activity. Network Rules can be edited but cannot be deleted.

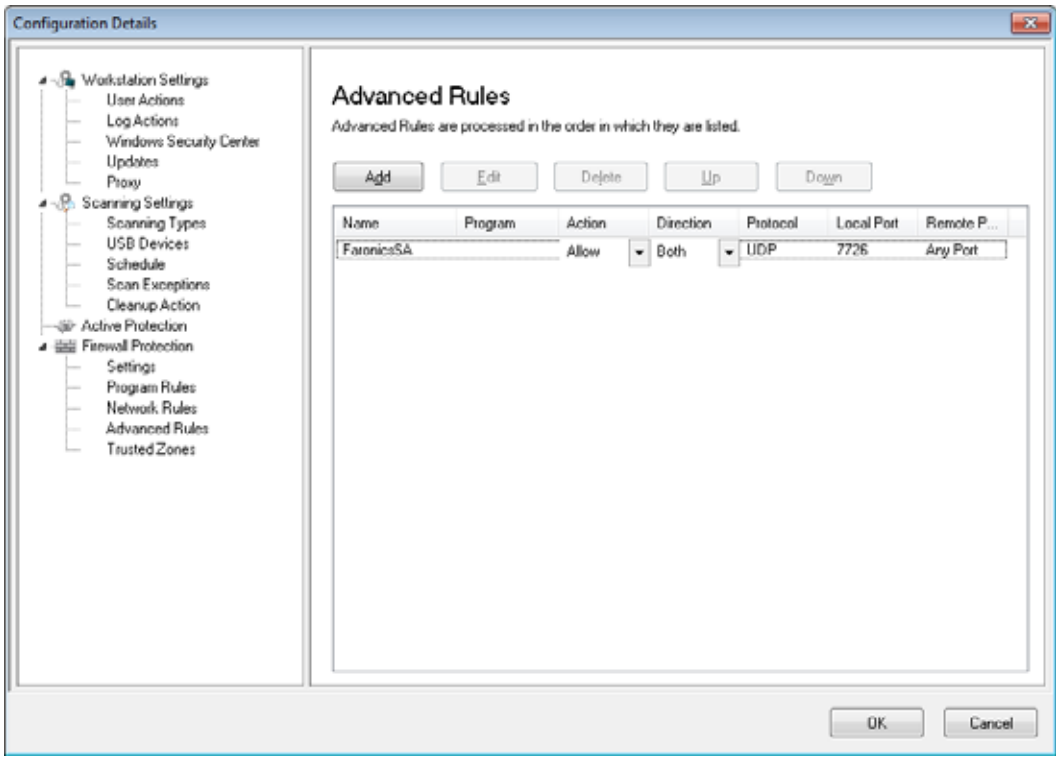


Select the Network Rules for the following:

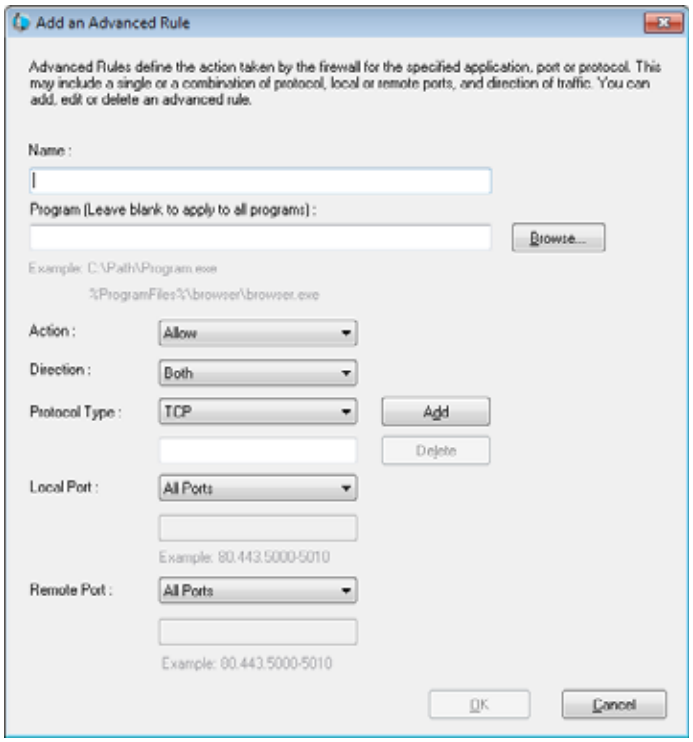
Name	Description	Trusted Zone Inbound	Trusted Zone Outbound	Untrusted Zone Inbound	Untrusted Zone Outbound
IGMP	Internet Group Management Protocol	Select Allow or Block	Select Allow or Block	Select Allow or Block	Select Allow or Block
Ping	Ping and Tracert	Select Allow or Block	Select Allow or Block	Select Allow or Block	Select Allow or Block
OtherIcmp	Other ICMP packets	Select Allow or Block	Select Allow or Block	Select Allow or Block	Select Allow or Block
DHCP	Dynamic Host Configuration Protocol	Select Allow or Block	Select Allow or Block	Select Allow or Block	Select Allow or Block
DNS	Domain Name System	Select Allow or Block	Select Allow or Block	Select Allow or Block	Select Allow or Block
VPN	Virtual Private Network	Select Allow or Block	Select Allow or Block	Select Allow or Block	Select Allow or Block
BCAST	Broadcast	Select Allow or Block	Select Allow or Block	Select Allow or Block	Select Allow or Block
LDAP	Lightweight Directory Access Protocol	Select Allow or Block	Select Allow or Block	Select Allow or Block	Select Allow or Block
Kerberos	Kerberos Protocols	Select Allow or Block	Select Allow or Block	Select Allow or Block	Select Allow or Block
NETBIOS	Microsoft File and Printer Sharing	Select Allow or Block	Select Allow or Block	Select Allow or Block	Select Allow or Block

- Advanced Rules pane

  Advanced Rules define the action taken by the firewall for the specified application, port or protocol. This may include a single or a combination of protocol, local or remote ports, and direction of traffic. You can add, edit or delete an advanced rule.



Click *Add* to add a new Advanced Rule. Specify or select the options and click *OK*. The following parameters are displayed in the Advanced Rules pane:



> Name – Name of the rule.

> Program – Name of the program and path.

> Action – The action taken by the Firewall for communication from the specified application, port or protocol (Allow or Block).

> Direction – The direction of communication (*Both*, *In or Out*).

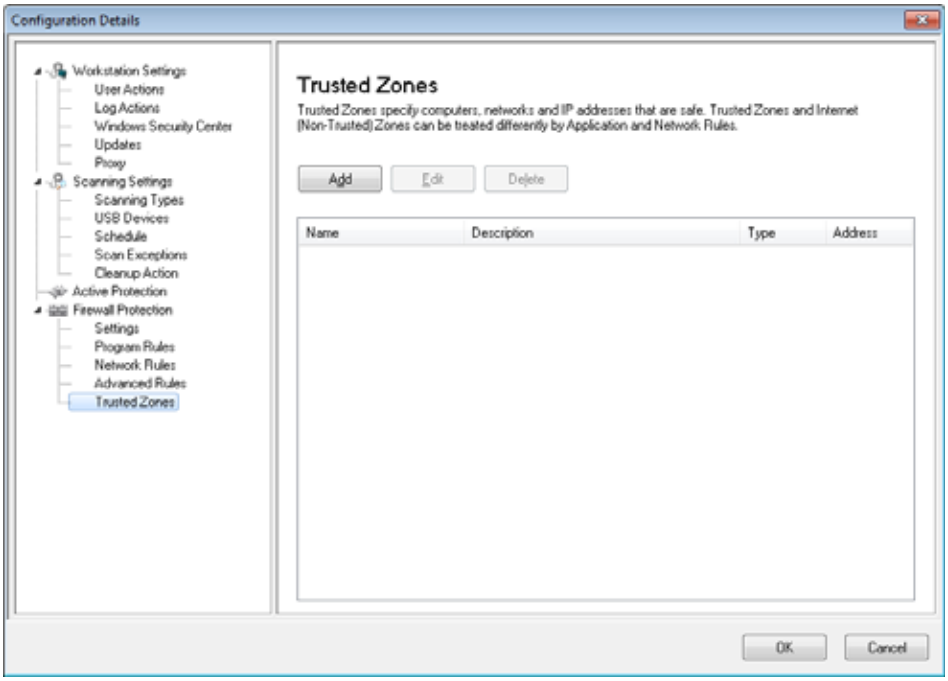
> Protocol – The name of the protocol.

> Local Port – Details of the local port.

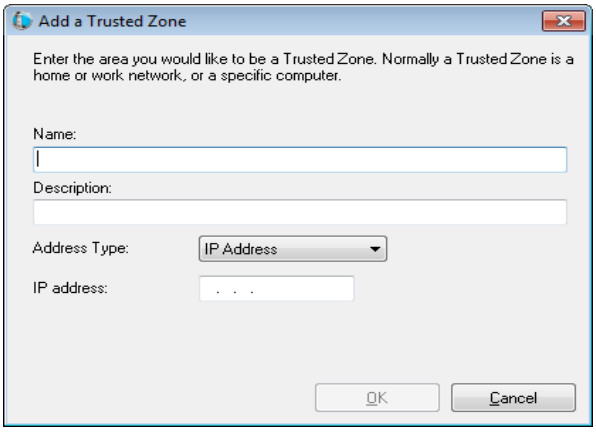
> Remote Port – Details of the remote port.

- Trusted Zones pane

  Trusted Zones specify computers, networks and IP addresses that are trusted. Trusted Zones and Internet (Non-Trusted) Zones can be treated differently by Program and Network Rules.



Click *Add* to add a new Trusted Zone. Specify or select the options and click *OK*. The following parameters are displayed:



> Name – Name of the Trusted Zone.

> Description – Description of the Trusted Zone.

> Type – Type of the Trusted Zone (IP Address or Network).

8. Click *OK*. The new policy, *New Policy 1* is displayed below the *Anti-Virus* node.

Applying Anti-Virus Configuration

Complete the following steps to apply the Anti-Virus configuration:

1. Go to *Workstations* pane.
2. Select one or more workstations.
3. Right-click on one or more workstations and select *Update Configuration* > *Anti-Virus* > *[Configuration Name]*.

The configuration is applied on the selected workstation(s).



Configuration changes will be automatically applied to the online workstations. If the workstations are offline, the configuration changes will be applied when the workstations come back online.

Editing Anti-Virus Configuration

Complete the following steps to edit the Anti-Virus configuration:

1. Go to Networks and Groups Pane in Enterprise Console.
2. Select *Available Configurations* > *Anti-Virus* > *[Configuration Name]*.
3. Right-click on the selected configuration and select *Edit Selected Configuration.*
4. Edit the settings as required.
5. Click *OK*.

Deleting Anti-Virus Configuration

Complete the following steps to delete the Anti-Virus configuration:

1. Go to Networks and Groups Pane in Enterprise Console.
2. Select *Available Configurations* > *Anti-Virus* > *[Configuration Name]*.
3. Right-click on the selected configuration and select *Delete Selected Configuration.*
4. Click *OK*.

Using Faronics Anti-Virus from the Enterprise Console

Once Faronics Anti-Virus Client is installed on the workstation, various actions can be performed on the workstation via Deep Freeze Console.

Anti-Virus Commands

There are two ways the same commands via Deep Freeze Console:

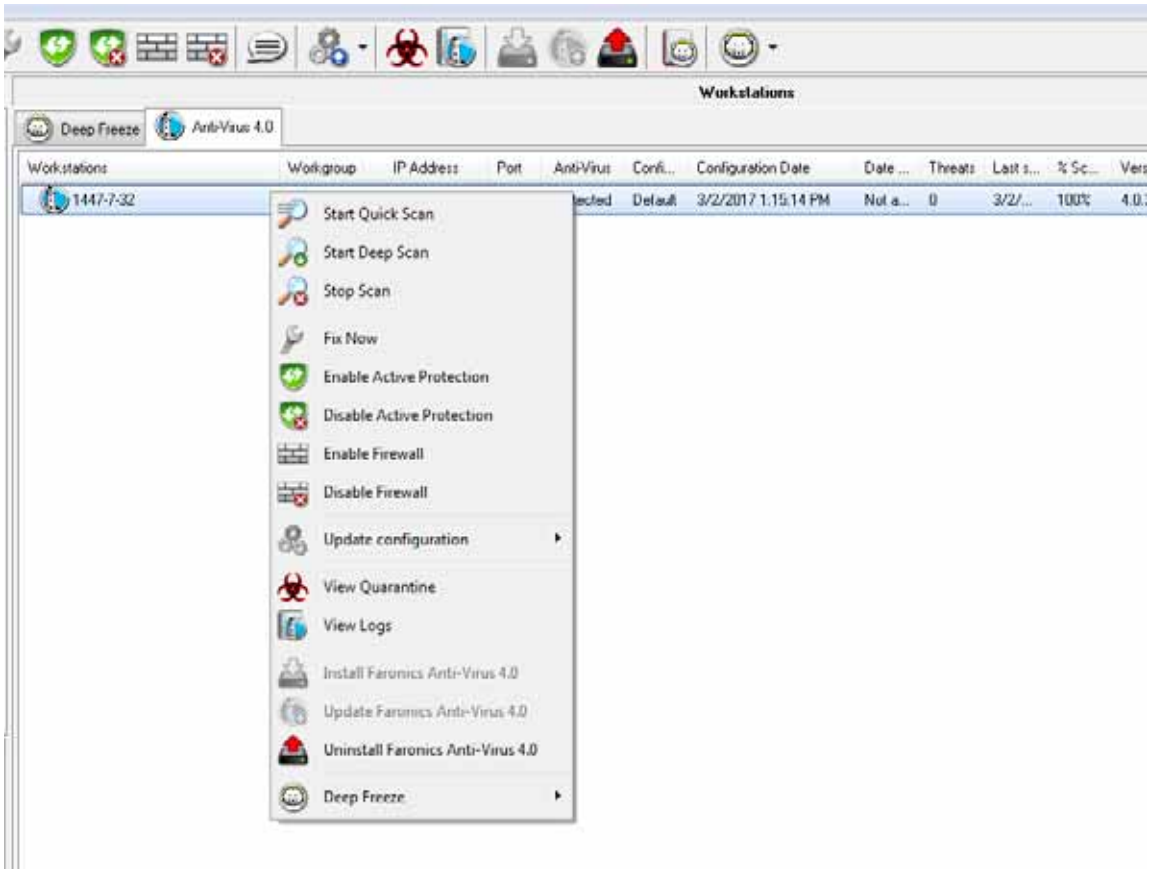
- Anti-Virus menu (in the menu bar)
- Anti-Virus context menu (right-click context menu)

The menu commands are explained further in this section.

The following commands are available in the Anti-Virus menu:



The same commands are available from the *Workstations* pane > *Anti-Virus* tab > Right-click context menu:



Quick Scan

Quick Scan checks the commonly affected areas of your computer. This is shorter in duration than the Deep System Scan. Quick Scan also uses less memory than the Deep System Scan.

- To start a Quick Scan – Select one or more workstations. Right-click and select *Start Quick Scan*.
- To stop a Quick Scan – Select one or more workstations. Right-click and select *Stop Scan*.
- To pause a Quick Scan – Select one or more workstations. Right-click and select *Pause Scan*.
- To resume a Quick Scan – Select one or more workstations. Right-click and select *Resume Scan*.

Deep Scan

Deep Scan performs a through scan of all areas of the computer. The time taken for the scan depends on the size of your hard drive.

- To start a Deep Scan – Select one or more workstations. Right-click and select *Start Deep Scan*.
- To stop a Deep Scan – Select one or more workstations. Right-click and select *Stop Deep Scan*.
- To pause a Deep Scan – Select one or more workstations. Right-click and select *Pause Scan*.
- To resume a Deep Scan – Select one or more workstations. Right-click and select *Resume Scan*.

Fix Now

The Fix Now option downloads the latest virus definitions and performs a quick scan on the workstation.

- To Fix Now – Select one or more workstations. Right-click and select *Fix Now*.

Active Protection

Active Protection (AP) is a real-time method for detecting malware. AP sits quietly in the background as you work or browse the Internet, constantly monitoring files that are executed (run) without causing noticeable strain to your system.

- To Enable Active Protection – Select one or more workstations. Right-click and select *Enable Active Protection*.
- To Disable Active Protection – Select one or more workstations. Right-click and select *Disable Active Protection*.

Firewall

A Firewall provides bi-directional protection, protecting you from both incoming and outgoing traffic. A Firewall protects your network from unauthorized intrusion.

- To Enable Firewall – Select one or more workstations. Right-click and select *Enable Firewall*.
- To Disable Firewall – Select one or more workstations. Right-click and select *Disable Firewall*.

Send Message

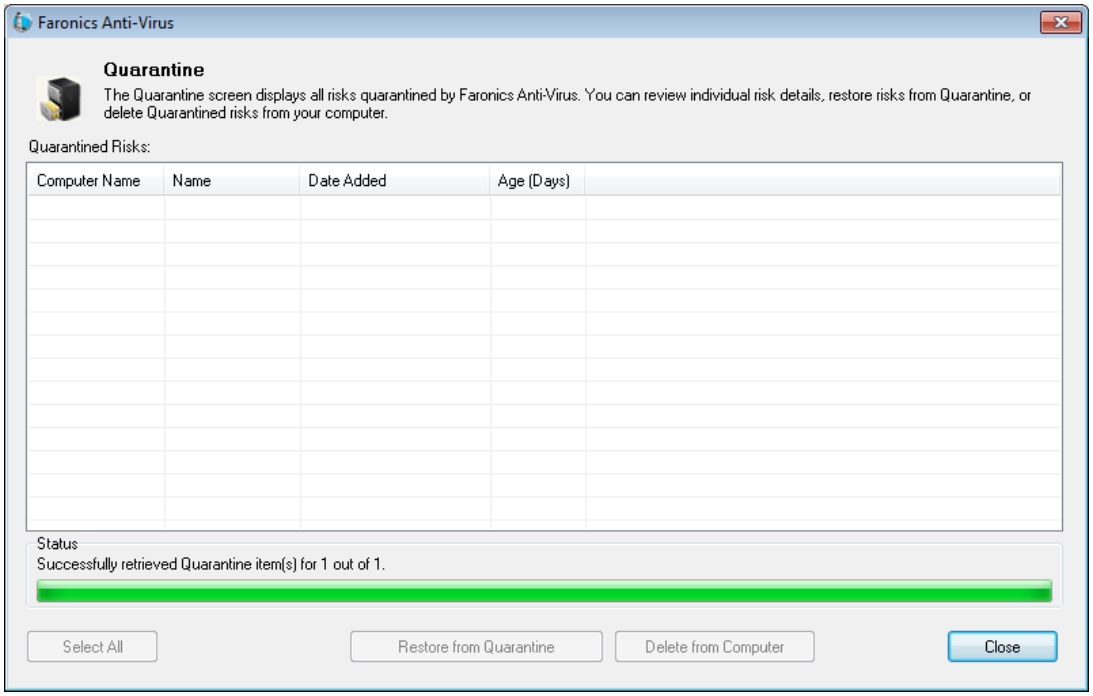
The Send Message option is used to send message to online workstations.

- To send a message – Select one or more workstations. Right-click and select *Send Message*.

View Quarantine Info

The Quarantine is a safe place on your computer that Faronics Anti-Virus uses to store malware or infected files that could not be disinfected. If your computer or files on your computer are not acting normal after an item has been placed here, you have the opportunity to review the details of a risk and research it further and remove it from Quarantine, restoring it back to your computer in its original location. You can also permanently remove the risks from Quarantine.

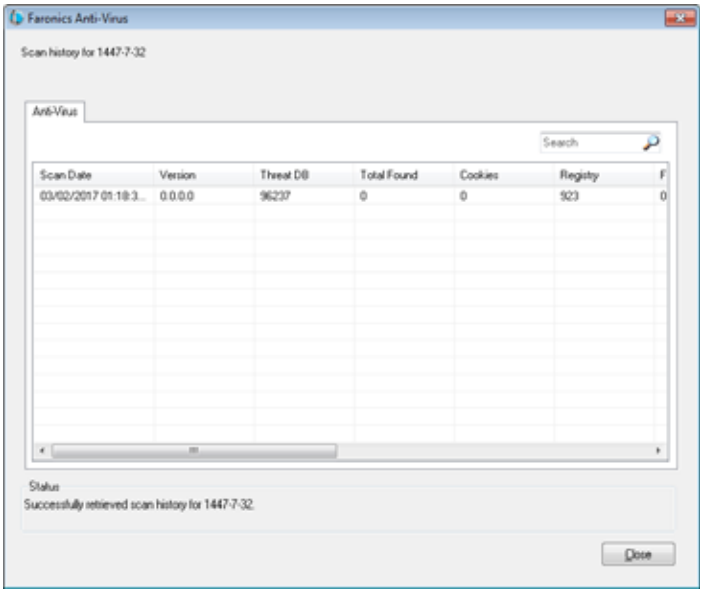
- To View Quarantine – Select one or more workstations. Right-click and select *Faronics Anti-Virus > Get Quarantine Info*.



View Scan History

Faronics Anti-Virus scan history displays all tasks performed by Faronics Anti-Virus on the workstation.

Select a single workstation, right-click and select *View Scan History* to view the log information.



Scheduling Anti-Virus Tasks

The following Anti-Virus tasks can be run from the Deep Freeze Console based on a pre-defined schedule.

- Disable Active Protection
- Enable Active Protection
- Start Quick Scan
- Start Deep Scan

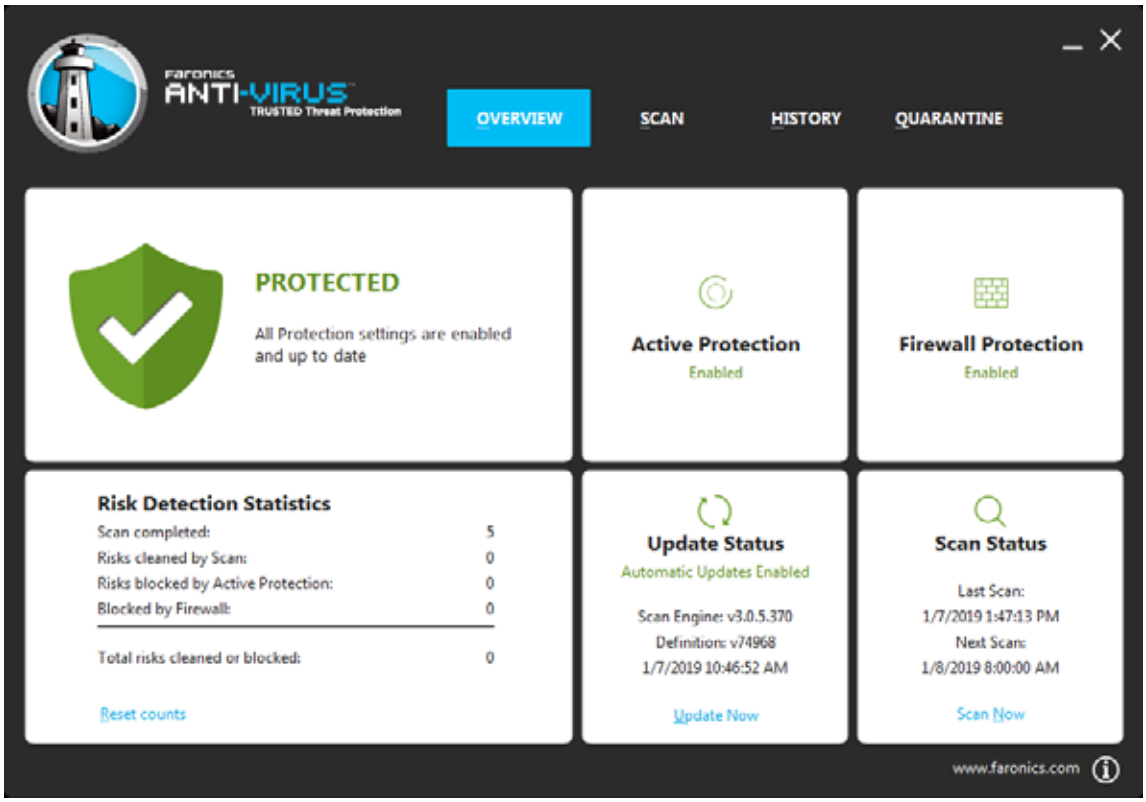
The procedure to schedule tasks is explained in detail in the section Scheduling Deep Freeze Tasks.

Using Anti-Virus on the Workstation

The features available in Anti-Virus on the workstation fully depends on the settings selected in the Anti-Virus Configuration. For more information about Anti-Virus Configuration, refer to Anti-Virus Configuration.

Launching Anti-Virus on the Workstation

Go to *Start* > *Programs* > *Faronics* > *Anti-Virus Enterprise* > *Faronics Anti-Virus Enterprise*. Alternatively, you can double-click on the Faronics Anti-Virus icon in the System Tray.



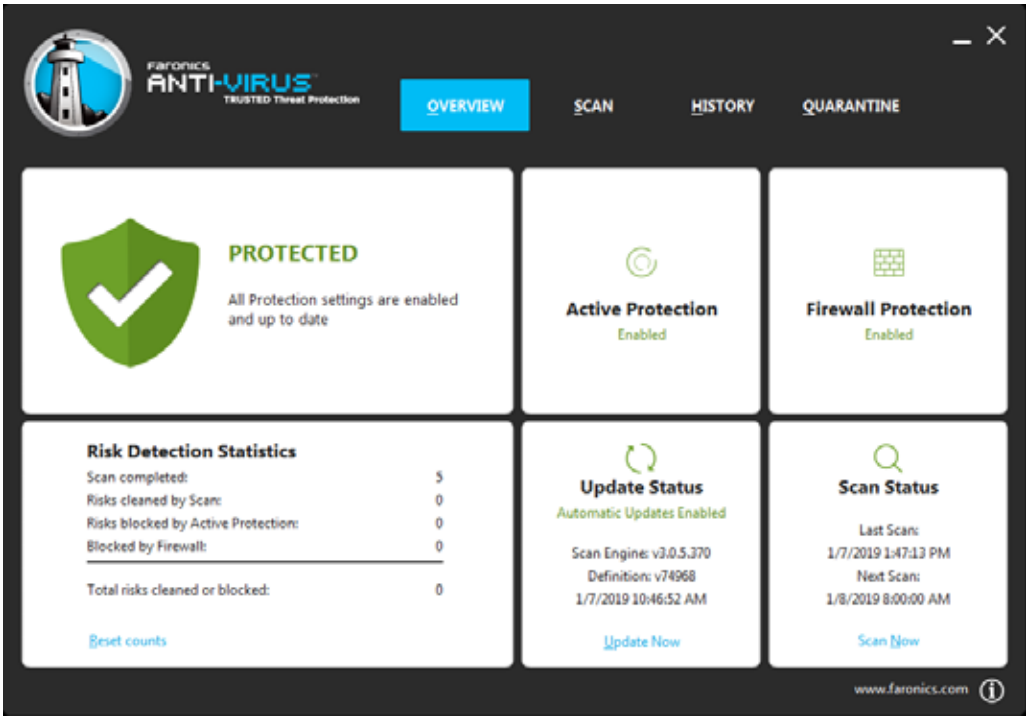
The following panes display important information to the user:

- *Protected* or *Not Protected is* displayed notifying if the computer is protected or not. If Not Protected is displayed, click the *Fix Now* button below the *Not Protected* sign.
- *Scan Status* displays when the last scan was performed. To scan now, click the *Scan Now* link.
- *Update Status* displays when the last update was performed. To update virus definitions, click the *Update Now* link.
- *Active Protection* displays if real-time protection is enabled.
- *Firewall Protection* displays if the workstation is protected by the Firewall.
- *Risk Detection Statistics* displays the statistics for the actions taken by Faronics Anti-Virus. Click *Reset counts* to reset the counts to zero.

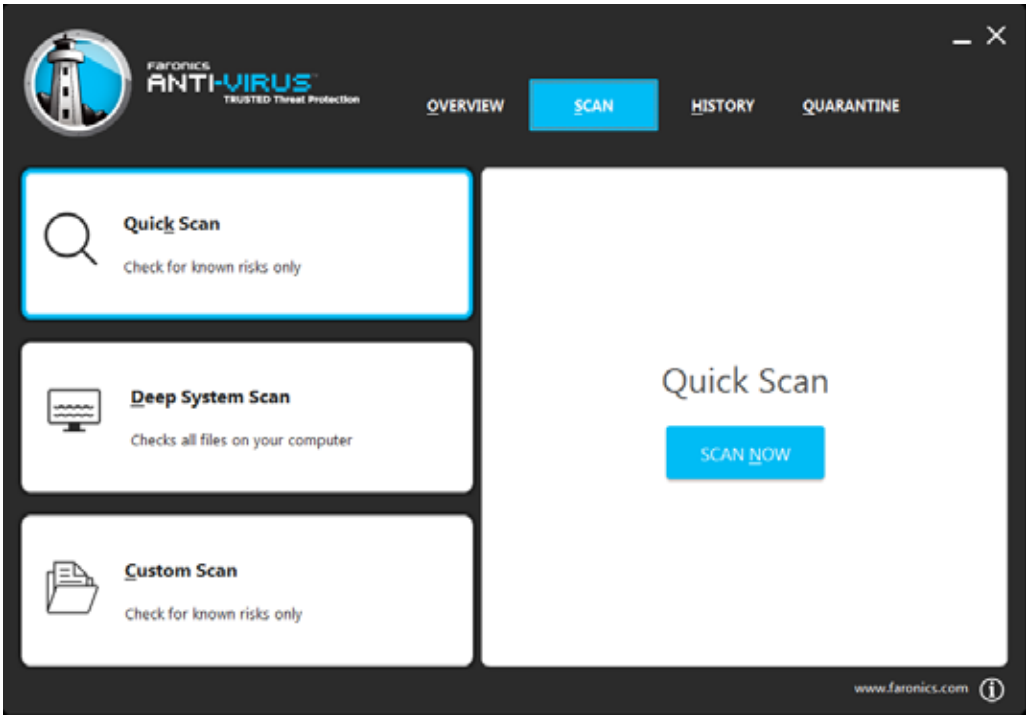
Scanning the Workstation

Complete the following steps to scan a workstation:

1. Go to *Start* > *Programs* > *Faronics* > *Anti-Virus Enterprise* > *Faronics Anti-Virus Enterprise*. Alternatively, you can double click on the Faronics Anti-Virus icon in the System Tray.



2. In the *Scan Status* pane, click *Scan Now*. The *Scan* tab is displayed. Alternatively, you may also click the *Scan* tab.



3. Select one of the following options:
   > Quick Scan – Scans only known threats.
   > Deep System Scan – A detailed scan of all files on the workstation.
   > Custom Scan (select one of the following):
      ~ Scan Running Processes – Scans the process running on the workstation.
      ~ Scan Registry – Scans the registry.
      ~ Specify drives and folders to scan – Click *Browse* and select the folders.
4. Click *Scan Now*. The spinning icon indicates that a scan is in progress. The scan results are displayed after the scan is completed.
5. Select the file and the following options are available:
   > Select *Change Clean Action* > *Recommended Action* to take the action as recommended by Faronics Anti-Virus.
   > Select *Change Clean Action* > *Quarantine/Disinfect* to quarantine or disinfect the file.
   > Select *Change Clean Action* > *Delete* to delete the file.
   > Select *Change Clean Action* > *Allow* to allow the file.
   > Click *Select All* to select all the files displayed in the *Scan Result*.
   > Click *Details* to display details of the risk.
   > Click *Cancel* to close the dialog without taking action.
   > Click *Clean* to remove the file and close the dialog.

Scanning a File or a Folder via Right-Click

Files or folders (single or multiple) can be easily scanned for a virus. When Faronics Anti-Virus is installed on a workstation, the Scan for Virus option is added in the right-click menu.

Complete the following steps to scan a file or a folder on the computer:

1. Right-click on the file or folder.
2. Select *Scan for viruses*.

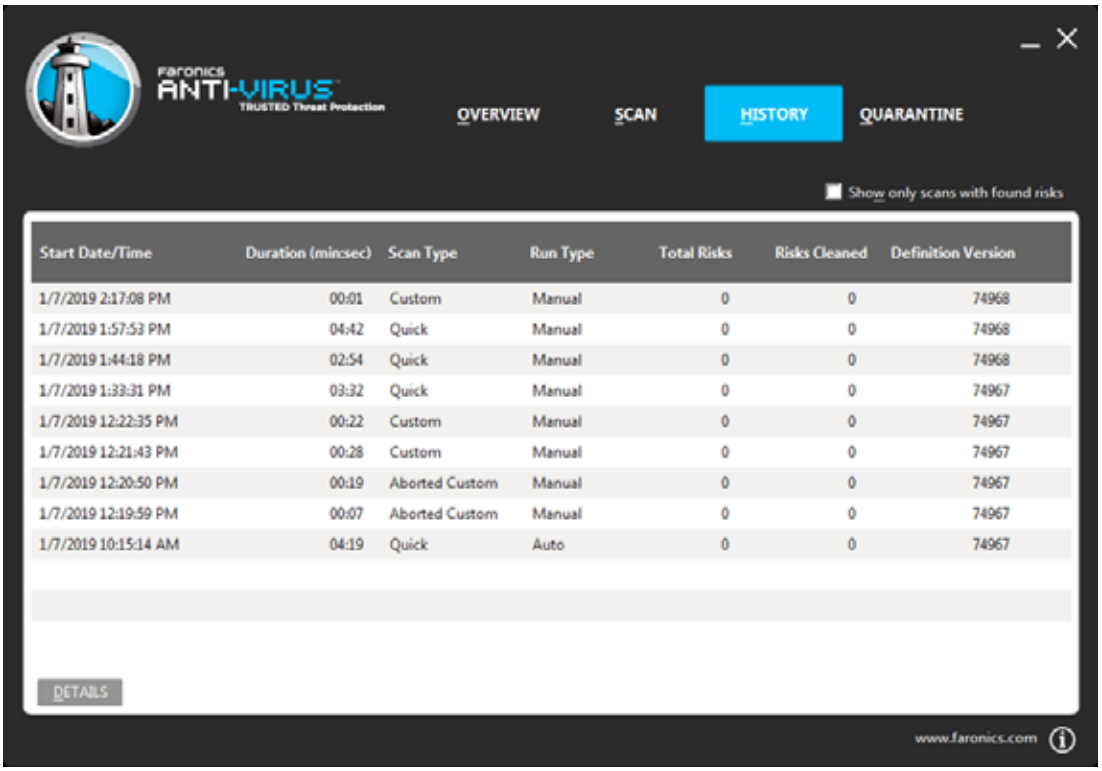
The scan is performed and the results are displayed.

View Scanning History

Complete the following steps to view the scanning history:

1. Go to *Start* > *Programs* > *Faronics* > *Anti-Virus Enterprise* > *Faronics Anti-Virus Enterprise*. Alternatively, you can double click on the Faronics Anti-Virus icon in the System Tray.

2. Click the *History* tab.



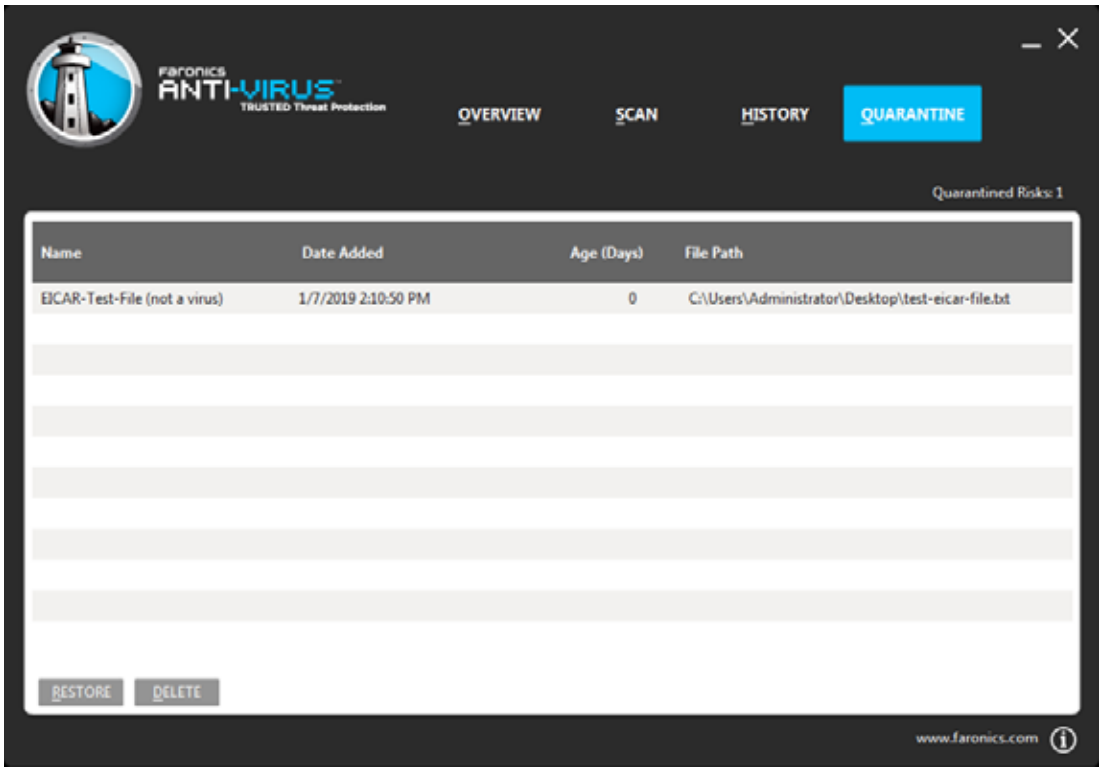
3. Select the following actions:
   > Show only scans with found risks – Select this option to view only the scans where risks were found.
   > Details – Select an entry and click details to view the details of the scan.

View and Take Action on Quarantined Files

Complete the following steps to view Quarantine:

1. Go to *Start* > *Programs* > *Faronics* > *Anti-Virus Enterprise* > *Faronics Anti-Virus Enterprise*. Alternatively, you can double click on the Faronics Anti-Virus icon in the System Tray.

2. Click the *Quarantine* tab.

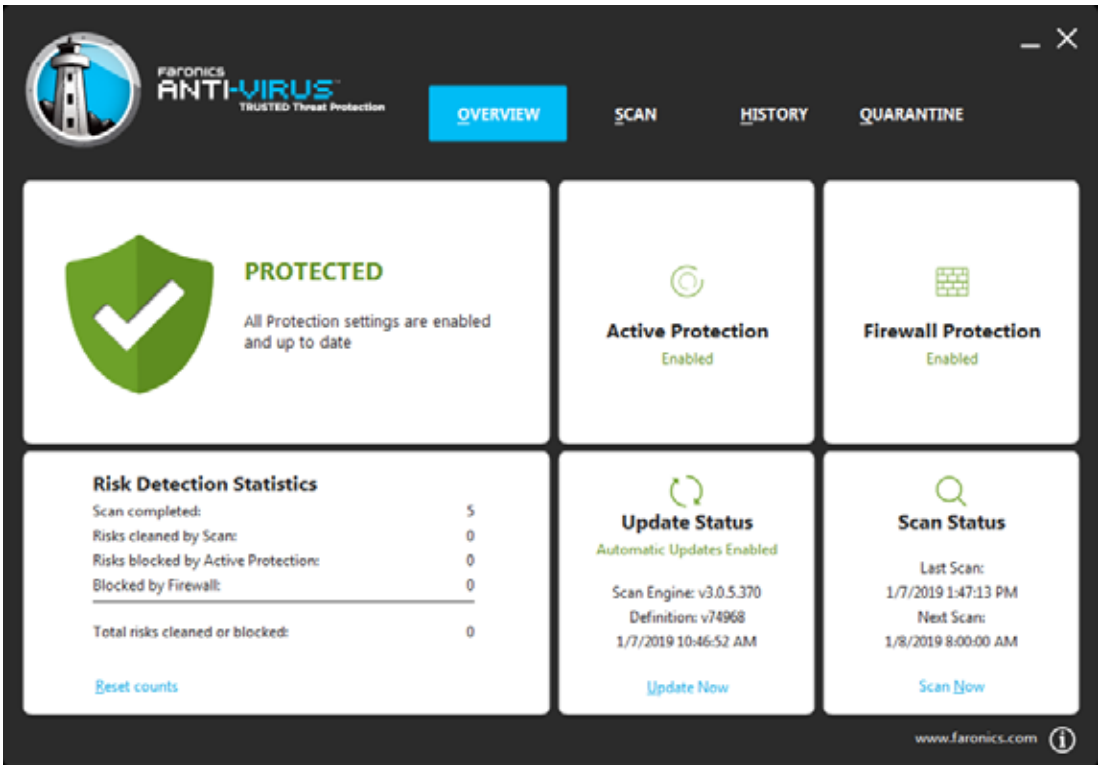


3. Click *Risk Details*. The following information about each infected file is displayed:
   > Name
   > Date Added
   > Age (Days)
4. Select the following actions:
   > Details – Select a file and click *Details* to view details of the infected file. This also displays the recommended action.

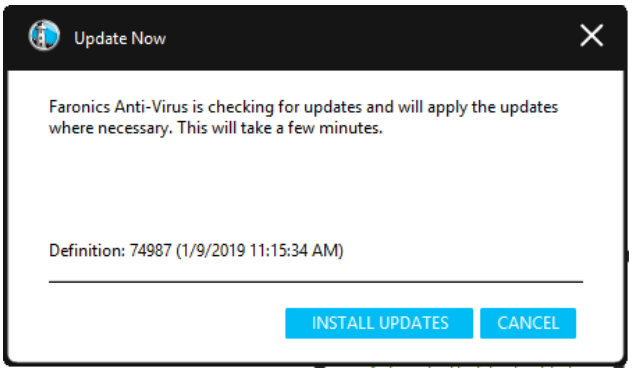
Updating Anti-Virus Definitions on the Workstation

Complete the following steps to update Anti-Virus definitions on a workstation:

1. Go to *Start* > *Programs* > *Faronics* > *Anti-Virus Enterprise* > *Faronics Anti-Virus Enterprise*. Alternatively, you can double-click on the Faronics Anti-Virus icon in the System Tray.



2. In the *Update Status* pane, click *Update Now*. The *Update Now* dialog is displayed.



3. Click *Install Updates*. The virus definitions are updated on the workstation.

Managing Anti-Virus on the Workstation via the System Tray

Faronics Anti-Virus can be managed on the workstation via a menu available from the System Tray.

Right-click on the Faronics Anti-Virus icon in the System Tray. The following options are available:

- Open Faronics Anti-Virus – Launches Faronics Anti-Virus on the workstation.
- Active Protection
  - > Active Protection > Enable Active Protection – Enables Active Protection.
  - > Active Protection > Disable Active Protection > [Select the option] – Select the duration for which Active Protection is to be disabled. Select 5 minutes, 15 minutes,

30 minutes, 1 Hour, Until Computer Restart or Permanently. This option is displayed only if it has been selected in the Anti-Virus policy.

- Scan Now > [Select the option] – Select Cancel Scan, Quick Scan or Deep Scan. This option is displayed only if it has been selected in the Anti-Virus policy.
- Firewall Protection > Enable or Disable.

Check for Anti-Virus Updates

Deep Freeze Console allows you to check if there are newer versions of Faronics Anti-Virus available.

Go to *Help* > *Check for updates*. This checks if there is a new version of Faronics Anti-Virus available.

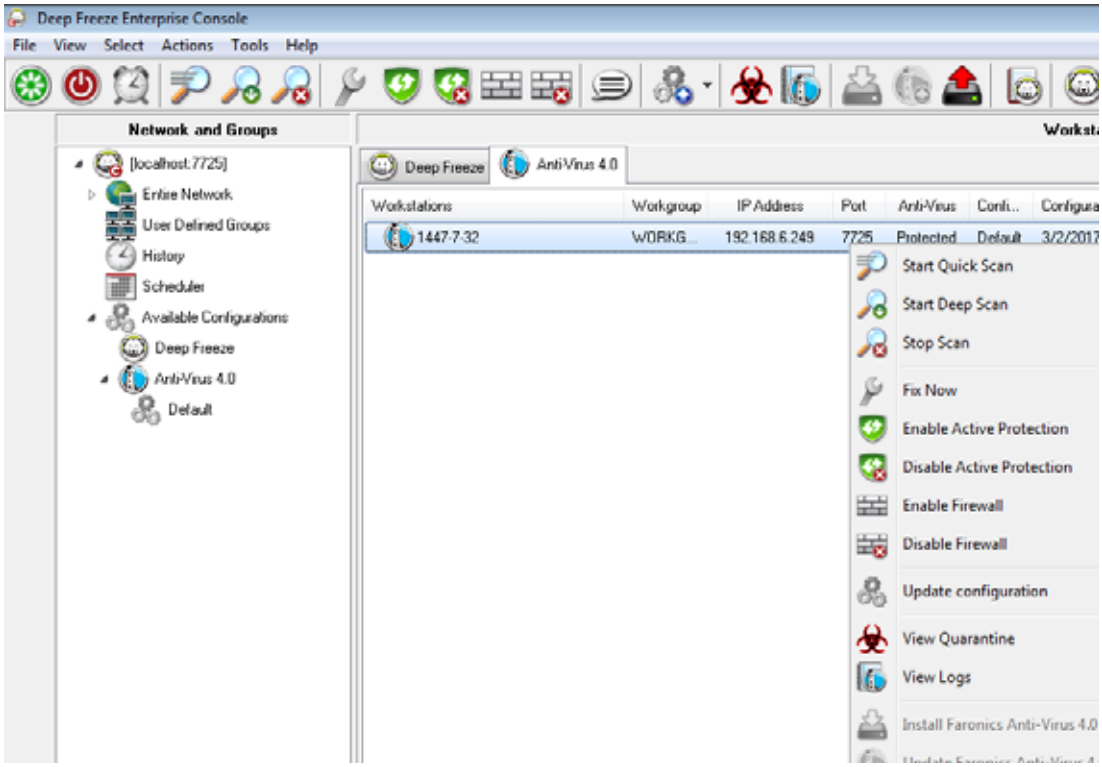


If a new version is available, click *Download the latest version* to update Faronics Anti-Virus.

Update Faronics Anti-Virus

If you have checked for updates and a new version of is available, complete the following steps to update a new version on the workstation:

1. Go to *Anti-Virus* tab in the *Workstations* pane.
2. Select a workstation (or multiple workstations).
3. Right-click and select *Update Faronics Anti-Virus*.



4. Click *OK* to confirm the action.

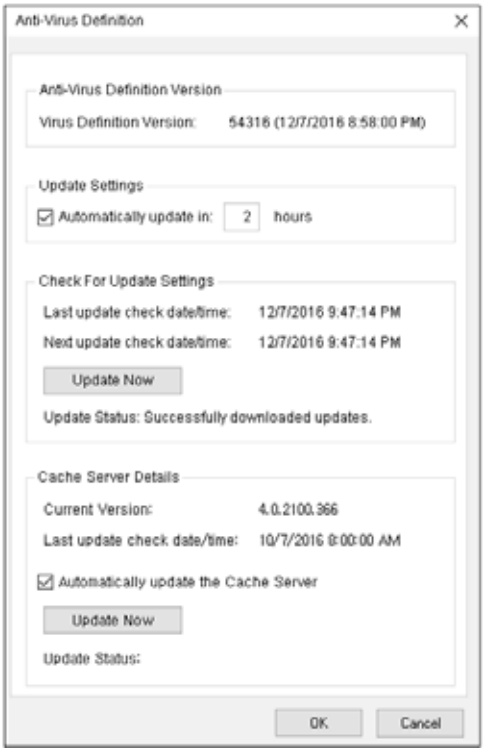
The workstation reboots and Faronics Anti-Virus client is updated on the workstation(s).

Updating Anti-Virus Definitions

The Anti-Virus Definition Server is installed along with Faronics Anti-Virus on the same computer where the Deep Freeze Console is installed. The Anti-Virus Definition Server downloads the latest virus definitions and distributes to the workstations managed by Deep Freeze.

Complete the following steps to update virus definitions:

1. Launch Deep Freeze Console.
2. Go to *Tools > Anti-Virus Definition*.
3. The following settings and action are available:

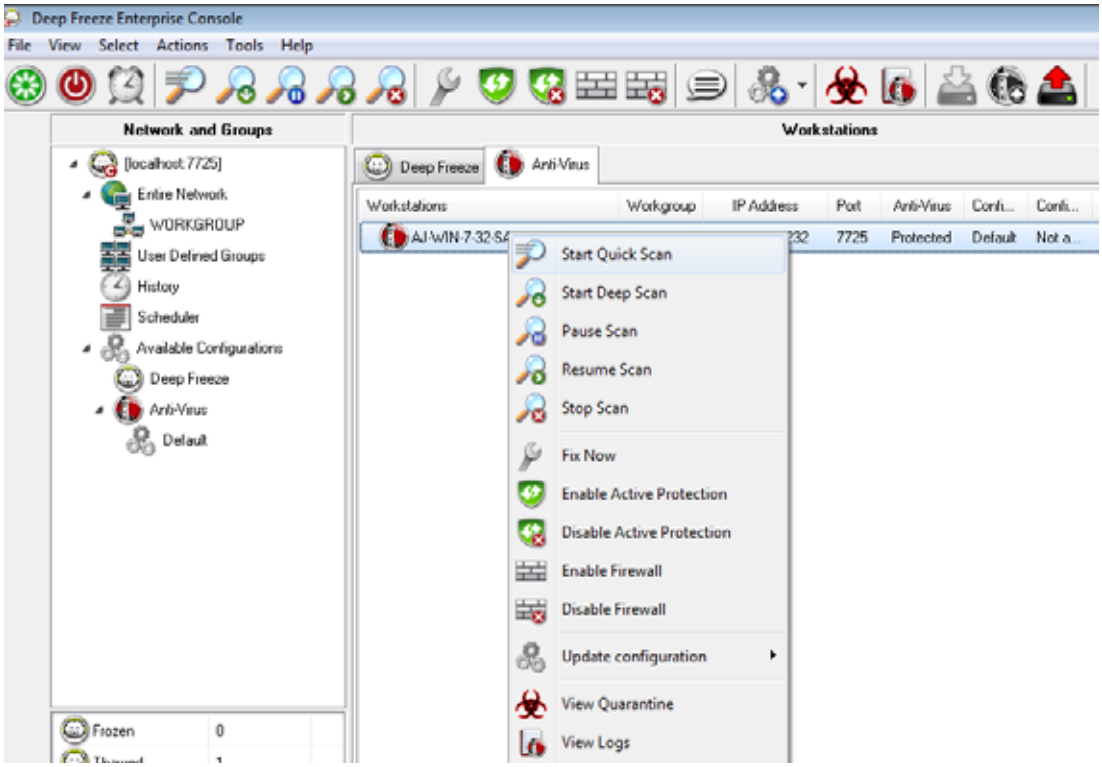


   > Anti-Virus Definition Version – The current Anti-Virus definition version is displayed.
   > Update Settings – Select the *Automatically update in* checkbox and enter a value in hours.
   > Check for Update Settings – The Last update check date/time and Next update check date/time is displayed. Click *Update Now* to update the virus definitions immediately. The Update Status is displayed.
   > Cache Server Details – The Current Version and Last update check date/time is displayed. Select the *Automatically update the Cache Server* checkbox if you want to automatically download and update the Cache Server with the latest definitions. Click *Update Now* to update the cache server immediately.
4. Click *OK*.

Uninstall Anti-Virus Client from the Enterprise Console

Complete the following steps to uninstall Faronics Anti-Virus on the workstation from the Enterprise Console:

1. Go to *Anti-Virus* tab in the *Workstations* pane.
2. Select a workstation (or multiple workstations) from the
3. Right-click and select *Uninstall Faronics Anti-Virus*.



4. Click *OK* to confirm the action.

The workstation reboots and Faronics Anti-Virus client is uninstalled on the workstation(s).

If Anti-Virus Client is uninstalled from the workstation, the Deep Freeze Seed will be left behind.

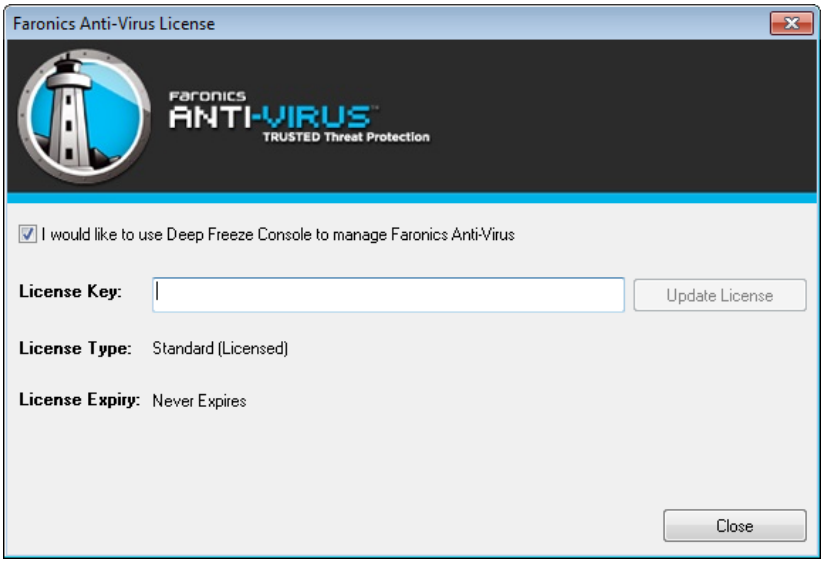
The Deep Freeze Seed cannot be uninstalled when Anti-Virus Client is installed on the workstation.

Disable Faronics Anti-Virus from the Enterprise Console

Anti-Virus can be disabled on the Deep Freeze Console in case it is not required to be used.

Complete the following steps to disable Faronics Anti-Virus from the Deep Freeze Console:

1. Go to *Tools* > *Licensing* > *Faronics Anti-Virus License*.
2. Clear the *I would like to use Deep Freeze Console to manage Faronics Anti-Virus* checkbox.



3. Click *Close*.
4. Restart the Enterprise Console for the settings to take affect.



Deep Freeze Command Line Control

This chapter describes using the Deep Freeze Commands.

Topics

Deep Freeze Command Line Control (DFC.EXE)
Deep Freeze Command Line Syntax
Faronics Anti-Virus Command Line Syntax

Deep Freeze Command Line Control (DFC.EXE)

Deep Freeze Command Line Control (DFC) offers network administrators increased flexibility in managing Deep Freeze computers. DFC works in combination with third-party enterprise management tools and/or central management solutions. This combination allows administrators to update computers 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.

DFC commands require a password with command line rights. OTPs cannot be used.

List all commands by calling DFC without parameters.

The files are copied to (32-bit)

```
<WINDOWS>\system32\DFC.exe
```

The files are copied to (64-bit)

```
<WINDOWS>\syswow64\DFC.exe
```

DFC Return Values

On completion of any DFC command, the DFC returns the following values:

Syntax	Description
`0`	SUCCESS or Boolean FALSE, for commands returning a Boolean result
`1`	Boolean TRUE
`2 ERROR`	User does not have administrator rights
`3 ERROR`	DFC command not valid on this installation
`4 ERROR`	Invalid command
`5 - * ERROR`	Internal error executing command

Deep Freeze Command Line Syntax



Deep Freeze has a maximum password limit of 63 characters. If a longer password is entered, the command will not be successful.

Syntax	Description
`DFC password /BOOTTHAWED`	Restarts computer in a Thawed state; only works on Frozen computers.
`DFC password /THAWNEXTBOOT`	Sets computer to restart Thawed the next time it restarts; only works on Frozen computers and does not force computer to restart.
`DFC password /BOOTFROZEN`	Restarts computer into a Frozen state; only works on Thawed computers.
`DFC password /FREEZENEXTBOOT`	Sets up computer to restart Frozen the next time it restarts; only works on Thawed computers and does not force computer to restart.
`DFC get /ISFROZEN`	Queries computer if it is Frozen. Returns error level 0 if Thawed. Returns 1 if Frozen.
`DFC get /CLONE`	Sets the clone flag for the purpose of imaging.
`DFC password /CFG=[path] depfrz.rdx`	Replaces Deep Freeze configuration information. Works on Thawed or Frozen computers. Password changes are effective immediately. Other changes require restart.
`DFC get /version`	Displays Deep Freeze version number.
`DFC password /UPDATE=[path to installer file]`	Sets up computer to restart in a Thawed state and install a Deep Freeze update.
`DFC password /LOCK`	Disables keyboard and mouse on computer. Works on Frozen or Thawed computer and does not require a restart.
`DFC password /UNLOCK`	Enables keyboard and mouse on computer. Works on Frozen or Thawed computer and does not require a restart.
`DFC password /THAWLOCKNEXTBOOT`	Sets up computer to restart in a Thawed state with keyboard and mouse disabled; only works on Frozen computers

Syntax	Description
`DFC password /BOOTTHAWEDNOINPUT`	Restarts computer in a Thawed state with keyboard and mouse disabled; only works on Frozen computers
`DFC get /LICENSESTATUS`	Displays the status of the license and the expiry date of the license (if any). The different possible types of license and the associated return codes are: 111: Unlicensed – Deep Freeze is not licensed and will operate in *Evaluation* mode for 30 days since installation. 112: Evaluation – Licensed for evaluation with a fixed expiry date. 113: Licensed – Licensed with no expiry date. 114: Expired – The Evaluation period has expired.
`DFC get /LICENSETYPE`	Displays the status of the license and the expiry date of the license (if any). The different possible types of license and the associated return codes are: 111: None (Unlicensed) – Deep Freeze is not licensed and will operate in *Evaluation* mode for 30 days since installation. 112: Evaluation – Licensed for evaluation with a fixed expiry date. 113: Standard (Licensed) – Licensed with no expiry date. 114: Not for Resale – Licensed with no expiry date. 115: Subscription 116: Subscription – Evaluation 117: Subscription – Not For Resale
`DFC password /LICENSE=licensekey`	Changes the License Key. *password* is the Deep Freeze Administrator password. *licensekey* is the License Key for Deep Freeze. If there is an error, the following error codes are displayed: 101: The License Key is not valid 102: The License Key provided has already expired.
`DFC password /ACTIVATE`	Activates the workstation after checking with the Faronics License Activation Server.

Syntax	Description
`DFC get /ACTIVATION`	Displays the Deep Freeze license activation status. Returns the following values: 0: Pending activation 1: Active 2: Authorized 3: Deactivated 4: Rogue
`DFC password /WU [/UNLOCK] [/NOMSG | /NOMESSAGE] [/THAW]`	Windows Updates will be downloaded and installed on the workstation. [/UNLOCK] Optional parameter to enable the Keyboard and Mouse during Windows Update. [/NOMSG | /NOMESSAGE] Optional parameter to suppress all informational/warning messages from Deep Freeze during Windows Update. [/THAW] Optional parameter to return the machine into Thawed State after completion of Windows Update.
`DFC password /ENDTASK`	Ends the ongoing Workstation Task and reboots into Frozen state. Batch File Task and Thawed Period Task end immediately. Windows Update Task is completed.
`DFC password /ENDTASK [/SHUTDOWN]`	Ends the ongoing Workstation Task and reboots into Frozen state. Batch File Task and Thawed Period Task end immediately. Windows Update Task is completed. `[/SHUTDOWN]`Optional parameter to shut down the workstation.
`DFC password /FORMATTHAWSPACE`	Formats all the ThawSpaces on the workstation. Data stored on the ThawSpaces will be deleted permanently.
`DFC password /DELETETHAWSPACE`	Deletes all the ThawSpaces on the workstation. Data stored on the ThawSpaces will be deleted permanently.

Faronics Anti-Virus Command Line Syntax

Complete the following steps to run the commands for Faronics Anti-Virus:

1. On the workstation, go to <*System Directory*>:*Program Files**Faronics**Faronics Anti-Virus Enterprise* via command prompt.
2. Enter `AVECLI/[Command]`

The following commands are available:

Syntax	Description
`definitionversion`	Displays Virus Definition version.
`scanengineversion`	Displays Scan Engine version.
`updatedefs`	Updates and applies Virus Definitions.
`fixnow`	Downloads the latest Virus Definition. Enables Active Protection and Email Protection. Performs the default Deep Scan.
`scanquick`	Starts a Quick Scan.
`scandeep`	Starts a Deep Scan.
`enableap`	Enables Active Protection.
`applydefs [path to definitions]`	Applies definitions file from a saved location.
`fixnow /quick`	Performs a Quick Scan if applicable.
`setlicense [key]`	Applies a given license key.

Syntax:

```
AVECLI/definitionversion
```

Appendix A Ports and Protocols

The key to setting up the Deep Freeze architecture is knowing which ports to use. The important factor is knowing which ports are in use on the network and using ports that will not conflict with those. The default port, 7725 has been officially registered to Deep Freeze.

The following three components make up the Deep Freeze architecture:

- Client (with seed installed)
- Remote Console (local service enabled)
- Console (connects to the Remote Console)

As long as the clients and Remote Console connection use the same port there should not be any port conflicts between the different components:



Ports can also be used to divide the clients. If the local service is setup to run three ports (7725, 7724 and 7723), Enterprise Consoles can connect to the three different ports to see a different set of clients under each port.

In the diagram above, the client(s) use both the TCP and UDP protocols to communicate with the Remote Console. The Console(s) that connects to the Remote Console uses only the TCP protocol to communicate with the Remote Console. It is important to remember the ports and protocols being used in order to prevent firewalls, switches or routers from blocking them.



Appendix B Network Examples

The following examples show different scenarios involving local service or Remote Console.

- Example 1: Single Subnet
- Example 2: Multiple Subnets, One Local Service
- Example 3: Multiple Ports, Console Accessed Remotely
- Example 4: Multiple Subnets, Multiple Local Services

Each example explains how different Deep Freeze components interact in different networking environments.

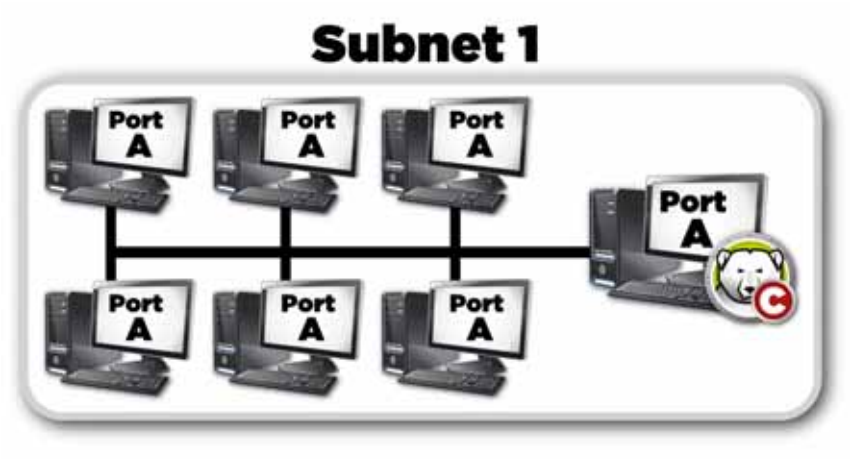


In the following examples, the client machines have either the Deep Freeze workstation installation or Workstation Seed installed. Both installs contain the communications component which talks to the Console/Remote Console. The difference between the workstation install and Workstation Seed is that the workstation install actually installs Deep Freeze while the Seed has only the communication component.

Example 1: Single Subnet

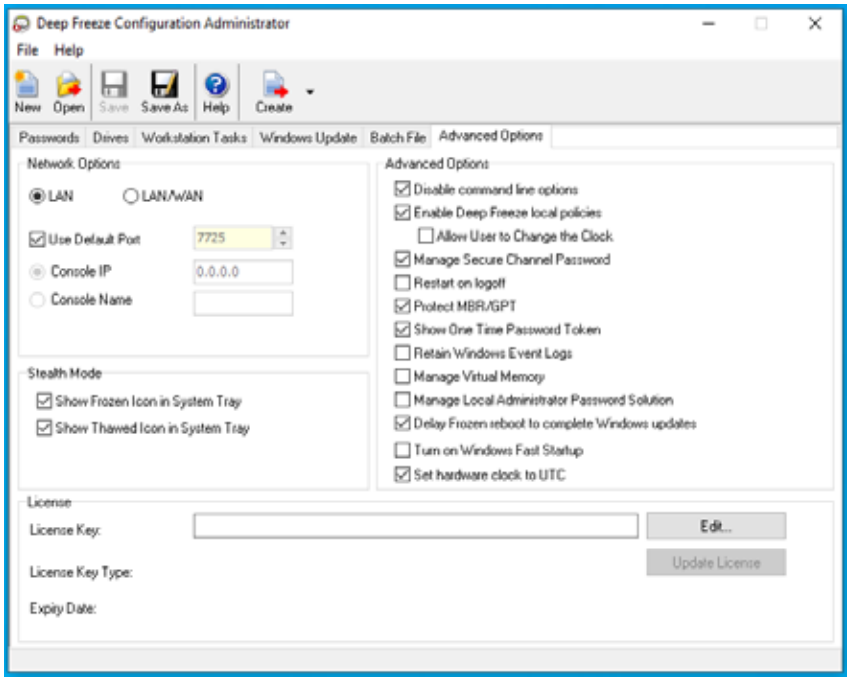
In this environment, all client machines are contained in the same subnet as the Console machine. This environment does not require a remote controlled Console, although one could be used. In this example, the Remote Console is not used. This is the simplest networking environment. It is also the easiest to configure.

The following diagram shows the network topology:



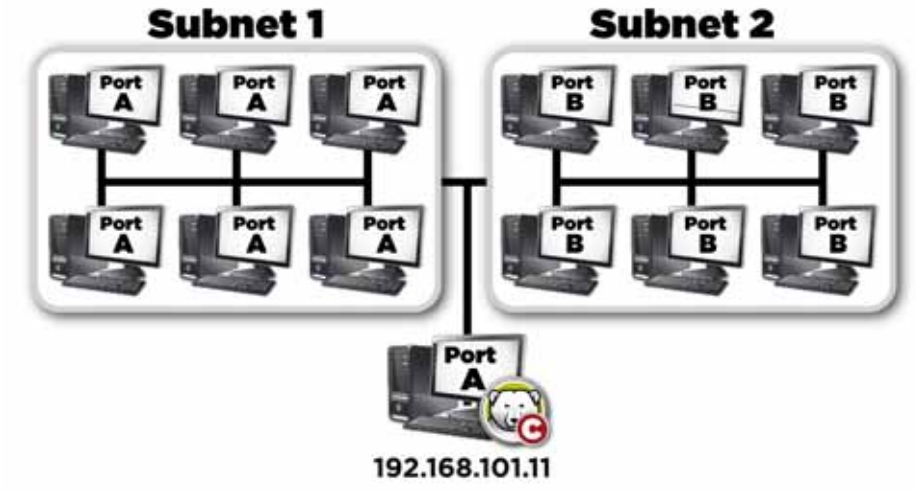
The client machines, represented by the computer icons, are located on the same subnet as the Deep Freeze Enterprise Console machine represented by the Deep Freeze Console icon.

In this scenario, clients are using port A while the Console has set up a local service connection for the same port. This port is configured in the *Advanced Options* tab, before creating the Workstation Install file or Workstation Seed.



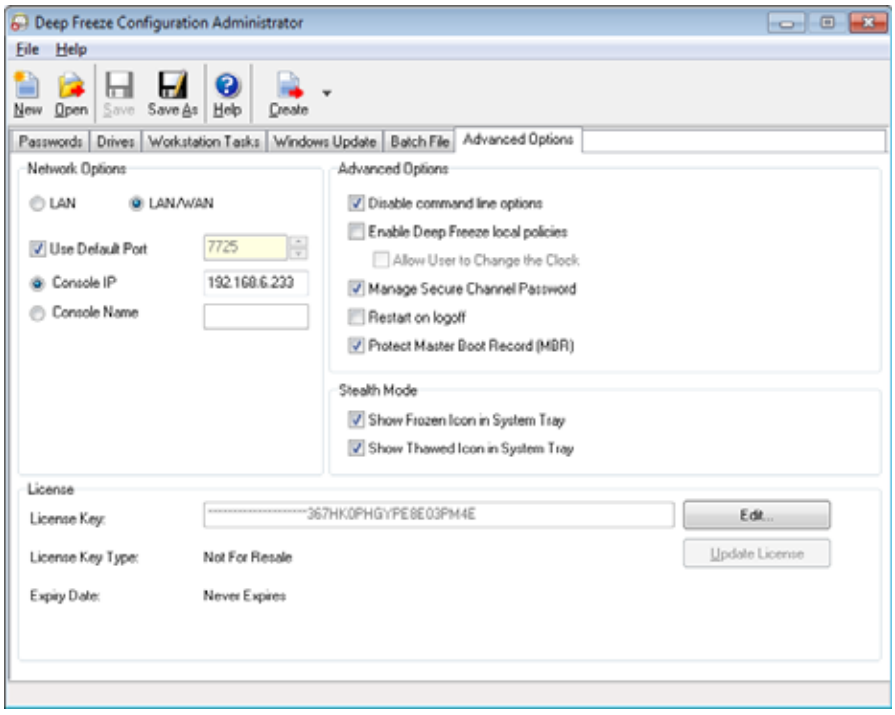
Example 2: Multiple Subnets, One Local Service

In this environment, the clients are located across more than one subnet. There is still only one Console being used. This environment does not require a Remote Console, although one could be used. The following diagram shows the network topology:



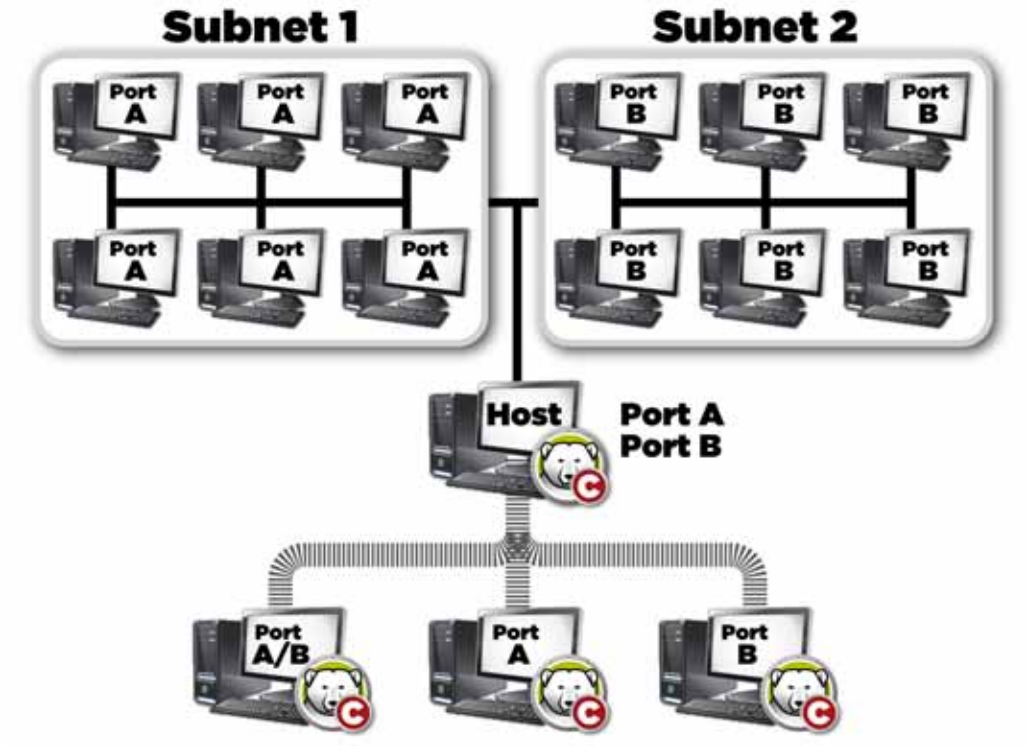
In this scenario (similar to Example 1: Single Subnet) both the clients and the connection hosted by the Console are using the same port. This port is configured in the Deep Freeze Enterprise Configuration Administrator in the *Advanced Options* tab, before creating the Workstation Install file or Workstation Seed.

In order for the clients to be seen, they need to be configured to use a LAN/WAN connection. When the LAN/WAN option is selected, a *Console IP* field appears. Specify the IP of the machine that will run the Enterprise Console. An example of these settings are shown in the *Advanced Options* tab below:



Example 3: Multiple Ports, Console Accessed Remotely

In this environment the clients are again located across multiple ports. In this case, more than one Console is being used. Multiple Consoles are accessed using a local service whose administrator (host) has released the connection information. The following diagram shows the network topology:



In this scenario, the host has set up a connection using the local service. Looking at the above diagram, three other Consoles connect to the host in order to see the clients according to their ports. The Consoles do not have to be a part of individual subnets as long as they can see the host.

More specifically, The Console connected through port A/B can see the host Console as well as each individual computer assigned to ports A and B. The other Consoles connected through port B can see the host and only the computers assigned to port B.

Example 4: Multiple Subnets, Multiple Local Services

In this example, there are two separate locations.

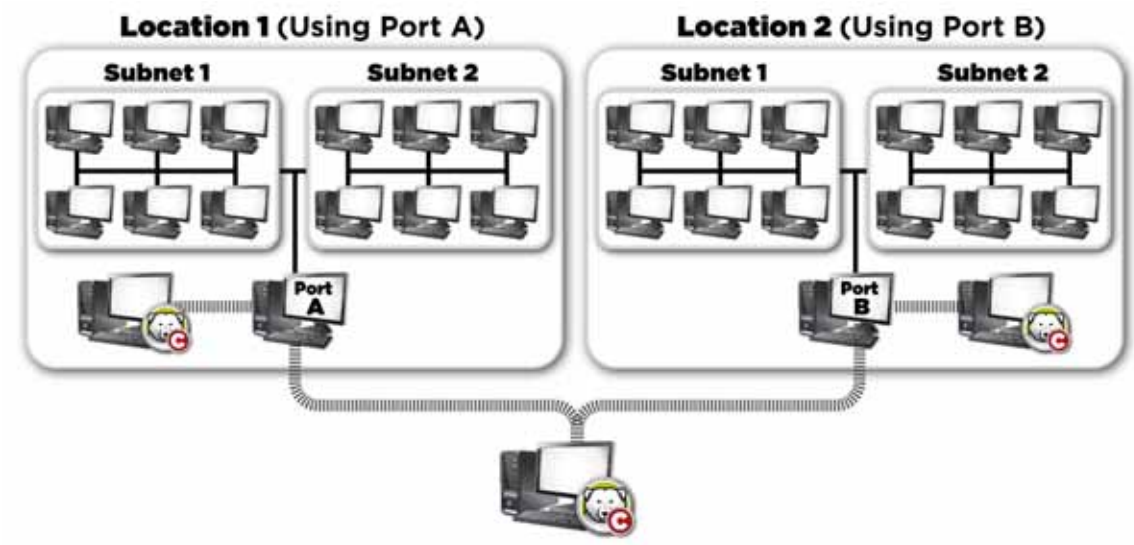
The following is a list of assumptions that are made regarding this particular example:

- The locations are spread apart and have only a minimal connection to each other.
- There is a network administrator at each location who is responsible for looking after Deep Freeze at that location.
- Both locations need to be administered from a third location.

In this example, the Remote Consoles are set up at each location and a local service is used:

- Location 1 (a computer lab on campus) uses port A to communicate with the clients and the connections hosted by the Console. The school library's computers use port B. The Console in the technical support department uses the connections hosted by both lab and library Consoles.
- Any console not directly communicating with a computer should have the local service turned off.

The following diagram shows the network topology:



The benefit of this setup is that it allows all the packets sent from the clients in Location 1 to be contained at that location. The less distance a packet must travel, the less chance there is of the packet failing.

The administrator in the lab can connect to the local service in the same location 1 but cannot connect to the local service in the library. The reason for this is that the lab administrator does not know the password to access the local service for the library. The same goes for the administrator in the library. If technical support knows the password to both local services (lab and library) the local service at both locations can be connected to, in order to administer all the clients.



Appendix C Troubleshooting a Remote Console Connection

No Clients In the Console

The following are some common reasons why clients fail to appear in the Console.

1. The Console and clients do not contain the correct network settings.

   If the Console is set up to run under one port and the clients are using another, they will not be able to see each other. Also, if the computers are configured for LAN/WAN, the IP must be equal to the IP of the machine where the Console is running.

   The default LAN setup works as long as all the machines running the computer and Console exist on the same subnet. However, if a VLAN is being run, or if there are several subnets where the clients exist, the computer install must be configured to run under the LAN/WAN settings.

2. Something on the network is blocking the port used between the Console and the clients.

   Check for a connection using a ping. The clients are unable to send packets to the Console/Remote Console because there does not seem to be a route to the host. Attempting to ping the IP of the Console/Remote Console does not seem to work. To resolve this issue, make sure the two machines can connect to each other.

   If a server, router, or switch on the network is not allowing the port to get through, the clients will not be seen. By default, 7725 is the port being used.

3. The workstations were created under a different Customization Code than the Console.

   When the Deep Freeze Enterprise Configuration Administrator is first run, a prompt for a Customization Code appears. This code is very important as it encrypts the software. This means that any workstations created are encrypted with this Customization Code. If a Console was created using another administrator that was installed with a different Customization Code, it cannot see workstations created under the original code. The workstations and Console must be created under a Configuration Administrator installed using the same exact Customization Code.

Port is in Use Error When Starting the Console

When attempting to start the Console, the error message *Unable to start Console: Port is in use* appears. There are several reasons why this error message may be appearing:

1. There is a Deep Freeze Workstation Installation/Workstation Seed installed under the same port as the Console or on the same computer.

   It is possible that Deep Freeze was installed is in stealth mode (the icon does not appear in the system tray). The seed does not show an icon. The best test is to run a Workstation Install file on the computer. If the uninstall option is displayed, the Workstation Install file or Workstation Seed is installed and can be uninstalled. If the uninstall option does not appear, the Workstation Install file or Workstation Seed is not installed.

   The simplest solution would be to first turn off the local service and then connect to a Console that can be accessed remotely.

2. Another program or service is using the port on this machine.

   This may involve running a port sniffer on the machine in question to see what ports are open. There are several tools available on the web to perform this action. The *netstat.exe* application found in Windows also should show whether the port Deep Freeze is using is already in use.

3. The network cable is unplugged.

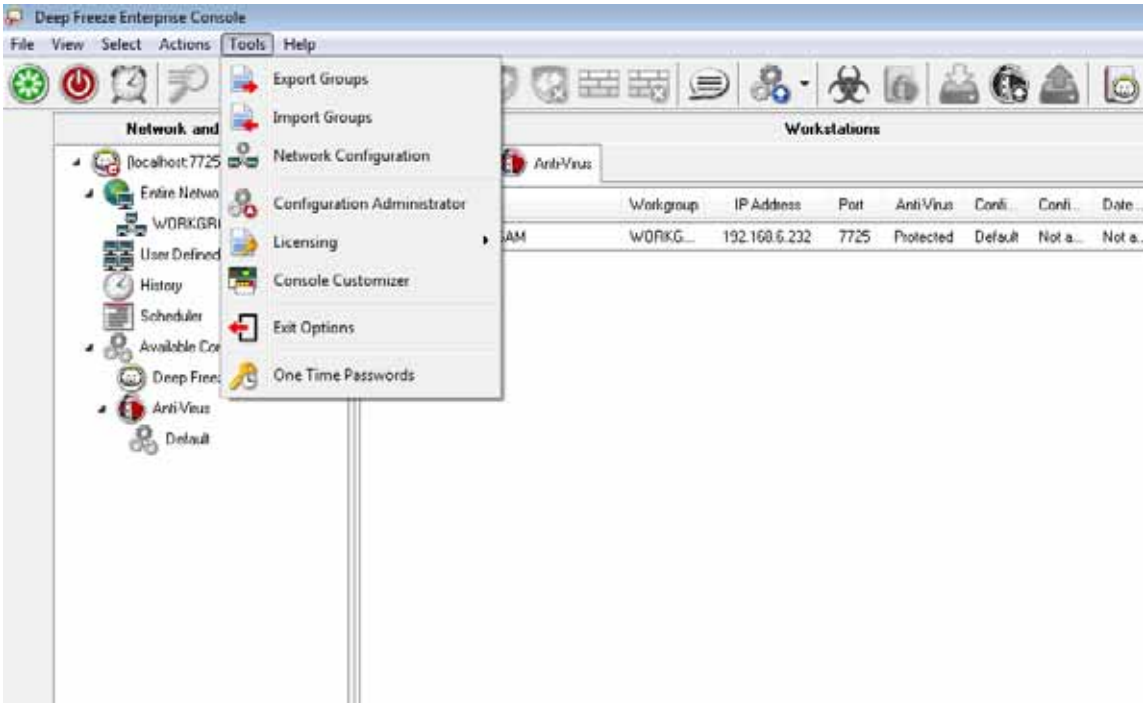
   This message can occur if there is no network connection on the machine.

Appendix D Creating a Customized Deep Freeze Enterprise Console

The Deep Freeze Enterprise Console includes the ability to create a new Enterprise Console with limited capabilities. A customized, limited console can be distributed in your organization to allow certain users to perform desired tasks, while ensuring they do not have access to the full capabilities of the Enterprise Console.

In this example, we will create a limited Console suitable for distribution to a teacher or computer lab instructor. In this scenario, we want the teacher to be able to restart machines, lock the keyboard and mouse on demand, and send messages to the students. However, we do not want the teacher to be able to boot the machines into a Thawed state, uninstall Deep Freeze, or perform other IT-exclusive tasks.

The Console Customizer can be launched from *Tools* > *Console Customizer*.



We will leave *Console functions* > *Activation* selected. This will ensure that if the new Console is moved to a different computer, a One Time Password will need to be entered on the computer the new Console is moved to. If this security precaution is not a concern in your environment, do not select this option.

Console functions > *One Time Password* is not selected because we do not want a teacher to be able to reboot the computer in Thawed mode under any circumstances. If a teacher reboots the computer in Thawed mode, students might install unnecessary software on the computer which will be retained even after a reboot.

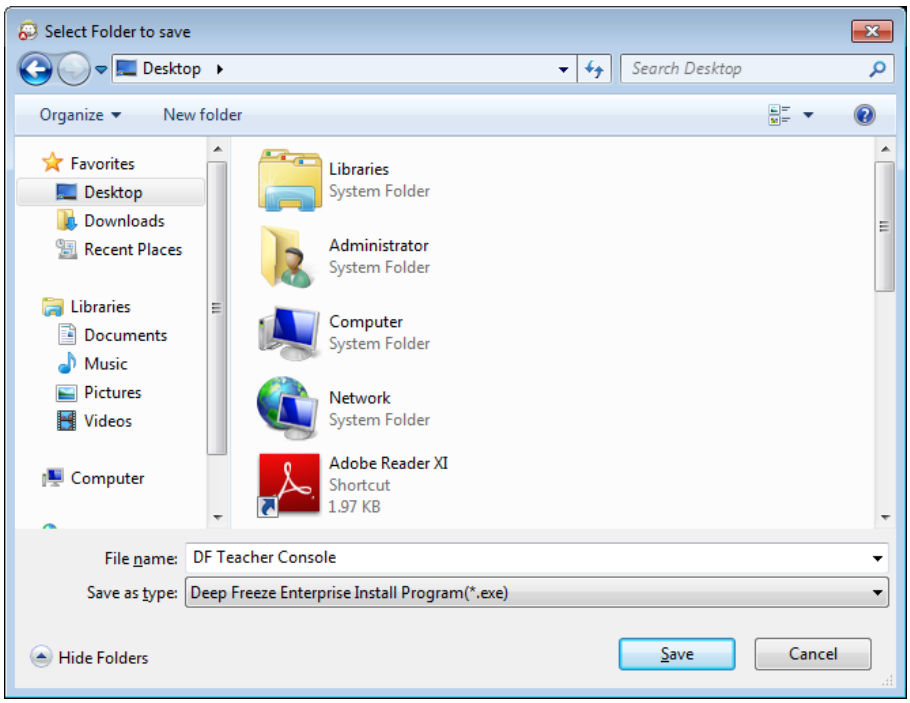
We will leave all options under *Workstation commands* selected because we want a teacher to be able to send messages to students, and to shutdown, restart, and wake computers as required.

We will only leave three options under Deep Freeze commands selected: *Unlock*, *Lock*, and *Reboot in Frozen* state. This will allow a teacher to lock (and unlock) the keyboard and mouse on student computers as required, as well as to reboot computers *Frozen* (just in case a computer is ever accidentally left *Thawed* by IT staff). Leaving all other options cleared will ensure a teacher is unable to permanently modify a computer.

Finally, we will clear all *Workstation install/uninstall commands* and all *Scheduler commands* because we don't want our teacher to use any of these options.



Once all options have been selected, click *Save As* to save a new Enterprise Console. A standard *Save As* dialog is displayed:



Save the new limited Enterprise Console and distribute it to the required users.

Appendix E Deep Freeze Action Files (RDC Example)

Deep Freeze Action Files

A Deep Freeze Action File is an XML file that allows administrators to define additional functionality into the Deep Freeze Enterprise Console. An Action File defines a method for calling an external batch file and passing some information (for example, machine IP addresses, computer names) to the batch file or script.

Action Files simply call an external program or script. Therefore, any scripting language that can be called from the command line can be used.

Action File Example

The structure of the Deep Freeze Action file that we will be using is shown below. The *DFEntConsoleCustomActions.xml* is available at *C:\Program Files\Faronics\Deep Freeze Enterprise*. The file can be edited to add additional actions like the one explained below:

```
<?xml version="1.0" encoding="UTF-8"?>
<!--Deep Freeze Default Custom Action file-->
<CUSTOMDEFINEDACTIONS>
 <ACTION1>
  <CAPTION>
   <ENGLISH>Control with RDC</ENGLISH>
   <GERMAN>Control with RDC German</GERMAN>
   <JAPANESE>Control with RDC Japanese</JAPANESE>
   <SPANISH>Control with RDC Spanish</SPANISH>
   <FRENCH>Control with RDC French</FRENCH>
   <CHINESE>Control with RDC Chinese</CHINESE>
</CAPTION>
  <FILEMENU>Y</FILEMENU>
  <POPUPMENU>Y</POPUPMENU>
  <SILENT>Y</SILENT>
  <SUBITEMS/>
  <PARAMS/>
  <SYNC/>
  <LOG/>
  <EXECUTE>C:\Windows\system32\mstsc.exe /v:%%WKSNAME%% /f</EXECUTE>
  <WORKDIR>C:\Windows\system32\</WORKDIR>
```

In the above example, the custom action file contains the command for running Remote Desktop on the Console computer and connect the remote computer specified in the parameter %%WKSNAME%%.

The *DFEntConsoleCustomActions.xml* file contains 3 samples:

- Control with RDC
- Remote Execution
- Push and Install MSI file

For more information on using the above samples, refer to the Configure Custom Actions section. You can edit the The *DFEntConsoleCustomActions.xml* file as per your needs.

Deep Freeze Action File Structure

The following XML schema outlines the custom defined actions available to the user. Multiple XML files can be saved based on the number of commands required. Each file must be saved to the Console folder and the read only attribute must not be selected.

Any changes made must be accompanied by a restart of the Deep Freeze Console in order to take effect.

Parameter	Usage
<?xml version="1.0" encoding="UTF-8"?>	
<CUSTOMDEFINEDACTIONS>	
<CAPTION>	Text that appears in file menu or submenu
<ENGLISH>Caption</ENGLISH>	Text in various languages
<GERMAN>Caption</GERMAN>	Text in various languages
<JAPANESE>Caption</JAPANESE>	Text in various languages
<SPANISH>Caption</SPANISH>	Text in various languages
<FRENCH>Caption</FRENCH>	Text in various languages
<CHINESE>Caption</CHINESE>	Text in various languages
<FILEMENU>y</FILEMENU>	Defines if this action will be in file menu
<POPUPMENU>y</POPUPMENU>	Defines if this action will be in right-click popup menu
<SILENT>y</SILENT>	Defines if user will be asked a confirmation message

Parameter	Usage
<SUBITEMS>	In sub-items, the item that is a child to this item can be defined
</SUBITEMS>	If the sub-items are defined then action for this items will be ignored
<SYNC>y</SYNC>	Specifies if command will be executed synchronously or asynchronously
<PARAMS>	Choosing this action prompts user to enter custom parameters
<PASSWORD>	Name on parameter
<VAR>%PARAM1%</VAR>	Name of variable which will be used in EXECUTE
<ENGLISH>USERNAME Param (ENGLISH)</ENGLISH>	Text in various languages
<GERMAN>USERNAME Param (GERMAN)</GERMAN>	Text in various languages
<JAPANESE>USERNAME Param (JAPANESE)</JAPANESE>	Text in various languages
<SPANISH>USERNAME Param (SPANISH)</SPANISH>	Text in various languages
<FRENCH>USERNAME Param (FRENCH)</FRENCH>	Text in various languages
<CHINESE>USERNAME Param (CHINESE)</CHINESE>	Text in various languages
</CAPTION>	
</USERNAME>	
</PARAMS>	
<LOG>	Defines behavior of the log file
<APPEND>y</APPEND>	Defines if log file will be appended or created new
<FILENAME>C:\a1command.log</FILENAME>	Defines filename
<EXECUTE>C:\windows\vpn.exe %%IP%% %USERNAME% %PASSWORD% %%WKSNAME%%</EXECUTE>	Defines command which will be executed. Here, parameters and/or console items can be used
<WORKDIR>C:\windows</WORKDIR>	Defines working directory

Console Parameters

The following console parameters can be passed to the executed application or script through the Enterprise Console:

Parameter	Usage
%%WKSNAME%%	Workstation name
%%DOMAIN%%	Workstation domain
%%IP%%	Workstation IP
%%PORT%%	Workstation port
%%STATUS%%	Workstation status
%%CFGDATETIME%%	Workstation configuration date/time
%%MAC%%	Workstation MAC address
%%DFVERSION%%	Workstation Deep Freeze version
%%CFGNAME%%	Workstation Configuration name
%%LOGGEDONUSER%%	Workstation logged on user
%%DFINSTALLATIONFILE%%	Workstation installation file
%%LICENSESTATUS%%	Workstation license status
%%LICENSEEXPIRYDATETIME%%	Workstation license expiry date and time
%%AVSTATUS%%	Workstation Anti-Virus status
%%OSVERSION%%	Workstation Operating System version