



# Deep Freeze

ADVANCED System Integrity

---

## 用户指南

---



最近修改日期：2025 年

© 1999 – 2025 Faronics Corporation。保留所有权利。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 和 WINSelect 是 Faronics Corporation 的商标和 / 或注册商标。所有其他公司名称和产品名称均为其各自所有者的商标。

受专利保护：US 7,539,828 | US 7,917,717 | US 9,152,824 | US 9,785,370



# 目录

<b>序言</b> .....	<b>9</b>
<b>重要信息</b> .....	<b>10</b>
关于 Faronics .....	10
产品文档 .....	10
<b>技术支持</b> .....	<b>11</b>
联系信息 .....	11
<b>简介</b> .....	<b>13</b>
Deep Freeze 概述 .....	14
系统要求 .....	15
Deep Freeze Enterprise 文件 .....	16
<b>安装 Deep Freeze</b> .....	<b>17</b>
安装概述 .....	18
安装 Deep Freeze Enterprise 配置管理程序和企业控制台 .....	18
自定义代码 .....	21
重新初始化自定义代码 .....	21
更新模式 .....	21
次性密码 .....	23
<b>使用 Deep Freeze Enterprise 配置管理程序</b> .....	<b>25</b>
访问配置管理程序 .....	26
工具栏和菜单 .....	26
"密码"选项卡 .....	28
"驱动器"选项卡 .....	29
Frozen 驱动器 .....	29
ThawSpace .....	30
现有 ThawSpace 解冻空间 .....	32
始终解冻外置硬盘驱动器 .....	33
"工作站任务"选项卡 .....	34
Windows 更新 .....	35
重启 .....	39
关机 .....	40
空闲时间 .....	42
批处理文件 .....	43
Thawed 期间 .....	45
"Windows 更新"选项卡 .....	48
"批处理文件"选项卡 .....	51
"高级选项"选项卡 .....	53
网络 .....	53



高级选项 .....	54
隐蔽模式 .....	57
许可证 .....	57
创建工作站安装程序和 .....	58
<b>使用 Deep Freeze 企业控制台 .....</b>	<b>61</b>
Deep Freeze 配置 .....	62
应用 Deep Freeze 配置 .....	62
编辑 Deep Freeze 配置 .....	63
删除 Deep Freeze 配置 .....	63
导出 Deep Freeze 配置 .....	63
配置生成器 .....	64
从命令行使用配置生成器 .....	65
配置文件参数 .....	65
Deep Freeze 企业控制台 .....	69
启动 Deep Freeze 企业控制台 .....	69
激活 Deep Freeze 企业控制台 .....	70
状态图标 .....	70
查看列 .....	72
基于状态的选择 .....	73
管理控制台与工作站之间的通信 .....	74
配置本地服务 .....	74
编辑或删除本地服务连接 .....	76
配置代理服务器连接 .....	76
远程控制台 .....	78
设置启用远程控制的连接 .....	78
连接到远程控制台 .....	79
使用控制台管理 Deep Freeze .....	80
以指定次数重启 Thawed 解冻/重启 Thawed 解冻锁定 .....	81
登录用户 .....	81
正在向计算机发送消息 .....	82
更新 Deep Freeze 配置文件 .....	83
运行 Windows 更新 .....	83
远程启动 .....	84
推送并启动 .....	85
格式化 ThawSpace 解冻空间 .....	86
删除 ThawSpace 解冻空间 .....	86
查看控制台日志文件 .....	87
针对性安装 Deep Freeze .....	88
更新 Deep Freeze 软件 .....	88
Thawed 解冻警报 .....	88
许可证 .....	89
手动激活 .....	90
许可证图标 .....	91
报告 .....	92



自定义网格 .....	93
标签 .....	95
创建/分配标签 .....	95
移除/取消分配标签 .....	95
删除标签 .....	96
注释 .....	97
添加注释 .....	97
计划 Deep Freeze 任务 .....	98
编辑计划的任务 .....	102
为计划的任務分配计算机 .....	103
添加任务 .....	103
编辑任务 .....	103
暂停任务 .....	103
恢复任务 .....	103
删除任务 .....	104
立即执行任务 .....	104
计划任务的属性 .....	104
管理网络和组 .....	105
添加组 .....	105
构建用户定义的组结构 .....	109
从 Active Directory 导入组 .....	109
历史记录 .....	110
将计算机添加到组 .....	111
配置自定义操作 .....	112
使用 RDC 控制 .....	112
远程执行 .....	113
推送并安装 MSI 文件 .....	114
推送并启动 .....	115
远程启动 .....	116
删除、导入和导出自定义操作 .....	117
控制台自定义程序 .....	118
关闭 Deep Freeze 企业控制台 .....	119
在工作站上安装 Deep Freeze .....	120
有人参与安装或卸载 .....	120
通过控制台在工作站上卸载 Deep Freeze .....	122
无提示安装或卸载 .....	123
命令行示例 .....	123
使用快捷方式无提示安装或卸载 .....	124
在多个计算机上进行网络安装 .....	124
在现有 Deep Freeze 版本基础上安装 .....	125
使用映像安装 .....	125
针对性安装 .....	126
检查更新 .....	127
<b>管理 Deep Freeze 计算机 .....</b>	<b>129</b>
登录屏幕 .....	130



在触摸屏设备上启动 Deep Freeze 冰点 .....	130
"启动控制"选项卡 .....	131
下次启动时状态 .....	131
克隆 .....	131
许可证 .....	132
"密码"选项卡 .....	134
"网络"选项卡 .....	135
"解冻空间"选项卡 .....	136
软件永久性安装 · 更改或删除 .....	137
<b>管理 Anti-Virus .....</b>	<b>139</b>
Anti-Virus 概述 .....	140
Anti-Virus 防病毒报告 .....	141
迁移到新的 Anti-Virus 防病毒 .....	142
在企业版控制台上启用 Anti-Virus 防病毒 .....	143
在工作站上安装 Anti-Virus 防病毒客户端 .....	144
Anti-Virus 配置 .....	145
创建 Anti-Virus 配置 .....	145
应用 Anti-Virus 配置 .....	163
编辑 Anti-Virus 配置 .....	163
删除 Anti-Virus 配置 .....	163
从企业控制台使用 Faronics Anti-Virus .....	164
Anti-Virus 命令 .....	164
计划 Anti-Virus 任务 .....	168
在工作站上使用 Anti-Virus .....	169
在工作站上启动 Anti-Virus .....	169
扫描工作站 .....	170
通过右键单击扫描文件或文件夹 .....	171
查看扫描历史记录 .....	171
查看隔离的文件并对其进行操作 .....	172
在工作站上更新 Anti-Virus 定义 .....	173
通过系统任务栏管理工作站上的 Anti-Virus .....	174
检查 Anti-Virus 更新 .....	176
更新 Faronics Anti-Virus .....	177
更新 Anti-Virus 防病毒定义 .....	178
从企业控制台卸载 Anti-Virus 客户端 .....	179
从企业控制台禁用 Faronics Anti-Virus .....	180
<b>Deep Freeze 命令行控制 .....</b>	<b>181</b>
Deep Freeze 命令行控制 (DFC.EXE) .....	182
DFC 返回值 .....	182
DFC 命令行语法 .....	183
Faronics Anti-Virus 命令行语法 .....	186
<b>附录 A 端口和协议 .....</b>	<b>187</b>



<b>附录 B 网络示例</b> .....	<b>189</b>
示例 1 – 单个子网 .....	190
示例 2 – 多个子网 · 一个本地服务.....	191
示例 3 – 多个端口 · 远程访问控制台.....	192
示例 4 – 多个子网 · 多个本地服务.....	193
<b>附录 C 远程控制台连接的故障排除</b> .....	<b>195</b>
控制台中无客户端 .....	195
启动控制台时出现端口正在使用错误.....	196
<b>附录 D 创建自定义 Deep Freeze 企业控制台</b> .....	<b>197</b>
<b>附录 E Deep Freeze 操作文件 – RDC 示例</b> .....	<b>199</b>
Deep Freeze 操作文件.....	199
操作文件示例 .....	199
Deep Freeze 操作文件结构.....	200
控制台参数 .....	202





# 序言

本用户指南介绍如何安装、配置和使用 Deep Freeze Enterprise。

## 主题

---

[重要信息](#)

[技术支持](#)



## 重要信息

---

本部分包含有关 Faronics 产品的重要信息。

### 关于 Faronics

Faronics 致力于提供各种业内领先的解决方案帮助企业管理，简化复杂的 IT 环境并确保其安全。我们的产品能够完全确保机器的正常工作，并使成千上万的信息技术人员的日常工作得到了重大改善。在以市场为中心的理念推动下，Faronics 的技术创新能够让教育机构，医疗机构，图书馆，政府部门以及企业获益。

### 产品文档

以下文档构成了 Deep Freeze Enterprise 文档集：

- Deep Freeze Enterprise 用户指南 – 即本文档。本文档将指导您如何使用本产品。
- Deep Freeze Enterprise 发布声明 – 此文档列出了最新功能以及已知问题和已解决的问题。



## 技术支持

---

在设计本软件时，我们竭尽所能确保其易于使用并尽量不出问题。如果遇到问题，请与技术支持部联系。

电子邮件 [support@faronics.com](mailto:support@faronics.com)

电话 800-943-6422 或 +1-604-637-3333

工作时间上午 7:00 至下午 5:00 太平洋时间

## 联系信息

- 网址 [www.faronics.com](http://www.faronics.com)
- 电子邮件 [sales@faronics.com](mailto:sales@faronics.com)
- 电话 800-943-6422 或 +1-604-637-3333
- 传真 800-943-6488 或 +1-604-637-8188
- 工作时间上午 7:00 至下午 5:00 太平洋时间
- 地址

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





# 简介



Deep Freeze 冰点可保护设置为从硬盘驱动器启动的计算机。将 CMOS 配置为仅从硬盘驱动器启动。必须对 CMOS 使用密码保护，以防止未经授权更改。Deep Freeze 冰点会在计算机处于 Frozen 冻结状态时保护主引导记录 (MBR)。

## 主题

---

[Deep Freeze 概述](#)

[系统要求](#)

[Deep Freeze Enterprise 文件](#)



## Deep Freeze 概述

---

Faronics Deep Freeze 可为计算机配置添加一道坚不可摧的防护墙，从而帮助企业消除计算机故障和停机问题。将 Deep Freeze 安装到计算机后，对计算机所做的任何更改——无论是无意更改还是恶意更改——都不会得到保存。Deep Freeze 可对当今困扰计算机的很多问题提供即时防护能力，可防范的问题包括：不可避免的配置漂移，意外的系统配置错误，恶意软件行为和偶然的系统性能下降。

现在，可以使用 Deep Freeze Enterprise 管理 Faronics Anti-Virus ( Faronics Anti-Virus 需要单独的许可证 )。Faronics Anti-Virus 保护计算机不受安全风险攻击，并且不会因为慢速扫描时间和占用大量资源而降低计算机速度。采用新一代技术构建的 Faronics Anti-Virus 集强大的防病毒，防 Rootkit 和防间谍软件于一体，可保护您不受现今高度复杂的恶意软件侵害，同时与 Deep Freeze 无缝集成。

与 Deep Freeze 集成后，通过 Deep Freeze 企业控制台的部署和管理功能，可确保以最简单的方式获得最新的 Faronics Anti-Virus 防护。Faronics Anti-Virus 可与 Deep Freeze 无缝地协同工作，即使工作站处于 Frozen 状态亦可随时更新，从而提供功能最全面的保护系统。



## 系统要求

---

### 桌面版

Deep Freeze 冰点客户端与 Faronics Anti-Virus 防病毒客户端

- Windows 7 和 8.1 ( 32 位和 64 位 )
- Windows 10 ( 最高 22H2 版 ) ( 32 位和 64 位 )
- Windows 11 ( 最高 24H2 版 )
- Windows Embedded 7 和 8

Deep Freeze Enterprise 配置管理程序和企业控制台的平台：

- Windows 7 和 8.1 ( 32 位和 64 位 )
- Windows 10 ( 最高 22H2 版 ) ( 32 位和 64 位 )
- Windows 11 ( 最高 24H2 版 )
- Windows Server 2008 R2 ( 32 位和 64 位 )
- Windows Server 2012 · 2016 · 2019 · 2022 · 2025

### 服务器版

Deep Freeze 冰点客户端：

- Windows Server 2008 R2 ( 32 位和 64 位 )
- Windows Server 2012 · 2016 · 2019 · 2022 · 2025

Deep Freeze Enterprise 配置管理程序和企业控制台的平台：

- Windows 7 和 8.1 ( 32 位和 64 位 )
- Windows 10 ( 最高 22H2 版 ) ( 32 位和 64 位 )
- Windows 11 ( 最高 24H2 版 )
- Windows Server 2008 R2 ( 32 位和 64 位 )
- Windows Server 2012 · 2016 · 2019 · 2022 · 2025

Deep Freeze 要求硬盘上至少有 10% 的可用空间。



Deep Freeze 与 Windows 的核心隔离功能兼容。

请访问 <https://www.faronics.com/core-isolation>，了解更多信息



## Deep Freeze Enterprise 文件

Deep Freeze 采用不同颜色的图标来表示它的各个组件。由红色图标指示的文件通常只应安装在管理计算机中。

图标	定义
	Deep Freeze Enterprise 配置管理程序和企业控制台安装文件。
	配置管理程序：用于创建自定义，预配置的计算机安装程序文件和工作站种子。
	企业控制台应用程序：用于集中部署，监控，管理和维护所安装的 Deep Freeze。
	自定义的 Deep Freeze 工作站安装文件：在配置管理程序中创建，并部署到企业的各个工作站。此文件包含工作站种子。因此，如果安装了 Deep Freeze 工作站安装文件，则无需单独安装工作站种子。
	通过工作站种子，企业控制台与网络中计算机之间可以实现无缝通信。在计算机上安装了工作站种子之后，该计算机将显示在企业控制台上。一旦计算机显示在企业控制台中，即可远程对该计算机执行各种操作，例如重启，关机和远程唤醒。也可以远程将 Deep Freeze 安装在显示的计算机上，从而允许对远程计算机执行 Deep Freeze 相关操作。



# 安装 Deep Freeze

本章描述 Deep Freeze 的安装过程。

## 主题

---

[安装概述](#)

[自定义代码](#)

[次性密码](#)



## 安装概述

### 安装 Deep Freeze Enterprise 配置管理程序和企业控制台

配置管理程序应仅安装在用于管理 Deep Freeze 的计算机上。配置管理程序用于创建自定义 Deep Freeze 安装文件和工作站种子。Deep Freeze 企业版控制台会自动随 Deep Freeze Enterprise 配置管理程序一起安装。



如果您使用的是 Deep Freeze 冰点 6.5 版（或更高版本），在安装 Deep Freeze 冰点 8.1 版（或更高版本）时，可以在安装过程中选择自动升级企业版控制台，配置管理程序和 Deep Freeze 冰点安装 / 配置文件（位于安装程序文件夹下）。更新 Deep Freeze 时无需 Customization Code 自定义代码。

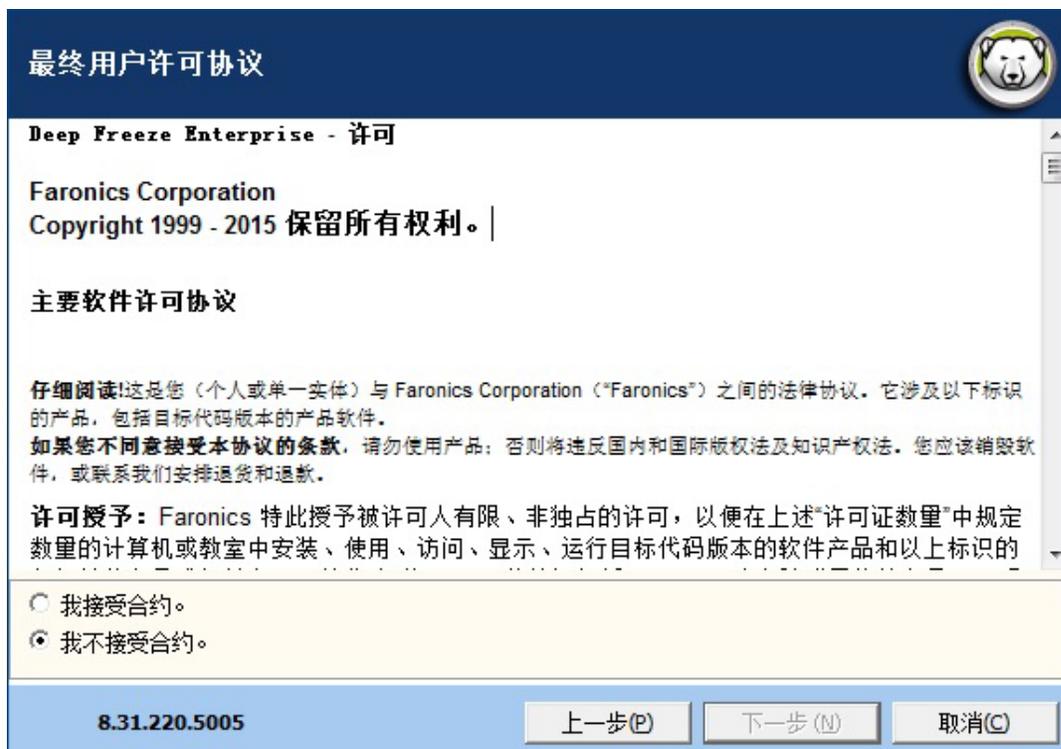
若要安装配置管理程序，请完成以下步骤：

1. 双击 *DFEnt.exe* 文件开始安装过程。此时将显示以下屏幕：





2. 单击 **下一步**。阅读并接受许可协议。单击 **下一步**。



3. 在 **许可证密钥** 字段中输入许可证密钥，或者选中 **使用评估版** 复选框以 **评估模式** 安装。单击 **下一步**。( Deep Freeze 冰点将自动激活工作站许可证。必须在 30 天之内激活 Deep Freeze 冰点，以免过期。 )





- 在 **许可证密钥** 字段中输入许可证密钥，或者选中 **使用评估版** 复选框以 **评估模式** 安装。单击 **安装**。



- 此时将显示 **自定义代码** 屏幕。



- 指定 **Customization Code** 自定义代码，然后单击 **下一步**。**Customization Code** 自定义代码必须至少包含 8 个字符。



## 自定义代码

自定义代码是一个唯一标识符，用于对配置管理程序、企业控制台、计算机安装文件、一次性密码生成系统和 Deep Freeze 命令行控制进行加密。此代码不是用于访问 Deep Freeze 的密码。

使用自定义代码可防止未经授权的管理员访问或控制计算机。如果同一组计算机由多个 Deep Freeze 管理员控制，则这些管理员必须使用同一自定义代码。



您必须记录并妥善保管自定义代码。如果丢失或忘记自定义代码，Faronics 将无法恢复。

### 重新初始化自定义代码

如果其他管理员希望使用不同的自定义代码在同一配置管理程序中创建多个安装文件，请完成以下步骤：

1. 运行 DFInit.exe。
2. 此操作将重置配置管理程序的现有自定义代码。
3. 输入新的自定义代码。
4. 单击 *确定* 使新的自定义代码生效。

### 更新模式

更新模式可用于自动创建 Deep Freeze Enterprise 现有文件的更新版本，方法是执行相应的 Update 命令。此命令将完成两个任务：

- Deep Freeze 企业控制台和 Deep Freeze Enterprise 配置管理程序的原有版本。（位于 Faronics > Deep Freeze Enterprise 目录下。）
- 更新用户创建的存储在以下文件夹中的所有文件：Faronics > Deep Freeze Enterprise > Install Programs。

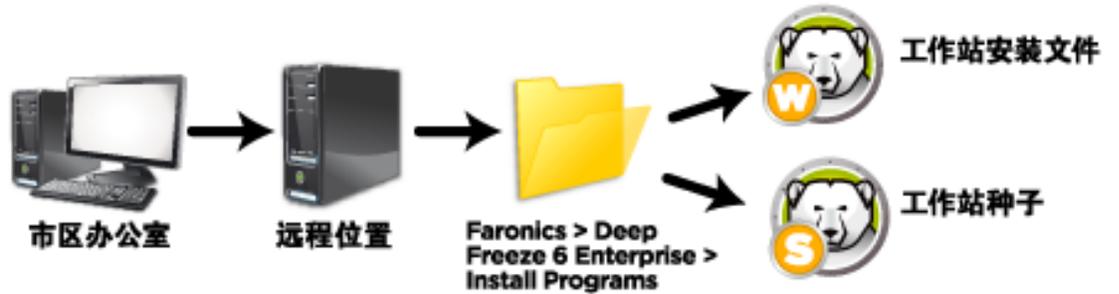
这些更新的好处是可将一些文件更新为最新版本，而同时保持其配置数据（由旧版 Deep Freeze Enterprise 创建）不变。

该命令自动更新由管理程序创建的位于 Faronics > Deep Freeze Enterprise > Install Programs 目录和以下子目录中的文件（包括 .exe 文件和 .rdx 文件）：

- Workstation install files
- Workstation Seed files



在下例中，市区办公室收到一个新版本的 Deep Freeze Enterprise 配置管理程序，它能够自动更新位于远程位置的任何现有 Deep Freeze 工作站安装文件和工作站种子。



执行更新命令不需要提供密码，但需要提供自定义代码。该命令的语法如下：

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

- PathToFile 必须用安装文件 (DFEnt.exe) 的实际路径替换
- DFEnt.exe 必须是安装文件的实际名称（如果该文件是通过下载获得的，则名称可能有所不同）
- "Customization Code"（自定义代码）中若包含空格，则必须加上引号
- "Customization Code" 必须与原安装文件的自定义代码一致

日志文件将记录所更新文件的所有详细信息。

完成更新过程可能需要几分钟时间。

更新模式不能更新计算机上的现有 Deep Freeze 版本。计算机的更新必须通过企业控制台来进行。



## 一次性密码

一次性密码生成系统用于生成 Deep Freeze 的临时密码，此类密码将在生成日的午夜到期。

可从以下位置访问 *一次性密码* 对话框：

- 企业控制台上的 *工具* > *一次性密码*。有关详细信息，请参阅[使用 Deep Freeze 企业控制台](#)。
- 配置管理程序中的 *文件* > *一次性密码*。有关详细信息，请参阅。

一次性密码 (OTP) 在某些情况下十分有用，例如，忘记了 Deep Freeze 密码或者在创建配置文件时没有设定密码。OTP 还可用于为执行维护工作的人员提供访问计算机的权限，从而避免将 Deep Freeze 的永久性密码告知该人员。

若要创建一次性密码，请完成以下步骤：

1. 选择 *只能使用一次的密码或能多次使用的密码*。所有类型的一次性密码都会在生成当日午夜到期。
2. 在需要 OTP 的计算机上，在 *令牌* 字段中输入 OTP 令牌。计算机的 OTP 令牌可在登录对话框中找到，如下图所示。



3. 单击 *生成*。



在 Deep Freeze 命令行界面中不能使用一次性密码。





# 使用 Deep Freeze Enterprise 配置管理程序

## 主题

---

[访问配置管理程序](#)

["密码" 选项卡](#)

["驱动器" 选项卡](#)

["工作站任务" 选项卡](#)

["Windows 更新" 选项卡](#)

["批处理文件" 选项卡](#)

["高级选项" 选项卡](#)

[创建工作站安装程序和](#)



## 访问配置管理程序

从开始菜单中进行如下选择以打开配置管理程序：

开始 > 所有程序 > Faronics > Deep Freeze Enterprise > Deep Freeze 管理程序

配置管理程序中有多个选项卡，用于配置密码，处于 Frozen 状态的驱动器，工作站任务，Windows 更新，批处理文件和高级选项。在配置了这些设置后，即会创建一个工作站安装文件。可将工作站安装文件安装到需要受 Deep Freeze 保护的计算机上。也可以通过 Deep Freeze Enterprise 控制台访问 Deep Freeze Enterprise 管理程序。

## 工具栏和菜单

### 工具栏

工具栏位于配置管理程序的各个选项卡的顶端。



图标	功能
新建	清空现有的所有配置设置。以默认的配置设置打开。
打开	打开任何保存的 .rdx，工作站安装文件或者 Workstation Seed 文件。
保存	保存 .rdx，工作站安装文件或者 Workstation Seed 文件。文件名和路径列表位于配置管理程序底部的状态区中。
另存为	将配置设置保存为 .rdx 文件。
帮助	访问 Deep Freeze 帮助文件。
创建	<p><i>创建工作站安装文件</i>可为工作站上面的安装创建一个定制的安装程序。工作站可以从 Deep Freeze 企业控制台管理。</p> <p><i>创建 Workstation Seed 文件</i>可创建一个 Seed，允许 Deep Freeze 通过网络与工作站进行通信。一旦 Seed 安装在工作站上面，即可远程部署 Deep Freeze 工作站安装文件。</p>



## 文件菜单

文件菜单包含工具栏中的所有选项，还包含用于选择语言的选项和 *密码保护* 选项。



## 密码保护

*密码保护* 提供了一层额外的安全保护，供管理员选择使用。

若要对配置管理程序的访问实施密码保护，请完成以下步骤：

1. 打开文件菜单，选择 *密码保护*。
2. 选中 *受密码保护* 复选框。
3. 输入并确认密码。
4. 单击 *确定* 设置密码，或单击 *取消* 关闭对话框而不设置密码。

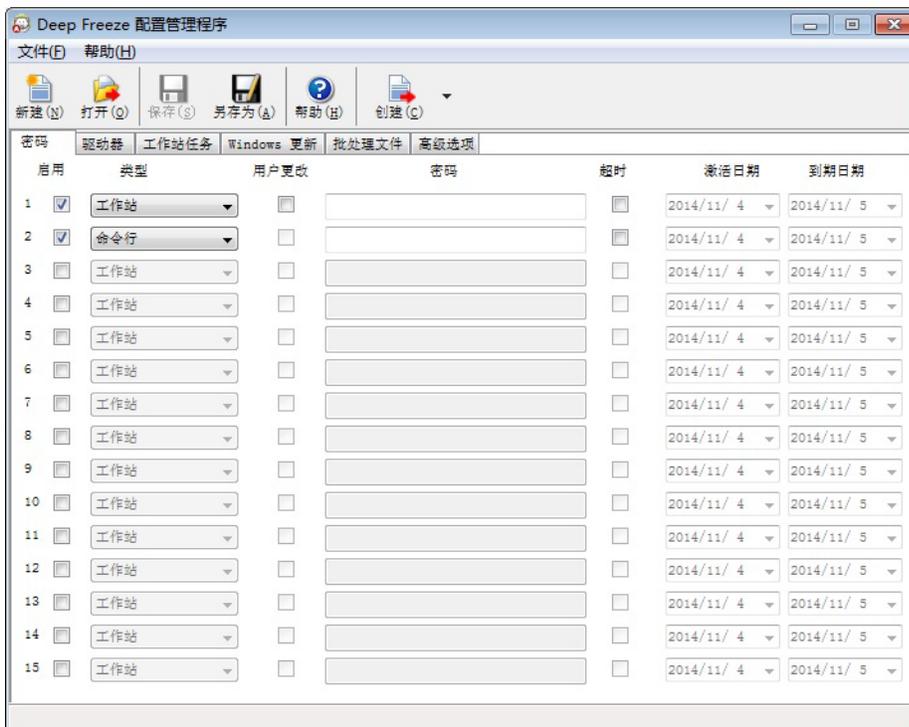


将密码保存在一个安全的地方。如果密码丢失，您不能恢复它。您必须重新安装 Deep Freeze。



## " 密码 " 选项卡

Deep Freeze Enterprise 允许管理员最多选择 15 个固定密码。



若要创建密码，请完成以下步骤：

1. 在相应行中选择 **启用**。
2. 从 **类型** 下拉列表中，选择所需的密码类型。系统将显示以下选项：
  - > 工作站：用于工作站中启动 **登录屏幕** 时。
  - > 命令行：用于命令行控制。只有至少定义了一个命令行密码，才可使用命令行控制工具 (*DFC.exe*)。
3. 可选：对于这些密码，选中 **用户更改** 复选框可允许用户在计算机上更改密码。
4. 输入密码。



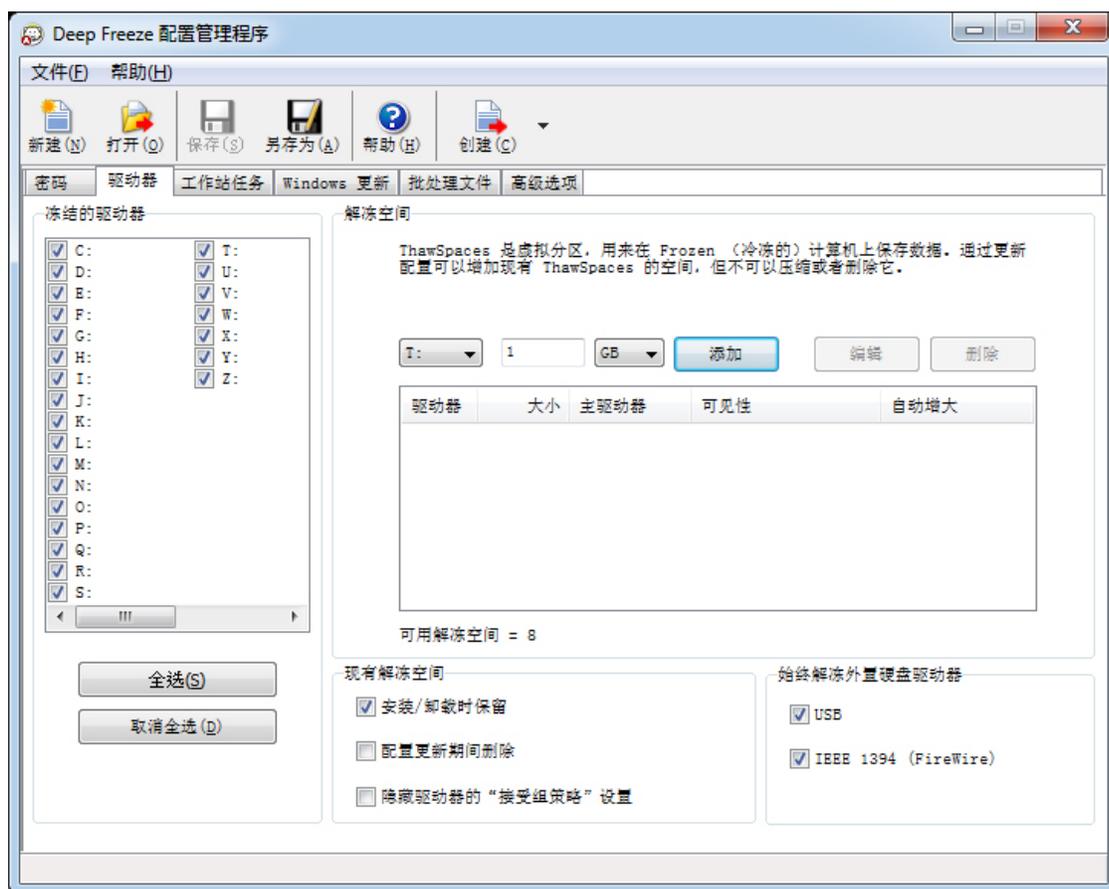
在 **密码域** 中输入的密码不是隐藏的。  
命令行和 GUI 不得使用相同的密码。

5. 若要将密码设置为在指定日期激活和到期，请选中 **超时** 复选框，然后使用下拉日历指定 **激活日期** 和 **到期日期**。



## " 驱动器 " 选项卡

*驱动器*选项卡用于选择将处于 Frozen（受 Deep Freeze 保护）或 Thawed（不受保护）状态的驱动器。您也可以创建一个 ThawSpace——由 Frozen 或者 Thawed 驱动器托管的虚拟分区，这里的数据可以永久保存，在重新启动时不会被删除。



### Frozen 驱动器

默认情况下，所有驱动器都处于 Frozen 冻结状态。要将某个驱动器设置为 Thawed 解冻状态，请清除该驱动器对应的复选框。

虽然只能将本地驱动器（分区或物理驱动器）设置为 Frozen 冻结状态，但此处显示出了所有驱动器盘符，因为预先配置的安装文件可以安装到硬件和软件设置不同的多台计算机上。

### 示例

在以上屏幕中，D: 在 *Frozen 驱动器* 列表中没有被选中。因此，除 D: 之外的所有驱动器都将处于 Frozen 状态。



## ThawSpace

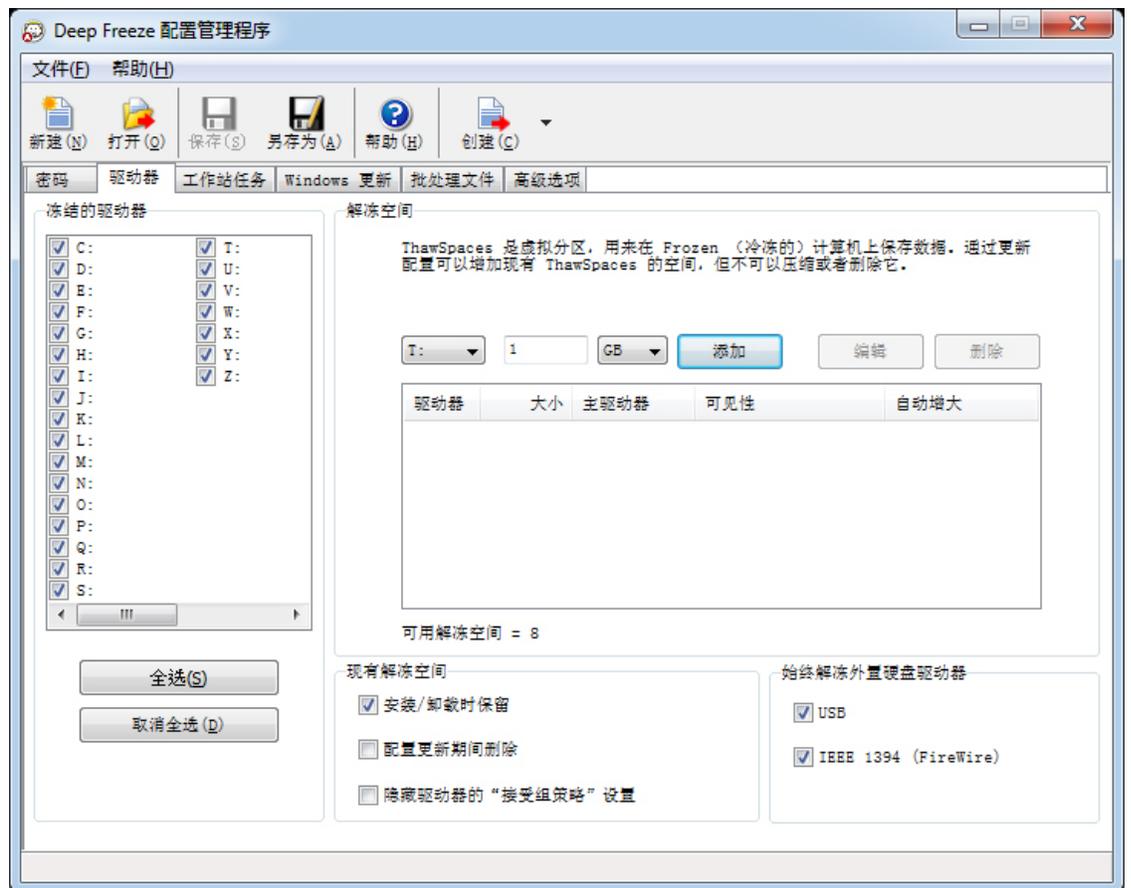
ThawSpace 是一个虚拟分区，可用于存储程序，保存文件或进行永久性更改。ThawSpace 中存储的所有文件均在重启后保留，即便计算机处于 Frozen 状态。可以在一个配置为 Frozen 或 Thawed 状态的驱动器上面创建一个 ThawSpace。

ThawSpace 解冻空间可以设置为通过 *自动扩充* 选项进行自动扩展，以防止空间不足。当可用空间仅为 25% 或以下时，ThawSpace 解冻空间将自动扩展当前大小的 25%。该空间可扩展为 ThawSpace 解冻空间配置中所定义的最大大小。



ThawSpace 解冻空间仅在 Thawed 解冻状态下扩展。

一旦 ThawSpace 解冻空间扩展后，即使可用空间超过 25%，或者使用给定 ThawSpace 解冻空间驱动器盘符更新较小的工作站配置时，ThawSpace 解冻空间也不会再缩小。



要使用配置管理程序创建单个 ThawSpace 解冻空间或多个 ThawSpace 解冻空间，请完成以下步骤：

1. 选择盘符。默认号是 T。但是，可将其更改为任何可用盘符。如果所选的盘符在安装 Deep Freeze 冰点时已经存在于计算机上，系统将自动使用下一个可用盘符。



- > 如果从下拉列表中选择了某个 *驱动器盘符* 并使用该盘符创建 ThawSpace 解冻空间，则系统会从该下拉列表中将其删除。
  - > 删除某个 ThawSpace 解冻空间后，对应的 *驱动器盘符* 将会再次添加到下拉列表中。
  - > *盘符* 不能与 *主机驱动器* 相同。
2. 单击 **添加**。此时将显示 **添加 ThawSpace 解冻空间** 对话框：

3. 输入 *大小* 值。这是 ThawSpace 解冻空间的大小，最大为 1024 GB，最小为 16 MB。
- > 如果计算机没有足够的可用空间来容纳所选的 ThawSpace 解冻空间，则 ThawSpace 解冻空间的大小将缩减，以确保计算机正常工作。
  - > 如果您选择小于 16 MB 的大小，则 ThawSpace 解冻空间将设置为 16 MB。
  - > 如果您选择大于 1024 GB (1 TB) 的大小，则 ThawSpace 解冻空间将设置为 1024 GB (1 TB)。
4. 选择 ThawSpace 解冻空间存储单位 ( MB 或 GB )。
5. 选择 *主机驱动器*。
- > *主机驱动器* 是指 ThawSpace 解冻空间所在的驱动器。
  - > ThawSpace 解冻空间所需的存储空间来自 *主机驱动器* 上的总存储空间。
6. 从 *可见性* 复选框选择 *可见* 或 *隐藏*。
- > 如果选择 *可见*，Windows 资源管理器中将会显示该驱动器。
  - > 如果选择 *隐藏*，Windows 资源管理器中将不会显示该驱动器。
  - > 不过，可通过在 *开始* > *运行* 中输入相应盘符来访问隐藏的驱动器。
7. 勾选 *自动将 ThawSpace 解冻空间扩充到最大值* 复选框，并配置 ThawSpace 解冻空间的最大大小。
8. 单击 **添加** 以添加 ThawSpace 解冻空间。

## 删除 ThawSpace 解冻空间

若要删除某个 ThawSpace 解冻空间，请将其选中并单击 **删除**。此时 ThawSpace 解冻空间被删除，其驱动器盘符将再次出现在 *驱动器盘符* 下拉列表中。单击 **全部删除** 可删除所有 ThawSpace 解冻空间。



在配置管理程序中删除某个 ThawSpace 解冻空间后，此解冻空间将在配置应用至工作站后方可生效。

在删除一个 ThawSpace 解冻空间之前，请先删除任何用户配置文件重定向或者符号链接。

如果 ThawSpace 解冻空间被删除，则保存在其上的数据也将被删除。

ThawSpace 解冻空间不受 Deep Freeze 冰点的保护。部署标准数据保护选项，如 Anti-Virus 防病毒程序和备份程序。

## 示例

在以上屏幕中，在 *主机驱动器 C:* 上创建一个 16 MB 的 ThawSpace 解冻空间，且该 ThawSpace 解冻空间的盘符为 T:。将 ThawSpace 解冻空间 T: 设置为 *可见*，并可通过 Windows 资源管理器访问。



建议使用字母表中靠后的字母（如 X、Y、Z）来指定驱动器盘符，以避免在拔下可移动驱动器时系统自动重新指定盘符。

## 现有 ThawSpace 解冻空间

默认情况下，*安装/卸载时保留*复选框处于选中状态，以避免删除在之前的安装过程中创建的 ThawSpace 解冻空间。在有人参与的卸载过程中，无论是否选中了 *安装/卸载时保留*，屏幕始终会显示一个对话框，询问是保留还是删除 ThawSpace 解冻空间。如果通过企业版控制台执行卸载，此选项不显示。

选择 *配置更新期间删除*，删除工作站上所有的现有 ThawSpace 解冻空间，然后在应用此配置时重新创建。现有的 ThawSpace 解冻空间和 ThawSpace 解冻空间中的数据将被删除，并在应用此配置后根据设置创建新的 ThawSpace 解冻空间。

*服从隐藏驱动器的组策略设置*会确保隐藏驱动器的组策略设置与隐藏驱动器的 Deep Freeze 冰点设置不冲突。

隐藏驱动器的组策略设置是用户特定的。如果禁用 *服从隐藏驱动器的组策略设置*选项，则 Deep Freeze 冰点的隐藏驱动器设置为全局性设置。



如果没有隐藏驱动器的组策略，建议停用此选项。

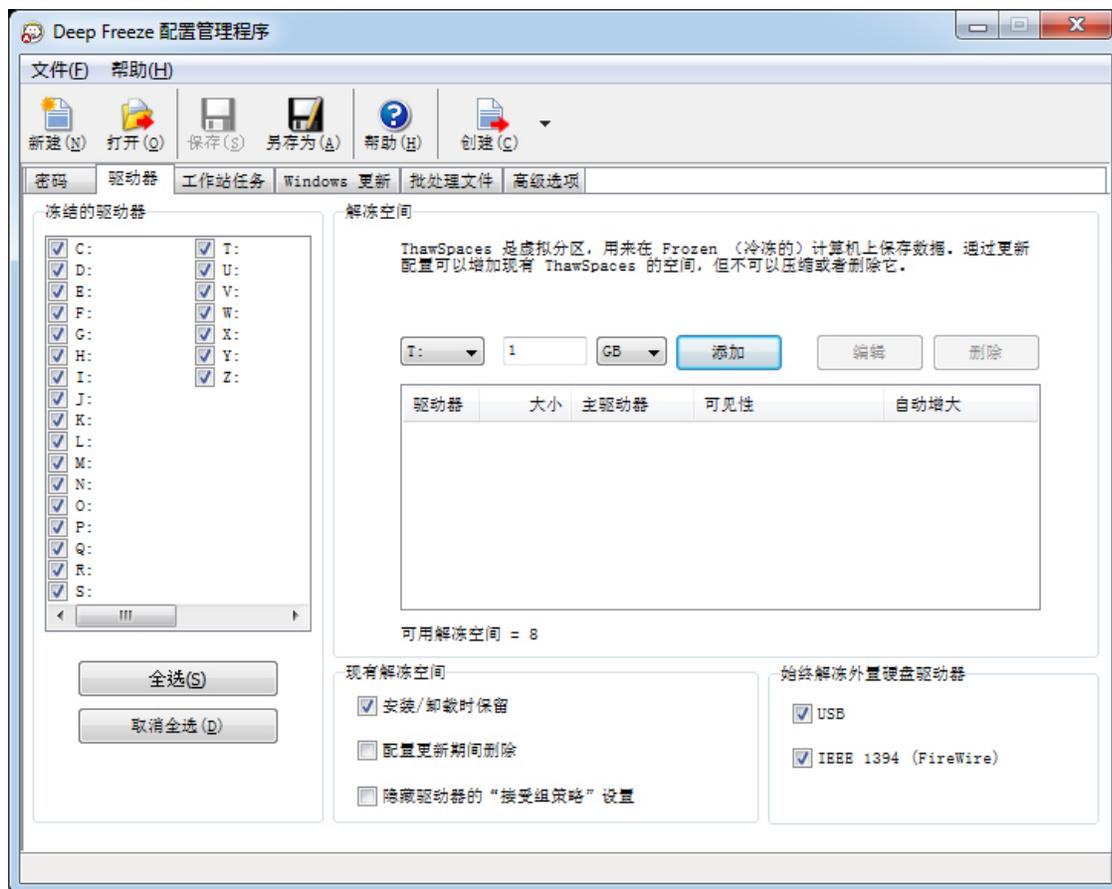


## 始终解冻外置硬盘驱动器

始终解冻外置硬盘驱动器窗格中有两个复选框：*USB* 和 *IEEE 1394 (FireWire)*，默认情况下都处于选中状态。这样可确保 *USB* 或 *IEEE 1394 (FireWire)* 硬盘驱动器始终处于 *Thawed* 状态。

如果 *USB* 和 / 或 *IEEE 1394 (FireWire)* 外置硬盘驱动器对应的复选框没有选中，则该驱动器是处于 *Frozen* 还是 *Thawed* 状态，取决于每个驱动器所挂载的盘符在 *Frozen 驱动器* 区域中的状态。

网络驱动器和可移动媒体设备（软盘，U 盘，CD-RW 等）不受 Deep Freeze 的影响，因而不会处于 *Frozen* 状态。



### 示例

在以上屏幕中，E: 和 F: 在 *Frozen 驱动器* 窗格中处于选中状态。

假设 E: 对应于 *USB* 硬盘驱动器，而 F: 对应于 *IEEE 1394 (FireWire)* 硬盘驱动器。

在 *始终解冻外置硬盘驱动器* 窗格中，*USB* 和 *IEEE 1394 (FireWire)* 复选框被选中，外置硬盘驱动器将处于 *Thawed* 状态。

*USB* 复选框被选中。*IEEE 1394 (FireWire)* 复选框被清除。在此例中，*USB* 驱动器 (D :) 将处于 *Thawed* 状态，而 *IEEE 1394 (FireWire)* 驱动器 (F :) 则会处于 *Frozen* 状态。

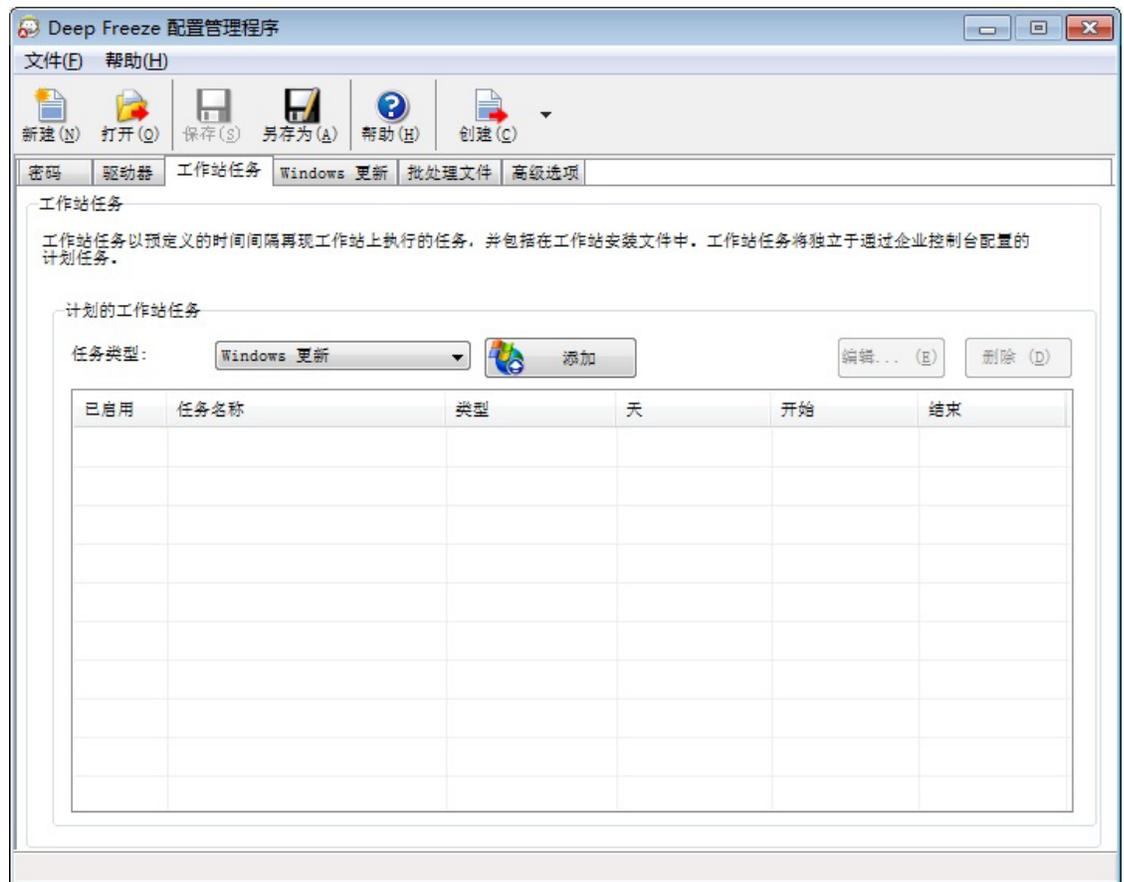


## " 工作站任务 " 选项卡

**工作站任务**选项卡允许您计划在工作站上运行的各项任务。工作站任务一直位于工作站上，即使工作站的网络链接丢失或者不能与 Deep Freeze 控制台进行通信，这些任务也能够运行。工作站任务是工作站安装文件或者 Deep Freeze 配置 (.rdx) 文件的一部分。以下工作站任务是可用的：

- **Windows 更新** – 计划 Windows 更新。您可以在 *Windows 更新*选项卡中配置额外的设置。
- **重启** – 定期重启工作站，使得它们恢复为原始的配置或者删除不想要的数据库。
- **关机** – 每天在指定的时间关闭工作站，以节省电源。
- **空闲时间** – 如果工作站在特定的时段处于空闲状态，则将其关闭或者重启。
- **批处理文件** – 在目标工作站上运行一个批处理文件。您可以在 *批处理文件*选项卡中配置其他设置。
- **Thawed 时期** – 在特定的时期重新启动 Thawed，以手动安装软件，通过第三方工具自动安装软件或者实施其他的永久性配置更改。

以下章节介绍了每个任务的详情。





**工作站任务 vs. 计划任务**：如果企业控制台和目标计算机之间的通信出现故障，则工作站任务仍然会被执行，因为它们一直在目标计算机上。



通过 Deep Freeze 企业控制台中的 *计划任务向导* 计划的任务存在于企业控制台上，而不是目标计算机上。因此，要执行这些计划任务，企业控制台与目标计算机之间必须保持连接状态。有关详细信息，请参阅[计划 Deep Freeze 任务](#)部分。



不能在 *工作站任务* 选项卡中创建重叠的任务。如果新建的任务与现有任务发生重叠，则会显示一条消息。



消息的最长显示时间不能超过 5 分钟。在任意两个任务之间必须至少间隔 5 分钟。



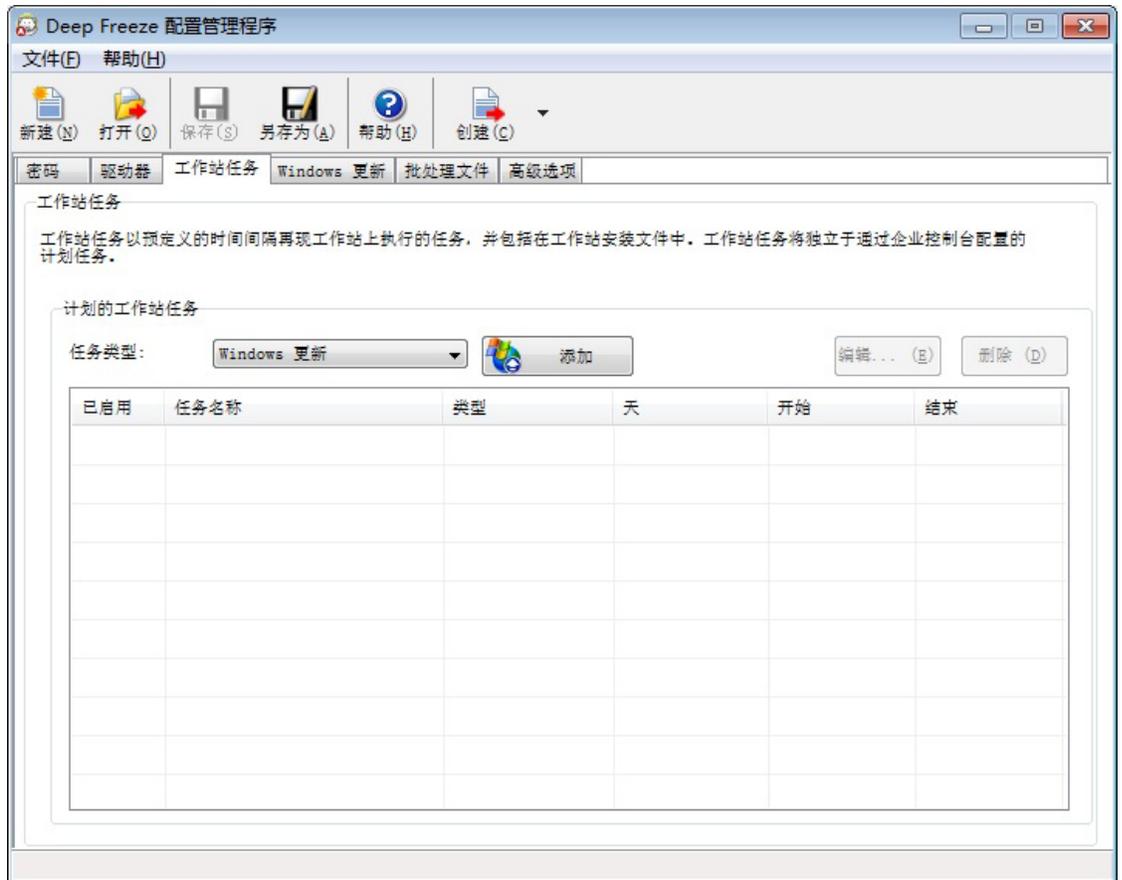
工作站任务仅会在 Deep Freeze 处于 Frozen 状态时触发。

## Windows 更新

工作站上为下载 Windows 更新而计划 Windows 更新任务。即使工作站处于 Frozen 状态，也可以下载 Windows 更新。Windows 更新任务有 *起始时间* 和 *结束时间* 选项。下载 Windows 更新以后，处于 Thawed 状态的工作站将重启并应用该更新。

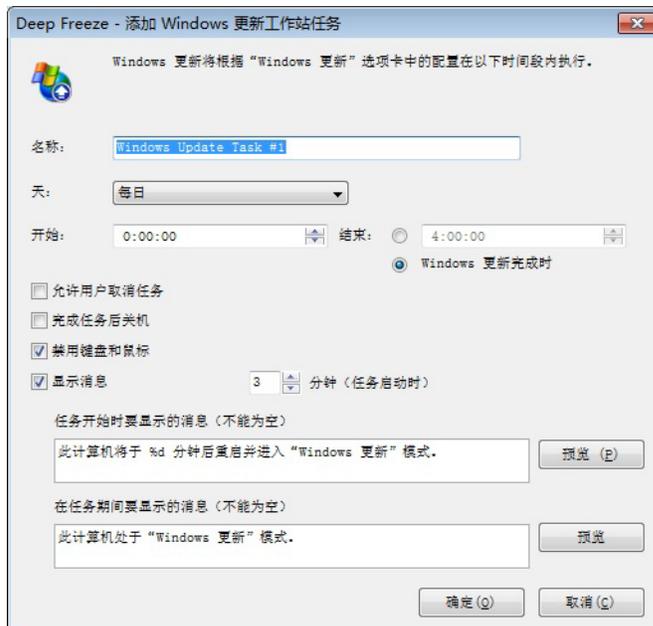


还可通过选择工作站并通过 Deep Freeze 控制台的上下文菜单中的 *运行 Windows 更新* 命令，在工作站上手动应用 Windows 更新。有关详细信息，请参阅[使用控制台管理 Deep Freeze](#)。



要计划 Windows 更新任务，请完成以下步骤：

1. 从任务类型下拉列表中选择 *Windows 更新*，并单击 *添加*。
2. 此时将显示以下选项：





- > 名称 – 指定任务的名称。
- > 天 – 选择日期，或者指定任务在工作日还是周末执行。
- > 开始 – 选择开始时间。
- > 结束 – 选择结束时间。最短时间间隔为 15 分钟。或者，您也可以选择 *Windows 更新完成时*。如果在 6 个小时之内 Windows 更新任务没有完成，则 Deep Freeze 将平稳结束任务。



如果 Windows 更新完成，Windows 更新任务即为结束；如果计算机在任务的计划开始时间处于关机状态，那么如果计算机在计划开始时间后 15 分钟内开机，则会触发计算机的 Windows 更新任务。

例如，当 Windows 更新任务设置为在晚上 11:40 开始时，计算机处于关机状态。如果计算机在晚上 11:40 至 11:55 之间开机，Windows 更新任务将在计算机上自动执行。

- > 允许用户取消任务 – 如果允许用户在任务启动前取消任务，则选中此复选框。
- > 尝试本地唤醒 – 选中此复选框，从而唤醒本地工作站，无需与企业版控制台进行任何通信。



本地唤醒工作站取决于工作站的硬件规格。此选项仅在硬件支持的情况下才生效。

- > 任务完成后关机 – 选中此复选框可在任务完成后关闭计算机。
- > 禁用键盘和鼠标 – 选中此复选框可在执行任务时禁用键盘和鼠标。
- > 显示消息 – 选中此复选框可在任务执行之前或期间在计算机上显示一条消息。指定时间间隔（分钟），并输入将在任务启动之前显示的简要消息。

3. 单击 *确定*。您将被引导至 "Windows 更新" 选项卡以配置其他尚未配置的设置。



此计算机将于 %d 后重启以进行 Windows 更新的消息将于在任务之前显示的消息字段中显示。此消息可以编辑。在该消息的 %d 后添加分钟一词，可在消息中显示分钟。



当计划 Windows 更新任务时，选中 *Windows 更新完成时* 选项或者确保允许足够的时长，以实施所有必需的更新活动。查看 Technet 网站 (<http://technet.microsoft.com/en-us/security/bulletin>) 上的 Microsoft 安全公告，以根据发布的键和安全更新确定适当的时长。



如果您未使用 WSUS，Deep Freeze 冰点 Windows 更新进程将仅应用无用户介入的关键和安全更新，以及 Windows 10 及以上版本的功能更新。如果您使用了 WSUS，则 WSUS 认可的所有更新都将被应用。

如果您未使用 WSUS，则只要有适用于 Windows 10 及以上版本的功能更新，Windows 更新任务总会尝试安装这些更新。您可以推迟安装功能更新，方法是：使用 *Windows 更新* 系统设置的 *高级选项* 下的 *选择何时安装更新*，或者启用本地计算机策略，即使用 *计算机配置* > *管理模板* > *Windows 组件* > *Windows 更新* > *Windows Update for Business* 中的 *选择何时接收预览版本和功能更新*。

或者，为了应用其他可用更新，请访问 Microsoft 更新目录网站 (<http://catalog.update.microsoft.com>)，以获取可以通过 Deep Freeze 批处理文件工作站任务应用的 KB 下载。批处理文件任务也可用于应用其他第三方软件更新。



Deep Freeze *Windows 更新* 选项卡将覆盖 workstation 上的 Windows 更新设置。

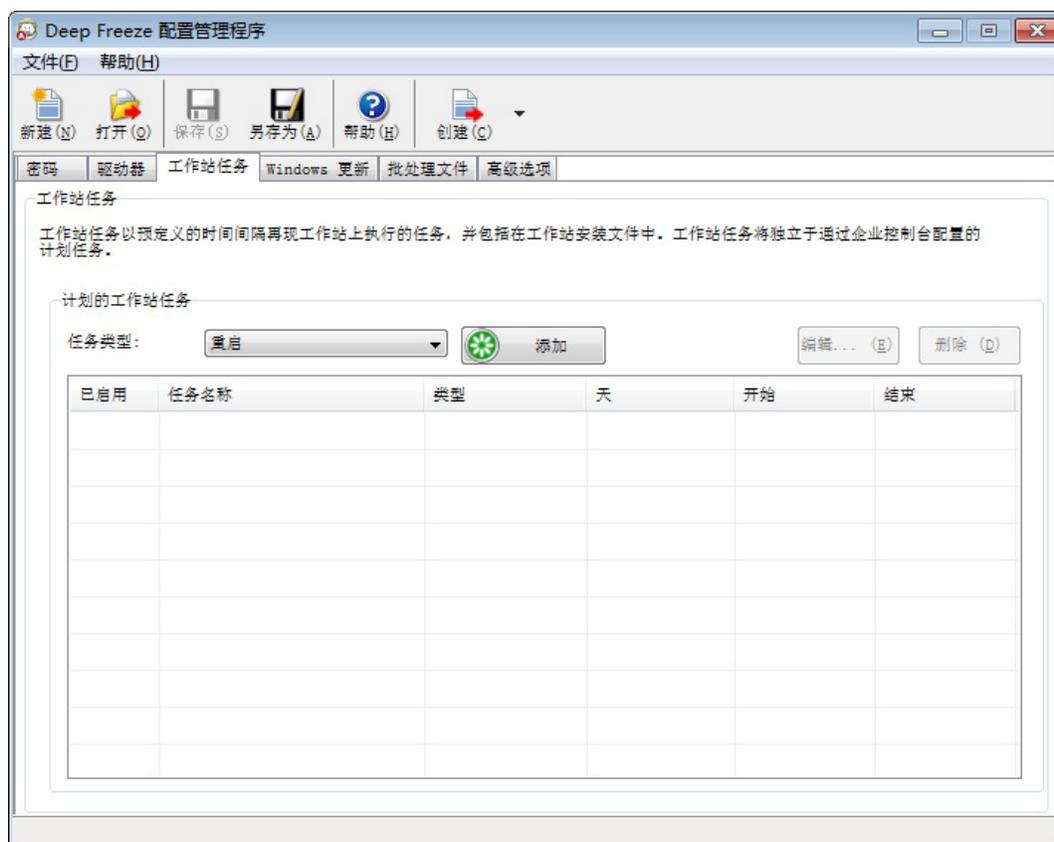
## 示例

以上屏幕中创建了 Windows 更新任务：每天上午 12:00 开始在计算机上运行 Windows 更新，直至 *Windows 更新* 完成时结束。配置该任务后，系统将在 Windows 更新前向用户显示一条消息。键盘和鼠标已禁用。



## 重启

要计划重新启动任务，请完成以下步骤：



1. 从任务类型下拉列表中选择 *重新启动*，并单击 *添加*。
2. 此时将显示以下选项：



- > 名称 – 指定任务的名称。
- > 天 – 选择日期，或者指定任务在工作日还是周末执行。
- > 开始 – 选择开始时间。
- > 允许用户取消任务 – 如果允许用户在任务启动前取消任务，则选中此复选框。
- > 显示消息 – 选中此复选框可在任务启动之前在计算机上显示一条消息。指定时间间隔（分钟），并输入将在任务启动之前显示的简要消息。



### 3. 单击 **确定**。



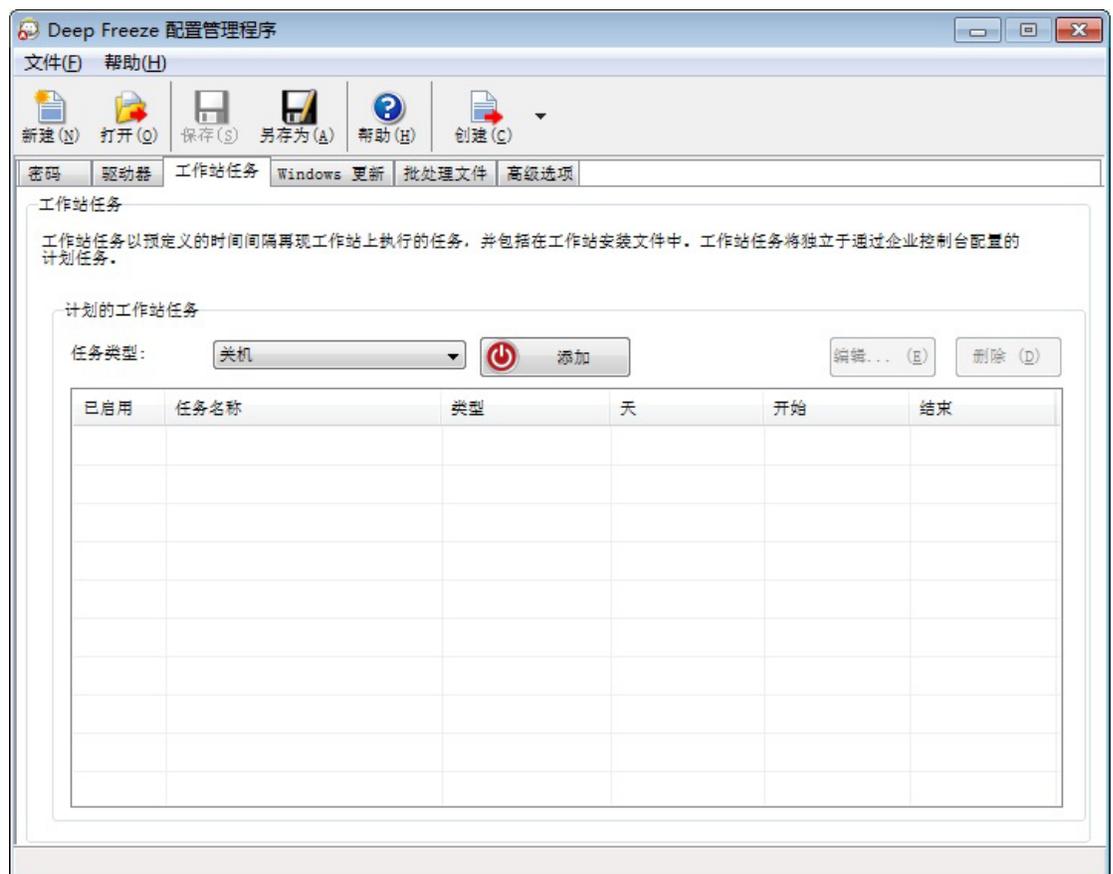
此计算机将于 %d 秒后重启的消息将于在任务之前显示的消息字段中显示。此消息可以编辑。在该消息的 %d 后添加 **分钟** 一词，可在消息中显示分钟。

## 示例

以上屏幕中创建了一个工作站任务：每天上午 12:00 点重新启动计算机。该任务配置为在重启之前 1 分钟向用户显示一条消息。

## 关机

要计划关机任务，请完成以下步骤：



1. 从 **任务类型** 下拉列表中选择 **关机**，并单击 **添加**。



2. 此时将显示以下选项：

- > 名称 – 指定任务的名称。
- > 天 – 选择日期，或者指定任务在工作日还是周末执行。
- > 开始 – 选择开始时间。
- > 允许用户取消任务 – 如果允许用户在任务启动前取消任务，则选中此复选框。
- > 显示消息 – 选中此复选框可在任务启动之前在计算机上显示一条消息。指定时间间隔（分钟），并输入将在任务启动之前显示的简要消息。

3. 单击 *确定*。



消息 *此计算机将于 %d 秒后关机* 将于 *在任务之前显示的消息* 字段中显示。此消息可以编辑。在该消息的 *%d* 后添加 *分钟* 一词，可在消息中显示分钟。

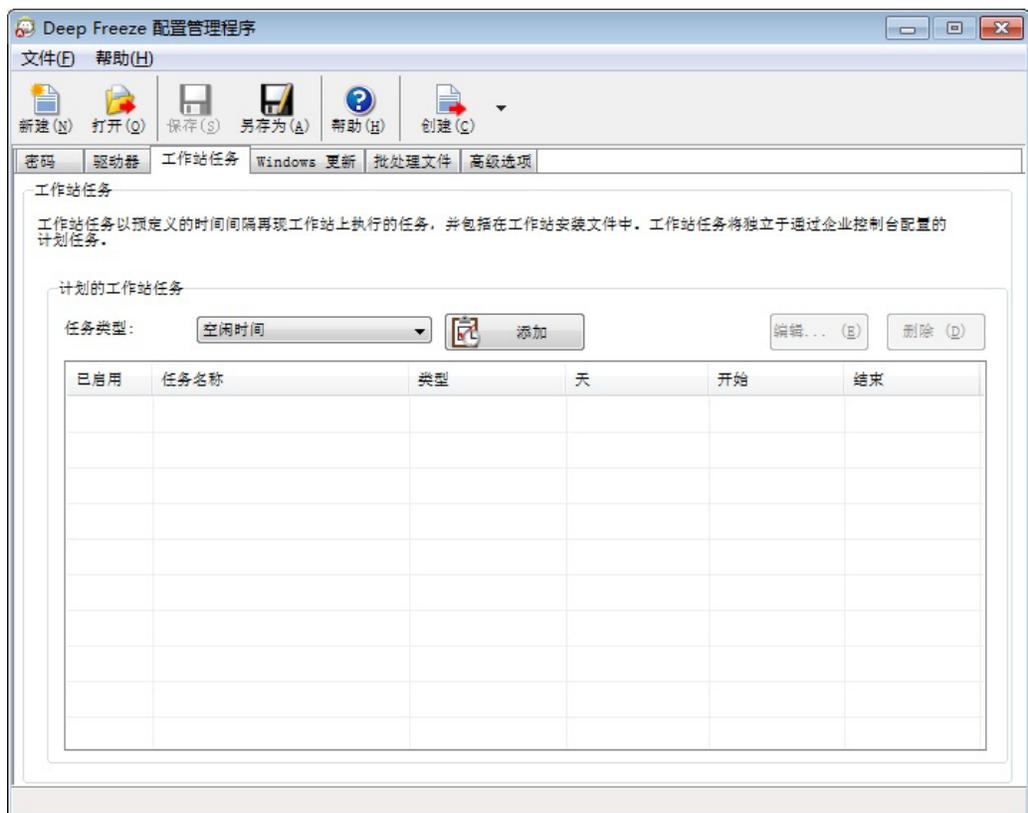
## 示例

以上屏幕中创建了一个关机任务：每天上午 12:00 点关闭计算机。该任务配置为在关机任务执行之前 1 分钟向用户显示一条消息。

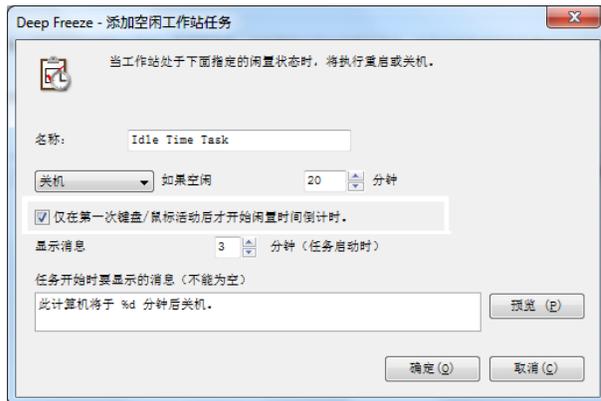


## 空闲时间

要计划空闲时间任务，请完成以下步骤：



1. 从任务类型下拉列表中选择 *空闲时间*，并单击 *添加*。
2. 此时将显示以下选项：



- > 名称 – 指定任务的名称。
- > 重新启动或关机 – 选择 *重新启动*或*关机*，并指定空闲时间（分钟），在此之后必须执行任务。
- > 仅在第一次键盘 / 鼠标活动后才开始闲置时间倒计时 – 此选项仅适用于关机任务。选中此复选框后，计时器只会在第一次键盘 / 鼠标活动后才开始倒计时。例如，如果将闲置时间指定为 20 分钟，并且选择了此选项，则工作站任务将在第一次键盘和鼠标活动后 20 分钟关闭计算机。



- > 显示消息 – 选中此复选框可显示一条消息。指定时间间隔（分钟）并输入一条简要消息。



启动计算机后，只有在首次敲击键盘或使用鼠标后，空闲时间计数器才会被激活。在远程桌面会话期间，控制计算机的空闲时间用于激活该任务。

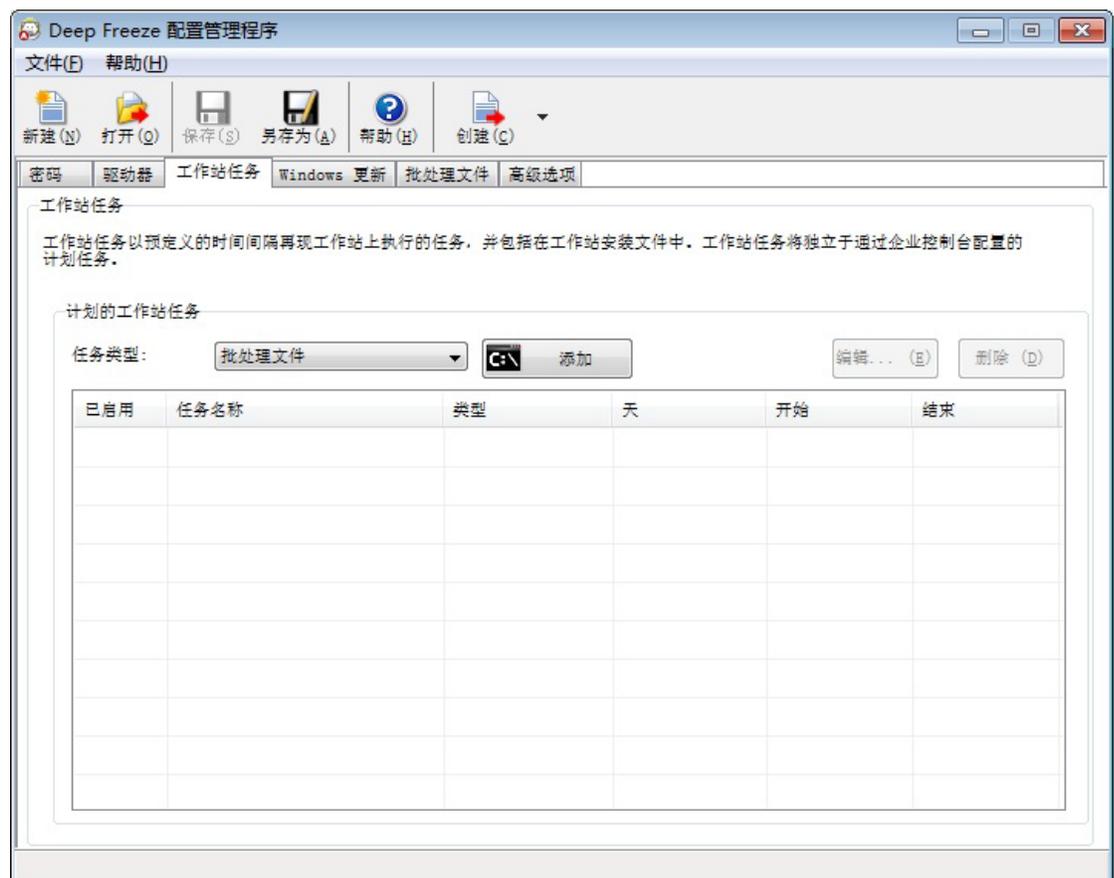
3. 单击 *确定*。

## 示例

在以上屏幕中，空闲时间任务设置为计算机在空闲 1 分钟后 *重新启动*。在空闲时间达到设定值时，将向用户显示一条消息，显示时间持续 1 分钟。除非用户在显示的消息框中取消了该任务，否则计算机将会重新启动。

## 批处理文件

计划批处理文件任务，以便在工作站上执行批处理文件。批处理文件任务有 *起始时间*和 *结束时间*选项。在此期间，批处理文件将在工作站上执行。您必须在 *批处理文件*选项卡上配置额外的设置，以执行批处理文件任务。您可以配置为在批处理文件任务完成之后关闭工作站。在执行批处理文件之后，工作站将重新启动 *Frozen*。





要计划批处理文件任务，请完成以下步骤：

1. 从 **任务类型** 下拉列表中选择 **批处理文件**，并单击 **添加**。
2. 此时将显示以下选项：

Deep Freeze - 添加批处理文件工作站任务

批处理文件任务将根据“批处理文件”选项卡中的配置，在以下时间段内执行。

名称:

天:

开始:  结束:

允许用户取消任务

完成任务后关机

禁用键盘和鼠标

显示消息  分钟 (任务启动时)

任务开始时显示的消息 (不能为空)

在任务期间显示的消息 (不能为空)

- > 名称 – 指定任务的名称。
- > 天 – 选择日期，或者指定任务在工作日还是周末执行。
- > 开始 – 选择开始时间。
- > 结束 – 选择结束时间。最短时间间隔为 15 分钟。
- > 允许用户取消任务 – 如果允许用户在任务启动前取消任务，则选中此复选框。
- > 尝试本地唤醒 – 选中此复选框，从而唤醒本地工作站，无需与企业版控制台进行任何通信。



本地唤醒工作站取决于工作站的硬件规格。此选项仅在硬件支持的情况下才生效。

- > 任务完成后关机 – 选中此复选框可在任务完成后关闭计算机。
- > 禁用键盘和鼠标 – 选中此复选框可在执行任务时禁用键盘和鼠标。
- > 显示消息 – 选中此复选框可在任务执行之前或期间在计算机上显示一条消息。指定时间间隔（分钟），并输入将在任务启动之前显示的简要消息。

3. 单击 **确定**。
4. 转到 **"批处理文件"** 选项卡，以配置其他设置。



此计算机将于 %d 后重启以执行批处理文件的消息将于在任务之前显示的消息字段中显示。此消息可以编辑。在该消息的 %d 后添加分钟一词，可在消息中显示分钟。

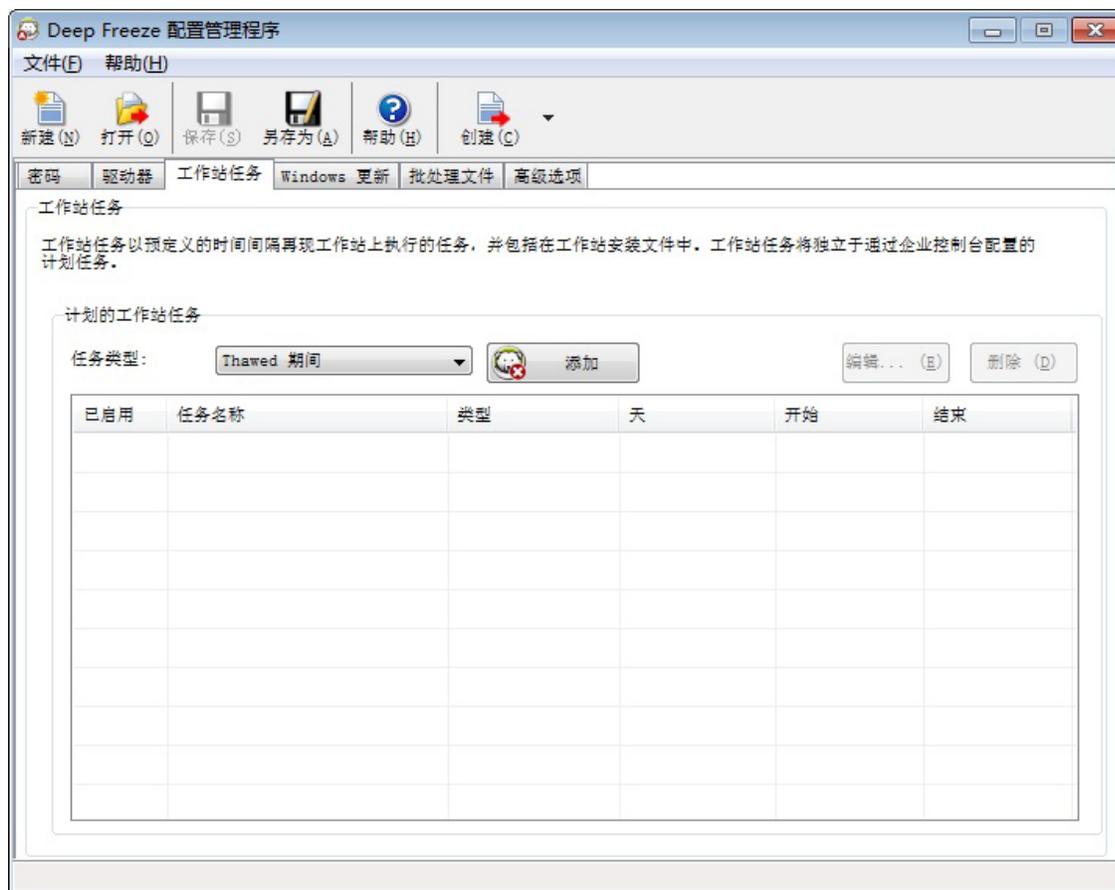


## 示例

以上屏幕中创建了一个批处理文件任务：每天上午 12:00 到 12:15 执行批处理文件。该任务配置为在执行批处理文件之前向用户显示一条消息。键盘和鼠标已禁用。

## Thawed 期间

计划 Thawed 期间任务的目的是重新启动处于 Thawed 状态的工作站。对于一些定期自动更新的应用程序来说，Thawed 期间是非常有用的。对于要计划维护任务以及对计算机实施永久性更改的管理员来说，Thawed 期间同样非常有用。这可能包括安装新软件，更新软件，配置更改和其他维护功能。Thawed 期间有 *开始时间* 和 *结束时间* 选项。



要计划 Thawed 期间任务，请完成以下步骤：

1. 从 *任务类型* 下拉列表中选择 *Thawed 期间*，并单击 *添加*。



## 2. 此时将显示以下选项：

- > 名称 – 指定任务的名称。
- > 天 – 选择日期，或者指定任务在工作日还是周末执行。
- > 开始 – 选择开始时间。
- > 结束 – 选择结束时间。最短时间间隔为 15 分钟。
- > 允许用户取消任务 – 如果允许用户在任务启动前取消任务，则选中此复选框。
- > 尝试本地唤醒 – 选中此复选框，从而唤醒本地工作站，无需与企业版控制台进行任何通信。



本地唤醒工作站取决于工作站的硬件规格。此选项仅在硬件支持的情况下才生效。

- > 任务完成后关机 – 选中此复选框可在任务完成后关闭计算机。
- > 禁用键盘和鼠标 – 选中此复选框可在执行任务时禁用键盘和鼠标。
- > 显示消息 – 选中此复选框可在任务执行之前或期间在计算机上显示一条消息。指定时间间隔（分钟），并输入将在任务启动之前显示的简要消息。

## 3. 单击确定。



此计算机将于 %d 后重启进行维护的消息将于在任务之前显示的消息字段中显示。此消息可以编辑。在该消息的 %d 后添加分钟一词，可在消息中显示分钟。



## 示例

为了能够保护系统，防病毒程序要求定期更新病毒定义。病毒定义可以在 Thawed 期间更新。

以上屏幕中创建了一个 Thawed 期间任务：每天上午 12:00 到 12:15 期间执行。在任务启动之前，用户不能取消该任务。在执行维护后，计算机不会关闭。维护期间，键盘和鼠标会被禁用。该任务配置为在任务启动之前 5 分钟向用户显示一条消息。上午 11:55 在计算机上将显示以下消息：*此计算机将于 5 分钟后重启并进入 Thawed 期间。*

为确保病毒定义得到永久应用，应将防病毒软件的病毒定义更新设置为在 Deep Freeze 成功启动 Thawed 期间任务之后开始，至 Deep Freeze 结束 Thawed 期间任务之前终止。这样可以确保由防病毒程序下载和更新的病毒定义在系统上永久存留，从而使得防病毒软件和 Deep Freeze 能为系统提供全面保护。



**Faronics Anti-Virus**：Faronics Anti-Virus 与 Deep Freeze 配合使用时，无需通过 Thawed 期间任务来更新病毒定义。即使由 Deep Freeze 管理的计算机处于 *Thawed* 状态，Faronics Anti-Virus 也可以更新病毒定义。

**其他防病毒程序**：为了能够保护系统，所有其他防病毒程序都要求安排定期的 Thawed 期间任务来更新病毒定义。请参阅您的防病毒程序用户指南，了解病毒定义是如何下载的。此外，也可以在 Deep Freeze 管理的计算机处于 *Thawed* 状态时手动应用病毒定义。您也可以通过批处理文件任务计划一个 *无用户干预* 任务，用于安装病毒定义。

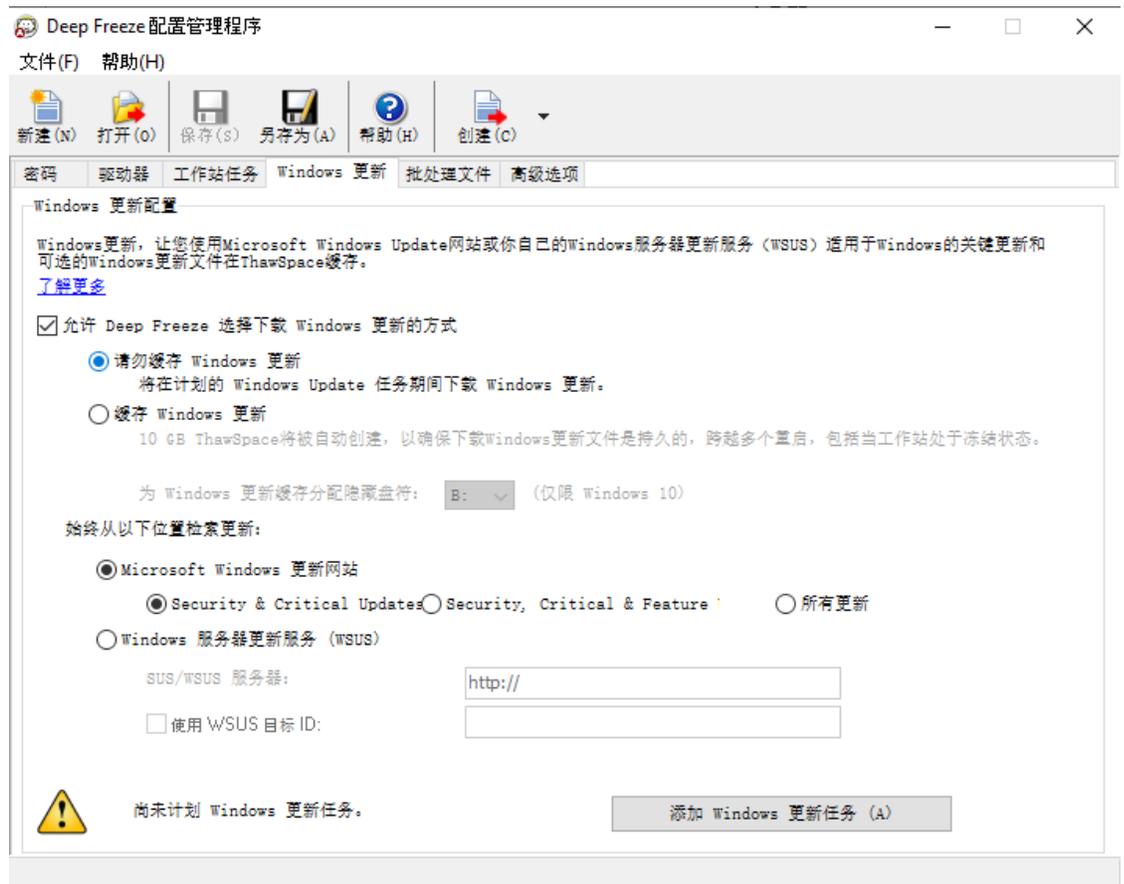


## "Windows 更新" 选项卡

*Windows 更新* 选项卡允许您自定义 Windows 更新设置。当您首次创建一个 Windows 更新任务时，您可以通过给定的选项修改 *Windows 更新* 选项卡中的默认设置。修改默认设置不是强制性的。即使是使用默认设置，Windows 更新也会被执行。*Windows 更新* 选项卡中的设置将应用到所有的 Windows 更新任务中。



Deep Freeze *Windows 更新* 选项卡将覆盖 workstation 上的 Windows 更新设置。



*Windows 更新* 选项卡中的设置可以自定义，如下所示：

允许 Deep Freeze 选择下载 *Windows 更新* 的方式 — 选中复选框，允许 Deep Freeze 选择如何下载 Windows 更新。系统将显示以下选项：

- 选择 Windows 更新下载选项：



- > 请勿缓存 Windows 更新 — 选择这个选项之后，则仅会在 Windows 更新任务执行期间下载 Windows 更新。
- > 缓存 Windows 更新 — 选择这个选项之后，则在工作站处于 Frozen 或 Thawed 状态时下载，并在执行 Windows 更新任务期间安装。选择此选项将创建一个 10 GB 的 ThawSpace，Windows 更新保存在 ThawSpace 中，以确保 Windows 更新文件在多次重启期间保持不变。

适用于 Windows 10 及以上版本：选择 *缓存 Windows 更新* 时，启用驱动器盘符下拉列表。从下拉菜单中选择一个驱动器盘符，分配为用于存储 Windows 更新缓存的隐藏驱动器盘符。为 Windows 更新缓存分配的隐藏驱动器盘符将在 Windows 资源管理器中不可见。



隐藏驱动器盘符在工作站上不可见，且仅适用于 Windows 10 及以上版本。

- 始终从以下位置检索更新：
  - > Microsoft Windows 更新网站 — 选择此选项将从 Microsoft Windows 更新网站直接下载更新。

您可以选择下载 *安全和关键更新 (Security and Critical updates)*、*安全、关键和功能更新 (Security, Critical, and Features updates)* 或 *所有更新*。

    - ~ 安全和关键更新 — 选择此选项可下载关键更新和安全更新。
    - ~ 安全、关键和功能更新 — 选择此选项可下载关键更新、安全更新和功能更新。
    - ~ 所有更新 — 选择此选项将下载所有更新。
  - > Windows 服务器更新服务 (WSUS) – 选择此选项将从 WSUS 服务器下载。指定 *SUS/WSUS 服务器*。此外，选择 *使用 WSUS 目标* 并指定目标。Microsoft SUS 客户端和 SUS/WSUS 服务器可从以下网站下载：<http://www.microsoft.com/wsus>。



系统将为每个独立的工作站创建一个日志文件，并保存在本地工作站上。

Deep Freeze Windows 更新日志文件的默认名称是 *DFWuLogfile.log*，可以通过以下路径找到它：

C:\Program Files\Faronics\Deep Freeze\Install C-[X]\DFWuLogfile.log (32 位系统) 和 C:\Program Files (x86)\Faronics\Deep Freeze\Install C-[X]\DFWuLogfile.log (64 位系统)。

- 您不能更改日志文件的名称或者位置。
- Deep Freeze 日志文件和 Windows 更新日志文件（位于 c:\windows\windowsupdate.log）对于解决您的 Windows 更新问题非常有用。
- X 是一个增量数值，它取决于您在工作站上安装 Deep Freeze 的次数。



请联系 Faronics 技术支持人员，以帮助解决与 *DFWuLogfile.log* 相关的问题（位于 <http://support.faronics.com>）。

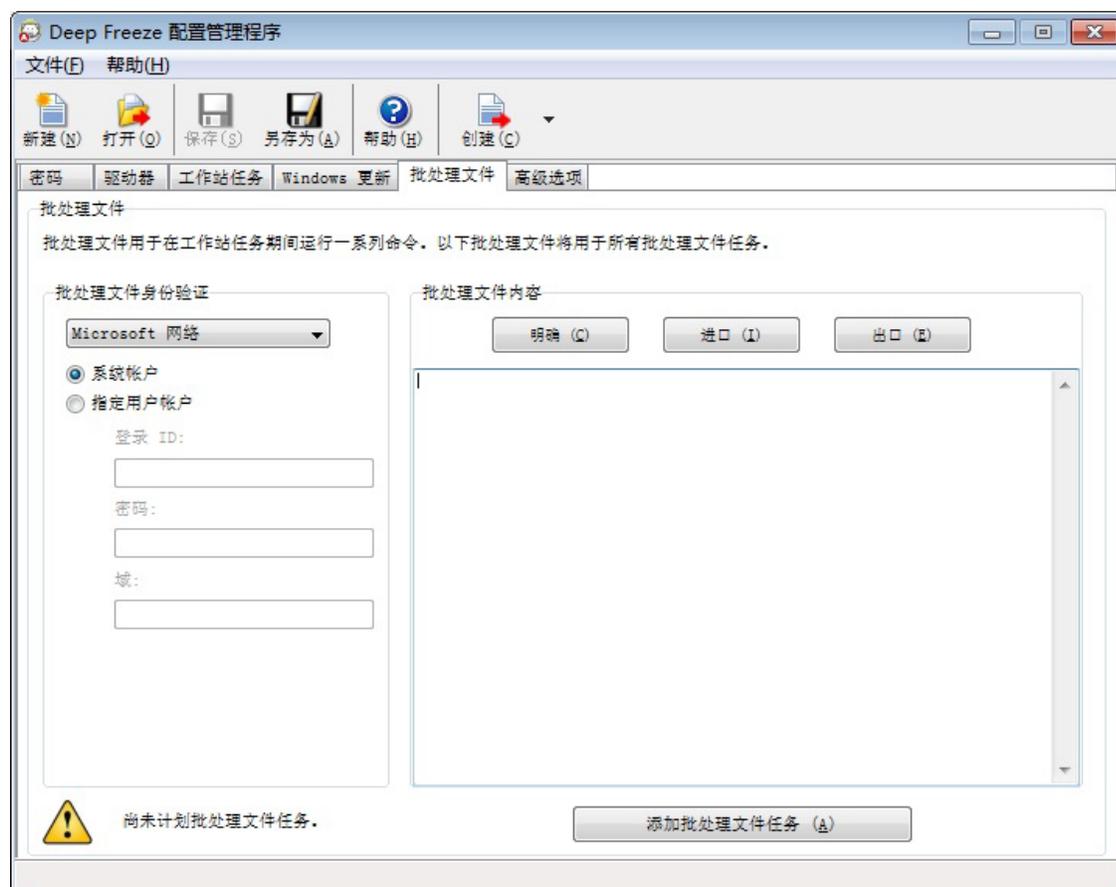
联系 Microsoft 技术支持人员，以解决与 Windows 更新相关的错误。（请查看 <http://support.microsoft.com/kb/906602>）

另请查看 Microsoft KB 902093 *如何解读 Windows 更新日志文件*，位于：<http://support.microsoft.com/kb/902093/> 或者访问 <http://support.microsoft.com>。



## "批处理文件"选项卡

*批处理文件*选项卡允许您自定义批处理文件任务的设置。通过*工作站任务*选项卡计划批处理文件任务时，您必须配置*批处理文件*选项卡中的设置。



请配置以下选项：

- 批处理文件身份验证

选择 Microsoft 网络，并选择要使用的帐户是系统帐户还是指定的用户帐户。如果选择指定的用户帐户，请指定登录 ID，密码和域。对于 Novell 网络，请选择 Novell，并指定登录 ID，密码，树，上下文和服务。



在使用替代的证书之前，必须通过 Microsoft 网络 / 系统帐号认证测试默认的配置。通常，使用这个机器级别的帐号对于完成任务是足够的。如果批处理文件需要访问网络以保证资源安全，则可能需要使用指定的用户帐号。



- 批处理文件内容

输入一个将在批处理文件任务执行期间运行的自定义批处理文件。相同的批处理文件应用于所有的批处理文件任务。运行自定义批处理文件时有以下可用选项：

- > 若要清除当前批处理文件，请单击 *清除*。
- > 若要载入现有文件，请单击 *导入*，然后浏览到文件所在位置。
- > 若要保存字段中的内容，请单击 *导出*，然后浏览到要保存的位置。

批处理文件可以是命令处理程序能够执行的任何命令或命令序列。您可以在第三方脚本引擎支持的前提下运行自定义脚本，方法是在批处理文件中调用脚本，就像在命令行中运行脚本一样。

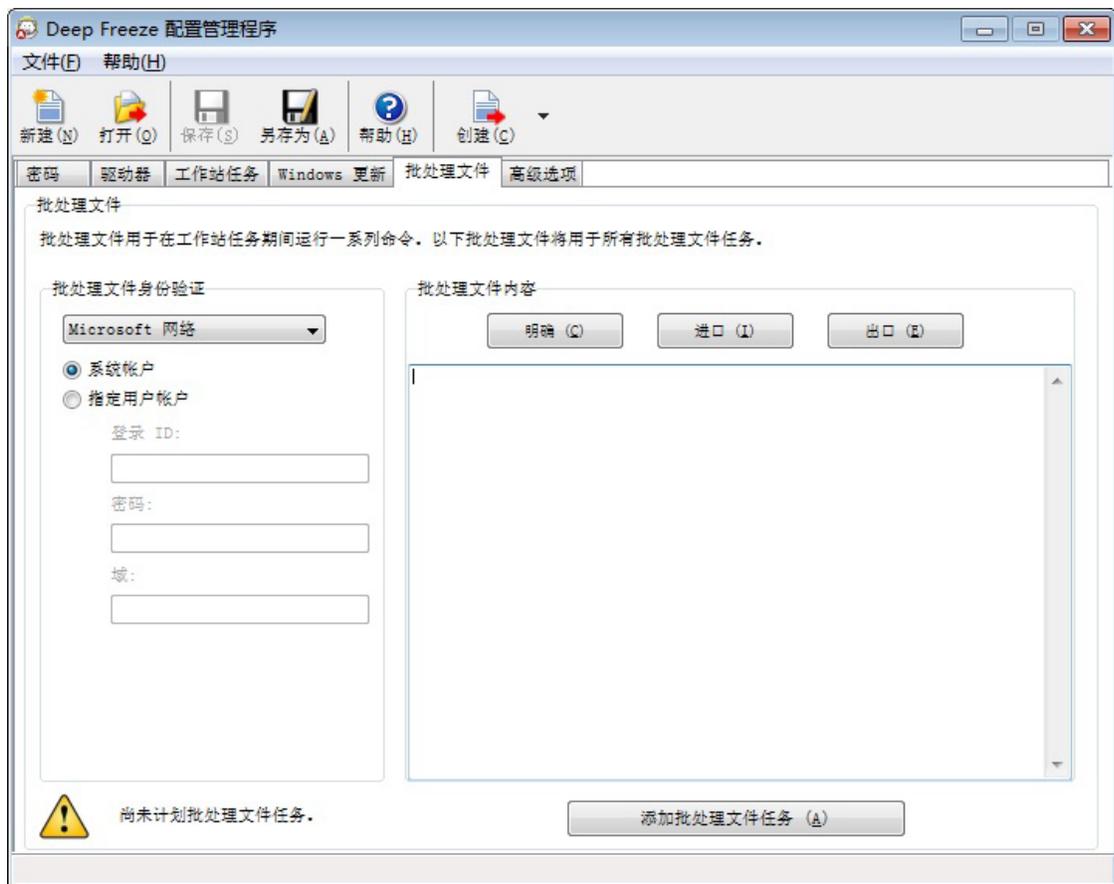


批处理文件允许您使用 VB 脚本，PowerShell 脚本，Ninite 和第三方解决方案。联系您的软件供应商或者参阅您的第三方解决方案用户指南，了解更多包含 *无用户干预* 选项的脚本解决方案。



## "高级选项" 选项卡

高级选项选项卡用于配置网络设置（计算机使用这些设置与控制台进行通信），配置各种安全选项，以及管理许可证密钥。



## 网络

Deep Freeze 企业控制台和安装有 Deep Freeze 的计算机之间可采用两种不同模式进行通信：LAN 模式或 LAN/WAN 模式。

- LAN：选择 LAN 可将 Deep Freeze 配置为在局域网 (LAN) 内通信。LAN 模式是一种自配置模式，只需要一个端口号。默认端口号是 7725。如果该端口号与局域网内的其他程序冲突，可以进行更改。在 LAN 模式下，Deep Freeze 目标计算机和企业控制台将通过 UDP 广播找到彼此。只有在计算机或企业控制台启动后才会发生广播，从而确保目标计算机和控制台之间的通信流量处于较低水平。
- LAN/WAN：选择 LAN/WAN 可将 Deep Freeze 配置为同时在 LAN 和 WAN（广域网）内通信。LAN/WAN 模式可用于 LAN 或 WAN 环境中以及 Internet。此模式需要用到 IP 地址或计算机名称以及端口号，以便在企业控制台和受控计算机之间进行通信。



控制台的标识方法有以下两种：

- 指定控制台 IP，它必须是静态的
- 指定控制台名称，在这种情况下，IP 地址可以是动态的（如果有效 DNS 名称解析可以作为域名基础结构的一部分）。

如果企业控制台位于防火墙或 NAT（网络地址转换）路由器之后，则必须配置该防火墙或路由器，以允许流量到达企业控制台。可能需要使用防火墙的 IP 地址来配置计算机，以便通信流量能够被转发，具体取决于防火墙或路由器。



在 Windows 防火墙中，Deep Freeze 会自动配置所需的异常。不需要手动配置 Windows 防火墙。

有关在具体网络环境中配置和使用 Deep Freeze 的详细信息，请参阅附录 B，或联系技术支持部。

如果使用的端口号不是默认的 7725（注册给 Deep Freeze），则应特别注意，确保不会与网络中运行的其他应用程序发生冲突。另外，应避免使用常见端口（0–1023），并在部署前检查所有已注册端口（1024–49151），以防冲突。



建议使用 49152 以上的未分配范围中的端口。使用端口分段，您可以通过配置工作站以及 Deep Freeze 企业控制台的端口号，隔离一个实验室或者一栋建筑。您可以使用这种方法为特定的工作站组合而非您的整个组织提供管理功能。这些端口需要 UDP 和 TCP 异常。有关详细信息，请参阅示例 3 – 多个端口，远程访问控制台。

若要获得分配给各种应用程序的端口的完整列表，可访问 Internet 编号分配机构网站：<http://www.iana.org/assignments/port-numbers>。

## 高级选项

- 禁用命令行选项 – 默认情况下此选项处于选中状态。清除此复选框允许在使用无提示安装系统时对 Deep Freeze 安装程序进一步自定义。选中此选项可防止在安装期间对预先存在的配置选项进行更改。
- 启用 Deep Freeze 本地策略 – 为提高安全性，Deep Freeze 删除了下列本地权限：调试程序，修改固件以及更改系统时间；清除此选项则可以使用现有权限。
- 允许用户更改时钟 – 选择此选项可允许 Frozen 用户调整系统时钟。在夏令时期间激活这个功能，以允许 Windows 在每个季节自动更新时间。



- 管理安全通道密码 – 安全通道密码是所有 Windows 操作系统具备的一项功能，仅在系统运行于 Windows Server 域环境时才适用。安全通道密码用于实现服务器与工作站之间的安全通信。该密码会根据操作系统设置自动更改。在使用 Deep Freeze 时，新更改的安全通道密码会在系统重启时丢失。管理安全通道密码选项可以避免这一情况的发生。Deep Freeze 的管理安全通道密码功能可以根据 Deep Freeze 的状态 (Frozen 或 Thawed) 来更改组策略的计算机帐户密码的最长使用期限。
  - > 如果要让 Deep Freeze 管理安全通道密码，请选择管理安全通道密码选项。
    - 当工作站处于 Frozen 状态 — 工作站不会更改安全通道密码。这可确保服务器和工作站之间始终保持安全通信。
    - 当工作站处于 Thawed 状态 — 工作站将更改安全通道密码并将该密码与服务器同步。
  - > 如果不想让 Deep Freeze 管理安全通道密码，请不要选择管理安全通道密码选项。
    - 当工作站处于 Frozen 状态：安全通道密码更改并与服务器同步之后，一旦系统重启，该密码将重置为旧密码。
    - 当工作站处于 Thawed 状态：如果工作站在安全通道密码更改的当天处于 Thawed 状态，那么新密码将生效并且工作站将与服务器同步。



Deep Freeze 的管理安全通道密码功能始终会覆盖组策略的计算机帐户密码的最长使用期限。

要使管理安全通道密码功能正常工作，请设置组策略的下述项目：

域控制器：拒绝计算机帐户密码更改设置为未定义

- 注销时重启 – 选中此复选框可使计算机在注销时自动重新启动。如果选中了此选项，则处于 Frozen 状态的计算机在用户注销时将会重新启动。
- 保护 (MBR/GPT) — 如果您希望 Deep Freeze 保护主启动记录，请选中此复选框。如果此选项被选中，则当计算机处于 Frozen 状态时，更改主启动记录将被撤销。
- 显示一次性密码令牌 – 选择此选项后，OTP 一次性密码令牌将显示在 Deep Freeze 冰点工作站的密码输入对话框中。

如果未使用 OTP 一次性密码令牌功能，建议停用此选项。
- 保留 Windows 事件日志 – 选中此复选框，从而保留 Windows 事件日志。因为 Deep Freeze 冰点可以创建 100 MB 的 ThawSpace 解冻空间并存储所有 Windows 事件日志，所以即使计算机处于 Frozen 冻结状态，这些事件日志也不会计算机重启时被删除。一旦达到 100 MB，日志文件将被回收。日志文件包含与应用程序，硬件，系统和安全相关的事件。
- 管理虚拟内存 — 启用此选项，以便应对搭载有限 RAM 的硬件可能遇到性能问题的情况（这种情况十分罕见）。选择此选项后，Deep Freeze 冰点可管理页面文件的大小。



默认情况下，此选项是停用的。如果启用了此选项，系统将调整页面文件的大小以与 RAM 容量相匹配，这样做有助于在工作站上分配更多硬盘驱动器空间。



- 管理本地管理员密码解决方案 - 本地管理员密码解决方案 (LAPS) 是 Windows 的一项功能，可自动管理并备份加入 Active Directory 活动目录或加入 Windows Server Active Directory 活动目录的计算机上的本地管理员帐户密码。

在检测到 LAPS 设置的系统上启用此选项后，Deep Freeze 将停用 LAPS 在 Frozen 冻结状态下更改已配置的本地管理员密码的功能，并允许在 Thawed 解冻状态下更改密码。此功能可确保当前管理员密码仅能在 Thawed 解冻状态下更改，并与 Active Directory 活动目录保持同步。

- 延迟 Frozen 冻结重启来完成 Windows 更新 — 如果在执行 Windows 更新任务期间，Windows 更新的配置或安装正在挂起，则可选择此选项来延迟重启进入 Frozen 冻结状态。如果选择此选项并执行 Windows 更新（通过除 Deep Freeze 冰点以外的方式），重启进入 Frozen 冻结状态将确保所有 Windows 更新安装与配置在重启进入冻结状态之前完成。



如果您选择 *延迟 Frozen 冻结重启来完成 Windows 更新* 并安装 Deep Freeze 冰点，安装程序会检查是否所有 Windows 更新都已完成。如果 Windows 更新未完成，Deep Freeze 冰点安装将无法继续。完成 Windows 更新并再次尝试安装 Deep Freeze 冰点。

如果您停用 *延迟 Frozen 冻结重启来完成 Windows 更新* 并安装 Deep Freeze 冰点，请确保手动完成所有 Windows 更新。由于未完成 Windows 更新，停用此选项可能会导致计算机陷入重启循环。

## 示例

在一个使用 Windows Server 2008 R2 管理多个工作站的 Windows 域环境中，安全通道密码用于实现服务器和工作站之间的安全通信。

请转至 Deep Freeze Enterprise 配置管理程序的 *高级选项* 选项卡，选择 *管理安全通道密码*。创建工作站安装文件并将其部署到工作站。

要使管理安全通道密码功能正常工作，请设置组策略的下列项目：

*域控制器*：拒绝计算机帐户密码更改设置为未定义

*域成员*：禁用计算机帐户密码更改设置为禁用

在工作站处于 Frozen 状态时，安全通道密码不会更改。在工作站处于 Thawed 状态时，安全通道密码在工作站发生更改并与服务器同步。



## 隐蔽模式

- 在系统任务栏上显示 Frozen 图标 – 选择此选项可显示 Frozen 图标，指示安装了 Deep Freeze 且计算机处于 Frozen 状态。
- 在系统任务栏上显示 Thawed 图标 – 选择此选项可显示 Thawed 图标，指示安装了 Deep Freeze 但计算机处于 Thawed 状态。

如果清除了在系统任务栏中显示 Deep Freeze 图标的选项，则必须使用键盘快捷键 CTRL+ALT+SHIFT+F6 来访问登录窗口。

## 许可证

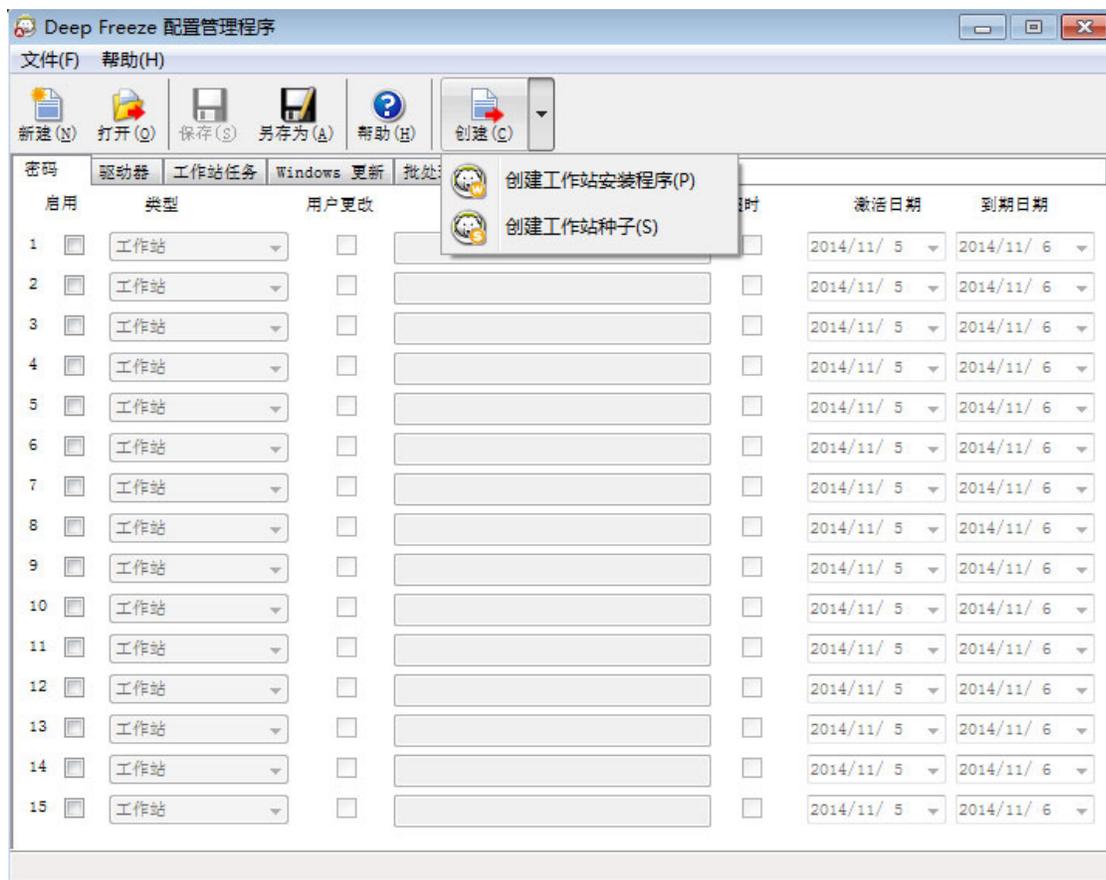
- 许可证密钥 – 单击 *编辑* 并输入许可证密钥。
- 许可证密钥类型 – 显示许可证密钥类型。无论是评估版还是完全版，都会显示此字段。
- 过期日期 – 显示 Deep Freeze 的 *过期日期*。

许可证密钥可通过下列途径更新：

- 通过工作站安装文件更新 – 在配置管理程序中更新许可证密钥，并会生成一个工作站安装文件。现在许可证密钥便包含在该工作站安装文件中。
- 通过企业控制台更新 – 可以直接在企业控制台上更新许可证密钥。许可证密钥在企业控制台上更新之后，将自动在所有连接的计算机上更新。有关直接通过企业控制台更新许可证密钥的详细信息，请参阅 [许可证](#) 部分。
- 手动在每台计算机上更新 – 可手动在各台计算机上更新许可证密钥。有关详细信息，请参阅 ["启动控制" 选项卡](#) 部分。



## 创建工作站安装程序和



若要使用在以前部分中配置的所有选项来创建自定义 Deep Freeze 安装程序文件，请单击配置管理程序工具栏中的 **创建** 按钮，然后选择 **创建工作站安装程序**。



该程序的默认文件名称为 DFWks.exe。我们建议您保留默认的名称，但是在较大型的部署中，您可能希望对其添加与配置相关的后缀：如 DFWks\_10gbThawSpace.exe、DFWks\_NoMaintenance.exe 或者 DFWks\_Wed-5pmUpdates.exe，以协助组织和识别安装程序功能。同样的建议也适用于 Deep Freeze 配置文件 (.rdx)。



此时便可使用此文件在计算机上安装 Deep Freeze。方法如下：

- 有人参与的安装（安装过程中需要用户输入）
- 无提示安装系统 – 安装过程中不为用户显示进度或提供消息。有关无提示安装命令的详细信息，请参阅[无提示安装或卸载](#)。
- 目标安装 – 通过拥有 Seed 或者拥有使用相同 Customization Code 创建的较早版本的 Deep Freeze 的 Deep Freeze 企业控制台。

若要创建 Workstation Seed，请单击配置管理程序工具栏中的 *创建* 按钮，然后选择 *创建 Workstation Seed*。Workstation Seed 是一个小型程序，使管理员能够通过企业控制台远程安装和控制计算机。Workstation Seed 可作为主映像的一部分进行安装，然后通过映像软件进行部署。局域网中安装了 Workstation Seed 的所有计算机都将显示在企业控制台中。此程序的默认文件名为 DFWksSeed.exe。

默认情况下所有文件都保存在 Deep Freeze Enterprise > Install Programs 文件夹。如果需要，可选择其他保存位置，也可以更改文件名。要将另一个位置设置为默认位置，请选择安装程序和工作站种子的所需保存位置，并单击 *保存*。出现提示时，勾选 *将此文件夹设置为默认保存位置* 复选框。单击 *确定*。

如果您要创建多个自定义安装文件，建议采用一种命名规范。



可以创建 DFwks.exe、DFwksseed.exe 和 deprfz.rdx 文件，并且交替部署至任何使用相同 Customization Code 的 Deep Freeze 计算机上。Deep Freeze Seed 可以用作模板 / 占位符，以确保您的基本元素，如密码、网络配置或者标准化工作站任务始终保持一致。Seed 将不会运用任何配置设置，但是会将其保留在文件中。若要将此文件仅用作一个模板，请使用配置管理程序打开 DFwksseed.exe 文件，并进行任何必要的修改。接下来，若要创建工作站安装文件，请单击 *创建* > *创建工作站安装文件*。



出于安全的原因，建议在较大型环境中限制配置管理程序的使用。为达到此目的，可以启用 Deep Freeze 管理程序的密码保护功能，或者移除 c:\program files\farionics\Deep Freeze Enterprise 文件夹中的 DFAdmin.exe，使其变为不可用。此文件将移至域管理程序的工作台，并从通用的 Deep Freeze 企业控制台中删除。若要恢复它，可以从安装相同版本的另外一个程序将其复制并使用 OTP 密码进行授权，或者重新安装或升级使用相同 Customization Code 的 Deep Freeze Enterprise。





# 使用 Deep Freeze 企业控制台

本章介绍如何使用 Deep Freeze 企业控制台。

## 主题

---

- [Deep Freeze 配置](#)
- [配置生成器](#)
- [Deep Freeze 企业控制台](#)
- [查看列](#)
- [基于状态的选择](#)
- [管理控制台与工作站之间的通信](#)
- [远程控制台](#)
- [连接到远程控制台](#)
- [使用控制台管理 Deep Freeze](#)
- [许可证](#)
- [报告](#)
- [标签](#)
- [注释](#)
- [计划 Deep Freeze 任务](#)
- [为计划的任务分配计算机](#)
- [管理网络和组](#)
- [历史记录](#)
- [将计算机添加到组](#)
- [配置自定义操作](#)
- [控制台自定义程序](#)
- [关闭 Deep Freeze 企业控制台](#)
- [在工作站上安装 Deep Freeze](#)
- [通过控制台在工作站上卸载 Deep Freeze](#)
- [无提示安装或卸载](#)
- [检查更新](#)

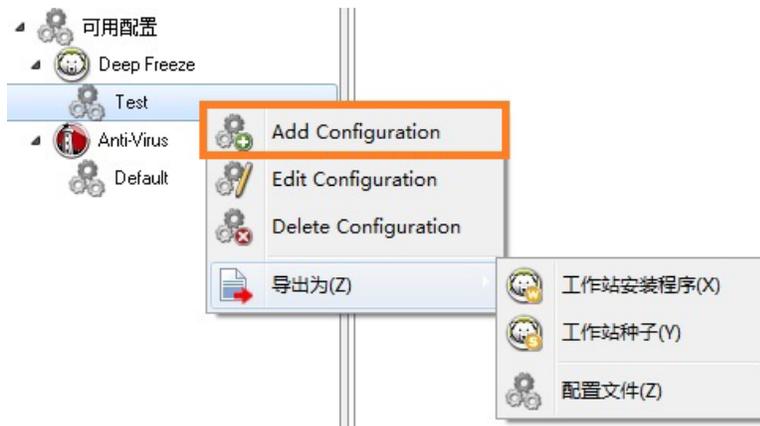


## Deep Freeze 配置

Deep Freeze 配置是一组定义 Deep Freeze 在工作站上的行为的设置，可以通过 Deep Freeze 控制台创建和应用。

要创建 Deep Freeze 配置，请完成以下步骤：

1. 启动 Deep Freeze 控制台。
2. 转至 *网络和组 > 可用配置 > Deep Freeze*。
3. 右键单击并选择 *创建新配置*。



4. 按照[使用 Deep Freeze Enterprise 配置管理程序](#)中所述，选择或指定每个选项卡上的设置。
5. 指定配置名称并单击 *确定*。
6. 或者，从下拉列表中选择 *导出为 > 工作站种子* 或者 *导出为 > 工作站安装程序* 以导出配置。
7. 单击 *确定*。

## 应用 Deep Freeze 配置

配置创建后，可应用到多个工作站。

要应用 Deep Freeze 配置，请完成以下步骤：

1. 转至 *工作站窗格*。
2. 选择一个或多个工作站。
3. 右键单击并依次选择 *更新配置 > Deep Freeze > [配置名称]*。

该配置将应用至所选工作站。



如果更改了密码，工作站任务或注销时重启的 Deep Freeze 冰点配置并应用了此配置，那么这些设置将会即时应用。

一旦在创建安装文件时选择了配置更新期间删除选项，那么现有 ThawSpace 解冻空间和 ThawSpace 解冻空间中的数据将被删除，并在应用此配置后根据设置创建新的 ThawSpace 解冻空间。

所有其他设置都需要重启才能使设置生效。禁用命令行更改不能通过应用配置更改来修改。

## 编辑 Deep Freeze 配置

要编辑 Deep Freeze 配置，请完成以下步骤：

1. 转至企业版控制台中的 *网络和组* 窗格。
2. 选择 *可用配置* > *Deep Freeze* > [配置名称]。
3. 右键单击所选配置，然后选择 *编辑所选配置*。
4. 根据需要编辑设置。
5. 单击 *确定*。

## 删除 Deep Freeze 配置

要删除 Deep Freeze 配置，请完成以下步骤：

1. 转至企业版控制台中的 *网络和组* 窗格。
2. 选择 *可用配置* > *Deep Freeze* > [配置名称]。
3. 右键单击所选配置，然后选择 *删除所选配置*。
4. 单击 *确定*。

## 导出 Deep Freeze 配置

要导出 Deep Freeze 配置，请完成以下步骤：

1. 转至企业版控制台中的 *网络和组* 窗格。
2. 选择 *可用配置* > *Deep Freeze* > [配置名称]。
3. 右键单击所选配置，然后选择 *导出为*。有如下三种选择：
  - > 选择工作站安装程序。指定名称并单击 *保存*。
  - > 选择工作站种子。指定名称并单击 *保存*。
  - > 选择配置文件。指定名称并单击 *保存*。



## 配置生成器

Deep Freeze 冰点控制台提供一种名为配置生成器的工具，可根据 CSV 文件中指定的参数自动创建 Deep Freeze 冰点安装或 Deep Freeze 冰点配置文件。可对提供的 CSV 示例文件进行编辑，使条目数不受限。CSV 文件的设置参数与 Deep Freeze Enterprise 冰点配置管理程序的设置参数相同。CSV 文件的列标题代表特定设置，行则代表单个 Deep Freeze 冰点配置或 Deep Freeze 冰点安装文件的条目。

使用配置生成器完成下列步骤以生成多个 Deep Freeze 冰点安装文件：

1. 启动 Deep Freeze 冰点控制台。转至 **工具** > **配置生成器**。或者，您也可以从 Deep Freeze Enterprise 冰点配置管理程序的 **文件** > **配置生成器** 启动。



2. 在配置生成器中单击 **浏览**。
3. 选择配置文件 (.csv)。
4. 单击 **生成**。

Deep Freeze 冰点安装文件或 Deep Freeze 冰点配置文件创建完成。



如果您第一次使用配置生成器，单击 **CSV 示例** 以下载文件模板。您可以使用生成 Deep Freeze 冰点安装或 Deep Freeze 冰点配置文件所需的值来更新 CSV 示例文件。建议使用更具描述性的名称保存文件。



## 从命令行使用配置生成器

您也可以从命令行生成 Deep Freeze 冰点安装或 Deep Freeze 冰点配置文件。从 Deep Freeze 冰点安装位置启动命令行，提供下列参数，然后按 Enter 键：

32 位系统：

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

64 位系统：

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

Deep Freeze 冰点安装或 Deep Freeze 冰点配置文件在 CSV 文件指定的位置生成并保存。

如果要在同步模式下运行该命令，请按如下所示指定命令：

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

## 配置文件参数

下表介绍了配置文件中的参数：

- 请勿修改列标题。修改标题将导致 Deep Freeze 冰点忽略特定的单元值。系统将使用 Deep Freeze Enterprise 冰点配置管理程序的默认值。
- 为包含多个条目的参数添加多个列。例如，密码、ThawSpace 解冻空间等可以有多个列：*Password1Enable*、*Password2Enable*、*ThawSpace1Drive*、*ThawSpace2Drive*。
- 保留条目空白或删除一整列将使用 Deep Freeze 冰点配置管理程序的默认值。如果必填字段没有值或者代表必填字段的列被删除，Deep Freeze 冰点安装或 Deep Freeze Enterprise 冰点配置文件将不会生成。错误消息将生成并存储于日志文件。单击配置生成器中的 [查看失败的配置的日志文件链接](#)，查看错误日志。
- 请勿将逗号 (,) 用于参数名称或值。
- 参数名称和值不区分大小写。
- 需填日期的字段请使用 yyyy/mm/dd 格式。
- 需填时间的字段请使用 hh:mm:ss (24 小时) 格式。



列 / 参数	描述
FileName	指定文件名以及文件的保存路径。
rdx	指定 1：生成 Deep Freeze 冰点配置文件。指定 0：不生成 Deep Freeze 冰点配置文件。
exe	指定 1：生成 Deep Freeze 冰点安装文件。指定 0：不生成 Deep Freeze 冰点安装文件。
Password1Enable	指定 1：启用密码 1。指定 0：停用密码 1。
Password1Type	指定工作站或命令行。
Password1UserChange	指定 1：允许用户更改。指定 0：不允许用户更改。
Password1	指定密码。
Password1TimeOut	指定 1：密码将超时。指定 0：密码不会超时。
Password1Activation	指定密码激活日期。
Password1Expiration	指定密码到期日期。
FrozenDrives	指定单行的 Frozen 冻结驱动器盘符（如 CDEF）。
ThawSpace1Drive	指定 ThawSpace 解冻空间驱动器盘符。
ThawSpace1Size	指定 ThawSpace 解冻空间大小。
ThawSpace1SizeUnit	指定单位为 MB 或 GB。
ThawSpace1HostDrive	指定 ThawSpace 解冻空间主驱动器盘符。
ThawSpace1Visibility	指定 1：ThawSpace 解冻空间可见。指定 0：ThawSpace 解冻空间不可见。
RetainExistingThawSpace	指定 1：保留 ThawSpace 解冻空间。指定 0：删除 ThawSpace 解冻空间。
HonorGPSettings	指定 1：启用服从组策略设置。指定 0：停用服从组策略设置。
USB	指定 1：保持 USB 外置驱动器为 Thawed 解冻状态。指定 0：保持 USB 外置驱动器为 Frozen 冻结状态。
FireWire	指定 1：保持 FireWire 外置驱动器为 Thawed 解冻状态。指定 0：保持 FireWire 外置驱动器为 Frozen 冻结状态。
LAN_WAN	指定 1：工作站与 Deep Freeze 冰点控制台之间的通信为 LAN/WAN 模式。指定 0：工作站与 Deep Freeze 冰点控制台之间的通信非 LAN/WAN 模式。



列 / 参数	描述
UseDefaultPort	指定 1：使用默认端口 7725。指定 0：不使用默认端口。
Port	指定端口。
ConsoleIP_NAME	指定控制台 IP（必须为静态）或名称。
DisableCMD	指定 1：停用命令行。指定 0：启用命令行。
EnableLocalPolicies	指定 1：启用 Deep Freeze 冰点本地策略。为提高安全性，Deep Freeze 冰点删除了下列本地权限：调试程序，修改固件以及更改系统时间。指定 0：停用 Deep Freeze 冰点本地策略。
AllowChangeClock	指定 1：允许 Frozen 冻结用户调整系统时钟。指定 0：不允许 Frozen 冻结用户调整系统时钟。
ManageSCP	指定 1：管理安全通道密码。指定 0：停用安全通道密码。
RestartOnLogoff	指定 1：注销时重启工作站。指定 0：停用注销时重启工作站。
ProtectMBR	指定 1：保护主引导记录。指定 0：Deep Freeze 冰点不保护主引导记录。
ShowFrozenIcon	指定 1：在系统任务栏中显示 Frozen 冻结图标。指定 0：在系统任务栏中隐藏 Frozen 冻结图标。
ShowThawedIcon	指定 1：在系统任务栏中显示 Thawed 解冻图标。指定 0：在系统任务栏中隐藏 Thawed 解冻图标。
DelayFrozenReboot	指定 1：延迟 Frozen 冻结重启以完成 Windows 更新。指定 0：停用 <i>延迟 Frozen 冻结重启以完成 Windows 更新</i> 选项。
BatchAuthentication	指定 1：允许批处理身份验证。指定 0：不允许批处理身份验证。
UserAccount	指定 1：使用用户账户。指定 0：使用系统账户。
LoginID	指定登录 ID。
Password	指定密码。
Domain	指定域。
Tree	指定树。
Context	指定上下文。



列 / 参数	描述
Server	指定服务器名称。
BatchFile	指定批处理文件的内容。仅支持 1 行。
AllowWUDownload	指定 1：允许 Deep Freeze 冰点选择下载 Windows 更新的方式。指定 0：不允许 Deep Freeze 冰点选择下载 Windows 更新的方式。
CacheWU	指定 1：缓存 Windows 更新。指定 0：不缓存 Windows 更新。
WSUS	指定 1：使用 WSUS 更新 Windows。指定 0：不使用 WSUS 更新 Windows。
UseWSUSTarget	指定 1：使用 WSUS 目标。指定 0：不使用 WSUS 目标。
WSUSServer	指定 WSUS 的 URL。
WSUSTarget	指定 WSUS 目标。
Task1Enabled	指定 1：启用工作站任务。指定 0：停用工作站任务。
Task1Type	指定任务类型 – 重启，关闭，批处理文件或 Windows 更新。
Task1Name	指定任务名称。
Task1Day	指定日期。
Task1Start	指定开始时间。
Task1End	指定结束时间。
Task1AllowCancel	指定 1：允许用户取消任务。指定 0：不允许用户取消任务。
Task1ShutdownAfterTask	指定 1：在任务完成后关闭工作站。指定 0：在任务完成后 Deep Freeze 冰点不关闭工作站。
Task1DisableInput	指定 1：停用键盘和鼠标。指定 0：不停用键盘和鼠标。
Task1ShowMessageFor	指定消息显示的分钟数。
Task1StartMessage	当任务开始时指定消息。仅支持 1 行。
Task1DuringMessage	在任务执行过程中指定消息。仅支持 1 行。



## Deep Freeze 企业控制台

---

Deep Freeze 企业控制台可显示网络中所有冻结、解冻和目标计算机的状态，使管理员能够在这些计算机上执行具体的任务。通过选择性或群组性的报告可获得详细的状态信息。

要搜索计算机，请点击控制台右上角显示的搜索栏并输入搜索字符串。执行搜索时可以使用通配符。该功能会搜索所有列。

企业控制台使管理员能够远程执行以下任务：

- 直接实施针对性计算机安装
- 选择性地冻结、解冻或解冻并锁定一台或多台计算机
- 锁定或解锁所选的计算机
- 重启或关闭计算机
- 停止计划维护
- 启动配备有远程唤醒网卡的计算机
- 更新 Deep Freeze 软件
- 直接通过控制台计划任务
- 向计算机发送消息
- 从 Active Directory 导入群组 and 容器
- 生成一次性密码
- 计划操作
- 自定义 Deep Freeze 企业控制台
- 更新许可证密钥
- 登录用户
- 为计算机添加标签或注释
- 查看并导出有关计算机性能、当前状态和历史记录的报告

企业控制台只能将计算机从关闭状态唤醒，前提是计算机已正确配置为在收到网络唤醒包时启动。

### 启动 Deep Freeze 企业控制台

企业控制台随 Deep Freeze Enterprise 配置管理程序一起安装。从 *开始* 菜单中进行如下选择以打开控制台：

*开始* > *所有程序* > *Faronics* > *Deep Freeze Enterprise* > *Deep Freeze 控制台*



## 激活 Deep Freeze 企业控制台

作为 Deep Freeze Enterprise 的安全功能，OTP 功能可防止未经授权使用 Deep Freeze 企业控制台。当 DFConsole.exe 文件复制到新计算机上时，必须激活控制台。在新计算机上首次运行该控制台时，屏幕将出现一个显示 OTP 令牌的对话框。

网络管理员需要在配置管理程序的 OTP 生成系统中输入此令牌，然后将生成 OTP。将该 OTP 输入对话框后，控制台便可运行。

安装了企业控制台的计算机上不能安装有工作站种子（使用相同端口）或完整的 Deep Freeze。

## 状态图标

企业控制台会根据所选视图，在计算机名称的旁边或上方通过以下图标显示局域网中计算机的状态：

经典外观	现代外观	定义
		目标：安装有 Deep Freeze 工作站种子而没有安装 Deep Freeze 的计算机；Deep Freeze 只能远程安装到带有此图标的计算机
		安装有 Deep Freeze 并处于冻结状态的计算机
		安装有 Deep Freeze 并处于解冻状态的计算机
		安装有 Deep Freeze 并处于解冻但锁定状态的计算机
		当前已关闭的计算机
		当前处于维护模式的计算机
		当前与控制台中断通信的计算机



经典外观

现代外观

定义



锁定的计算机



Thawed 解冻时间长于 Thawed 解冻警报设置中定义时间的计算机



Thawed 解冻锁定时间长于 Thawed 解冻警报设置中定义时间的计算机



## 查看列

---

Deep Freeze Enterprise 冰点企业版控制台提供指定在 *工作站* 窗格中显示的列的功能。要显示所需列，请完成以下步骤：

1. 转至 *视图 > 列*。
2. 选择以下列以显示：
  - > 配置
  - > 配置日期
  - > 过期日期
  - > 安装文件
  - > IP 地址
  - > 许可证状态
  - > 登录名称
  - > MAC 地址
  - > 注释
  - > 操作系统
  - > 端口
  - > 状态
  - > 标签
  - > Thawed 解冻时长
  - > 可用 ThawSpace 解冻空间 (GB)
  - > 版本
  - > 工作组
  - > 工作站
  - > Anti-Virus 防病毒

## 基于状态的选择

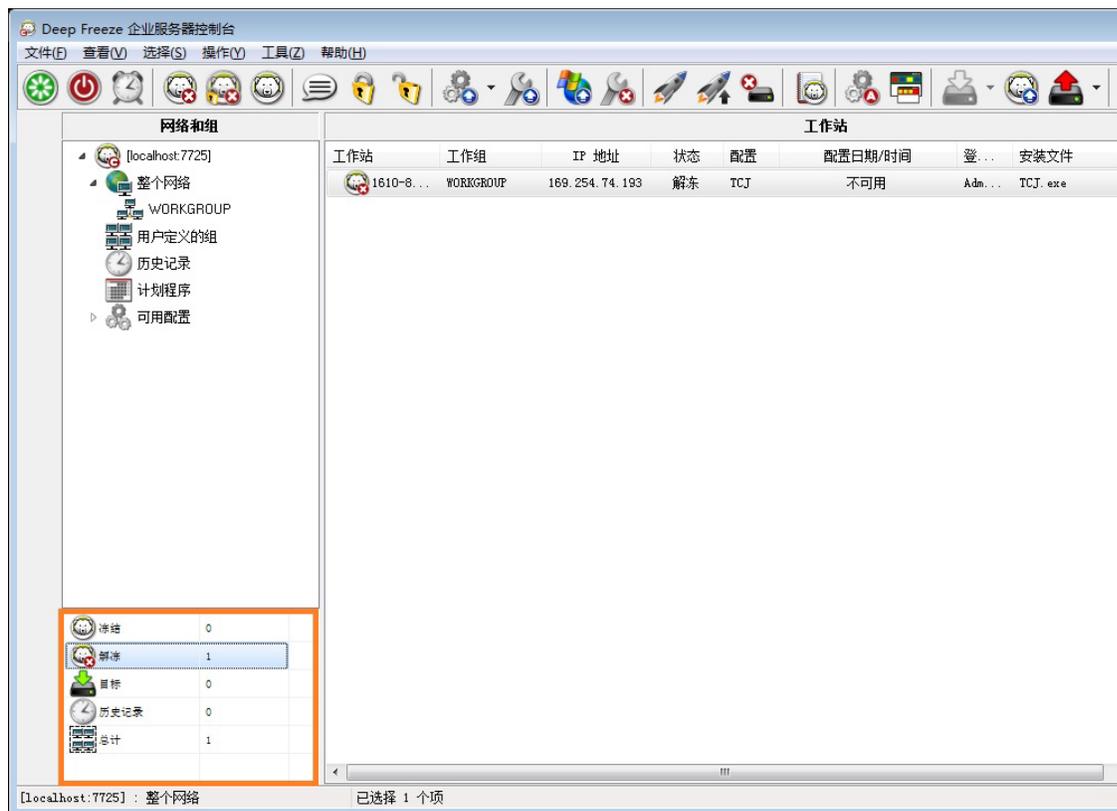
您可基于托管工作站上的 Deep Freeze 冰点状态选择工作站。通过 Deep Freeze Enterprise 冰点企业版控制台中的 *选择* 菜单可基于状态进行选择。*选择* 菜单具有以下选项：

- 选择所有冻结工作站 – 选择处于冻结状态的工作站。也会选择冻结并锁定的工作站。
- 选择所有解冻工作站 – 选择处于解冻状态的工作站。也会选择解冻并锁定的工作站。
- 选择所有目标工作站 – 选择可安装 Deep Freeze 冰点的所有目标计算机。
- 全选 – 选择所有工作站。

状态窗格也会提供以下选择选项：

- 冻结 – 选择处于冻结状态的工作站。也会选择冻结并锁定的工作站。
- 解冻 – 选择处于解冻状态的工作站。也会选择解冻并锁定的工作站。
- 目标 – 选择可安装 Deep Freeze 冰点的所有目标计算机。
- 历史记录 – 显示历史记录。
- 全部 – 选择所有工作站。

也可使用 Deep Freeze Enterprise 冰点企业版控制台上的状态窗格选择和显示特殊状态的工作站计数。





## 管理控制台与工作站之间的通信

控制台到工作站和控制台到控制台的连接有两种方式：

1. 本地连接 – 此类连接只能由承载这些连接的企业控制台访问。
2. 支持远程控制的连接 – 此类连接可由承载连接的控制台访问，也可由远程连接的其他控制台访问。



Deep Freeze 6.5 服务器服务不会自动更新 Deep Freeze 6.4 或更低版本的服务器服务。这两个服务可以安装在同一台计算机上，但是一次只能运行一个服务。

计算机与控制台之间的连接可能会因为以下任一原因中断：

- 计算机被手动关闭，或者没有警告便关闭
- 网络出现严重拥堵或断网
- 计算机的网络设置被更改为指向新控制台

在多数情况下，当计算机开机后，或者解决了造成通信中断的问题后，与计算机间的通信会再次建立。计算机向控制台做出回应并重新建立通信可能需要几分钟时间。如果通信未能重新建立，请联系[技术支持](#)了解故障排除的方法。

### 配置本地服务

本地服务是指建立和维护计算机连接的服务。

### 启用本地服务

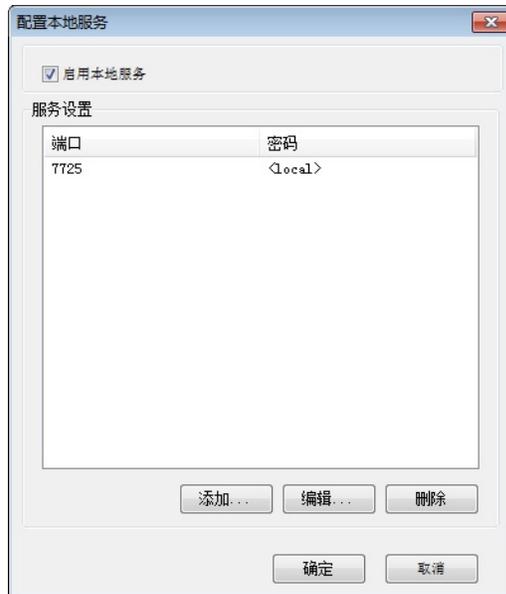
默认情况下，本地服务会在首次运行控制台时安装并启用。

在禁用（和 / 或卸载）本地服务后再次启用该服务

1. 选择 **工具 > 网络配置**。

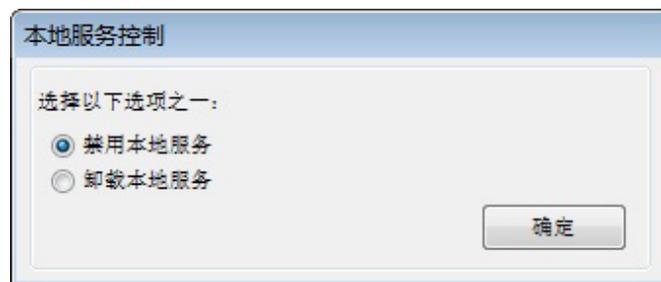


2. 选中 *启用本地服务* 复选框，启用该服务。



### 禁用本地服务

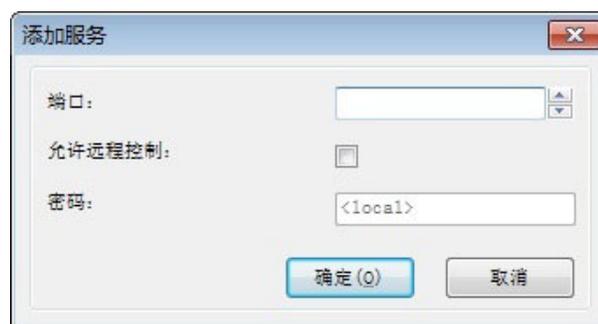
清除 *启用本地服务* 复选框并单击 *确定*，随即显示用于禁用或卸载本地服务的选项。



### 添加本地服务连接

1. 若要添加本地服务连接，请选择 *工具 > 网络配置*。
2. 若要添加连接，请选择 *添加* 并指定端口号（此处为 7725）。
3. 若要允许远程控制该控制台，请选中 *允许远程控制* 复选框并指定密码。

选择 *添加* 后，系统会在本地服务的连接列表和控制台的网络窗格中创建一个为端口 7725 提供服务的连接。





## 编辑或删除本地服务连接

添加本地服务连接后，可以通过 *工具 > 网络配置* 编辑或删除该连接。

若要编辑本地服务连接，请执行以下步骤：

1. 选择 *启用本地服务* 选项。
2. 从本地服务连接列表中选择 一个端口，然后单击 *编辑*。
3. 通过显示的 *编辑* 对话框可以对端口启用远程控制并设置密码保护。
4. 若要从本地服务中删除一个端口，请突出显示该端口并单击 *删除*。此操作不会从企业控制台的 *网络和组* 窗格中删除该条目，而只是从本地服务连接列表中删除该端口。
5. 若要将条目从控制台的网络窗格中删除，请选择此条目并单击位于边栏上的 *删除* 图标。

## 配置代理服务器连接

如果您使用代理服务器来连接互联网，您必须指定代理服务器设置以使以下功能运行正常：

- 检查更新
- 公告
- 许可证激活

完成下列步骤以指定代理服务器设置：

1. 选择 *工具 > 网络配置*。
2. 转到 *代理服务器* 选项卡。



3. 选中 *启用代理服务器* 复选框，启用代理服务器。

The screenshot shows a '网络配置' (Network Configuration) dialog box with a '代理' (Proxy) tab selected. The '启用代理' (Enable Proxy) checkbox is checked. Under '代理服务器信息' (Proxy Server Information), the '地址' (Address) field contains '123.12.23.34' and the '端口' (Port) field contains '5678'. Under '用户身份验证' (User Authentication), the '代理服务器需要授权 (登录凭据)' (Proxy server requires authentication (login credentials)) checkbox is unchecked. The '身份验证类型' (Authentication type) dropdown is set to 'Basic'. There are empty input fields for '用户名' (Username), '密码' (Password), and '域' (Domain). At the bottom, there are '确定' (OK) and '取消' (Cancel) buttons.

4. 指定以下代理服务器设置：
  - > 地址 – 指定代理服务器的 IP 地址。
  - > 端口 – 指定代理服务器的端口号。
5. 此步骤为可选步骤。仅在您的代理服务器需要授权的情况下遵循此步骤。选中 *代理服务器需要授权 (登录凭据)* 复选框并指定以下字段的值：
  - > 身份验证类型 – 选择身份验证类型。
  - > 用户名 – 指定用户名。
  - > 密码 – 指定密码。
  - > 域 – 指定域。
6. 单击 *确定*。



## 远程控制台

---

远程控制台是一个能够承载一个或多个连接的控制台，其他控制台可以通过这些连接与远程控制台连接。现有连接必须经过编辑才能实现远程访问。

### 设置启用远程控制的连接

若要对连接启用远程访问，请执行以下步骤：

1. 打开 *工具 > 网络配置*。
2. 选中 *启用本地服务* 复选框。
3. 从列表中选择一个端口，然后单击 *编辑*。
4. 选中 *允许远程控制*。
5. 指定一个密码。
6. 单击 *确定*。



## 连接到远程控制台

主机控制台建立远程控制台后，另一台计算机的其他控制台便可对该远程控制台进行访问。

1. 选择边栏上的 *连接到远程控制台* 图标或右键单击网络项。完成选择后即出现 *连接到远程控制台* 对话框：

2. 在 *连接到远程控制台* 对话框中，指定连接的详细信息，例如 *远程控制台名称*、*远程控制台 IP*、*端口号* 和 *密码*。此信息由主机控制台的管理员提供。输入信息后，您可以在 *网络和组* 窗格中右键单击一个端口并选择 *属性* 查看此信息。



如果与远程控制台的连接已中断，可单击边栏上的 *重新连接到远程控制台* 图标或者右键单击 *网络和组* 窗格中的一个条目，重新建立连接。



## 使用控制台管理 Deep Freeze

企业控制台包含一个位于屏幕顶部的工具栏，可用于快速访问控制台的各项功能。

转至 **视图 > 经典外观** 以采用经典 Windows 格式查看图标。



转至 **视图 > 现代外观** 以采用现代 Windows 格式查看图标。



也可以使用上下文菜单访问这些命令，如下所示；右键单击一个或多个计算机时将显示上下文菜单。当您选择一个特定操作时，所选计算机会执行该操作，同时状态图标也会相应更新。如果选择多个计算机，操作仅应用于适用计算机。例如，如果选择解冻和冻结的计算机并应用重启解冻操作，则将仅解冻冻结的计算机。此操作将不会应用于已解冻的计算机。

### 经典外观



### 现代外观



如果所选计算机不支持此操作，则某些特定的图标会被禁用。例如，一个具有目标图标的计算机无法显示 **解冻** 或 **冻结** 选项，因为程序尚未安装。



## 以指定次数重启 Thawed 解冻 / 重启 Thawed 解冻锁定

您可以选择在 Thawed 解冻或 Thawed 解冻锁定状态下以指定次数重启工作站。选定后，每当工作站在后续指定的重启次数内重启时，此选项均会使工作站保持在 Thawed 解冻状态。

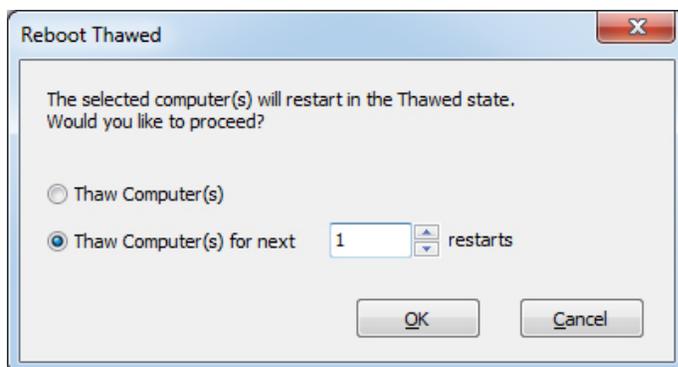
完成以下步骤：

1. 选择一个或多个工作站。
2. 右键单击并选择 *重启 Thawed 解冻* 或 *重启 Thawed 解冻锁定*。
3. 选择 *在后续 X 次重启后 Thaw 解冻的计算机*，并指定重启次数。

选择此选项将在 Thawed 解冻或 Thawed 解冻锁定状态下以指定重启次数来重启工作站。

例如，当您将重启次数指定为 3 时，工作站将在后续 3 次重启后保持在 Thawed 解冻或 Thawed 解冻锁定状态。

在 Thawed 解冻状态下重启工作站的 **最大可选次数为 99**。



## 登录用户

管理员无需走到每台计算机旁，即可在所选计算机上登录用户。

要使此功能起作用，必须将计算机配置为从 Windows 登录屏幕隐藏用户账户，并在登录过程中显示用户名和密码字段。



在 Deep Freeze 中启用 *登录用户* 功能，必须执行此策略。

要在 Windows 欢迎屏幕上隐藏上次登录的用户名，请转至 **本地安全策略 > 安全设置 > 本地策略 > 安全选项 > 交互式登录：不显示上次登录（登录时不显示用户名）** > 选择 **启用**。请注意，默认情况下已禁用此策略。



如果用户登录 Windows 需要按 CTRL+ALT+DEL，您将需要额外配置以下策略：

- 转至本地安全策略 > 安全设置 > 本地策略 > 安全选项 > 交互式登录：无须按 CTRL+ALT+DELETE > 选择启用。
- 转至本地计算机策略 > 管理模板 > Windows 组件 > Windows 登录选项 > 禁用/启用软件安全注意序列（或 SAS）。选择已启用，然后选择服务和辅助功能应用程序。



如 Deep Freeze 许可证已过期，此功能将无法使用。

系统会记录最近 10 次的用户登录信息，每次选择用户时都需要输入密码。

此功能不适用于仅安装了工作站种子的计算机。

Log in User

User name:

Password:

OK Cancel

## 正在向计算机发送消息

若要向一个或多个计算机发送消息，请完成以下步骤：

1. 选择要向其发送消息的计算机。
2. 右键单击并从上下文菜单中选择 *发送消息*。
3. 在出现的对话框中键入消息，然后单击 *发送*。或者，还可以从 *记录* 下拉列表中发送先前发送的消息。此时会出现对话框，询问是否确定要将消息发送给所选计算机。
4. 单击 *确定* 发送消息，或单击 *取消* 不发送消息并关闭对话框。



## 更新 Deep Freeze 配置文件

要使用现有 .rdx 文件的设置更新一台或多台计算机的配置，请完成以下步骤。rdx 文件中包含 Deep Freeze Enterprise 配置管理程序中指定的各种条件。

1. 右键单击计算机并选择 *使用 RDX 文件更新*。
2. 此时出现一则消息，要求提供现有的 .rdx 文件。
3. 单击 *确定*。随后弹出一个标准的 *打开文件* 对话框，可在其中选择 .rdx 文件。
4. 找到相应文件并单击 *打开*，以使用 .rdx 文件中的设置更新所选计算机的配置。单击 *取消* 可取消配置更新。

## 运行 Windows 更新

可以按需从右键单击上下文菜单中应用 Windows 更新。

要在工作站上运行 Windows 更新，请完成以下步骤：

1. 右键单击计算机并选择 *运行 Windows 更新*。
2. 单击 *确定*。

此时 Windows 更新将在所选工作站上应用。“Windows 更新”选项卡选项卡上配置的设置将被使用。

除了按需从右键单击上下文菜单应用 Windows 更新，您还可以计划 Windows 更新任务。有关如何计划 Windows 更新任务的详细信息，请参阅 [计划 Deep Freeze 任务](#)。



如果新配置中的 *网络* 选项发生更改，计算机可能会中断与现有企业控制台的通信。如果断开了与计算机的通信，请检查已更新计算机的 *网络* 设置，确保控制台的端口号和 / 或 IP 地址未被更改。



对密码所做的更改会立即生效。所有其他更改将在计算机重启后生效。无法通过更新配置文件的方式更改解冻空间和 / 或冻结的驱动器。



## 远程启动

此功能允许 IT 管理员远程启动托管工作站上的可执行程序。可执行文件可以通过由 Deep Freeze 冰点管理的网络在多个工作站上远程安装。支持的文件类型包括 .exe (可执行程序) · .msi (MSI 安装程序) · .bat/.cmd (批处理脚本文件) · .vbs (VB Ccript) · 以及 .ps1 (PowerShell)。选择 MSI 安装程序后，Deep Freeze 冰点使用 MSIEXEC 来运行此程序。

您还可以指定 Web URL 或 FTP 位置，用于下载和安装可执行文件。文件将从指定位置自动下载并在工作站上启动。

要在工作站上远程启动可执行文件，请完成以下步骤：

1. 可以通过以下任一方式在工作站上启动可执行程序：
  - > 右键单击一个或多个工作站，然后从上下文菜单中选择 *远程启动*。
  - > 通过 Deep Freeze 冰点任务制定计划。
2. 指定下列字段的值，或者从 *记录* 下拉列表中选择先前指定的值：



- > 文件名和路径 – 指定目标计算机上可用文件的文件名和路径。或者，也可浏览以选择可执行文件。或者指定 URL 或 FTP 位置。支持的文件类型包括 .exe · .msi · .bat/cmd/ · .vbs · 以及 .ps1。默认情况下，MSI 安装程序在安装模式下运行。例如，如果可执行程序 MyApplication.exe 位于 C:/AppFolder 上，请指定 C:/AppFolder/MyApplication。
3. 使用环境变量指定命令行参数（可选）：
    - > 参数 – 通过此可执行程序指定要应用的参数。例如，如果在命令提示符处使用 C:\AppFolder\MyApplication -o logFile.log 命令运行此可执行程序，则为参数指定 -o logFile.log。对于 .msi 文件，指定使用 MSIEXEC 启动 .msi 文件时通常要指定的参数。如果您没有为 .msi 文件指定任何参数，Deep Freeze 冰点将自动附加 "/i" (安装)。Deep Freeze 冰点也会使用 /qn (安静，无 UI) 取代任何显示选项。
  4. 单击 *确定*。
- 文件即在所选工作站上远程启动。



## 推送并启动

此功能允许 IT 管理员推送并启动托管工作站上的可执行文件。可执行文件可以通过由 Deep Freeze 冰点管理的网络在多个工作站上远程安装。

您还可以指定 Web URL 或 FTP 位置，用于下载和安装可执行文件。文件将从指定位置自动下载并在工作站上启动。

要在托管工作站上推送并启动文件，请完成以下步骤：

1. 可以通过以下任一方式在工作站上启动可执行程序：
  - > 右键单击一个或多个工作站，然后从上下文菜单中选择 *推送并启动*。
  - > 通过 Deep Freeze 冰点任务制定计划。
2. 浏览以选择文件路径或指定文件路径（或者，也可从 *记录* 下拉列表中选择先前指定的值）：



- > 文件名和路径 – 指定控制台计算机上可用文件的文件名和路径。或者，也可浏览以选择可执行文件。或者指定 URL 或 FTP 位置。支持的文件类型包括 .exe、.msi、.bat/cmd/、.vbs、以及 .ps1。默认情况下，MSI 文件在安装模式下运行。例如，如果可执行程序 MyApplication.exe 位于 C:/AppFolder 上，请指定 C:/AppFolder/MyApplication。
3. 使用环境变量指定命令行参数（可选）：
    - > 参数 – 通过此可执行程序指定要应用的参数。例如，如果在命令提示符处使用 C:\AppFolder\MyApplication -o logFile.log 命令运行此可执行程序，则为参数指定 -o logFile.log。对于 .msi 文件，指定使用 MSIEXEC 启动 .msi 文件时通常要指定的参数。如果您没有为 .msi 文件指定任何参数，Deep Freeze 冰点将自动附加 "/i"（安装）。Deep Freeze 冰点也会使用 /qn（安静，无 UI）取代任何显示选项。
  4. 单击 *确定*。
- 文件将被推送到所选工作站并在所选工作站上远程启动。

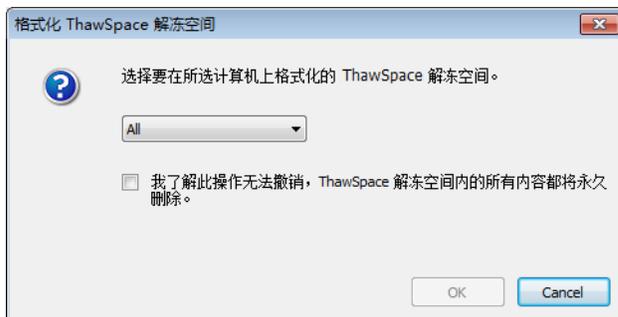


## 格式化 ThawSpace 解冻空间

Deep Freeze Enterprise 冰点企业版控制台提供在托管工作台上格式化特定 ThawSpace 解冻空间或所有 ThawSpace 解冻空间的功能。

要格式化 ThawSpace 解冻空间，请完成以下步骤：

1. 选择一个或多个工作站。
2. 右键单击并选择 *ThawSpace 解冻空间* > *格式化 ThawSpace 解冻空间*。或者，也可单击工具栏中的格式化 ThawSpace 解冻空间图标。
3. *格式化 ThawSpace 解冻空间*对话框随之显示。选择 *全部*或选择要格式化的特定驱动器。



4. 选择 *我了解此操作无法撤销，ThawSpace 解冻空间内的所有内容都将永久删除*。
5. 单击 *确定*。



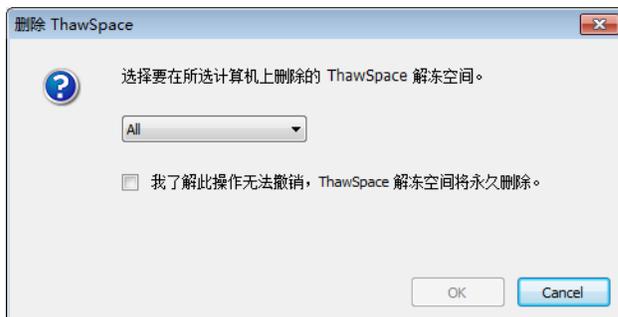
格式化 ThawSpace 解冻空间命令会删除 ThawSpace 解冻空间上的所有数据。一旦删除此数据，则无法恢复。在格式化 ThawSpace 解冻空间之前备份重要文件。

## 删除 ThawSpace 解冻空间

Deep Freeze Enterprise 冰点企业版控制台提供在托管工作站上删除特定 ThawSpace 解冻空间或删除所有 ThawSpace 解冻空间的功能。

要删除 ThawSpace 解冻空间，请完成以下步骤：

1. 选择一个或多个工作站。
2. 右键单击并选择 *ThawSpace 解冻空间* > *删除 ThawSpace 解冻空间*。或者，也可单击工具栏中的删除 ThawSpace 解冻空间图标。
3. *删除 ThawSpace 解冻空间*对话框随之显示。选择 *全部*或选择要删除的特定驱动器。





4. 选择 *我了解此操作无法撤销*，*ThawSpace* 解冻空间将永久删除。
5. 单击 *确定*。

## 查看控制台日志文件

企业控制台将所有已连接计算机的状态和活动历史记录保存在一个日志中。该日志存储了过去 7 天的信息。超过 7 天的信息将自动从日志中删除。

工作站	域	时间	状态	IP 地址	MAC 地址	Applied Command
DESKTOP	WORKGROUP	星期四 10/03/2019 09:03:00	冻结 (Console)	192.168.2...	000c2978f4b0	
DESKTOP	WORKGROUP	星期三 09/25/2019 15:38:33	解冻 (Console)	192.168.2...	000c2978f4b0	重启后冻结

- 若要查看一个或多个计算机的日志文件，请右键单击相应计算机并选择 *显示日志*。
- 若要排序日志文件，请单击所需标题。可用的列如下：
  - > 工作站
  - > 域
  - > 时间
  - > 状态
    - 状态栏显示计算机的当前状态以及计算机的重启方式。
    - 例如，如果计算机通过控制台重启为 Thawed 解冻状态，该状态将显示为 *Thawed 解冻 (控制台)*。
  - > IP 地址
  - > MAC 地址
  - > 应用的命令 (Frozen 冻结，Thawed 解冻，重启，关闭)
  - > 安装文件
- 要导出日志文件，请单击 *导出为* 并选择 *文本* 或 *CSV*。指定文件名称并单击 *确定*。



## 针对性安装 Deep Freeze

完成以下步骤可以通过远程方式，将完整的工作站安装在任何安装有工作站种子的计算机上。

1. 右键单击一个或多个计算机，然后选择 **安装**。此时将显示一个对话框，询问是否继续进行安装。单击 **确定**。
2. 在出现的对话框中，选择要安装在远程计算机上的文件。
3. 选择需要的安装文件，然后单击 **打开**。
4. 计算机会安装 Deep Freeze 并重启。
5. 安装完成后，可以从企业控制台查看到计算机状态的变化，且其状态将显示为 **冻结**。

## 更新 Deep Freeze 软件

若要使用新版本的 Deep Freeze 更新 Deep Freeze 计算机（安装了 Deep Freeze 7.7 或更高版本），请完成以下步骤：

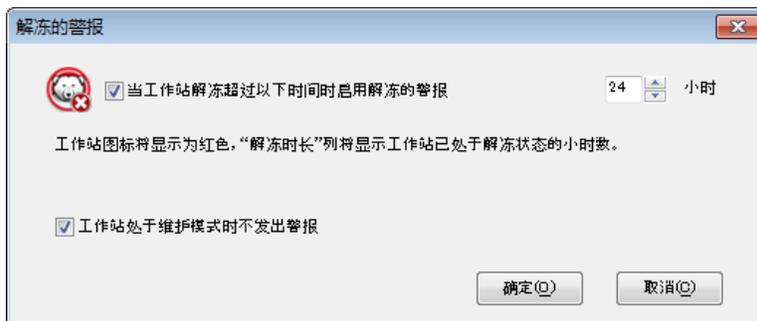
1. 在企业版控制台中，选择要更新的计算机。这些计算机可以处于 **Frozen** 冻结也可以处于 **Thawed** 解冻状态。
2. 右键单击并从上下文菜单中选择 **更新 Deep Freeze**。
3. 所选计算机会更新到新版本的 Deep Freeze 软件，但会保留当前版本的所有设置。这些计算机将重启两次以完成更新。

## Thawed 解冻警报

Thawed 解冻警报通知管理员计算机是否在特定时段内已处于 Thawed 解冻状态。工作站图标将在 Deep Freeze Enterprise 冰点企业版控制台显示为红色，**Thawed 解冻时长**列将显示工作站已处于 Thawed 解冻状态的小时数。

要设置 Thawed 解冻警报，请完成以下步骤：

1. 转至 **工具 > Thawed 解冻警报**。
2. 此时将显示 **Thawed 解冻警报**对话框。当工作站解冻超过 x 小时，选择 **启用 Thawed 解冻警报**。选择 x 的值。



3. 如果不想收到工作站正在维护的警报通知，请选择 **工作站处于维护模式时不发出警报**。
4. 单击 **确定**。



## 许可证

可通过 Deep Freeze 冰点企业版控制台更新许可证密钥，并且可以自动或手动激活工作站许可证。

若要自动激活 Deep Freeze 冰点工作站许可证，请完成以下步骤：

1. 启动 *Deep Freeze 冰点企业版控制台*。
2. 转到 *工具 > 许可*。
3. 此时将显示 *许可对话框*。



4. 单击 *编辑*并在 *许可证密钥*字段中输入许可证密钥。
5. 单击 *更新许可证*。此操作会将 Deep Freeze 冰点从 *评估版本*转换为 *许可版本*。*许可证密钥类型*字段中显示了 *许可证密钥*。*过期日期*中显示了许可证的过期日期和时间。

Deep Freeze 冰点可通过企业版控制台或直接连接至 Faronics 许可证激活服务器来自动激活每个工作站的许可证。



必须激活产品许可证才能验证副本并避免过期。无法 Frozen 冻结 30 天之内未激活的 Deep Freeze 冰点工作站。



工作站将通过本地控制台连接或直接连接至 Faronics 激活服务器并在 Internet 连接可用时向我们的安全服务器传送有关计算机的一些信息（包括产品版本，许可证密钥，计算机 ID，MAC 地址，CPU ID 以及控制台设备 ID）。



## 手动激活

若要手动激活 Deep Freeze 冰点工作站许可证，请先完成上述步骤 1-5。之后，请完成以下步骤：

1. 单击**立即激活**。系统将显示两个选项：



- > 选择**在线激活**，以通过 Internet 激活 Deep Freeze 冰点工作站许可证。单击**下一步**后，工作站上的许可证即会激活。计算机必须连接到 Internet 才能在线激活。
- > 选择**离线激活**，以通过电子邮件或电话激活 Deep Freeze 冰点工作站许可证。单击**下一步**。此时将显示**离线激活**屏幕：





- 单击 **创建离线激活请求文件**，然后单击 **保存**。将文件发送至 **activation@faronics.com** 以获取激活回复文件。浏览并选择从 Faronics 获取的 **激活回复文件**。单击 **应用离线激活请求文件**。



许可证密钥会在与企业版控制台通信的所有计算机上自动更新。如果计算机脱机（关机或从网络断开），则许可证密钥将在该计算机连接到企业版控制台时更新。

## 许可证图标

如果您工作站的 Deep Freeze 冰点许可证并未通过 Faronics 许可证激活服务器激活，则工具栏上将显示激活图标。您可以在线或离线激活待激活的工作站。

若要使用激活图标激活工作站，请完成以下步骤：

- 单击激活图标中的下拉列表。

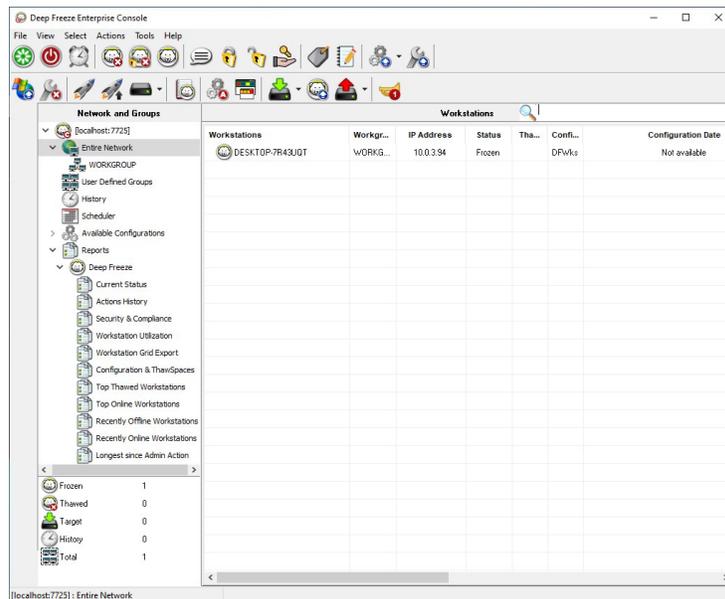


- 选择 **在线激活所有工作站**。Deep Freeze 冰点控制台将联系 Faronics 许可证激活服务器，然后激活许可证。在线激活时需要连接 Internet。
- 或者，选择 **离线激活所有工作站**。有关离线激活的更多信息，请转到 [手动激活](#)。



## 报告

Deep Freeze 控制台可编译有关工作站性能、当前状态、历史记录等各类报告以及 **Anti-Virus 防病毒报告**。您可以从“网络和组”面板访问以下报告。



点击“导出为 XLS”可将信息导出为电子表格格式。

- 当前状态：显示工作站的 Deep Freeze 状态，以及工作站处于 Thawed 解冻状态的时间。
- 操作历史记录：记录在工作站上应用的操作，包括操作时间、更新后的 Deep Freeze 版本、配置、相关标签或用户定义的组。
- 安全与合规：显示 Deep Freeze 的安全状态详情，方便判断产品是否需要更新、激活或是否长期处于 Thawed 解冻状态。
- 工作站使用情况：显示选定时段内每个工作站的使用详情。
- 工作站网格导出：导出时，报告内容将提供当前工作站网格的精确版本，保留控制台显示的网格结构和格式，包括可见列的顺序。
- 配置与 ThawSpace 解冻空间：提供工作站配置、ThawSpace 解冻空间、已排程任务的详情。
- 完整配置报告：全面报告所有可用配置、RDX 和安装文件中的每个配置设置。
- 解冻时间最长的工作站：识别解冻时间最长的工作站。
- 在线时间最长的工作站：识别正常运行时间最长的工作站。
- 最近离线的工作站：识别最近停止与 Deep Freeze 控制台通信的工作站。
- 最近在线的工作站：识别最近与 Deep Freeze 控制台通信的工作站。



- 自管理员操作以来的最长时间：识别长时间未收到任何控制台或工作站 UI 命令的工作站，这可能代表工作站被忽视或优先级较低。

## 自定义网格

### 查看或隐藏报告

要查看或隐藏报告，请右键单击 Deep Freeze，然后选择 / 取消选择要查看或隐藏的报告。

### 整理网格中的列

点击并拖动列标题到新位置，自定义信息显示方式。

### 搜索和筛选

点击每列右上方的筛选器以筛选视图，并使用条件参数自定义筛选器。

- 等于
- 不等于
- 小于
- 小于或等于
- 大于
- 大于或等于
- 类似于
- 不类似于
- 包括
- 不包括
- 开始为
- 结尾为
- 为空
- 不为空
- 介于以下两者之间
- 不介于以下两者之间
- 属于以下之一
- 不属于以下之一

在适用的情况下，您可以点击底部的时间戳并选择预定义的日期范围来选择筛选视图，也可以自定义日期偏好，然后点击 "应用筛选器"。



## 自定义筛选器

添加筛选器后，您可以自定义筛选器并添加更多筛选器组合，从而创建多个筛选器。您可以保存、重复使用这些筛选器，只需点击一下即可访问。点击右下角的“自定义”，然后在“筛选器构建器”中选择“添加条件”、“添加组”或“清除所有”。

点击“筛选器”>“添加条件”添加新条件，并按此格式指定条件：列名、参数、表达式。

例如：Workstation Name = (Equals) Desktop。

或点击“按下按钮添加新条件”。

点击“筛选器”>“添加组”添加子组条件，并为该条件指定参数。

点击“另存为”将筛选器保存在网络上。

点击“打开”，然后从保存的筛选器中选择，以应用筛选器。

## 分组方式

您还可以将列标题拖放到“将列标题拖放到此处，以按该列分组”区域，按组排列视图。



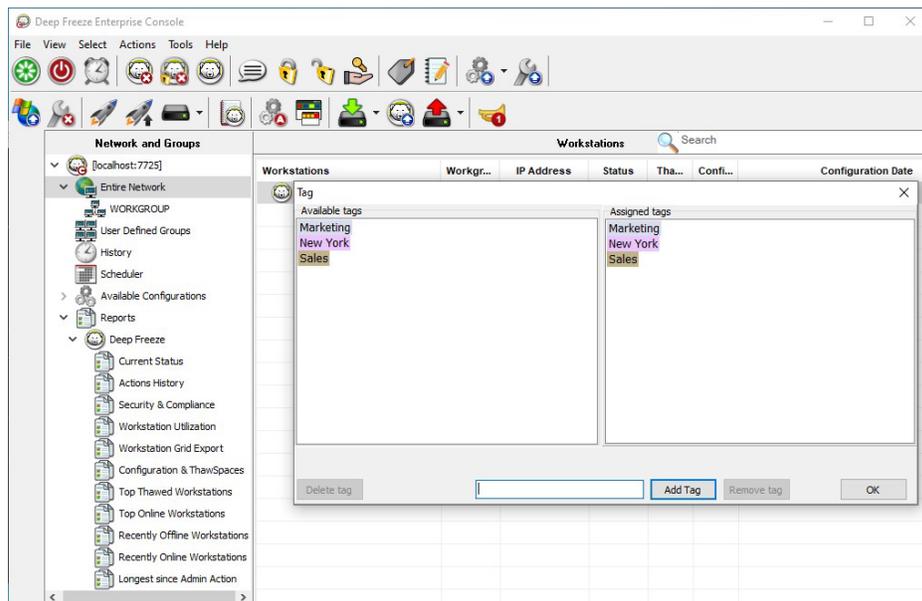
## 标签

标签即简单的数据片断，通常为提供关于某项（如计算机、群组等）详细信息的单字描述、关键词或标签，以便于通过浏览或搜索找到相关项。

例如，您可以按照财务部、营销部或销售部等部门来添加计算机标签。然后，您可以搜索标签“帐户”，将显示带指定标签的所有项。

### 创建 / 分配标签

标签可应用于多台计算机。



要创建或分配标签，请完成以下步骤：

1. 从网格中选择一个工作站。
2. 点击工具栏上的“标签”图标。
3. 在“为计算机添加标签”字段中，输入前几个字符并从列表中选择（如果标签已存在），或创建全新标签，然后点击“添加标签”。

新标签将自动分配到所选计算机。

或双击任意可用标签，将标签分配给工作站。

### 移除 / 取消分配标签

要移除 / 取消分配标签，请完成以下步骤：

1. 从网格中选择一个工作站。
2. 点击工具栏上的“标签”图标。
3. 在“已分配的标签”窗格中，选择要移除 / 取消分配的标签。
4. 点击“移除标签”。



标签将自动从所选计算机上移除 / 取消分配。



从计算机上取消分配的标签只会被移除，不会从标签列表中删除。

## 删除标签

要删除标签，请完成以下步骤：

1. 从网格中选择一个工作站。
2. 点击工具栏上的 " 标签 " 图标。
3. 从 " 可用标签 " 列表选择一个标签。
4. 点击 " 删除标签 " 。



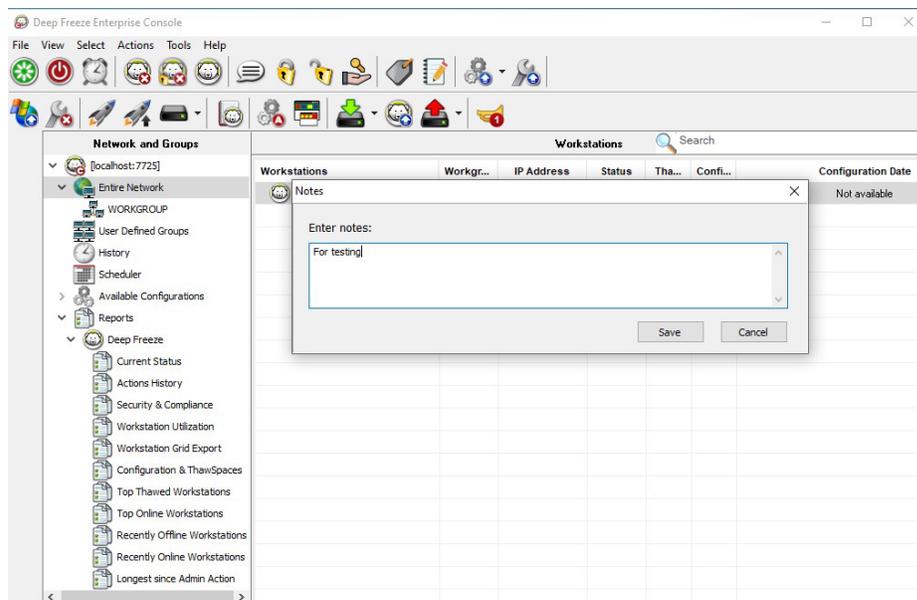
已删除的标签将从列表中全面删除（而不仅仅是从工作站中删除），并从已分配标签的计算机中自动移除。



## 注释

注释提供额外的背景信息或说明，用于为所选工作站解释、标注或添加信息。

### 添加注释



要添加注释，请完成以下步骤：

1. 从网格中选择一个工作站。
2. 点击工具栏上的 "注释" 图标。
3. 输入注释（最多 260 个字符）。
4. 点击 "保存"。

当鼠标悬停在网格的注释上时，注释将以工具提示的形式显示。

注释只能应用于单个工作站。



## 计划 Deep Freeze 任务

Deep Freeze Enterprise 冰点企业版提供两种 Deep Freeze 冰点任务：

- 单个任务 – 只包含一个 Deep Freeze 冰点任务
- 组合任务 – 最多可以包含 5 个 Deep Freeze 冰点任务，最长 20 小时。组合任务无法立即运行，只能提前安排。

若要使用 *计划任务向导* 在企业版控制台中计划单个 Deep Freeze 冰点任务，请完成以下步骤：

1. 使用以下任一方式打开 *计划任务向导*：

- > 在 *网络和组* 窗格中单击 *计划程序*，然后单击 *添加任务* 图标
- > 在 *网络和组* 窗格中右键单击 *计划程序*，然后选择 *添加任务*

此时将显示以下屏幕：



2. 双击要添加的任务，或在选择任务后单击 *下一步*。以下任务适用于 Deep Freeze 冰点：

- > 组合任务
- > 重启
- > 关闭
- > 局域网唤醒
- > 重启后 Frozen 冻结
- > 重启后 Thawed 解冻
- > 重启后 Thawed 解冻已锁定
- > 发送消息
- > 登录用户
- > 运行 Windows Update
- > 远程启动
- > 推送并启动



- > 更新
  - > 格式化 ThawSpace 解冻空间
3. 在以下屏幕中，为任务输入名称，并选择所需的任务执行排程：每日，每周，每月或仅一次。任务名必须唯一。两个任务不得重名。单击 **下一步**。

计划任务向导

FARONICS  
**DEEPFREEZE™**  
ENTERPRISE

为该任务键入名称：  
Restart

执行该任务：

每日

每周

每月

仅一次

< 上一步 (B)    下一步 > (N)    取消 (C)

4. 根据任务执行的选择，接下来的时间和日期配置选项也会有所不同。单击 **下一步**。

计划任务向导

FARONICS  
**DEEPFREEZE™**  
ENTERPRISE

选择要开始执行该任务的时间和日期。

开始时间：  
17:54:15

执行该任务：

每天

工作日

每    1    天

开始日期：  
2014/11/4

< 上一步 (B)    下一步 > (N)    取消 (C)



## 5. 完成配置之后，单击*完成*。



默认的任务开始时间为当前时间的五分钟之后。

若要使用 *计划任务向导* 在企业版控制台中计划组合任务，请完成以下步骤：

### 1. 使用以下任一方式打开 *计划任务向导*：

- > 在 *网络和组* 窗格中单击 *计划程序*，然后单击 *添加任务* 图标
- > 在 *网络和组* 窗格中右键单击 *计划程序*，然后选择 *添加任务*

此时将显示以下屏幕：





2. 选择 *组合任务* 并单击 *下一步*。
3. 在以下屏幕中，为任务输入名称，并选择所需的任务执行排程：每日、每周、每月或仅一次。任务名必须唯一。两个任务不得重名。单击 *下一步*。



4. 根据任务执行的选择，接下来的时间和日期配置选项也会有所不同。单击 *下一步*。





5. 从下拉列表中选择任务，并指定时间。单击 + 号，添加另一个任务。重复操作，最多可以添加 5 个任务，最长 20 小时。单击 下一步。



6. 复查任务列表，然后单击 *完成*。

## 编辑计划的任務

要编辑计划的任務，请右键单击该任务并选择 *编辑任务*。按照第 [计划 Deep Freeze 任务](#) 节中的步骤 1-5 进行操作。



## 为计划的任务分配计算机

计划了任务之后，该任务会出现在控制台的 *网络和组* 窗格中的 *计划程序* 下。



若要为任务分配计算机，请从控制台的工作站窗格中选择所需计算机，并将其拖到相应任务上。或者，将一个组拖到该任务上。

若要查看分配给某一特定任务的计算机，请单击该任务。分配的计算机将显示在工作站窗格中。

若要从任务中删除计算机，请单击该计算机并按 *Delete* 键。

### 添加任务

要添加任务，请右键单击 *计划程序* 并选择 *添加任务*。

### 编辑任务

要编辑任务，请右键单击该任务并选择 *编辑任务*。

### 暂停任务

要暂停任务，请右键单击该任务并选择 *暂停任务*。

### 恢复任务

要恢复任务，请右键单击该任务并选择 *恢复任务*。



## 删除任务

若要删除一项任务，请右键单击该任务并选择 *删除任务*。

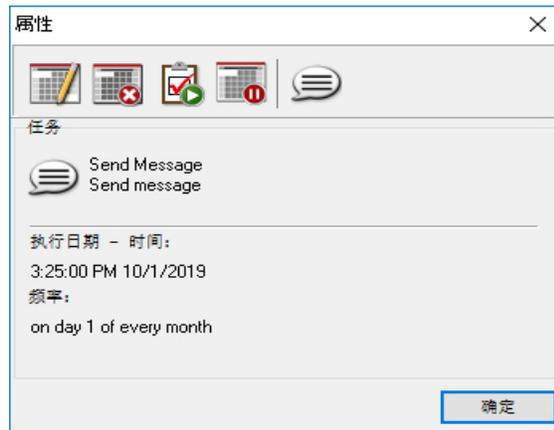
## 立即执行任务

若要立即执行一项任务，请右键单击该任务并选择 *执行任务*。

## 计划任务的属性

若要查看一项任务的属性，请右键单击该任务的名称并选择 *查看属性*。

随后将显示以下屏幕：



只要本地服务已启用并且退出企业控制台后未关闭网络连接，即便企业控制台已关闭，计划的任務仍将按计划执行。



## 管理网络和组

企业控制台可以根据计算机所在的工作组或域自动对其进行安排。您可以单击相应的工作组或域来查看其中的计算机。

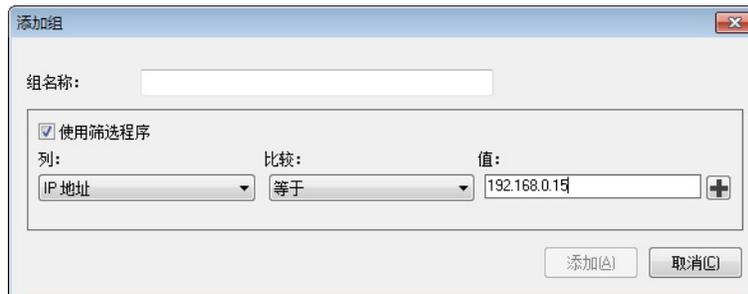
可以使用企业控制台定义特定的组来对计算机进行安排。

### 添加组

通过 *添加组* 对话框，您可以配置多个过滤器以将工作站分类到不同组中。此过滤器会根据所选参数中的更改自动更新工作站列表。

要通过过滤器添加一个组，请完成以下步骤：

1. 右键单击 *网络和组* 窗格中的 *用户定义组*。
2. 选择 *添加组*。此时将显示 *添加组* 对话框：



3. 指定 *组名*。
4. 选择 *列*。
5. 选择 *比较*。
6. 选择 *选项*和 / 或如果您要添加另一个过滤器。
7. 指定 *值*或 *正则表达式*。
8. 单击 *添加*。



下表显示了列·比较·选项以及值。

选择列	选择比较	选择选项	指定值或正则表达式
工作站	等于	和 或者	指定 <i>值</i> 或 <i>正则表达式</i> 。
	不等于		
	正则表达式		
	包含		
工作组	等于	和 或者	指定 <i>值</i> 或 <i>正则表达式</i> 。
	不等于		
	正则表达式		
	包含		
IP 地址	等于	和 或者	指定 <i>值</i> 或 <i>正则表达式</i> 。
	不等于		
	正则表达式		
	包含		
状态	等于	和 或者	Frozen 冻结 冻结并锁定 Thawed 解冻 解冻并锁定 应用 Windows 更新 应用批处理文件 Thawed 解冻期间 维护模式 许可证已过期 工作站种子 脱机
	不等于		
标签	等于	和 或者	指定 <i>值</i> 或 <i>正则表达式</i> 。
	不等于		
注释	包含	和 或者	指定 <i>值</i> 或 <i>正则表达式</i> 。



选择列	选择比较	选择选项	指定值或正则表达式
配置	等于	和 或者	指定 <i>值</i> 或 <i>正则表达式</i> 。
	不等于		
	正则表达式		
	包含		
配置日期	等于	和 或者	指定 <i>日期</i> 。
	不等于		
	大于		
	大于或等于		
	小于		
	小于或等于		
安装文件	等于	和 或者	指定 <i>值</i> 或 <i>正则表达式</i> 。
	不等于		
	正则表达式		
	包含		
版本	等于	和 或者	指定 <i>值</i> 或 <i>正则表达式</i> 。
	不等于		
	大于		
	大于或等于		
	小于		
	小于或等于		
操作系统	等于	和 或者	指定 <i>值</i> 或 <i>正则表达式</i> 。
	不等于		
	正则表达式		
	包含		
MAC 地址	等于	和 或者	指定 <i>值</i> 或 <i>正则表达式</i> 。
	不等于		
	正则表达式		
登录名	等于	和 或者	指定 <i>值</i> 或 <i>正则表达式</i> 。
	不等于		
	正则表达式		
解冻时长	大于	和 或者	指定 <i>值</i> 。
	大于或等于		
	小于		
	小于或等于		



选择列	选择比较	选择选项	指定值或正则表达式
可用 ThawSpace 解冻空间 (GB)	等于 不等于 正则表达式	和 或者	指定 <i>值或正则表达式</i> 。



## 构建用户定义的组结构

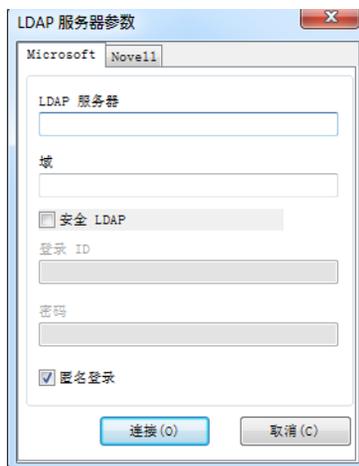
一个组添加完毕后，可以在其下添加一个或多个子组，而且作为区分环境的一种方式，还可以无限地继续添加子组，如下面的例子所示：



## 从 Active Directory 导入组

如果已经在 Active Directory 中设计了组结构，可以直接将此结构导入企业控制台。若要从 Active Directory 导入组，请完成以下步骤：

1. 选择 **工具 > 从 Active Directory 导入组**，或单击位于边栏上的 **LDAP** 图标。
2. 随后将显示以下对话框。选择 **Microsoft** 选项卡或 **Novell** 选项卡。



3. 输入导入位置的 LDAP 服务器信息。也可以使用匿名登录选项。如果未选中匿名登录复选框，则需要提供用户名和密码。
4. 如果您的网络使用的是安全 LDAP，选择安全 LDAP。（有关安全 LDAP 的更多信息，请转至 <https://support.microsoft.com/en-ca/kb/321051>）
5. 单击 **连接**。此时将出现 **Active Directory** 层次结构。选择所需条目，然后单击 **导入**。



## 历史记录

---

企业控制台中存储了目标计算机的历史记录。

如果计算机网络断开，关机或者重启，则企业控制台中的特定计算机下面会出现感叹号(!)。如果计算机恢复成联机状态，则感叹号图标将消失。

如果计算机连接永久性断开（例如，计算机网线被拔出）或者计算机关闭，则感叹号会继续显示在控制台上。

在企业控制台中，转到 **文件 > 退出**。选择 **关闭并中断网络链接** 选项，然后单击 **确定**。一旦您重新打开企业控制台，则带有感叹号(!)的计算机将出现在历史记录中。如果计算机被关闭并配置远程唤醒硬件，请在 **历史记录** 中右键单击计算机并选择 **远程唤醒** 以唤醒计算机。

*历史记录* 中的选项：

- 若要查看历史记录，请单击 **网络和组** 窗格中的 **历史记录**。
- 若要从历史记录中删除计算机，请选择相应计算机，右键单击并从上下文菜单中选择 **从历史记录中删除**。
- 为了通过远程唤醒功能唤醒计算机，请选择计算机，并且在上下文菜单中右键单击并选择 **远程唤醒**。



## 将计算机添加到组

---

可以通过两种方式将计算机添加到组：将计算机从*工作站*窗格拖至所需的组，或在创建组的过程中使用自动筛选集。

自动组筛选功能可以将计算机自动添加至用户定义的组。计算机是按名称进行添加的。

您可以使用通配符 (\*、?) 根据名称的特定部分添加计算机。

示例：*Lab1-\**将添加名称以 "Lab1-" 开始的所有计算机。

### 按字母顺序排序组

若要按字母顺序排序组，请右键单击*用户定义的组*，并选择*按字母顺序排序组*。

### 从用户定义的组中删除工作站

若要从组中删除计算机，请在*用户定义的组*中右键单击该计算机，然后选择*从组中删除*。

### 导入或导出组到文件

若要从文件导入组或将组导出至文件，请从*工具*菜单中选择所需的选项。

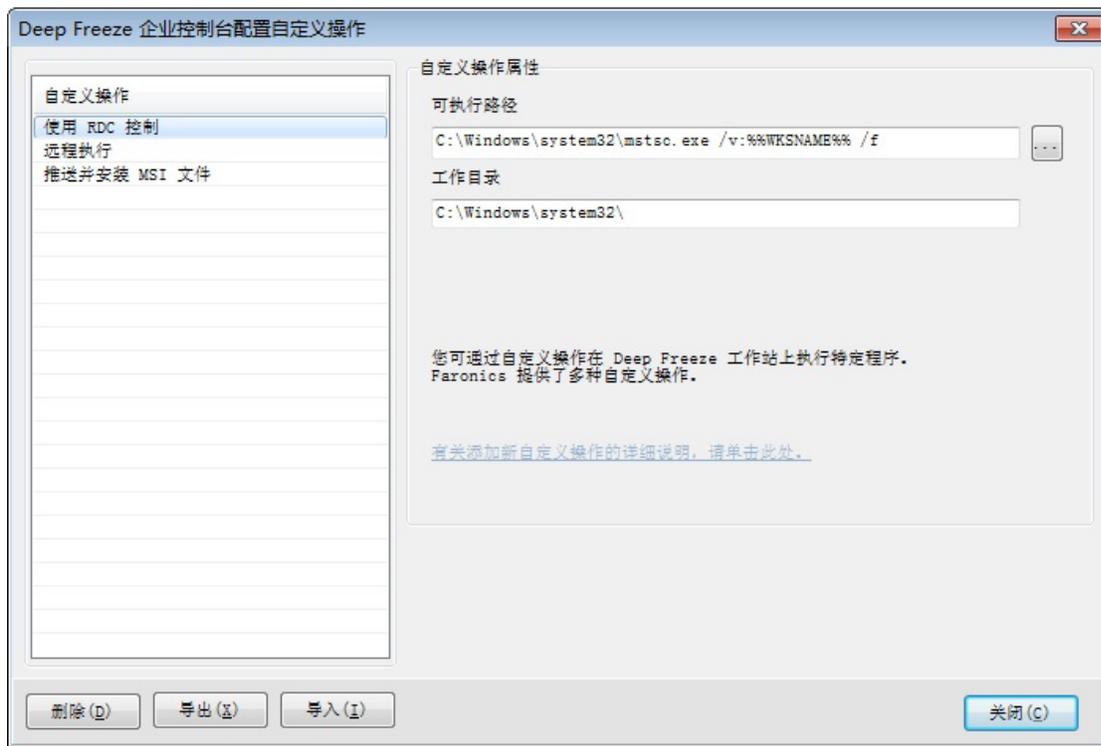


## 配置自定义操作

Deep Freeze 提供了下列自定义操作，可通过 *操作* 菜单进行访问。也可以创建其他操作以满足特殊需要。Deep Freeze 提供了三个默认操作。可通过在 Deep Freeze 控制台中导入相应 *.xml* 文件配置其他自定义操作。有关自定义操作，自定义操作文件的结构以及各个参数的详细信息，请参阅附录 E。

### 使用 RDC 控制

允许通过 Microsoft 远程桌面协议连接到计算机。必须已经在目标计算机上启用了远程桌面连接。



1. 单击 *操作* > *自定义操作*。
2. 选择 *使用 RDC 控制*。
3. 输入 *可执行路径*，或浏览并选择位置。
4. 输入 *工作目录*。
5. 单击 *应用*。



## 远程执行

使用远程执行，可以通过远程方式执行计算机上的可执行文件。PsExec 工具可用于远程执行计算机上的可执行文件。必须首先将 PsExec 下载并安装到该计算机上。有关 PsExec 的详细信息，请访问 <http://www.faronics.com/pstools>。



## 配置

1. 单击 **操作 > 自定义操作**。
2. 选择 **远程执行**。
3. 输入 **PSEXec 位置**，或浏览并选择位置。
4. 此时会自动添加 **可执行路径和工作目录**。可在以后修改 **可执行路径和工作目录**。
5. 单击 **关闭**。

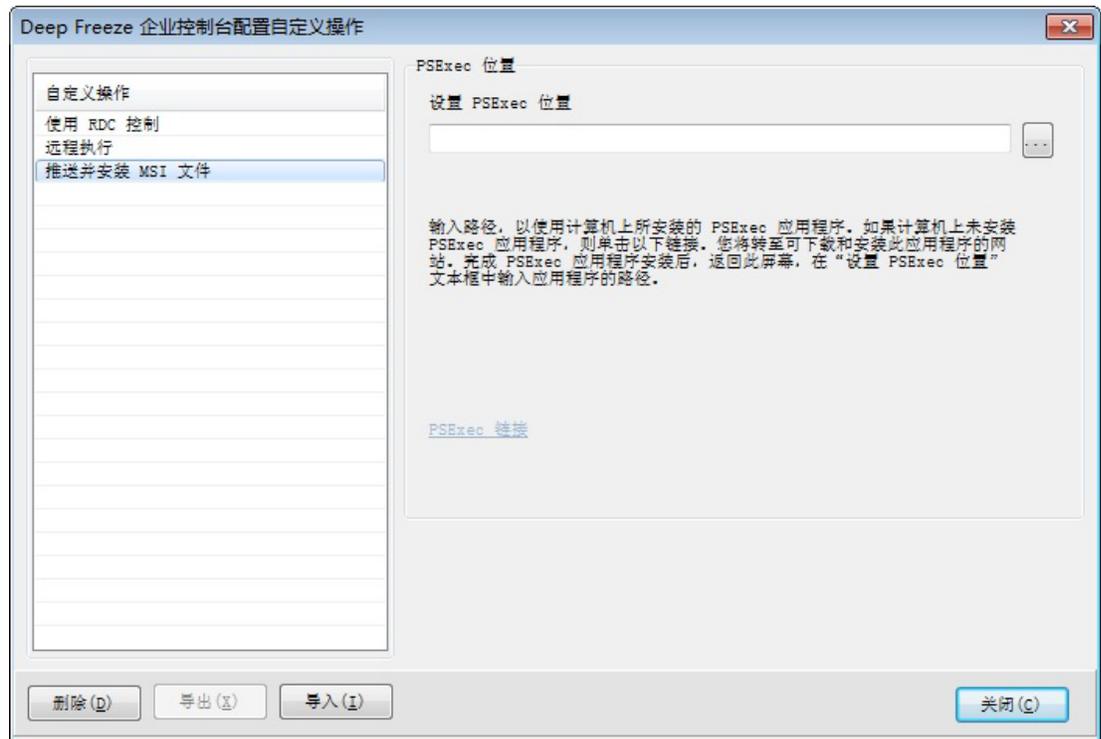
## 执行

1. 从 **工作站窗格** 中选择计算机。
2. 选择 **操作 > 远程执行**。
3. 此时将显示 **远程执行对话框**。
4. 输入 **用户名、密码和命令**。
5. 单击 **确定**。



## 推送并安装 MSI 文件

使用 *推送并安装 MSI 文件* 选项，可以通过企业控制台在计算机上推送并安装 .msi 文件。



### 配置

1. 单击 *操作 > 自定义操作*。
2. 选择 *推送并安装 MSI 文件*。
3. 输入 *PSEXec 位置*，或浏览并选择位置。
4. 此时会自动添加 *可执行路径和工作目录*。可在以后修改 *可执行路径和工作目录*。
5. 单击 *关闭*。

### 执行

1. 从 *工作站窗格* 中选择计算机。
2. 选择 *操作 > 推送并安装 MSI 文件*。
3. 此时将显示 *推送并安装 MSI 文件* 对话框。
4. 输入 *用户名*、*密码*、*文件名* 和 *驱动器盘符*。
5. 单击 *确定*。

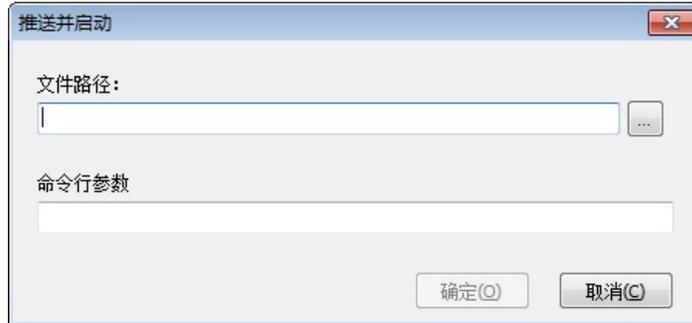


## 推送并启动

您可在托管工作站上推送并启动文件。

要在托管工作站上推送并启动文件，请完成以下步骤：

1. 从工作站窗格选择一个或多个工作站。
2. 右键单击并选择 **操作 > 推送并执行**。此时将显示 **推送并启动** 对话框。



3. 浏览以选择文件路径或指定文件路径。
  - > 文件名和路径 – 指定控制台计算机上可用文件的文件名和路径。或者，也可浏览以选择可执行文件。支持的文件类型包括 .exe（可执行文件）和 .msi（MSI 安装程序）。默认情况下，MSI 文件在安装模式下运行。例如，如果可执行文件 MyApplication.exe 位于 C:/AppFolder 上，请指定 C:/AppFolder/MyApplication。
4. 使用环境变量指定命令行参数（可选）：
  - > 参数 – 通过此可执行程序指定要应用的参数。例如，如果在命令提示符处使用 C:\AppFolder\MyApplication -o logFile.log 命令运行此可执行程序，则为参数指定 -o logFile.log。对于 .msi 文件，指定使用 MSIEEXEC 启动 .msi 文件时通常要指定的参数。如果您没有为 .msi 文件指定任何参数，Deep Freeze 冰点将自动附加 "/i"（安装）。Deep Freeze 冰点也会使用 /qn（安静，无 UI）取代任何显示选项。
5. 单击 **确定**。

文件将被推送到所选工作站并在所选工作站上远程启动。

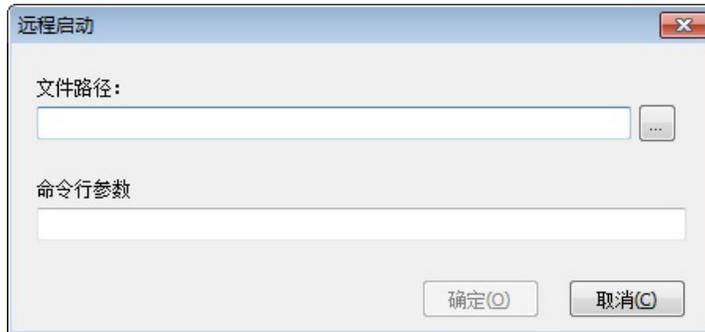


## 远程启动

您可在托管工作站上远程启动执行文件。

要在托管工作站上远程执行文件，请完成以下步骤：

1. 从 *工作站* 窗格选择一个或多个工作站。
2. 右键单击并选择 *操作 > 远程执行*。此时将显示 *远程执行* 对话框：



3. 浏览以选择文件路径或指定文件路径。
  - > 文件名和路径 – 指定控制台计算机上可用文件的文件名和路径。或者，也可浏览以选择可执行文件。支持的文件类型包括 .exe（可执行文件）和 .msi（MSI 安装程序）。默认情况下，MSI 安装程序在安装模式下运行。例如，如果可执行文件 MyApplication.exe 位于 C:/AppFolder 上，请指定 C:/AppFolder/MyApplication。
4. 使用环境变量指定命令行参数（可选）：
  - > 参数 – 通过此可执行程序指定要应用的参数。例如，如果在命令提示符处使用 C:\AppFolder\MyApplication -o logFile.log 命令运行此可执行程序，则为参数指定 -o logFile.log。对于 .msi 文件，指定使用 MSIEEXEC 启动 .msi 文件时通常要指定的参数。如果您没有为 .msi 文件指定任何参数，Deep Freeze 冰点将自动附加 "/i"（安装）。Deep Freeze 冰点也会使用 /qn（安静，无 UI）取代任何显示选项。
5. 单击 *确定*。

文件即在所选工作站上远程执行。



## 删除，导入和导出自定义操作

### 删除自定义操作

若要删除自定义操作，请完成以下步骤

1. 单击 *操作* > *自定义操作*。
2. 选择要删除的自定义操作。
3. 单击 *删除*。

### 导入自定义操作

若要导入自定义操作，请完成以下步骤

1. 单击 *操作* > *自定义操作*。
2. 单击 *导入*。
3. 浏览并选择要导入的 *.xml* 文件。
4. 单击 *打开导入文件*。

### 导出自定义操作

若要导出自定义操作，请完成以下步骤

1. 单击 *操作* > *自定义操作*。
2. 选择要导出的自定义操作。
3. 单击 *导出*。
4. 此时将显示 *将自定义操作导出至文件* 对话框。
5. 指定 *文件名* 并单击 *保存*。



## 控制台自定义程序

使用控制台自定义程序，您可以指定可以在控制台中使用的功能和命令，并可将结果另存为一个新控制台，且该控制台可在组织中分发。

可用设置分组为不同类别（控制台功能，工作站命令，Deep Freeze 命令，工作站安装/卸载命令和计划程序命令）。单击每个类别左端的加号 (+) 图标，可显示该类别中可用设置的完整列表。

根据需要选择或清除各个复选框。或者，一次选择或清除所有类别。被清除的设置在您新建的企业控制台中不能使用。有关在实际情形下如何使用控制台自定义程序的示例，请参阅[附录 D](#)。

若要创建具有有限功能的控制台，请完成以下步骤：

1. 选择 **工具 > 控制台自定义程序**。
2. 此时将显示控制台自定义程序。



3. 选择要在新控制台中显示的功能。
4. 单击另存为保存控制台。为文件指定名称。
5. 如果右键单击新建的 .exe 文件，则会启动具有有限功能的控制台。



## 关闭 Deep Freeze 企业控制台

若要关闭 Deep Freeze 控制台，请选择 **文件 > 退出**，或单击关闭窗口按钮。退出时可选择：

- 最小化控制台到系统任务栏。

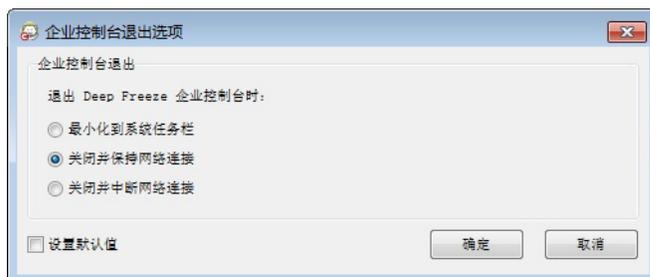
此操作不会停止控制台，同时使连接保持活动状态。Deep Freeze 控制台图标将出现在系统任务栏中。此时计划的任务仍将执行。若要重新打开 Deep Freeze 企业控制台，请右键单击任务栏上的控制台图标并选择 **还原 Deep Freeze 控制台**。

- 关闭 Deep Freeze 控制台并保持网络连接运行

此操作将关闭控制台，但与计算机的连接仍保持活动状态。此时计划的任务仍将执行。

- 关闭 Deep Freeze 控制台并关闭网络连接。

此操作将停止控制台进程并关闭连接（包括本地服务），计划的任务将不会开始执行。然而，已经开始执行的计划任务将继续执行。



选中 **设置默认值** 选项后，下次退出时将不再显示对话框。若要编辑这些设置，请选择 **工具 > 退出选项**。



## 在工作站上安装 Deep Freeze

使用配置管理程序创建自定义的安装程序文件后，可以使用 *有人参与安装*、*针对性安装*、*无提示安装系统* 或作为映像过程的一部分将 Deep Freeze 部署到计算机。



安装前应禁用所有后台实用程序和防病毒软件，并关闭所有应用程序。因为这些程序可能会干扰安装，导致 Deep Freeze 工作不正常。

在完成任何类型的安装之后，计算机将重新启动。要成功进行任何类型的卸载，Deep Freeze 必须处于解冻状态。

如果出现下列情况，任何现有的 ThawSpace 解冻空间都将在卸载时被删除：

- 配置管理程序中未选中用于保留现有 ThawSpace 解冻空间的选项。
- ThawSpace 解冻空间不是由 Deep Freeze Enterprise 5 或更高版本创建的。

### 有人参与安装或卸载

若要安装或卸载 Deep Freeze，请完成以下步骤：

1. 在计算机上运行安装程序文件 (*DFWks.exe*)。此时将显示以下屏幕
2. 单击 *安装* 开始安装。按照所示的步骤操作，然后阅读并接受许可协议。Deep Freeze 将进行安装，之后计算机将重新启动。



单击 *卸载* 以卸载 Deep Freeze。只有当之前安装了 Deep Freeze 且计算机当前处于解冻状态时，才能单击 *卸载*。如果存在解冻空间，Deep Freeze 会显示一个对话框，询问是保留还是删除该解冻空间。



如果硬盘驱动器碎片太多，则无法创建解冻空间。此时会显示一条消息，提示您中止安装或安装 Deep Freeze 而不创建解冻空间。



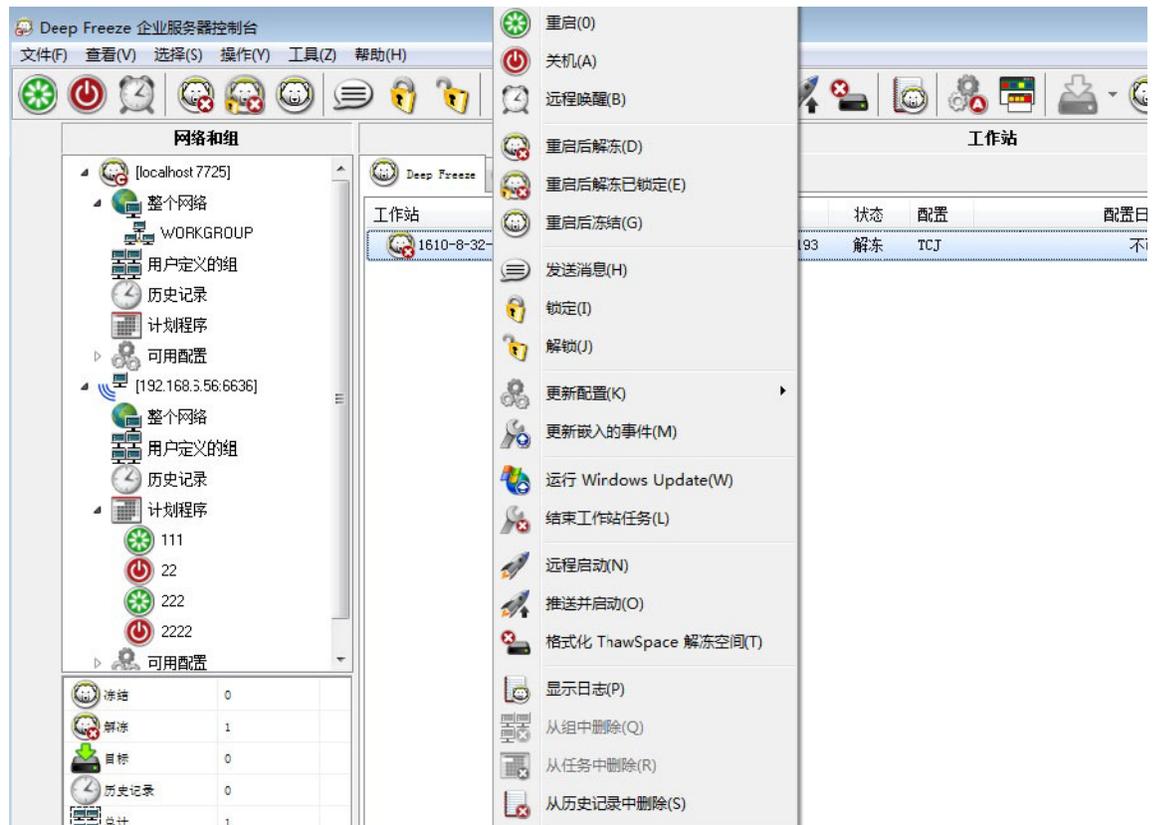
如果您选择 *延迟 Frozen 冻结重启来完成 Windows 更新* (配置管理程序的 *高级选项* 选项卡) 并安装 Deep Freeze 冰点, 安装程序会检查是否所有 Windows 更新都已完成。如果 Windows 更新未完成, Deep Freeze 冰点安装将无法继续。完成 Windows 更新并再次尝试安装 Deep Freeze 冰点。

如果您停用 *延迟 Frozen 冻结重启来完成 Windows 更新* 并安装 Deep Freeze 冰点, 请确保在不使用 Deep Freeze 冰点的情况下完成所有 Windows 更新。由于未完成 Windows 更新, 停用此选项可能会导致计算机陷入重启循环。



## 通过控制台在工作站上卸载 Deep Freeze

使用企业控制台可以完全卸载 Deep Freeze 或卸载 Deep Freeze 但保留工作站种子。要卸载该程序，计算机必须处于解冻状态。



若要卸载计算机上的 Deep Freeze 但保留工作站种子，请右键单击解冻的工作站并选择 *卸载 - 保留种子*，如上所示。或者，单击工具栏上的卸载图标。

若要完全卸载 Deep Freeze 和工作站种子，请选择要卸载的计算机，然后单击工具栏上的 *卸载* 图标。



要卸载 Deep Freeze，计算机必须处于解冻状态。企业控制台会弹出提示，要求确认卸载。确认要卸载后，Deep Freeze 即进行卸载，之后计算机重新启动。



## 无提示安装或卸载

借助无提示安装系统，可以通过网络将 Deep Freeze 快速安装到许多计算机。对于允许在远程计算机上执行命令行的任何部署实用程序，均可实现无提示安装系统。在完成无提示安装后，计算机将立即重新启动。命令行具有以下选项：

语法	说明
<code>[/Install]</code>	使用安装文件安装 Deep Freeze
<code>[/Install /Seed]</code>	仅安装指定的工作站种子文件
<code>[/Install /Thawed]</code>	使用安装文件安装 Deep Freeze 冰点并启动到解冻状态。
<code>[/Uninstall]</code>	卸载 Deep Freeze
<code>[/Uninstall /Seed]</code>	卸载 Deep Freeze，但仍保留工作站种子
<code>[/PW=password]</code>	在安装过程中设置密码 *
<code>[/AllowTimeChange]</code>	允许更改系统时钟 *
<code>[/Freeze=C,D,...]</code>	只冻结列出的驱动器，解冻所有其他驱动器 *
<code>[/Thaw=C,D,...]</code>	只解冻列出的驱动器，冻结所有其他驱动器 *
<code>[/USB]</code>	免除对外置 USB 硬盘的保护
<code>[/FireWire]</code>	免除对外置 FireWire 硬盘的保护

### 命令行示例

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

在上例中，Deep Freeze 安装程序文件被命名为 *DFWks.exe*。只有驱动器 C: 将被冻结。计算机上的任何其他驱动器都将被解冻。如果计算机只有一个驱动器 C:，则可省略 `[/Freeze]` 开关。此时将创建密码 (password)。执行该命令后，会安装 Deep Freeze，而计算机将在重启后冻结，并可继续使用。

在没有 `[/Install]` 或 `[/Uninstall]` 开关的情况下，无提示安装系统将不会工作。若要使用 `[/Uninstall]`，Deep Freeze 必须处于解冻状态。



若要运行配置命令行选项，必须清空高级选项选项卡上的禁用命令行选项。



\* 这些选项在默认情况下处于禁用状态。

## 使用快捷方式无提示安装或卸载

完成以下步骤可以在不使用安装对话框的情况下，直接在计算机上安装 Deep Freeze。

1. 在目标计算机上找到 Deep Freeze 安装程序文件 (*DFWks.exe*)。
2. 右键单击该图标并选择 *创建快捷方式*。
3. 右键单击该快捷方式并选择 *属性*。
4. 通过在路径的末尾键入 `/install` 或 `/uninstall`，编辑 *目标* 字段的路径。

快捷方式目标示例：

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

双击新的快捷方式会立即安装或卸载 Deep Freeze，随后计算机将重新启动。

若要使用 `/uninstall`，Deep Freeze 必须处于解冻状态。



如果硬盘驱动器碎片太多，则无法创建解冻空间。安装过程被中止。

## 在多个计算机上进行网络安装

*无提示安装系统*也可以用于通过网络在多个计算机上安装 Deep Freeze。如果网络上的工作站使用登录脚本，则该脚本可用于在所有联网工作站上自动安装 Deep Freeze。在安装完成后，所有的工作站会在重启后冻结，并可继续使用。

使用以下命令行语法可创建安装错误报告日志文件：

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



## 在现有 Deep Freeze 版本基础上安装

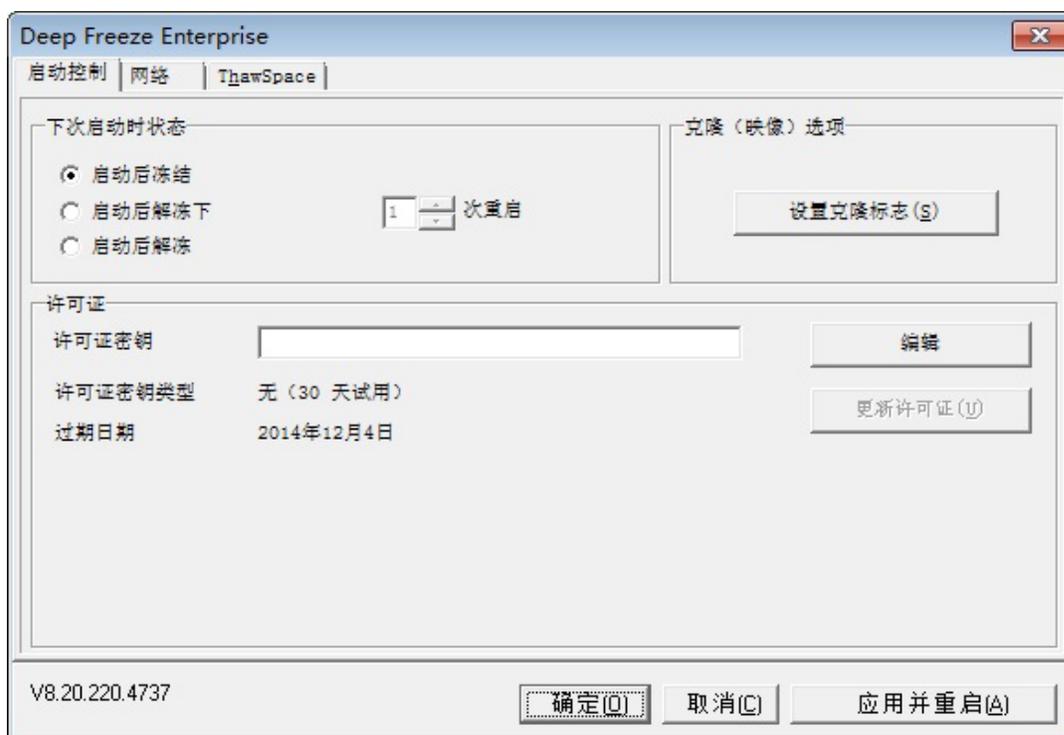
除非使用了更新 Deep Freeze 软件这一功能（Deep Freeze 6.3 及更高版本提供），否则必须先卸载所有现有的 Deep Freeze 版本后方可安装任何新版本的 Deep Freeze。

## 使用映像安装

Deep Freeze 冰点设计为可与所有主映像和桌面管理软件一起使用。可通过 *需人参与的安装* 或 *无提示安装* 在主映像上安装 Deep Freeze 冰点。

在最终完成主映像之前，Deep Freeze 冰点必须准备好进行部署。要准备主映像以进行部署，请完成以下步骤：

1. 重启计算机使其处于 *Thawed* 解冻状态。
2. 使用键盘快捷键 CTRL+SHIFT+ALT+F6 启动 Deep Freeze 冰点。或者，按住 SHIFT 并双击系统任务栏中的 Deep Freeze 冰点图标。
3. 输入密码并单击 *确定*。
4. 在 *启动控制* 选项卡上单击 *设置克隆标志*。
5. 此时将显示消息 *标志已成功设置。是否要立即重启计算机？* 单击 *是* 将立即重启计算机。单击 *否* 将在以后重启计算机。





设置克隆标志命令在映像期间十分重要，因为如果在映像安装成功后 Deep Freeze 冰点无法读取其配置文件，它会将计算机启动到 Thawed 解冻状态。如果未设置克隆标志，且如果 Deep Freeze 冰点无法读取其配置文件，则在映像安装成功后所有驱动器都会冻结。



如果您新使用的是 Sysprep，请确保在将系统准备好进行映射之后并在启动 Sysprep 之前设置克隆标志。

创建计算机映像之后，需要再次重启计算机，以使 Deep Freeze 冰点正确检测磁盘配置中的更改。如果在无人参与模式下创建计算机映像，则应执行相关步骤使计算机重新启动，以便更新配置。

若要在创建映像完毕后返回冻结状态，请将 Deep Freeze 冰点设置为在后续  $n$  次重启时启动解冻（在主映像中），以便在  $n$  次重启后计算机自动冻结。或者，也可以使用 Deep Freeze 命令行控制来冻结所选计算机。

## 针对性安装

也可以从企业控制台通过针对性安装部署 Deep Freeze。



## 检查更新

使用 Deep Freeze 可以检查是否有更高的版本可用。

访问 [帮助 > 检查更新](#)。此操作将检查是否有新版本的 Deep Freeze 可用。



如果有新版本可用，请单击 [下载最新版本更新 Deep Freeze](#)。





# 管理 Deep Freeze 计算机

本章介绍如何管理安装有 Deep Freeze 的计算机。

## 主题

---

[登录屏幕](#)

["启动控制" 选项卡](#)

["密码" 选项卡](#)

["网络" 选项卡](#)

["解冻空间" 选项卡](#)

[软件永久性安装 · 更改或删除](#)



## 登录屏幕

使用以下方式之一在计算机上访问 Deep Freeze。

1. 如果系统任务栏上显示了 Deep Freeze 图标，请按住 SHIFT 键并双击该 Deep Freeze 图标。如果 Deep Freeze 在隐蔽模式下运行且 Deep Freeze 图标未显示，那么必须使用键盘快捷键 CTRL+ALT+SHIFT+F6 来访问登录对话框。



2. 输入管理员密码并单击 **确定** 登录到 Deep Freeze。

作为一项附加安全功能，Deep Freeze 会在 10 次登录尝试失败后自动重启计算机来防止强力攻击。

## 在触摸屏设备上启动 Deep Freeze 冰点

您可使用 CTRL+ALT+SHIFT+6 或 CTRL+ALT+SHIFT+F6 在触摸屏设备上启动 Deep Freeze 冰点。然而，您必须在使用快捷键之前启用整个键盘。您也可触摸并按住系统托盘以启动 Deep Freeze 冰点上下文菜单。



## "启动控制" 选项卡

启动控制选项卡上有以下选项

### 下次启动时状态

启动控制选项卡用于设置 Deep Freeze 在下次重启后将处于的模式。



选择以下选项之一：

- 启动后冻结  
确保计算机在下次重启后冻结
- 启动后解冻下  
确保在后续指定的重启次数内，计算机在每次重启后解冻。当重启次数超过该指定的重启次数时，计算机启动后将被冻结。
- 启动后解冻  
确保计算机在每次重启后解冻

选择所需选项旁的单选按钮并单击 **确定** 保存所有更改。单击 **应用并重启** 将立即保存所有更改并重启计算机。

### 克隆

克隆窗格用于为部署过程准备主映像。有关详细信息，请参阅 [使用映像安装](#) 部分。



## 许可证

1. 若要更新许可证密钥，请单击 **编辑**并在 **许可证密钥**字段中输入许可证密钥。
2. 单击 **更新许可证**。此操作会将 Deep Freeze 冰点从 **评估版本**转换为 **许可版本**。**许可证密钥类型**字段中显示了 **许可证密钥**。**过期日期**中显示了许可证的过期日期和时间。
3. 单击 **立即激活**。系统将显示两个选项：



- > 选择 **在线激活**可在线激活 Deep Freeze 冰点许可证。此选项与步骤 1 相同。选择此选项后，单击 **下一步**。单击 **下一步**后，Deep Freeze 冰点即会在线激活。
- > 选择 **离线激活**。此选项允许您通过电话或电子邮件激活。激活后单击 **下一步**。此时将显示 **离线激活**屏幕。





- 通过电话或电子邮件将**激活详情**发送至 Faronics 激活支持人员。从 Faronics 收到激活码后，将其输入**激活码**字段，然后单击**下一步**。此时，Deep Freeze 冰点许可证便已激活。

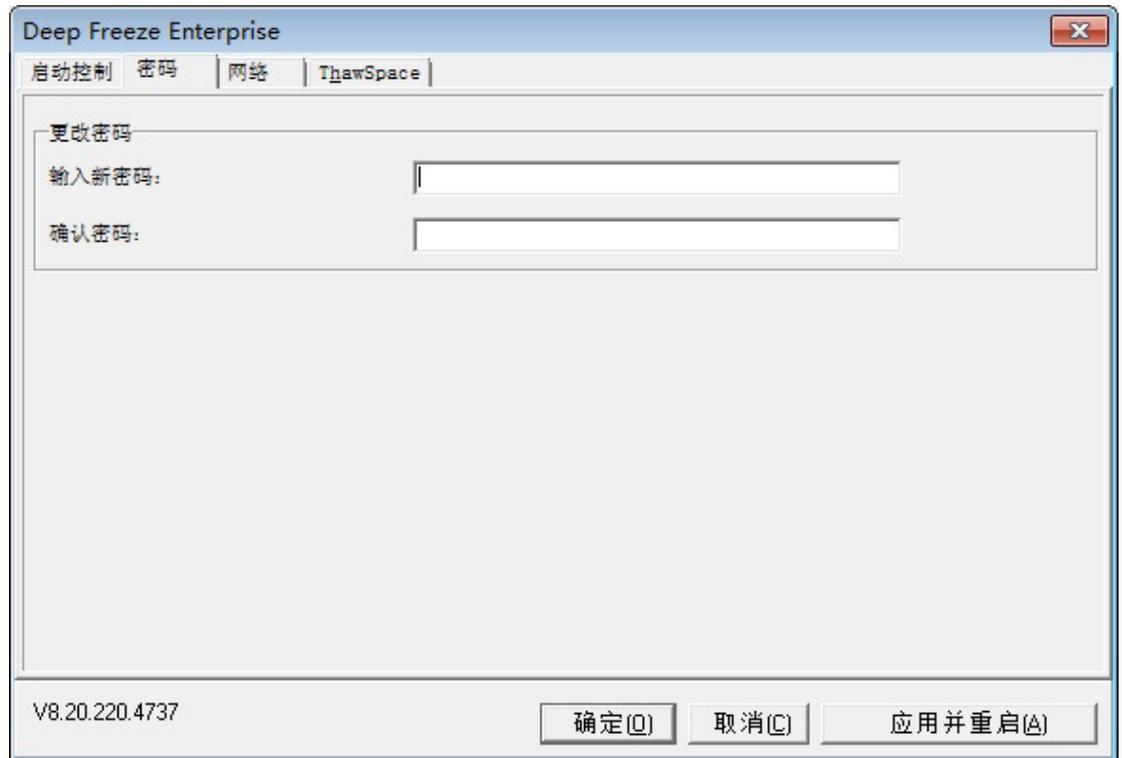


许可证密钥会在与企业版控制台通信的所有计算机上自动更新。如果计算机脱机（关机或从网络断开），则许可证密钥将在该计算机连接到企业版控制台时更新。



## " 密码 " 选项卡

密码选项卡用于更改密码。

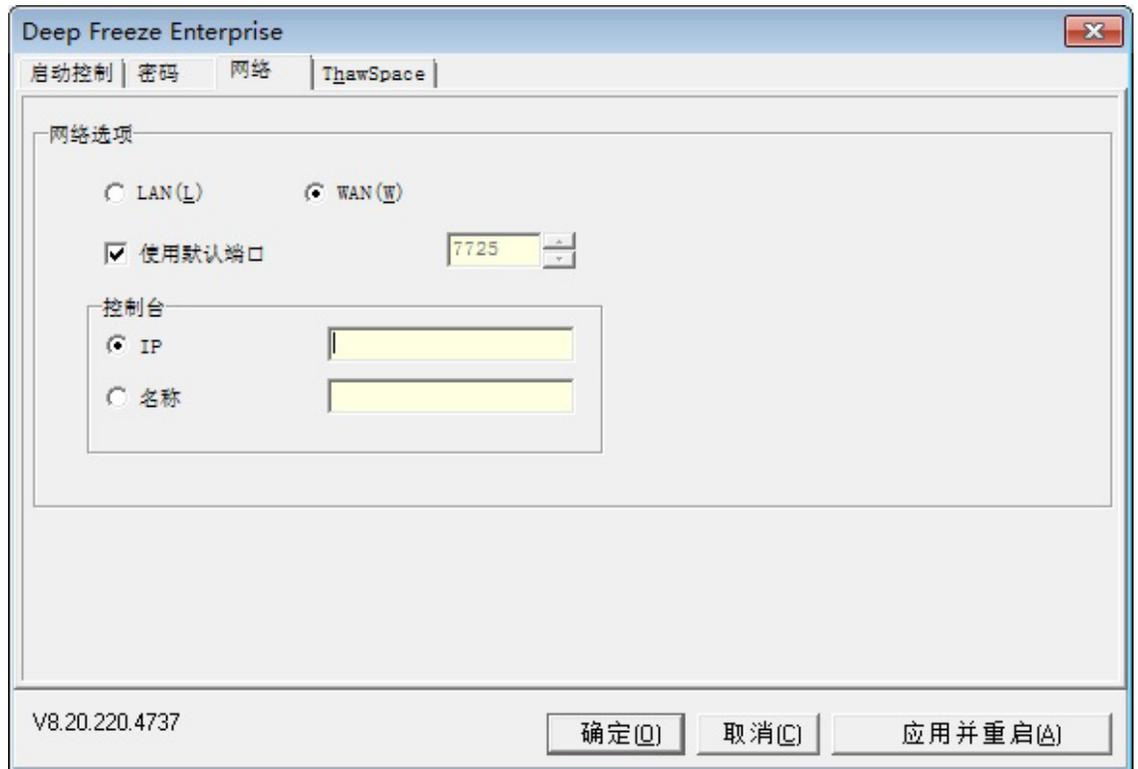


1. 在 **输入新密码** 字段中指定新密码。
2. 在 **确认密码** 字段中重新输入相同密码，以此确认新密码。
3. 单击 **确定**。
4. 此时将更改密码并显示一个确认对话框。



## "网络" 选项卡

网络选项卡可用于配置计算机的网络选项。



若要选择 LAN 或 WAN 通信方式，请单击相应的选项。

若要更改默认的端口号，可以清除 *使用默认端口* 复选框，然后输入需要的端口号。

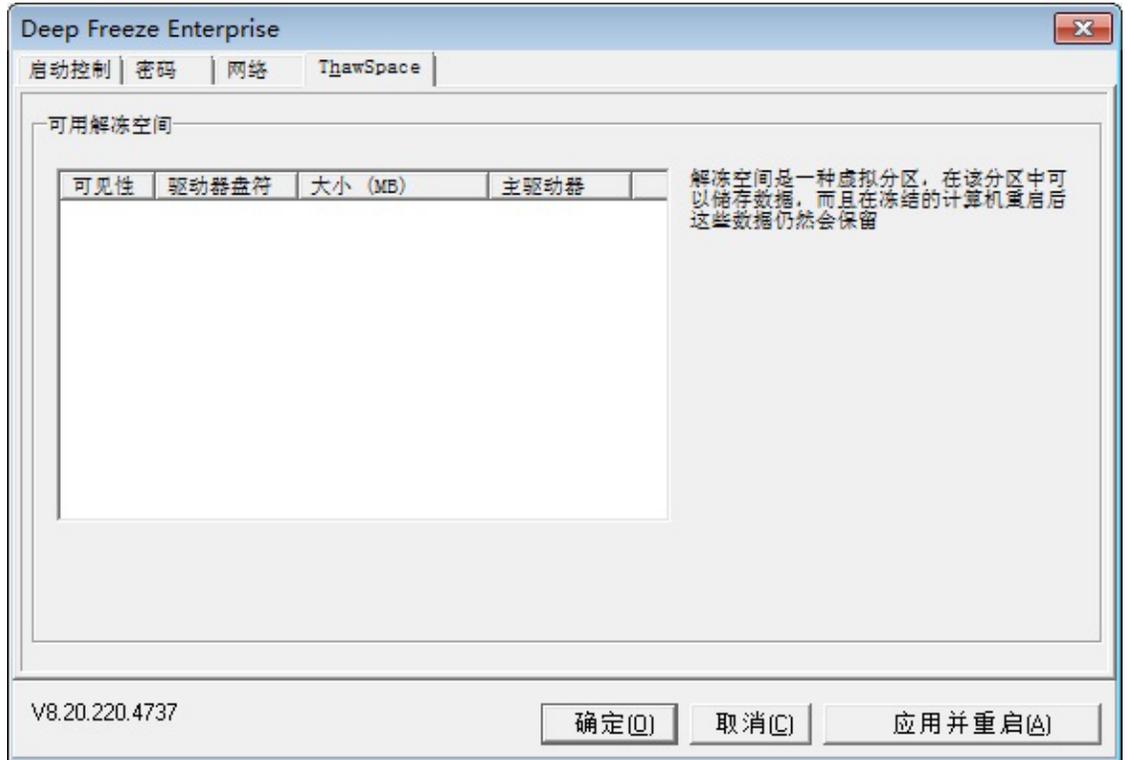
有关网络配置的详细信息，请参阅[附录 B](#)。



## "解冻空间" 选项卡

解冻空间是计算机上的一个虚拟分区，可用于存储程序，保存文件或进行永久性更改。解冻空间中存储的所有文件均在重启后保留，即便计算机处于冻结状态。

仅当设置为在 Deep Freeze Enterprise 配置管理程序中进行创建时，解冻空间才可用。



卸载 Deep Freeze 之后，所有解冻空间将会变得可见。重新安装 Deep Freeze 后，解冻空间根据解冻空间选项卡上的初始设置可见或隐藏。

在满足下列任意情况时，任何现有的解冻空间均将在卸载程序时被删除：

- 配置管理程序中未选中用于保留现有解冻空间的选项
- 解冻空间不是由 Deep Freeze 5 或更高版本创建的



## 软件永久性安装，更改或删除

---

若要使任何永久性更改生效，必须解冻计算机。通常，安装软件需要经过一次或多次重启才能完成。

Deep Freeze 可帮助管理员克服在生产环境中维护计算机配置的难题。Deep Freeze 可防止计算机受到未经授权的更改，病毒和间谍软件的危害，这些可能导致计算机无法正常工作。在保护计算机的同时，Deep Freeze 还提供保留用户数据的功能。

有关如何实施 Deep Freeze 并保留用户数据的详细信息，请参阅 <http://www.faronics.com/library> 中的 Deep Freeze – Retaining User Data available





# 管理 Anti-Virus

本章介绍如何通过企业控制台安装和使用 Anti-Virus。

## 主题

---

[Anti-Virus 概述](#)

[Anti-Virus 防病毒报告](#)

[迁移到新的 Anti-Virus 防病毒](#)

[在企业版控制台上启用 Anti-Virus 防病毒](#)

[在工作站上安装 Anti-Virus 防病毒客户端](#)

[Anti-Virus 配置](#)

[从企业控制台使用 Faronics Anti-Virus](#)

[计划 Anti-Virus 任务](#)

[在工作站上使用 Anti-Virus](#)

[检查 Anti-Virus 更新](#)

[更新 Faronics Anti-Virus](#)

[更新 Anti-Virus 防病毒定义](#)

[从企业控制台卸载 Anti-Virus 客户端](#)

[从企业控制台禁用 Faronics Anti-Virus](#)



## Anti-Virus 概述

---

Anti-Virus 防病毒可以通过企业控制台安装和使用。使用 Anti-Virus 防病毒是可选项。Deep Freeze Enterprise 冰点企业版也可在不使用 Anti-Virus 防病毒的情况下单独使用。

下面将介绍以下各节：

- 在企业版控制台上启用 Anti-Virus 防病毒
- 在工作站上安装 Anti-Virus 防病毒客户端
- Anti-Virus 防病毒配置
- 从企业版控制台使用 Anti-Virus 防病毒
- 排程 Anti-Virus 防病毒任务
- 在工作站上使用 Anti-Virus 防病毒客户端
- 检查更新
- 更新 Faronics Anti-Virus 防病毒
- 从工作站卸载 Anti-Virus 防病毒客户端
- 在企业版控制台上停用 Anti-Virus 防病毒



## Anti-Virus 防病毒报告

---

Anti-Virus 防病毒报告概述每个工作站的防病毒版本、保护状态、主动保护及防火墙状态、病毒定义版本以及上次更新时间。还包括上次扫描日期以及上次检测到威胁的日期。

- Anti-Virus 防病毒定义更新状态：显示工作站上 Anti-Virus 防病毒定义更新活动的详细信息。
- Anti-Virus 防病毒状态：显示工作站上 Anti-Virus 防病毒活动详情。
- Anti-Virus 防病毒合规与威胁：显示 “按检测结果数量分类威胁” 的历史信息。
- Anti-Virus 防病毒扫描历史记录：显示过去扫描的历史信息。
- Anti-Virus 防病毒隔离：显示每个工作站上被隔离项目的信息。



## 迁移到新的 Anti-Virus 防病毒

---

要迁移到新的 Faronics Anti-Virus 防病毒，请完成以下步骤：

1. 卸载旧版 Anti-Virus 防病毒。
2. 配置新版 Anti-Virus 防病毒策略。
3. 安装新版 Anti-Virus 防病毒。



## 在企业版控制台上启用 Anti-Virus 防病毒

现在，Anti-Virus 防病毒是企业版控制台的一部分，可以从企业版控制台中启用。您需要为 Anti-Virus 防病毒购买单独的许可证。

要启用 Faronics Anti-Virus 防病毒，请完成以下步骤：

1. 启动 Deep Freeze 冰点企业版控制台。
2. 转到 **工具 > 许可 > Faronics Anti-Virus 防病毒许可证**。



3. 选中 *我想使用 Deep Freeze 冰点控制台来管理 Faronics Anti-Virus 防病毒* 复选框。
4. 单击 *编辑*。
5. 输入许可证密钥并单击 *更新许可证*。
6. 单击 *关闭*。此时，将下载 Anti-Virus 防病毒安装程序文件。Anti-Virus 防病毒列将在 *工作站* 窗格中显示，Anti-Virus 防病毒子节点将添加到 *网络和组* 窗格中 *可用配置* 的下方。



## 在工作站上安装 Anti-Virus 防病毒客户端

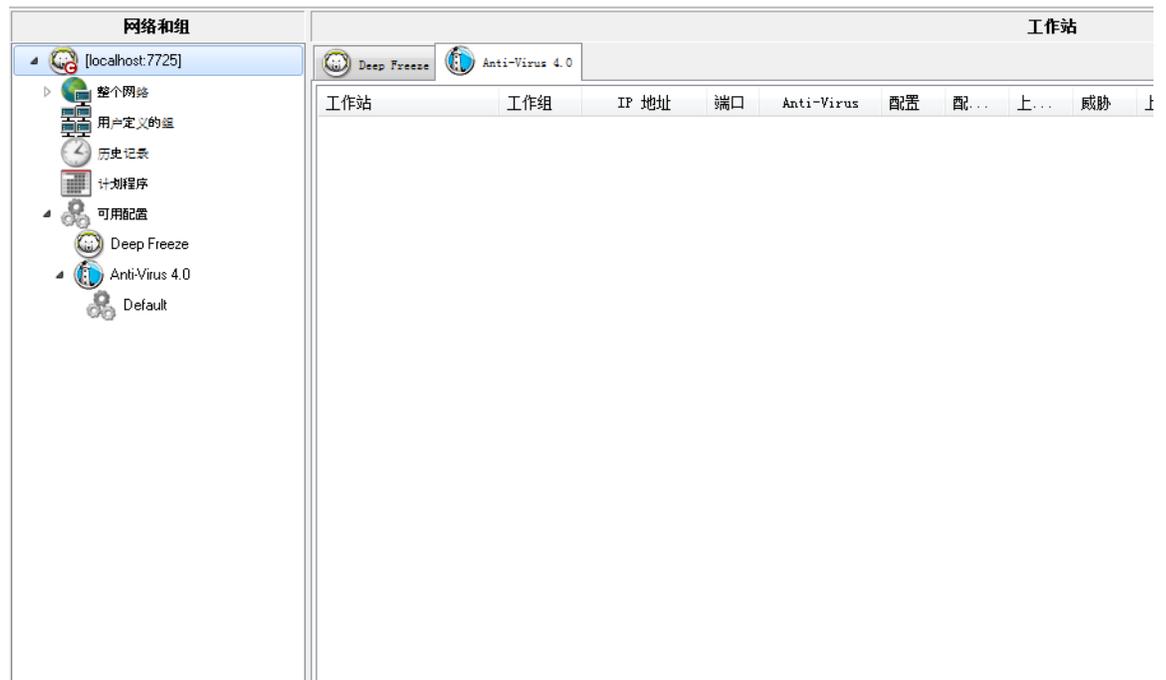
在工作站上安装 Anti-Virus 防病毒之前，请确保 Deep Freeze 冰点工作站安装文件或 Deep Freeze 冰点种子已部署到工作站，且工作站处于 Thawed 解冻状态。

要在工作站上安装 Anti-Virus 防病毒，请完成以下步骤：

1. 从 *工作站窗格* > *Anti-Virus 防病毒* 选项卡选择一个或多个工作站。
2. 单击菜单栏中的 Anti-Virus 防病毒图标，并选择 *安装 Faronics Anti-Virus 防病毒*。
3. 选中 *安装 Faronics Anti-Virus 防病毒之前删除所有不兼容的防病毒产品* 复选框，以删除现有的防病毒程序。
4. 单击 *确定* 以确认操作。

工作站将重启，并会在工作站上安装 Anti-Virus 防病毒客户端。

在 *Anti-Virus 防病毒* 选项卡中启用 Anti-Virus 防病毒选项。





## Anti-Virus 配置

Anti-Virus 配置包含所有与 Anti-Virus 在工作站上运行方式相关的设置。配置包含程序进行的操作，计划，代理服务器，错误报告以及工作站上用户可执行的功能。以下各节说明如何创建和应用 Anti-Virus 配置。



Anti-Virus 包含一个默认配置。该默认配置包含管理 Anti-Virus 的最佳配置设置。

### 创建 Anti-Virus 配置

要新建一个 Anti-Virus 配置，请完成以下步骤：

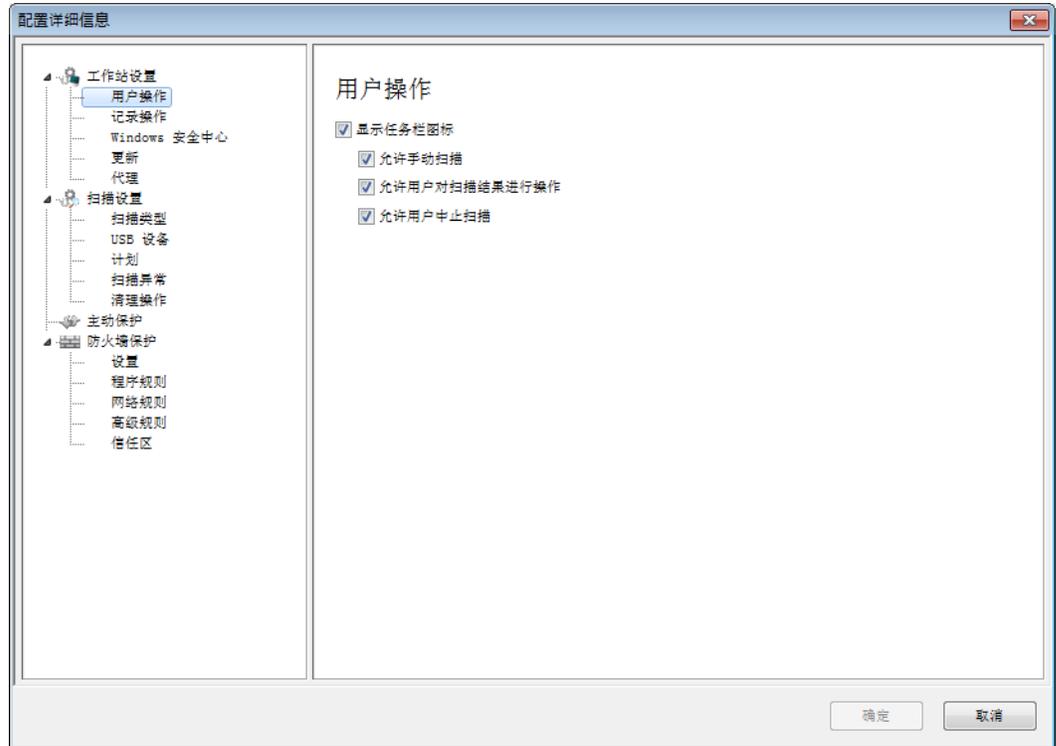
1. 启动企业控制台。
2. 在 *网络和组* 窗格中，转至 *可用配置 > AntiVirus*。
3. 右键单击并选择 *创建新配置*。



4. 指定 *工作站设置* 节点中的设置：



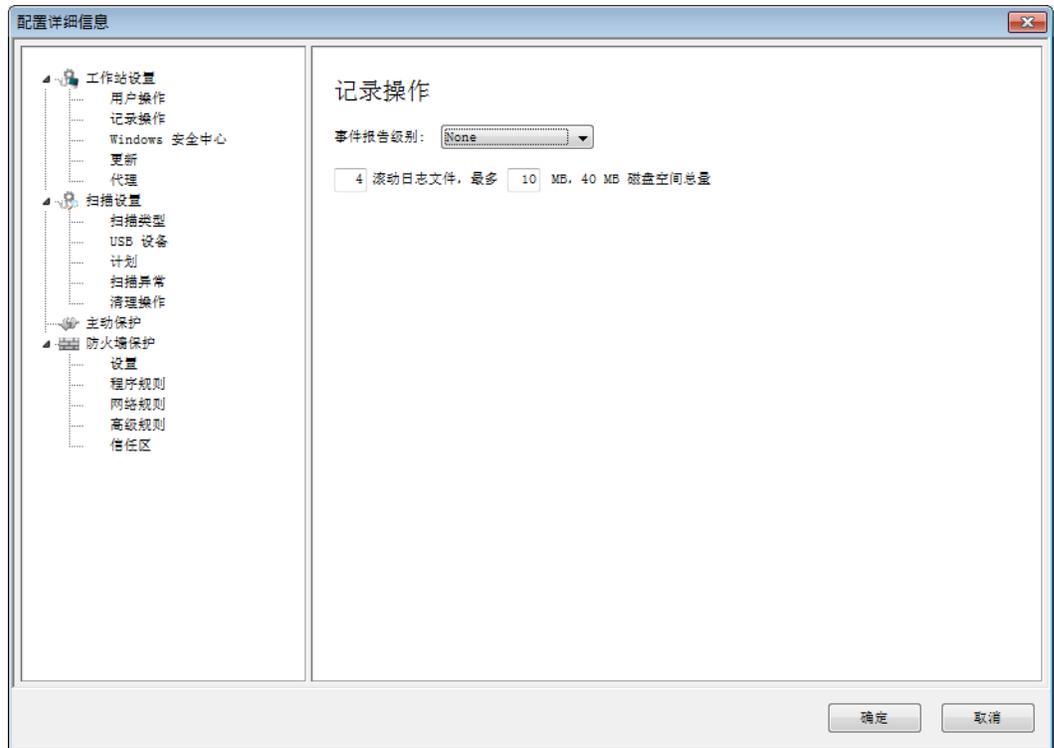
- 用户操作窗格



- > 显示任务栏图标 – 选中此复选框可在工作站的任务栏中显示 Faronics Anti-Virus 防病毒图标。如果没有选中此复选框，则 Faronics Anti-Virus 防病毒将对用户隐藏。
  - ~ 允许手动扫描 – 选中此复选框可允许用户手动启动工作站的 Faronics Anti-Virus 防病毒扫描。
  - ~ 允许用户对扫描结果进行操作 – 选中此复选框可允许工作站用户对扫描结果进行操作。
  - ~ 允许用户中止本地启动扫描 – 选中该复选框可让用户中止在工作站本地启动的扫描。



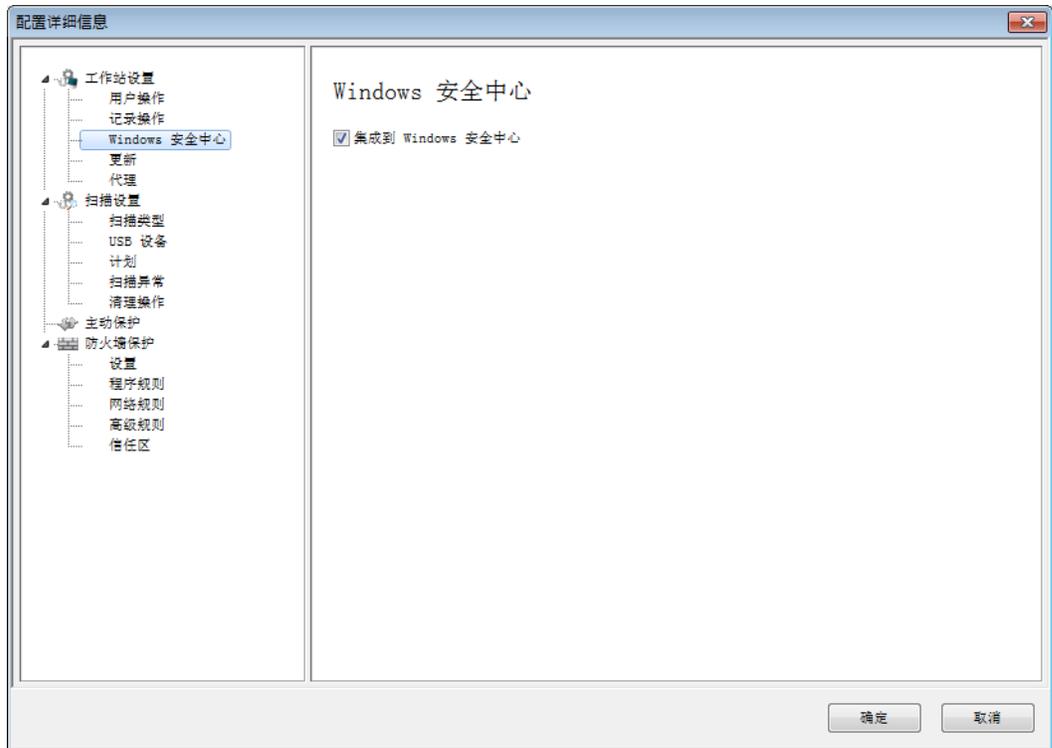
- 记录操作窗格



- > 日志记录级别 – 选择日志记录级别。选择 *无* 不记录日志。选择 *错误* 记录错误消息。选择 *跟踪* 以进行跟踪。选择 *详细* 以详细记录。
- > 日志记录文件数 – 指定日志记录文件的数目。日志记录信息按顺序存储到文件。例如，如果指定了 3 个文件 A、B 和 C，则 Faronics Anti-Virus 防病毒首先将错误日志写入到文件 A。如果文件 A 已满，则开始写入到文件 B，最后写入到文件 C。一旦文件 C 已满，将删除文件 A 中的数据，并写入新的日志记录数据。
- > 文件大小 – 选择每个文件的大小（以 MB 为单位）。



- Windows 安全中心窗格



- > 集成到 Windows 安全中心 – 选中此复选框可将 Faronics Anti-Virus 防病毒集成到 Windows 安全中心。Windows 安全中心将通过系统任务栏通知您 Faronics Anti-Virus 防病毒是否处于活动状态。



- 更新窗格



- > 如果在过去 X 小时内未与 Faronics Core Server 通信，连接到更新 Web 服务器：选中该复选框以连接到 **更新 Web 服务器** 并下载病毒定义（如果工作站与 Faronics Core Server 失去连接）。如果您没有选中此复选框，则工作站与 Faronics Core Server 失去连接时不会更新病毒定义。

- 代理窗格





- > 启用代理 – 如果工作站需要代理访问 Faronics Core Server 或更新 Web 服务器，则选中该复选框。指定地址和端口。
- > 代理服务器信息 – 指定 *地址*和*端口*。
- > 用户身份验证  
代理服务器需要授权（登录凭据）- 如果服务器需要身份验证，请指定以下字段的值：
  - ~ 身份验证类型 – 选择身份验证类型。
  - ~ 用户名 – 指定用户名。
  - ~ 密码 – 指定密码。
  - ~ 域 – 指定域。

#### 5. 指定 *扫描设置*节点中的设置：

- *扫描类型*窗格



Faronics Anti-Virus 提供三种类型的扫描：

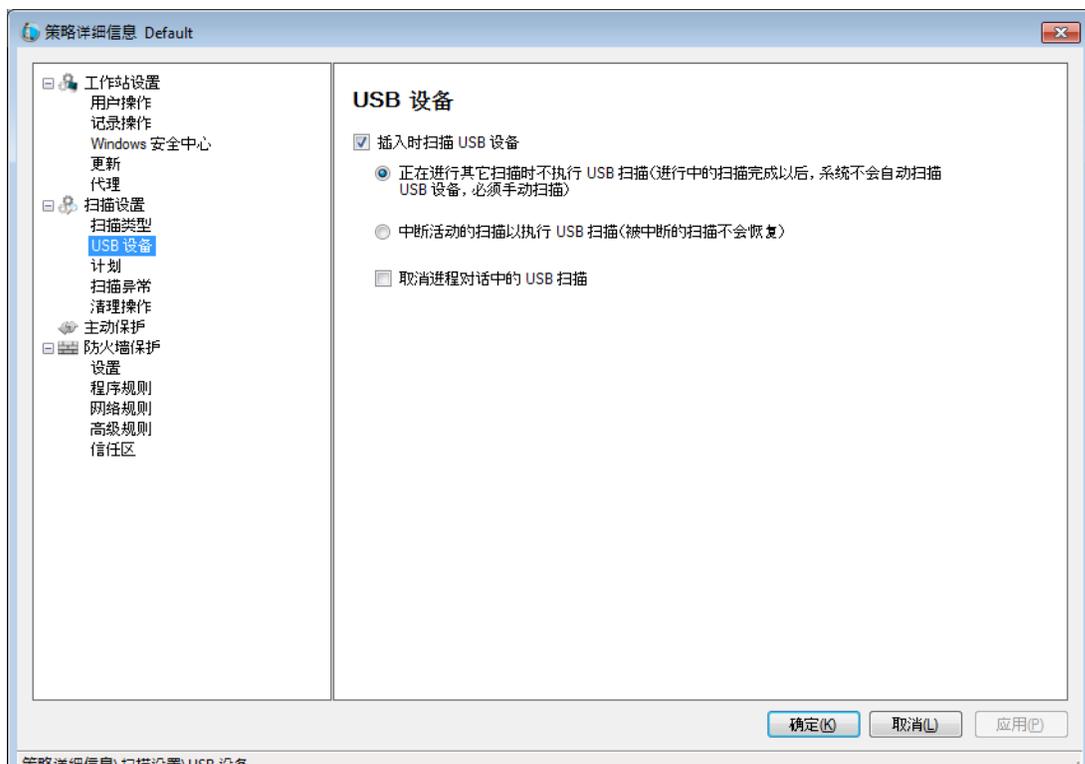
- > 快速扫描 – 扫描计算机中容易受影响的区域。快速扫描比深度系统扫描持续时间短，使用的内存更少。
- > 深度系统扫描 – 对计算机的所有区域进行全面扫描。这类扫描所花的时间取决于您的硬盘驱动器大小。
- > 自定义扫描 – 基于 *策略详细信息*对话框中所做的选择进行扫描。

为每种类型的扫描选择以下选项（视扫描类型的不同，某些选项可能会灰显，无法使用）：

- > 启用 Rootkit 检测 – 检测计算机是否感染 Rootkit。



- > 扫描压缩包 – 扫描 zip 文件中的内容。选中该选项，在扫描时扫描存档文件（例如，.RAR 和 .ZIP 文件）。当发现 .RAR 文件内包含受感染的文件时，将隔离该 .RAR 文件。如果发现 .ZIP 文件内包含受感染的文件，则受感染的文件会被隔离，并替换为一个说明该文件受到感染而已被隔离的 .TXT 文件。指定文件大小限制。
  - > 排除可移动驱动器（例如，USB）— 从扫描进程中排除可移动驱动器。此时将不会扫描任何外部硬盘，USB 驱动器等。
  - > 扫描注册表 – 扫描注册表。
  - > 扫描正在运行的进程 – 扫描所有正在运行的进程。
- USB 设备窗格



插入时扫描 USB 驱动器 – 选中该复选框以在插入时扫描 USB 驱动器，并选择以下选项之一：

- > 正在进行其他扫描时不执行 USB 扫描 – 选择此选项可确保活动的扫描不会因 USB 驱动器的插入而中断。活动的扫描完成后，必须手动扫描 USB 驱动器。
- > 中断活动的扫描以执行 USB 扫描 – 选择此选项可在 USB 驱动器插入时，中断活动的扫描以执行 USB 扫描。活动的扫描一旦中断，将无法自动恢复，必须手动重启。
- > 抑制进行中的 USB 扫描对话 – 选择该选项可隐藏反病毒程序正在扫描所插入的 USB 驱动器的指示；无反病毒程序界面打开，系统托盘图标将不显示工具提示框来表明扫描正在进行中。如发现病毒，用户将在扫描结束后收到通知；如未检测到病毒，用户将不会收到扫描通知。

注意，如果插入时扫描 USB 驱动器选项未选择，该选项将被忽略。



如果 *工作站设置* 选项卡 > *用户操作* 窗格中的 *允许手动扫描* 复选框已选中，则系统会自动扫描 USB 设备。如果 *允许手动扫描* 复选框未选中，则系统不会自动扫描 USB 设备。



- 计划窗格



#### 快速扫描：

- > 启用快速扫描 – 选中此复选框可启用 *快速扫描*。
- > 启动 – 指定开始时间。
- > 停止 – 指定结束时间。启动时间与停止时间之间间隔不得超过 23.59 小时。如果所有文件在 *停止时间* 以前扫描完毕，则扫描结束。如果扫描在 *停止时间* 尚未完成，则会在 *停止时间* 中止扫描。或者，选择 *扫描完成时* 以确保扫描完成。
- > 天 – 选择执行已排程快速扫描的日期。

#### 深度扫描：

- > 启用深度扫描 – 选中此复选框可启用 *深度扫描*。
- > 启动 – 指定开始时间。
- > 停止 – 指定结束时间。*启动时间*与*停止时间*之间间隔不得超过 23.59 小时。如果所有文件在 *停止时间* 以前扫描完毕，则扫描结束。如果扫描在 *停止时间* 尚未完成，则会在 *停止时间* 中止扫描。或者，选择 *扫描完成时* 以确保扫描完成。
- > 天 – 选择执行已排程深度扫描的日期。



选项：

- > 以 x 分钟为单位随机排程扫描开始时间 – 指定分钟数。随机排程扫描开始时间以减少对网络流量的影响。Faronics Anti-Virus 将在扫描开始时向 Faronics Core 报告。如果同时开始对多个系统进行扫描，可能会影响网络流量。

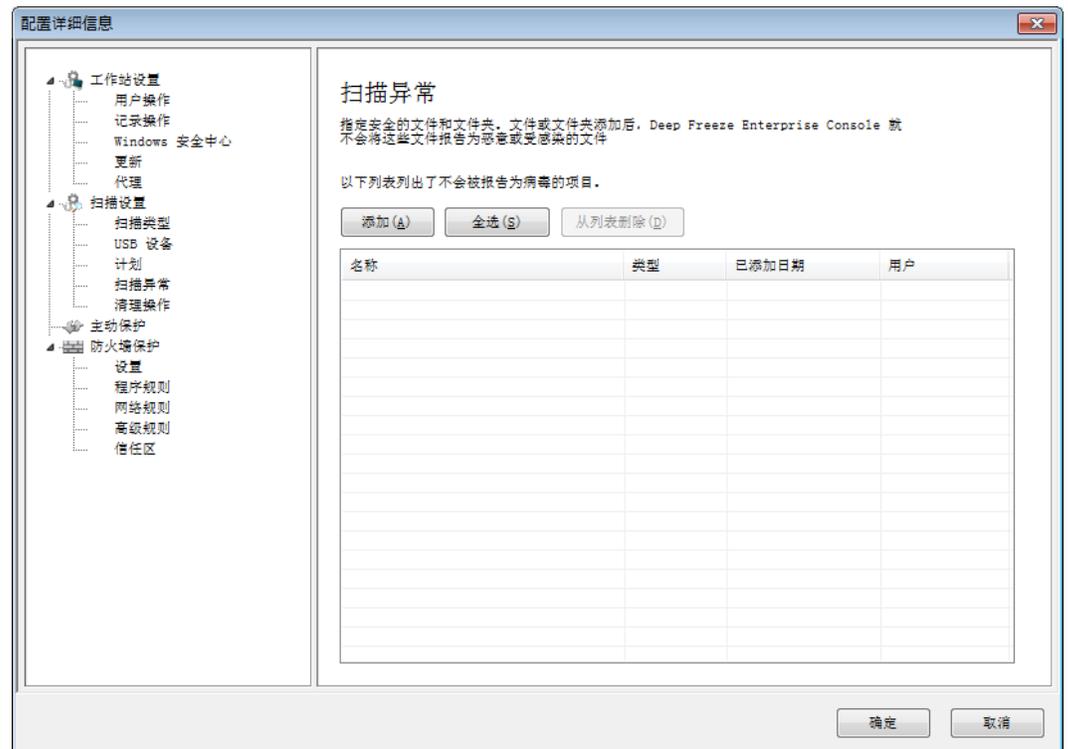
启动时未执行的扫描选项：如果排程扫描期间工作站没有 *开启*，选择以下任何一项扫描执行方式：

- > 不执行快速扫描 – 如果您不想在启动时执行快速扫描，请选择此选项。
- > 大约启动 x 分钟后执行快速扫描 – 指定 Faronics Anti-Virus 防病毒应在启动多少分钟后执行快速扫描。
- > 提示用户执行快速扫描 – 选择此选项可提示用户执行快速扫描。

- *扫描例外窗格*中的设置

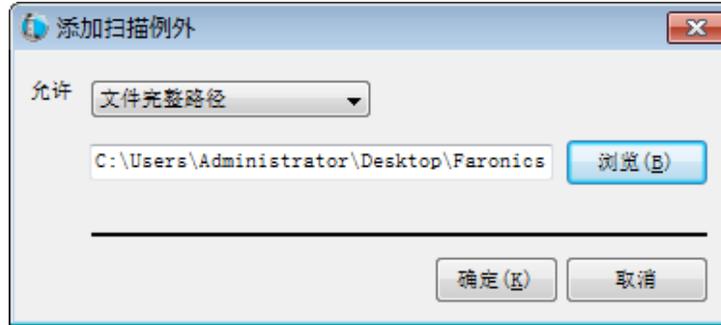
已经确认安全和没有感染的文件夹或文件可以添加到 *扫描例外*选项卡中。添加到 *扫描例外*选项卡的文件将始终被 Faronics Anti-Virus 防病毒扫描。但是，Faronics Anti-Virus 防病毒不会将这些文件报告为恶意或被感染。此功能很实用，因为管理员确认安全的文件和文件夹将不会被报告为恶意。

A. 单击 **添加**。

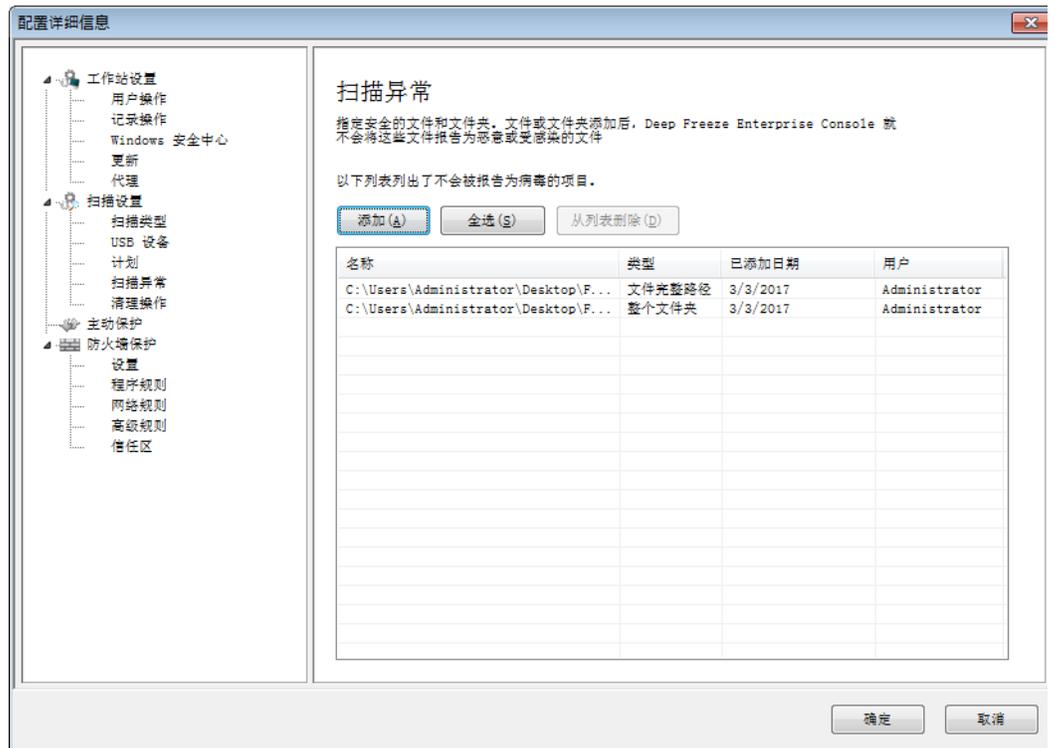




- B. 在添加对话框中，选择文件完整路径，或整个文件夹。单击浏览以选择文件或文件夹，然后单击确定。

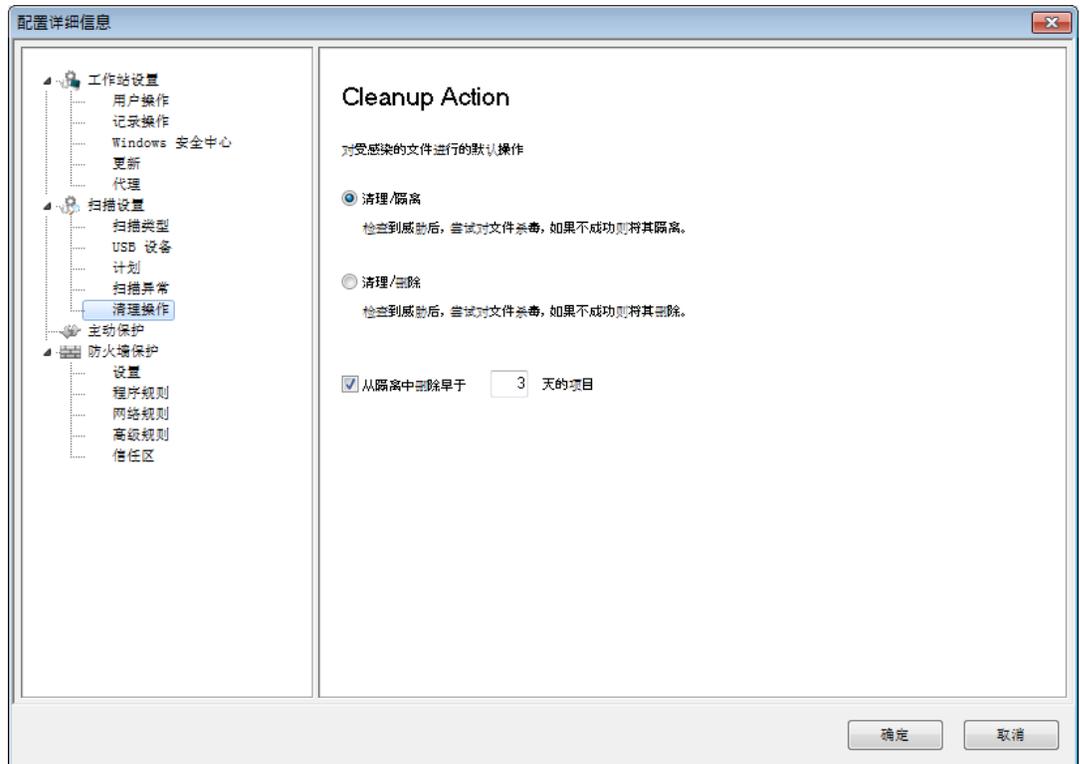


- C. 文件完整路径将添加到扫描例外窗格中。





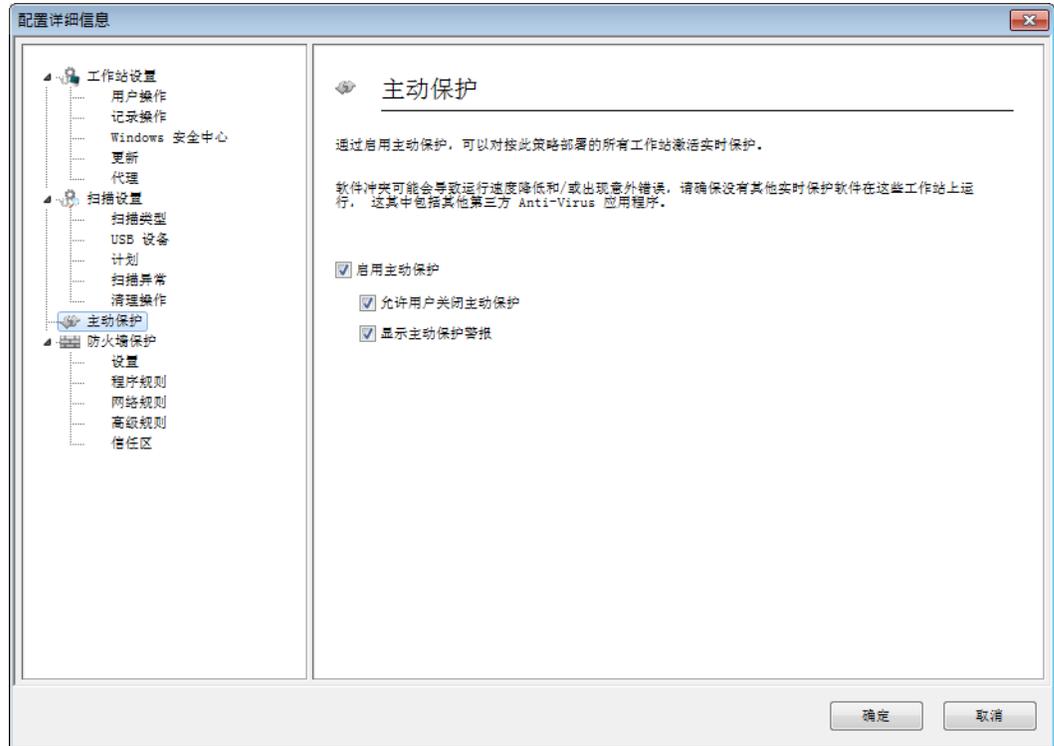
- 清理操作窗格



- > 清理 / 隔离 - 检查到威胁后，尝试对文件杀毒，如果不成功则将其隔离。
- > 清理 / 删除 - 检查到威胁后，尝试对文件杀毒，如果不成功则将其删除。
- > 删除隔离区中早于以下时间的项目 - 指定项目在隔离区中保留的天数。默认为 3 天。



## 6. 指定主动保护窗格中的设置：



- 启用主动保护 – 选择此选项可启用实时保护。主动保护是指 Faronics Anti-Virus 防病毒在后台进行实时扫描，不会对系统性能产生任何影响。如果存在实时从 Internet 感染病毒的风险，请选择此选项。
  - > 允许用户关闭主动保护 – 选择此选项可允许用户关闭主动保护。如果用户安装或使用了可能被误认为病毒的软件（例如，在 Microsoft Office 中运行的高级宏或复杂的批处理文件），请选择此选项。
  - > 显示主动保护警报 – 选择此选项可在主动保护期间检测到威胁时显示警报。如果不希望显示警报，请不要选中此复选框。



## 7. 指定 *防火墙保护* 节点中的设置：

防火墙保护节点可提供双向防护，同时限制入站和出站流量。您可以通过创建自定义规则来保护网络。您可 *允许* 或 *阻止* 通信。

- 设置窗格



### 防火墙保护设置

- > 启用防火墙保护 – 选中此复选框可启用防火墙保护。防火墙保护可阻止黑客或恶意软件通过 Internet 或网络获取对您计算机的访问权限。
  - ~ 允许用户禁用防火墙 – 选择此选项可允许用户在计算机上禁用防火墙。

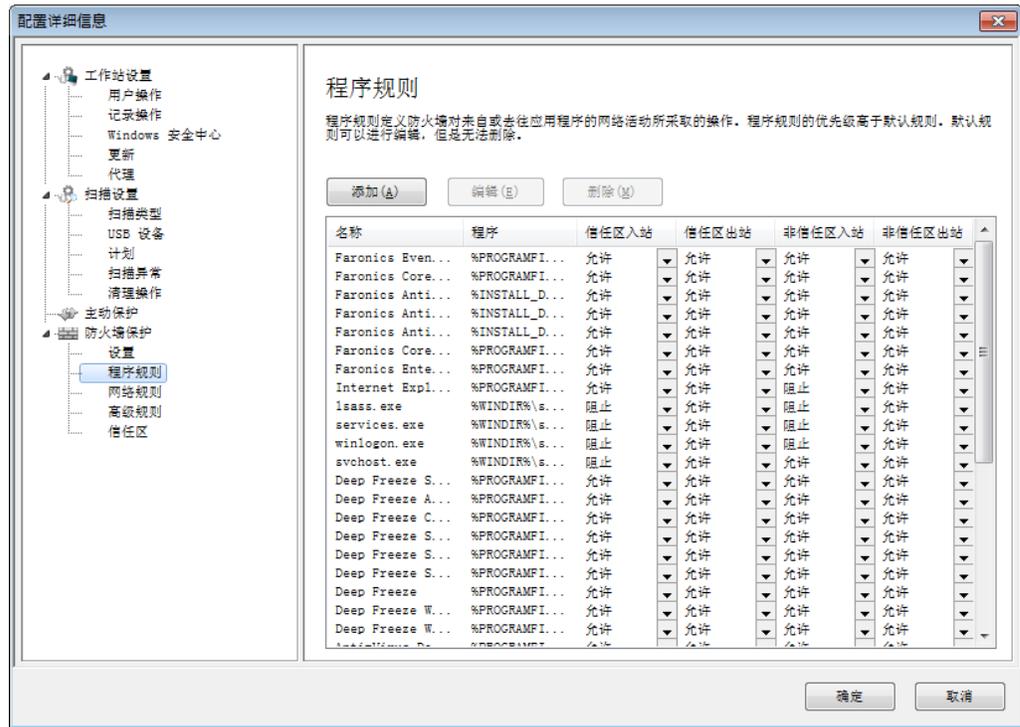
### 防火墙日志记录

- > 启用防火墙日志记录 – 选择此选项可将防火墙有关的所有操作进行日志记录。



- 程序规则窗格

程序规则定义防火墙对来自或去往应用程序的网络活动所采取的操作。程序规则的优先级高于默认规则。默认规则可以进行编辑，但是无法删除。



单击**添加**以添加新程序规则。指定或选择选项，然后单击**确定**。此时将显示以下参数：





- > 名称 – 规则的名称。
  - > 程序 – 程序的名称，包括完整路径和扩展名。
  - > 信任区入站 – 对去往信任区程序的入站通信应执行的操作（允许或阻止）。
  - > 信任区出站 – 对来自信任区程序的出站通信应执行的操作（允许或阻止）。
  - > 非信任区入站 – 对去往非信任区程序的入站通信应执行的操作（允许或阻止）。
  - > 非信任区出站 – 对来自非信任区程序的入站通信应执行的操作（允许或阻止）。
- 网络规则窗格

网络规则定义防火墙对网络活动所采取的操作。这类规则可以进行编辑，但是无法删除。





为以下选项选择网络规则：

名称	描述	信任区入站	信任区出站	非信任区入站	非信任区入站
IGMP	Internet 组管理协议	选择允许或阻止	选择允许或阻止	选择允许或阻止	选择允许或阻止
Ping	Ping 以及 Tracert	选择允许或阻止	选择允许或阻止	选择允许或阻止	选择允许或阻止
其他 ICMP	其他 ICMP 包	选择允许或阻止	选择允许或阻止	选择允许或阻止	选择允许或阻止
DHCP	动态主机配置协议	选择允许或阻止	选择允许或阻止	选择允许或阻止	选择允许或阻止
DNS	域名系统	选择允许或阻止	选择允许或阻止	选择允许或阻止	选择允许或阻止
VPN	虚拟专用网络	选择允许或阻止	选择允许或阻止	选择允许或阻止	选择允许或阻止
BCAST	发布	选择允许或阻止	选择允许或阻止	选择允许或阻止	选择允许或阻止
LDAP	轻量级目录访问协议	选择允许或阻止	选择允许或阻止	选择允许或阻止	选择允许或阻止
Kerberos	Kerberos P 协议	选择允许或阻止	选择允许或阻止	选择允许或阻止	选择允许或阻止
NETBIOS	Microsoft 文件和打印机共享	选择允许或阻止	选择允许或阻止	选择允许或阻止	选择允许或阻止



- 高级规则窗格

高级规则可以定义防火墙针对指定应用程序，端口或协议所采取的操作。其中可能包括单个协议，本地或远程端口以及流量方向，或者是它们的组合。您可以添加，编辑或删除高级规则。



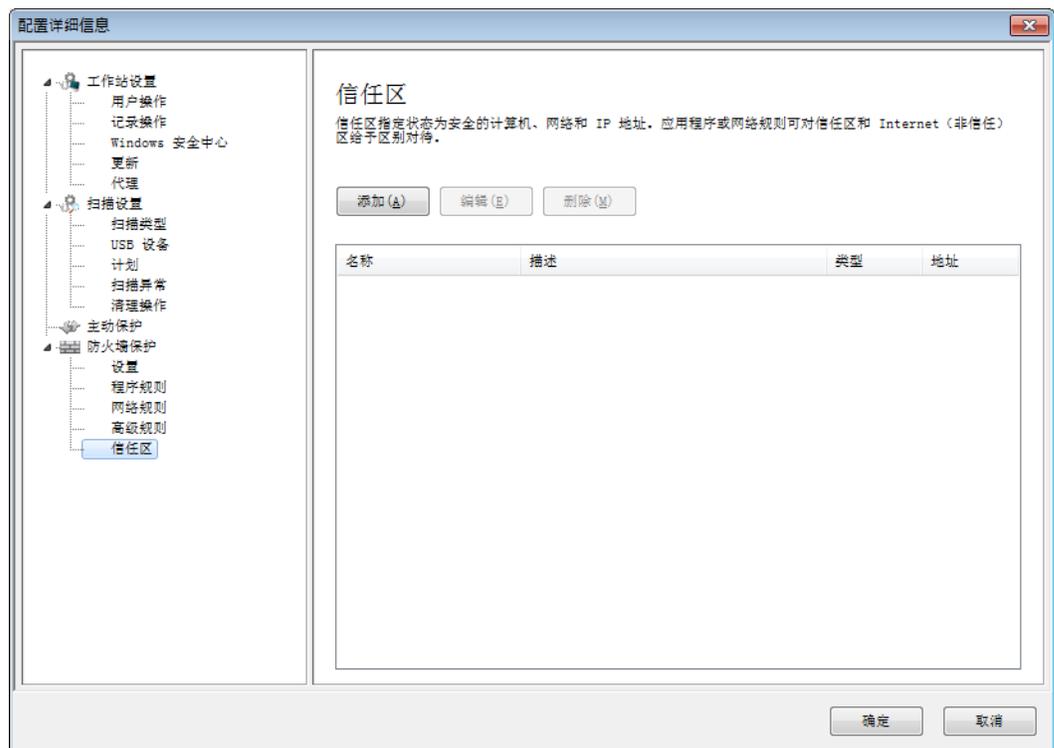
单击 **添加** 以添加新高级规则。指定或选择选项，然后单击 **确定**。在 **高级规则** 窗格中将显示下列参数：





- > 名称 – 规则的名称。
- > 程序 – 程序的名称和路径。
- > 操作 – 防火墙对来自指定的应用程序、端口或协议的通信所采取的操作（允许、阻止或）。
- > 方向 – 通信的方向（双向、入站或出站）。
- > 协议 – 协议的名称。
- > 本地端口 – 本地端口的详细信息。
- > 远程端口 – 远程端口的详细信息。
- 信任区窗格

信任区指定受信任的计算机、网络和 IP 地址。程序和网络规则可对信任区和 Internet（非信任）区给予区别对待。



单击 **添加** 可添加新的信任区。指定或选择选项，然后单击 **确定**。此时将显示以下参数：





- > 名称 – 信任区的名称。
  - > 说明 – 信任区的说明。
  - > 类型 – 信任区的类型 ( IP 地址或网络)。
8. 单击 *确定*。此时新策略 *New Policy 1* 将在 *Anti-Virus* 节点下显示。

## 应用 Anti-Virus 配置

要应用 Anti-Virus 配置，请完成以下步骤：

1. 转至 *工作站* 窗格。
  2. 选择一个或多个工作站。
  3. 右键单击一个或多个工作站，然后选择 *更新配置* > *Anti-Virus* > [配置名称]。
- 该配置将应用至所选工作站。



配置更改将自动应用到联机工作站。如果工作站处于脱机状态，则配置更改将在工作站恢复联机时应用。

## 编辑 Anti-Virus 配置

要编辑 Anti-Virus 配置，请完成以下步骤：

1. 转至企业控制台的 *网络和组* 窗格。
2. 选择 *可用配置* > *Anti-Virus* > [配置名称]。
3. 右键单击所选配置，然后选择 *编辑所选配置*。
4. 根据需要编辑设置。
5. 单击 *确定*。

## 删除 Anti-Virus 配置

要删除 Anti-Virus 配置，请完成以下步骤：

1. 转至企业控制台的 *网络和组* 窗格。
2. 选择 *可用配置* > *Anti-Virus* > [配置名称]。
3. 右键单击所选配置，然后选择 *删除所选配置*。
4. 单击 *确定*。



## 从企业控制台使用 Faronics Anti-Virus

在工作站上安装 Faronics Anti-Virus 后，可以通过 Deep Freeze 控制台在工作站上执行各种操作。

### Anti-Virus 命令

通过 Deep Freeze 控制台有两种方法执行相同的命令：

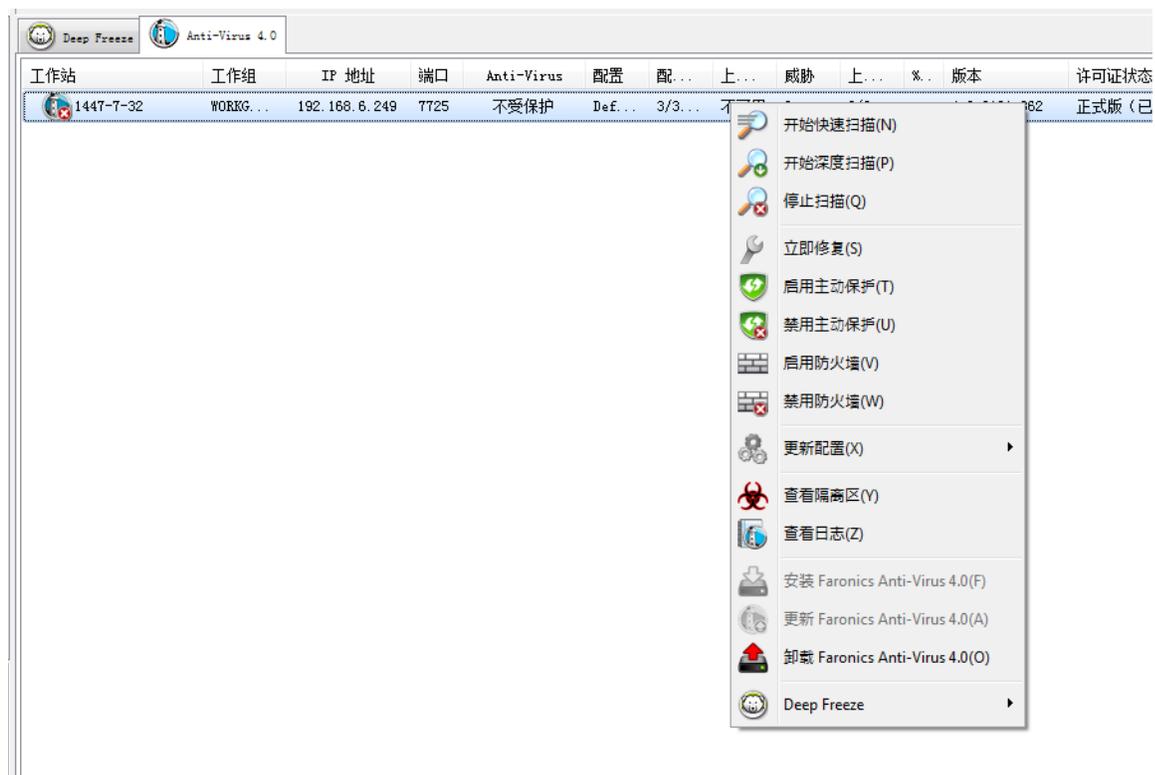
- Anti-Virus 菜单（在菜单栏上）
- Anti-Virus 上下文菜单（右键单击上下文菜单）

本节将详细介绍菜单命令。

Anti-Virus 菜单提供以下命令：



工作站窗格 > *Anti-Virus* 选项卡 > 右键单击上下文菜单提供相同的命令：





## 快速扫描

快速扫描会检查计算机中容易受影响的区域。快速扫描比深度系统扫描持续时间短，使用的内存更少。

- 要开始快速扫描  
选择一个或多个工作站。右键单击并选择 *开始快速扫描*。
- 要停止快速扫描  
选择一个或多个工作站。右键单击并选择 *停止扫描*。
- 要暂停快速扫描  
选择一个或多个工作站。右键单击并选择 *暂停扫描*。
- 要恢复快速扫描  
选择一个或多个工作站。右键单击并选择 *恢复扫描*。

## 深度扫描

深度系统会扫描对计算机的所有区域进行全面扫描。这类扫描所花的时间取决于您的硬盘驱动器大小。

- 要开始深度扫描  
选择一个或多个工作站。右键单击并选择 *开始深度扫描*。
- 要停止深度扫描  
选择一个或多个工作站。右键单击并选择 *停止深度扫描*。
- 要暂停深度扫描  
选择一个或多个工作站。右键单击并选择 *暂停扫描*。
- 要恢复深度扫描  
选择一个或多个工作站。右键单击并选择 *恢复扫描*。

## 立即修复

*立即修复*选项用于下载最新的病毒定义并在工作站上执行快速扫描。

- 要立即修复  
选择一个或多个工作站。右键单击并选择 *立即修复*。



## 主动保护

主动保护 (AP) 是一种实时检测恶意程序的方法。AP 在您工作或浏览 Internet 时安静地驻守在后台，一直监视执行（运行）的文件而不会对您的系统造成显著的压力。

- 要启用主动保护  
选择一个或多个工作站。右键单击并选择 *启用主动保护*。
- 要禁用主动保护  
选择一个或多个工作站。右键单击并选择 *禁用主动保护*。

## 防火墙

防火墙可以提供双向防护，同时限制入站和出站流量，从而保护您的网络免受非法入侵。

- 要启用防火墙  
选择一个或多个工作站。右键单击并选择 *启用防火墙*。
- 要禁用防火墙  
选择一个或多个工作站。右键单击并选择 *禁用防火墙*。

## 发送消息

*发送消息*选项用于向联机工作站发送消息。

- 要发送消息  
选择一个或多个工作站。右键单击并选择 *发送消息*。

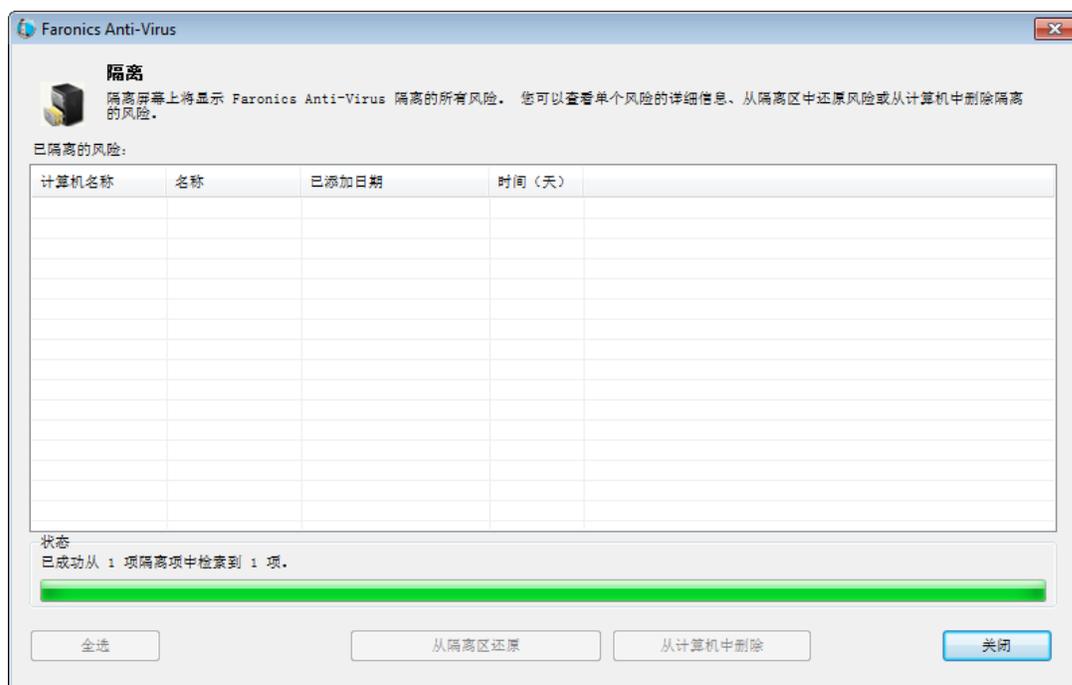
## 查看隔离信息

隔离区是指 Faronics Anti-Virus 在计算机上用于存储恶意程序或无法杀毒的受感染文件的安全位置。如果将某一项目存放到该位置后，您的计算机或计算机上的文件无法正常操作，您可以查看风险详细信息以进行进一步研究，并将其从隔离区删除，还原到其在计算机中原来的位置。您还可以从隔离区中永久删除该风险。



- 要查看隔离区

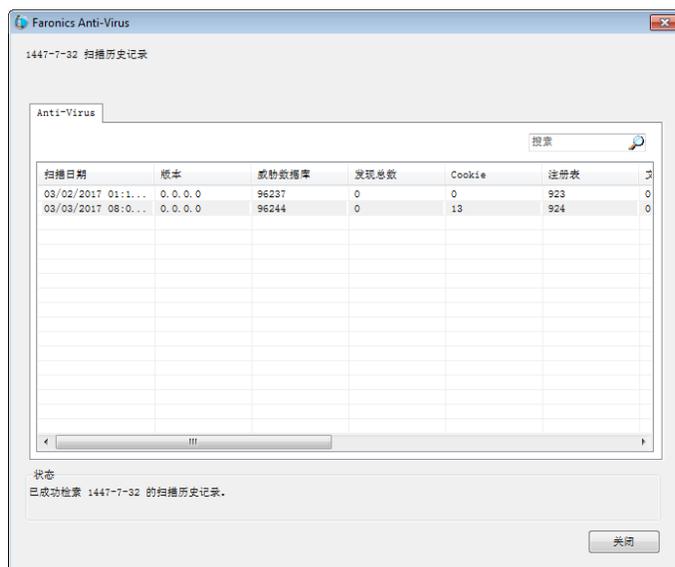
选择一个或多个工作站。右键单击并选择 *Faronics Anti-Virus* > 获取隔离详细信息。



## 查看扫描历史记录

Faronics Anti-Virus 防病毒扫描历史记录显示 Faronics Anti-Virus 防病毒在工作站上执行的所有任务。

选择一个工作站，右键单击并选择 *查看扫描历史记录* 以查看日志信息。





## 计划 Anti-Virus 任务

---

可以根据预定义计划从 Deep Freeze 控制台运行以下 Anti-Virus 任务。

- 禁用主动保护
- 启用主动保护
- 开始快速扫描
- 开始深度扫描

[计划 Deep Freeze 任务](#)一节中详细介绍了如何计划任务。



## 在工作站上使用 Anti-Virus

工作站上 Anti-Virus 中可用的功能完全取决于 Anti-Virus 配置中所选的设置。有关 Anti-Virus 配置的详细信息，请参阅 [Anti-Virus 配置](#)。

### 在工作站上启动 Anti-Virus

依次转至 *开始 > 程序 > Faronics > Anti-Virus Enterprise > Faronics Anti-Virus Enterprise*。或者，您可以双击系统任务栏中的 Faronics Anti-Virus 图标。



以下窗格将向用户显示重要信息：

- 显示 *受保护* 或 *不受保护*，指示计算机是否受到保护。如果显示 *不受保护*，请单击 *不受保护* 标志下的 *立即修复* 按钮。
- *扫描状态* 显示上次扫描的时间。要立即扫描，请单击 *立即扫描* 链接。
- *更新状态* 显示上次更新的时间。要更新病毒定义，请单击 *立即更新* 链接。
- *主动保护* 显示是否启用实时保护。
- *防火墙保护* 显示工作站是否受到防火墙的保护。
- *风险检测统计* 显示 Faronics Anti-Virus 所执行操作的统计信息。单击 *重置计数* 可将计数清零。



## 扫描工作站

要扫描工作站，请完成以下步骤：

1. 依次转至 *开始 > 程序 > Faronics > Anti-Virus Enterprise > Faronics Anti-Virus Enterprise*。或者，您可以双击系统任务栏中的 Faronics Anti-Virus 图标。



2. 在 *扫描状态* 窗格中，单击 *立即扫描*。此时将显示 *扫描* 选项卡。或者，您可以单击 *扫描* 选项卡。





3. 选择以下选项之一：
  - > 快速扫描 – 仅扫描已知的威胁。
  - > 深度系统扫描 – 详细扫描工作站上的所有文件。
  - > 自定义扫描（选择以下各项之一）：
    - ~ 扫描正在运行的进程 – 扫描工作站上正在运行的进程。
    - ~ 扫描注册表 – 扫描注册表。
    - ~ 指定要扫描的驱动器和文件夹 – 单击 *浏览* 并选择文件夹。
4. 单击 *立即扫描*。旋转的图标表示正在进行扫描。扫描完成后将显示扫描结果。
5. 选择文件，系统将显示以下选项：
  - > 依次选择 *更改清除操作* > *建议操作* 以执行 Faronics Anti-Virus 建议的操作。
  - > 依次选择 *更改清除操作* > *隔离/杀毒* 以隔离该文件或对其杀毒。
  - > 依次选择 *更改清除操作* > *删除* 以删除该文件。
  - > 依次选择 *更改清除操作* > *允许* 以允许该文件。
  - > 单击 *全选* 以选择 *扫描结果* 中显示的所有文件。
  - > 单击 *详细信息* 以显示风险的详细信息。
  - > 单击 *取消* 以关闭该对话框而不进行任何操作。
  - > 单击 *清除* 以删除文件并关闭该对话框。

## 通过右键单击扫描文件或文件夹

您可以轻松扫描文件或文件夹（一个或多个）有无病毒。当工作站上安装了 Faronics Anti-Virus 时，右键单击菜单中会添加 *扫描病毒* 选项。

要扫描计算机上的文件或文件夹，请完成以下步骤：

1. 右键单击文件或文件夹。
2. 选择 *扫描病毒*。

此时将执行扫描并显示结果。

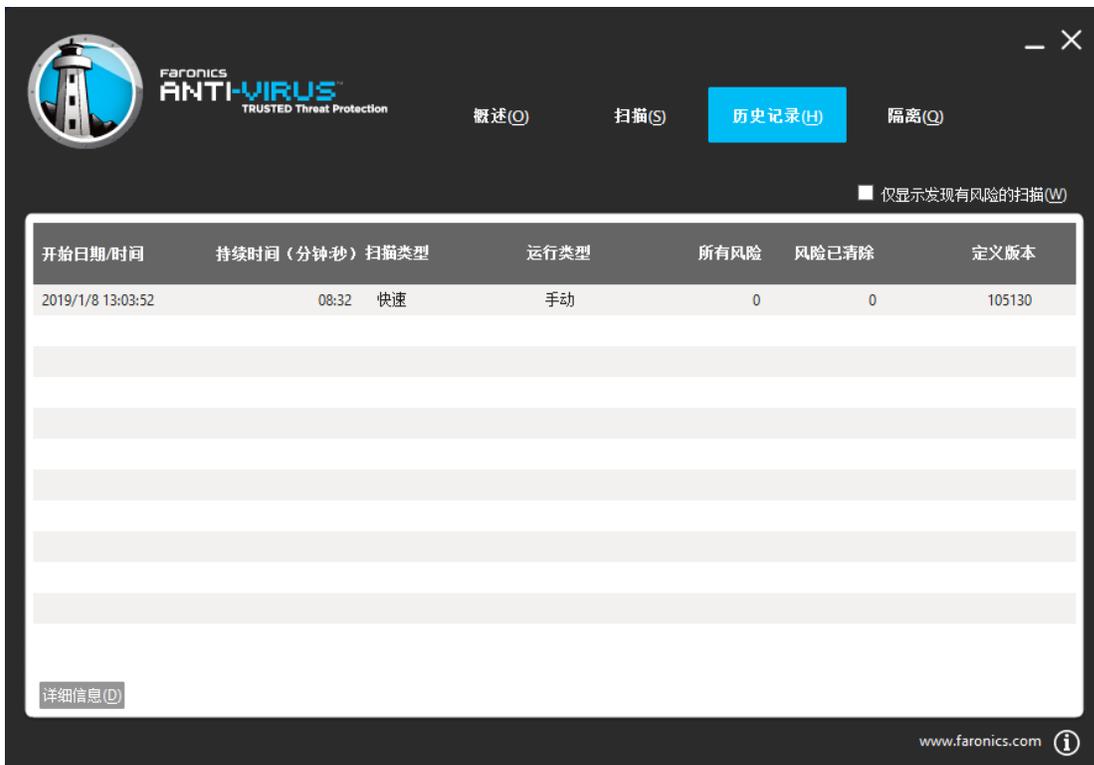
## 查看扫描历史记录

要查看扫描历史记录，请完成以下步骤：

1. 依次转至 *开始* > *程序* > *Faronics* > *Anti-Virus Enterprise* > *Faronics Anti-Virus Enterprise*。或者，您可以双击系统任务栏中的 Faronics Anti-Virus 图标。



2. 单击**历史记录**选项卡。



3. 选择以下操作：

- > 仅显示发现有风险的扫描 – 选择此选项仅查看发现有风险的扫描。
- > 详细信息 – 选择某个条目，然后单击详细信息以查看扫描的详细信息。

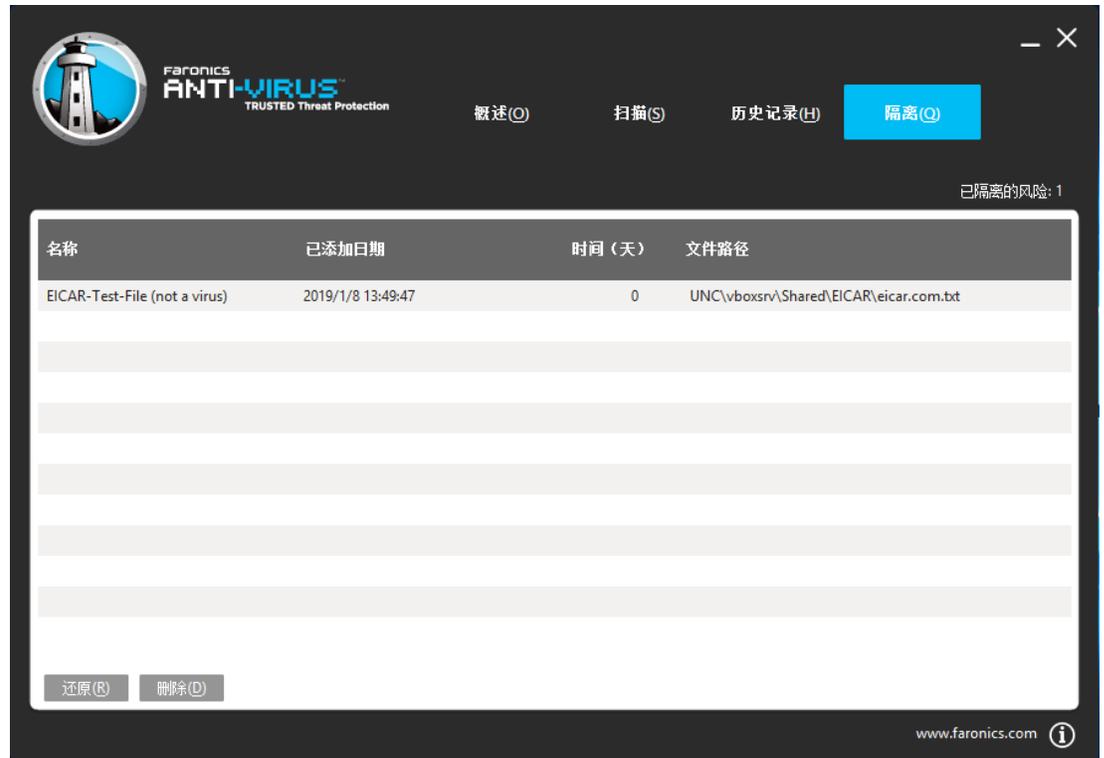
## 查看隔离的文件并对其进行操作

要查看隔离区，请完成以下步骤：

1. 依次转至 **开始 > 程序 > Faronics > Anti-Virus Enterprise > Faronics Anti-Virus Enterprise**。或者，您可以双击系统任务栏中的 Faronics Anti-Virus 图标。



- 单击 *隔离区* 选项卡。



- 单击 *风险详细信息*。将显示每个受感染文件的以下信息：
  - > 名称
  - > 已添加日期
  - > 时间(天)
- 选择以下操作：
  - > 详细信息 – 选择一个文件，然后单击 *详细信息* 以查看受感染文件的详细信息。执行此操作系统也会显示建议的操作。

## 在工作站上更新 Anti-Virus 定义

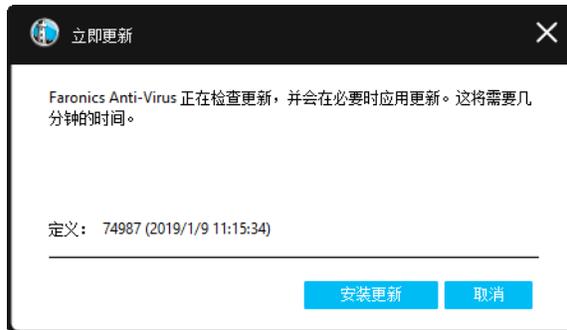
要在工作站上更新 Anti-Virus 定义，请完成以下步骤：



- 依次转至 *开始 > 程序 > Faronics > Anti-Virus Enterprise > Faronics Anti-Virus Enterprise*。或者，您可以双击系统任务栏中的 Faronics Anti-Virus 图标。



- 在 *更新状态* 窗格中，单击 *立即更新*。此时将显示 *立即更新* 对话框。



- 单击 *安装更新*。此时将更新工作站上的病毒定义。

## 通过系统任务栏管理工作站上的 Anti-Virus

Faronics Anti-Virus 可在工作站上通过系统任务栏上的菜单进行管理。右键单击系统任务栏中的 Faronics Anti-Virus 图标。系统将显示以下选项：

- 打开 Faronics Anti-Virus – 启动工作站上的 Faronics Anti-Virus。
- 主动保护
  - > 主动保护 > 启用主动保护 – 启用主动保护。



- > 主动保护 > 禁用主动保护 > [ 选择选项 ] – 选择要禁用主动保护的时间。可选择 5 分钟 · 15 分钟 · 30 分钟 · 1 小时 · *直到计算机重启*或*永久*。仅当在 Anti-Virus 策略中选择了此选项时，此选项方会显示。
- 立即扫描 > [ 选择选项 ] – 可选择 *取消扫描* · *快速扫描*或*深度扫描*。仅当在 Anti-Virus 策略中选择了此选项时，此选项方会显示。
- 防火墙保护 > 启用或禁用



## 检查 Anti-Virus 更新

您可以通过 Deep Freeze 控制台检查是否有更高版本的 Faronics Anti-Virus 可用。访问 [帮助 > 检查更新](#)。此操作将检查是否提供了新版本的 Faronics Anti-Virus。



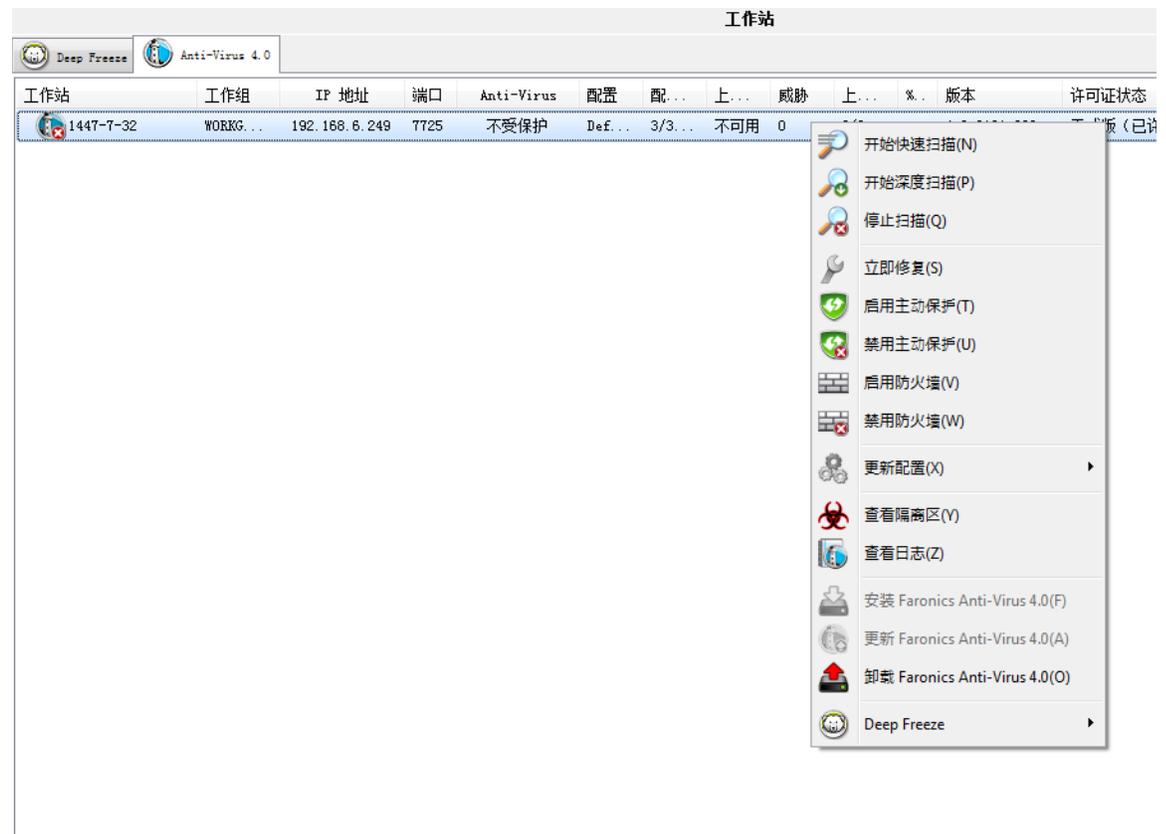
如果有新版本可用，请单击 [下载最新版本](#) 以更新 Faronics Anti-Virus。



## 更新 Faronics Anti-Virus

如果您已检查更新并有新版本可用，请完成以下步骤，以在工作站上更新到更高版本：

1. 转至 *工作站* 窗格中的 *Anti-Virus* 选项卡。
2. 选择一个或多个工作站
3. 右键单击并选择 *更新 Faronics Anti-Virus*。



4. 单击 *确定* 以确认操作。

重新启动工作站，并在工作站上更新 Faronics Anti-Virus 客户端。



## 更新 Anti-Virus 防病毒定义

Anti-Virus 防病毒定义服务器随 Faronics Anti-Virus 一起安装在装有 Deep Freeze 控制台的同一台计算机上。Anti-Virus 防病毒定义服务器下载最新的病毒定义并分发到 Deep Freeze 管理的工作站。

要更新病毒定义，请完成以下步骤：

1. 启动 Deep Freeze 控制台。
2. 转到 **工具 > Anti-Virus 防病毒定义**。
3. 可用的设置和操作如下：



- > Anti-Virus 防病毒定义版本 – 显示当前的 Anti-Virus 防病毒定义版本。
- > 更新设置 – 选中自动更新于复选框，并输入以小时为单位的值。
- > 检查更新设置 – 显示上次更新检查的日期 / 时间和下次更新检查的日期 / 时间。单击立即更新以立即更新病毒定义。显示更新状态。
- > 缓存服务器详情 – 显示当前版本和上次更新检查的日期 / 时间。如果您要自动下载并更新包含最新定义的缓存服务器，请选中自动更新缓存服务器复选框。单击立即更新以立即更新缓存服务器。

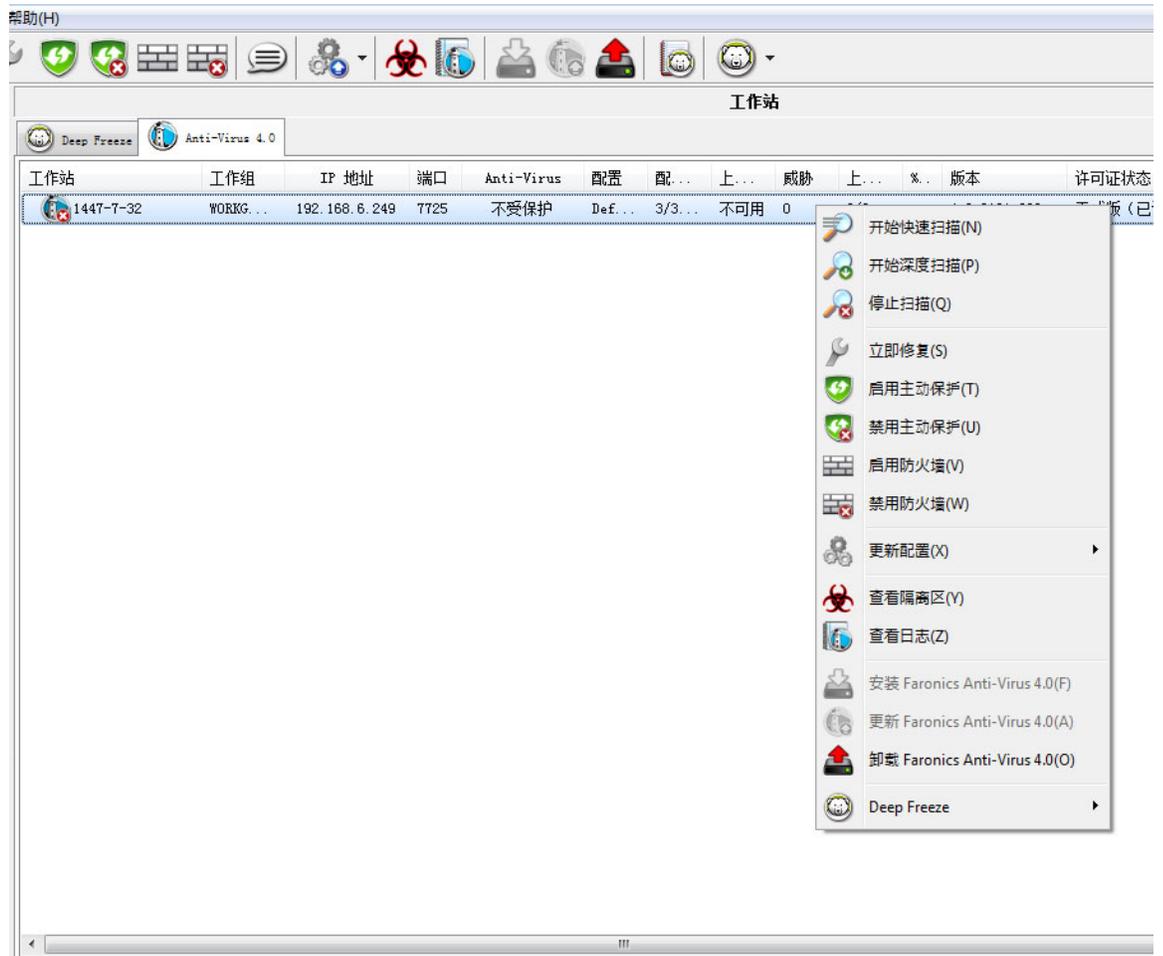
4. 单击 **确定**。



## 从企业控制台卸载 Anti-Virus 客户端

要从企业控制台卸载工作站上的 Faronics Anti-Virus，请完成以下步骤：

1. 转至 *工作站* 窗格中的 *Anti-Virus* 选项卡。
2. 选择一个或多个工作站
3. 右键单击并选择 *卸载 Faronics Anti-Virus*。



4. 单击 *确定* 以确认操作。

重新启动工作站，并在工作站上卸载 Faronics Anti-Virus 客户端。



如果 Anti-Virus 客户端从工作站卸载，Deep Freeze 种子将会留下。在工作站上安装 Anti-Virus 客户端后，Deep Freeze 种子将无法卸载。



## 从企业控制台禁用 Faronics Anti-Virus

如果无需使用 Anti-Virus，可以从企业控制台将其禁用。

要从 Deep Freeze 控制台禁用 Faronics Anti-Virus，请完成以下步骤：

1. 依次转至 **工具 > 许可 > Faronics Anti-Virus 许可证**。
2. 取消选中 **我想使用 Deep Freeze 控制台来管理 Faronics Anti-Virus** 复选框。



3. 单击**关闭**。
4. 重新启动企业控制台以使设置生效。



# Deep Freeze 命令行控制

本章介绍如何使用 Deep Freeze 命令。

## 主题

---

[Deep Freeze 命令行控制 \(DFC.EXE\)](#)

[DFC 命令行语法](#)

[Faronics Anti-Virus 命令行语法](#)



## Deep Freeze 命令行控制 (DFC.EXE)

Deep Freeze 的 *命令行控制* (DFC) 功能可帮助网络管理员提高管理 Deep Freeze 计算机的灵活性。DFC 能够与第三方企业管理工具和 / 或中央管理解决方案结合使用。通过结合使用它们，管理员可根据需要方便快捷地更新计算机。

需要特别注意的是，DFC 并非一套独立的应用程序。它可以与任何支持运行脚本文件（包括标准 RunOnce 登录脚本）的解决方案进行无缝集成。

使用 DFC 命令需要提供具有命令执行权限的密码，而不能使用 OTP。

调用不带参数的 DFC 时可以列出所有命令。

文件将复制到 (32-bit)

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

文件将复制到 (64-bit)

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

### DFC 返回值

DFC 命令执行完毕后，会返回下列值：

语法	说明
0	对于返回布尔型结果的命令，代表 SUCCESS 或布尔值 False
1	布尔值 True
2 错误	用户无管理员权限
3 错误	DFC 命令对于此安装无效
4 错误	命令无效
5 - * 错误	执行命令时出现内部错误



## DFC 命令行语法



Deep Freeze 的密码最长限制为 63 个字符。如果输入的密码超出此限制，命令将不会成功执行。

语法	说明
DFC password /BOOTTHAWED	将计算机重启后解冻，仅适用于冻结的计算机。
DFC password /THAWNEXTBOOT	将计算机设置为下次重启后解冻；仅适用于冻结的计算机，且不强制计算机重启。
DFC password /BOOTFROZEN	将计算机重启后冻结，仅适用于解冻的计算机。
DFC password /FREEZENEXTBOOT	将计算机设置为下次重启后冻结；仅适用于解冻的计算机，且不强制计算机重启。
DFC get /ISFROZEN	询问计算机是否处于冻结状态。处于解冻状态时返回错误级别 0，处于冻结状态时返回 1。
DFC password /CFG=[path] depfrz.rdx	替换 Deep Freeze 配置信息。同时适用于冻结和解冻状态的计算机。密码更改当即生效，而其他更改需要重启后才能生效。
DFC get /CLONE	出于映像目的设置克隆标志。
DFC get /version	显示 Deep Freeze 版本号。
DFC password /UPDATE=[ 安装 程序文件路径 ]	将计算机设置为重启后解冻并安装 Deep Freeze 更新。
DFC password /LOCK	在计算机上禁用键盘和鼠标。适用于冻结和解冻的计算机，且不要求重启。
DFC password /UNLOCK	在计算机上启用键盘和鼠标。适用于冻结和解冻的计算机，且不要求重启。
DFC password /THAWLOCKNEXTBOOT	将计算机设置为重启后解冻并禁用键盘和鼠标；仅适用于冻结的计算机。



语法	说明
DFC password /BOOTTHAWEDNOINPUT	将计算机重启后解冻并禁用键盘和鼠标；仅适用于冻结的计算机
DFC get /LICENSESTATUS	<p>显示许可证状态及许可证的过期日期（如果有）。可能的许可证类型和相关的返回代码包括：</p> <p>111：未许可 – Deep Freeze 未获得许可，安装后将以 <i>评估</i> 模式工作 30 天。</p> <p>112：评估 – 获得评估使用许可，具有固定过期日期。</p> <p>113：已许可 – 获得许可，无过期日期。</p> <p>114：过期 – 评估期已结束。</p>
DFC get /LICENSETYPE	<p>显示许可证状态及许可证的过期日期（如果有）。可能的许可证类型和相关的返回代码包括：</p> <p>111：无（未许可） – Deep Freeze 未获得许可，安装后将以 <i>评估</i> 模式工作 30 天。</p> <p>112：评估 – 获得评估使用许可，具有固定过期日期。</p> <p>113：标准（已许可） – 获得许可，无过期日期。</p> <p>114：非零售 – 获得许可，无过期日期。</p> <p>115：订阅版</p> <p>116：订阅评估版</p> <p>117：订阅版不得转售</p>
DFC password /LICENSE=licensekey	<p>更改许可证密钥。</p> <p><i>password</i> 是 Deep Freeze 管理员密码。</p> <p><i>licensekey</i> 是 Deep Freeze 的许可证密钥。</p> <p>如果有错误，将显示下列错误代码：</p> <p>101：许可证密钥无效</p> <p>102：提供的许可证密钥已过期。</p>
DFC password /ACTIVATE	检查 Faronics 许可激活服务器之后激活工作站。



语法	说明
<code>DFC get /ACTIVATION</code>	显示 Deep Freeze 许可激活状态。 返回以下值： 0：待激活 1：生效中 2：已授权 3：已取消激活 4：未授权
<code>DFC password /WU [/UNLOCK] [/NOMSG   /NOMESSAGE] [/THAW]</code>	Windows 更新将被下载并安装在工作站上。 [/ UNLOCK] 可选的参数，使键盘和鼠标在 Windows 更新。 [/NOMSG :   /NOMESSAGE] 可选参数，，压制在 Windows Update 中的所有信息 / 警告消息速冻。 [/THAW] 选参数的 Windows Update 完成后，机器返回到解冻状态。
<code>DFC password /ENDTASK</code>	结束正在进行的工作站任务并重启至冻结状态。批处理文件任务和解冻期间任务立即结束。Windows 更新任务即完成。
<code>DFC password /ENDTASK [/SHUTDOWN]</code>	结束正在进行的工作站任务并重启至 Frozen 冻结状态。批处理文件任务和 Thawed 解冻期间任务立即结束。Windows 更新任务即完成。 [/SHUTDOWN] 可选参数，关闭工作站。
<code>DFC password /FORMATTHAWSPACE</code>	格式化工作站上的所有 ThawSpace 解冻空间。存储在 ThawSpace 解冻空间中的数据将被永久删除。
<code>DFC password /DELETETHAWSPACE</code>	删除工作站上的所有 ThawSpace 解冻空间。存储在 ThawSpace 解冻空间中的数据将被永久删除。



## Faronics Anti-Virus 命令行语法

要运行 Faronics Anti-Virus 的命令，请完成以下步骤：

1. 在工作站上，通过命令提示符依次转至 < 系统目录 >:\Program Files\Faronics\Faronics Anti-Virus Enterprise。

2. 输入 AVECLI / [ 命令 ]

可用的命令如下：

语法	描述
definitionversion	显示病毒定义版本。
scanengineversion	显示扫描引擎版本。
updatedefs	更新并应用病毒定义。
fixnow	下载最新的病毒定义。启用主动保护和电子邮件保护。执行默认的深度扫描。
scanquick	开始快速扫描。
scandeeep	开始深度扫描。
enableap	启用主动保护。
applydefs [path to definitions]	从保存的位置应用定义文件。
fixnow /quick	执行 <i>快速扫描</i> （如果适用）。
setlicense[key]	应用授予的许可证密钥。

语法：

```
AVECLI/definitionversion
```



## 附录 A 端口和协议

设置 Deep Freeze 架构的关键在于了解需要使用的端口。重要的是需要了解网络中哪些端口正在使用，并选择与使用中的端口不发生冲突的端口。默认端口 7725 已经正式注册给 Deep Freeze。

Deep Freeze 的架构由下列三个部分构成：

- 客户端（安装了种子）
- 远程控制台（已启用本地服务）
- 控制台（连接至远程控制台）

只要客户端与远程控制台连接使用同一端口，不同组件之间应该不会存在任何端口冲突：



端口还可以用于分隔客户端。如果本地服务设置为运行三个端口（7725、7724 和 7723），则企业控制台可以连接至三个不同的端口，每个端口都对应一组不同的客户端。

在上图中，客户端使用 TCP 和 UDP 两种协议与远程控制台进行通信。与远程控制台相连的控制台仅使用 TCP 协议与远程控制台通信。记住哪些端口和协议正在使用中非常重要，这样可避免防火墙、交换机或路由器对其进行阻挡。





## 附录 B 网络示例

下列示例说明了几种涉及本地服务或远程控制台的不同方案。

- [示例 1 – 单个子网](#)
- [示例 2 – 多个子网，一个本地服务](#)
- [示例 3 – 多个端口，远程访问控制台](#)
- [示例 4 – 多个子网，多个本地服务](#)

每个示例均对不同网络环境下 Deep Freeze 各组件之间如何交互进行了说明。



在下列示例中，客户端计算机已安装了 Deep Freeze 工作站或工作站种子。两种安装均包含与控制台 / 远程控制台进行对话的通信组件。二者之间的不同在于工作站安装真正安装了 Deep Freeze，而工作站种子则仅安装了通信组件。



## 示例 1 – 单个子网

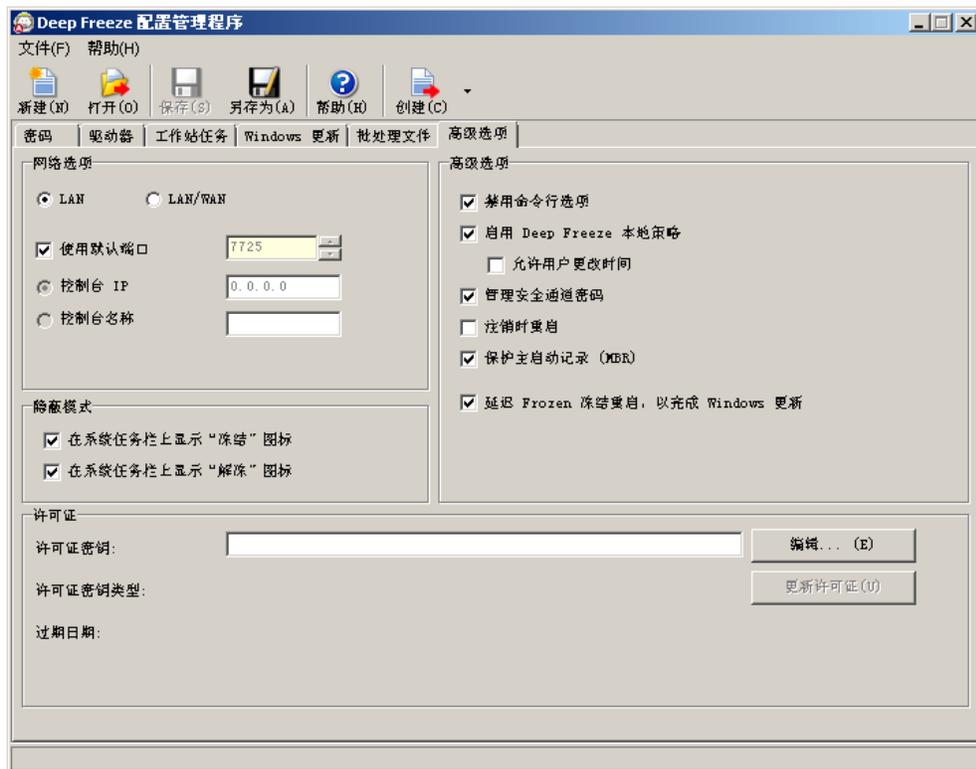
在此环境中，所有客户端计算机均作为控制台计算机位于同一子网中。此环境并不需要远程控制的控制台（虽然也可以使用此类控制台）。此示例未使用远程控制台。这是一个最简单的网络环境，配置起来也最为容易。

下图所示为网络拓扑结构：



客户端计算机（以计算机图标标识）与 Deep Freeze 企业控制台计算机（以 Deep Freeze 控制台图标标识）位于同一子网内。

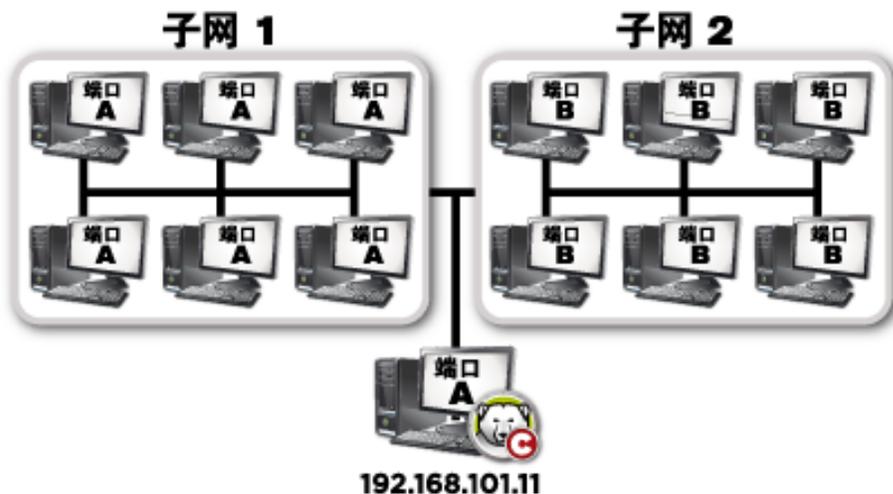
在此方案中，客户端使用端口 A，同时控制台在同一端口建立了一个本地服务连接。在创建工作站安装文件或工作站种子之前，已在高级选项选项卡上配置了此端口。





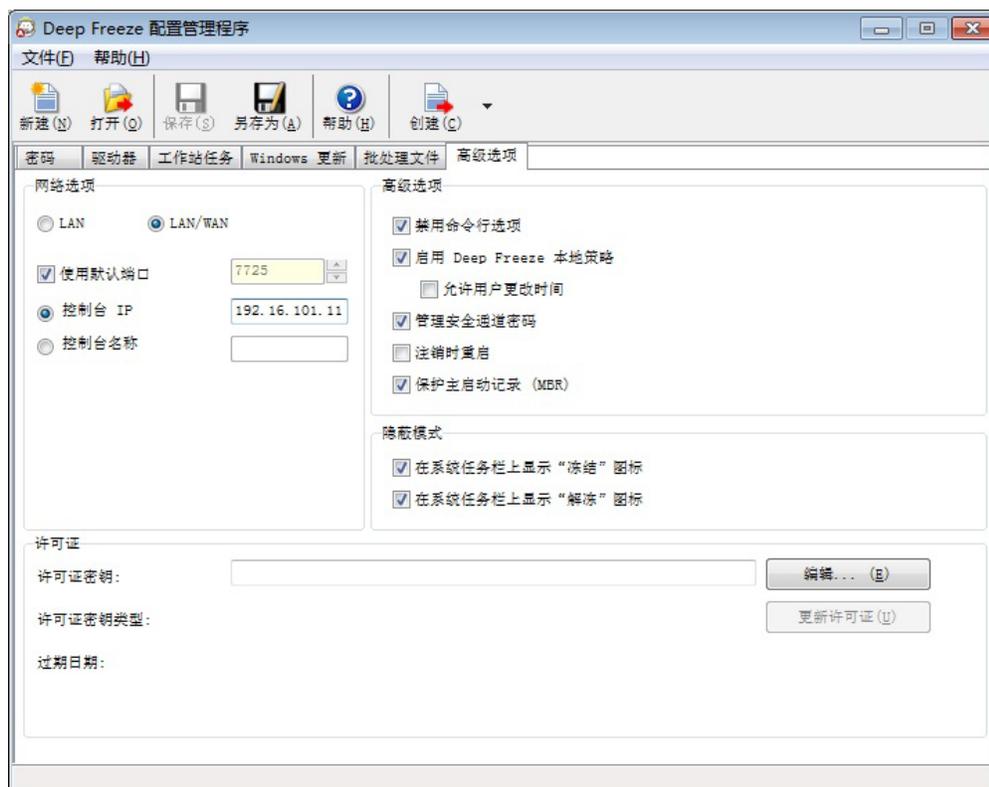
## 示例 2 – 多个子网，一个本地服务

在此环境中，客户端分布于多个子网。但仍只使用了一个控制台。此环境并不需要远程控制台（虽然可以使用此类控制台）。下图所示为网络拓扑结构：



在此方案中（与示例 1 – 单个子网类似），客户端和由控制台承载的连接均使用同一端口。在创建工作站安装文件或工作站种子之前，已在 Deep Freeze Enterprise 配置管理程序的高级选项选项卡上配置了此端口。

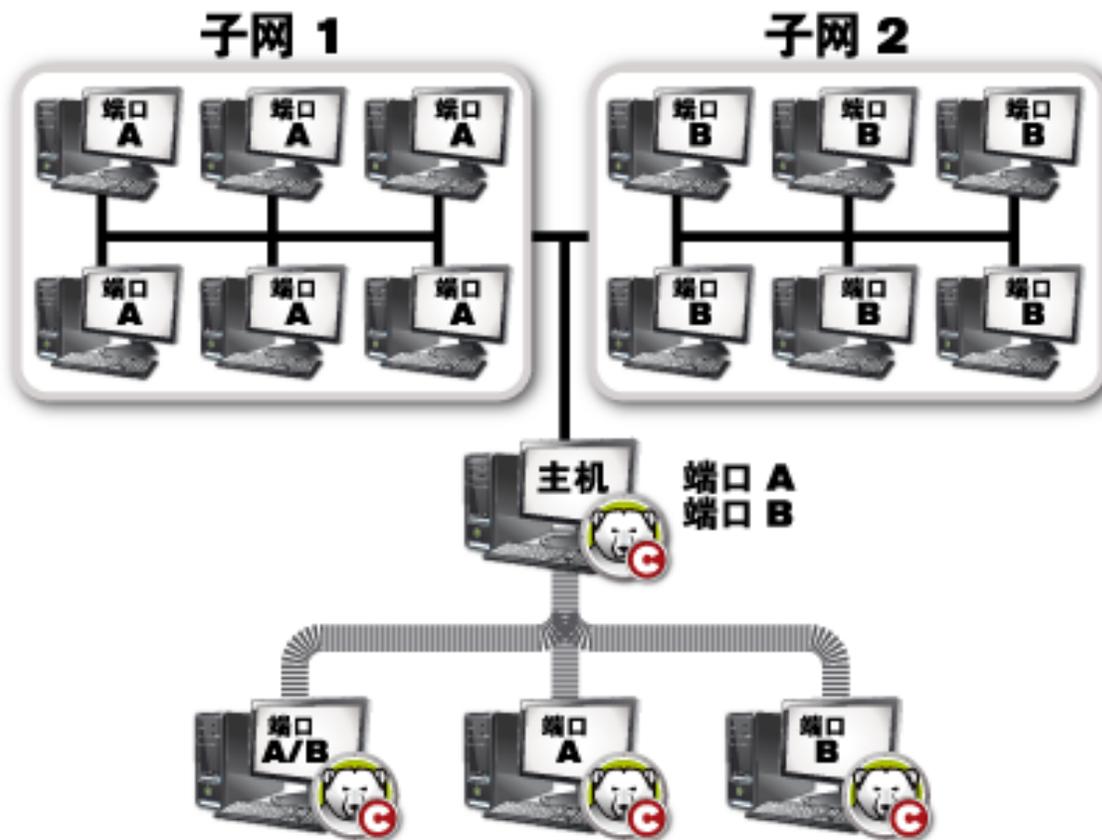
为了使客户端可见，需要将其配置为使用 LAN/WAN 连接。选中 LAN/WAN 选项时，会出现控制台 IP 字段。在此为要运行企业控制台的计算机指定 IP。下面的高级选项选项卡上显示了这些设置的示例：





## 示例 3 – 多个端口，远程访问控制台

在此环境中，客户端仍然跨多个端口分布。此例中使用了多个控制台。这些控制台使用本地服务进行访问，本地服务的管理机（主机）已经发布了有关连接的信息。下图所示为网络拓扑结构：



在此方案中，主机使用本地服务建立了一个连接。如上图所示，另外三个控制台连接到主机，以便按端口查看客户端。这些控制台只要可以看到主机，就不必再加入到各个子网中。

更具体地说，通过端口 A/B 相连的控制台可以看到主机和分配给端口 A 和 B 的每台计算机。而通过端口 B 相连的控制台则可以看到主机和分配给端口 B 的计算机。



## 示例 4 – 多个子网，多个本地服务

在此示例中，有两个相互分离的地点。

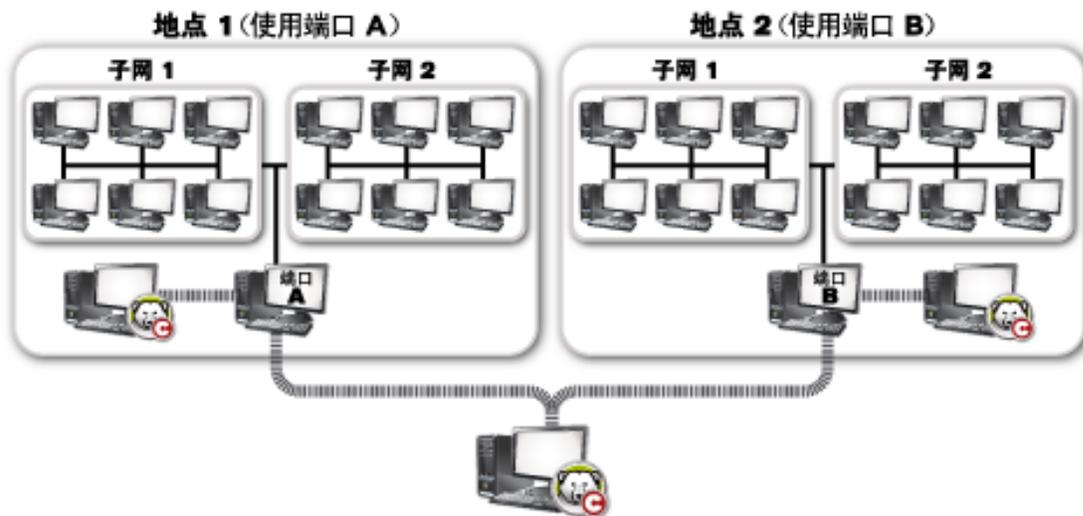
下面是有关此特殊示例的一系列假定：

- 两个地点相互分离，且相互之间仅存在最小连接
- 每个地点有一名网络管理员，负责管理该地点的 Deep Freeze
- 两个地点都需要从第三个地点进行管理

在此示例中，每个地点都设有远程控制台，并使用一个本地服务：

- 地点 1（校园网计算机实验室）使用端口 A 与客户端和控制台承载的连接进行通信。校园图书馆的计算机使用端口 B，位于技术支持部的控制台使用由实验室和图书馆控制台承载的连接。
- 任何不与计算机进行直接通信的控制台都应关闭本地服务

下图所示为网络拓扑结构：



这种设置的好处在于从地点 1 的客户端发送的所有数据包都可以保存在该位置。数据包传输的距离越短，丢失包的可能性越小。

实验室的管理员可以连接到位于同一地点 1 的本地服务，但却无法连接到图书馆的本地服务。这是因为实验室管理员并不知道访问图书馆本地服务所需的密码。对于图书馆的管理员来说也是一样。如果技术支持部知道实验室和图书馆的访问密码，则可以连接到二者的本地服务，以便对所有客户端进行管理。





## 附录 C 远程控制台连接的故障排除

### 控制台中无客户端

下面是控制台中不显示客户端的一些常见原因：

1. 控制台和客户端的网络设置不正确。

如果控制台设置为在某个端口下运行，而客户端则使用另一个端口，则二者将无法看到对方。而且，如果计算机配置为 LAN/WAN 连接，那么所输入的 IP 必须与运行控制台的计算机的 IP 相同。

只要所有运行该计算机与控制台的机器位于同一子网，使用默认的 LAN 设置就能保证工作正常。但是，如果运行的是 VLAN，或者客户端位于多个子网内，计算机安装就必须配置为以 LAN/WAN 设置来运行。

2. 控制台和客户端之间使用的端口被网络上的某些设备封锁。

使用 ping 命令检查连接。由于似乎不存在到主机的路由，因此客户端无法发送数据包到控制台 / 远程控制台。尝试 ping 控制台 / 远程控制台的 IP，但似乎没有响应。要解决此问题，请确保两台计算机可以连接到对方。

如果网络上的服务器，路由或交换机不允许通过端口通信，则客户端将不可见。默认情况下使用端口 7725。

3. 工作站不是由控制台，而是由其他自定义代码创建的。

在 Deep Freeze Enterprise 配置管理程序首次运行时，会弹出 *自定义代码* 的提示。此代码非常重要，因为软件是由它来加密的。这意味着，所创建的任何工作站都是使用此自定义代码加密。如果一个控制台是使用其他管理程序创建的，并且该管理程序使用不同的自定义代码进行安装，那么该控制台将无法看到以原始代码创建的工作站。工作站和控制台必须由使用完全相同的自定义代码安装的配置管理程序来创建。



## 启动控制台时出现端口正在使用错误

试图启动控制台时提示错误消息 *无法启动控制台：端口正在使用*。导致出现此错误消息的原因有以下几种：

1. 使用控制台所用的端口或者在同一台计算机上安装了 Deep Freeze 工作站 / 工作站种子。

Deep Freeze 可能安装在隐蔽模式下（图标未出现在系统任务栏）。种子不显示图标。最佳的测试是在计算机上运行工作站安装文件。如果显示了卸载选项，则表明安装了工作站文件或工作站种子，且可以将其卸载。如果未出现卸载选项，则表明未安装工作站安装文件或工作站种子。

最简单的解决方法是首先关闭本地服务，然后连接到一台可以远程访问的控制台。

2. 另一个程序或服务正在使用此计算机上的该端口。

这可能需要在该计算机上运行端口嗅探器来查看哪些端口是打开的。网络上有一些工具可以执行此类操作。Windows 提供的 *netstat.exe* 应用程序也可以显示 Deep Freeze 要使用的端口是否正在使用中。

3. 网络线缆已拔出。

当计算机未连接到网络时会出现此消息。

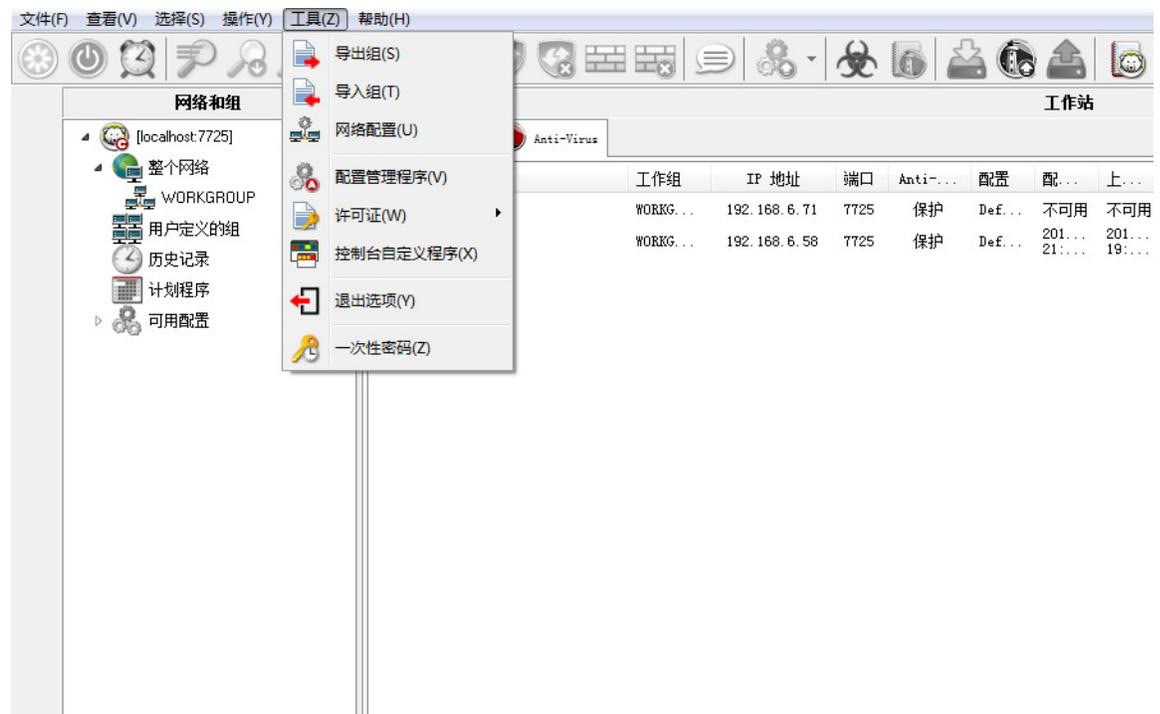


## 附录 D 创建自定义 Deep Freeze 企业控制台

Deep Freeze 企业控制台提供了创建具有有限功能的新企业控制台的功能。可将一个自定义、功能有限的控制台分发到您的组织中，以允许特定用户执行所需任务，而同时保证他们无权访问企业控制台的全部功能。

在此例中，将创建一个适于分发给教师或计算机实验室导师的功能有限的控制台。在此方案中，需要使教师能够重启计算机，根据需要锁定键盘和鼠标，以及向学生发送消息。但是，不希望该教师能够启动计算机使其进入解冻状态，卸载 Deep Freeze 或执行其他 IT 任务。

可从 **工具 > 控制台自定义程序** 启动控制台自定义程序。



我们将选中 **控制台功能 > 激活**。这样可确保将新控制台移到其他计算机上时，将需要在该计算机上输入一次性密码。如果这种安全保护措施不适于您的环境，请勿选择此选项。

**控制台功能 > 一次性密码**未选中，因为我们不希望教师能够以解冻模式重启计算机，无论在什么情形下。如果教师以解冻模式重启计算机，学生可能会在该计算机上安装不需要的软件，而此软件在计算机重启后可能仍然会保留。

我们将选中 **工作站命令**下的所有选项，因为教师应该能够向学生发送消息，以及根据需要关闭，重启和唤醒计算机。

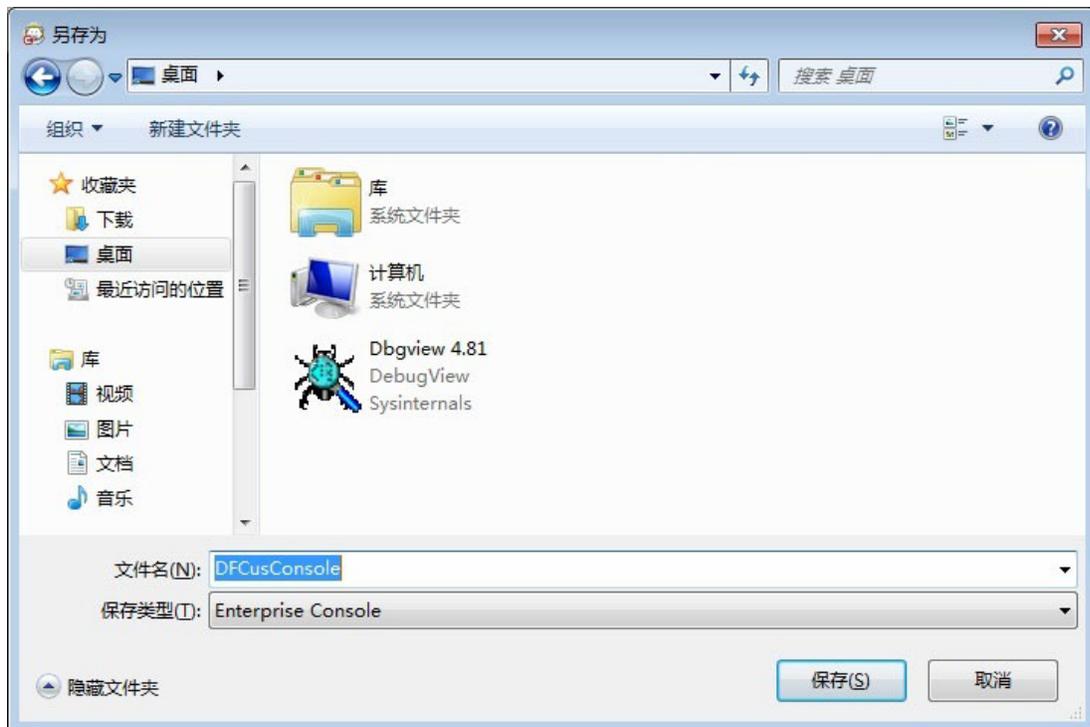


在 Deep Freeze 命令下只会选择以下三个选项：**解锁**、**锁定**和**重启后冻结**状态。这样教师可以根据需要在学生计算机上**锁定**（和**解锁**）键盘和鼠标，以及在**冻结**模式下**重启**计算机（以免万一 IT 人员无意中将计算机置于**解冻**状态）。将所有其他选项置于清除状态，可确保教师无法永久性修改计算机。

最后，将清除所有**工作站安装/卸载**命令及所有**计划程序**命令，因为我们不希望教师使用任何这些选项。



在选择所有选项后，单击**另存为**保存一个新企业控制台。此时将显示一个标准的**另存为**对话框：



选择新的功能有限的企业控制台，并将其分发给需要的用户。



## 附录 E Deep Freeze 操作文件 – RDC 示例

### Deep Freeze 操作文件

Deep Freeze 操作文件是一个 XML 文件，管理员可用该文件为 Deep Freeze 企业控制台定义更多功能。操作文件定义了调用一个外部批处理文件并将某些信息（例如，计算机 IP 地址，名称）传递给该文件或脚本的方法。

操作文件只是简单地调用一个外部程序或脚本，因此，任何可从命令行调用的脚本语言都可以使用。

### 操作文件示例

我们将使用的 Deep Freeze 操作文件的结构如下所示。

*DFEntConsoleCustomActions.xml* 位于 *C:\Program Files\Faronics\Deep Freeze Enterprise*。可以编辑该文件，以添加其他操作，如下所述：

```
<?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>
```



在上例中，自定义操作文件中包含用于在控制台计算机上运行远程桌面以及连接 %%WKSNAME%% 参数指定的远程计算机的命令。

*DFEntConsoleCustomActions.xml* 文件包含 3 个示例：

- 使用 RDC 控制
- 远程执行
- 推送并安装 MSI 文件

有关使用上述示例的详细信息，请参阅[配置自定义操作](#)部分。您可以根据需要编辑 *DFEntConsoleCustomActions.xml* 文件。

## Deep Freeze 操作文件结构

以下 XML 架构中列出了用户可以使用的自定义操作。可以根据所需的命令数保存多个 XML 文件。必须将各个文件保存到 Console 文件夹，而且不得选择只读属性。

只有在重启 Deep Freeze 控制台后，所做的任何更改才会生效。

参数	用法
<code>&lt;?xml version="1.0" encoding="UTF-8"?&gt;</code>	
<code>&lt;CUSTOMDEFINEDACTIONS&gt;</code>	
<code>&lt;CAPTION&gt;</code>	显示在文件菜单或子菜单上的文本
<code>&lt;ENGLISH&gt;Caption&lt;/ENGLISH&gt;</code>	各种语言的文本
<code>&lt;GERMAN&gt;Caption&lt;/GERMAN&gt;</code>	各种语言的文本
<code>&lt;JAPANESE&gt;Caption&lt;/JAPANESE&gt;</code>	各种语言的文本
<code>&lt;SPANISH&gt;Caption&lt;/SPANISH&gt;</code>	各种语言的文本
<code>&lt;FRENCH&gt;Caption&lt;/FRENCH&gt;</code>	各种语言的文本
<code>&lt;FILEMENU&gt;y&lt;/FILEMENU&gt;</code>	定义该操作是否将位于文件菜单中
<code>&lt;POPUPMENU&gt;y&lt;/POPUPMENU&gt;</code>	定义该操作是否将位于右键单击弹出菜单中
<code>&lt;SILENT&gt;y&lt;/SILENT&gt;</code>	定义是否向用户提示确认消息



参数	用法
<SUBITEMS>	在子菜单项中，可以定义该项的子项
</SUBITEMS>	如果定义了子菜单项，则该项的操作将被忽略
<SYNC>y</SYNC>	指定将同步还是异步执行命令
<PARAMS>	选择此操作将会提示用户输入自定义参数
<PASSWORD>	参数名称
<VAR>%PARAM1%</VAR>	将在 EXECUTE 中使用的变量的名称
<ENGLISH>USERNAME Param (ENGLISH) </ENGLISH>	各种语言的文本
<GERMAN>USERNAME Param (GERMAN) </GERMAN>	各种语言的文本
<JAPANESE>USERNAME Param (JAPANESE) </JAPANESE>	各种语言的文本
<SPANISH>USERNAME Param (SPANISH) </SPANISH>	各种语言的文本
<FRENCH>USERNAME Param (FRENCH) </FRENCH>	各种语言的文本
</CAPTION>	
</USERNAME>	
</PARAMS>	
<LOG>	定义日志文件的行为
<APPEND>y</APPEND>	定义将附加还是新建日志文件
mand.log</FILENAME>	定义文件名
<EXECUTE>c:\windows\vpn.exe %%IP%% %USERNAME% %PASSWORD% %%WKSNAME%%</EXECUTE>	定义将执行的命令。在此，可以使用参数和 / 或控制台条目
<WORKDIR>c:\windows</WORKDIR>	定义工作目录



## 控制台参数

可通过企业控制台将下列控制台参数传递给执行的应用程序或脚本：

参数	用法
%%WKSNAME%%	工作站名称
%%DOMAIN%%	工作站域
%%IP%%	工作站 IP
%%PORT%%	工作站端口
%%STATUS%%	工作站状态
%%CFGDATETIME%%	工作站配置日期 / 时间
%%MAC%%	工作站 MAC 地址
%%DFVERSION%%	工作站 Deep Freeze 版本
%%CFGNAME%%	工作站配置名称
%%LOGGEDONUSER%%	工作站已登录用户
%%DFINSTALLATIONFILE%%	工作站安装文件
%%LICENSESTATUS%%	工作站许可证状态
%%LICENSEEXPIRYDATETIME%%	工作站许可证过期日期和时间
%%AVSTATUS%%	工作站 Anti-Virus 状态
%%OSVERSION%%	工作站操作系统版本