戴尔硬盘保护增强套件用户手册

版本：1.5

日期：2018.9.17

目录

第 1 章硬盘保护控制台功能简介.....4
1.1 三种模式.....5
1.2 主要操作界面及初始密码.....5
第 2 章硬盘保护控制台首次部署.....6
2.1 安装前的准备.....6
2.2 第一次批量部署简要步骤.....7
2.3 在发送端安装硬盘保护控制台.....8
2.4 发送端数据网络同传至客户端.....16
第 3 章硬盘保护控制台日常维护与使用.....20
3.1 进度管理.....21
Windows 界面下的进度管理.....21
Pre-OS 界面下的进度管理.....25
3.2 分区及操作系统管理.....26
添加分区.....26
分配分区.....27
分区更新.....28
添加系统.....29
多系统安装方法.....32
3.3 网络部署.....33
网络设置功能说明.....35
其它设置功能说明.....36
3.4 系统设置.....39
3.5 辅助工具.....41
3.6 开机选单界面功能简介.....43
第 4 章卸载硬盘保护控制台.....46
4.1 pre-os 卸载.....46
4.2Windows 下卸载.....48
第 5章硬盘保护控制台注意事项.....49
第 6 章更换主板后设置 BIOS 注意事项.....52

第一章网络控制台产品简介.....52
第 2 章 安装和卸载.....54
第 3 章 登录学生端.....56
3.2 输入登录密码.....58
3.3 扫描计算机与登录客户端.....58
3.6 删除学生端.....60
第 4 章 客户端监视设置.....60
4.1 资产监视设置.....61
4.2 恶意进程监视设置.....61
4.3 网络监视设置.....64
第 5 章 客户端监视.....65
5.1 查看学生端资源.....65
5.1.1 查看某一客户端的状态信息.....66
5.2 查看学生端异常状态.....68
5.2.1 学生端 IP 地址改变.....68
5.2.2 学生端硬件信息改变.....69
5.3 学生端信息更新.....73
5.4 查看日志.....74
第 6 章 客户端控制.....75
6.1 屏幕监控.....75
6.2 屏幕广播.....76
6.3 时间同步.....76
6.4 远程重启、关机、唤醒操作.....76
6.5 发送消息.....77
6.6 文件传输.....77
6.7 锁定、启用键盘鼠标.....79
6.9 删除学生端进程.....81
6.10 取消登录.....82
6.11 禁用、启用 USB 端口.....82

第 1 章硬盘保护控制台功能简介

硬盘保护控制台是专门为电子教室、教学实验室等公共机房环境设计开发。主要包括：网络同传系统、硬盘保护系统、网络管理系统三大模块。重点解决机房管理员如何方便地在机房中快速部署，以及便捷地安全维护的问题，并充分满足机房复杂的教学应用。

该应用方案具有以下功能特色：

1、 能够同时给机房中的多台计算机（最多可达 254 台）进行系统、软件的快速部署，整个同传所花的时间比手工安装一台计算机系统的时间短很多，同时可以支持双硬盘保护和同传，高级功能可实现进度点中重要数据拷贝。

2、 允许管理员一次性给机房中所有计算机的不同系统分配好IP信息和计算机名。

3、 保护系统远离病毒和恶意破坏的困扰，极大地降低管理员维护机房计算机的难度及成本。

4、 能够保护机房用户常用的多种操作系统（其中包括Windows XP，Windows 7，Windows 8.1，Windows10,linux等）。

5、 允许管理员在每台计算机上安装多个完全隔离的系统，相当于把这些不同的系统安装在完全不同的计算机上，从而实现一台计算机当多台计算机使用。

6、 可以使计算机快速还原至先前正常的工作状态，大大降低管理员对机房内计算机的维护工作量。

7、 允许管理员使用智能同传的方式为机房内的所有计算机部署增量数据，如安全补丁、新增的软件或数据文件等。

8、 允许管理员远程监控和管理所有计算机的软硬件资产。

1.1 三种模式

硬盘保护控制台保护功能主要有三种模式。

机房模式

处于机房模式时，硬盘数据受到保护，各种对硬盘数据的操作，在下次开机时都会被还原。

机房模式下，可以设定还原的策略，但不可设定备份策略，只能手动做备份。

个人模式

处于个人模式时，硬盘数据受到保护，但对于硬盘上的操作，默认在下次开机时不会被还原，用户可以选择性还原或备份，不可修改计算机名，或者IP信息。

个人模式下，可以设定备份策略，但不可设定还原策略，是否还原需手动选择。

开放模式

开放模式是完全不保护的一种模式，在下次开机重启时，开放模式下用户对硬盘数据的操作完全保留。

1.2 主要操作界面及初始密码

硬盘保护控制台有两个主要操作界面。通过输入管理员密码，更登录管理界面。

初始密码：dell

用户可自定修改密码,本产品不提供密码找回。

Pre-OS 操作界面

在进入操作系统前，硬盘保护控制台可让用户选择进入那个操作系统的界面。

在Pre-OS操作界面，按[Home]键，并输入管理员密码，即可开启Pre-OS管理功能选项。

Windows操作界面

进入操作系统后，在Windows下的硬盘保护控制台管理界面。
点击任务栏的硬盘保护控制台图标，选择登录并输入管理员密码，即刻进入Windows下管理员界面。

第 2 章硬盘保护控制台首次部署

2.1 安装前的准备

本产品不能与系统自带的 recovery 功能一起使用。如果系统有自带的 recovery 分区，请删除并重新安装操作系统。

在正式安装使用硬盘保护控制台之前，需要完成以下工作：
第一步：首先完成机房中所有计算机的物理连线、电源接通、网络连通等工作；
第二步：确认需要部署的计算机应同型号、同配置；
第三步：需保证磁盘尾部有大于 2GB 未使用空间；
第四步：确保计算机 BIOS 设置符合以下要求；

1.HDD Protection is “Enabled”

必须要开启硬盘保护功能，才能使用戴尔硬盘保护增强套件。

2.SecureBootis“disabled”
安全引导“禁用”

3. Load Legacy Option ROMs is “Enabled”

加载传统选件 ROM 为“Enabled”

4. UEFI Network Stack is “Enabled”

开启 UEFI 网络堆栈

5.SATA Operation“AHCI”

SATA 模式是“AHCI”

6. Deep Sleep Control is “Disabled”

深度休眠控制“禁用”

7.Wake on LAN is“Enabled”

开启 LAN 唤醒功能

8.SetODD as lst boot device

将 ODD 或者 HDD 设置为第一引导设备

第四步：仔细阅读本手册内容，从而理解本产品的功能和使用注意事项。

2.2 第一次批量部署简要步骤

第一步：选机房内一台机器作为“发送端”，其余机器作为“客户端”。

第二步：在“发送端”安装好操作系统、硬件驱动、所需的软件、网络环境（IP、网关、子网掩码）。

注意：此时只创建用于安装操作系统的 C 盘，其它空间后续通过硬盘保护控制台来做分配。

第三步：在“发送端”，安装硬盘保护控制台。（具体步骤参照 2.3）

第四步：在“发送端”，进入网络同传功能界面。（具体步骤参照 2.4）

第五步：启动“客户端”，每台“客户端”登录到“发送端”。（具体步骤参照 2.4）

第六步：在“发送端”上把硬盘保护控制台驱动和参数，以及操作系统数据同传至“客户端”。（具体步骤参照 2.4）

首次部署完成，机房内所有计算机都具备相同的操作系统及驱动、软件环境以及硬盘保护功能。

2.3 在发送端安装硬盘保护控制台

在“发送端”安装操作系统、驱动程序、所需软件、网络环境（IP、网关、子网掩码）和硬盘保护控制台后，“发送端”会处于硬盘保护模式。以“发送端”为样机，可将“发送端”的系统环境通过网络同传功能，部署至机房其它的“客户端”计算机，机房内所有计算机都具备相同的操作系统及驱动、软件环境。

注意：安装硬盘保护控制台前，请先将 UAC(User Account Control，用户账户控制)关闭，否则在安装时，会提示“请先关闭 UAC”。

注意：安装硬盘保护控制台退出杀毒软件，或把硬盘保护程序添加信任白名单。

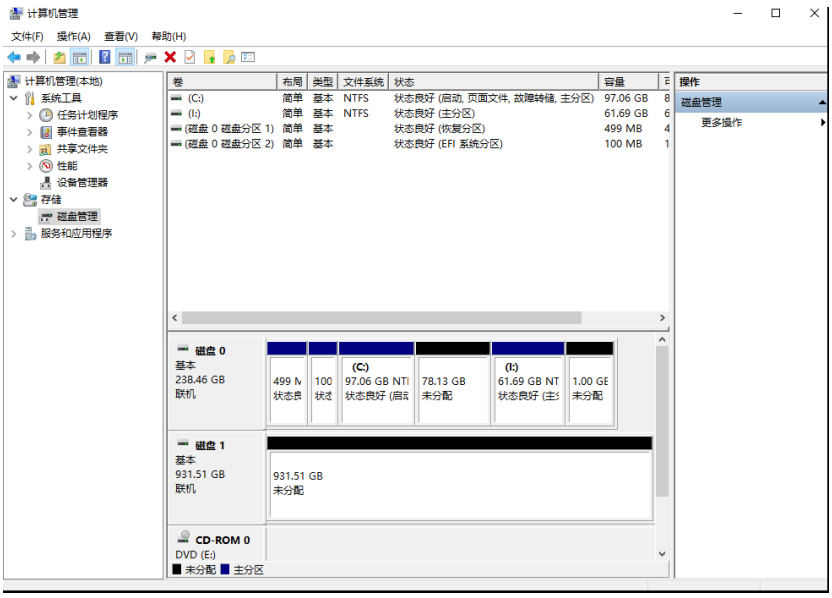
注意：安装硬盘保护控制台驱动时，磁盘管理中有二块硬盘时，是否是联机状态，不能是脱机状态，如果是脱机状态需要手动右键联机。

注意：在安装硬盘保护控制台前，请先配置网络环境（IP、网关、子网掩码、DNS ）否则使用网络同传功能时，会提示“无法绑定指定网卡”。

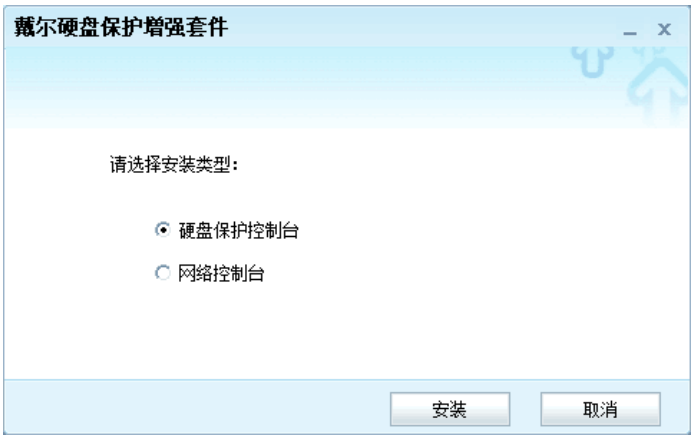
注意：在安装硬盘保护控制台前，系统更新服务关闭，防火墙关闭，否则使用网络同传功能时，会提示“请检查防火墙设置”。

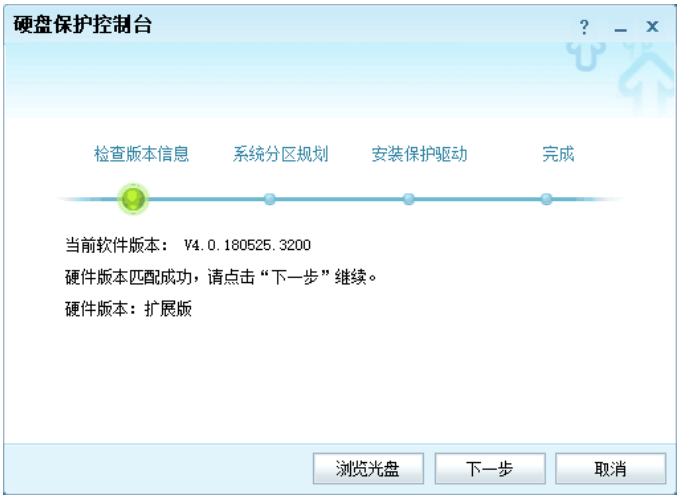
注意：安装硬盘保护控制台之前把当前系统内杀毒软件退出。

注意：安装硬盘保护驱动前打开磁盘管理查看硬盘状态，如果是脱机状态需要手动点击联机。第二块硬盘需要有分区表，MBR 或者 GPT 分区表，请查看下图。



1、在戴尔硬盘保护增强套件安装光盘中运行 Setup 程序,选择硬盘保护控制台,点击安装出现安装界面，单击[检查]。

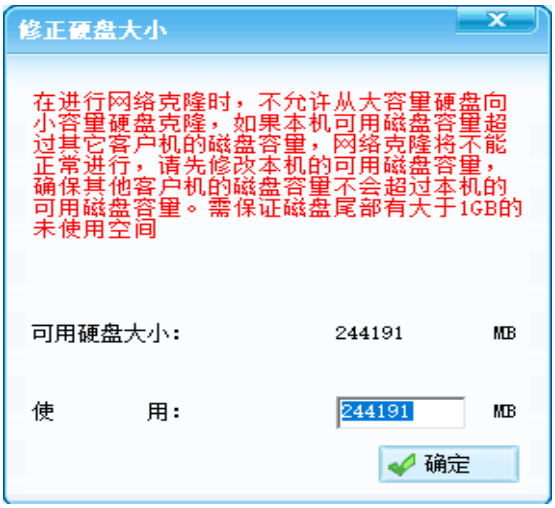




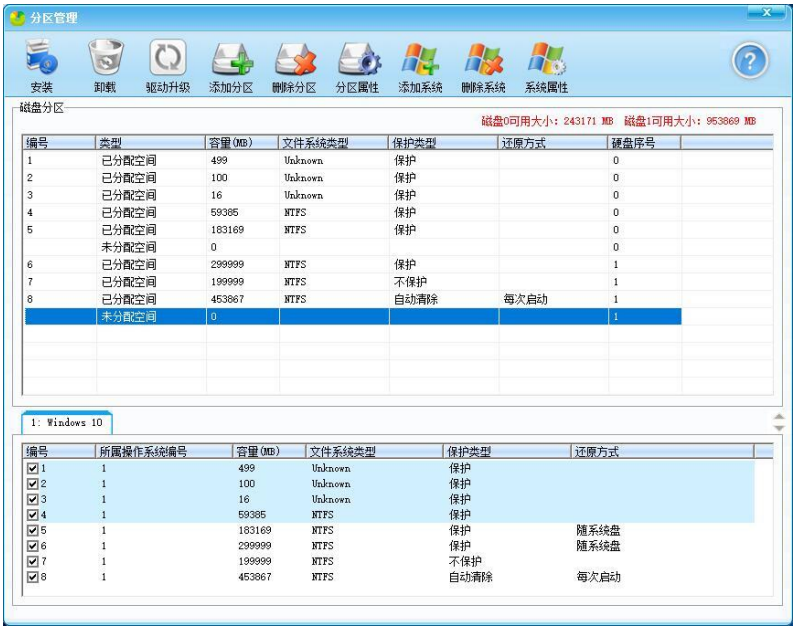
2、版本匹配成功后，点击[下一步]安装程序会弹出分区管理，双硬盘默认启用双硬盘保护，硬盘保护控制台建议安装到固态，点击确定。

3、此时如果硬盘保护控制台提示磁盘尾部空间不足时，请在磁盘管理删除最后一个分区后继续安装。（硬盘尾部要留 2G 未分配空间）

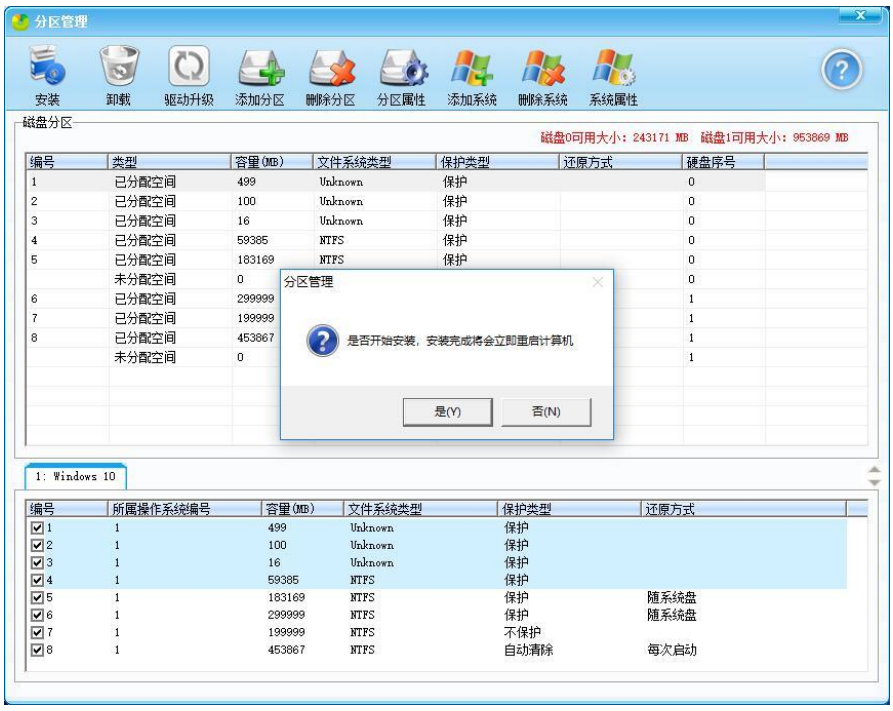
4、如果发送端与客户端机器系统所在硬盘容量一样大，默认点击[确认]。



5、 安装程序弹出分区管理，当前的系统名称为 Windows 10（可通过系统属性修改），在分区管理中可以双击未分配空间进行硬盘分区，（此时可规划硬盘分区装多个操作系统，如有需求详见 3.2 多系统安装）划分好分区后在所属操作系统下把分区编号打钩后点击[安装]即可。



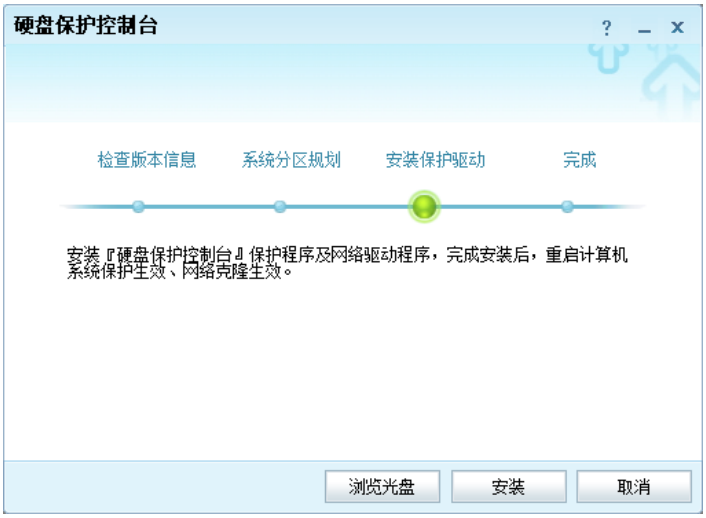
6、安装程序提示会重新启动系统，点击 [是] ，系统重新启动后需要手动执行 Setup.exe 选择硬盘保护控制台继续安装。



7、系统重新启动，会进入硬盘保护控制台系统选单界面，按回车以进入所选操作系统。

此时硬盘保护控制台还未安装完成，操作系统名称为“白色”。

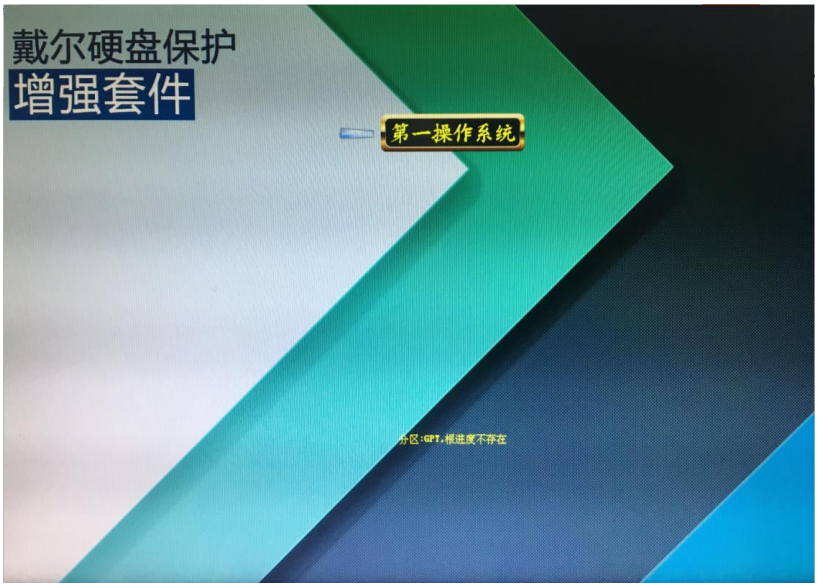
8、按回车进入操作系统后，如果有新添加分区将其格式化，然后打开戴尔硬盘保护增强套件驱动，运行 setup.exe 选择硬盘保护控制台程序，点击[安装]。



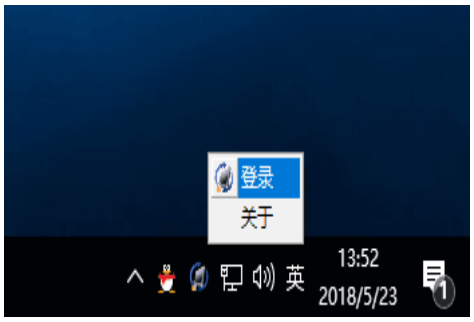
9、填写完整本机 IP 信息，点击[确定]，默认点击[下一步]进行安装，最后点击[完成]重启计算机。

10、完成安装后，系统重新启动，自动进入硬盘保护控制台系统选单界面，回车以进入所选操作系统。

此时硬盘保护控制台安装完成，操作系统名称为“黄色”。

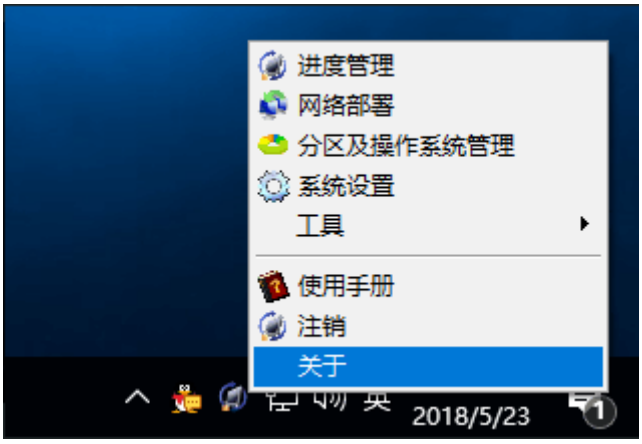


11、进入操作系统后，在任务栏界面找到硬盘保护控制台图标右击，点击[登录]。



12、此时会弹出登录窗口，请输入初始密码 dell，并点击[确定]。

13、此时在任务栏选择硬盘保护控制台后，可看到相关操作选项。



至此，“发送端”硬盘保护控制台部署完毕，“发送端”处于保护模式，硬盘保护生效。

2.4 发送端数据网络同传至客户端

作为样机支持双硬盘同传的“发送端”计算机，在操作系统、驱动程序、所需软件、网络环境（IP、网关、子网掩码）和硬盘保护控制台安装完成后，通过网络同传功能，将“发送端”的硬盘数据同传至所有“客户端”，使得“客户端”计算机处于等同于“发送端”的可用状态。

注意：网络环境（IP、网关、子网掩码、DNS）需要在安装硬盘保护控制台前配置好，否则使用网络同传功能时，会提示“无法绑定指定网卡”。

注意：在安装硬盘保护控制台前，请关闭防火墙，否则使用网络同传功能时，会提示“请检查防火墙设置”。

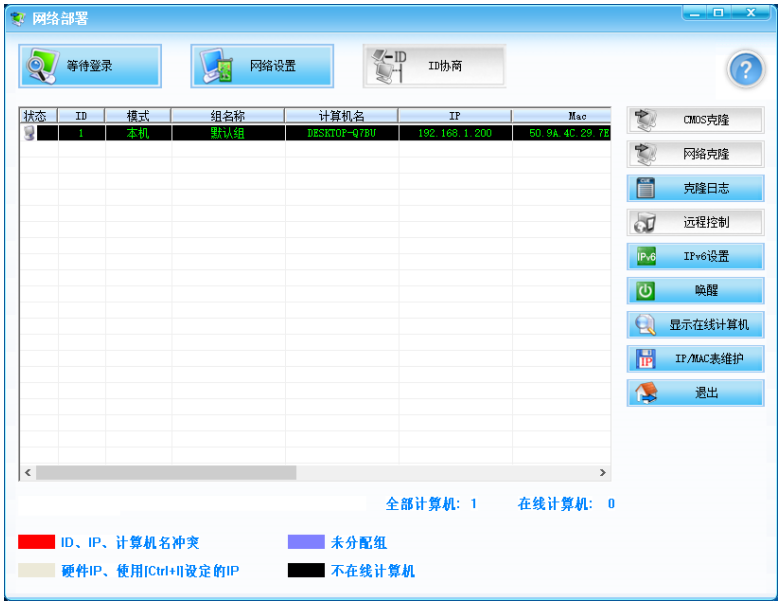
网络同传的细节参数设置，可参看 3.3 章。

发送端：安装好所有操作系统、驱动程序、所需软件和硬盘保护控制台的样本机，可通过网络同传，将该系统环境等复制到其它所有的客户端。

客户端：作为客户端，接收从发送端传送的系统、软件、数据等至本地硬盘。

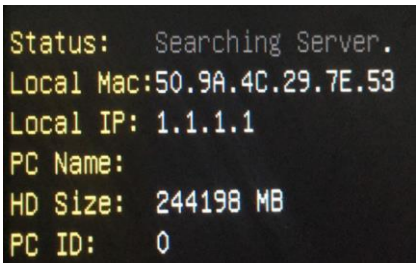
1、在“发送端”登录至硬盘保护控制台管理界面，单击[网络部署]。

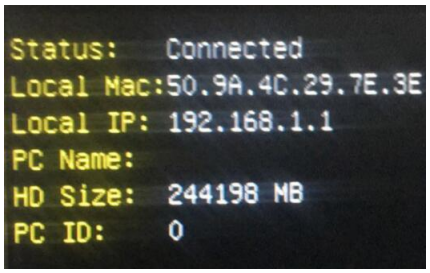
2、在出现硬盘保护控制台的网络部署界面，单击[等待登录]。



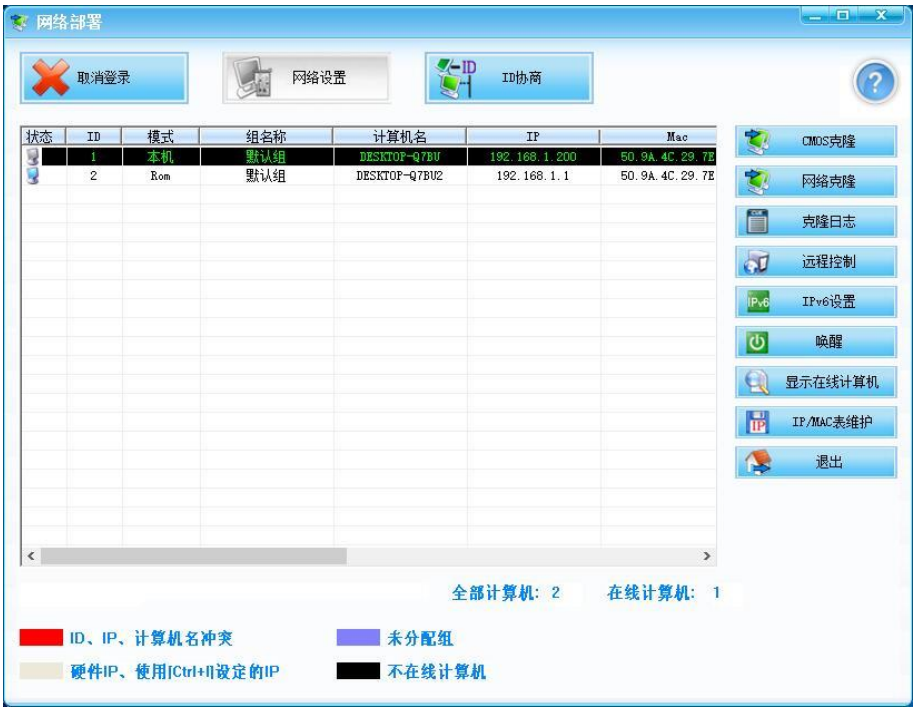
3、启动各“客户端”机器，“客户端”会自动登录至“发送端”，机器状态会以 Rom 模式登录到发送端。

搜索发送端“Searching Server”状态　　已连接”Connected”状态。

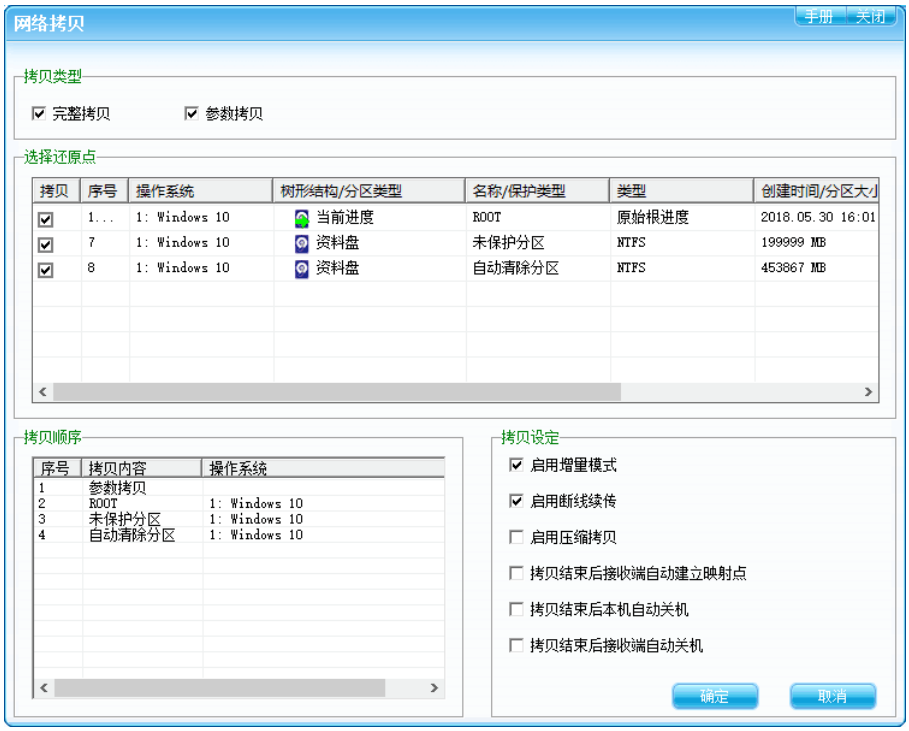




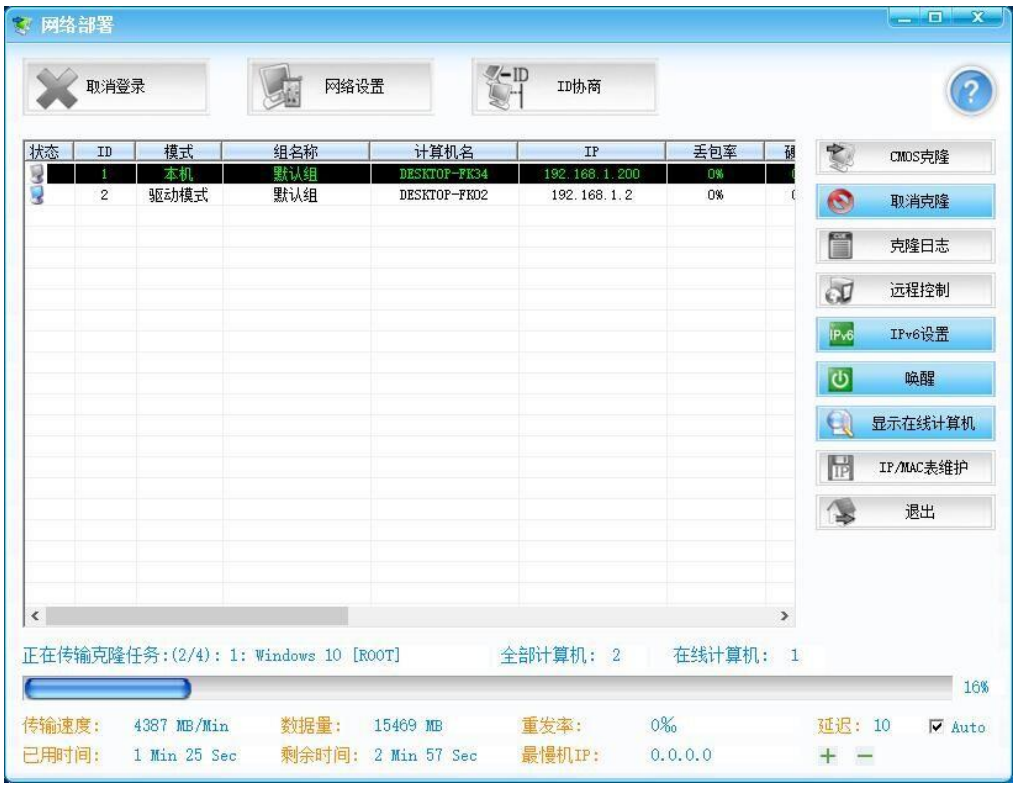
4、回到“发送端”的网络部署工具，可以看到“接受端”已经完成登录，且处于“Rom”模式。点击[完成登录]。



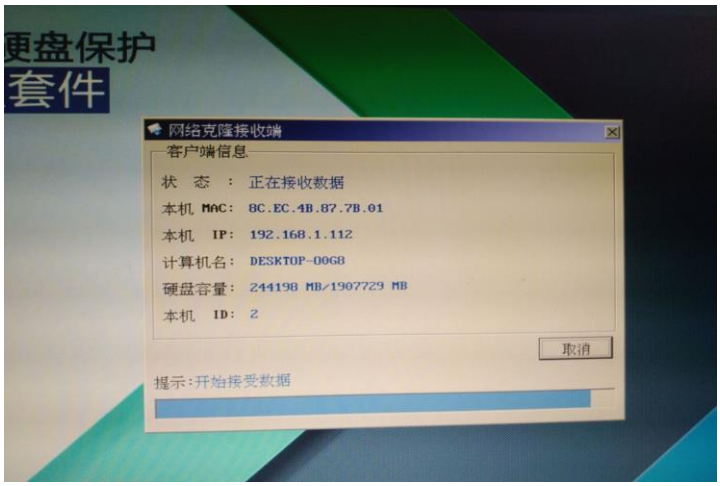
5、回到网络部署工具界面后，点击[网络克隆]，勾选“完整拷贝”，点击[确定]，“发送端”会将自身的硬盘保护控制台驱动和系统数据同传至各“客户端”。

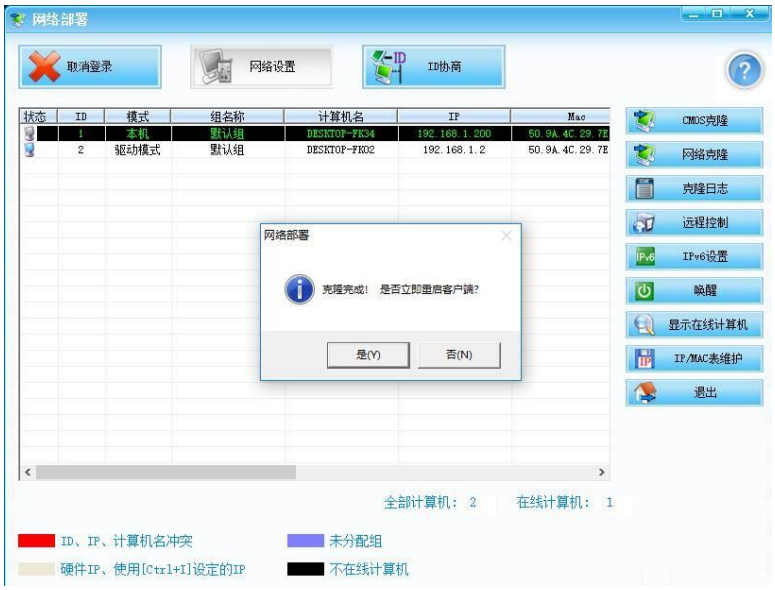


4、点击“确定”，开始执行网络克隆。

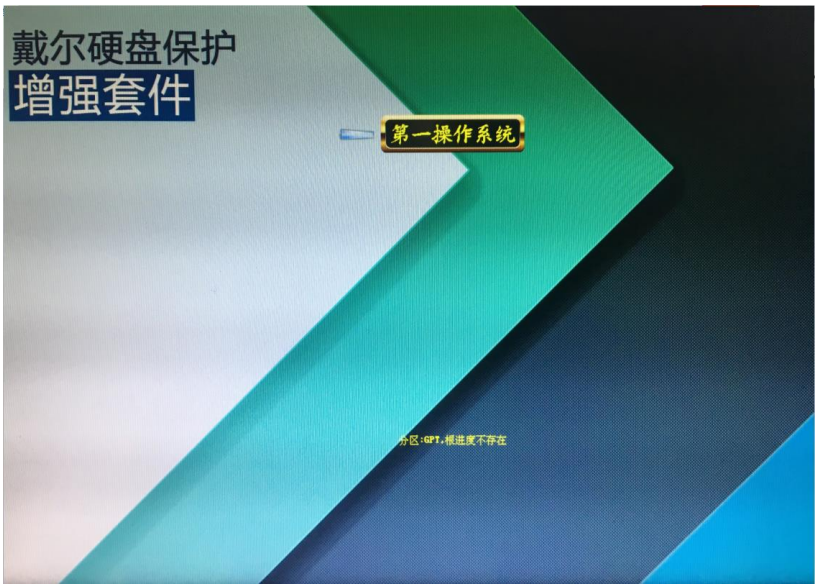


7、网络克隆过程中，此时客户端传完参数后会自动重启将以驱动模式登录发送端进行接收数据，会有进度条显示克隆进度，在克隆完成后，会提示重新启动“客户端”，单击[是]。





8 、此时各“客户端”会重新启动，并创建root进度，“客户端”具备与“发送端”相同的操作系统环境以及硬盘保护功能，此时操纵系统名称变为黄色。



至此，首次部署完成，机房内所有计算机都具备相同的操作系统及驱动、软件环境以及硬盘保护功能。

第 3 章硬盘保护控制台日常维护与使用

3.1 进度管理

硬盘保护控制台可以为每个操作系统创建多个还原进度（即备份点），并可对还原进度的使用做管理。

用户可以在Windows操作界面做进度管理，也可在Pre-OS操作界面做进度管理。

Windows 界面下的进度管理

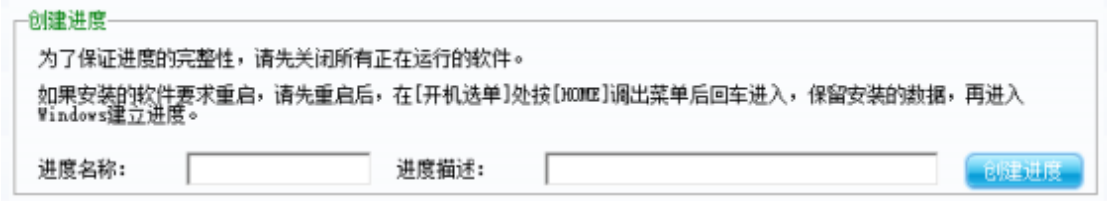
登录 Windows 界面下的硬盘保护控制台，并选择[进度管理]，可进入硬盘保护控制台的进度管理界面。

创建进度：

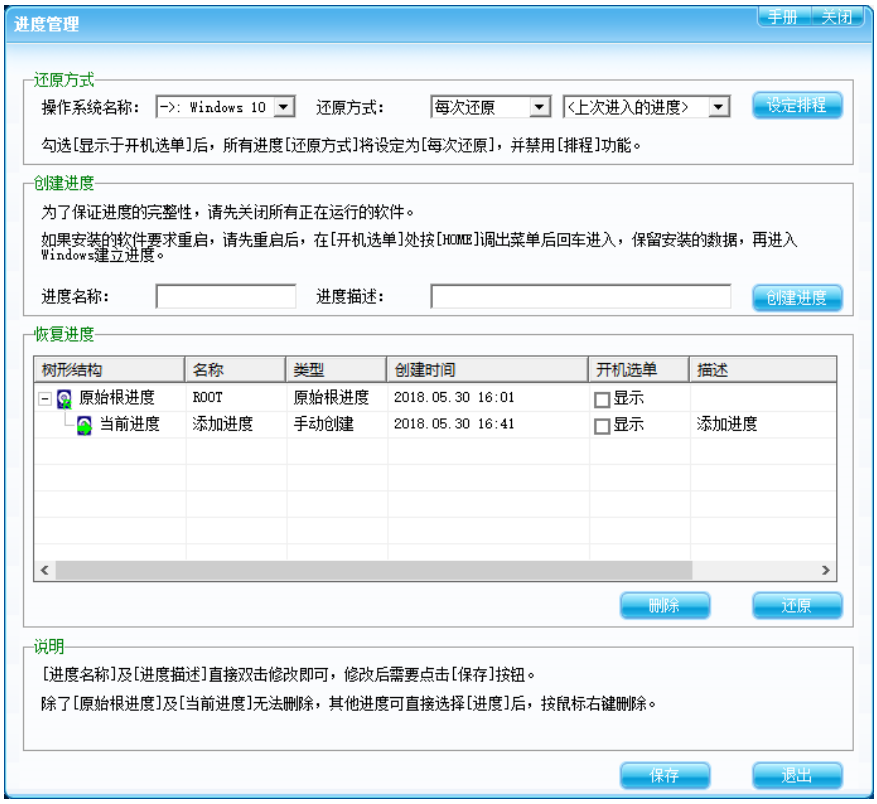
每个安装硬盘保护控制台的操作系统，都会有一个“原始根进度 ROOT”，

基于原始根进度，可以创建新的进度。

输入相应进度名称和进度描述点击[创建进度]，即可完成新进度（备份点）的创建。

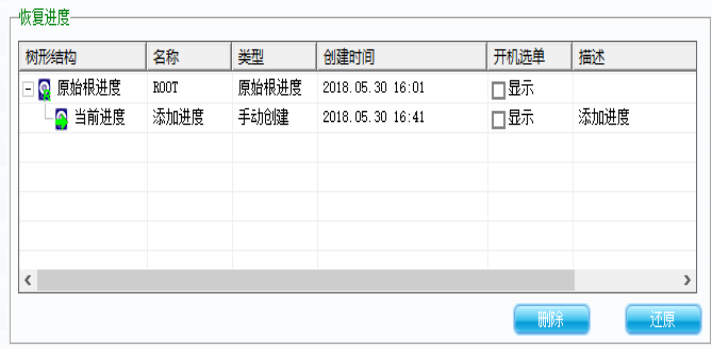


新进度创建完成后，在进度列表中可以看到，并且进度列表可以用树型方式显示，以表明各进度之间的关系。

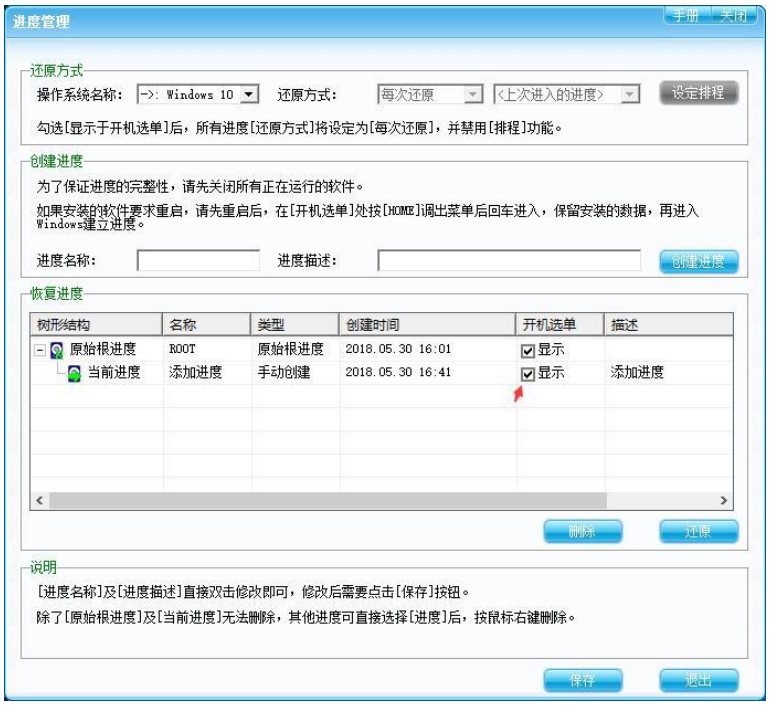


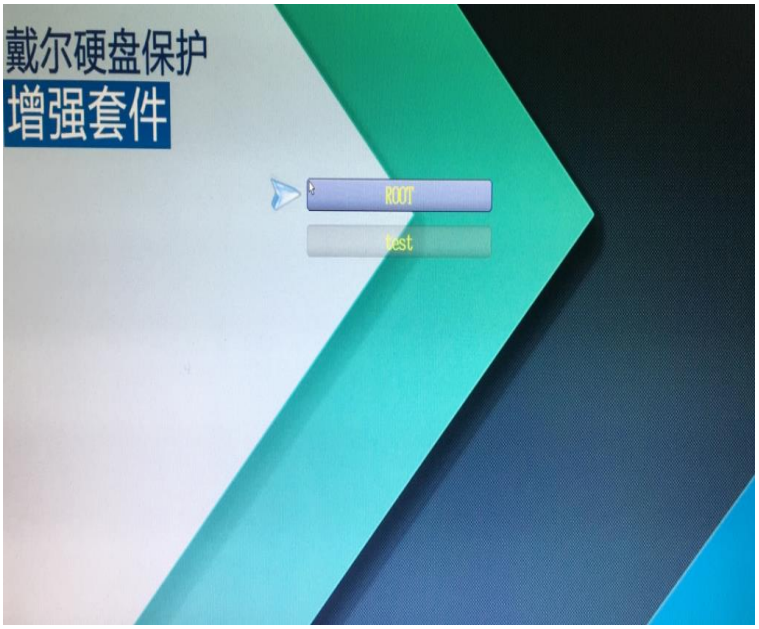
恢复进度：

在进度列表中，选择一个进度，点选[还原]，可将系统恢复至所选进度环境。



若勾选某些进度开机选单显示，则在 Pre-OS 系统选单界面，选择系统后，相应被勾选的进度也会显示出来，以供用户选择。





进度排程：

在进度管理界面中点击[设定排程]，可对进度做时间排程管理。

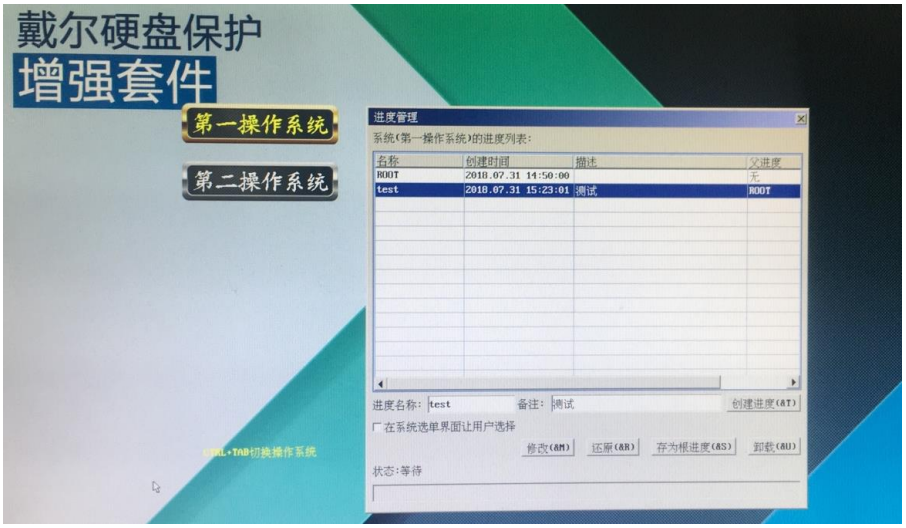
在机房模式下，可设定恢复进度排程，设定何时恢复至哪个进度。总共可设定 5 个恢复进度排程，每个排程都处于同等地位，任何一个排程条件被满足，都会触发相应的恢复进程。

在个人模式下，可设定创建进度排程，设定何时创建新的进度。总共可设定 5 个创建进度排程，每个排程都处于同等地位，任何一个排程条件被满足，都会触发相应的创建进程。

Pre-OS 界面下的进度管理

登录 Pre-OS 界面下的硬盘保护控制台，并选择[进度管理]，可进入硬盘保护控制台的进度管理界面。

在 Pro-OS 界面下的进度管理，可创建或还原进度，并且可将某一个进度“写入根”，即将当前所选进度转变为新的根进度 ROOT，注意，写入根操作后，原有根进度下的所有进度都将被删除。



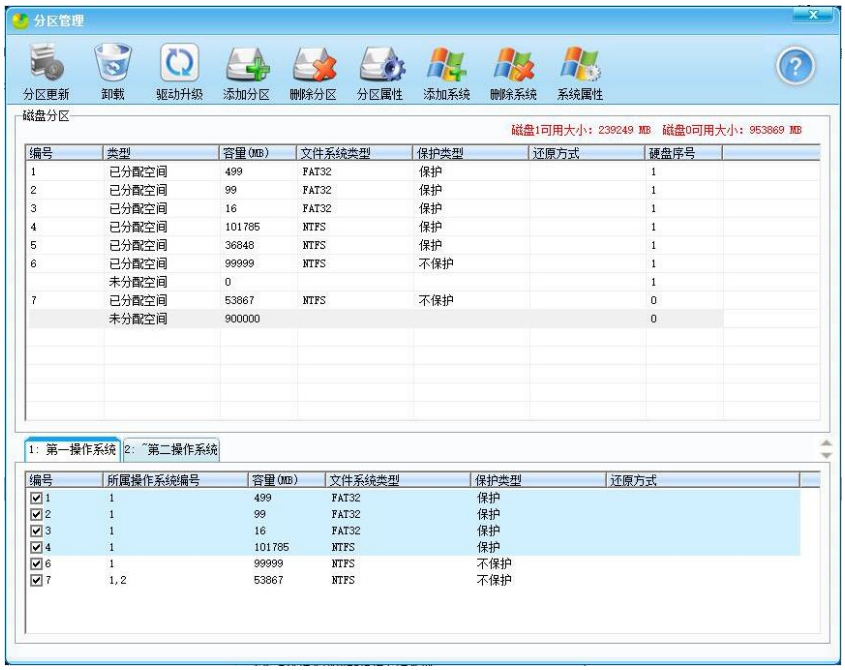
3.2 分区及操作系统管理

此工具可以对两块硬盘进行分区划分，登录 Windows 界面下的硬盘保护控制台，并选择[分区及操作系统管理]，可进入硬盘保护控制台的分区及操作系统管理界面。可对显示的硬盘进行分区划分。

添加分区

在分区及操作系统管理界面可看到相对应硬盘未分配的空间，选择未分配空间并点击[添加分区]，可以创建新的分区，对新的分区可设置容量、文件系统类型、保护类型和还原方式。

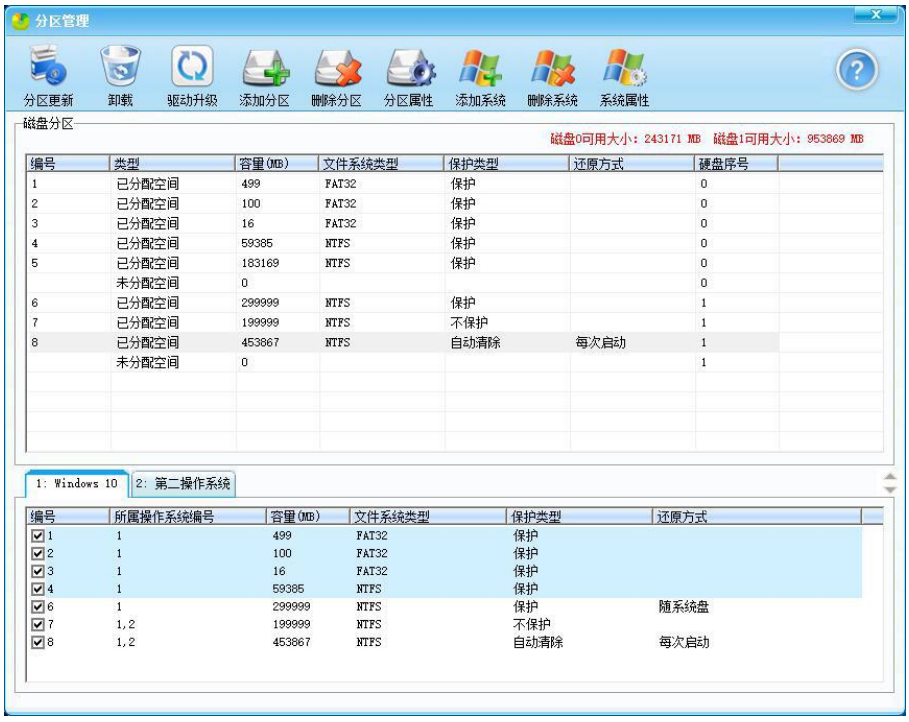
新创建的分区会罗列在分区列表中。通过[删除分区]和[分区属性]选项，可对已存的分区做调整。



分配分区

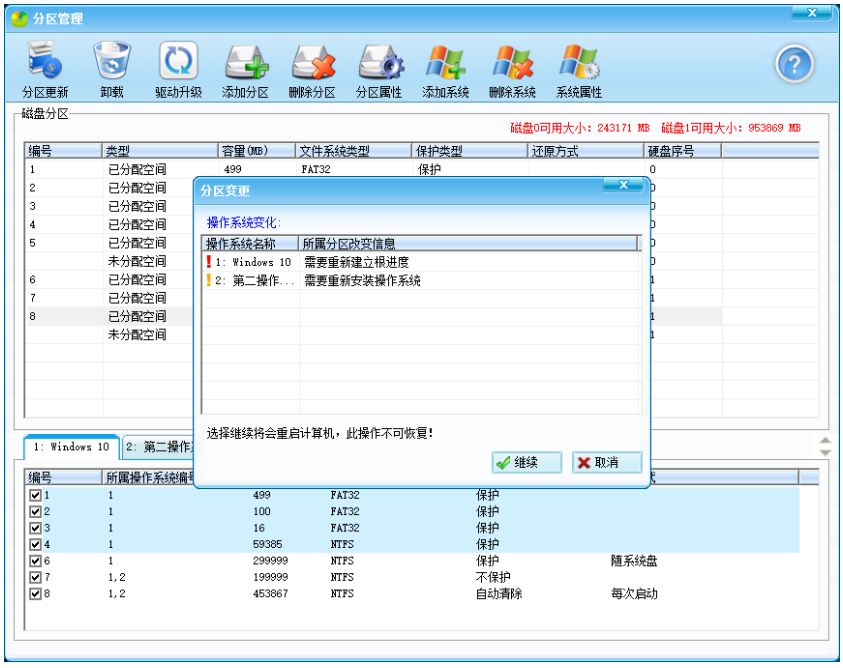
除了操作系统所必须的分区外，剩余的分区可自由分配给各操作系统，不保护和自动清除类型的分区可同时从属于不同操作系统。

保护型分区只能从属于一个操作系统，添加分区后，在所属操作系统下把分好的分区打钩分区更新即可。



分区更新

对分区和操作系统进行设定后，分区及操作系统管理界面点击[分区更新]，系统会保存相关更新内容，并重新启动系统。（如果提示初始化根进度，分区更新之前一定把要保留的进度写入根，分区更新后此操作不可恢复）。

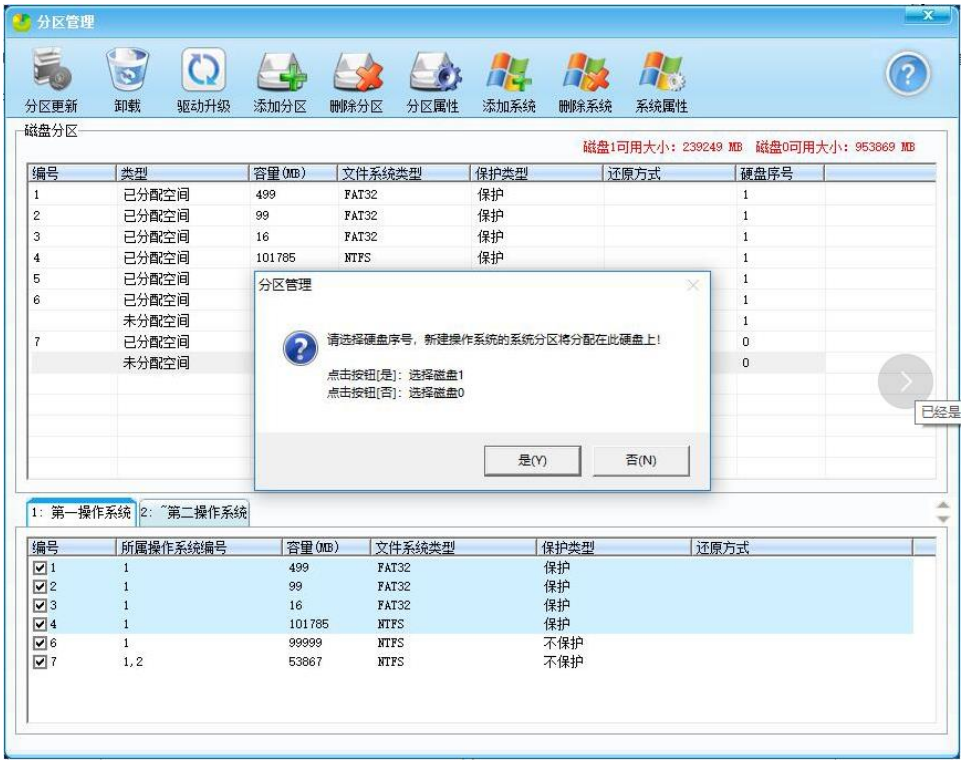


添加系统

在分区及操作系统管理界面点击[添加系统]，可以创建新的操作系统。首先会要求选择新创建操作系统硬盘序号，其次会要求对操作系统信息做设定，包括操作系统名称，以及操作系统类型。

每新建一个操作系统，系统盘都会顺序使用该硬盘分区，例如操作系统一使用了磁盘 0 上的编号 1、2 分区，则新建的操作系统如果还装磁盘 0 上则会使用编号 3 分区，添加系统之前确认此系统占用的分区是否有数据，请及时备份。

1、 首先添加系统分区后点击添加系统，控制台会提示对安装系统所在磁盘进行设置（建议系统优先安装固态上）



2、 选择安装磁盘后选择安装系统的操作系统类型 GPT 分区或 MBR 分区。

3、 控制台弹出系统属性界面，可对新添加操作系统做设置，点击[确定]。

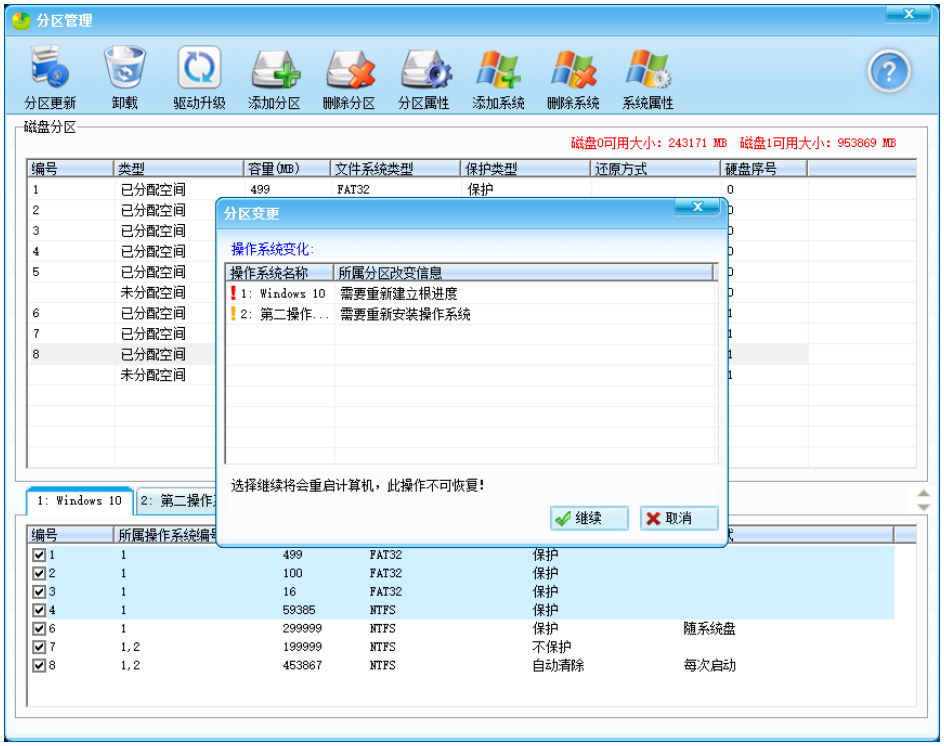
[输入密码才能进入] 设定密码后，在 Pre-OS 界面选择系统进入后，需输入相应密码才可以进系统。

[开放模式] 开放模式是完全不保护的一种模式，在下次开机重启时，开放模式下用户对硬盘数据的操作完全保留。

[隐藏操作系统] 在系统名称前加“~”可隐藏当前操作系统。（隐藏后将在开机选单界面不显示此系统，在底层开机选单界面进管理员界面方可调出此系统）

4、 对分区和操作系统进行设定后，分区及操作系统管理界面点击[分区更新]，系统会保存相关更新内容，并重新启动系统。

如果某个系统提示需要建立根进度，并且此系统有多个进度环境，一定在此系统下把要保留的进度提前写入根，然后分区更新，分区更新后此操作不可恢复。



5、系统重启后，在 Pre-OS 的操作系统选择界面，可以看到新创建的操作系统。此时操作系统和硬盘保护驱动还未进行安装，因此操作系统名称为白色。

多系统安装方法

6、 在 Pre-OS 的操作系统选择界面，光标移到新创建的操作系统，按[Home]键并输入硬盘保护控制台管理员密码，进入硬盘保护控制台管理员界面。在管理员界面，按[Ctrl+O]激活启动设备选单，此时选择相应启动设备，完成所选操作系统的安装。

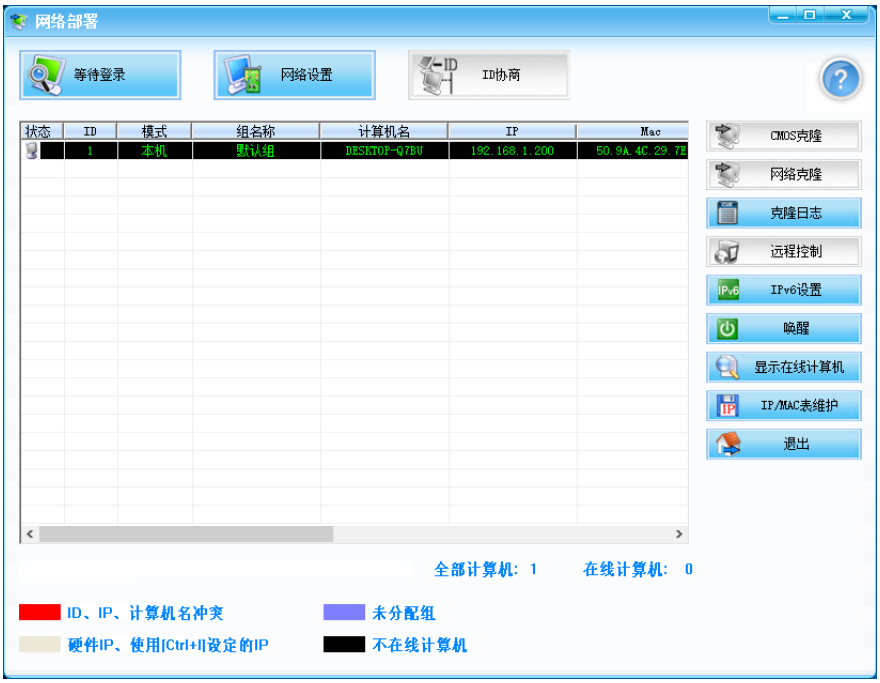
在安装操作系统时，选择“系统”类别的分区进行格式化、安装，这是该操作系统所对应的正确分区，其余分区不要做操作，否则会破坏硬盘保护控制台的分区状态。（如果是安装的 GPT 类型的系统选择引导分区下第一个主分区）

操作系统安装完成后，进入该操作系统，参照第 2.3 章，完成该操作系统下的硬盘保护控制台安装。

各操作系统及操作系统下的硬盘保护控制台安装完毕后，具备完整的硬盘保护功能，此时 Pre-OS 界面各操作系统名称变为黄色。

3.3 网络部署

登录 Windows 界面下的硬盘保护控制台，并选择[网络部署]，可进入硬盘保护控制台的网络部署管理界面。



登录到“发送端”的“客户端”计算机，根据状态不同，处于三种模式。

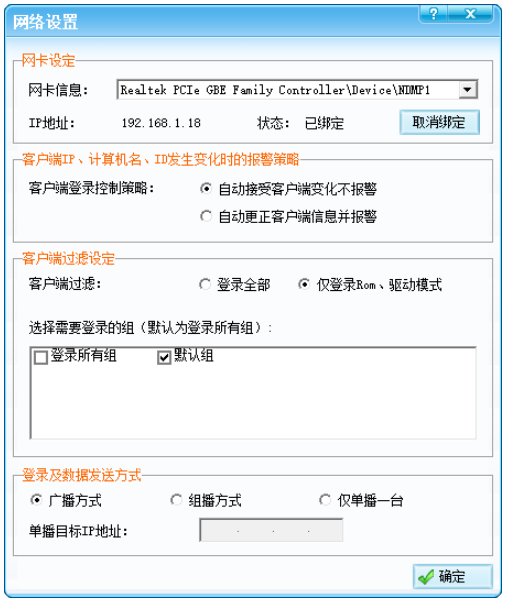
Rom 模式：“客户端”能够登录到“发送端”，但是仅能接收参数拷贝。

驱动模式：如果已经接收了参数拷贝，重启后，“客户端”计算机将处于驱动模式，可利用 Pre-OS 界面中提供的网络模块进行网络传输，驱动模式“客户端”能够接收“发送端”的分区数据克隆。

Windows 模式：进入 Windows 系统后的“客户端”处于模式，不能接收任何的克隆操作，但是能够被远程重启和关机。

网络设置功能说明

在网络部署管理界面点击[网络设置]，可触发网络设置工具，用以设定同传的基本参数。



网卡设定：如果本机有超过一块网卡，用户可以指定使用哪个网卡进行本次网络维护。如果一个网卡在开机阶段其 PXE 模块是打开的（能够接收其他计算机的网络维护），那么网络克隆程序将自动绑定到该网卡。

客户端 IP、计算机名、ID 发生变化时的报警策略：在已经安装了硬盘保护控制台的计算机中，会存在全局 IP/MAC 表格和用户组信息表。这些设置信息对机房内所有计算机来说应该是一致的。如果不一致，那么用户应该通过网络克隆程序的‘参数拷贝’对机房内计算机进行同步。当出现 IP/MAC 等信息不一致的情况时，克隆程序能检测到客户端的 IP 和 ID 等信息和本机存储的 IP 表中的内容不相符。

可以在此设定在检测到客户端 IP、ID 等变化时，是否强制用本机的设置更改客户端的设置。

客户端过滤设定：指定需要登录的计算机范围，本次网络维护仅对指定范围的计算机进行。计算机范围可以按计算机处于模式：ROM 模式、驱动模式、Windows 模式。也可以选择只对指定的用户组进行登录。

注意：用户必须属于一个已经存在的用户组，才可以被进行后续的网络维护。

登录及数据发送方式：设定网络克隆程序使用何种网络协议进行网络操作，包括广播、组播、单播。

对于广播方式方式，仅可以在一个局域网内进行网络维护，此时网络克隆程序不可以对跨网段的客户端计算机进行操作，因为路由器一般来说会丢弃广播数据包。

对于 IP 组播方式，可以对园区网络中的计算机进行网络维护，要求相连接的路由器支持并开启 IP 组播。如果用户的交换机支持组播，请开启交换机的组播支持，支持组播的交换机能够避免网络克隆对没有进行网络维护操作的计算机造成影响。

对大部分主板，即使在关机状态，其网卡仍处于 10M 工作状态（对有些主板，可以在 windows 上对网卡进行设置，将“网卡唤醒连接速率”设置为更高的速度，以避免主机处于关机状态时网卡工作在 10M 连接），此时由于其接收能力差而导致交换机的流控模块动作。当克隆的广播数据流量大于 10M 时，交换机会抑制发送端口的流量而造成克隆速度异常缓慢。出现这种情况时，用户应该使用支持组播的交换机，并选择网络克隆使用 IP 组播协议。

单播方式，对交换机和路由器没有限制。但是由于性能的考虑，克隆程序支持同时维护的计算机数量有限。

其它设置功能说明

ID 协商：

ID 协商是固定计算机的 ID，用户可以以驱动模式登录状态的“客户端”计算机上按上下方向键为客户端计算机指定 ID。该功能可以以所见即所得的方式为所有机房内客户端计算机分配 ID 号。

手动 ID 设定的“客户端”计算机必须处于驱动模式。

CMOS 克隆：不能同传 BIOS 中的密码和时间，因为 BIOS 中的密码和时间并没有存储在 CMOS 中。

将本机的 CMOS 数据克隆到所有登录的客户端计算机，本操作要求客户端计算机必须处于驱动模式，发送端进入 BIOS 里修改参数设置保存后重启后在硬盘保护套件界面按 HOME 键输入密码，ctrl+s 保存 BIOS 信息，进入系统后打开网络部署点击等待登录把客户端登录后，选择 CMOS 克隆，然后远程重启客户端机器。

传送 CMOS 时，要求“客户端”计算机必须处于 Driver 模式。

参数拷贝：

将本机的硬盘保护控制台驱动和硬盘保护控制台分区信息等参数克隆到登录的客户端计算机。

对于 ROM 模式的“客户端”，必须参数拷贝，重启客户端后，“客户端”才可以升级为驱动模式，只有处于驱动模式的计算机才可以接收数据克隆及 CMOS 克隆。

参数拷贝，要求“客户端”计算机必须处于 Rom 模式或驱动模式。

网络克隆：

将“发送端”分区数据发送到登录的“客户端”。如果操作系统的引导分区被选择克隆，那么该操作系统的根进度将被克隆到客户端。

网络克隆时，要求“客户端”处于驱动模式。

增量克隆：

网络克隆“发送端”选择进度点和参数拷贝进行增量拷贝。

当“客户端”和“发送端”有一样的根进度时，可以接受进度克隆。

进度同步要求“客户端”处于驱动模式。

克隆日志：

查看上次克隆操作的完成情况。网络克隆程序仅保留上次的克隆操作完成情况

要求“发送端”处于离线状态。

远程控制重启：

重新启动所有登录列表中的“客户端”计算机。如果需要重启部分“客户端”，用户应该在登录列表中选择一个或多个“客户端”后，点击鼠标右键，并在右键菜单中选择重启。

“客户端”可以处于任何模式。

远程控制关机：

关闭所有登录列表中的“客户端”计算机。如果需要关闭部分“客户端”，用户应该在登录列表中选择一个或多个“客户端”后，点击鼠标右键，并在右键菜单中选择关机。

“客户端”可以处于任何模式。

远程唤醒：

对所有历史计算机列表中的计算机进行网络唤醒操作。如果需要对部分计算机进行唤醒，用户应该在历史计算机列表中选择一个或多个计算机后，点击鼠标右键，并在右键菜单中选择‘唤醒’。

对已经处于开机状态的计算机，对其进行唤醒操作不会对该机有任何影响。

要求“客户端”处于关机状态。

显示历史计算机：

切换登录计算机列表到历史计算机列表。显示所有历史计算机。历史计算机指以前进行过网络维护的所有机房内的计算机。

此功能可以辅助查看哪些计算机还没有登录，或者，对已经关机的计算机进行远程开机操作。

IP/MAC 维护：

在 IP/MAC 维护界面中，用户可以对客户端计算机的 IP、计算机名称、所属组等信息进行编辑。

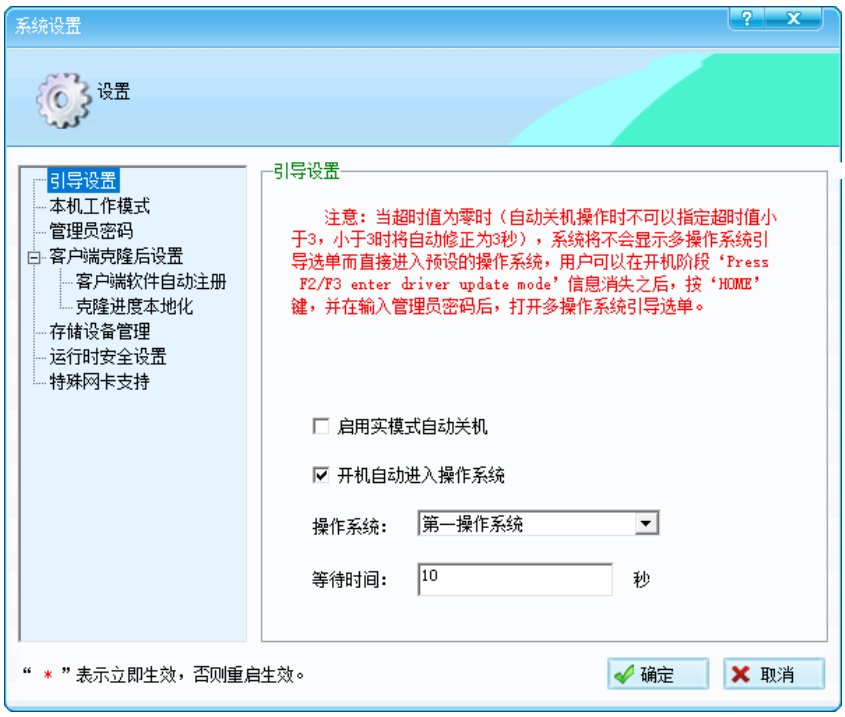
客户端计算机必须被指定给一个已存在的用户组才可以被网络维护。

对 IP/MAC 表格及组信息的任何更新操作之后，用户都应该通过‘参数拷贝’将本机的戴尔硬盘保护控制台参数克隆到机房内其他计算机中，以保证设置的一致性和全局性。

3.4 系统设置

用户在系统设置界面可以对硬盘保护控制台的运行方式进行更改。设置信息将会存储在本地硬盘保护数据区。用户可以通过硬盘保护控制台克隆程序的“参数拷贝”，将本机的全部硬盘保护控制台参数数据克隆到机房内其他计算机。完成后，接收‘参数拷贝’的其他计算机将使用和本机同样的硬盘保护控制台参数工作。

注意：硬盘保护控制台参数数据包括分区信息，操作系统信息，进度排程信息，及其他一切硬盘保护控制台的运行参数。“参数拷贝”的过程中，客户端计算机硬盘保护控制台的所有参数数据都会被更新。



引导设置：

勾选[启用实模式自动关机]功能后默认 10 秒，系统启动至 Pre-OS 系统选择界面时，如果在规定时间内没有操作，系统就会自动关机。

勾选[开机自动进入操作系统]功能后默认 10 秒，系统启动至 Pre-OS 系统选择界面时，如果在规定时间内没有操作，系统就会自动进入所设定的操作系统。

本机工作模式：

设定本机处于[个人模式]或是[机房模式]。

处于个人模式时，硬盘数据受到保护，但对于硬盘上的操作，默认在下次开机时不会被还原，用户可以选择性还原或备份。

个人模式下，可以设定备份策略，但不可设定还原策略，是否还原需手动选择。

处于机房模式时，硬盘数据受到保护，各种对硬盘数据的操作，在下次开机时都会被还原。

机房模式下，可以设定还原的策略， 但不可设定备份策略，只能手动做备份。

管理员密码：

修改硬盘保护控制台管理员密码。

软件自动注册：

对一些类型（不是所有类型）的用户应用软件提供支持，对这些软件，如果已经在发送端正确注册，那么克隆后，客户端计算机无需再次手工注册，即克即用。

克隆进度本地化：

如果“客户端”与“发送端”存在硬件差异，在克隆完成后，Windows 会发现新的硬件，并为新的硬件安装驱动程序。开启此项设置后，硬盘保护控制台检测到上述情况，会自动创建‘映射进度’，以保留客户端软件环境的变化。

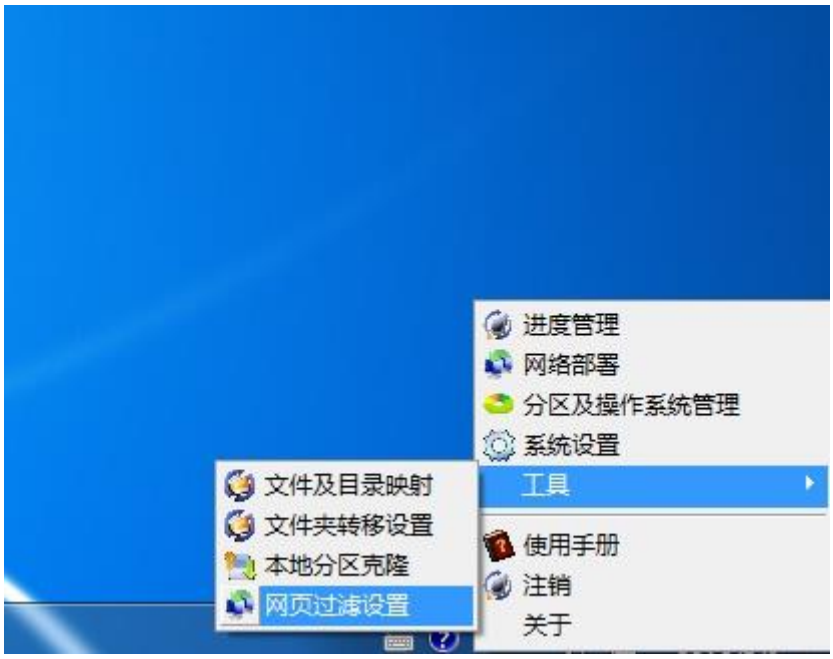
存储设备管理：

禁止 / 允许使用者在 Windows 之上使用 USB 存储设备。

禁止 / 允许使用者在 Windows 之上使用光驱设备。

3.5 辅助工具

登录硬盘保护控制台管理界面后，选择[工具]，可以看到四个辅助工具。



文件及目录映射：

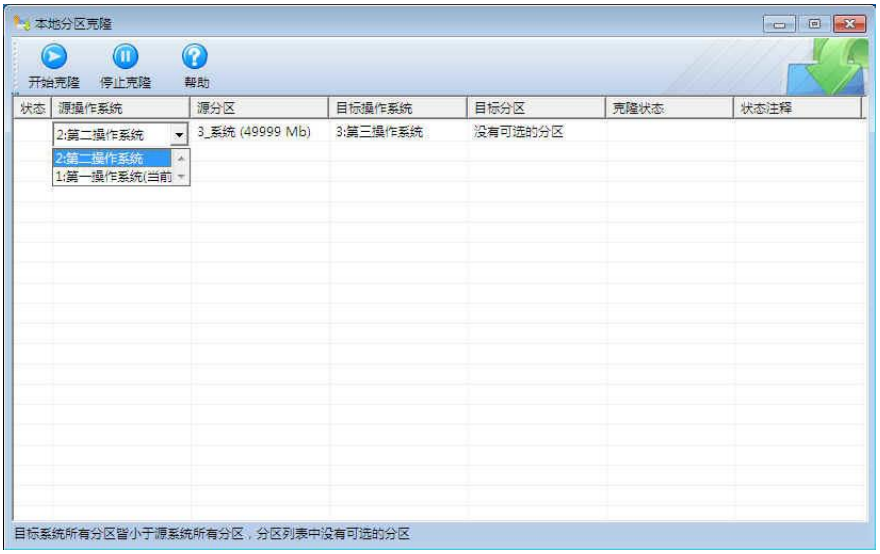
文件及目录映射功能可将用户选择的文件夹或某种扩展名文件映射到非保护分区中。这样，每次系统重新启动后，这些文件夹或文件将不会被自动还原。

文件夹转移：

将一些常用的重要文件复制到指定位置。

本地分区克隆：（只针对MBR系统win7）C盘前面没有100M小分区。

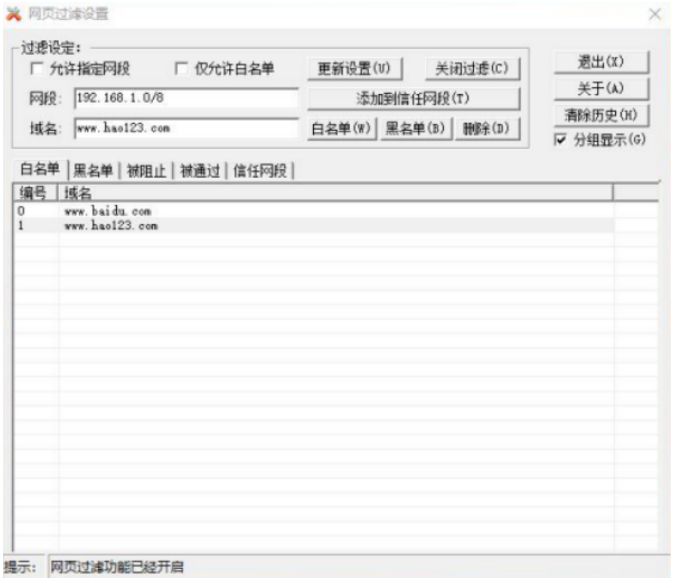
将某一分区或操作系统中的数据，复制到所选的目标操作系统或分区。



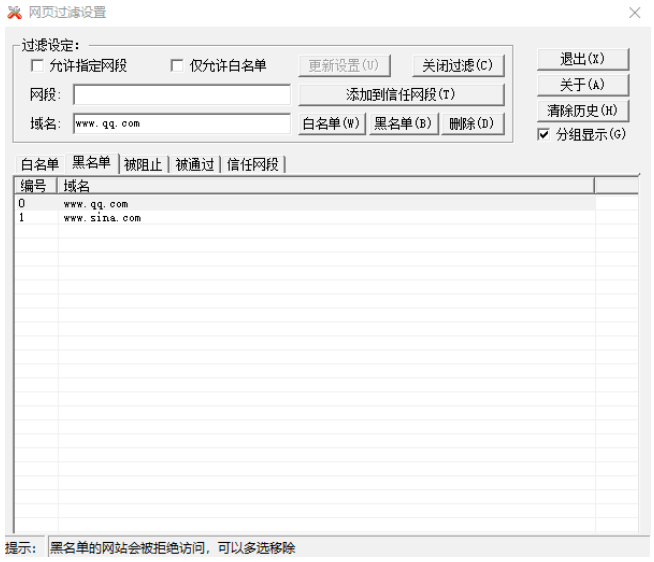
网页过滤设置：

1. 打开-工具-网页过滤器-开启过滤

2. 设置可以访问网站如www.baidu.com或者www.hao123.com 点击白名单按钮



3.设置不可访问的网站如www.qq.com或者www.sina.com 点击黑名单按钮，将不可访问此链接。



3.6 开机选单界面功能简介

在 Pre-OS 界面输入管理员密码后，即可看到相应的功能按钮和使用以下快捷键。

进度管理： 可对所选操作系统对进度环境做修改（创建、还原、存为根进度、勾选开机选单显示、修改进度名称和描述）

克隆接收： 使本机进入驱动模式为网络同传做准备

热键说明：详细的Pre-OS功能介绍

1、Windows键+Q　　关机

2、Windows键+W　　重启

3、Ctrl+O　　引导设备选单

4、Alt+O　　自动清除盘保留模式进入

5、Ctrl+方向右键　　切换背景图片

6、Ctrl+R　　还原当前操作系统上次进的进度

7、Ctrl+S　　备份BIOS设置信息

8、Ctrl+Z　　恢复BIOS设置信息

9、Ctrl+T　　更换按钮图标

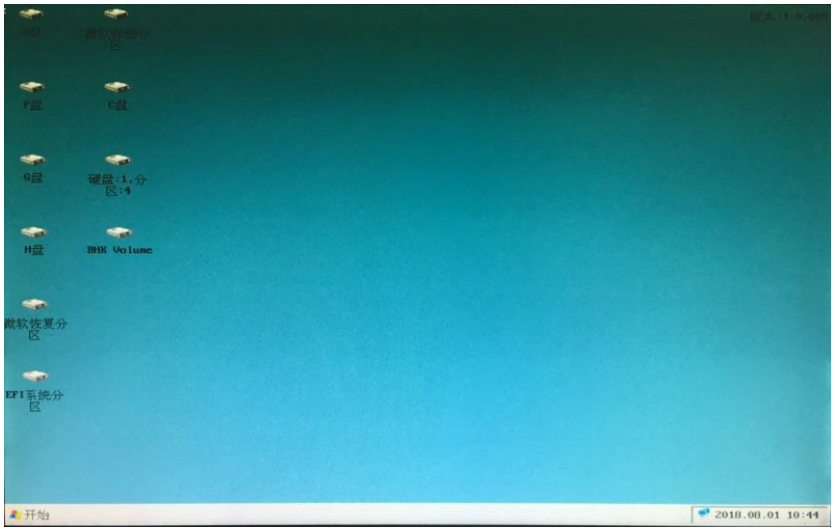
10、Ctrl+W　　保存目前开机选单布局

11、Ctrl+A　　可以进高级模式访问当前进度里面的数据，并可以拷贝到不保护分区或移动设备。

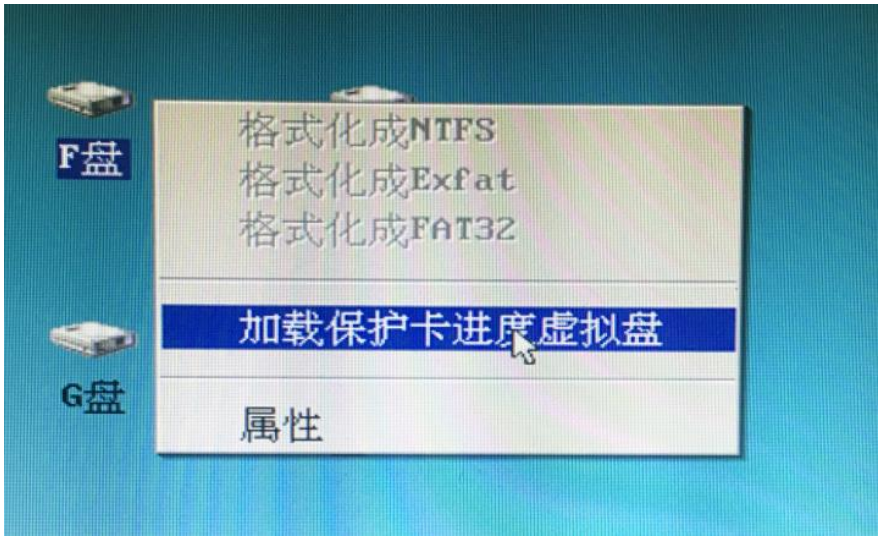
高级模式

可在高级界面访问当前进度里的数据，并可以把重要数据拷贝到不保护分区或移动设备。

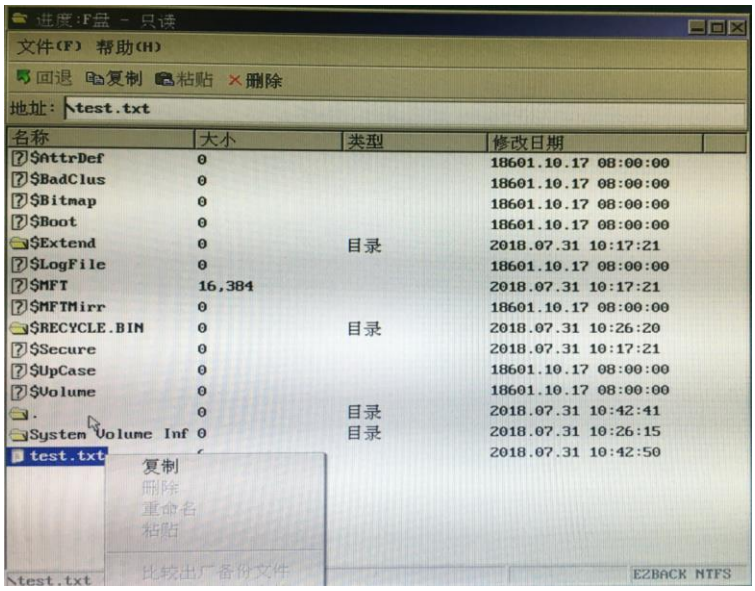
1、 在Pre-OS开机选单界面选中该系统，输入管理员密码后，按Ctrl+A进入高级界面。



2、 选择需要拷贝的资料盘，鼠标右击文件所在保护的盘符，加载保护卡虚拟磁盘



3、 在高级桌面上即可看到带‘进度’的此盘符。选中需要拷贝的资料，右击此文件点击复制后即可粘贴到不保护分区或移动设备。拷贝完成之后即可重启电脑。

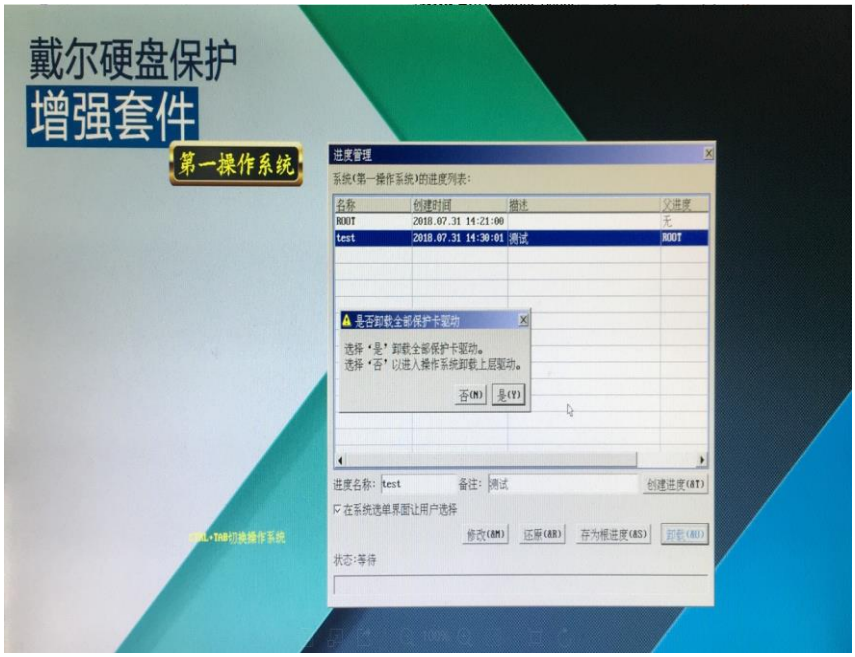


第 4 章卸载硬盘保护控制台

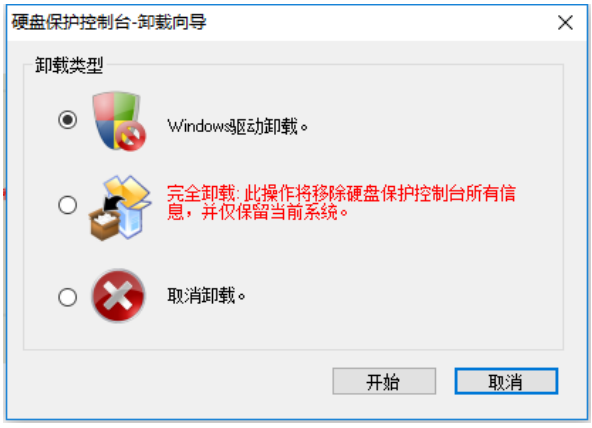
4.1 pre-os 卸载

在 Pre-OS 界面下，按[Home]键并输入硬盘保护控制台管理员密码，登录至管理界面，选择[进度管理]，点击[卸载]。提示选择何种拆卸类型。如果选择是则卸载控制台全部驱动且保留当前系统根进度的用户环境（如需保留某进度环境

请提前选择此进度写入根）



如果选择“否”，则只卸载当前系统的上层保护驱动，选择“是”，则卸载硬盘保护控制台的所有驱动，并且只保留当前系统的 ROOT 环境。且此操作系统进度环境将被删除（如需保留某进度环境请提前选择此进度写入根），进系统后会弹出卸载类型界面；



Windows 驱动卸载：

仅会卸载当前操作系统下的硬盘保护控制台保护驱动。Pre-OS 界面，以及其他操作系统下的硬盘保护控制台驱动不会被卸载。

完全卸载：

会卸载所有操作系统下硬盘保护控制台驱动，并卸载 Pre-OS 界面，并仅保留当前操作系统。

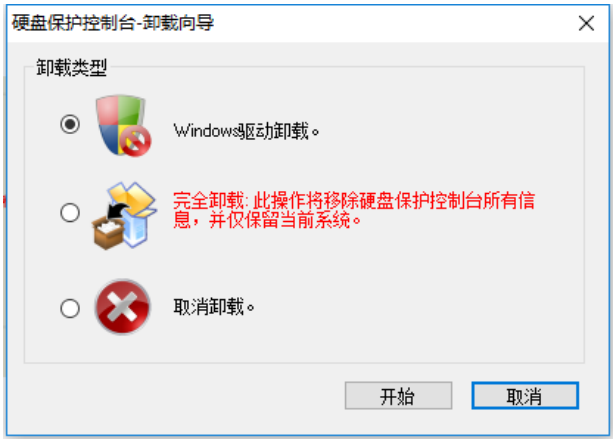
4.2Windows 下卸载

从[控制面板-程序和功能]中卸载：

首先硬盘保护控制台改为个人模式。

然后从[控制面板-程序和功能]中卸载硬盘保护控制台，硬盘保护控制台卸载后，点击[重启动]。（只保留当前操作系统 ROOT 进度环境）

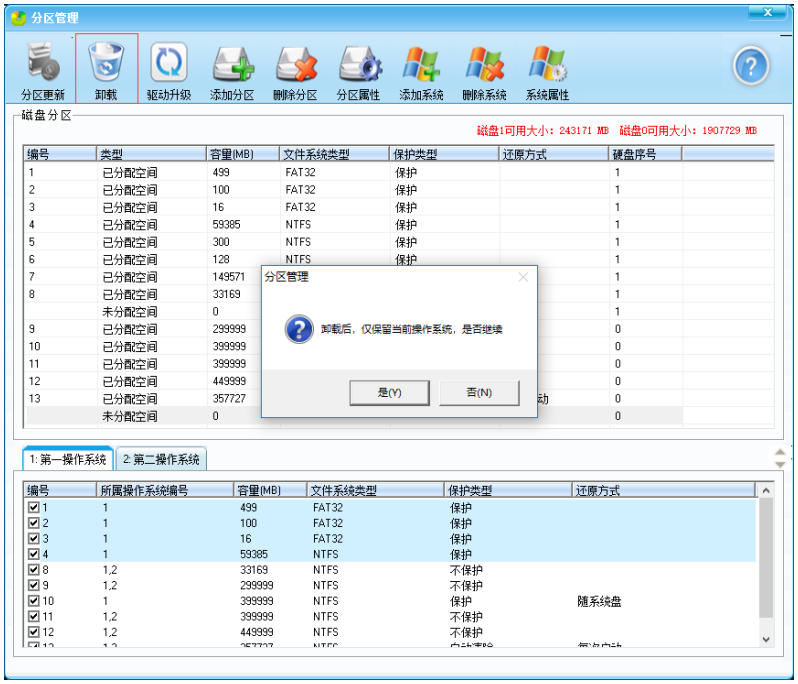
出现卸载类型选择界面，请选择相应类型进行卸载。



从分区管理工具中卸载：

当各操作系统中的硬盘保护控制台 Windows 驱动都被卸载后，Pre-OS 界面还存在，但 Pre-OS 下的拆卸和控制面板-程序和功能中的卸载都已不可用，此时如果想卸载 Pre-OS 界面，可按以下方式操作。

进入硬盘保护控制台安装包，管理员运行 Partition.exe 程序，打开分区管理工具，点击[卸载]，系统会提示卸载后，仅保留当前操作系统，点击[是]继续。



此时系统会自动卸载 Pre-OS 界面并重新启动操作系统(此操作仅保留当前操作系统)。

第 5 章硬盘保护控制台注意事项

1、初始密码是什么

dell

2、关闭 UAC

➢安装硬盘保护控制台前，请先将 UAC(User Account Control，用户帐户控制)关闭，否则在安装时，会提示“请先关闭 UAC”。

3、无法绑定指定网卡

➢在安装硬盘保护控制台前，请先配置网络环境（IP、网关、掩码、DNS），否则使用网络同传功能时，会提示“无法绑定指定网卡”。

4、提示检查防火墙设置

➢在安装戴尔硬盘保增强套件前，请关闭防火墙，否则使用网络同传功能时会

提示“请检查防火墙设置”。

5、安装操作系统

➢在通过硬盘保护控制台创建分区后，在该分区安装操作系统时，选择“系统”类别的分区进行格式化、安装，这是该操作系统所对应的正确分区，其余分区不要做操作，否则会破坏硬盘保护控制台的文件体系。

6、如何进入 Pre-OS 的管理界面

Pre-OS 的管理界面按[Home]键,输入管理员密码

7、怎么解决网络传输速度异常缓慢的问题？

主要有以下几种解决方法：

（1）用户网络设备（交换机或路由器）必须支持广播，如果网络设备不支持广播，请进行更换。

（2）在网络同传时请断开网络的外部连接，仅保障局域网内计算机网络畅通，这样可提高同传效率。

（3）在存在多台计算机和多级网络设备的复杂环境下，用户网络中可能存在慢速设备（可能是不良网线或者不良交换机）。这可以通过让相关人员先使用用户所用的单台交换机来进行同传，从而对慢速设备进行定位（如果在整个网络中进行测试，较难定位问题）。对慢速设备定位完成之后更换相应设备，再次进行单台交换机的同传测试，速度正常后再进行所有计算机的网络测试。如果速度仍有异常，建议排查网线。

8、为什么在使用网络管理的网络唤醒功能时，不能正常唤醒被控端计算机？

BIOS 中必须开启唤醒功能，关闭深度休眠。

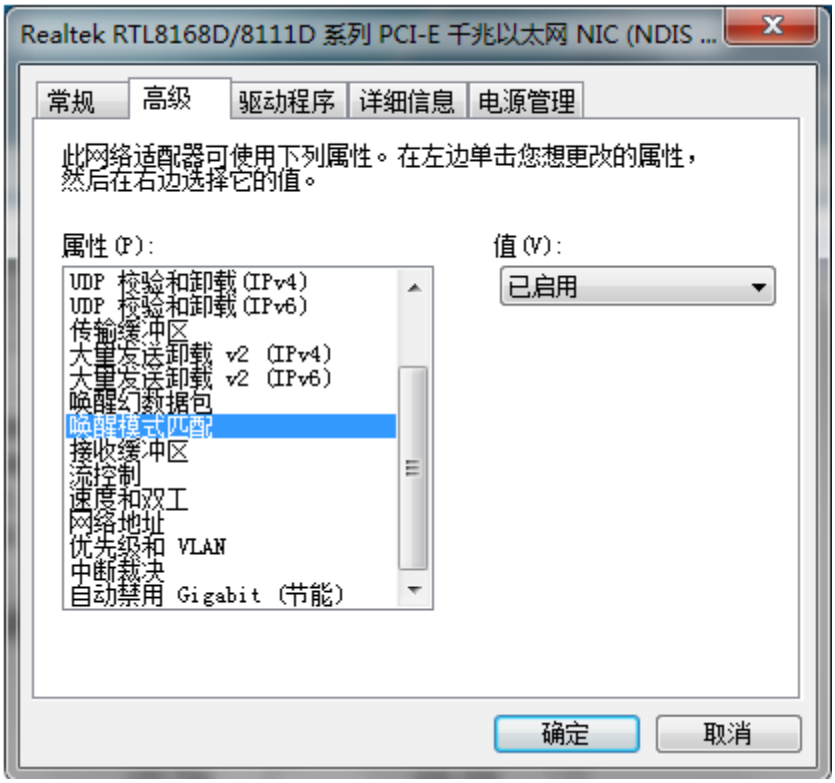
在您使用网络唤醒功能之前，应保证所有被控端计算机的网卡都支持网络唤醒的功能，这可以通过以下方式设置：

（1）对于所有被控端计算机（可通过网络复制实现），打开“设备管理器”，右键单击网卡，选择“属性”；

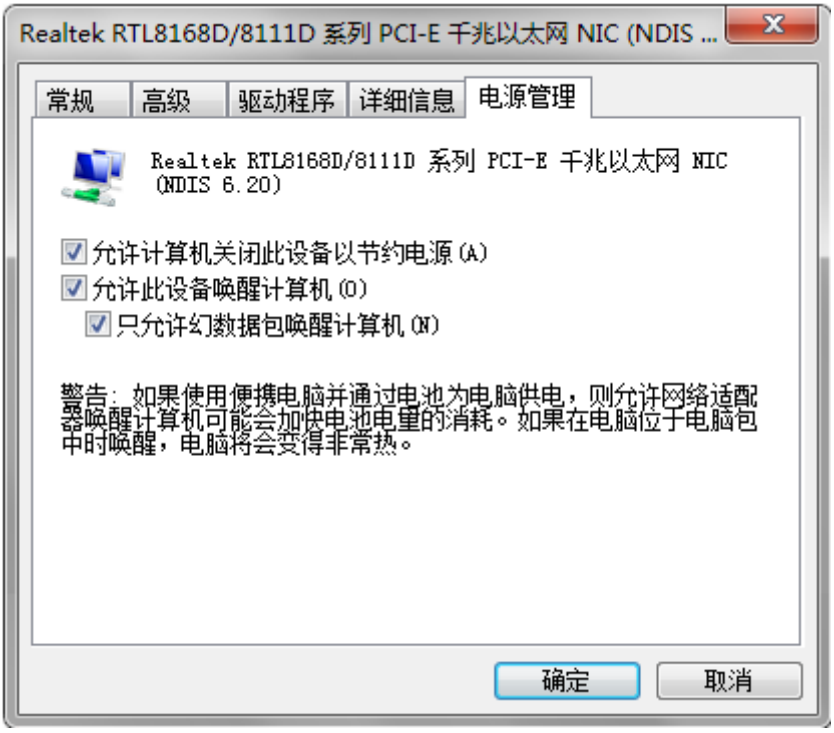
（2）单击“电源管理”，勾选“允许这台设备使计算机脱离待机状态”选项；

（3）单击“高级”，在属性栏中选择“唤醒模式匹配”，将值设置为“已

启用”，如下图所示，这样就可以实现网络唤醒功能了。



以及在“电源管理”中勾选允许唤醒该计算机。



这样就可以实现网络唤醒功能了。

9、网络同传功能对网络环境有什么样的要求？

（1）交换机不限制广播及多播传输功能。

（2）网络中的设备使用五类双绞线连接，并且保证双绞线的质量优良。

（3）网络环境中的布线合理，无环路。

（4） 网络中的计算机不能连接串口设备，否则将不能进行网络同传功能。

10、采用多操作系统安装，安装完操作系统后，不能正常引导。

可能的原因：在规划完分区后，安装操作系统时，没有安装在规划的系统分区，而是安装在其它的未分配磁盘空间上，还有可能破坏其它已安装的操作系统；磁盘上的原有分区（运行硬盘保护控制台磁盘分区工具之前，存在用第三方非微软的分区工具创建的分区），硬盘保护控制台仅支持微软分区工具创建的磁盘分区。

11、自动还原设置失效。

可能的原因：用户将本机状态设置为“个人模式”，自动还原功能将会被屏蔽。

12、进行网络克隆时，提示存在重复的 IP、ID、计算机名称。

可能的原因：已登录的客户端计算机 IP、ID、计算机名称和发送端保存的曾经登录过的客户端计算机 IP、ID、计算机名称有重复，点击显示历史计算机按钮就可以看到重复的机器。

13、修改客户端计算机的 IP 后，重新登录修改未生效。

可能的原因：修改客户端计算机的 IP 等信息后，需要勾选“参数拷贝”对客户端传送硬盘保护控制台参数。

第 6 章更换主板后设置 BIOS 注意事项

1. 重新启动硬盘保护功能前，请务必登录戴尔官方支持网站获取最新的 BIOS。
2. 请按 2.1 “安装前的准备”的第三步设置 BIOS。
3. 更换主板后 BIOS 选项中必须带有 dell 硬盘保护的支持选项，HDD Protection support

第一章网络控制台产品简介

网络控制台系统是针对戴尔硬盘保护控制台而研发的远程监控操作平台，是

对公共机房内计算机的维护和监视管理中心。可以使用系统对机房内的计算机进行有效的监控，包括对客户端计算机的硬件资产监控，客户端恶意进程监控、客户端计算机安装软件监控，客户端网络使用情况监控；重启、唤醒、关闭客户端；远程为客户端计算机时钟同步，还可以对客户端发送消息，锁定客户端键盘鼠标、屏蔽客户端外网、屏幕监控、屏幕广播等。

网络控制台是对机房维护与监控的完美结合，必将成为机房管理员的有力助手。拥有网络控制台系统，您便可以分享到功能强大的机房维护客户控制技术，使您的工作变得更加轻松！

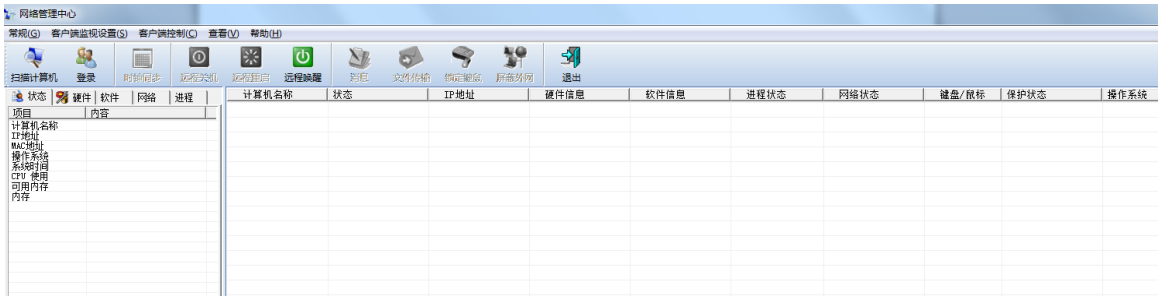
1.1 监控构成

网络控制台由两部分构成：教师端和学生端。

教师端是指任意一台已安装戴尔硬盘控制台的计算机。

学生端是指已安装戴尔硬盘控制台驱动程序的计算机。

1.2 网络控制台主界面布局



网络控制台界面

1.3 网络控制台的功能

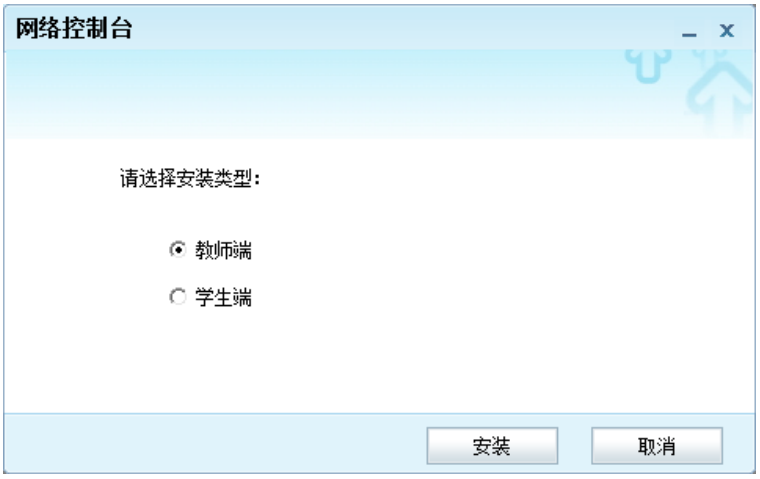
网络控制台系统功能包含客户端监视和客户端控制两大功能模块。监视模块可以查看客户机实时属性或者历史属性、监视客户端恶意进程、软硬件资产和网络状态；控制模块可以对被控端进行远程重启、远程唤醒、远程关机、时钟同步、屏幕监看、屏幕广播以及对所有学生端计算机发送消息，锁定客户端键盘鼠标、屏蔽客户端外网和全部网络等操作。

第 2 章 安装和卸载

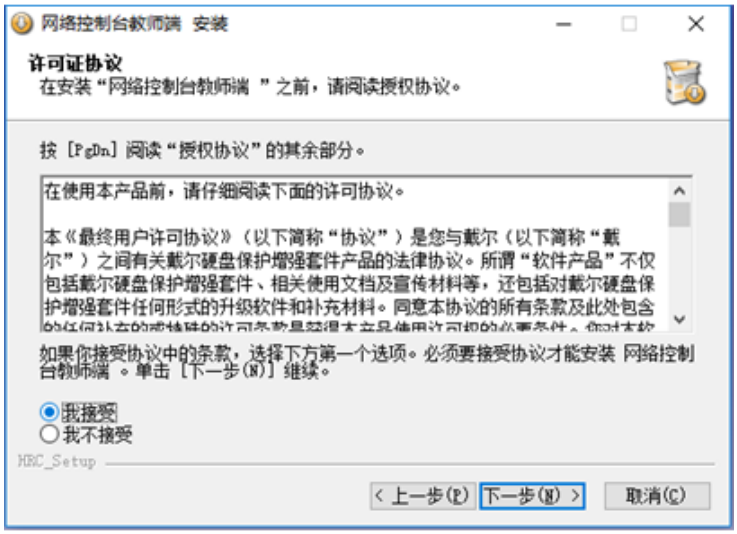
2.1 软件安装

网络控制台系统是由教师端和学生端两部分组成。

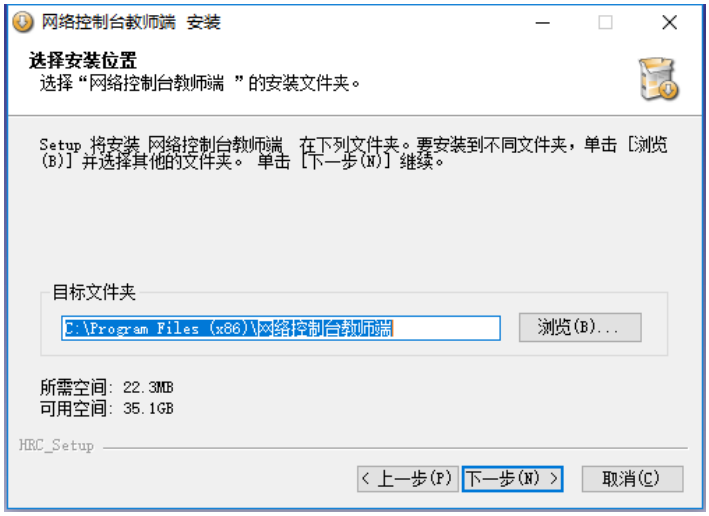
1. 在教师机 Windows 操作系统下执行 setup 程序来进行安装，教师端。



2. 下一个页面是关于网络控制台系统的使用协议，请仔细阅读，然后点击**接受**。如果您想继续安装过程，您必须接受这一协议。

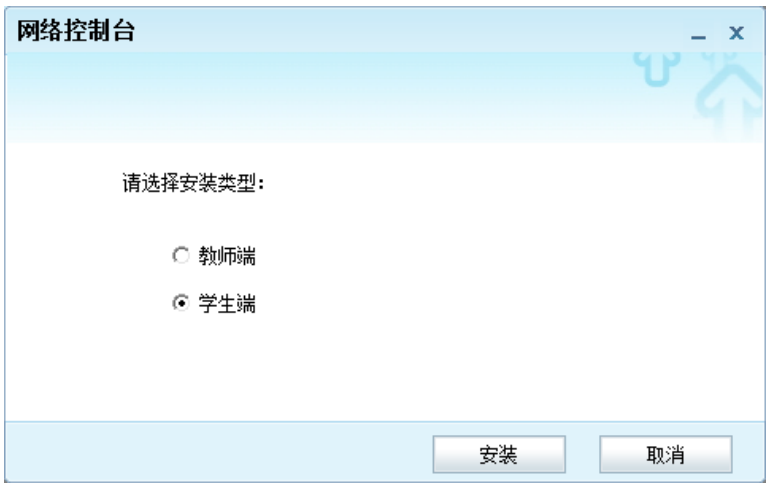


3、然后选择安装路径，您可以将安装文件保存在默认位置或输入新的路径。

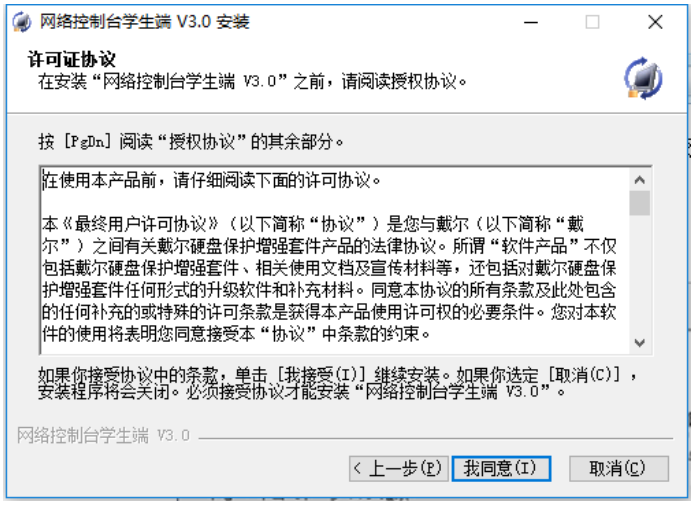


4、安装完成后，用户不需要重启计算机就可以使用网络控制台教师端。

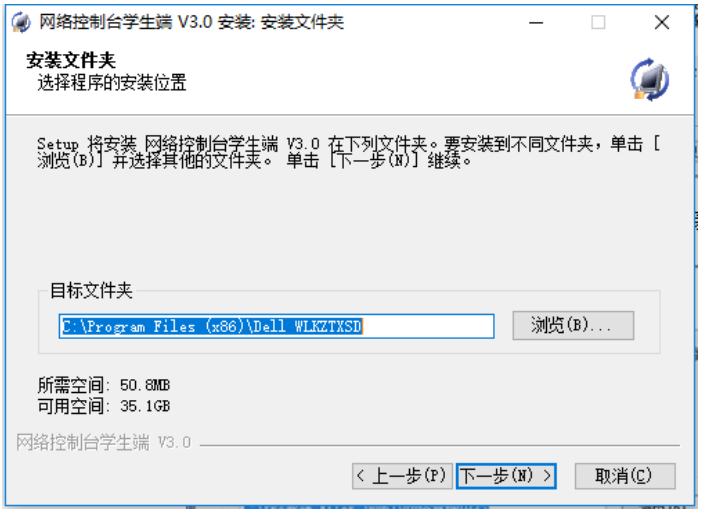
5. 在学生机 Windows 操作系统下执行 setup 程序来进行安装，选择安装学生端。



6. 下一个页面是关于网络控制台系统的使用协议，请仔细阅读，然后点击**接受**。如果您想继续安装过程，您必须接受这一协议。



7. 然后选择安装路径，您可以将安装文件保存在默认位置或输入新的路径。



注意：教师端必须关闭网络防火墙才可以使用。

2.2 软件卸载

网络控制台卸载可以通过以下方式：

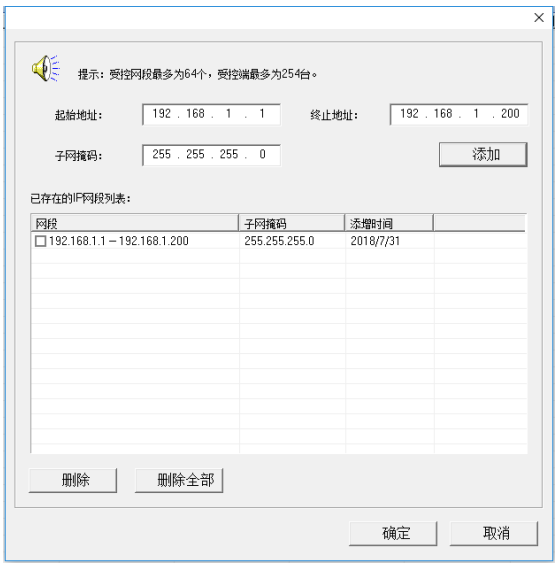
通过【控制面板】【添加或删除程序】卸载网络网络控制台。

第 3 章 登录学生端

3.1 设置扫描网段

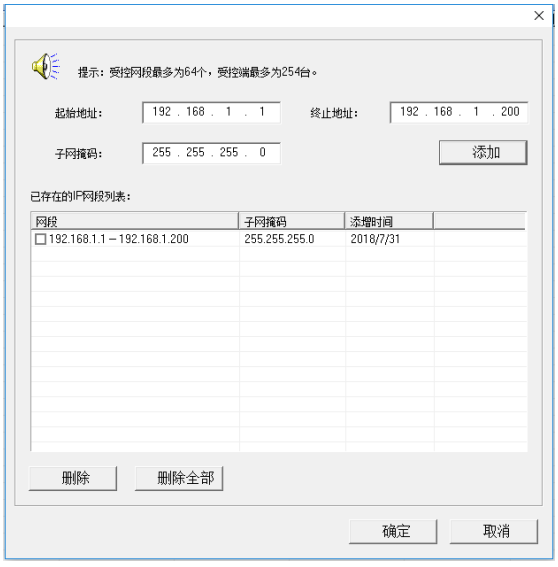
必须设置客户端的 IP 地址范围才可以进行客户端扫描，网络控制台仅会扫描‘扫描网段’内活动的学生端计算机。添加的网段对应的子网掩码也必须正确设置。

扫描网段的添加：



打开网络控制台主界面，单击菜单栏【常规】选项卡（键盘 Alt+G），单击【设置扫描网段】（键盘 A），在弹出的扫描网段设置对话框中输入需要扫描的网段（客户端 IP 地址范围）和子网掩码，单击【添加】按钮，单击【确定】按钮完成添加。

扫描网段的删除：

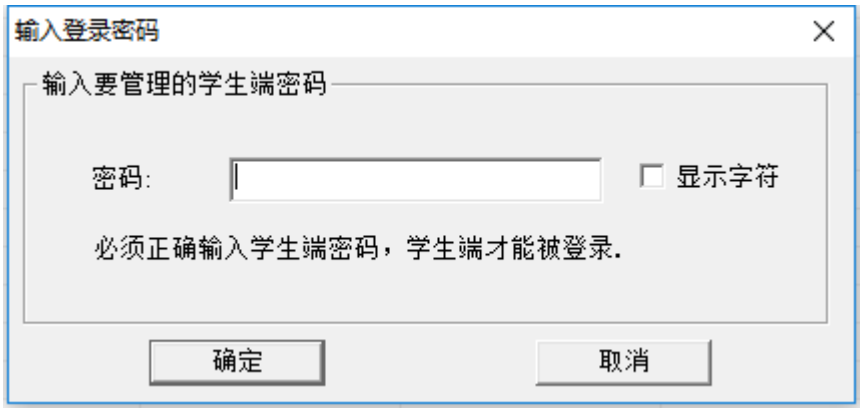


单击【删除全部】按钮，删除所有已存在的网段，或者勾选网段列表中已存在的网段，单击【删除】按钮删除选中的网段。此操作是可恢复的，如果用户错误的删除了不应删除的网段，那么单击【取消】按钮可以撤销本次操作。

注意：以上操作在点击确定按钮后有效。

3.2 输入登录密码

登录密码为学生端密码默认 dell，（如后期更改密码需要在硬盘保护控台进度管理中创建进度保存），网络控制台仅能扫描和控制与输入密码相同的计算机。使用过程中程序会记住最后一次输入的密码；退出网络控制台后用户输入的密码将自动被清空（本机教师端不会存储任意客户端的任何密码信息）。



单击菜单栏【常规】（键盘 Alt+G），单击【输入登录密码】（键盘 Ctrl+P），输入密码点击【确定】按钮。

3.3 扫描计算机与登录客户端

用户可以开启网络控制台的扫描，扫描发现扫描网段内活动的客户端计算机。网络控制台可以将扫描到学生端列表。学生端列表会一直存储在教师端计算机中，教师端仅能控制学生端列表中的计算机。首次使用网络控制台系统，因为学生端列表为空，用户必须通过扫描计算机并将扫描到的客户端计算机添加到学生端列表方可进行后续的操作。点击工具栏‘扫描计算机’扫描客户端计算机：

扫描计算机

完成扫描

点击【扫描计算机】后按钮会变为‘完成扫描’，待所有计算机都被扫描上来后，点击【完成扫描】按钮，然后选择是否将扫描到的客户端计算机添加到学生端列表。

如果学生端列表不为空，可以点击【登录】按钮对学生端计算机开始连接控制。

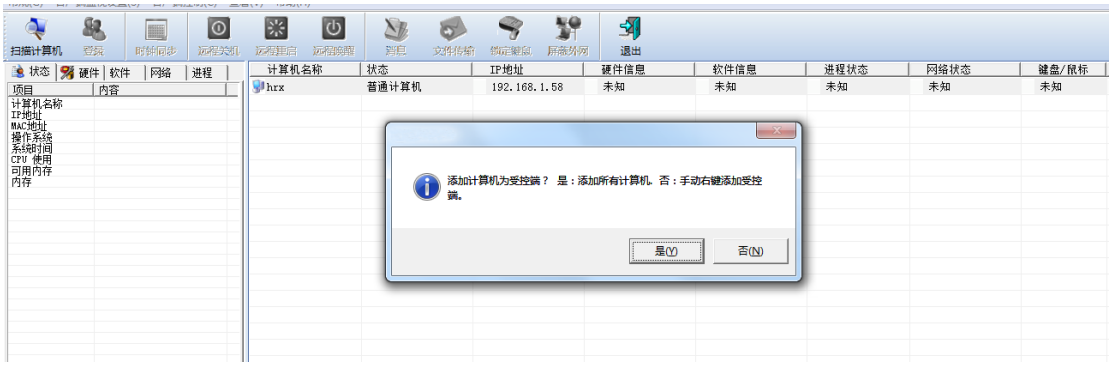
3.4 普通计算机、未登录学生端和登录学生端的区分

在计算机列表中三种状态的计算机，分别为非受控计算机显示“普通计算机”图示：  ，用户不能对该计算机进行任何监视和控制。未登录的学生端显示“未登录”图示：  ，用户仅可以对其进行网络唤醒（该计算机必须支持此功能）。登录的学生端显示“登录”图示：  ，用户可以使用网络控制台提供的功能进行监视和控制。

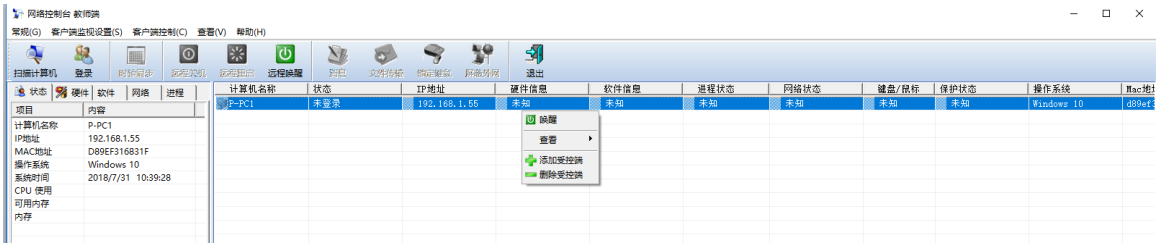
3.5 添加学生端

扫描上来的普通计算机必须添加为学生端，才能被网络控制台监视与控制。用户可以将所有“普通计算机”添加为学生端，也可以选择性的添加。以下为添加学生端的两种方式：

1.完成扫描按照提示添加学生端



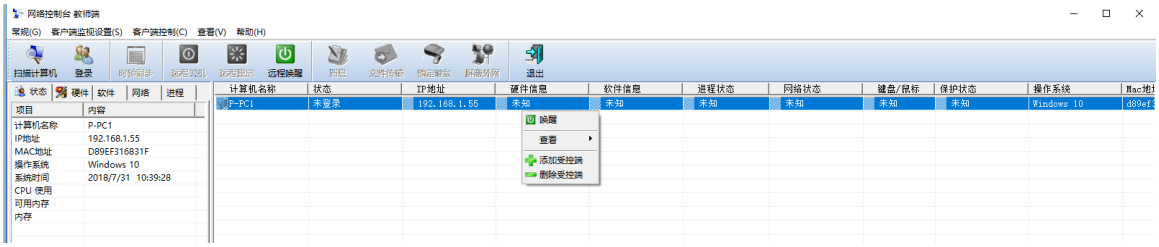
2.通过列表右键菜单添加学生端



单击【完成扫描】，如果存在普通计算机（非学生端计算机在计算机列表状态列显示），会弹出提示添加学生端对话框。单击【是】将所有普通计算机添加为学生端，单击【否】，放弃添加所有普通计算机。还可以通过在计算机列表中单选或者多选普通计算机，单击鼠标右键选择【添加学生端】。

3.6 删除学生端

在计算机列表中可以通过鼠标选择一个或多个学生端，单击鼠标右键选择【删除学生端】删除选中的学生端。



第 4 章 客户端监视设置

4.1 资产监视设置

在非监控状态（登录学生端之前）可以设置需要监视的资产。资产监控默认监视硬件、软件、进程、网络。用户可以更改监视的轮询时间（信息更新的时间间隔）或者取消某一项资源的监控。如果取消某一项资源的监控，那么相应的计算机列表中相应的列显示状态为“未知”，该资源的改变将不受网络控制台系统的监视。如果学生端某一项资源与上次登录时没有发生改变则显示为“正常”，否则显示为“异常”。异常状态参考查看学生端异常状态。

单击菜单栏【客户端监视设置】（键盘 Alt+S），选择【资产监视设置】（键盘 A），弹出资产监视设置对话框，设置相应选项。

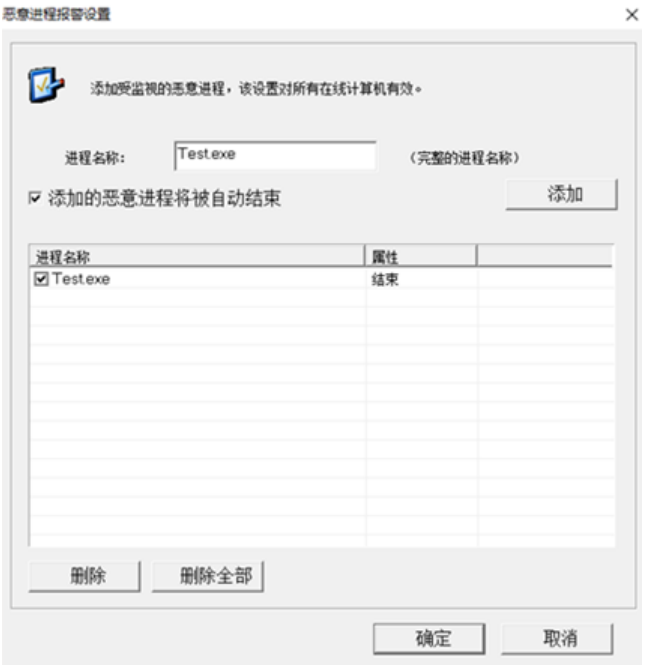
4.2 恶意进程监视设置

恶意进程监视设置是实时生效的，无需重新登录学生端。对监视到的客户端恶意进程有两种处理模式：自动结束和界面报警。被设置自动结束的恶意进程，将会在客户端检测到之后强行终止。设置为界面报警的进程被检测到后，教师端在计算机列表的进程状态列中显示“警告进程”，用户可以通过【资源栏】中【进程】列表查看警告进程详细），如果需要结束该进程可以选择【资源栏】中进程选项卡，在进程列表中选择相应的进程单击鼠标右键，选择菜单中的结束进程操作。

输入的进程名称必须是完整的，比如 Test.exe 或者 cmd.exe。

单击菜单栏【客户端监视设置】（键盘 Alt+S），选择【恶意进程监视设置】，弹出恶意进程监视设置对话框。

添加报警进程：



输入恶意进程名称，单击【添加】按钮，单击【确定】按钮。在已添加列表属性列中显示对该进程的处理类型。

添加主动结束进程：

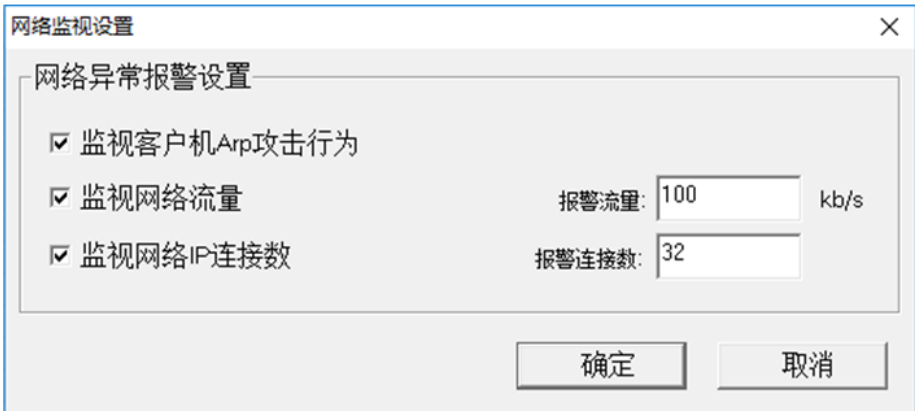
输入恶意进程名称，勾选【恶意进程将被自动结束】，单击【添加】按钮，单击【确定】按钮。在已添加列表属性列中显示“结束”属性。

删除恶意进程设定：

在恶意进程设置界面中，单击【删除全部】，可以删除所有已添加的恶意进程（不需要勾选进程操作）。也可以勾选单个或者多个进程，单击【删除】，删除勾选的恶意进程。注意，删除的操作是可以恢复的，如果用户想取消以上的操作，点击取消按钮直接退出本界面。点击【确定】后恶意进程设置将被真实删除。

4.3 网络监视设置

网络状态监视功能可以对客户端的网络状态进行实时监测。在网络监视设置中，可以设置开启对客户端 ARP 扫描攻击进行监控（默认开启），还可以设置客户端网络流量异常的阈值（默认为 100kb/s），客户端 IP 链接数异常阈值（默认为 32），开启监测后，一旦客户端的网络流量，IP 连接数超过了设定的阈值，网络控制台将进行报警：在客户端登录列表栏中客户端的网络状态属性显示为“异常”。可以双击该客户端的相应属性字段查看该客户端的网络流量信息（参考查看学生端异常状态）。



在主菜单中选择【客户端监视设置】（键盘 Alt+S），然后选择【网络监控设置】（键盘 N），可以打开‘网络监视设置’对话框。

第 5 章 客户端监视

5.1 查看学生端资源

对于处于登录状态的学生端在资源栏中显示的是该客户端当前的信息，对于处于非登录状态的学生端，资源栏将用于显示该客户端的历史信息。资源栏中包括学生端的基础信息、软硬件信息、网络信息和进程信息。

在网络控制台界面，点击【登录】后将开始对登录列表中的计算机进行监控。网络控制台将根据‘资产监视设置’设定的查询时间间隔获取客户端的软硬件，进程及网络信息，并将获取的客户端当前信息与客户端的历史信息对比，或者判定是否客户端的实时信息是否已经超过了设定的阈值并产生报警信息。

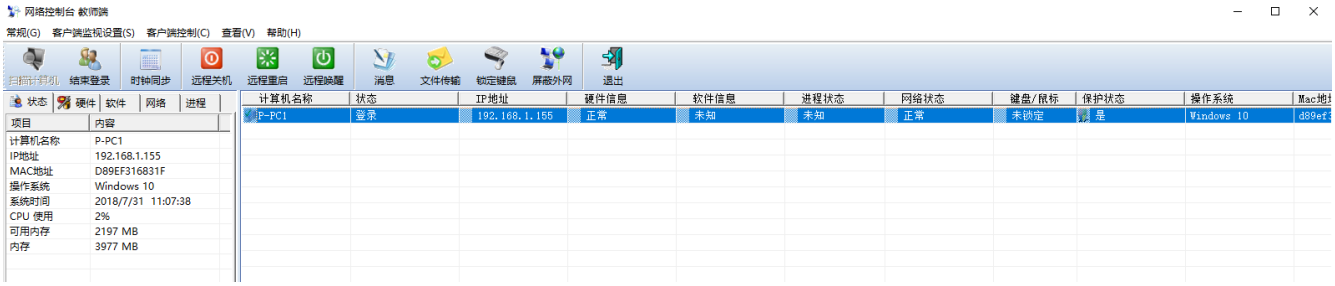
当客户端的某一属性异常，那么该客户端该属性将会显示为‘异常’，否则该客户端的该属性将显示‘正常’，如果网络控制台在一定时间内未能获得该客户端的某一属性信息，那么该属性字段将会显示‘未知’。客户端各个属性的详细信息在‘资源栏’中显示，单击某一客户端，资源栏中将切换到该客户端的各个属性信息，可以在资源栏中切换属性页查看该客户端的各个属性信息（参考查看学生端异常状态）。

可以在主菜单中‘查看’菜单项中勾选‘资源栏’打开‘资源栏’的显示。

提示：在资源栏中的‘进程’属性页，可以在选中某一客户端进程后，通过右键菜单选择【结束进程】，结束该进程。

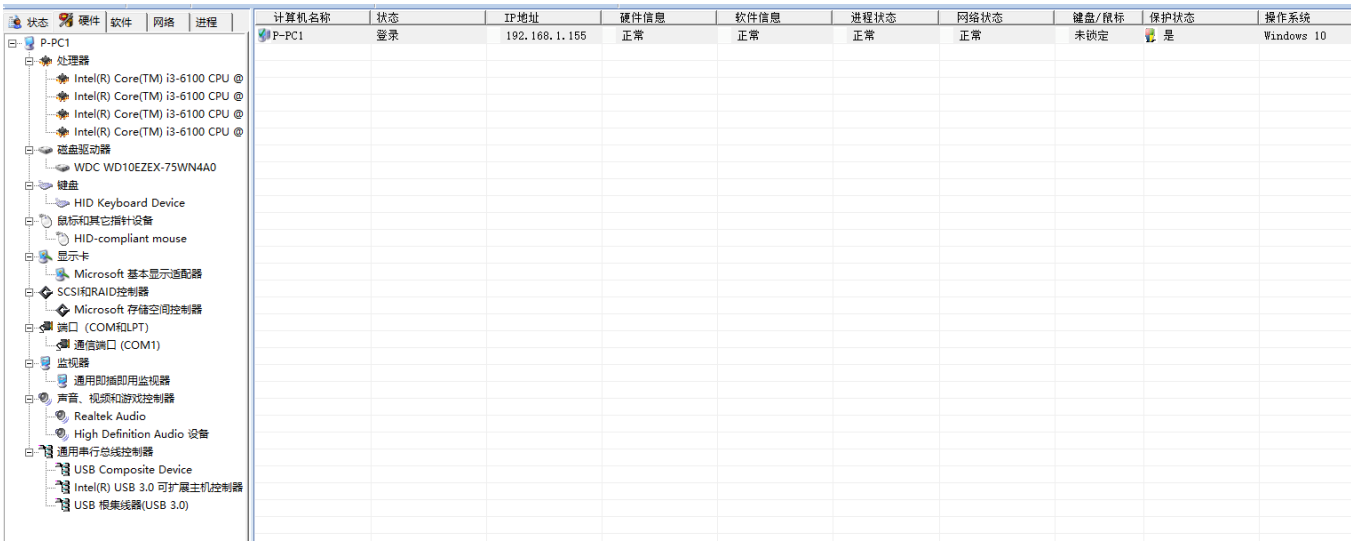
5.1.1 查看某一客户端的状态信息

在登录列表中单击某客户端，在资源栏中选择‘状态’属性页。



查看某一客户端的硬件信息

在登录列表中单击某客户端，在资源栏中选择‘硬件’属性页。



查看某一客户端的软件信息

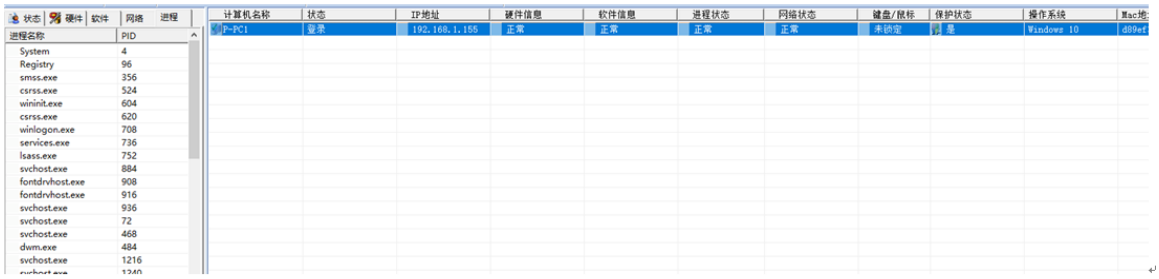
在登录列表中单击某客户端，在资源栏中选择‘软件’属性页。

查看某一客户端的网络信息

在登录列表中单击某客户端，在资源栏中选择‘网络’属性页。

查看某一客户端的进程信息

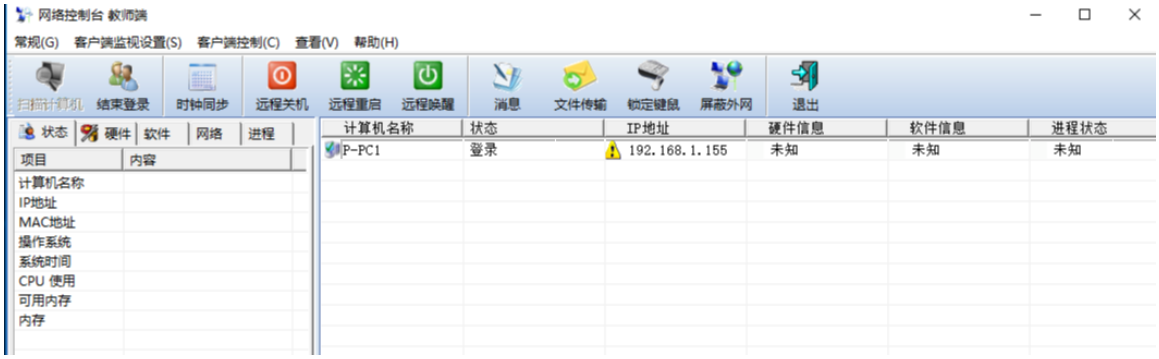
在登录列表中单击某客户端，在资源栏中选择‘进程’属性页。

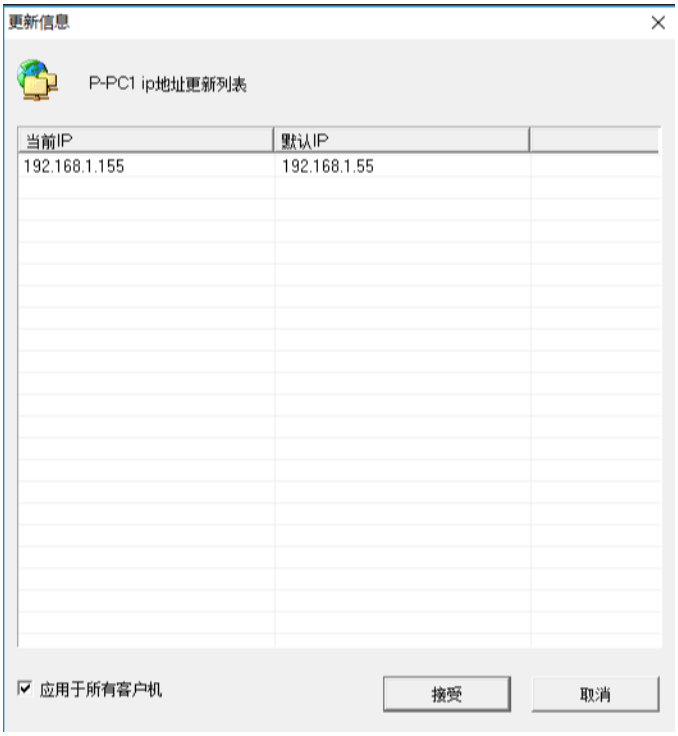


5.2 查看学生端异常状态

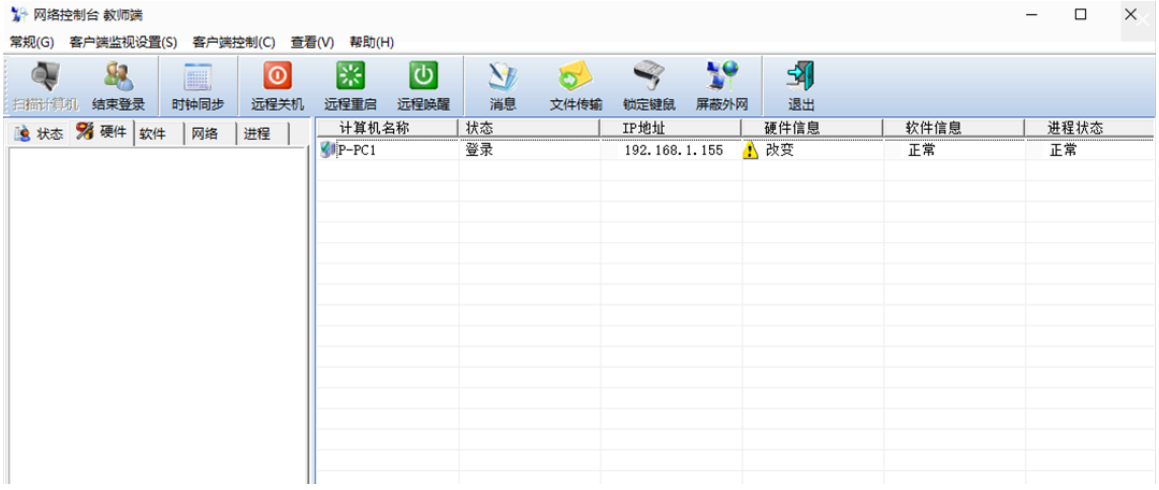
5.2.1 学生端 IP 地址改变

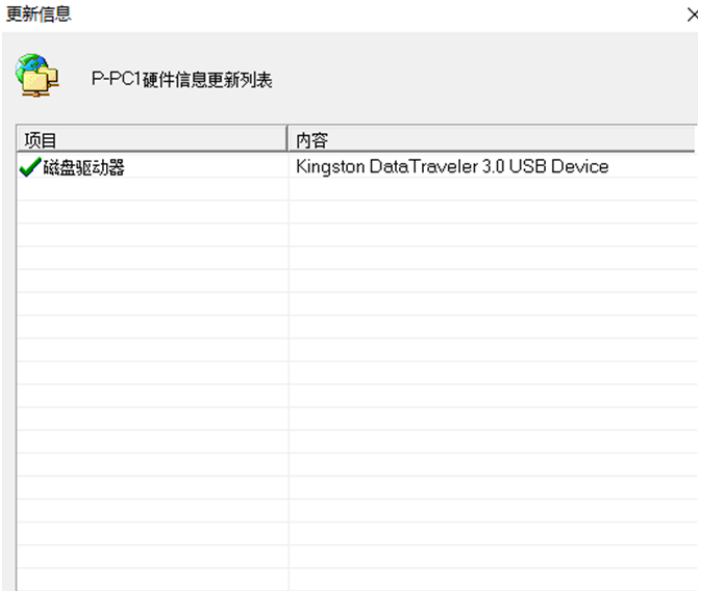
若某客户端当前使用的 IP 地址发生了变化，在客户端登录列表栏中该客户端 IP 地址属性字段会出现黄色惊叹号报警。双击该属性，在弹出的‘更新信息’对话框中能查看给客户端的 IP 变化详细。可以在‘更新信息’界面选择取消对该客户端的 IP 地址变更的报警。





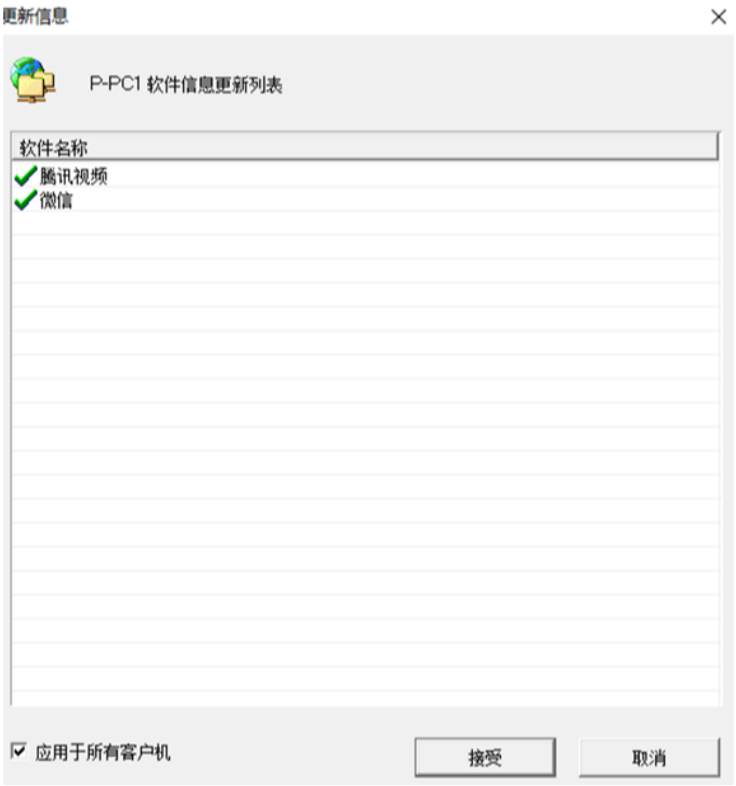
5.2.2 学生端硬件信息改变





学生端硬件信息与上次保存信息不一致（学生端的硬件发生变化），那么客户端登录列表该客户端的硬件属性字段将会出现黄色的惊叹号报警。双击该字段，在弹出的‘更新信息’对话框中能看到新增的或者移除的硬件信息。可以单击更新信息对话框中【接受】，取消该报警。

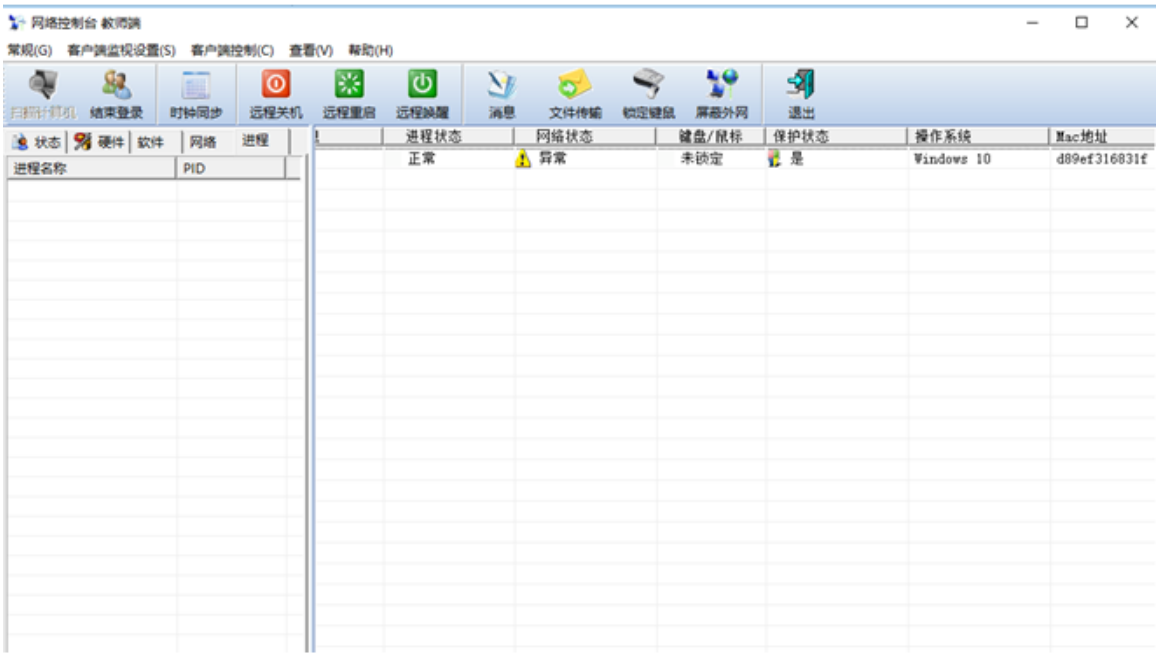
学生端软件信息改变：



学生端软件信息与上次保存信息不一致（学生端的软件发生变化），那么客户端登录列表该客户端的软件属性字段将会出现黄色的惊叹号报警。双击该字段，在弹出的‘更新信息’对话框中能看到新增的或者移除的软件信息。可以单击更新信息对话框中【接受】，取消该报警。

学生端网络状态异常：

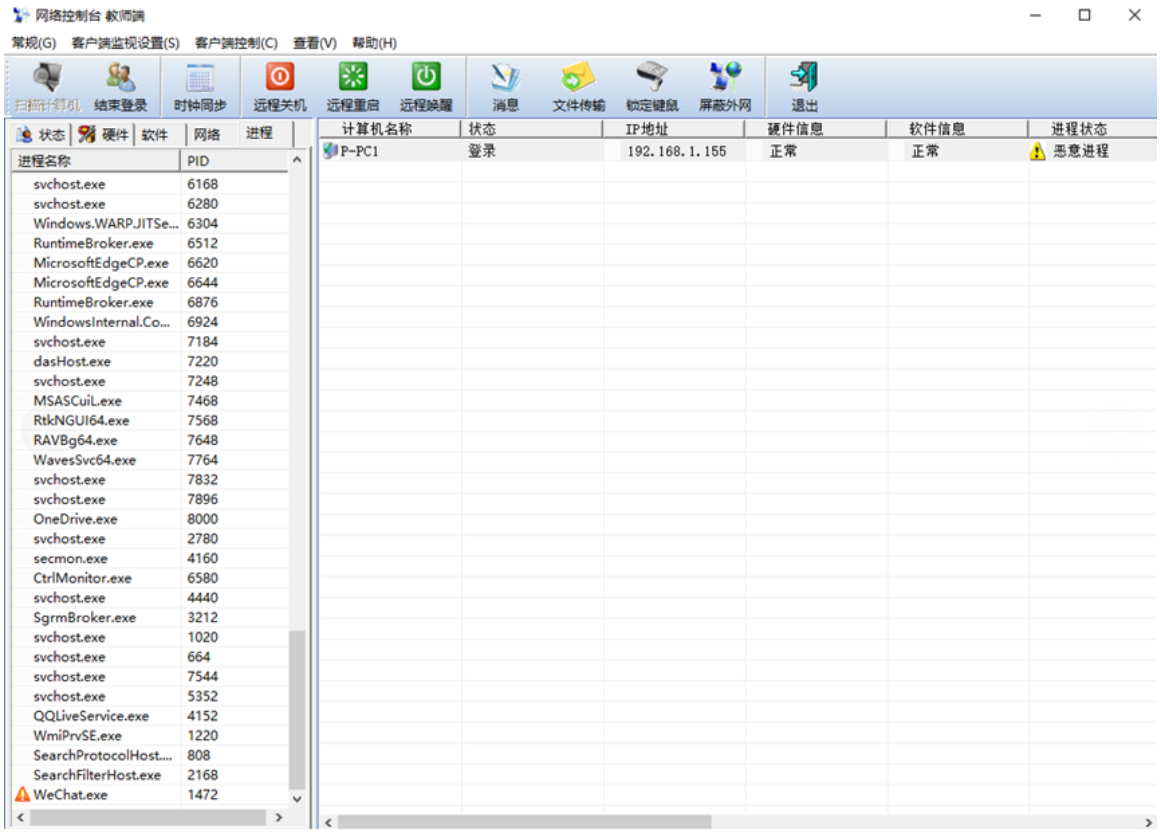
学生端网络状态属性有四种：屏蔽外网、禁用网络、异常和正常，前面两种状态是网络控制台系统已经对该客户端进行了网络屏蔽（参考屏蔽外网、禁用网络），异常状态表式该客户端的网络行为发生异常（网络属性字段出现黄色惊叹号报警），双击该学生端网络状态属性，在弹出网络信息对话框可以看到该学生端实时的网络状态统计信息。



学生端进程状态异常：

学生端计算机中出现已经预先设置的恶意进程。在登录列表中学生端的进程属性字段会出现黄色惊叹号报警。可在登录列表中选中该客户端后，在资源栏中选择进程属性页查看该学生端的进程资源列表。在进程列表中，可以选中该进程后，右键点击该进程，在弹出的右键菜单中执行进程删除操作（结束客户端该进

程）。



学生端保护状态：

当学生端戴尔硬盘控制台处于正常中工作状态时，已登录的学生端保护状态属性字段显示为“是”，否则显示“否”。

5.3 学生端信息更新

当学生端信息与历史信息不一致时，网络控制台会对该客户端的相应属性字段进行报警提示，用户可以取消该报警信息。双击该属性字段，在弹出的‘更新信息’对话框中显示了相应的更新信息，点击【接受】以接受学生端的信息变化，网络控制台将更新该客户端的历史信息，以后不再对该属性信息中的相应项作出报警。勾选【应用于所有计算机】，则存在相同信息变化（如，软件更新）的学生端的历史信息将同时被更新，网络控制台以后将不再对所有学生端的该属性的信息中的相应项进行报警。

5.4 查看日志

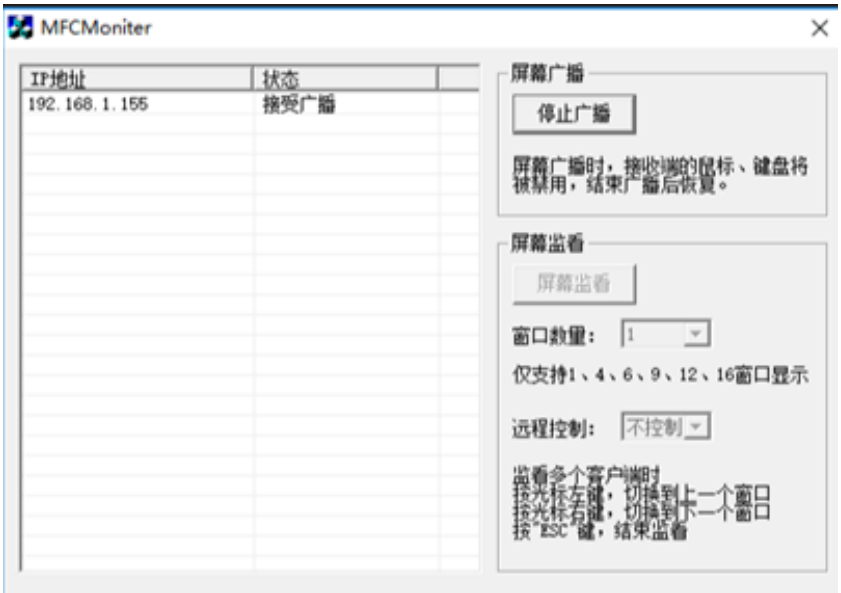
在监控日志中用户可以查看学生端在监控时间内发生的事件。日志是保存在内存中的，重新启动网络控制台系统，监控日志就会被清空。在监控日志中可以看到的事件有：掉线、创建进度、恢复进度、删除进度、发起 Arp 攻击等。

单击菜单栏【常规】中的【日志】，弹出日志信息对话框。

第 6 章 客户端控制

6.1 屏幕监控

通过网络控制台可以实时（循环）监视一个或多个学生的电脑屏幕画面。



选择菜单栏中【客户端控制】，【屏幕监控】，点击【屏幕监看】选择【窗口数量】，屏幕监看到客户端机器的桌面。

6.2 屏幕广播

通过网络控制台【屏幕广播】，将“教师机”的屏幕图象内容同步广播到网络上的“学生机”上。

6.3 时间同步

将学生端的系统时钟设置为教师端的系统时钟。

可以在资源栏中的‘基础’属性页中查看学生端的系统时间。

6.4 远程重启、关机、唤醒操作

用户可以通过网络控制台系统对某一台或者所有学生端执行重启、关机、唤醒命令。

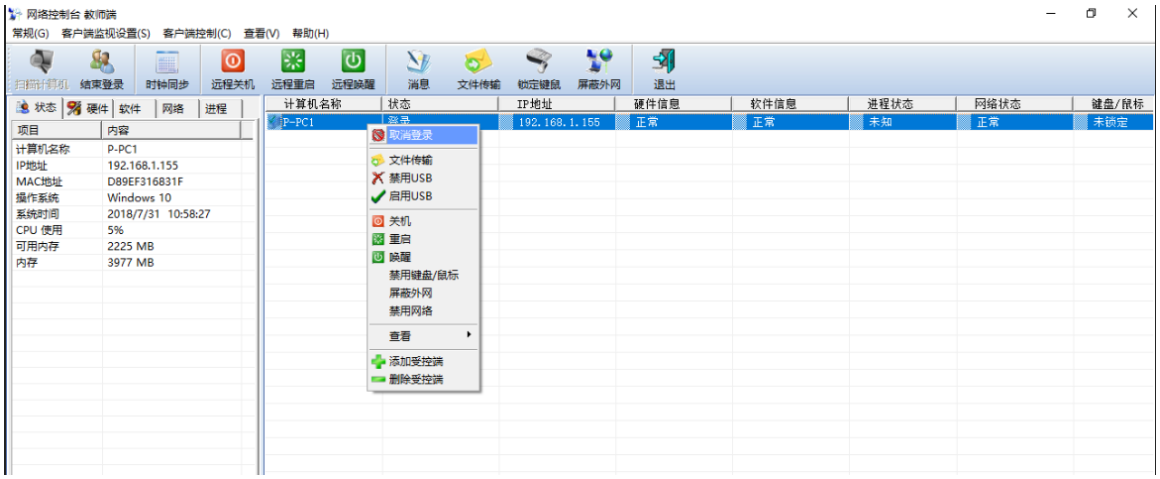
注意：**唤醒**操作需要学生端主板支持，并已经打开了相关选项。

工具条操作：

工具条的按钮对登录列表中的所有学生端进行操作。

右键菜单操作：

右键菜单对选择的部分学生端进行操作，在登录列表中选中部分学生端后在选择范围内点击鼠标右键弹出右键菜单。

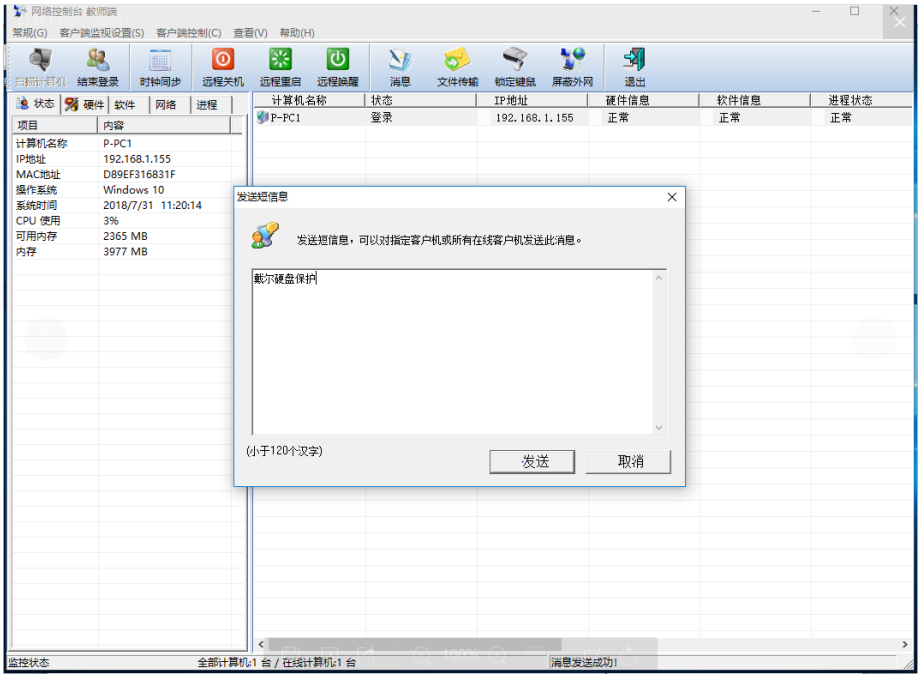


6.5 发送消息

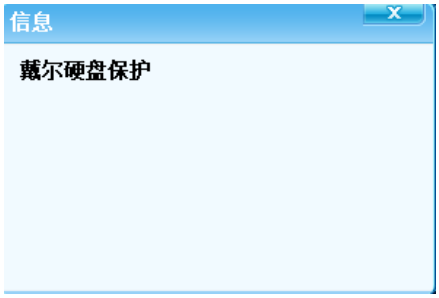
对所有在线的学生端发送广播消息，消息将以气泡的形式出现在学生端屏幕右下角。

单击工具栏中的【发送消息】，在弹出的发送短消息对话框中输入消息，单击【发送】完成操作。

消息发送：

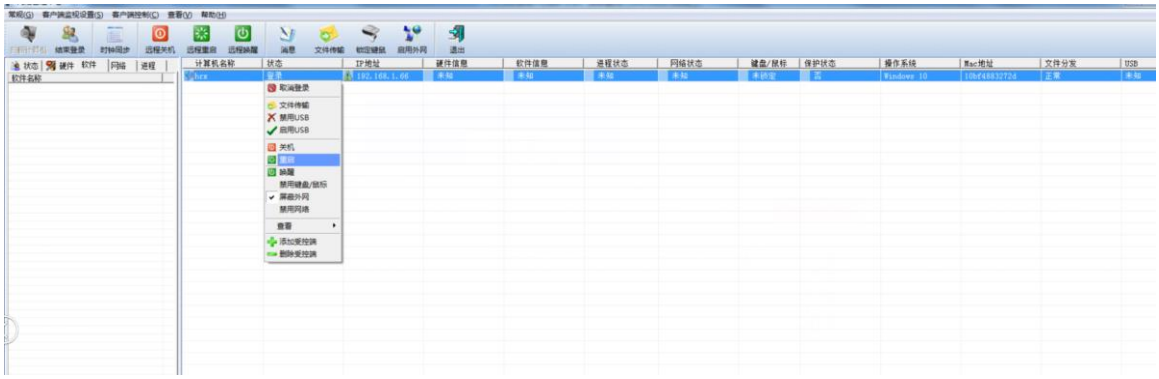


客户端消息提示：

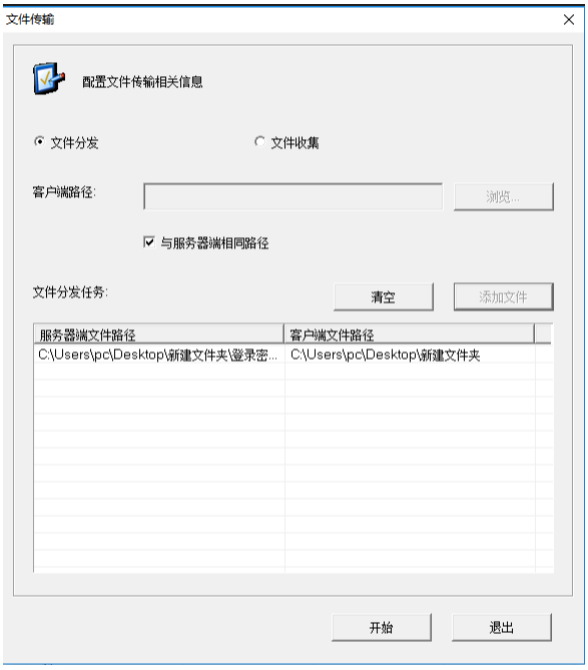


6.6 文件传输

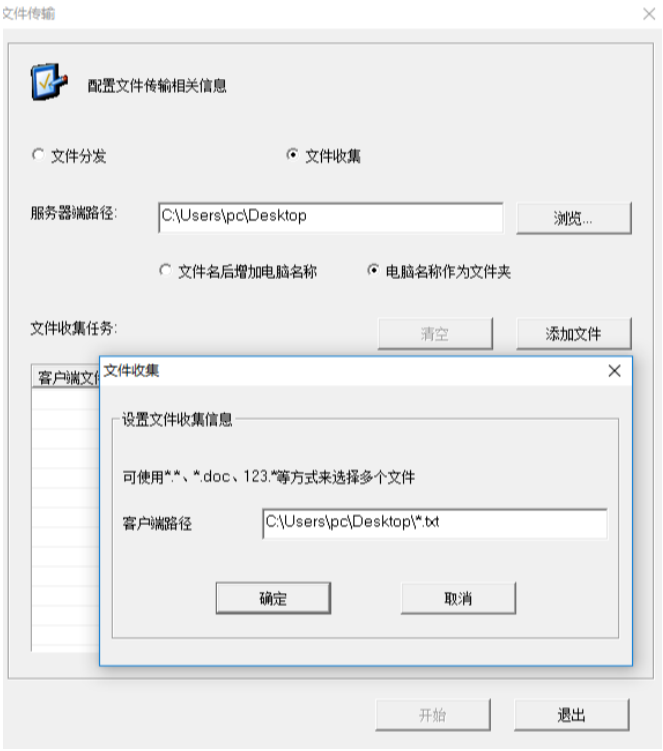
将主控端的文件发送到学生端的磁盘上，也可以将学生端的文件收集到主控端的磁盘上。



点击按钮后在弹出的对话框中选择是文件分发还是文件收集，设置好路径后，点击添加文件。选择需要操作的文件后进行分发或者收集，如下图



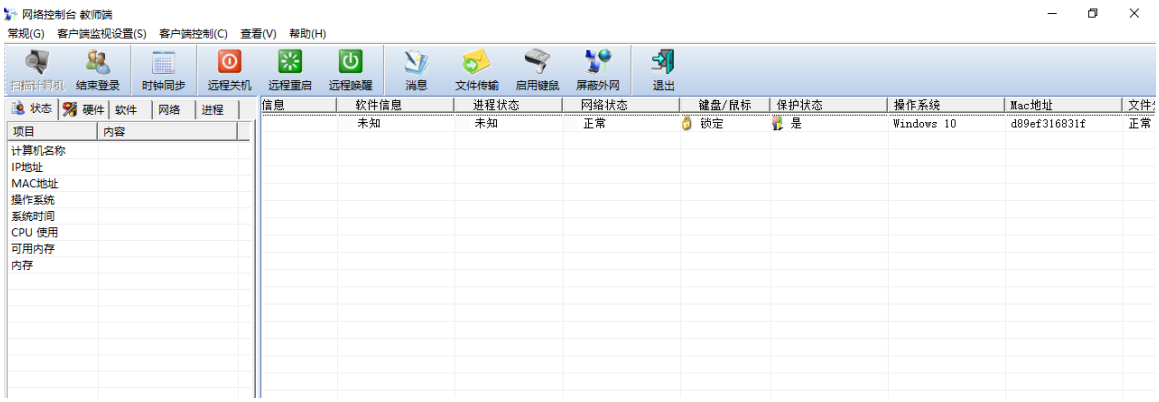
文件分发



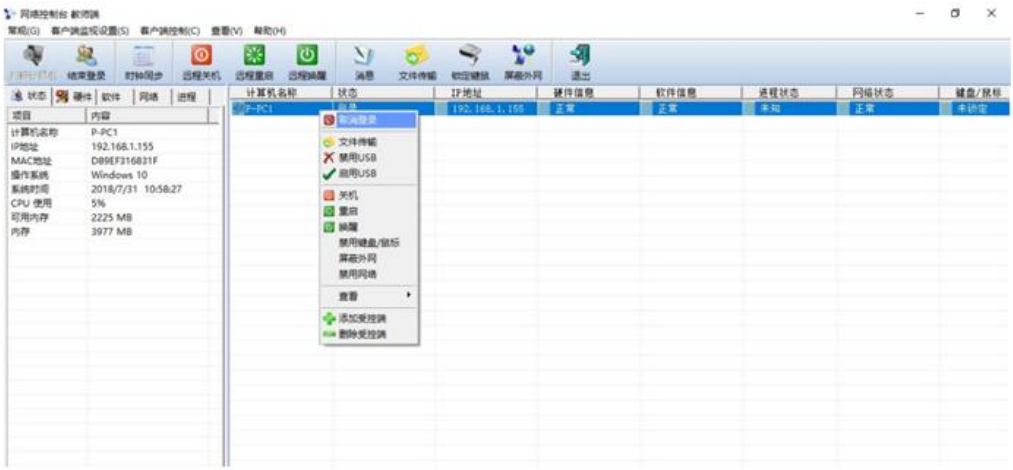
文件收集

6.7 锁定、启用键盘鼠标

可以远程锁定学生端的鼠标和键盘，使之不可用。学生端重启计算机后键盘鼠标锁定状态失效。在锁定键盘鼠标命令发送成功后，被锁定学生端的鼠标/键盘属性字段将显示黄色锁和文字“锁定”，并且右键菜单中的【禁用键盘/鼠标】为勾选状态，解除锁定后将显示为“未锁定”。



处于锁定状态时的学生端右键菜单状态如下：



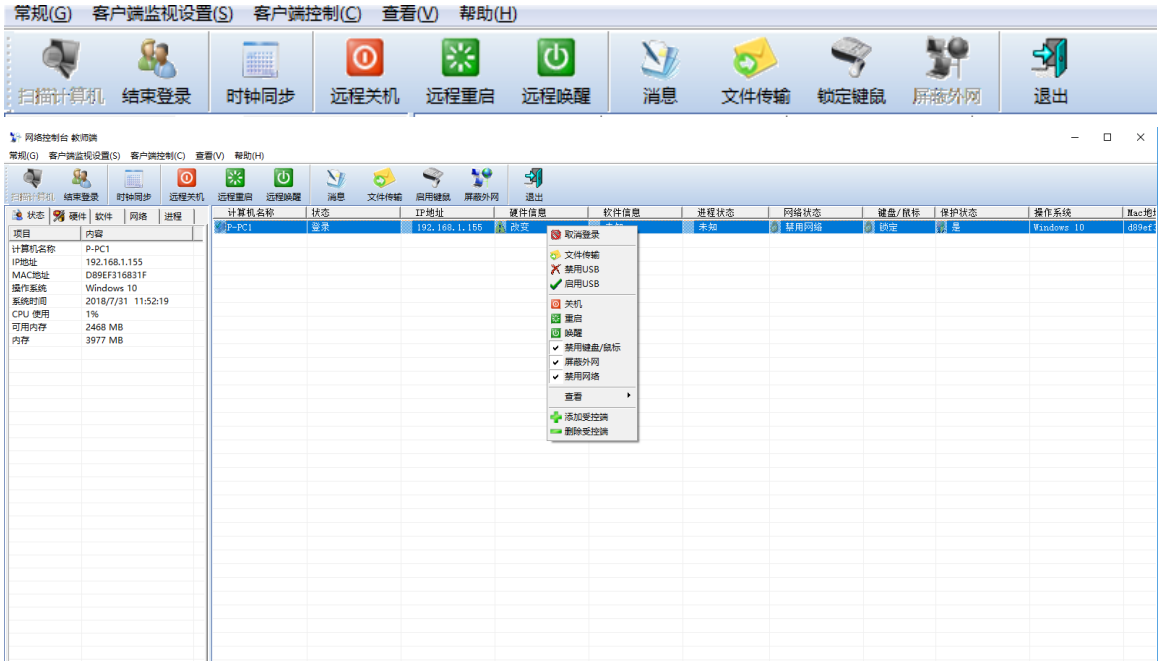
6.8 屏蔽外网、禁用网络与启用

用户可以屏蔽学生端的外网，使之只能访问与它属于同一网段的计算机。禁用网络则彻底屏蔽学生端与外部计算机的联系。被屏蔽外网的学生端，在网络状态属性字段显示为“屏蔽外网”，并且在右键菜单中的【屏蔽外网】为勾选状态，被禁用网络的学生端，在网络状态属性字段显示为“禁用网络”，并且在右键菜单中的【禁用网络】为勾选状态。用户可以对任意一台学生端或者全部执行屏蔽外网和禁用网络的操作。

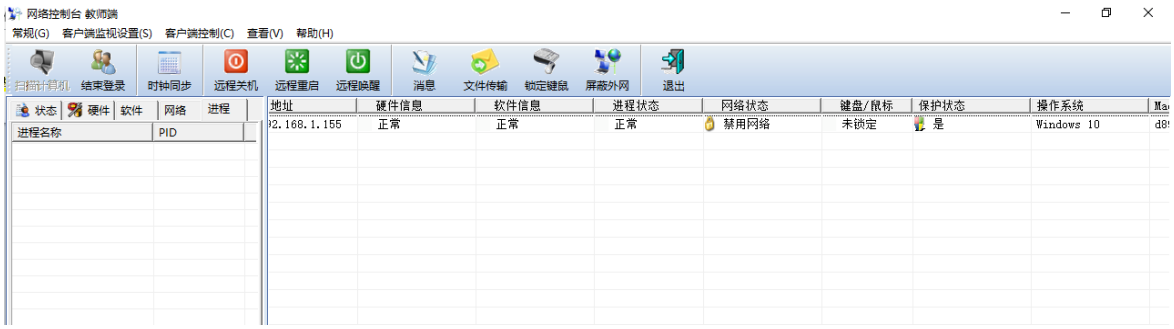
通过点击工具条按钮屏蔽所有学生端外网：

通过右键菜单屏蔽部分选中的学生端外网与禁用网络：

学生端外网被屏蔽：

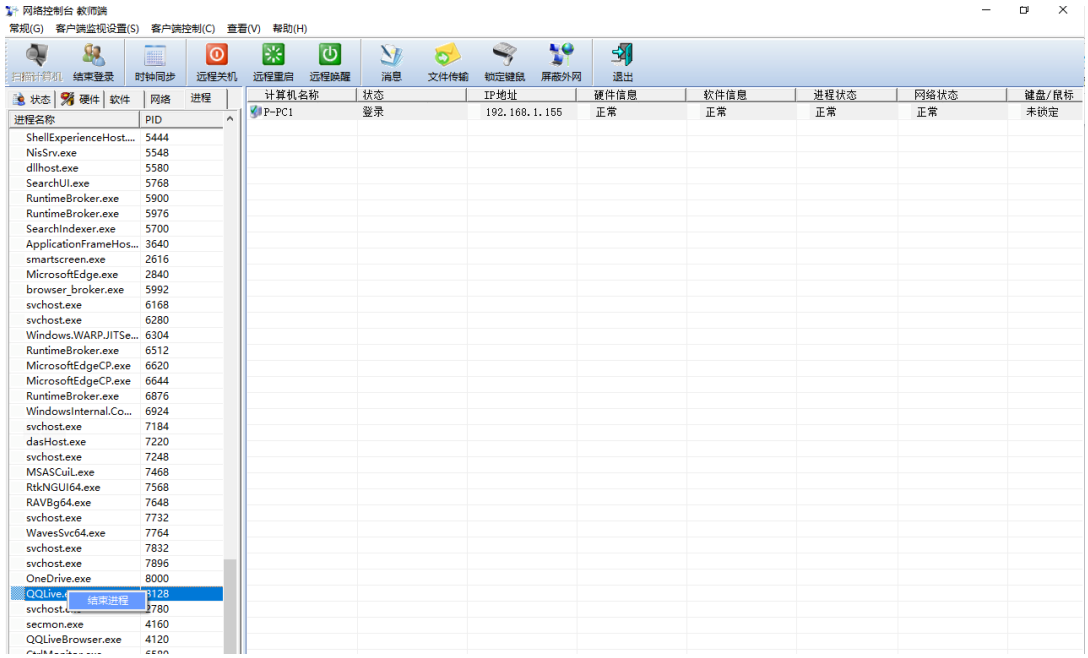


学生端网络被禁用：



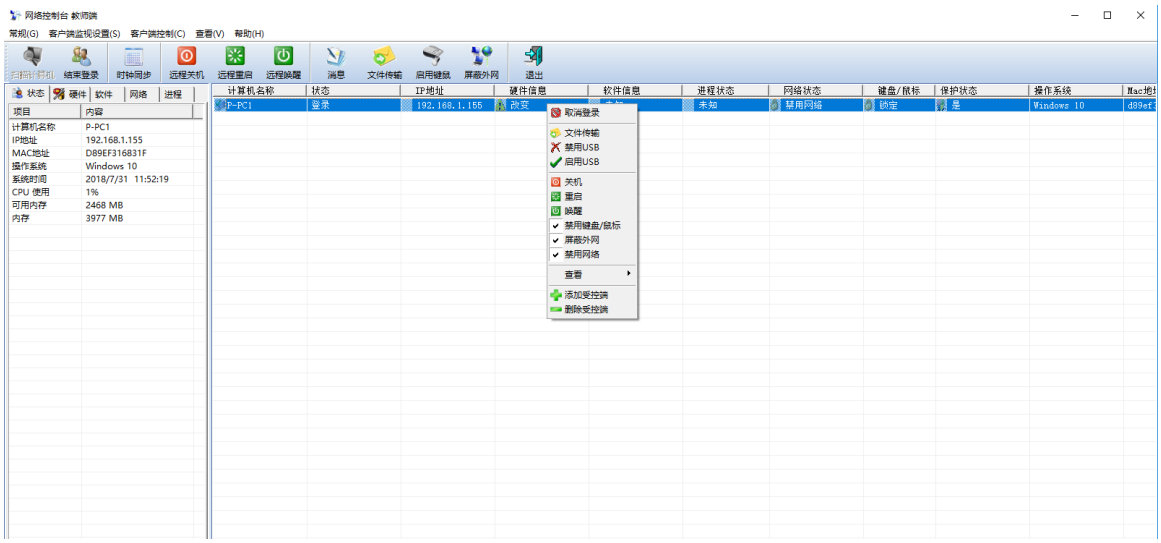
6.9 删除学生端进程

删除（结束）某一客户端的指定进程（参考查看学生端异常状态）。



6.10 取消登录

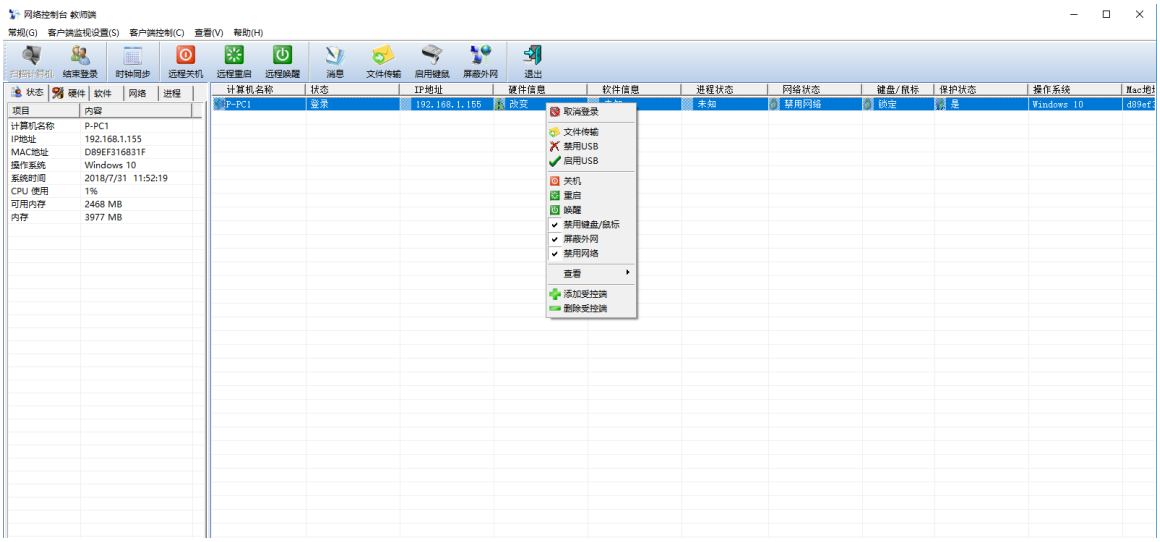
取消对某一学生端的网络监控。



选择一台学生端，单击鼠标右键选择菜单中的【取消登录】。

6.11 禁用、启用 USB 端口

禁止和启用学生端的 USB 存储设备的使用。



选择一台学生端，单击鼠标右键选择菜单中的【启用 USB】或者【禁用 USB】。