

关于本手册

本手册为南京瑞泰尼尔信息技术有限公司知识产权的一部分。我们非常用心地编写、整理这本手册，希望能让用户尽快了解我们的软件。但是，由于时间和水平的有限，手册中难免会出现一些纰漏，我们期待广大用户的及时指正，同时我们也会继续改进和更新我们的技术和服务，感谢您对我们的支持。

本手册是瑞泰尼尔安全防御系统软件 V1.0 的通用手册，因此您使用的软件可能存在存在部分功能和手册中的描述不符的情况，敬请谅解。

为了响应国家低碳环保的号召，本手册将主要以电子版的方式发布，如有特殊需要，请向本公司申请获得帮助手册的纸质版本。

软件说明

瑞泰尼尔安全防御系统软件 V1.0(英文名称 :Returnil Virtual System 2010 ,以下简称 RVS) 是瑞泰尼尔公司采用最新虚拟技术实现的新一代桌面安全系统。和传统的杀毒软件完全不同，瑞泰尼尔防毒系统软件可以瞬间“克隆”用户当前的操作系统，“制造”出实际存在于用户内存中的虚拟操作系统，并利用虚拟的操作系统来替代真实的操作系统，从而达到保护真实操作系统的目的。

处于 RVS 的虚拟保护之下，任何试图对于用户操作系统发动的攻击和感染，实际上都将发生在内存中的虚拟操作系统中，用户重启系统后，内存中的虚拟系统自动消失，所有的攻击和感染也随之消失，被保护的真正系统将再次回到保护前的状态，而保护时及时遭到攻击和感染也不会对用户的真实系统造成任何的伤害。

RVS 为用户系统全面保护的同时，还为用户提供更加高级和高效的功能，方便用户的使用和管理。

- (1) 在保护状态下，用户可以有选择的保存虚拟系统中存在的文件/文件夹到真实的操作系统中。
- (2) 在保护状态下，用户可以将选择将所有在虚拟系统中的修改全部保存在真实的操作系统中，以应对系统升级等复杂的维护工作。

RVS 为用户提供全新的“主动防御”附加模块。任何未经授权的驱动程序，都将被“主动防御”所拦截或者警告。在虚拟系统保护基础上再为用户增加一层全面的保护，以应对未知的外来攻击和威胁，如 U 盘病毒和网页木马病毒等。还可以使管理者方便的管理计算机所安装使用的软件，阻止使用者使用未经许可的程序和驱动，减少因此带来的安全威胁。

面对以几何倍数快速增长的病毒和木马威胁，面对用户更强更快的安全需求，传统的杀毒技术已经开始变得力不从心。其升级不够及时，病毒库不够广泛，占用系统资源极大的缺点正为广大用户所诟病。而新一代虚拟安全技术构架下的 RVS 将为用户带来全新的安全体验：无需频繁的升级病毒库，无需实时拦截和监控，无需消耗巨大的系统资源，无需具备深厚的安全知识和技能，只要用户按下保护按钮，系统瞬间将进入保护状态，只要用户按下重启按钮，所有的威胁即刻消失的无影无踪。

RVS 一次安装，永久有效。使用 RVS 将大大减少用户的运营和维护成本，减少因病毒和木马对于本地系统攻击所造成的数据损失和经济损失，为用户的网络冲浪保驾护航，为用户的计算

机安全提供最强大的支持和保障。

产品特点

1. 软件为全中文操作，使用极其简单和方便。
2. 系统保护功能无需实时过滤和拦截用户的文件和注册表操作，不占用系统资源。
3. 系统保护功能使用户长期使用系统后无需磁盘整理，永远都像新装的一样。
4. 保护功能使用户能够应付任何未来的，未知的攻击和威胁。
5. 保护功能为用户测试和使用未知软件提供了方便的保护。
6. 保护功能无需升级病毒库，为用户节省升级系统的时间成本和网络成本。
7. 保护功能无需经常扫描系统，为用户节省了维护系统的时间和支出。
8. 保护功能自动清理用户的上网时留下的浏览记录和密码，保护用户的隐私。
9. 防火墙功能可以方便管理者阻止用户使用未被授权的驱动运行。
10. 占用系统资源极少，对用户的使用干预度极低，极大的提高了用户的安全体验。
11. 支持 RAID 等磁盘阵列体系，同时兼容 IDE,SATA,CF 卡等硬盘设备。
12. 支持 FAT32 和 NTFS 文件系统，和操作系统无缝集成。
13. 虚拟分区功能使得单一分区用户可以方便简单的存储和修改数据。
14. 支持 NT 的非管理员权限运行。
15. 支持 XP , Vista , Win7, 2003, 2008 等操作系统的 32 位和 63 位版本
16. 支持服务器集中管理，可以同时管理上百个软件客户端，并进行统一的设置
17. 内置小型的防毒模块，对于常见的 Autorun 病毒，机器狗病毒都有很好的免疫

产品试用

本软件为用户提供长达 30 天的试用体验，试用版在试用期内在功能上和正式版完全相同，试用期之后除虚拟系统保护之外的其它功能将继续有效，用户可以随时使用有效的注册码激活本软件，成为正式版的客户。

支持环境

操作系统：

Windows XP, Windows 2003, Windows Vista, Windows 7, Windows 2008

CPU：

赛扬 566 以上

内存：

64MB 以上

硬盘：

系统盘大于 1024MB 的剩余空间

安装准备

如果您购买了本软件，那么请从我们的网站或者经销商处获得本软件的最新安装版本，然后将安装程序放置于即将安装的系统中，做好安装准备。

安装本产品之前，强烈建议用户临时关闭防火墙和杀毒软件。在 Windows XP, 2003, Vista, Win7, Windows 2008 下安装时，请注意您是否拥有管理员权限，而且是否以管理员帐户运行了我们的安装软件程序。

安装本产品之前，请检查以下情况：

(1) 本机是否已经安装了 RVS，如果安装了比当前版本更低的版本，请退出安装程序，卸载之前较低版本。

(2) 如果本机已经安装了 RVS，并且正处于虚拟保护的状态，请退出安装程序，进入瑞泰尼尔安全防御系统软件的控制界面，将保护关闭并退出运行中的 RVS，然后再进行安装。

(3) 如果本机已经安装了 RVS，并且 RVS 正在运行中，请退出运行中的 RVS，然后再进行安装。

开始安装

1. 双击如下图标即可。如果您的系统是 Vista 或者 Win7，同时系统的 UAC 功能已经打开，那么建议您在如下图标上右击鼠标，然后选择以管理员的身份运行本软件，以确保本程序的安装程序在管理员权限下运行。

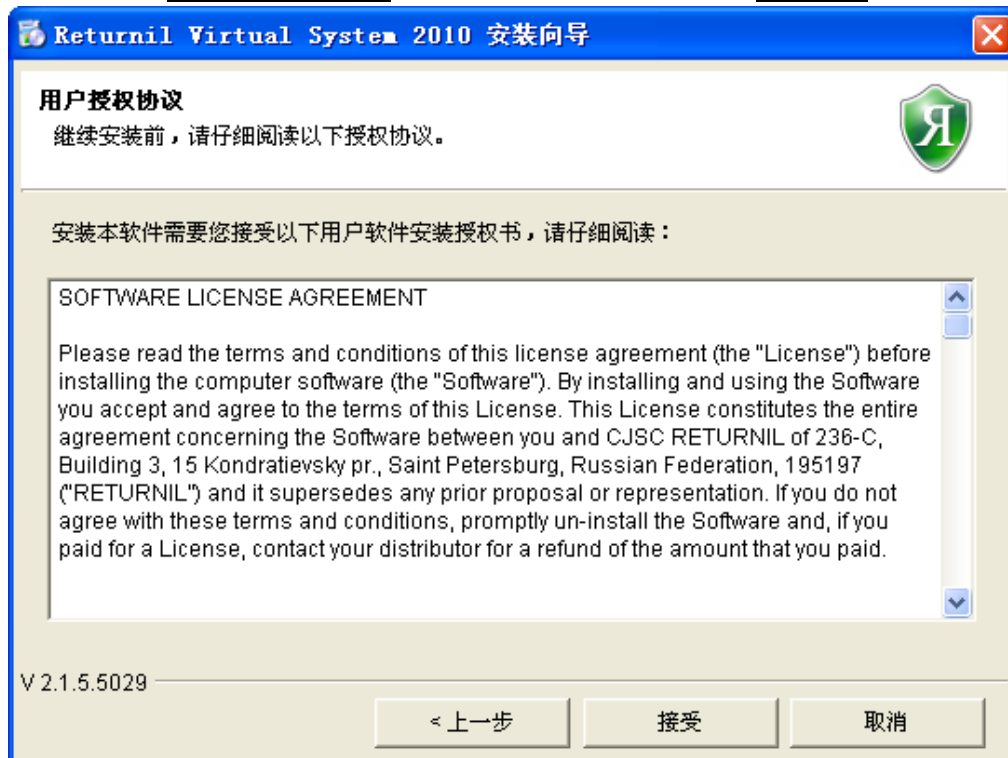


2. 进入“安装向导”，选择下一步。



在这里您可以选择不同的安装语言，比如英语，简体中文等，也可以点击使用帮助按钮来打开本软件的试用帮助，进而获得更多的安装帮助信息。如果您不想继续安装本软件，那么请选择取消退出本软件向导。

3. 仔细阅读以下“用户许可协议”来了解您的权利和义务。点击“接受”来继续安装。



4. 本安装程序同时包含了客户端和服务器的安装，您可以选择不同的安装选项，然后点击下一步。

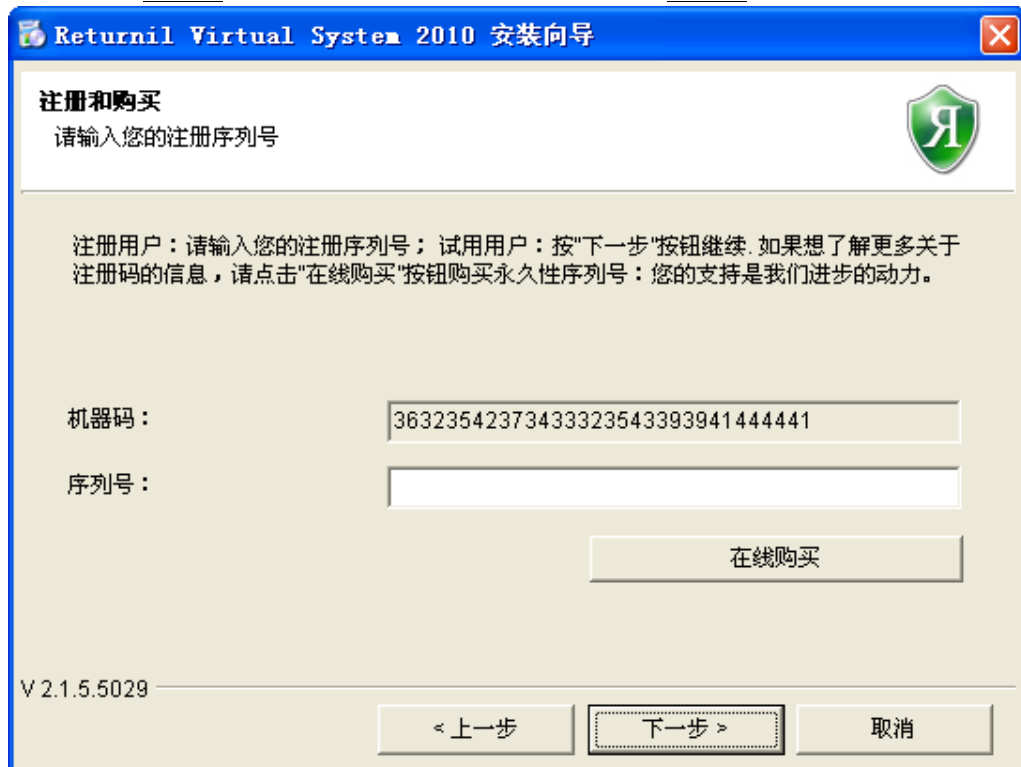


5. 如果您选择的是安装客户端，那么将出现如下界面：选择软件的安装路径。点击下一步。



您可以在这里设置您希望本软件被安装的目录和位置。

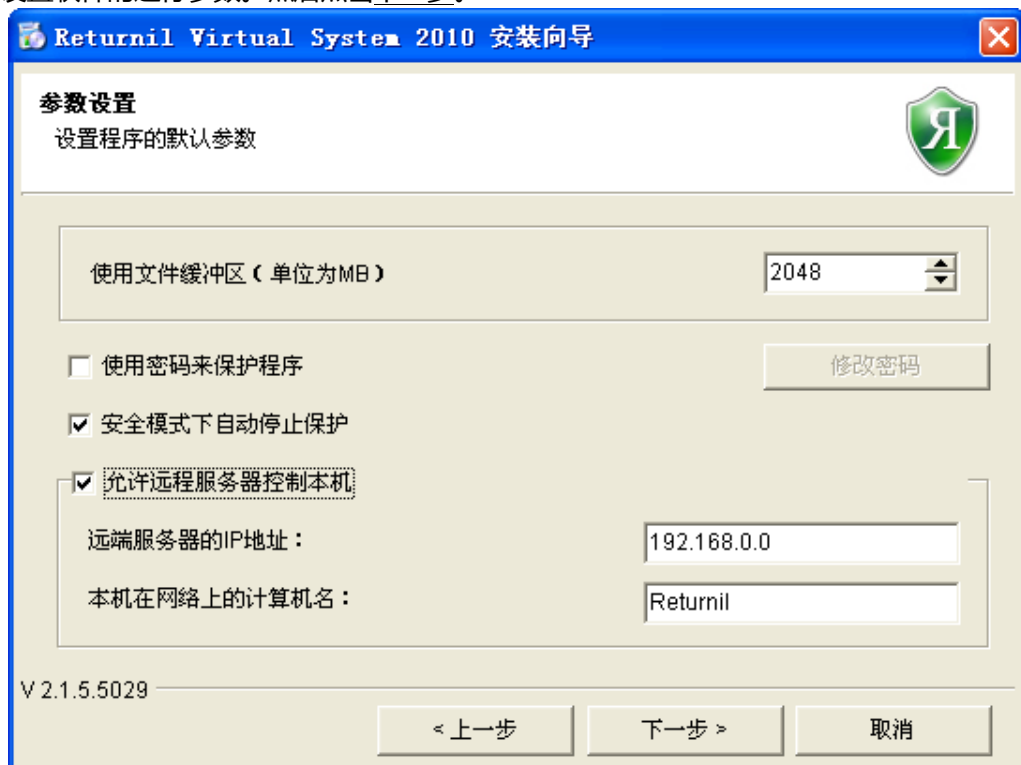
6. 如果您有注册码，那么请在序列号输入框中填写您的正版注册码。如果您想试用本软件，那么请选择下一步，您将获得 30 天的软件试用期。点击下一步。



The screenshot shows the 'Returnil Virtual System 2010' installation wizard window. The title bar reads 'Returnil Virtual System 2010 安装向导'. The main heading is '注册和购买' (Registration and Purchase) with the instruction '请输入您的注册序列号' (Please enter your registration serial number). A green shield logo with a white 'R' is in the top right. The text below says: '注册用户：请输入您的注册序列号；试用用户：按"下一步"按钮继续。如果想了解更多关于注册码的信息，请点击"在线购买"按钮购买永久性序列号；您的支持是我们进步的动力。' (Registered user: please enter your registration serial number; Trial user: click 'Next Step' to continue. If you want to know more about the registration code, click 'Online Purchase' to buy a permanent serial number; your support is our motivation for progress.) There are two input fields: '机器码：' (Machine Code) with the value '36323542373433323543393941444441' and '序列号：' (Serial Number) which is empty. A '在线购买' (Online Purchase) button is to the right of the serial number field. At the bottom, there are three buttons: '< 上一步' (Previous Step), '下一步 >' (Next Step), and '取消' (Cancel). The version number 'V 2.1.5.5029' is in the bottom left.

如果您已经购买了本软件，还没有得到注册码，那么请将机器码发送给我们或者相关的代理商邮箱，然后我们将会把相应的注册码发送给您。**如果您从我们代理处获得的是 USB 加密狗的作为注册工具，那么请在点击下一步前插入相关的 USB 加密狗。**

7. 设置软件的运行参数。然后点击下一步。



The screenshot shows the 'Returnil Virtual System 2010' installation wizard window. The title bar reads 'Returnil Virtual System 2010 安装向导'. The main heading is '参数设置' (Parameter Settings) with the instruction '设置程序的默认参数' (Set the default parameters of the program). A green shield logo with a white 'R' is in the top right. The settings include: '使用文件缓冲区（单位为MB）' (Use file buffer (in MB)) set to '2048'; an unchecked checkbox '使用密码来保护程序' (Use password to protect program) with a '修改密码' (Change Password) button; a checked checkbox '安全模式下自动停止保护' (Automatically stop protection in safe mode); a checked checkbox '允许远程服务器控制本机' (Allow remote server control of this computer); '远端服务器的IP地址：' (Remote server IP address) set to '192.168.0.0'; and '本机在网络上的计算机名：' (Computer name on the network) set to 'Returnil'. At the bottom, there are three buttons: '< 上一步' (Previous Step), '下一步 >' (Next Step), and '取消' (Cancel). The version number 'V 2.1.5.5029' is in the bottom left.

文件缓冲区是本软件的影子保护功能所需的缓冲区的大小，建议您设置至少为 2G 的文件缓冲区，这样才能让软件的虚拟保护获得最佳的发挥和应用。

试用密码来保护程序：您可以为软件设置一个密码，将来在打开主界面时，软件将弹出密码输入界面。如果用户没有输入正确的密码，将无法打开主界面进行设置和修改。

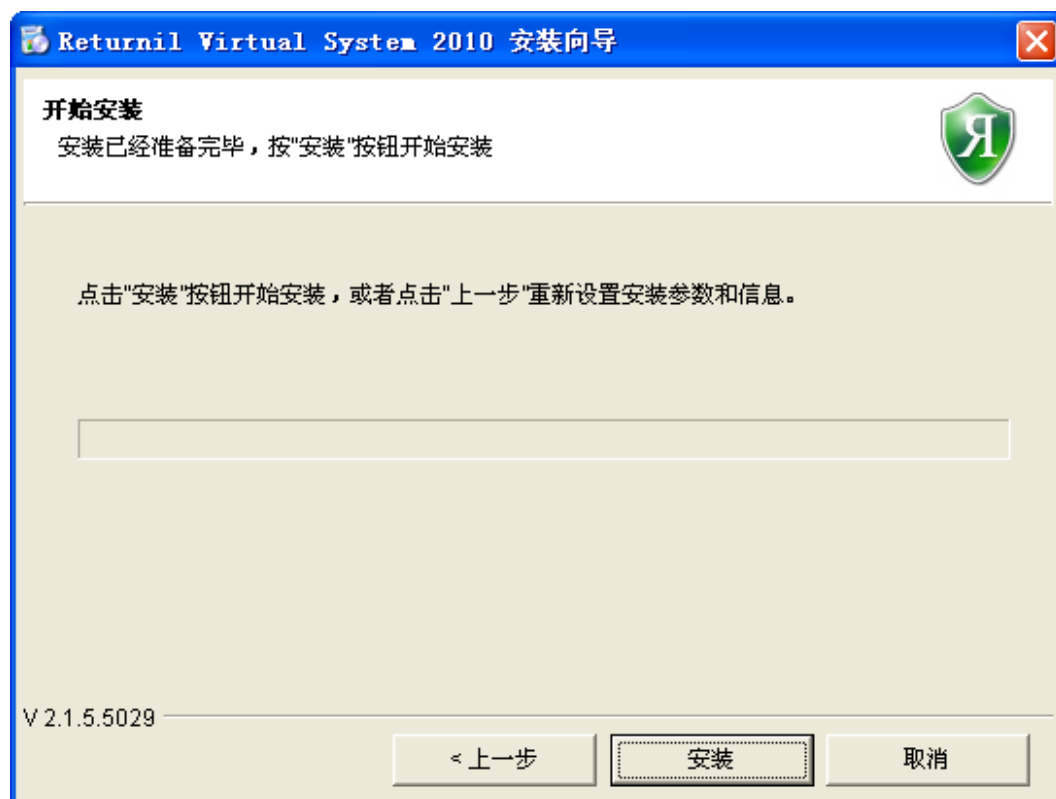
安全模式下自动停止保护：如果您选中了本项，那么将来在安全模式下，软件的虚拟保护功能将自动停止，这将有利于您在安全模式下进行软件的修复和卸载。

允许远程服务器控制本机：如果您选择了本项，那么安装后的本软件将定时自动尝试连接在“**远程服务器的 IP 地址**”中设置的服务器地址。

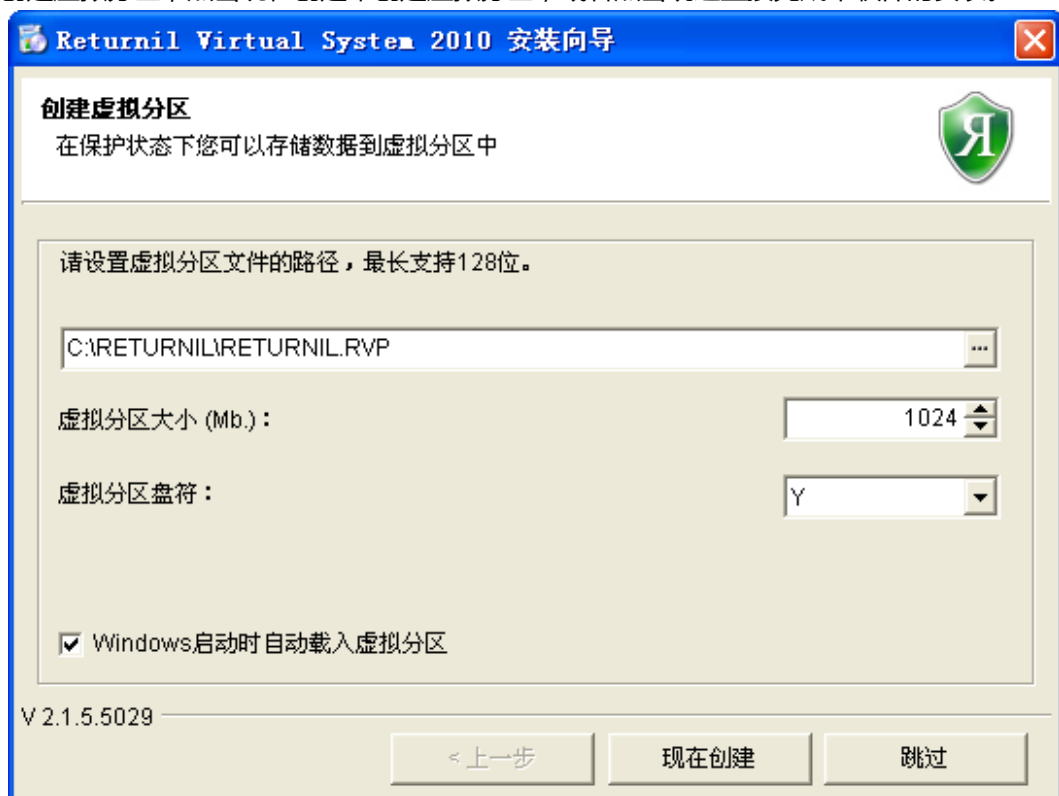
远程服务器的 IP 地址：您可以在这里输入远程服务器安装所在的机器的 IP 地址（仅支持数字格式的 IP 地址）。

本机在网络上的计算机名：此处的计算机名将在服务器中选择，在这里设置计算机名将有助于您在服务器上区分和鉴别不同的客户机。

8. 开始安装软件。点击下一步将把软件安装到您之前指定的位置。



9. 创建虚拟分区，点击现在创建来创建虚拟分区，或者点击跳过直接完成本软件的安装。



10. 完成安装。点击完成来重启计算机。



软件的虚拟保护是在系统内核层工作的驱动来实现的，因此安装本软件后，您需要重新启动您的计算机来使本软件的相关驱动得以被系统加载。

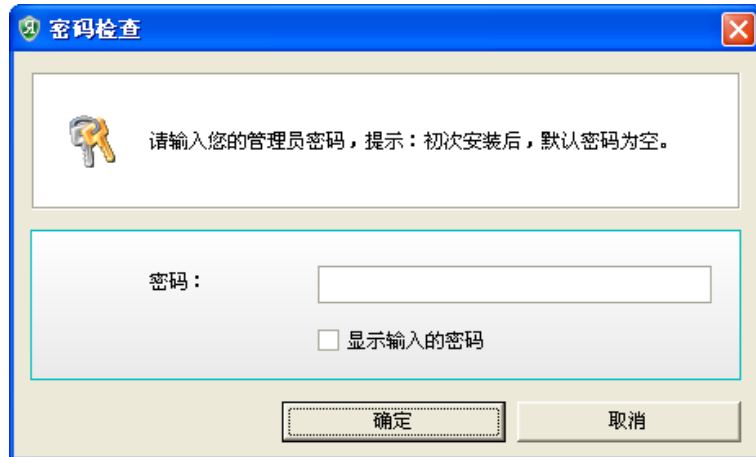
产品使用（客户端）

● 打开软件

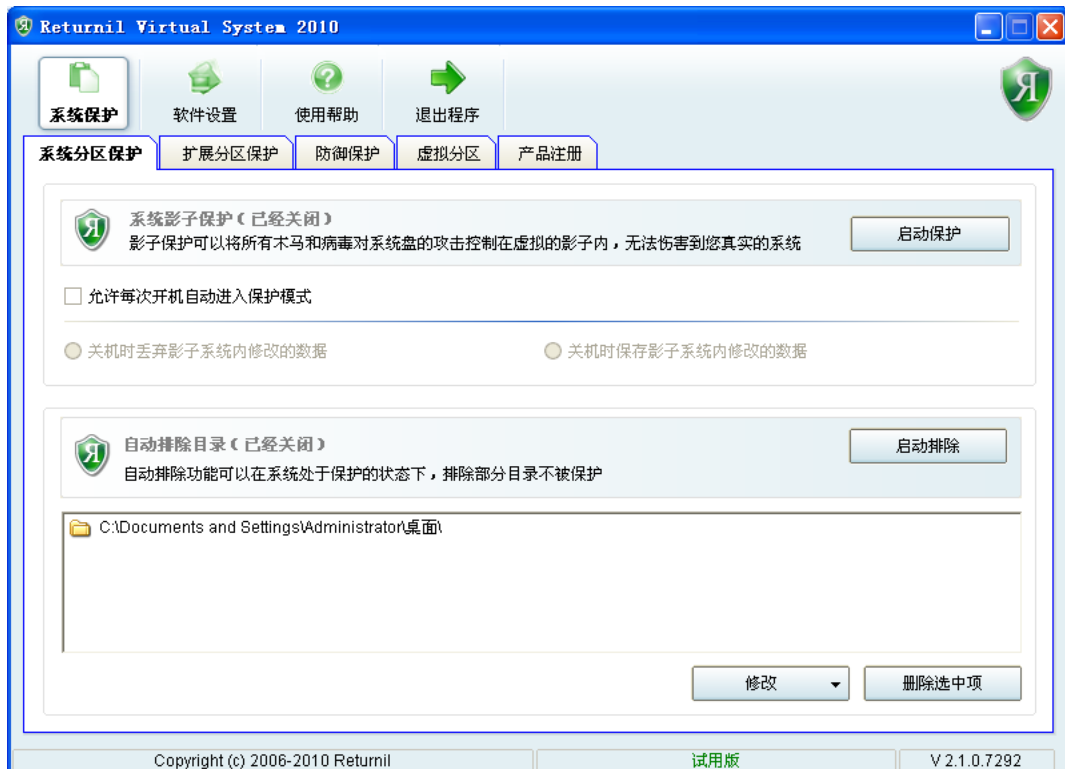
当您正确的安装了本软件的客户端之后，软件将在每次开机后自动运行，并且在系统的托盘区域显示一个图标。如下图所示：



双击本软件在系统托盘区域的图标后，您将打开本软件的主界面。如果您为本软件设置了密码，那么在打开主界面前，将显示密码输入对话框，需要来验证您是否为本软件的管理员。



● 软件主界面



● 系统保护

系统保护是本软件的核心功能，在当前版本中，系统保护包含了如下功能模块：

1. 系统分区保护
2. 扩展分区保护
3. 防御保护
4. 虚拟分区
5. 产品注册

什么是影子保护呢？

当系统保护被打开后，系统将被临时产生的“影子”系统所代替，所有的运行将在此“影子系统”上发生，因此任何病毒和木马都无法感染您真实的系统。

1. 系统分区保护

系统分区在这里是指操作系统所在的分区，一般为 C 分区。如果您可以开启对系统分区的保护，那么请点击“**启动保护**”来快速启动对系统分区的虚拟保护。启动保护不需要重新启动计算机即可立即开始保护当前的系统。

如果您已经开启了系统保护，那么可以点击“**退出保护**”来退出对系统盘的保护。退出保护需要重新启动计算机。

允许每次开机自动进入保护模式：如果您选中了本选项，那么每次开机后，系统将自动进入保护模式，无需每次手工开启对系统分区的保护。

关机时丢弃影子系统内修改的数据：本选择项默认是开启的。如果您选中了本选项，那么在您开启系统的虚拟保护后，系统分区所作的任何修改，将在系统重启后被自动清除。

关机时保存影子系统内修改的数据：本选择项默认是关闭的。如果选中了本选项，那么在您开启系统的虚拟保护后，系统分区的所有修改，将在系统关机时，被自动保存。（注意：请慎重开启本功能，因为如果您的系统不幸中毒或者被感染，那么系统虚拟保护功能将自动清理系统运行时任何被感染的的数据，如果您开启了本功能，那么这些感染的的数据将被保存）。

自动排除：本功能是本产品的特色功能。它可以允许用户在开启保护前将多个文件夹加入排除列表，那么在系统保护开启后，这些文件夹内的修改将被自动保存。点击“**启动排除**”来开启本功能，点击“**停止排除**”来停止本功能。

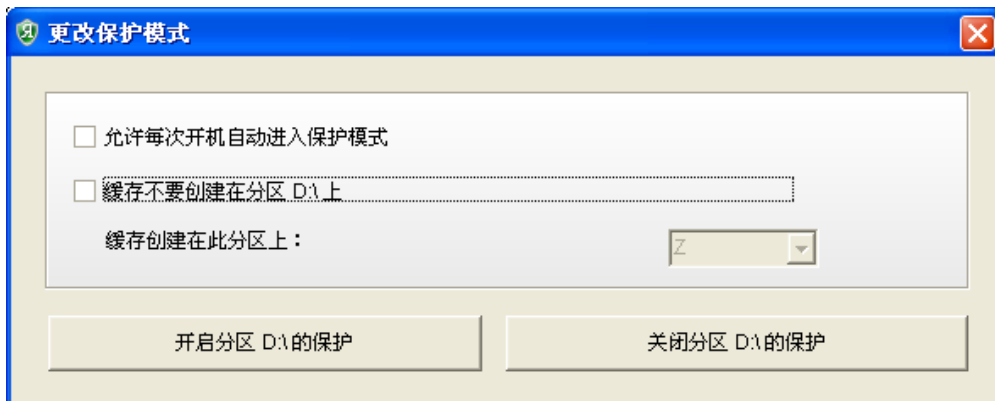
注意：排除列表在系统虚拟保护已经开启之后，将无法添加和删除。如果您需要修改排除列表，则首先请停止系统虚拟保护。

2. 扩展分区保护

在很多情况下，我们的系统除了系统盘，还有其它一些分区，通常这些分区都用来存放一些安装软件或者用户数据。如果除了保护系统盘，您还希望保护这些分区，那么可以使用本功能来实现您的需求。



开启保护：选择一个分区，然后点击“启动保护”，则出现如下窗口：



允许每次开机自动进入保护模式：如果您选中了本项，那么对扩展分区的保护，将在每次开机后自动被开启，无需用户每次手工开启对本分区的保护。

缓存不要创建在分区上：本选项允许系统在保护本分区时，将缓存区设置在其它分区上，这样可以解决在保护本分区时，缓冲区不足的问题。

开启分区的保护：选择本项则可以快速开始对本分区的保护。无需重启电脑。

关闭分区的保护：选择本项则可以快速退出对本分区的保护。注意本功能也无需重启电脑，但需要等待数秒或者数分钟来等待系统退出对此分区的保护。

3. 防御保护



在多数情况下，系统的虚拟保护已经可以满足和防御常见的病毒和木马的需要。但是随着机器狗等病毒的出现，特别是对于网吧机房等客户复杂，计算机使用相对危险较大的场所，我们建议您开启防御保护来使机器狗，Autorun 等病毒，使得这些病毒无法来穿透我们的系统虚拟保护，从而减少您的系统因为被穿透而造成的损失。

防御保护的核心为一个小型的病毒识别库和一个驱动防火墙。驱动防火墙能够检查任何被加载的驱动是否在保护前已经存在于本机的系统分区上。如果是新建的驱动，或者临时生成的驱动，那么驱动防火墙将自动停止这些驱动的加载，以防止这些病毒和木马使驱动技术来破坏我们的系统虚拟保护。

注意：当您需要更新或者升级 Windows 时，请关闭系统防御保护功能，以防止出现无法正常更新的情况出现。

启动保护：点击[启动保护](#)来开启系统的防御保护。

停止保护：点击[停止保护](#)来关闭系统的防御保护。

4. 虚拟分区



虚拟分区是用一个文件虚拟出来的分区，您可以在资源管理器中看到这个分区，并且可以像操作真实分区那样去修改和编辑分区内的数据。和真实的分区的差别在于，这个分区可以被您随意的卸载和加载，同时虚拟分区内的修改，在系统处于保护的情况下，并不会在关机时被清除掉。

加载：点击加载按钮可以立刻将一个虚拟分区显示出来。

卸载：点击卸载按钮可以将一个虚拟分区快速的从资源管理器中删除。

Windows 启动时自动载入虚拟分区：选中本项，在 Windows 系统启动时，虚拟分区将在资源管理器中自动显示。如果未选中本项，您需要在本软件的虚拟分区设置界面，点击加载来手工加载虚拟分区。

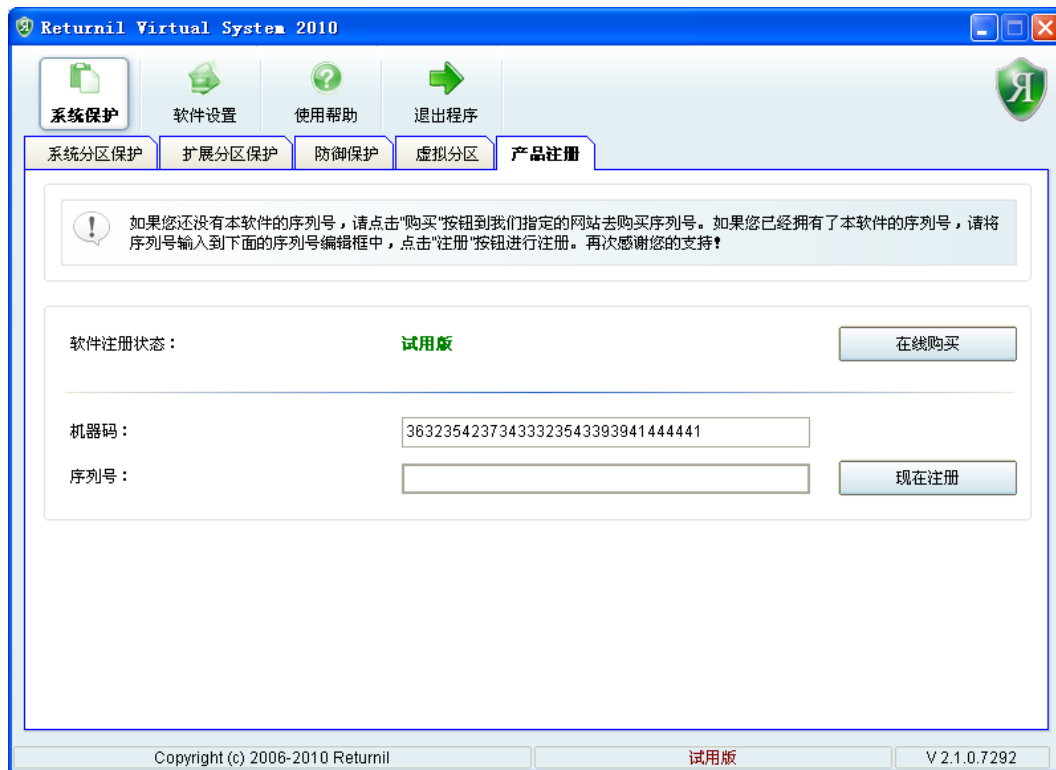
以只读方式加载虚拟分区：选中本项，虚拟分区被加载后，将会变成一个只读的分区，和只读的光盘类似，任何对系统的修改都将被拒绝。

虚拟分区盘符：虚拟分区和真实的分区一样，都需要有一个在资源管理器中显示的盘符，比如 X 盘或者 Q 盘，在这里，您可以设置虚拟分区的盘符，在下次加载时，这个修改将会生效。

5. 产品注册

一个好的产品离不开用户的支持，作为注册用户，将享受我们终身的免费升级服务。如果您购买了我们的产品，那么当购买完成后，需要您发送如下图所示的机器码给我们，我们将在第一时间提供注册码。

当您拿到注册码之后，输入下图所示的序列号中，然后点击现在注册来存储您的注册码。然后请重新启动系统来检查刚才的注册码。



如果注册码是正确的，如上图所示，在软件注册状态一栏，将显示“正式版”字样，否则将显示试用版，如果您的试用超过的试用期，那么此处将显示“过期的版本”。

● 软件设置

软件的运行有很多可设置项，这些可设置项都可以在软件设置单元得到修改和设置。

安全模式下自动停止保护：使用本功能可以让软件的虚拟保护功能在系统进入安全模式后自动停止。

允许快速保护而不输入密码：如果本项被选中，同时您为本软件设置的了密码，那么使用在系统托盘区域的右键菜单中的开启保护功能时，您将不需要输入密码。

在系统托盘显示图标：如果您希望本软件在系统托盘区域显示图标，那么可以选中此功能，否则请不要勾选本功能。

在桌面显示快捷工具栏：如果您希望在桌面上显示快捷工具栏来提示您系统保护的状态，那么可以选中本选项。



使用密码来保护本程序：如果您选中了本选项，那么在打开本软件的主界面时，将出现一个密码输入框来强制用户必须先输入正确的密码。否则，将无法打开软件的主界面。

允许远程控制本机：如果选中了本选项，那么服务器和客户机之间将能够远程连接。关于服务器的使用，请参考服务器的使用章节。

注意：修改本功能需要退出本程序，然后再次打开本程序才能生效。

打开 IE 浏览器时自动开启保护：如果选中了本选项，那么系统将在打开 IE 浏览器之后自动开启系统保护，为用户的互联网浏览保驾护航。



● 使用帮助

点击使用帮助，可以显示本手册。如果您需要更多的帮助信息，请参观我们的网站，或者在网络相关的群和贴吧中获得帮助。

● 退出程序

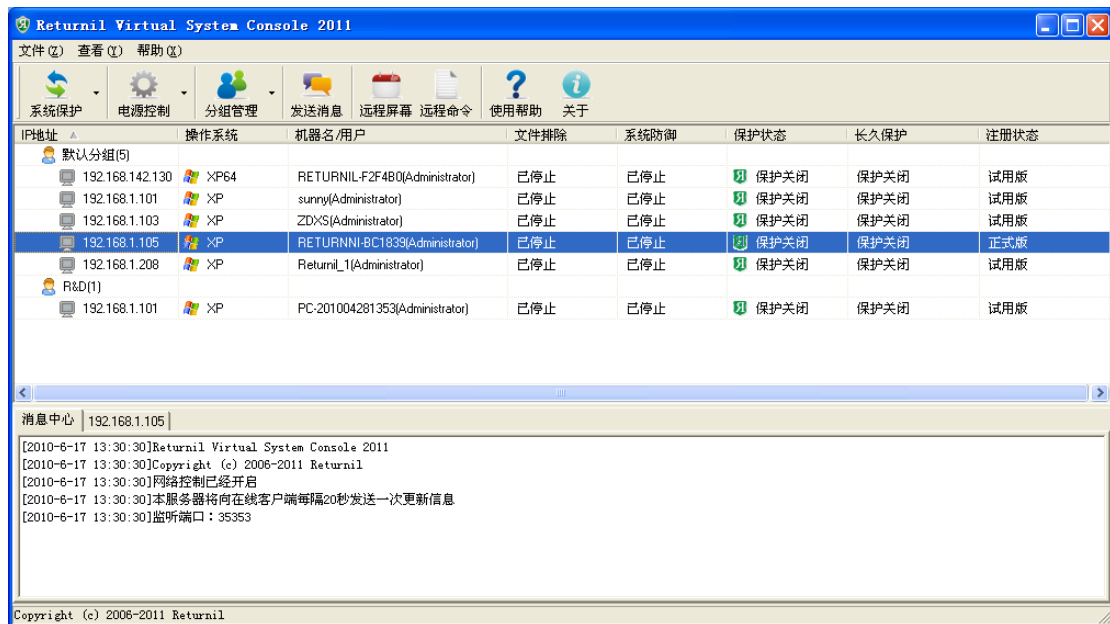
点击退出程序，您可以退出主界面程序，注意：在系统处于保护的状态下，退出主界面程序并不能关闭本软件的保护以及系统防御功能。

产品使用（服务器端）

本软件的安装程序集成了客户端和服务器两个系统的安装（可参考软件安装章节）。在安装软件时可以选择本机将作为服务器，还是作为客户机。如果作为服务器，那么本机需要具备以下条件：

1. 本机的 IP 地址必须固定的，如果使用 DHCP 分配，最好绑定本机的相关硬件，使得每次分配的 IP 地址都是唯一和固定的。
2. 本机具有较好的网络连接环境。比如在网卡，CPU 配置上，最好使用较高的控制，这样才能在控制成百上千台客户机时，具有较高的效率。
3. 在网络防火墙上开放本程序所使用的端口，在本机防火墙中放过本程序的所有网络连接。

本软件的服务器端是从一个台机器集中管理和控制多台客户机的系统。其主界面如下：



从总体上看，主界面分为三个功能：

1. 客户端列表
2. 远程控制功能
3. 消息和日志

● 客户端管理

所有远程的客户端在首次连接本机后将被放置于默认分组中，管理员可以新建分组，然后在客户端列表中选中相应的机器，然后右击鼠标在弹出的菜单中选择移动这些选中的客户端到新的分组中，这样就能在分组中转移客户端。

同时，管理员也可以用相同的右击操作来删除某些未连接的客户端。

● 远程控制功能

1. 系统保护

使用系统保护功能前，请首先选中您希望控制的客户端，然后在工具栏选择系统保护，然后在弹出的菜单中选择您希望远程修改的系统保护功能。

持久保护：选择此功能可以远程开启选中客户机的持久保护，每次客户机开机后将自动进入保护模式。注意：远程执行本功能将自动重启客户机的电脑。

退出保护：选择此功能可以远程关闭客户机的持久保护功能。每次客户机开机后将关闭保护功能。注意：远程执行本功能将自动重启客户机的电脑。

快速保护：选择此功能可以远程开启选中客户机的保护，注意：远程执行本功能将不会重启客户机的电脑。

启动文件排除：选择此功能可以远程开启选中客户机的文件排除功能。

停止文件排除：选择此功能可以远程关闭选中客户机的文件排除功能。

启动系统防御：选择此功能可以远程开启选中客户机的系统防御功能。

停止系统防御：选择此功能可以远程停止选中客户机的系统防御功能。

设置密码：选择此功能可以远程设置选中客户机的密码。

更改服务器：可以修改选中客户机的连接服务器。客户机在重启后将会自动连接到新的服务器上。

设置注册码：选择此功能可以远程设置选中客户机的注册码，需要重启客户机才能检查注册码是否正确。

2. 电源控制

使用电源控制功能前，请首先选中您希望控制的客户端，然后在工具栏选择电源控制按钮，然后在弹出的菜单中选择您希望远程控制的电源功能。

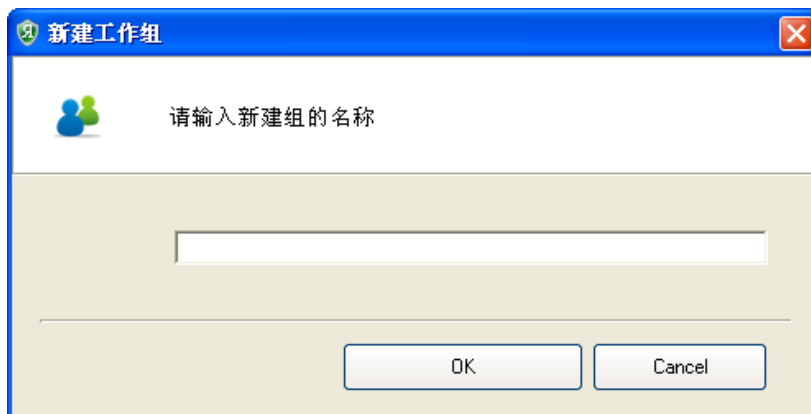
关机：选择此功能可以远程关闭选中的客户机电脑。

重启：选择此功能可以远程重启选中的客户机电脑。

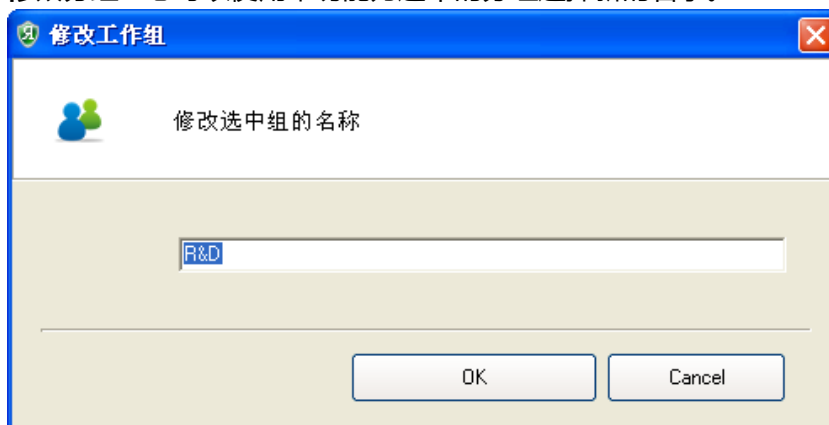
3. 分组管理

使用分组管理功能前，请首先选中您希望控制的客户端，然后在工具栏选择系统保护，然后在弹出的菜单中选择您希望远程修改的系统保护功能。

新建分组：您可以新建一个分组，注意：新建组的名称不能和已建立的分组重复。



修改分组：您可以使用本功能为选中的分组选择新的名字。



删除分组：删除选中的分组后，所有本分组中的客户机将自动进入默认分组中。
注意：您无法删除默认分组。

移动客户端到新组：如果希望将某些客户端移动到新的分组中，那么只需选中这些客户端，然后右击鼠标，在弹出的菜单中选中移动客户端即可。

删除客户端：如果希望删除某些客户端，那么需要首先选中这些客户端，然后右击鼠标，在弹出的菜单中选中删除客户端即可。注意：如果客户端被删除后，客户端还是可以继续连接到本服务器。

4. 发送消息

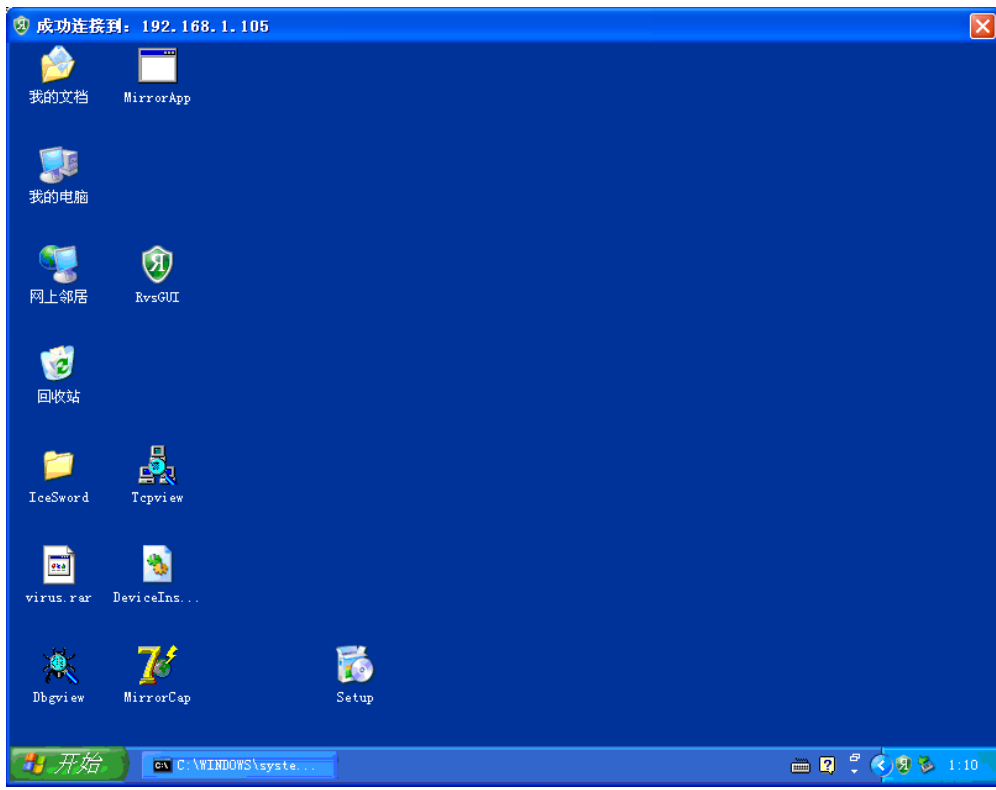
使用本功能，您可以和选中的客户端进行文字聊天，服务器发送的消息在所有选中的客户端中可见，但是请注意：客户端回复的消息只在服务器端显示，其它客户机无法看到其它客户机向服务器回复的信息。

在消息框中输入您希望传达到客户端的消息，然后按 CTRL+ENTER 或者点击发送按钮将把信息传递到客户机中。单次发送的最大消息长度为 1024 字节。



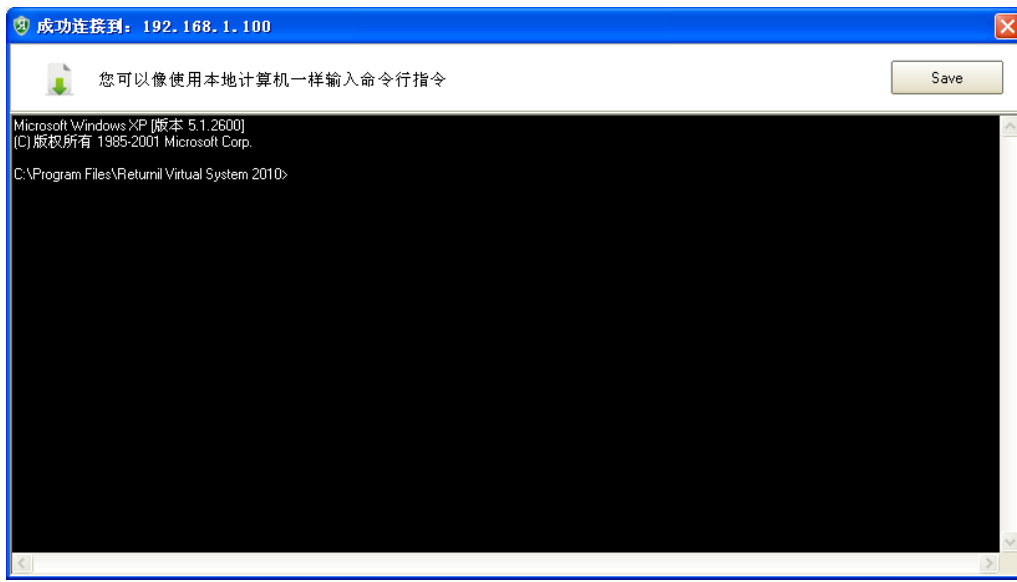
5. 远程屏幕

使用本功能，您可以远距离监控客户机的桌面画面，并查看其实时的桌面变化。注意：当客户机进入屏保状态，或者桌面被锁定后，远程屏幕功能将无法更新客户机的桌面图像。



6. 远程命令

使用本功能，您可以像在本地使用命令工具(CMD)一样的远程执行命令。如下图所示，在任何提示符下都可以输入符合条件的语句，例如：输入 Dir，然后回车，那么将显示当前路径所有的文件和文件夹。



售后服务

所有本软件的正版用户都可以通过向 support-china@returnnil.com 发送邮件来获得相应的帮助和支持。

南京研发中心：

联系电话：025-83608065

传真电话：025-83608067

芬兰总部：

Fredrikinkatu 45 A

00100, Helsinki, Finland

Phone: +358 442056919

email: finland@returnnil.com

美国分公司：

email: usa @returnnil.com

俄罗斯分公司

Office 328C, Building 3

15 Kondratyevskiy Prospekt

St.Petersburg, 195197, Russia

Phone/Fax: +7 812 4585601

email: russia @returnnil.com