瑞星杀毒软件网络版使用手册

北京瑞星科技股份有限公司

软件产品说明

1.1 产品组成

当您通过合法途径获得瑞星杀毒软件网络版的使用权后，在安装使用前，请仔细检查核对包装内的《产品组件清单》。

1. 光盘：包含用户所购买的瑞星杀毒软件网络版所有程序。

2. 《使用手册》：即本手册，通过阅读它，掌握本软件的详细使用方法和技巧。

3. 《客户服务指南》：该指南将帮助用户获取技术支持和服务方面的信息。

4. 用户注册卡：用于确认用户合法使用本套软件的合法资格（注意：在打开包装后，请填写并以“挂号”或“快递”方式寄回瑞星公司客户服务中心）。

5. 《快速安装指南》：指导用户快速掌握软件安装的方法。

6. 回寄信封：用于邮寄“用户注册卡”。

7. 产品序列号：为本套产品分配的唯一身份证明，缺少它，本软件将无法安装。（注意：产品序列号见本手册封二和“用户注册卡”）。

8. 《产品组件清单》：用于核对产品组件，以确定产品的完整性。

1.2 应用环境

1.2.1 系统中心

a. 软件环境

1）操作系统

Windows NT Server 4.0 with Service Pack 6.（不推荐）

Windows 2000 Advanced Server with Service Pack 4 or later

Windows 2000 Server with Service Pack 4 or later

Windows Server 2003 Enterprise with Service Pack 1 or later（推荐）

Windows Server 2003 Standard with Service Pack 1 or later

Windows Server 2003 Web with Service Pack 1 or later

Windows Server 2003 R2 Enterprise.

Windows Server 2003 R2 Standard.

2）其它

Microsoft Internet Explorer 6.0 with Service Pack 1 or later

b. 硬件和网络要求

剩余磁盘空间：2GB以上，如果有漏洞扫描功能，建议将漏洞补丁保存路径所在盘保留2G以上空间

CPU： Intel Pentium IV 3.0G以上

内存：1GB以上，最大支持4GB

网络环境：100M以上网络，需一个固定IP地址

说明：

如果管理250台以上的客户端，建议将系统中心部署在专用服务器上。

为保证防病毒系统的及时更新，请确保计算机能够实时连接Internet。

1.2.2 客户端/服务器端

a. 软件环境

1）Microsoft Windows家族、主要的Unix操作系统（Linux、FreeBSD、Solaris）。包括：

客户端：

Windows 95

Windows 98

Windows Me

Windows NT Workstation 4.0

Windows 2000 Professional

Windows XP Professional/Home Edition

Windows Vista

FreeBSD

UNIX（SUN Solaris系列、IBM AIX系列）

Linux（RedHat Linux、红旗Linux等基于Intel x86芯片的系统）

服务器端：

Windows NT Server

Windows 2000 Server/Advanced Server

Windows 2003 Server

2）Internet Explorer 6.0以上

b. 硬件环境

剩余磁盘空间：600MB以上；作为升级代理时，1GB以上

CPU： 800MHz以上

内存：256MB以上，最大支持4GB

1.2.3 管理控制台

管理控制台软件必须安装在 Windows 家族的操作系统平台上。

2 软件概述

瑞星杀毒软件网络版整个防病毒体系是由以下几个相互关联的子系统组成。每一个子系统均包括若干不同的模块，除承担各自的任务外，还与其它子系统通讯，协同工作，共同完成对网络的病毒防护工作。

说明：本使用手册针对网吧版、中小企业版、企业版、企业专用版、高级企业版和高级企业专用版等六个版本软件的使用方法进行阐述，由于各个版本的软件功能不同，请用户在使用软件前详细了解所购买的相关产品的功能。

具体差异参考下面的各个版本的功能差异表格：

功能	网吧版	中小企业版	企业版	企业专用版	高级企业版	高级企业专用版
客户端远程安装	无	有	有	可定制	有	可定制
远程查杀	无	有	有	可定制	有	可定制
漏洞扫描	无	有	有	可定制	有	可定制
广播信息	无	有	有	可定制	有	可定制
IE 历史记录	有	无	无	无	无	无
授权计数的限制	无	有	无	无	无	无
防火墙功能	无	无	无	无	有	可定制
Lotus Notes 嵌入式杀毒	无	有	有	可定制	有	可定制
Office/IE 嵌入式杀毒	无	有	有	可定制	有	可定制
邮件监控	无	有	有	可定制	有	可定制
瑞星助手	无	有	有	可定制	有	可定制
硬盘备份	无	有	有	可定制	有	可定制
客户端漏洞扫描工具	无	有	有	可定制	有	可定制

说明：表格中的“有”代表在相应的版本中默认有此功能，“无”代表在相应的版本中默认没有此功能，“可定制”代表该功能在相应的版本中，用户需要在购买时根据需要定制该功能，未定制的功能在所购买的产品中不能被使用。

2.1 系统中心

系统中心是瑞星杀毒软件网络防病毒系统命令发布、信息存储以及安全状况分析的管理核心。它实时记录防护体系内每台计算机上的查杀病毒情况、主动防御信息、漏洞情况、安全状况等，为超级管理员分析整个网络中的安全情况提供了大量的依据。通过管理控制台发布查杀病毒、升级等各项命令，统一设置网络安全的各种策略，实现对整个防护系统的自动控制，保障整个网络安全。

注意：

1. 其它子系统只有在系统中心工作后，才可实现各自的网络防护功能。
2. 系统中心必须先于其它子系统安装到符合条件的服务器上。

按照系统中心在局域网中的安装规模可以分为单级系统中心、多级系统中心和超级系统中心。

单级系统中心：一个级别的系统中心，即在网络环境中仅有一个级别的系统中心，管理其客户端防病

毒子系统。说明：网吧版和中小企业版属于单级系统中心产品。

多级系统中心：在网络环境中可以安装两级系统中心，实现上级系统中心对下级系统中心及其客户端的管理。说明：企业版和企业专用版属于多级系统中心产品。

超级系统中心：在大型企业中（如跨国公司），存在着复杂的网络结构，为了提供统一的防毒管理，通过部署多层次的系统中心，将整个企业的防毒结构构建成一棵逻辑树。父系统中心可以管理其所有直属子系统中心（包括其客户端）和间接下属的系统中心（包括其客户端）；即超级系统中心可以管理到其下属的任何一级的子系统中心（包括其客户端），但是不能管理其父中心。说明：在高级企业版和高级企业专用版属于超级中心产品。

2.2 服务器端

服务器端是专门为可以应用于网络服务器的操作系统而设计的防病毒子系统。

2.3 客户端

客户端是专门为网络工作站（客户机）设计的防病毒子系统。它利用其有效的病毒查杀，可控的危险行为防御，及时的电脑安全检测，定期的日志上报和分析，全方位地保障用户计算机乃至整个网络的安全。

注意：在本文中所涉及到的防病毒子系统描述均使用“客户端”一词，不再单独区分“客户端”与“服务器端”。

2.4 管理控制台

管理控制台是在网络上集中管理所有安装有瑞星杀毒软件网络版客户端软件计算机的管理工具。通过管理控制台可以了解整个网络中的总体安全状况并且远程管理网络中任何一台计算机中的瑞星杀毒软件。网络上任何一台计算机的病毒警告信息都能在管理控制台得到汇总，通过管理控制台也能直观地查看网络上所有计算机当前的实时监控状态、病毒查杀情况、主动防御状态和当前版本信息等。管理控制台能对远程计算机安装瑞星杀毒软件和移动管理控制台，让管理控制台自由移动到管理员认为合适的计算机上去。管理员通过对管理控制台的操作就能对网络上所有计算机进行定期、实时地查杀病毒和全网统一升级管理，真正做到在整个网络中建立一套坚实的网络病毒防护系统。

2.5 多级中心

瑞星杀毒软件网络版多级中心系统支持大型的、多层级的、复杂的网络。通过该系统可实现对本级系统中心和临近的系统中心及所有下属客户端的统一管理和分布管理，统一管理表现为由上级中心统一发送查杀病毒命令、下达版本升级指示，并及时掌握全部系统中心（包含下级中心）的病毒分布情况等；分布管理表现为下级中心既可以在收到上级中心的命令后作出响应，也可以管理本级系统中心下属客户端，并主动向上级中心发送请求和汇报信息。多级中心通讯代理包括 Receiver 上级通讯代理和 Sender 下级通讯代

理两个功能模块，用于实现在多级中心中不同层级间的系统中心的互通和管理。

2.6 超级中心

瑞星杀毒软件网络版超级中心系统基于多级中心系统的工作原理，对多级中心系统进一步扩充，能够实现对涉及范围内的任意级系统中心及下属客户端的集中管理，适合大型网络用户。

3 安装与卸载

瑞星杀毒软件网络版的基本安装对象包括“系统中心的安装”、“服务器端的安装”、“客户端的安装”和“管理控制台的安装”。安装时建议先在服务器上安装“系统中心”，然后在其它计算机上安装客户端或服务器端。

3.1 系统中心安装与卸载

系统中心负责管理、协调瑞星杀毒软件网络版所有子系统的工作；实现授权许可证的验证和管理；负责瑞星杀毒软件网络版中各系统版本更新及检测和清除病毒等工作。

注意：安装系统中心时，安装程序将在该服务器上同时安装一套服务器端系统和一套管理控制台系统。

3.1.1 建议系统中心的安装条件

A） 全天候开机：为确保正常实现系统中心所有功能，安装系统中心的计算机应该在有效工作期内保持全天候的开机状态。

B） 可方便的连接 Internet：瑞星杀毒软件网络版具有自动升级的功能，为保证此功能的顺利实现，系统中心所在服务器应能接入互联网。

注意：为了保障防病毒系统顺利工作，建议将系统中心安装在独立的服务器上面。

3.1.2 安装过程

第一步：将瑞星杀毒软件网络版光盘放入光驱内，启动瑞星杀毒软件网络版安装主界面后，选择【安装系统中心组件】按钮开始安装。

图 31

第二步：进入安装程序欢迎界面，提示用户使用安装向导以及相关建议和警告等，用户可以通过【下一步】按钮继续安装，还可以通过【取消】按钮退出安装过程。

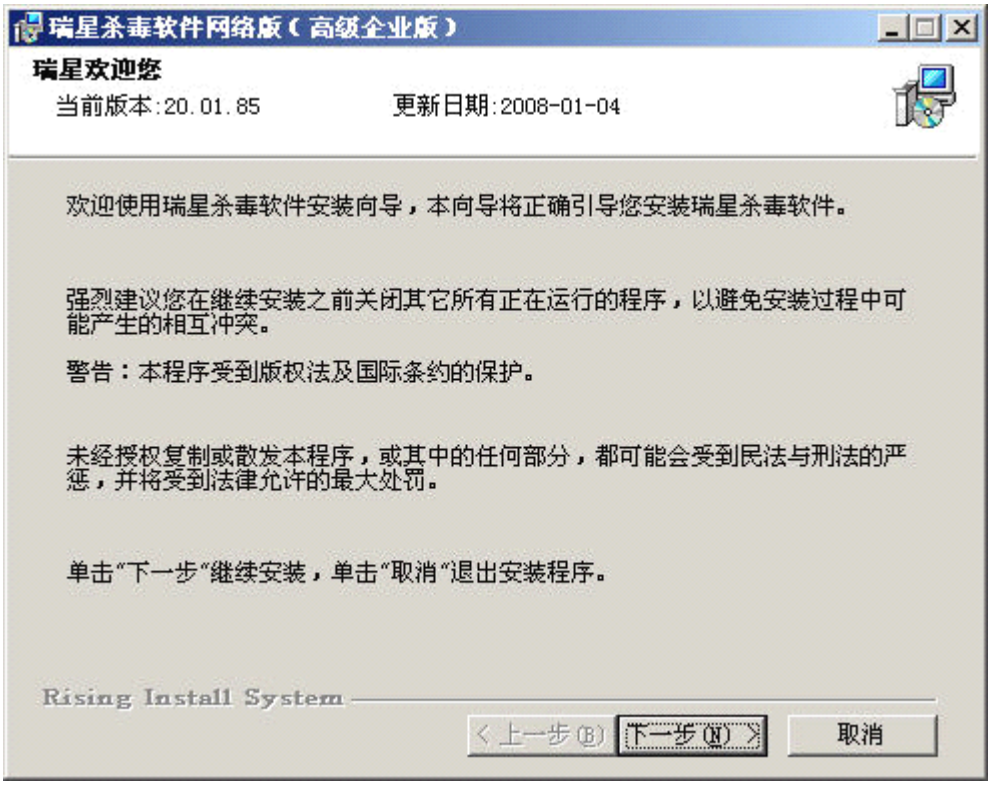

图 32

注意：如果用户安装了与瑞星杀毒软件网络版冲突的软件，会在该页面出现前弹出冲突软件提示界面。如果再继续安装本软件可能会产生问题，建议卸载后再执行本程序。

第三步：提示用户在安装前阅读【最终用户许可协议】，用户认真阅读本协议后可以选择【我接受】或【我不接受】。选择【我接受】，单击【下一步】继续安装；选择【我不接受】，安装终止；单击【取消】直接退出安装过程。

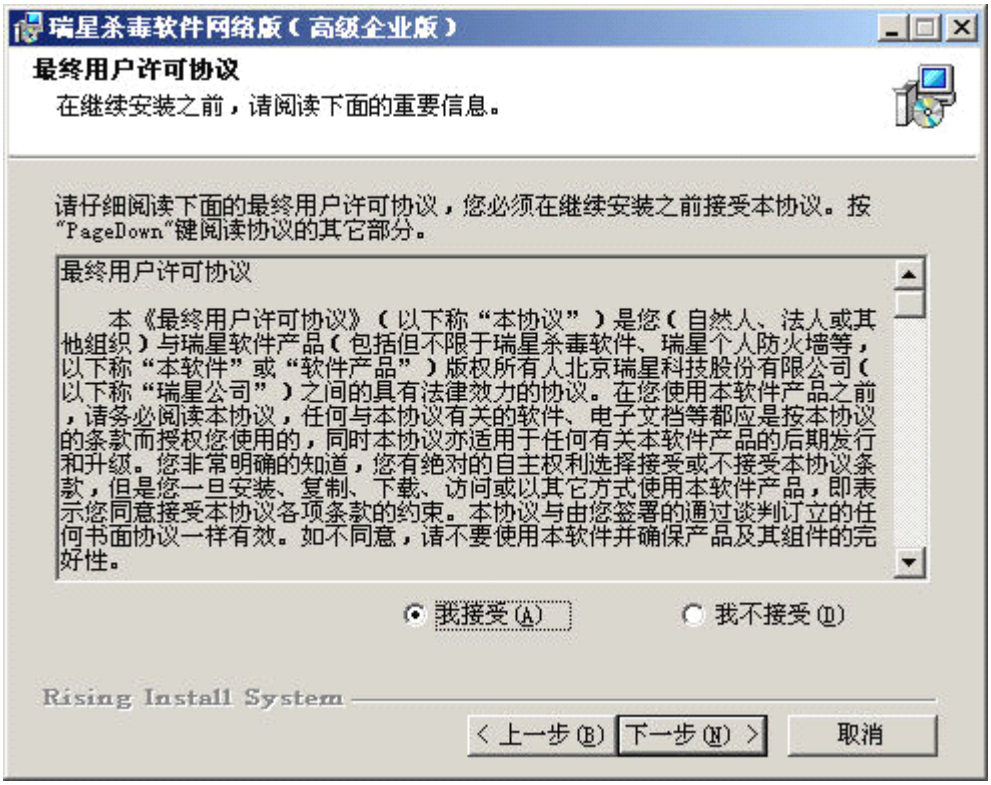

图 33

注意：选择【我接受】继续安装后，如果计算机配置了多网卡或存在多个 IP 地址将会出现【选择 IP 地址】界面。由用户指定所需 IP 作为通讯 IP，为了高效通讯建议采用内部网络地址。

第四步：根据实际需要选择相应的组件，单击【下一步】继续安装。

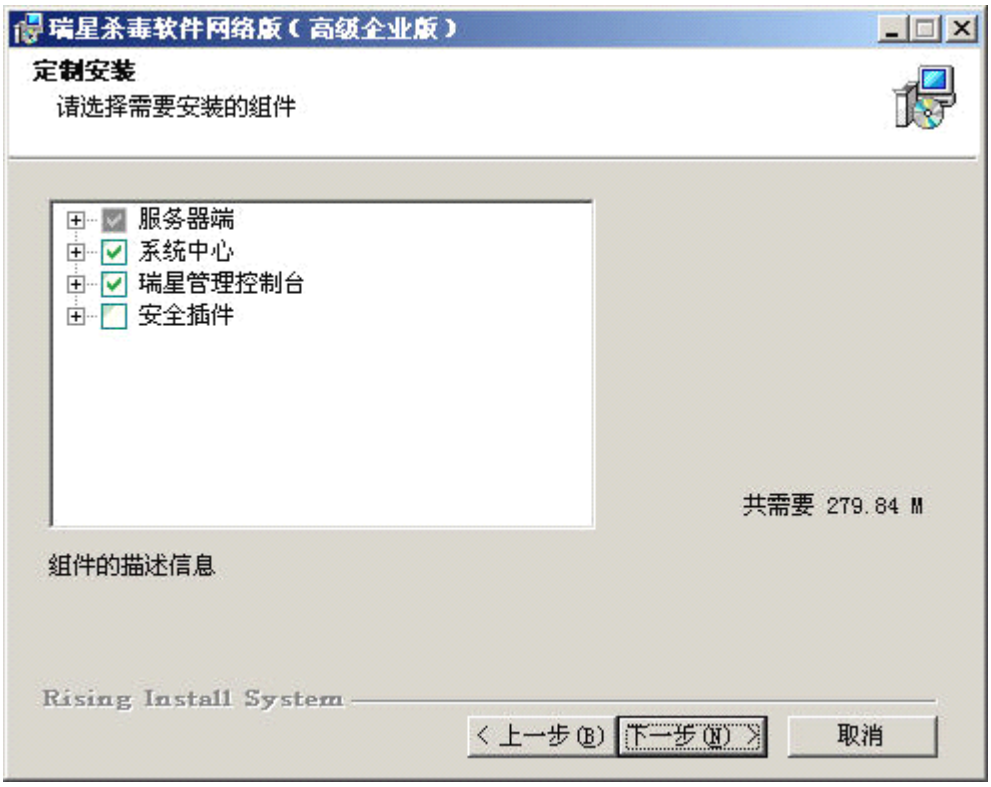

图 34

注意：安全插件功能依赖华为 3COM 设备和软件的支持。

第五步：进入数据库的安装界面，选择数据库的类型及相关参数。有三种数据库类型可选择，分别为【在本机上安装 MSDE】、【正在运行的 MS SQL SERVER】、【已经存在的 MSDE 数据库】。默认设置为【在本机上安装 MSDE】，若网络中没有 SQL SERVER，在磁盘空间许可的情况下建议选择此项。设置 MSDE 数据库各项参数后，单击【下一步】继续安装；

图 35

若安装环境中已有 SQL SERVER，可以选择【正在运行的 MS SQL SERVER】，设置各项参数后，单击【下一步】继续安装。

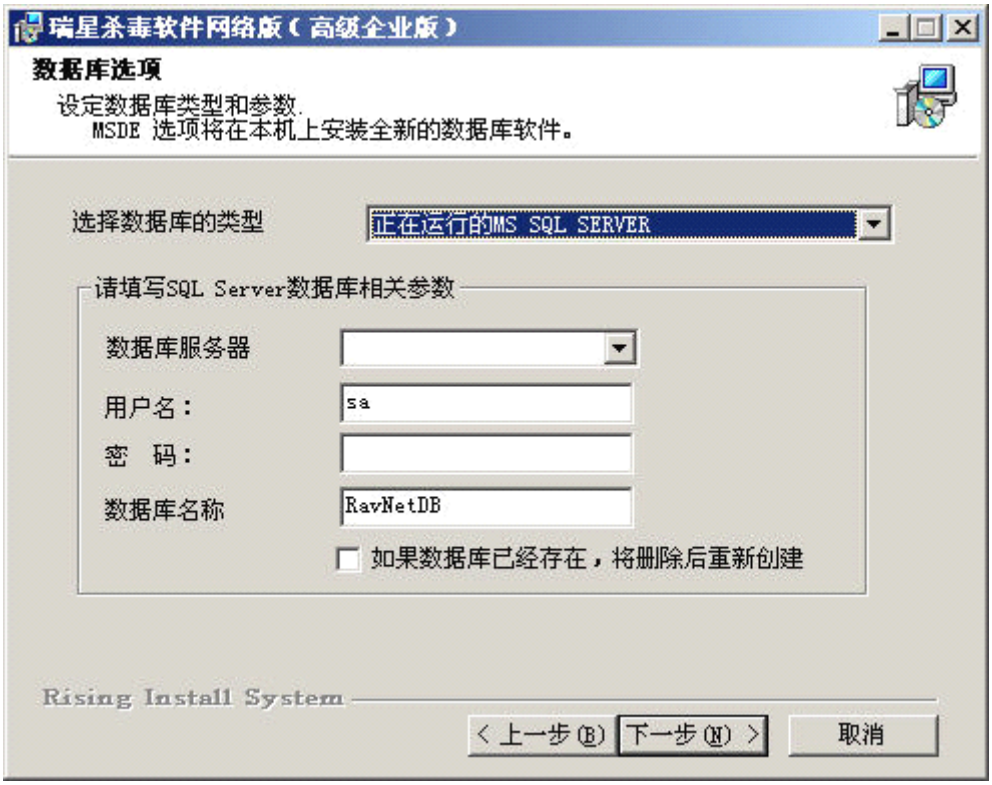

图 36

若安装环境中已有 MSDE，可以选择【已经存在的 MSDE 数据库】，设置各项参数后，单击【下一步】继续安装。

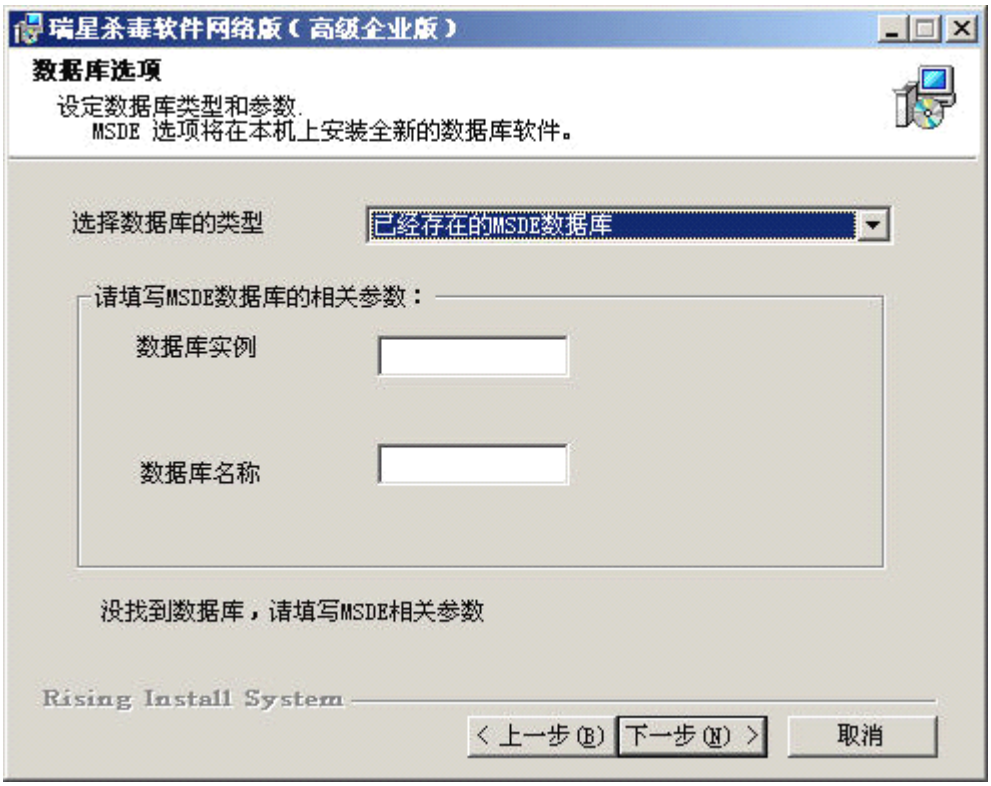

图 37

第六步：输入瑞星杀毒软件网络版产品序列号（序列号见本使用手册封二）；正确输入产品序列号后，立即显示产品类型、服务器端和客户端允许安装的数量，如下图：

图 38

第七步：在【网络参数设置】界面显示系统中心 IP 地址，单击【下一步】继续安装。

图 39

第八步：在【选择目标文件夹】界面中选择安装瑞星软件的目标文件夹，单击【下一步】继续安装。

图 310

第九步：在【设置补丁包共享目录】界面中，设置提供客户端下载补丁包的共享目录和共享名称，为了安装方便用户可使用默认名称，单击【下一步】继续安装。

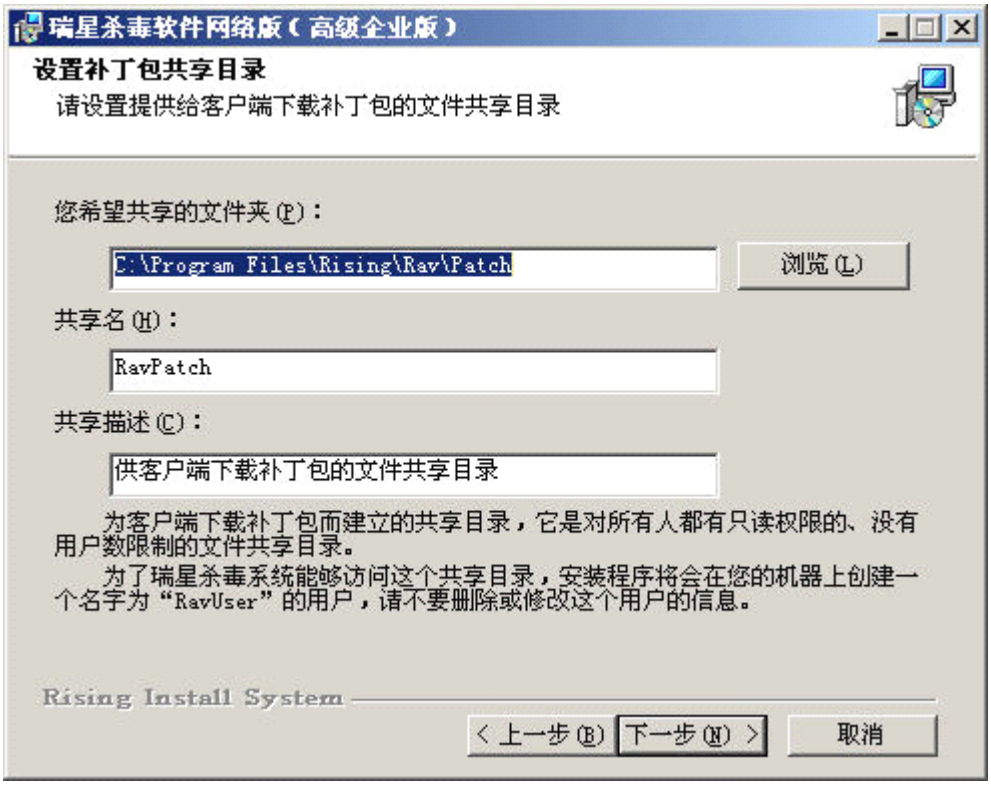

图 311

第十步：在【瑞星杀毒系统密码】界面中，输入系统管理员密码和客户端保护密码，如不设置，默认口令都为空，在此也可以为瑞星日志查询工具中的计划任务管理预先配置向管理员发送报表的 SMTP 服务器参数，还可以单击【详细】按钮进行详细设置，设置完毕后，单击【下一步】继续安装。

图 312

第十一步：【选择开始菜单文件夹】界面中，输入用户需要在开始菜单文件夹中创建的程序快捷方式名称，单击【下一步】继续安装。

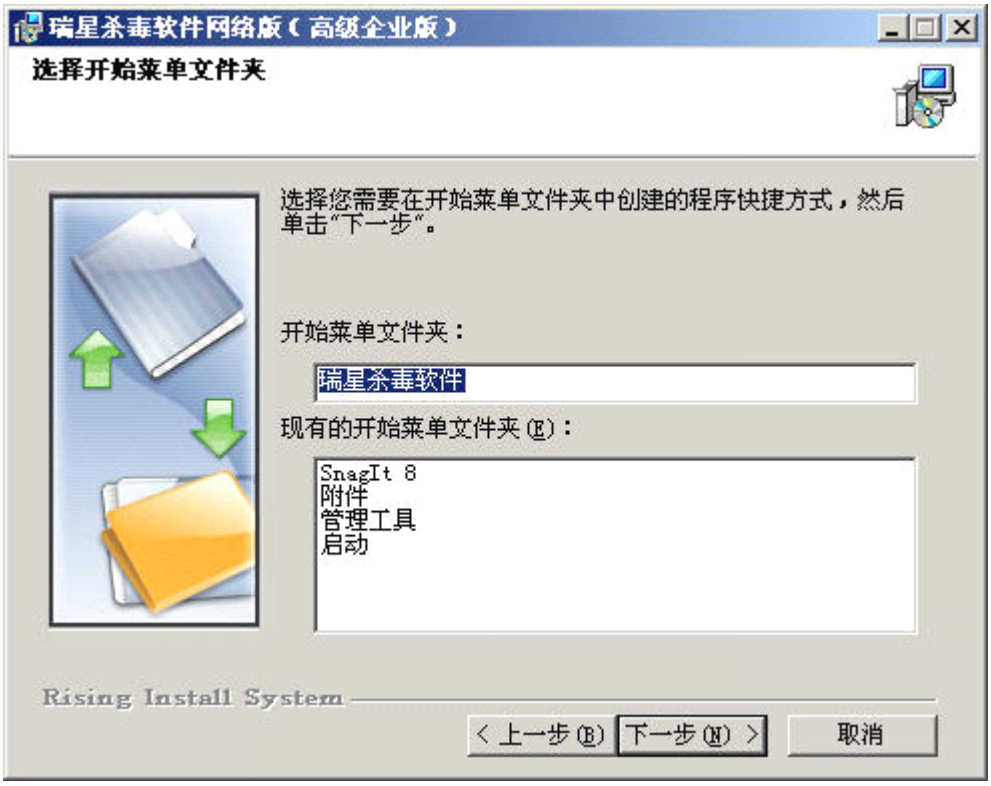

图 313

第十二步：在【安装准备完成】界面中确认安装信息，单击【上一步】可进行修改，单击【下一步】继续安装；若不勾选【安装之前执行内存病毒扫描】，将直接进入第十三步。

图 314

第十三步：安装程序将进行安装前的系统内存查毒，单击【跳过】可直接开始复制文件，建议完成系统内存查毒操作后再开始复制文件，查毒完成后单击【下一步】继续，安装程序将开始复制文件。

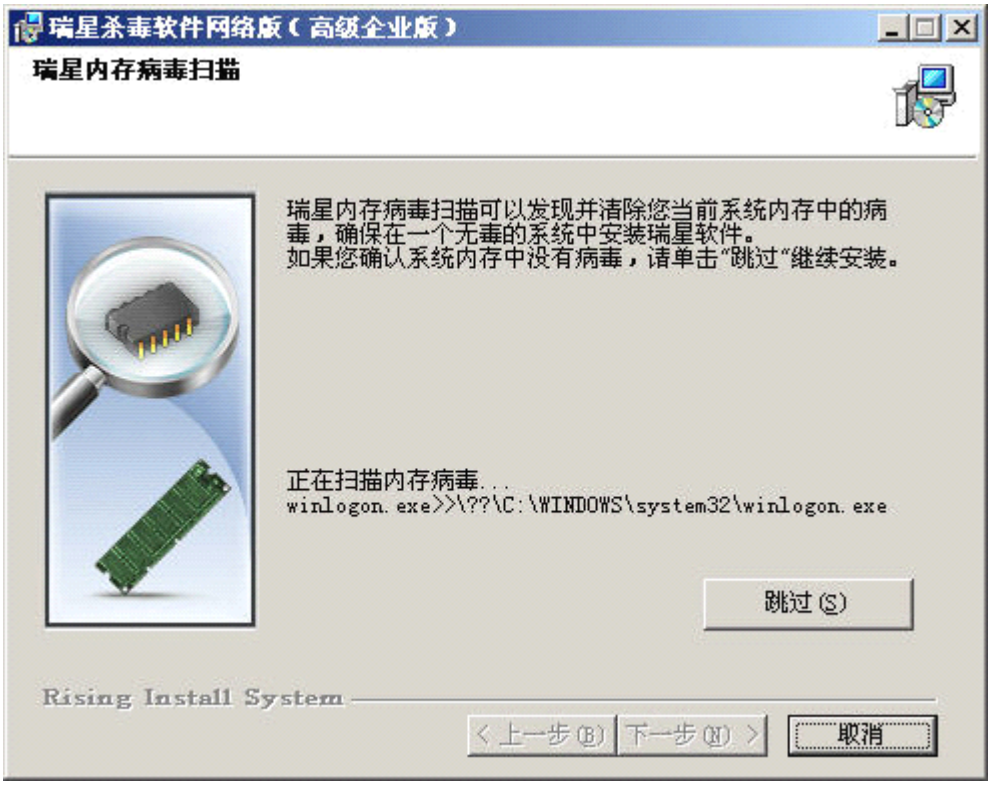

图 315

第十四步：显示安装过程，单击【显示信息】按钮可详细查看具体过程信息。

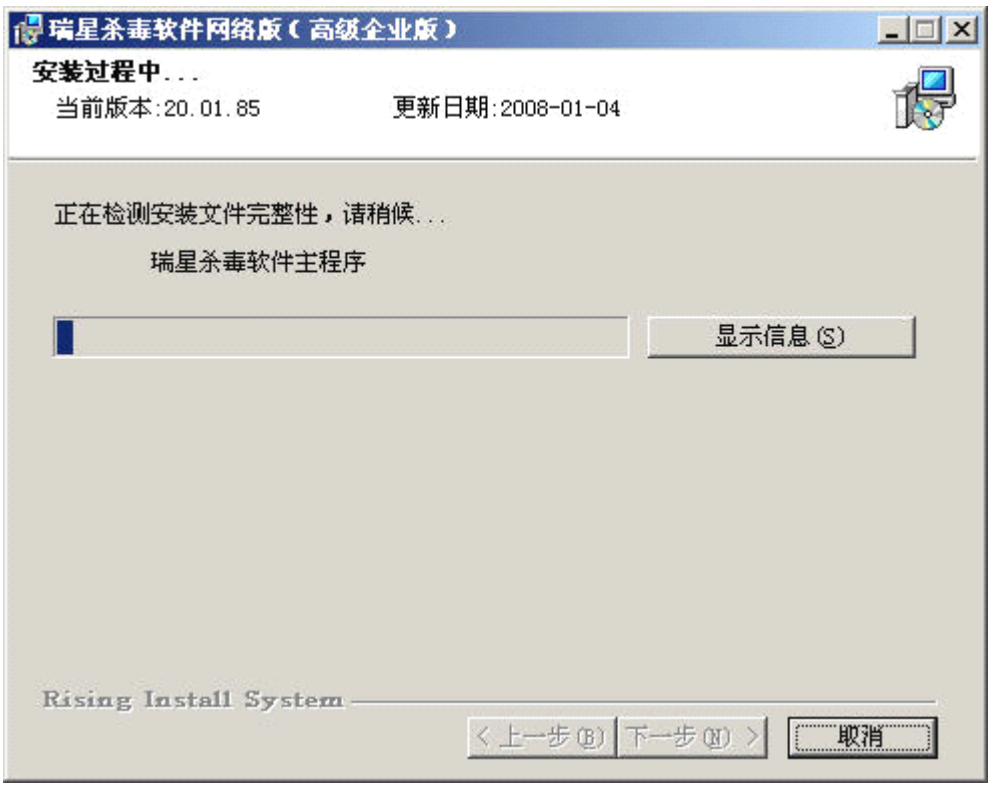

图 316

第十五步：安装完成，默认勾选【重新启动计算机】选项，点击【完成】按钮重新启动计算机完成安装。若不希望立即重新启动计算机可不勾选该选项，今后再重新启动计算机完成安装过程。

图 317

第十六步：重新启动计算机后将显示瑞星杀毒软件网络版安装过程。安装完成后，提示用户选择是否运行监控中心、管理控制台和杀毒软件主程序，并且还可以添加瑞星图标到桌面或者快速启动工具条。

图 318

3.1.3 卸载过程

第一步：在 Windows 画面中，选择【开始】/【程序】/【瑞星杀毒软件】/【添加删除组件】，在弹出的【瑞星软件维护模式选项】界面中选择【卸载】，单击【下一步】开始卸载。

另一种方式：在 Windows 画面中，选择【开始】/【控制面板】/【添加/删除程序】/【瑞星杀毒软件网络版】/【更改/删除】，开始卸载瑞星杀毒软件。

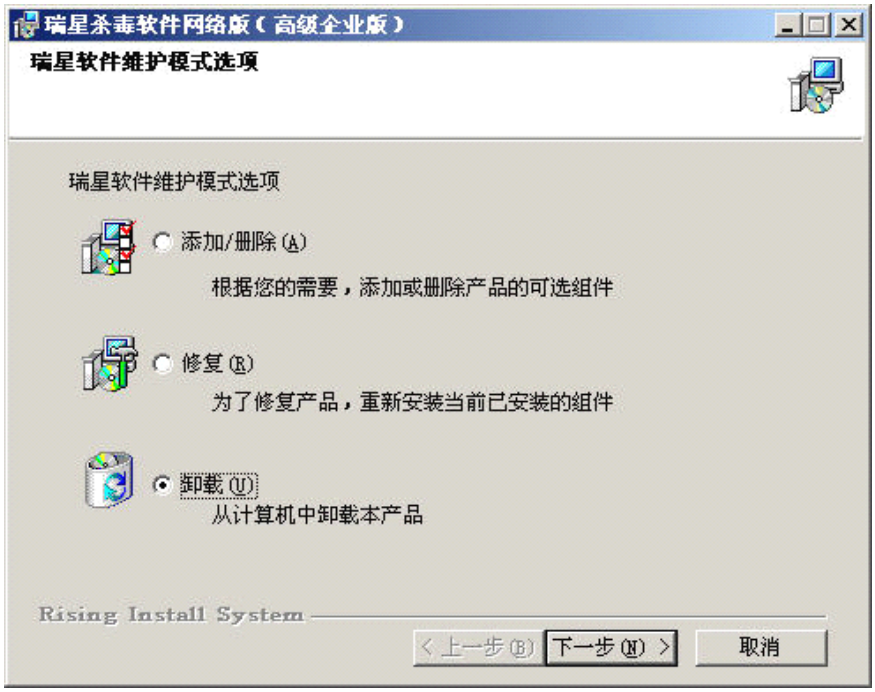

图 319

第二步：在【数据文件删除确认】界面中选择是否删除数据文件，包括存放补丁包的目录和补丁文件，

病毒记录和事件日志数据库文件。若用户不需要保留上述文件，勾选准备删除的文件，单击【下一步】继续，在此建议用户在卸载时保留或备份补丁包文件和日志数据库。

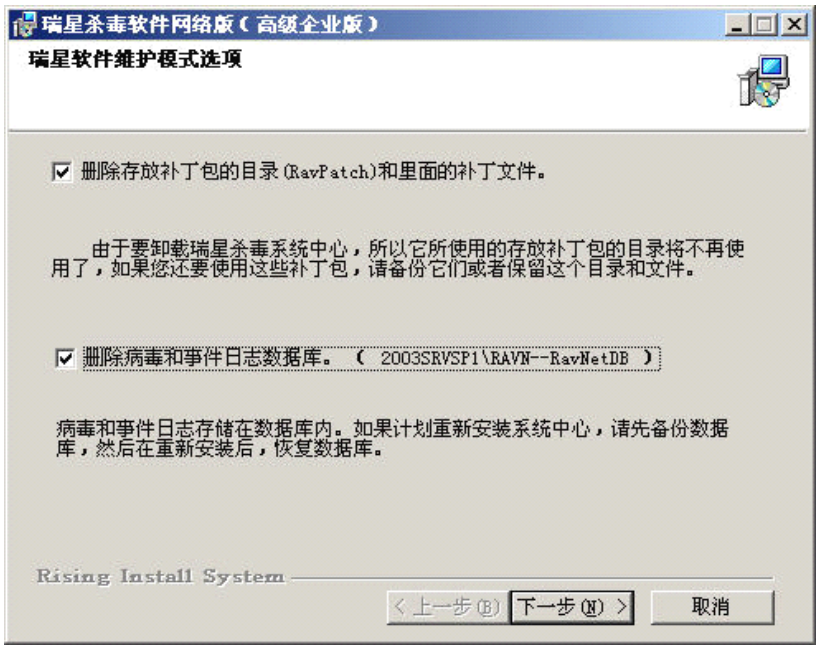

图 320

第三步：确认卸载信息，单击【上一步】可进行修改，单击【下一步】继续。

图 321

第四步：显示卸载进度，单击【显示信息】按钮查看详细卸载信息。

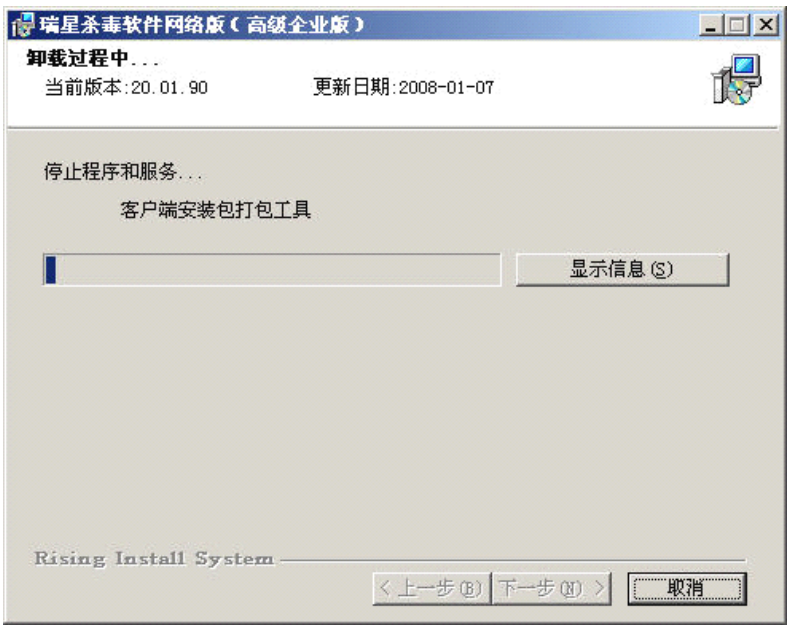

图 322

第五步：单击【完成】卸载结束。

图 323

注意：卸载后系统要求用户重新启动计算机，如果不希望立即重新启动计算机可以不勾选【重新启动计算机】项，瑞星杀毒软件网络版将在下次重新启动计算机时完成全部卸载工作。如果用户不选择重新启动，将不影响用户使用计算机，但用户不能再次安装瑞星相关软件，只有在用户重新启动之后才能再次安装瑞星软件。

3.1.4 添加删除组件

第一步：在 Windows 画面中，选择【开始】/【程序】/【瑞星杀毒软件】/【添加删除组件】，在弹出的【瑞星软件维护模式选项】界面中选择【添加/删除】，单击【下一步】继续。

另一种方式：在 Windows 画面中，选择【开始】/【控制面板】/【添加/删除程序】/【瑞星杀毒软件

网络版】/【更改/删除】，在弹出的【瑞星软件维护模式选项】界面中选择【添加/删除】，单击【下一步】继续。

第二步：在【定制安装】页面中选择需要添加或者删除的组件，单击【下一步】按钮继续，直到添加删除组件结束。

3.2 服务器端和客户端的安装与卸载

3.2.1 本地安装

本地安装是直接利用安装程序在本地完成安装的方法。无论是客户端和服务器端都可以采取本地安装的方式。

3.2.1.1 安装过程

第一步：单击光盘自动运行程序界面上的【安装瑞星杀毒软件网络版】，或运行光盘中的 Ravsetup.exe 安装程序（Ravsetup.exe 安装程序可脱离原有介质复制到本地计算机中运行），单击【安装瑞星杀毒软件客户端】按钮。

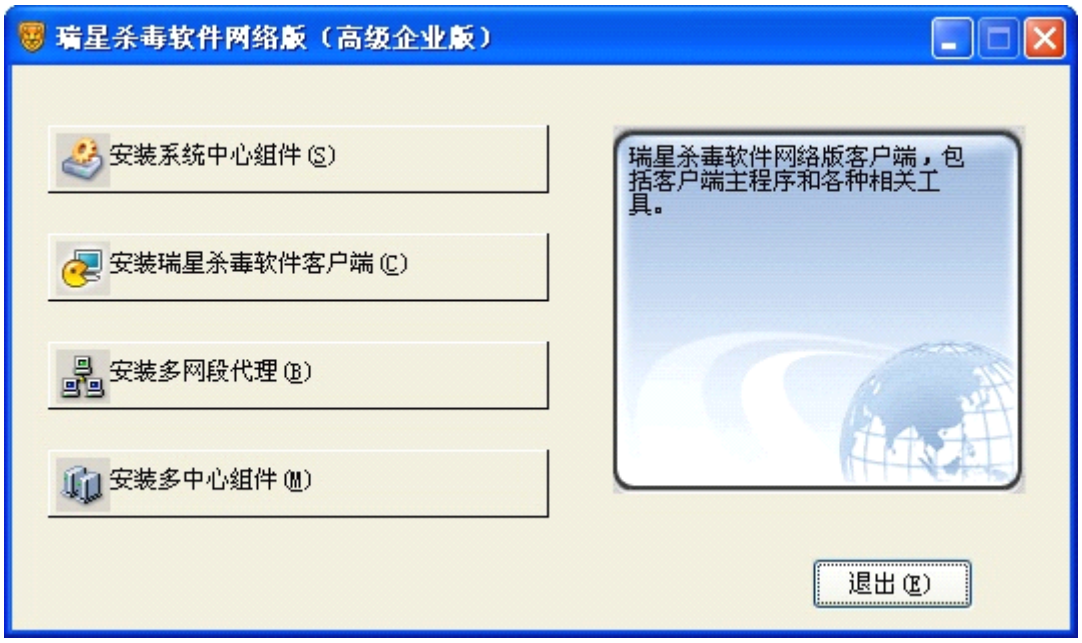

图 324

第二步：进入安装程序欢迎界面，单击【下一步】继续安装，还可以通过【取消】按钮退出安装过程 。

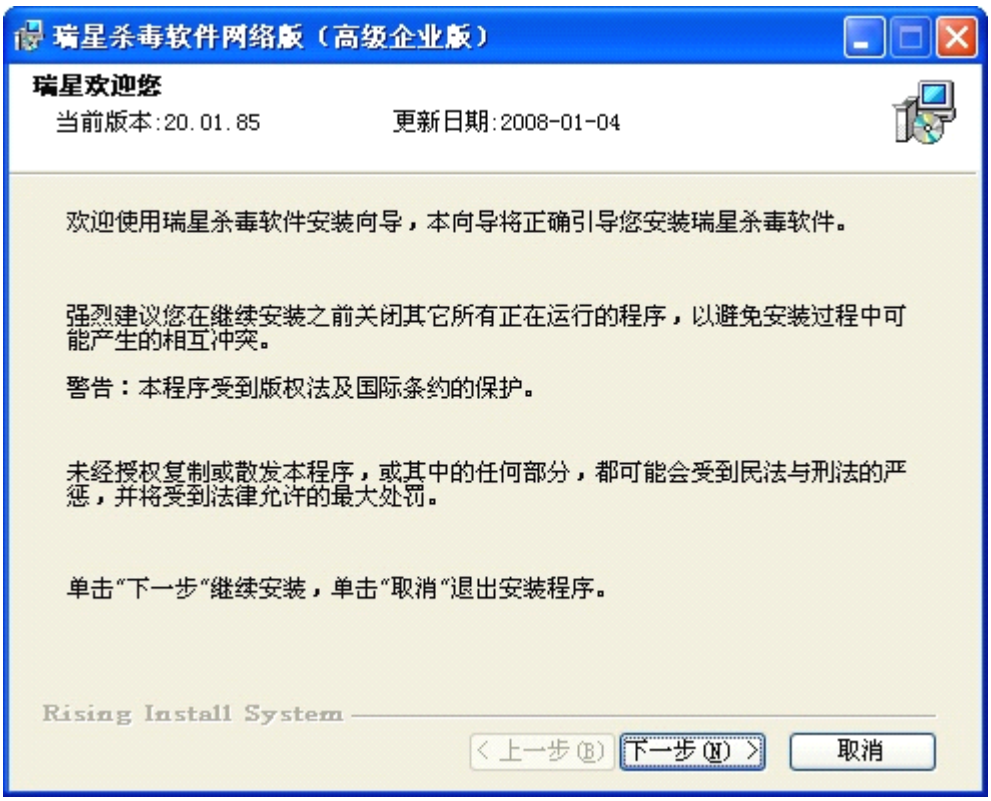

图 325

第三步：弹出【最终用户许可协议】窗口，请仔细阅读软件许可协议。如果接受，请选择【我接受】单击【下一步】继续安装；如不接受该协议，选择【我不接受】退出安装程序。

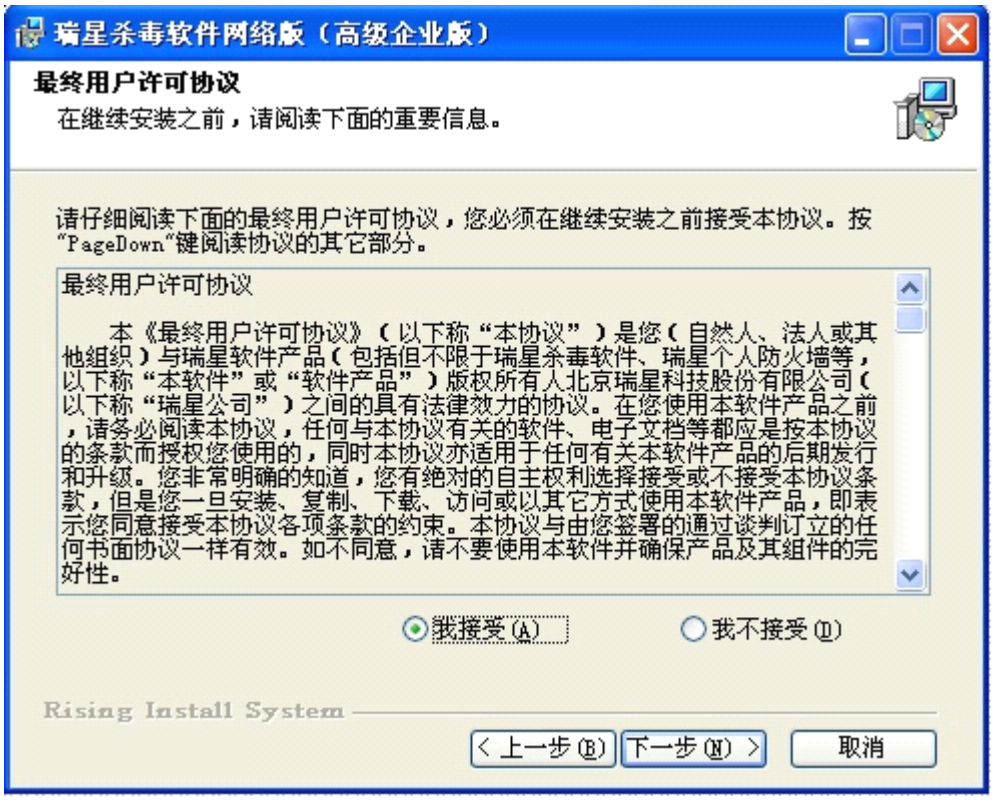

图 326

第四步：进入【定制安装】界面，选择需要安装的【客户端】组件，单击【下一步】继续安装。

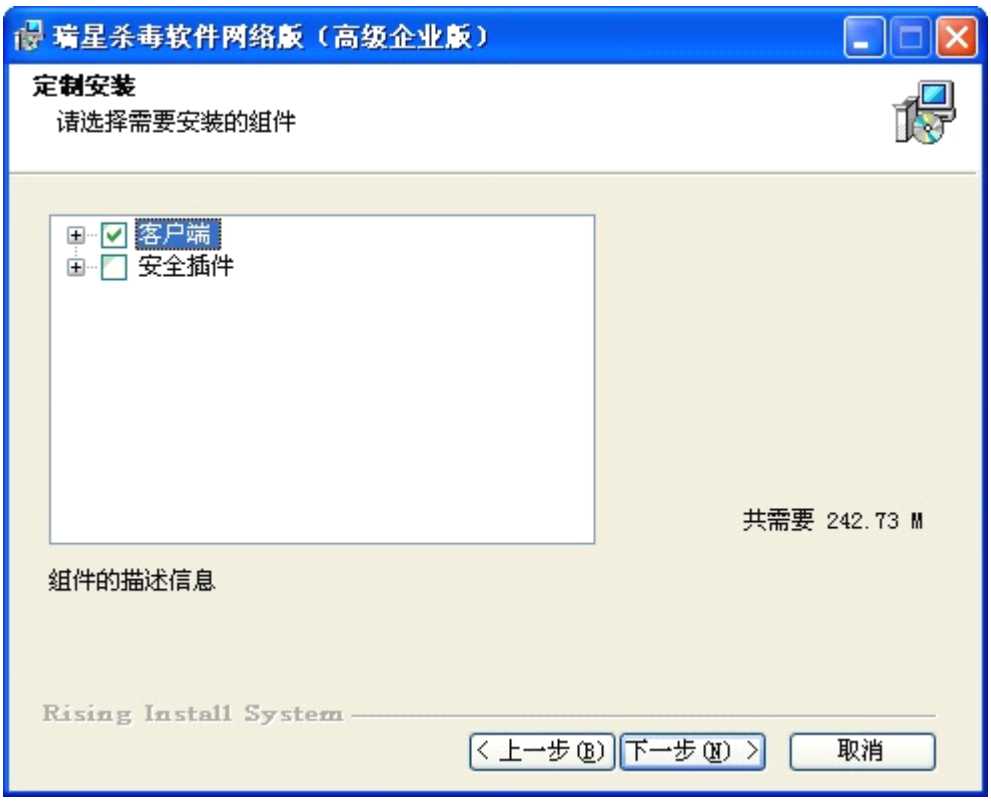

图 327

第五步：进入【网络参数设置】界面，指定系统中心 IP 地址，单击【测试】按钮可以测试客户端与系统中心之间的连通性，单击【下一步】继续安装。

图 328

第六步：在【选择目标文件夹】界面中，选择安装瑞星杀毒软件网络版的目标文件夹，单击【下一步】继续安装。

图 329

第七步：在【选择开始菜单文件夹】界面中，输入用户需要在开始菜单文件夹中创建的程序快捷方式名称，单击【下一步】继续安装。

图 330

第八步：在【安装准备完成】界面中确认安装信息，单击【上一步】可进行修改，单击【下一步】继续安装；若不勾选【安装之前执行内存病毒扫描】，直接进入第十步。

图 331

第九步：安装程序将进行安装前的系统内存查毒，单击【跳过】可直接开始复制文件，建议完成系统内存查毒操作后再开始复制文件，查毒完成后单击【下一步】继续。

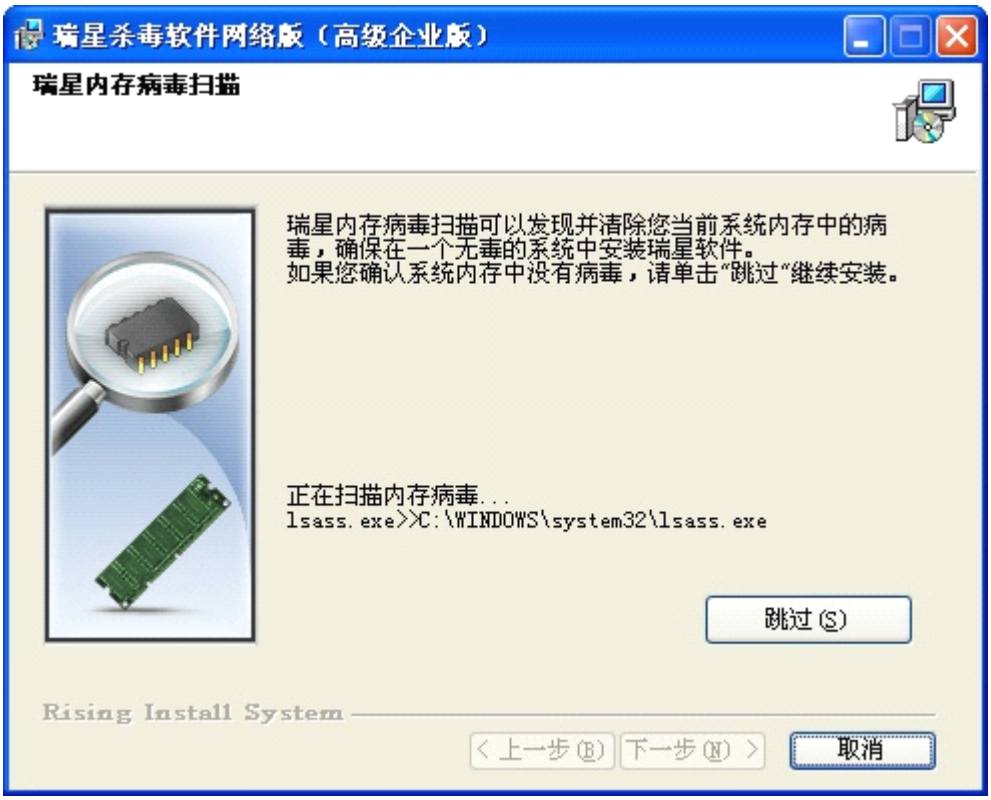

图 332

第十步：文件复制结束后，单击【完成】按钮，建议用户勾选【重新启动计算机】则立刻重新启动计算机完成安装，若用户不勾选此项则软件不能使用，需重新启动计算机后才能正常使用。

图 333

3.2.2 客户端远程安装

说明：在企业专用版和高级企业专用版中，该功能在购买时可以定制；网吧版无此功能；企业版、高级企业版和中小企业版中有此功能。

系统管理员通过管理控制台，给指定的基于 Windows NT WorkStation / Windows NT Server / Windows 2000 Professional / Windows 2000 Server / Windows 2000 Advanced Server / Windows Server 2003 系统的客户端进行远程安装瑞星杀毒软件网络版的操作。

另外，可以在 Windows XP 进行设置，使 Windows XP 操作系统支持远程安装杀毒软件网络版客户端。设置方法：打开【我的电脑】，选择【工具】/【文件夹选项】/【查看】选项页中，不勾选【使用简单共享（推荐）】，如下图。

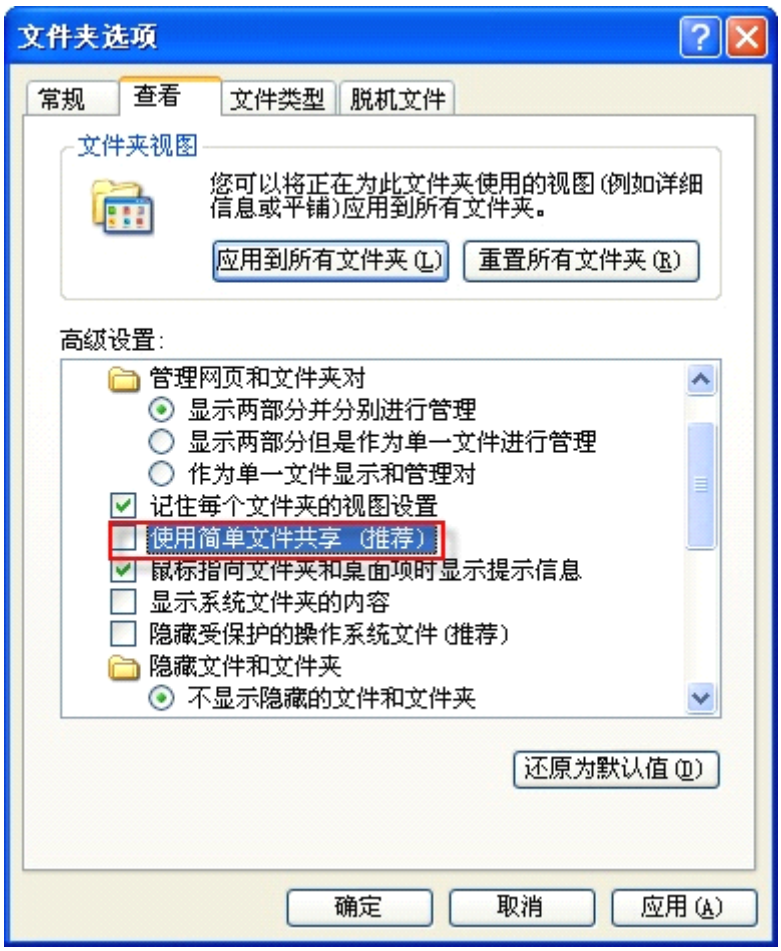

图 334

3.2.2.1客户端远程安装过程

第一步：在管理控制台上，选择【工具】/【NT 客户端安装工具】。

第二步：在【客户端远程安装工具】对话框中，选中将要远程安装瑞星杀毒软件的计算机，或直接输入计算机名或 IP 地址，单击【添加】按钮。用户还可以单击【选择组件】按钮，在弹出的选择组件界面中选择需要为客户端安装的组件。

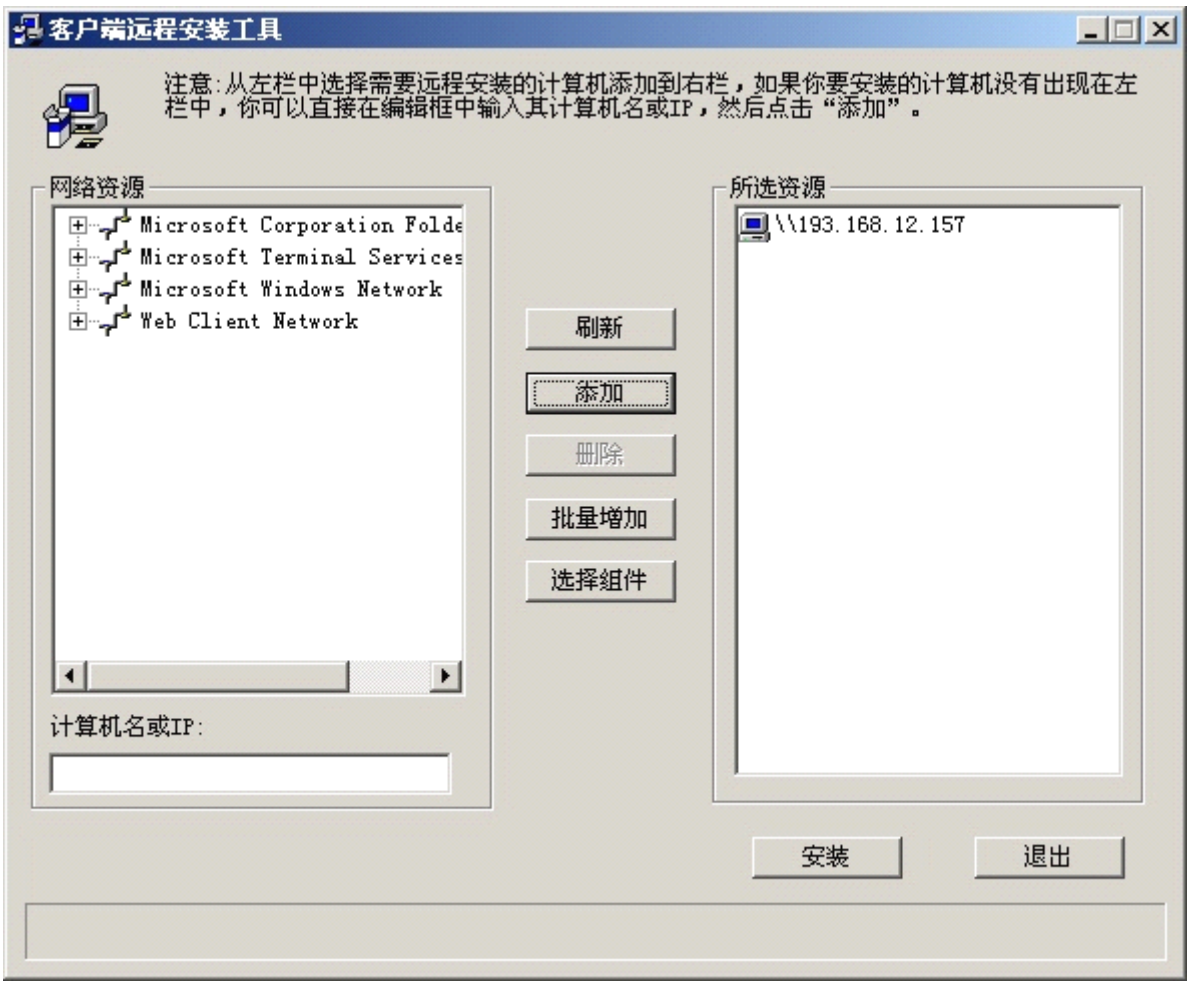

图 335

网络资源中计算机图标识别：

：未在本中心注册或未安装瑞星杀毒软件的计算机；

：在本中心注册但未激活的计算机；

：在本中心注册并已激活的计算机。

注意：用户可以通过网络资源中的图标区分哪些网络中哪些计算机已经安装了瑞星杀毒软件网络版客户端。

第三步：在【登录计算机 XXX】（ XXX 为计算机名或 IP）对话框中，输入目标计算机的本地管理员用户名和密码，单击【确定】。

图 336

第四步：目标计算机添加到【所选资源】框中后，单击【安装】按钮，开始为目标计算机远程安装瑞星杀毒软件，显示安装过程界面。

第五步：显示安装进度，单击【详细信息】按钮则在下方展开安装的详细信息界面。

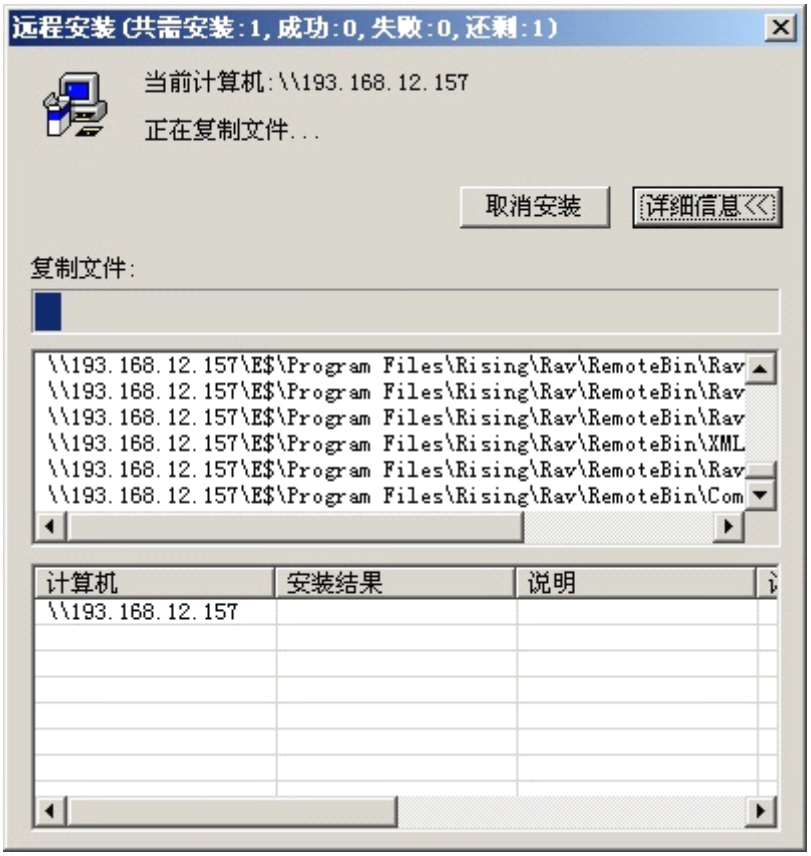

图 337

第六步：安装完成后，在安装状态栏中显示“完成远程安装!”的提示。这时被安装计算机会自动完成后续的安装工作。

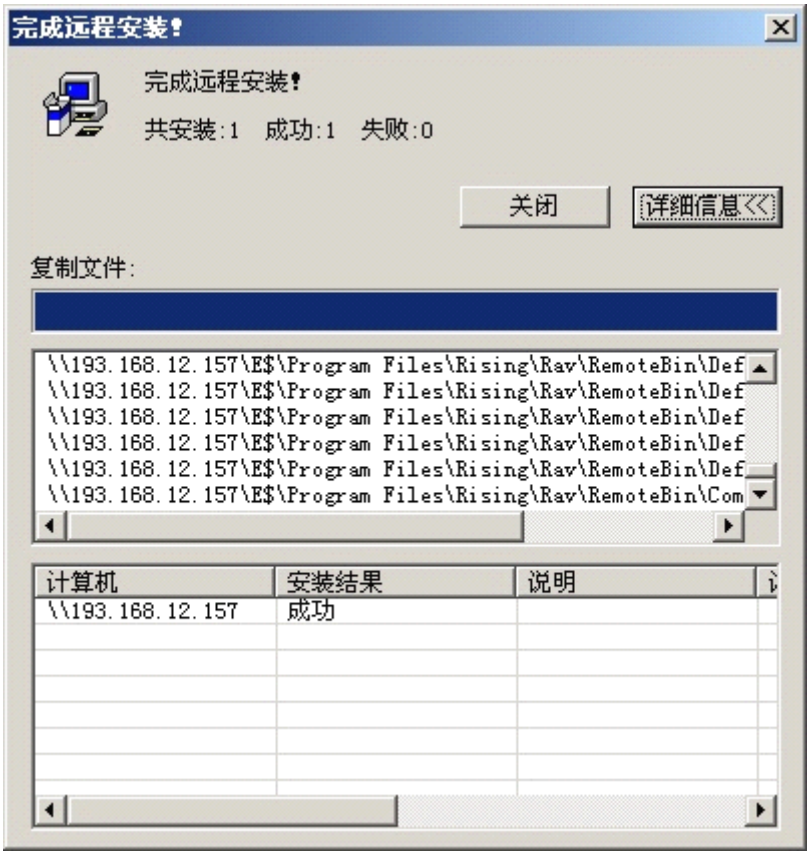

图 338

注意：因操作系统的局限，针对 Windows 9x/Me、Windows Vista 系统的客户端，不能实现对其进行远程安装瑞星杀毒软件的操作。

3.2.3 Web 安装

Web 安装是指用户通过浏览指定位置的网页来实现瑞星杀毒软件网络版的安装。

3.2.3.1Web 安装过程

3.2.3.1.1 搭建环境

第一步：指定网络内的一台计算机提供 Web 安装功能，首先确定这台计算机已经安装了 Internet 信息服务（IIS）组件。

3.2.3.1.2 安装过程

第二步：单击光盘自动运行程序界面上的【网络版 Web 安装】，弹出【瑞星网络安装程序】对话框，指定【目标文件夹】（默认路径是系统盘下的 Inetpub\wwwroot\ravweb），输入瑞星杀毒软件网络版安装程序路径，界面中将自动显示瑞星 Web 安装 URL 地址。单击【安装】按钮开始安装，完成后单击【确定】结束安装。

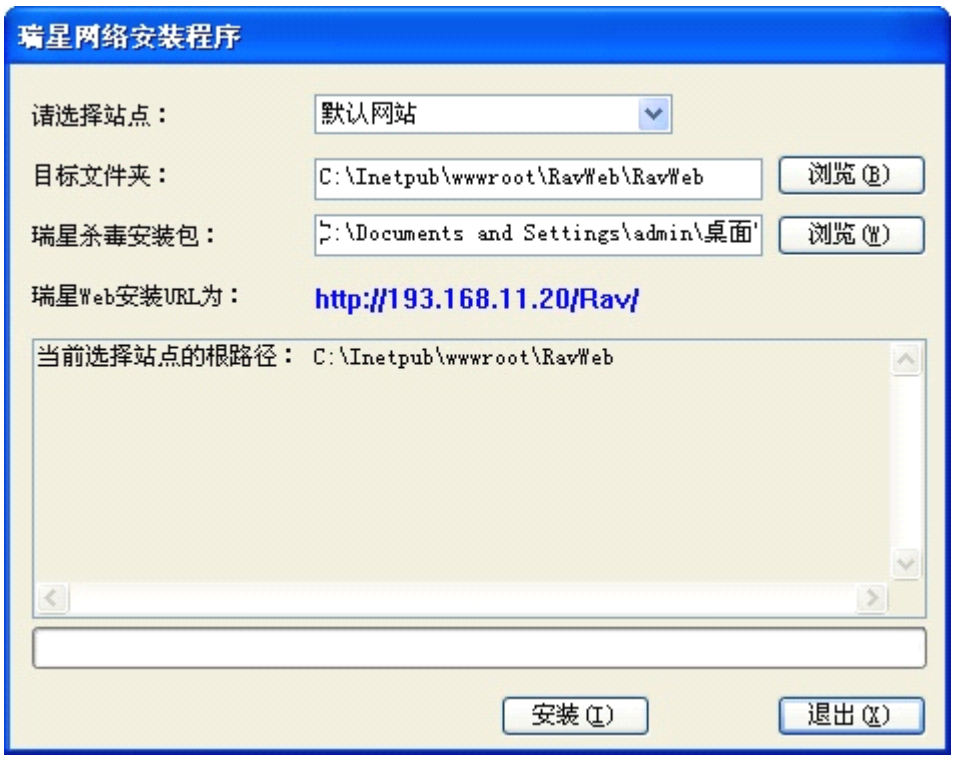

图 339

3.2.3.1.3 客户端安装

第三步：在网络内的任一客户端上打开浏览器，在地址栏中输入提供 Web 安装 URL 地址，显示【瑞星杀毒软件网络版安装程序下载】页面，单击【立即下载】按钮，将安装程序下载至本地进行安装。

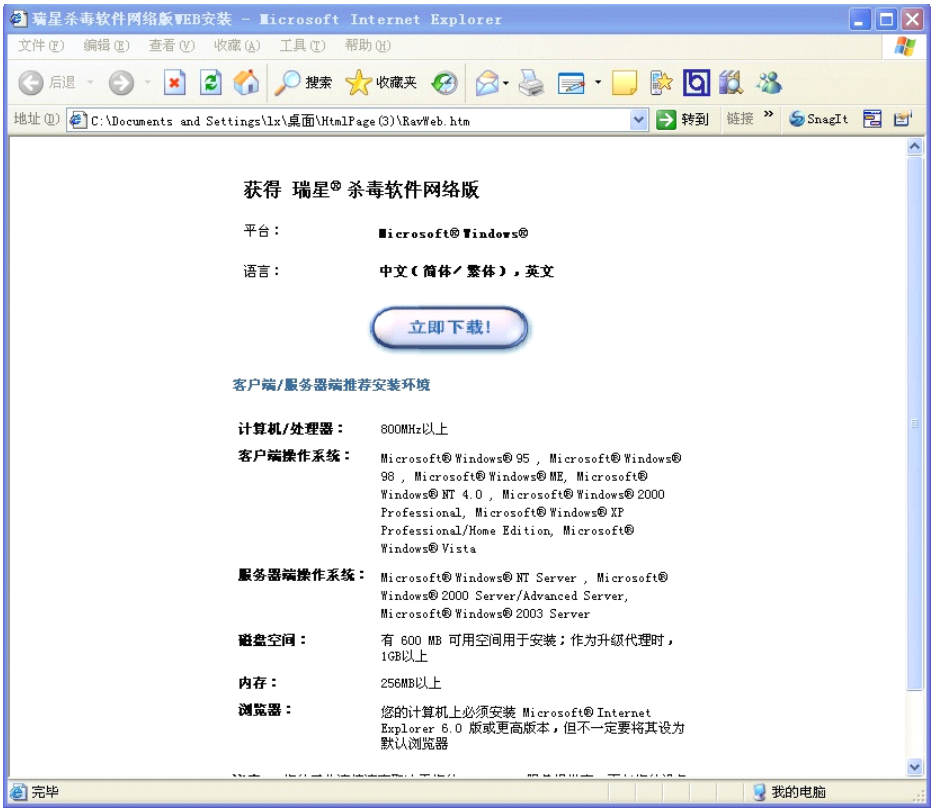

图 340

3.2.4 登录脚本安装

脚本登录安装是实现瑞星杀毒软件网络版快速自动安装的一种方法。瑞星杀毒软件网络版利用域的启动服务概念，在域服务器上配置登录脚本。当用户登录到所在域时，实现自动运行网络版安装程序。

3.2.4.1登录脚本安装过程

第一步：将瑞星杀毒软件网络版光盘放入域控制器所在计算机光驱内，启动瑞星杀毒软件网络版安装主界面后，选择【安装/卸载瑞星杀毒软件网络版的登录脚本】，开始安装。

第二步：程序自动检查本计算机是否为域控制器，如果计算机是域控制器则出现安装界面；否则程序提示“此计算机不是域控制器，不能安装瑞星登录脚本”，程序退出。

添加脚本请选【添加登录脚本】，卸载脚本请选【删除登录脚本】。添加脚本和卸载脚本的以下步骤相同，单击【下一步】继续。

图 341

第三步：在用户列表中单击用户名选择要安装或卸载脚本的用户，也可以通过【用户名】或【姓名】来快速查找用户，单击【下一步】继续。

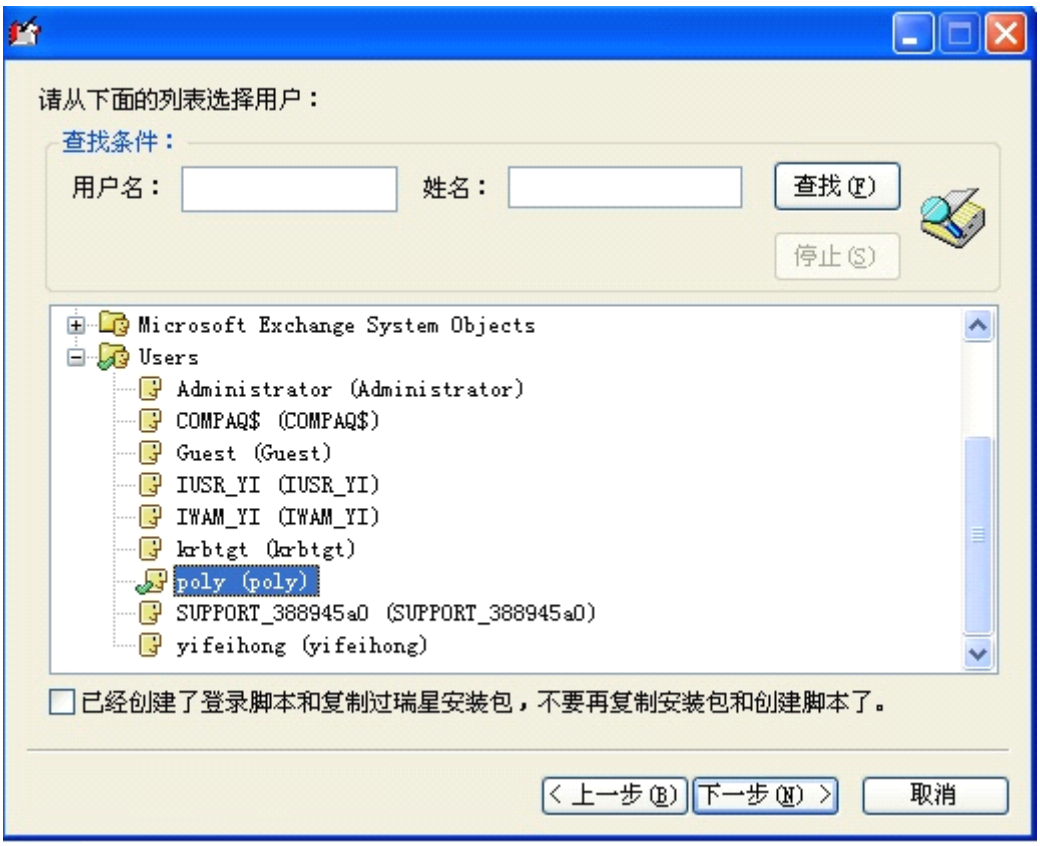

图 342

第四步：输入系统中心 IP 地址，选择瑞星杀毒软件网络版安装程序路径，单击【下一步】继续。

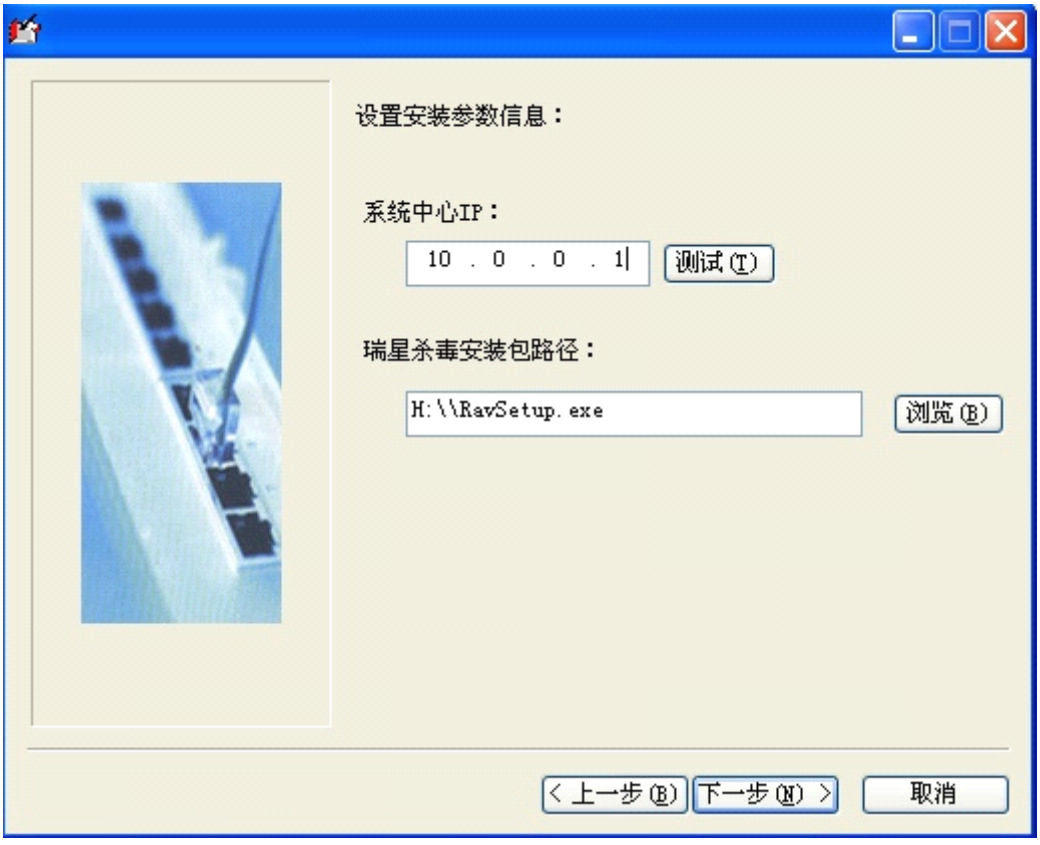

图 343

第五步：单击【完成】结束脚本设置。

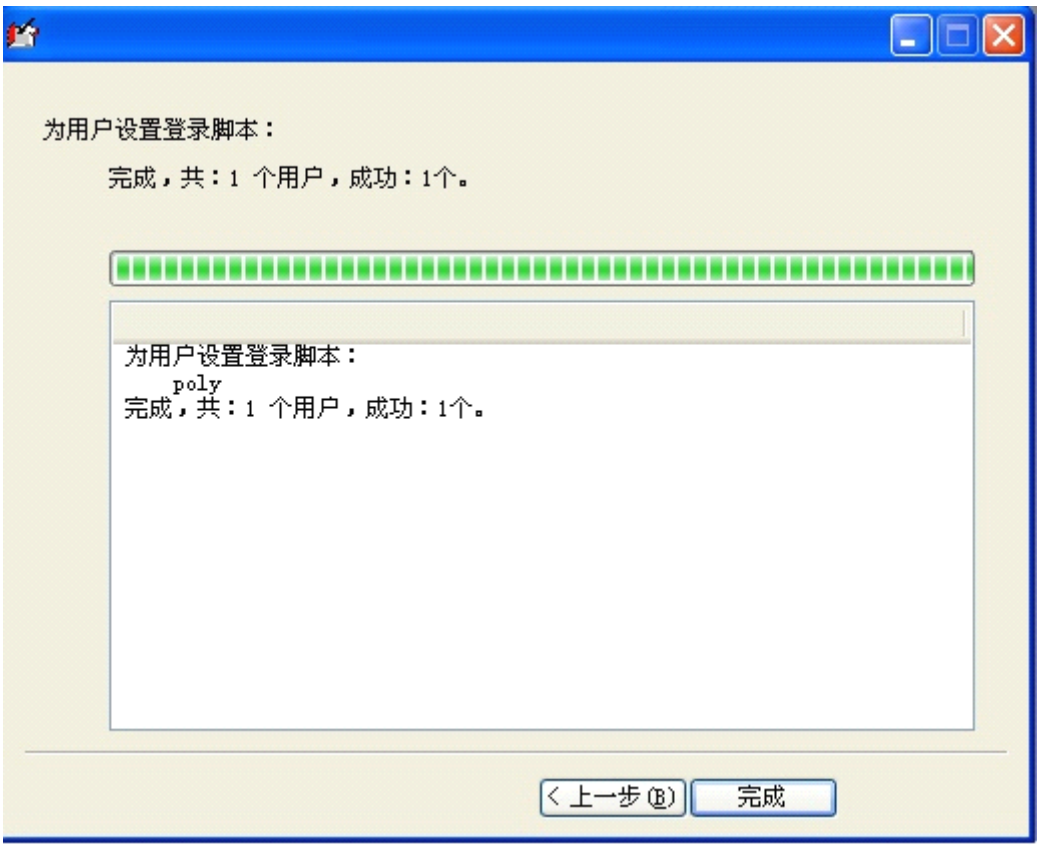

图 344

第六步：客户端使用人员使用域用户登录系统，瑞星杀毒软件网络版的安装脚本自动运行。

脚本登录安装需要被安装客户端的使用人员参与以完成所有的安装步骤，详细步骤请参阅 3.2.1 本地安装。

3.2.5 通过客户端安装包制作工具定制的安装程序安装

第一步：选择【开始】/【程序】/【瑞星杀毒软件】/【瑞星工具】/【客户端安装包打包工具】，则出现定制瑞星客户端安装程序页面，显示瑞星安装路径，单击【下一步】进行制作。

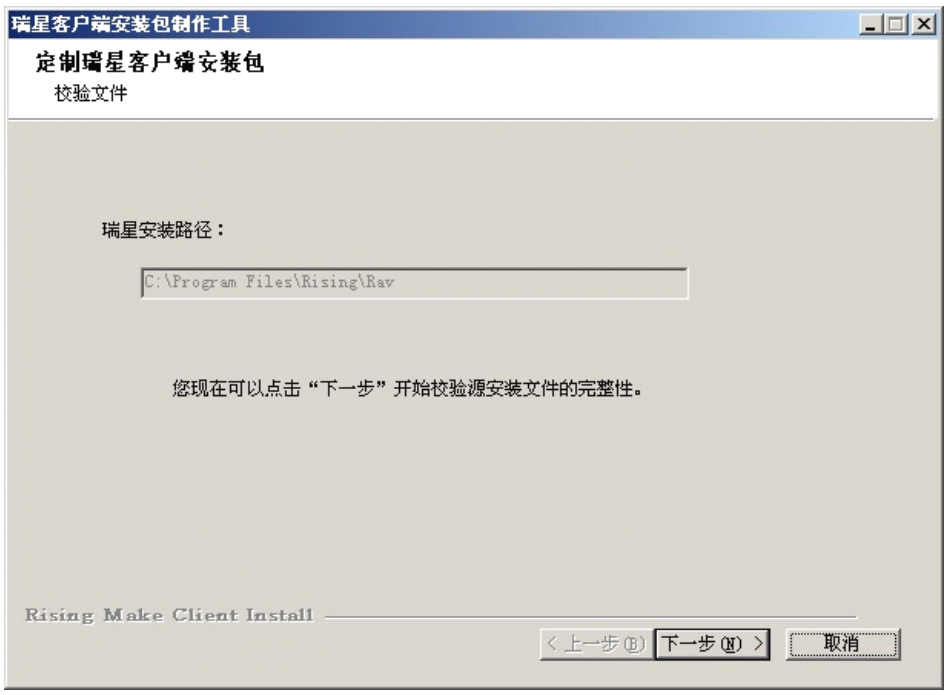

图 345

第二步：在定制瑞星客户端安装程序界面，设置将要制作的安装程序的参数，设置完毕后单击【下一步】进行制作。其中 AgentIP 的地址，用来设置今后用此安装程序进行安装时，指定的系统中心地址；另外有普通安装、自动安装和静默安装三种运行模式。

- 普通安装方式指允许用户设定全部必要的安装参数，安装过程中有全部安装进度界面；
- 自动安装方式指采用安装包定制时设定的安装参数自动安装，不出现这些设定安装参数的界面，只是显示整个安装进度界面；
- 静默安装方式指全部采用安装包定制时设定的安装参数自动安装，在不影响用户正常工作的情况下，在后台静默运行，这种方式下用户将不会看到安装进度。

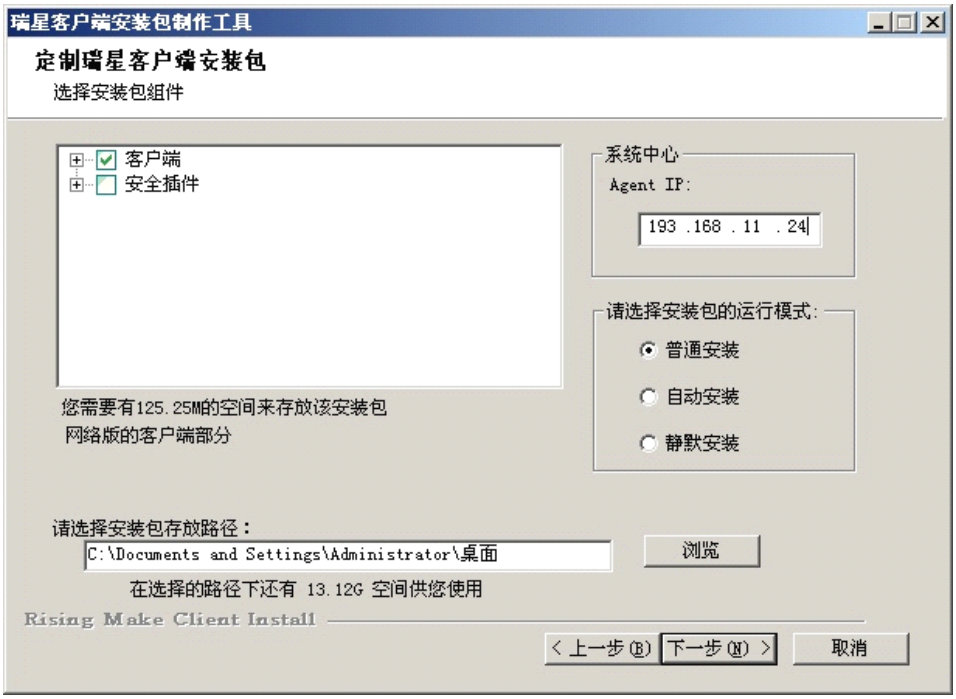

图 346

注意：为了控制客户端安装程序的大小，客户端安装包制作工具将根据选择的组件进行打包，没有选择的组件将不被制作到安装程序里，在客户端安装时，选择组件界面里将不会出现这些组件。

第三步：显示制作进度，拷贝文件。

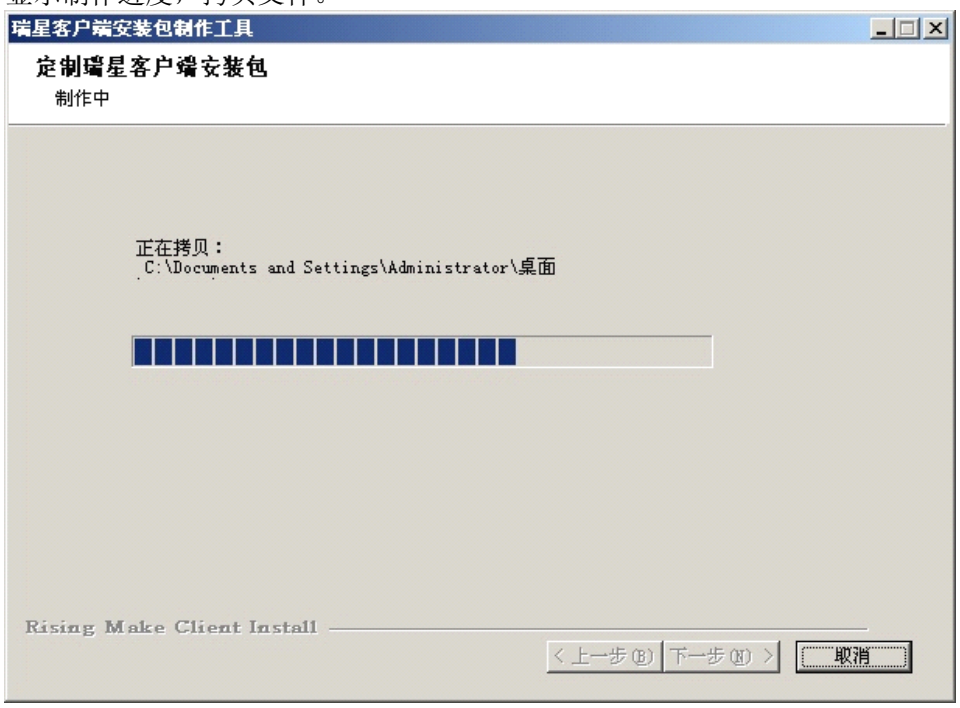

图 347

第四步：显示制作完成信息，单击【完成】按钮结束。

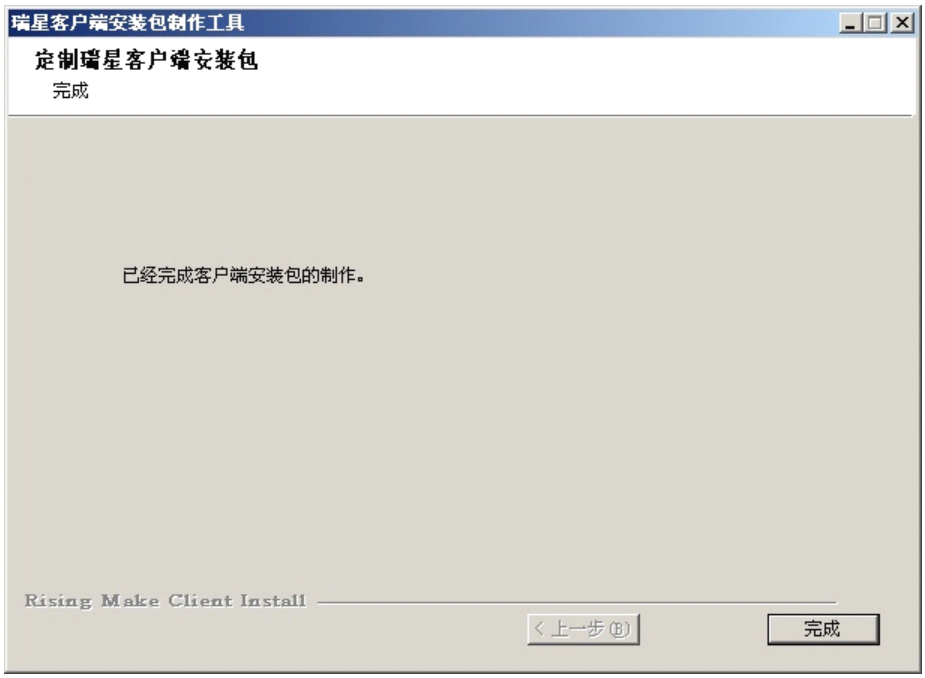

图 348

制作完安装程序后，用户可以利用此安装程序进行客户端杀毒软件的安装。

3.2.6 服务器端和客户端的卸载

方法一：在 Windows 画面中，选择【开始】/【程序】/【瑞星杀毒软件】/【添加删除组件】，在弹出的【瑞星软件维护模式选项】界面中选择【卸载】。

方法二：远程卸载客户端。在管理控制台上的计算机列表栏中，选中准备卸载的客户端，单击【操作 】

/【卸载客户端】，或者在选中的计算机上单击右键，弹出菜单中选择【卸载客户端】开始卸载指定客户端。

注意：卸载完成后建议重新启动计算机，以保证完全卸载。对于安装了移动控制台的客户端，需要卸载控制台后再执行远程卸载。

3.3 控制台的安装与卸载

网络上任何一台计算机的病毒警告信息都能在管理控制台得到汇总，管理员为了灵活控制和管理，可以将管理控制台安装到方便的计算机。控制台的安装和卸载方便了网络管理员随时随地的掌控整个网络的安全情况。

3.3.1 管理控制台的安装

控制台的安装可以有通过光盘安装和通过控制台远程安装两种方式。

方法一：通过光盘安装管理控制台。通过光盘安装管理控制台的操作步骤，用户可以参照系统中心的安装过程，在定制安装界面中勾选管理控制台，其它操作步骤类似。

方法二：远程安装管理控制台，系统管理员可以将管理控制台远程安装在其它计算机上。在计算机列表栏选中将要远程安装管理控制台的计算机，单击【操作】菜单，选择【安装管理控制台】，或在选中的计算机上单击右键，在弹出菜单中选择【安装管理控制台】。

完成远程安装管理控制台后，在计算机列表栏中相应计算机的图标有所变化，表示该计算机已安装控制台。

注意：不要在局域网上安装过多的管理控制台，以保障管理的统一化。

3.3.2 管理控制台的卸载

方法一：在 Windows 画面中，选择【开始】/【程序】/【瑞星杀毒软件】/【添加删除组件】。在弹出的【瑞星软件维护模式选项】界面中选择【添加/删除】，在【定制安装】界面中取消【瑞星管理控制台】的勾选，单击【下一步】开始卸载。

方法二：远程卸载管理控制台。在管理控制台内的计算机列表栏选中将要远程卸载管理控制台的计算机，单击【操作】/【卸载管理控制台】，或在选中的计算机上单击右键，在弹出菜单中选择【卸载管理控制台】。

3.4 多中心的安装

说明：企业版、企业专用版、高级企业版和高级企业专用版中涉及多中心的安装，安装时候请参考本部分内容。

3.4.1 安装前的准备

在安装瑞星杀毒软件网络版多级中心系统之前，需要做的准备工作有：

- 先安装瑞星杀毒软件网络版系统中心；
- 明晰整体网络的隶属关系，分清不同层级的系统中心，以便安装相应的功能模块；
- 保证整体网络的通讯畅通，以便获得相应的通讯端口；
- 瑞星杀毒软件网络版多级中心系统是在多个单系统中心间建立通讯的基础上实现的。上级通讯代

理和下级通讯代理模块是建立多级系统的重要组成部分。这两个模块的安装相互独立，安装时不存在先后顺序之分。

3.4.2 安装环境

对系统资源的要求：

CPU：Intel PIII 800MHz 以上的处理器
内存：512MB 以上内存，最大支持 4GB
显卡：标准 VGA，256 色显示模式以上
硬盘：400MB 以上可用硬盘空间

对操作系统的支持：

服务器系统：

Windows NT 4.0 Server
Windows 2000 Server
Windows 2000 Advanced Server
Windows Server 2003

客户端系统：

Windows 95/98/Me
Windows NT 4.0 Workstation
Windows 2000 Professional
Windows XP Home Edition
Windows XP Professional
Windows Vista

对通信协议的要求：

TCP/IP

3.4.3 关于上级通讯代理和下级通讯代理设置的特别说明

在以下的上级通讯代理和下级通讯代理的安装过程中，用户需要对上级通讯代理和下级通讯代理的监听端口进行设置。

在【上级通讯代理】和【下级通讯代理】画面中，上级通讯代理的【指向的 RavSender 端口】和下级通讯代理的【监听端口】是两两对应的。只有保证两两对应的关系，才能保证正常通讯。

3.4.4 上级通讯代理的安装

上级通讯代理的功能是用于建立与对应的远程上级中心的通讯，并接收上级中心发布的命令，同时发送下级中心的数据给上级中心。

3.4.4.1上级通讯代理的安装条件

安装上级通讯代理的计算机必须与安装对应的下级通讯代理的计算机保持双向网络通讯状态（支持 TCP/IP 协议）。

建议把上级通讯代理安装在系统中心所在的计算机上。

全天候开机：为确保正常实现多级中心通讯和管理，安装上级通讯代理的计算机应该在有效工作期内保持全天候的开机状态。

3.4.4.2上级通讯代理的安装过程

首先确定瑞星杀毒软件网络版已经安装，再进行以下安装步骤：

第一步：将瑞星杀毒软件网络版安装光盘放入光驱内。

第二步：单击【安装瑞星杀毒软件网络版】进入安装程序界面，选择【安装多中心组件】。

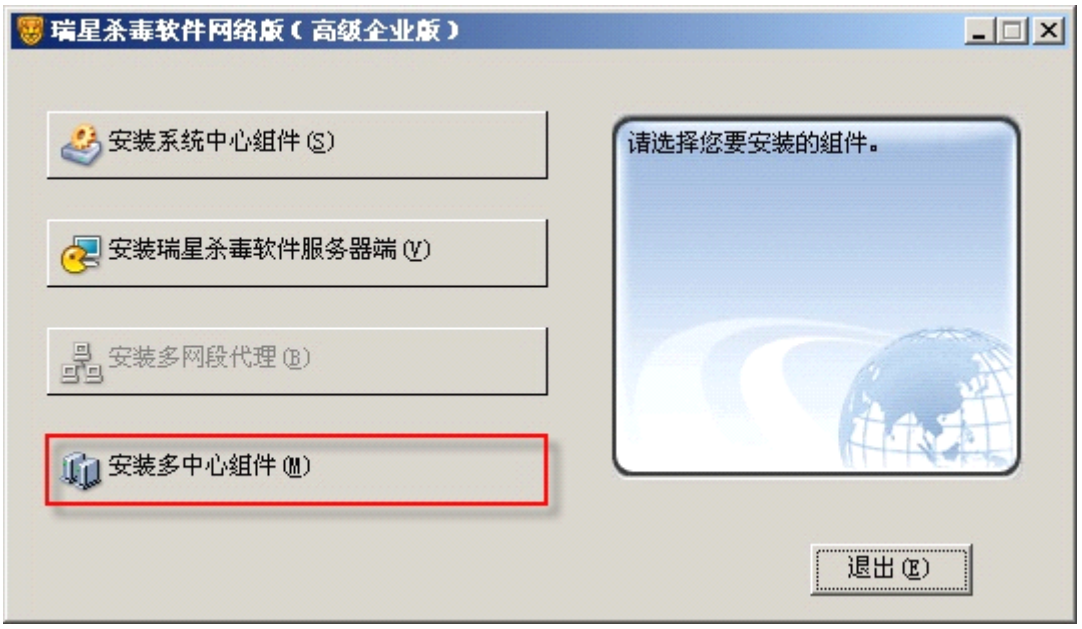

图 349

第三步：在【定制安装】画面中，选择【上级通讯代理】，单击【下一步】继续安装。

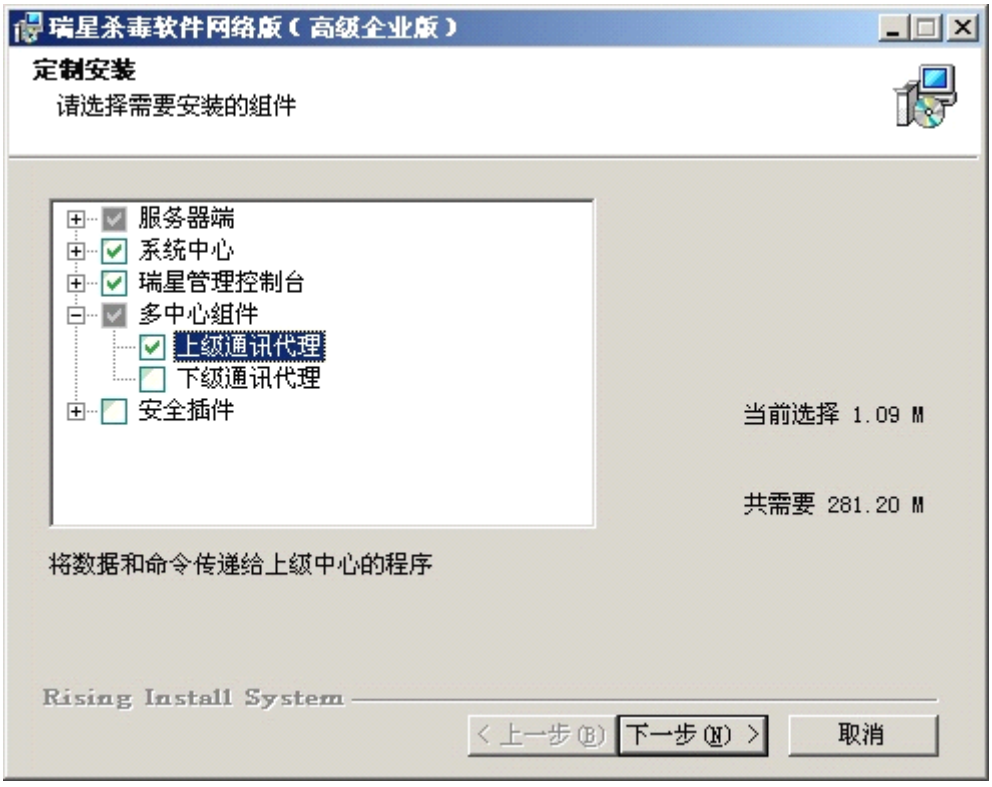

图 350

第四步：在【网络参数设置】界面中，填写上级通讯代理的监听端口、指向的 RavSender IP 和指向的

RavSender 端口，单击【下一步】继续安装。

图 351

注意：

1. 上级通讯代理【指向的 RavSender 端口】的配置必须与已安装相对应的下级通讯代理的【监听端口】配置保持一致。如果在安装上级通讯代理时与之相对应的下级通讯代理没有安装，则用户可以自行设定上级通讯代理的【指向的 RavSender 端口】；如果在安装上级通讯代理时与之相对应的下级通讯代理已经安装了，则上级通讯代理的【指向的 RavSender 端口】必须与相对应的下级通讯代理的【监听端口】保持一致。
2. 在配置上级通讯代理的【监听端口】时，要求用户设定的值在 1024～65535 之间。

第五步：文件复制结束后，单击【完成】按钮结束安装。

图 352

3.4.5 下级通讯代理的安装

下级通讯代理的功能是发送命令给下级中心，同时接收下级中心传送的数据。

安装下级通讯代理时必须保证已经安装了瑞星杀毒软件网络版。安装下级通讯代理的计算机不必限于系统中心所在计算机，可以安装在该网段任何一个客户端上。

3.4.5.1下级通讯代理的安装条件

安装下级通讯代理的计算机必须与安装对应的上级通讯代理的计算机保持双向网络通讯状态（支持 TCP/IP 协议）。

全天候开机：为确保正常实现多级中心通讯和管理，安装下级通讯代理的计算机应该在有效工作期内保持全天候的开机状态。

建议把下级通讯代理安装在系统中心所在的计算机上。

3.4.5.2下级通讯代理的安装过程

首先确定瑞星杀毒软件网络版已经安装，再进行以下安装步骤：

第一步：将瑞星杀毒软件网络版安装光盘放入光驱内。

第二步：单击【安装瑞星杀毒软件网络版】进入安装程序界面，选择【安装多中心组件】。

第三步：在【定制安装】画面中，选择【下级通讯代理】，单击【下一步】继续安装。

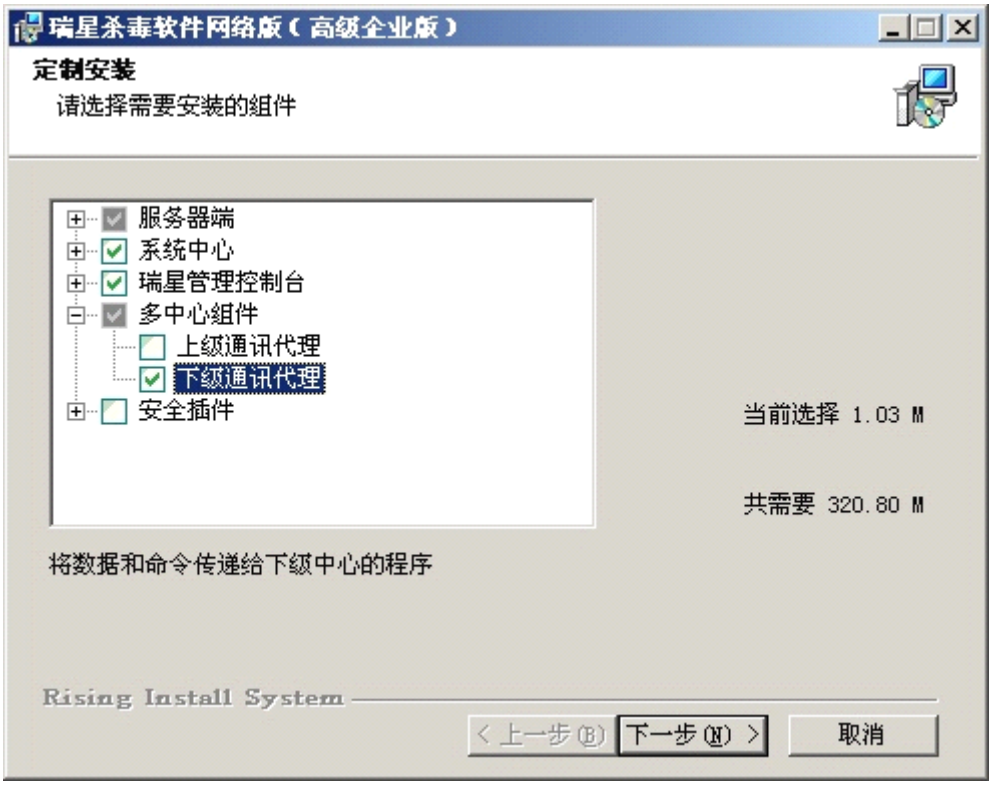

图 353

第四步：在【网络参数设置】画面中，输入下级通讯代理的监听端口，单击【下一步】继续安装。

图 354

注意：

1. 下级通讯代理【监听端口】的配置必须与已安装相对应的上级通讯代理的【指向的 RavSender 端口】配置保持一致。如果在安装下级通讯代理时与之相对应的上级通讯代理没有安装，则用户可

以自行设定下级通讯代理的【监听端口】；如果在安装下级通讯代理时与之相对应的上级通讯代理已经安装了，则下级通讯代理的【监听端口】必须与相对应的上级通讯代理的【指向的 RavSender 端口】保持一致。

2. 在配置下级通讯代理的【监听端口】时，要求用户设定的值在 1024～65535 之间。

第五步：在【安装准备完成】界面中，确认安装信息，单击【下一步】继续安装。

第六步：文件复制结束后，单击【完成】按钮结束安装。

3.4.6 远程安装上下级通讯代理

系统管理员可以通过管理控制台远程安装上下级通讯代理。

3.4.6.1上级通讯代理的远程安装

第一步：在管理控制台上，选择【管理】/【通讯代理管理】/【Receiver（上级通讯代理）设置】，进入上级通讯代理设置页面。

第二步：输入准备安装上级通讯代理的主机 IP 地址、端口及指向的下级通讯代理 IP 地址、端口。单击【安装】按钮开始安装。

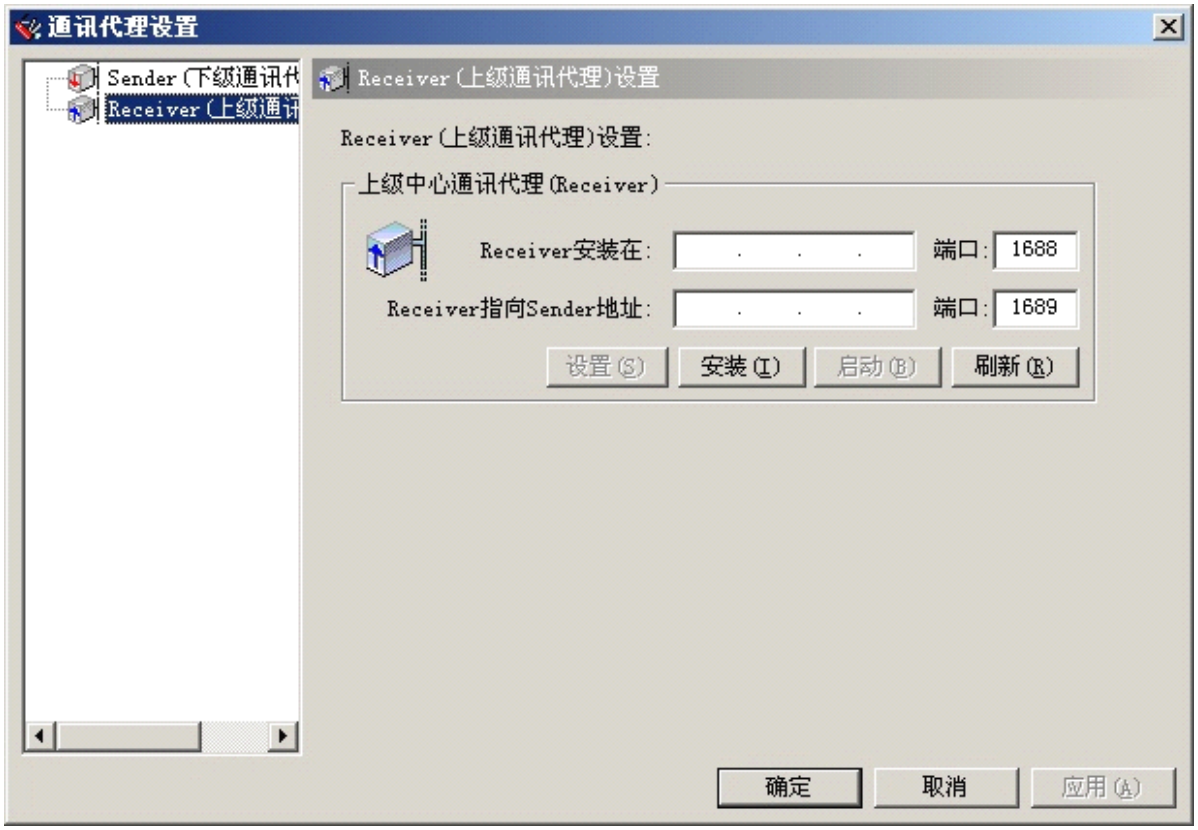

图 355

3.4.6.2下级通讯代理的远程安装

第一步：在管理控制台上，选择【管理】/【通讯代理管理】/【Sender（下级通讯代理）设置】，进入

下级通讯代理设置页面。

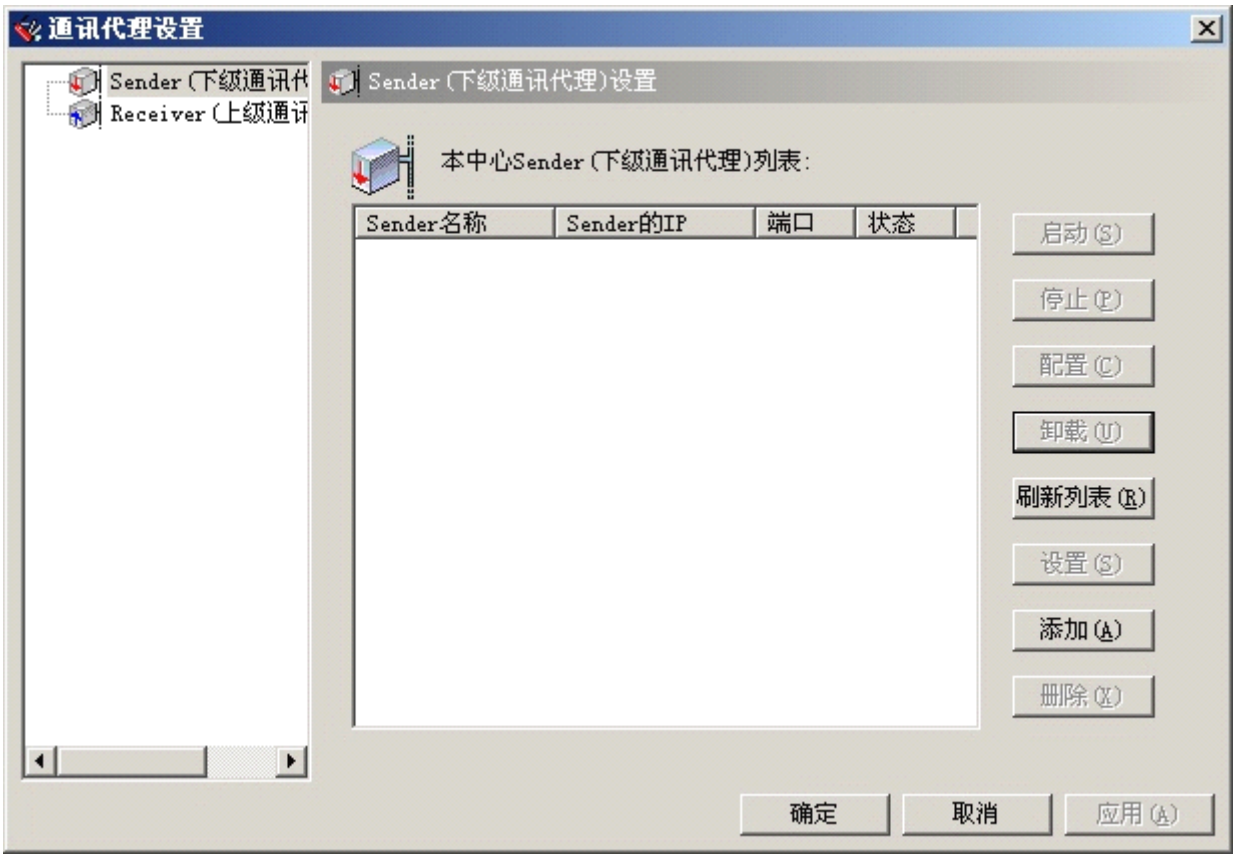

图 356

第二步：【Sender（下级通讯代理）设置】页面，单击【添加】按钮弹出 Sender 设置页面，输入 Sender 名称、所在主机 IP 地址和监听端口。

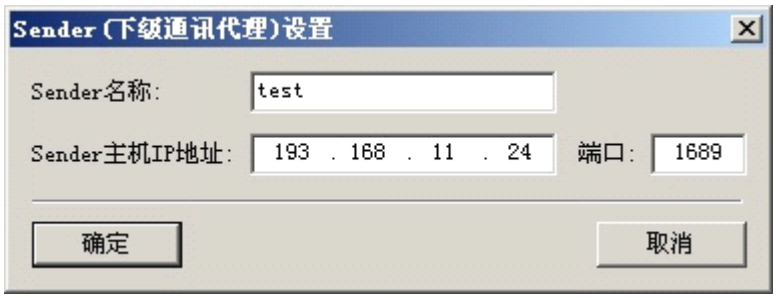

图 357

第三步：在本中心 Sender 列表中显示添加成功的 Sender（下级通讯代理），可以启动、停止或设置该 Sender（下级通讯代理）。

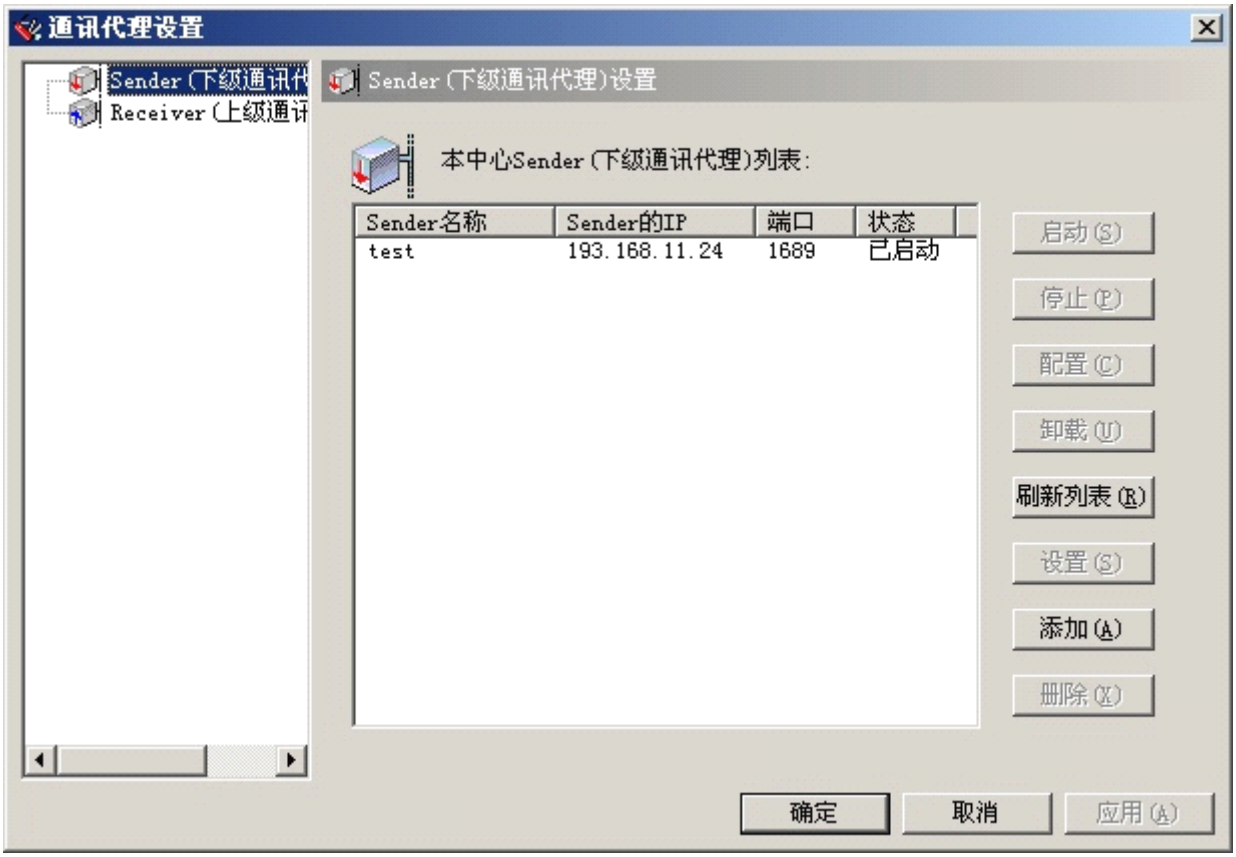

图 358

3.5 多网段代理的安装与卸载

多网段代理协助客户端在多网段间寻找系统中心，与其进行连接。

3.5.1 多网段代理的安装

第一步：将瑞星杀毒软件网络版光盘放入光驱内，启动瑞星杀毒软件网络版安装主界面后，选择【安装多网段代理】按钮开始安装。

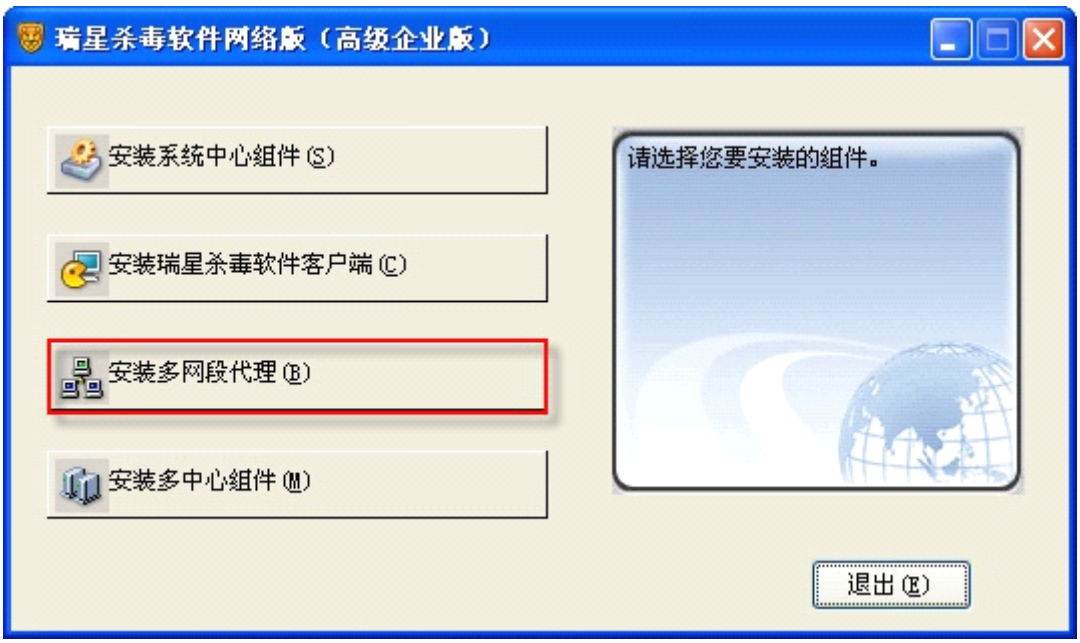

图 359

第二步：在【定制安装】页面中勾选【多网段工具】（即多网段代理），单击【下一步】继续安装。

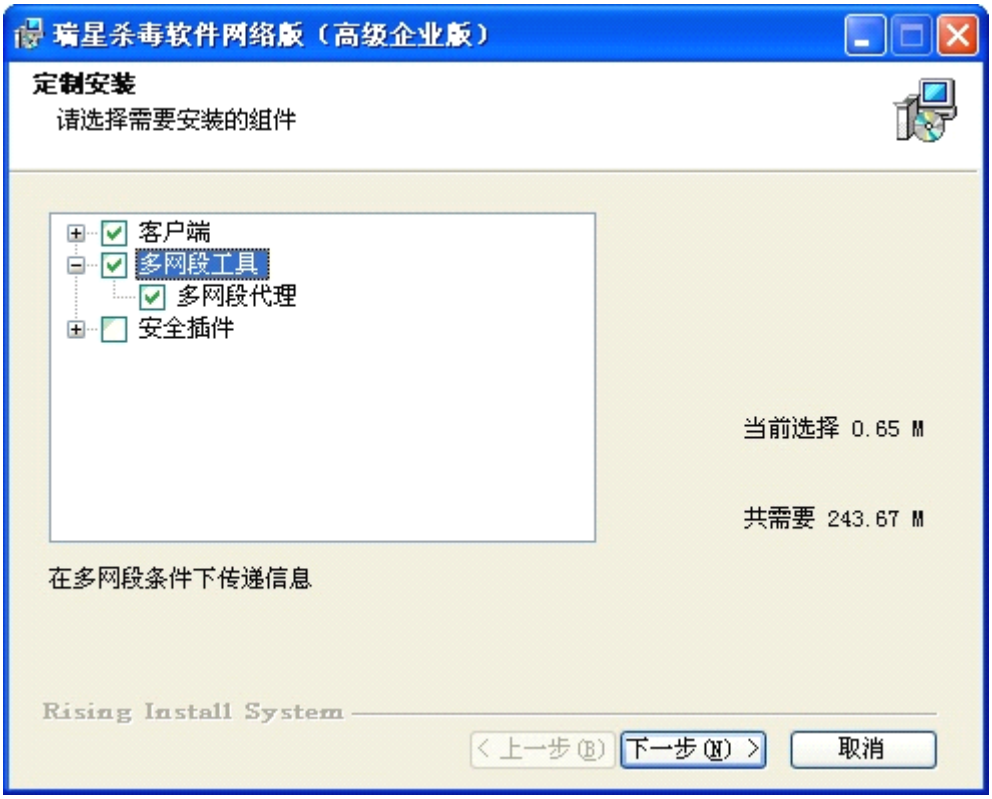

图 360

第三步：进入【安装准备完成】页面，单击【下一步】继续。

图 361

第四步：安装完成后，单击【完成】按钮结束安装。

图 362

3.5.2 多网段代理的卸载

在 Windows 画面中，选择【开始】/【程序】/【瑞星杀毒软件】/【添加删除组件】。在弹出的【瑞星软件维护模式选项】界面中选择【添加/删除】，在【定制安装】界面中取消【多网段代理】的勾选，单击【下一步】进行卸载。

3.6 附表

附表一：系统中心、服务器端和客户端所支持的操作系统

操作系统	系统中心	服务器端	客户端
Windows 95	网吧版支持		√
Windows 98	网吧版支持		√
Windows Me	网吧版支持		√
Windows NT WorkStation	网吧版支持		√
Windows NT Server	√	√	
Windows 2000 Professional	网吧版支持		√
Windows 2000 Server	√	√	
Windows 2000 Advanced Server	√	√	
Windows XP Home Edition	网吧版支持		√
Windows XP Professional	网吧版支持		√
Windows Server 2003	√	√	
Windows Vista			√

附表二：

操作系统		本地安装	脚本安装	远程安装	Web 安装
客户端	Windows 95	√	√		√
	Windows 98	√	√		√
	Windows Me	√	√		√
	Windows NT WorkStation	√	√	√	√
	Windows 2000 Professional	√	√	√	√
	Windows XP Home Edition	√			√
	Windows XP Professional	√	√		√
	Windows Vista	√			√
服务器端	Windows NT Server	√	√	√	√
	Windows 2000 Server	√	√	√	√
	Windows 2000 Advanced Server	√	√	√	√

	Windows Server 2003	√	√	√	√

4 安全管理

安全管理功能使得网络管理员能够对网络中的所有计算机进行统一配置、管理以及监测网络安全状况，从而保障整个网络的安全。

4.1 管理功能

管理功能是对整个网络中的计算机进行安全管理，涉及到监测网络安全状况、策略设置管理（杀毒策略、监控策略和主动防御策略等）、升级管理以及日志管理等。

4.1.1 管理控制台

管理控制台是在网络上集中管理所有安装有瑞星杀毒软件网络版客户端软件的计算机的管理工具。通过管理控制台可以了解整个网络中的总体安全状况并且远程管理网络中的任何一台计算机中的瑞星杀毒软件。网络上任何一台计算机的病毒警告信息都能在管理控制台得到汇总，通过管理控制台也能直观地查看网络上所有计算机当前的实时监控状态、病毒查杀情况、主动防御状态和当前版本信息等。管理控制台能对远程计算机安装瑞星杀毒软件和移动管理控制台，让管理控制台自由移动到管理员认为合适的计算机上去。管理员通过对管理控制台的操作就能对网络上所有计算机进行定期、实时地查杀病毒和全网统一升级管理，真正做到在整个网络中建立起坚实的网络病毒防护系统。

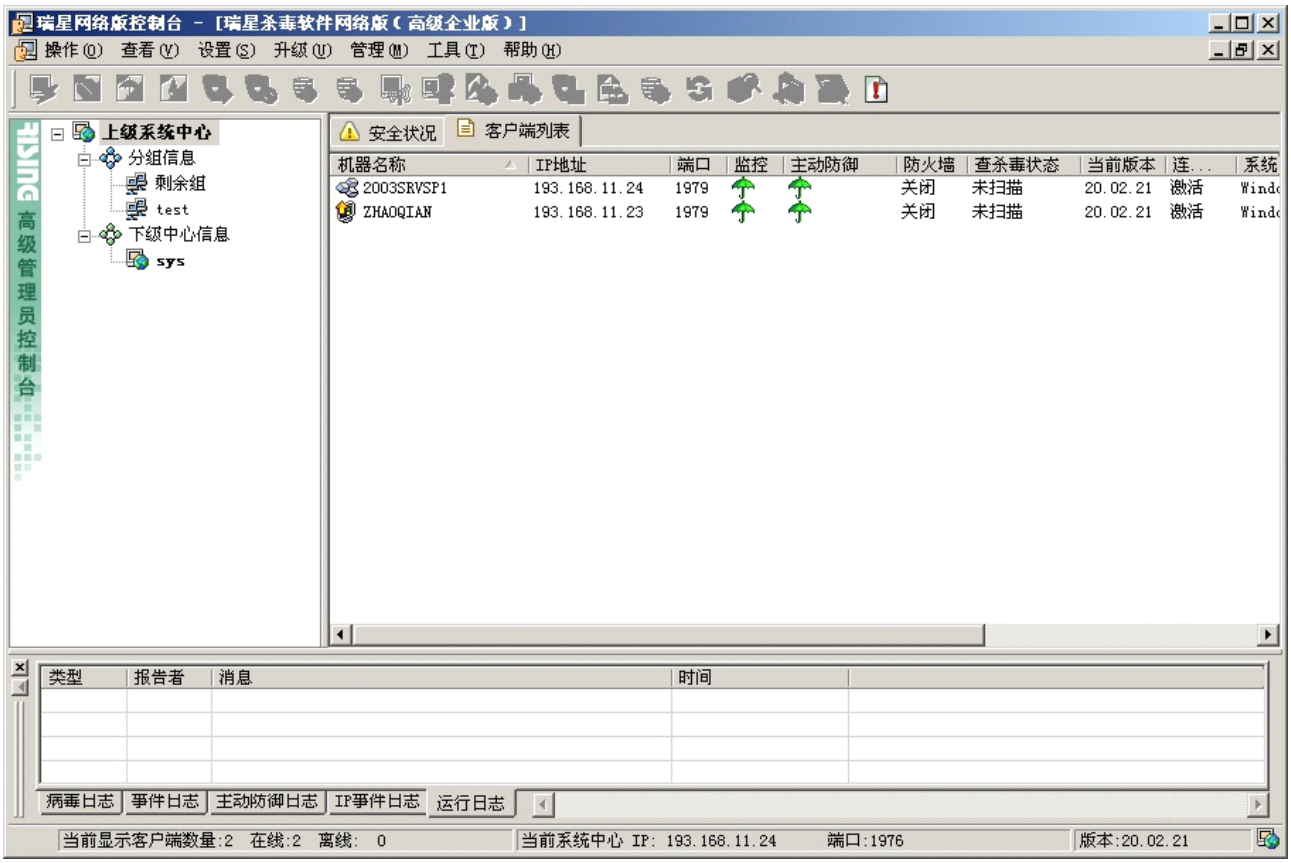

图 41

4.1.1.1管理控制台的启动

依次选择【开始】/【程序】/【瑞星杀毒软件】/【管理控制台】，或者双击桌面【管理控制台】图标，进入登录界面。

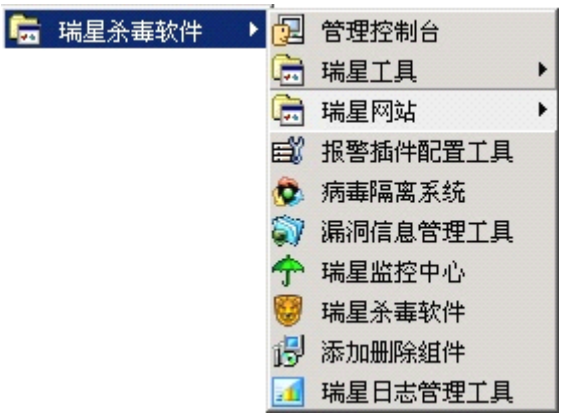

图 42

在【管理员登录】界面中，输入帐号和口令后（默认用户名称为 admin、密码为空），单击【登录】进入管理控制台界面。

图 43

4.1.1.2管理控制台界面说明

管理控制台界面包括六个部分：菜单、组管理界面、安全状况、客户端列表、日志栏和状态栏。

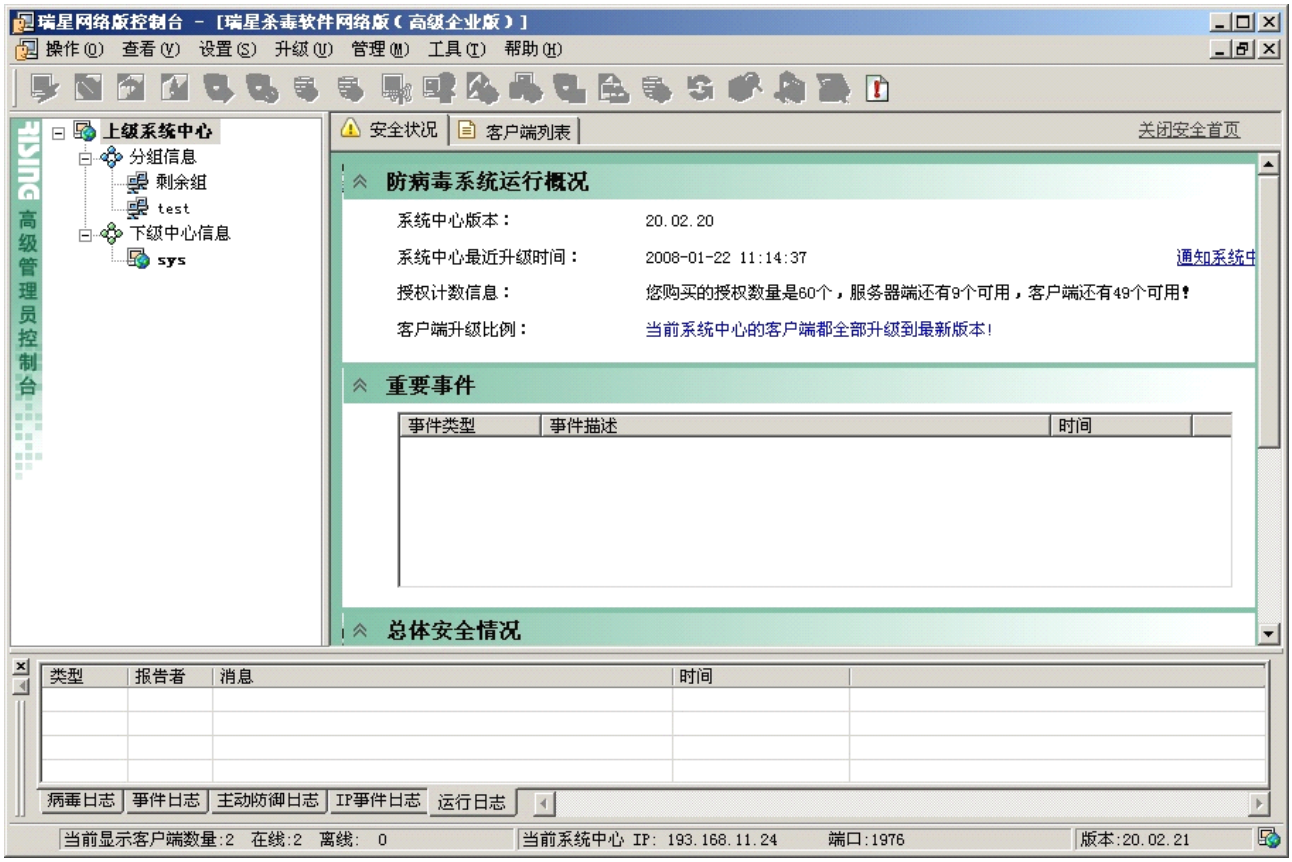

图 44

菜单：操作、查看、设置、升级、管理、工具、帮助

组管理界面：系统中心名称和分组信息（分组信息中默认组为“剩余组”）

安全状况：显示整个网络安全情况

客户端列表：列出所有客户端及其状态

日志栏：包括病毒日志、事件日志、主动防御日志、IP 事件日志和运行日志

说明：其中 IP 事件日志在高级企业版中会显示；在高级企业专用版中，购买时定制了防火墙功能的情况下会显示；网吧版、中小企业版、企业版和企业专用版中无此项功能

状态栏：当前显示客户端数量、当前系统中心、端口和版本

组管理界面图标识别

	系统中心
	分组信息
	组信息
	下级中心分组信息

客户端列表图标识别

	系统中心
	已激活的客户端
	未激活的客户端
	安装有管理控制台的已激活客户端
	安装有管理控制台的未激活客户端
	已激活的 Unix 客户端
	未激活的 Unix 客户端
	已激活的安装有多网段代理的客户端
	未激活的安装有多网段代理的客户端
	启用升级代理的客户端
	启用升级代理且安装有管理控制台的客户端
	启用升级代理的系统中心

4.1.1.2.1 菜单说明

用户通过菜单管理应用管理控制台中各个功能。

说明：仅在高级企业版中在工具栏中显示关于防火墙的开启、关闭和规则设置图标；高级企业专用版购买时定制了防火墙功能的情况下显示相关图标；网吧版、中小企业版、企业版和企业专用版中不显示图标。

图 45

4.1.1.2.1.1【操作】菜单

管理员进行管理控制台的操作选项。

图 46

以下是对各个选项的具体说明：

【全网查杀】：选择此项则对所有计算机进行远程查杀病毒。如果此时某些计算机处于离线状态，则这些计算机在开机后将自动查杀病毒（网吧版无此菜单项）

【查杀病毒】：对选中的一台或多台处于激活状况的计算机进行远程查杀病毒（网吧版无此菜单项）

【停止查杀】：停止查杀病毒操作 （网吧版无此菜单项）

【扫描漏洞】：对选中的计算机进行漏洞扫描，可以设置“最高”、“中级以上”、“低级以上”和“全部”四个漏洞严重级别进行扫描

【打开实时监控】：对选中的计算机启动实时监控，可以选择所有监控或指定监控

【关闭实时监控】：对选中的计算机关闭实时监控，可以选择所有监控或指定监控

【打开主动防御】：对选中的计算机启动主动防御，可以选择所有主动防御或指定防御功能

【关闭主动防御】：对选中的计算机关闭主动防御，可以选择所有主动防御或指定防御功能

【开启自我保护】：对选中的计算机启动自我保护功能

【关闭自我保护】：对选中的计算机关闭自我保护功能

【开启防火墙】：对选中的计算机启动防火墙功能

说明：在高级企业版有此菜单；高级企业专用版中，在购买时定制了防火墙功能的情况下，显示此菜单；网吧版、中小企业版、企业版、企业专用版中无此菜单。

【关闭防火墙】：对选中的计算机关闭防火墙功能

说明：在高级企业版有此菜单；高级企业专用版中，在购买时定制了防火墙功能的情况下，显示此菜单；网吧版、中小企业版、企业版、企业专用版中不显示此菜单。

【发送广播消息】：对选中的计算机发送广播消息

【设置防毒策略】：对选中的计算机设置防毒策略，其中当组策略不存在时，有“缺省配置”和“导入设置策略”两种方式，用户可根据需要选择。具体防毒策略选项包括：实时监控设置、嵌入式杀毒、手动查杀、快捷方式查杀、定制任务、硬盘备份和其它设置等

【设置客户端选项】：对选中的计算机进行选项设置，其中当组策略不存在时，有“缺省配置”和“导入设置策略”两种方式，用户可根据需要选择。具体客户端选项包括“基本设置"、“日志上报设置"、“定时升级设置"、“下载中心设置"、“漏洞扫描设置"、“升级代理设置”和“其它设置”等

【设置主动防御规则】：对选中的计算机进行主动防御策略设置，其中当组策略不存在时，有“缺省配置"和“导入设置策略”两种方式，用户可根据需要选择。主动防御设置选项包括：“主动防御设置"、“系统加固"、“应用程序访问控制"、“应用程序保护"、“程序启动控制"、“恶意行为检测"、“隐藏进程检测”等

【设置防火墙规则】：对选中的计算机进行防火墙策略设置，可以设置防火墙的 IP 规则和是否客户端开机启用防火墙功能。

说明：在高级企业版显示此菜单；高级企业专用版中，在购买时定制了防火墙功能的情况下，显示此菜单；网吧版、中小企业版、企业版、企业专用版中不显示此菜单。

【系统中心设置】：对选中的系统中心进行设置，其中设置内容为：“系统中心设置"、“网络设置"、“升级设置"、“黑白名单设置"、“漏洞扫描设置”和“对象端口设置”等

【查看日志】：查看病毒日志、事件日志、主动防御日志和防火墙事件日志

说明：在高级企业版显示防火墙事件日志菜单；高级企业专用版中，在购买时定制了防火墙功能的情况下，显示此菜单；网吧版、中小企业版、企业版、企业专用版中不显示此菜单。

【查看客户端诊断信息】：查看选中的客户端的诊断信息，其中信息内容包括：“加载当前进程列表"、“加载系统启动项"、“加载已安装软件列表"、“加载 IE 资源插件"、“加载 IE 工具条”和“加载文件关联项"等

【加入黑名单】：将选中的计算机加入黑名单列表，黑名单中的计算机不能在系统中心注册，除非此计算机从黑名单中删除

【卸载客户端】：远程卸载选中客户端的瑞星杀毒软件网络版

【远程修复】：远程修复选中客户端的瑞星杀毒软件网络版

【安装管理控制台】：对选中的计算机远程安装管理控制台

【卸载管理控制台】：对选中的计算机远程卸载管理控制台

【安装补丁程序】：通知客户端安装漏洞补丁程序

【修复不安全设置】：修复选中客户端的不安全设置

【开启客户端作为升级代理】：将选中计算机设置为客户端升级代理

【关闭客户端作为升级代理】：取消选中计算机的客户端升级代理功能

【导出客户端信息】：导出客户端信息保存为*.csv 文件

【刷新】：刷新选中计算机或系统中心的最新状态

【属性】：查看选中计算机的属性，包括“机器名称”、“计算机 ID”、“IP 地址”、“子网掩码”、“端口”、“系统类型”、“当前版本”、“查杀毒状态”、“自我保护”状态和“系统中心名称”等详细信息

【退出】：退出管理控制台

4.1.1.2.1.2【查看】菜单

用户可以根据需要来设置管理控制台各个部分的显示方式，并且用户可以查看注册信息、漏洞信息和安全首页等。

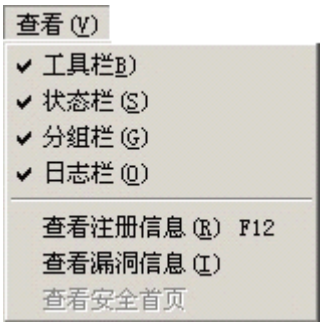

图 47

4.1.1.2.1.3【设置】菜单

用户可以设置管理控制台参数的功能，包括超时设置和安全首页设置两个选项页。

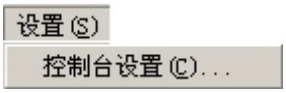

图 48

【控制台设置】：管理控制台缓存、通讯超时时间和安全首页设置，如下图：

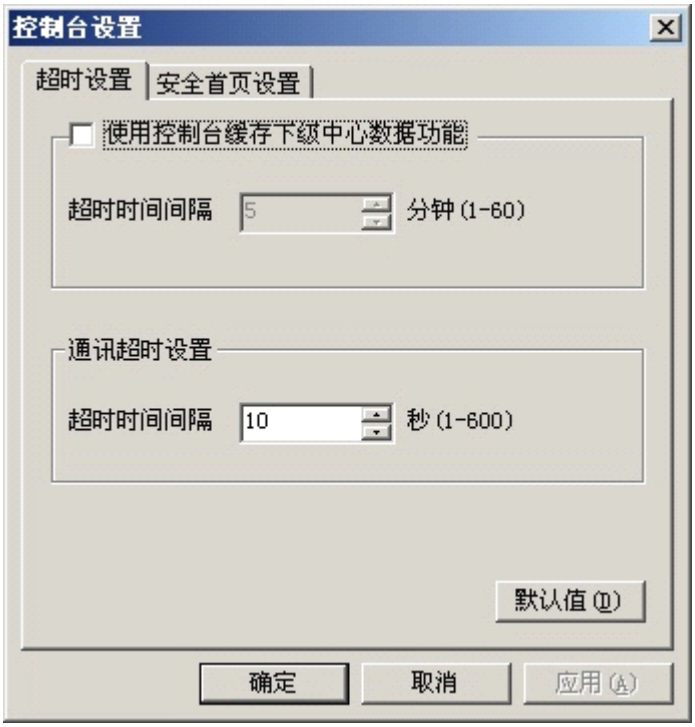

图 49

- **【超时设置】选项页：**

【使用控制台缓存下级中心数据功能】：勾选此项能够开启控制台缓存下级中心数据功能，其下的【超

时时间间隔】用于设置控制台缓存的下级中心信息有效时间，超过该时间后缓冲将不再生效，可以输入时间，也可以通过上下箭头按钮设置时间。输入内容只能是数字，不能为字符等

通讯超时设置用于设置瑞星杀毒软件网络版各程序模块内部通讯超时的时间间隔，【超时时间间隔】中可以输入时间，也可以通过上下箭头按钮设置时间。输入内容只能是数字，不能为字符等

- **【安全首页设置】选项页：**

【启动控制台时显示安全状况首页】：勾选此项使得管理控制台启动时显示安全状况页面

4.1.1.2.1.4【升级】菜单

用户通过菜单选项对系统中心和客户端进行升级操作。

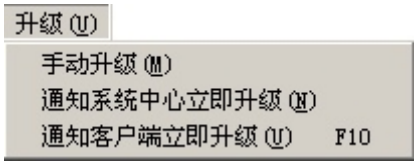

图 410

以下是对各个选项的具体说明：

【手动升级】：选择该项后，在弹出的【打开】对话框中选择升级包程序，再单击【打开】按钮即可对系统中心进行升级

【通知系统中心立即升级】：选择该项后，将会通知指定的系统中心自动进行升级

【通知客户端立即升级】：选择该项后，将通知所有激活的或手动指定的客户端自动进行升级

注意：使用手动升级方式，需要升级前先从瑞星网站下载升级包。

4.1.1.2.1.5【管理】菜单

用户通过管理中的各个菜单选项进行各种管理操作。

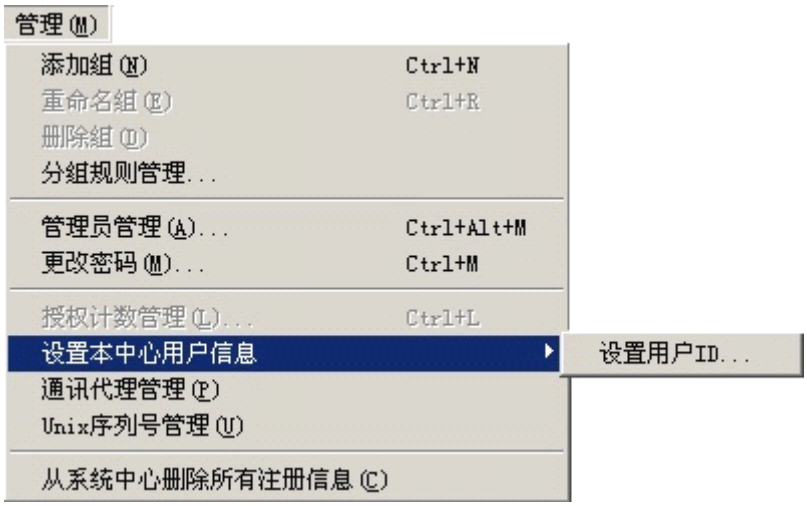

图 411

以下是对各个选项的具体说明：

【添加组】：在组管理界面里添加组

【重命名组】：在组管理界面里对选中的组重命名

【删除组】：在组管理界面里删除选中的组

【分组规则管理】：设置自动分组的规则信息

【管理员管理】：添加删除管理员，修改管理员密码及管理权限等

【更改密码】：更改当前登录管理员密码

【授权计数管理】：查看产品的授权计数信息及使用情况，添加、删除序列号

【设置本中心用户信息】：弹出设置本中心用户 ID 菜单

【设置本中心用户信息】/【设置用户 ID】：弹出设置用户 ID 界面

【设置专用版信息】：输入专用版信息码，设置专用版的定制信息，单击【确定】按钮则在下次升级后可以使用购买时候定制的功能。同时，为方便统一设置，还可以将此应用到所有的下级中心。

说明：在企业专用版和高级企业专用版中有【设置专用版信息】选项；网吧版、中小企业版、企业版和高级企业版中无此选项。

【通讯代理管理】：当安装多级系统中心的时候，可以在此添加上下级通讯代理

【Unix 序列号管理】：查看 Unix 序列号列表，管理员可以查看和删除 Unix 序列号

【从系统中心删除所有注册信息】：用于清除当前系统中心维护的所有客户端信息。主要目的是初始化系统中心上客户端注册信息列表

4.1.1.2.1.6【工具】菜单

工具菜单包括当前系统中心设置、NT 客户端安装工具、日志管理工具、漏洞管理工具和 Unix 客户端升级工具等。

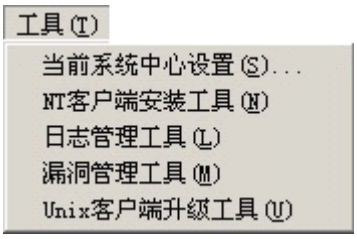

图 412

以下是对各个选项的具体说明：

【当前系统中心设置】：可对系统中心、网络设置、升级设置、黑白名单、漏洞扫描和对象端口等选项进行配置

【NT 客户端安装工具】：通过此工具为客户端远程安装瑞星杀毒软件网络版

【日志管理工具】：瑞星日志查询统计工具，此工具支持日志查询及分类统计，还可以通过图表直观地反映一段时间内的病毒发作趋势，最近发作最多的病毒排行和最近感染病毒最多的客户端排行等状况

【漏洞管理工具】：瑞星漏洞信息管理工具可以对漏洞信息进行分类查询、管理，负责客户端补丁管理、分发、安装等

【Unix 客户端升级工具】：通过此工具可以对 Unix 客户端进行升级

4.1.1.2.1.7【帮助】菜单

用户通过此菜单选项能够查看管理控制台使用帮助以及管理控制台版本信息。

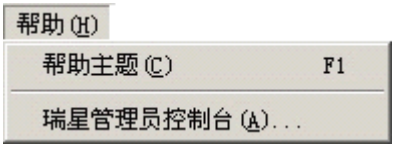

图 413

4.1.1.2.2 组管理界面

在用户分组管理的功能界面中，能够以树型结构显示多级系统中心的层次结构。在此可以创建组、添加组成员，对各个组进行统一操作与管理。

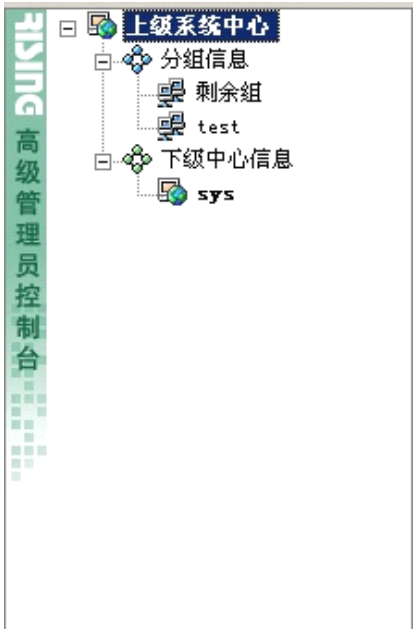

图 414

4.1.1.2.3 安全状况

管理控制台通过安全状况页面显示本级中心的重要安全状况信息，使得管理员能够全面直观地了解整个网络的安全状况，其中主要内容包括：防病毒系统运行概况、重要事件和总体安全情况。

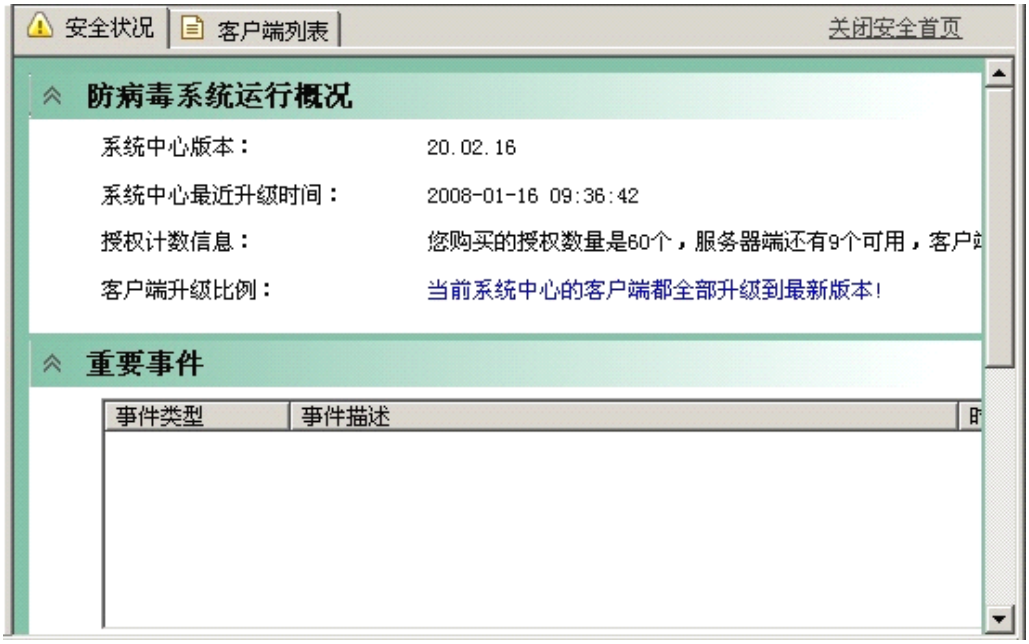

图 415

注意：总体安全情况中显示当前系统中心内感染最多的前 5 名病毒排行和被病毒感染最多客户端前 5 名排行情况，用户对显示的内容不能进行自定义设置。

4.1.1.2.4 客户端列表栏

在客户端列表页面中，显示已注册到系统中心的计算机名、IP 地址、端口、实时监控状态、主动防御状态、防火墙状态、查杀毒状态、当前版本、连接状态以及系统类型。

说明：其中防火墙状态在高级企业版中显示；在高级企业专用版定制了防火墙的情况下显示该项；网吧版、中小企业版、企业版和企业专用版中无此项。

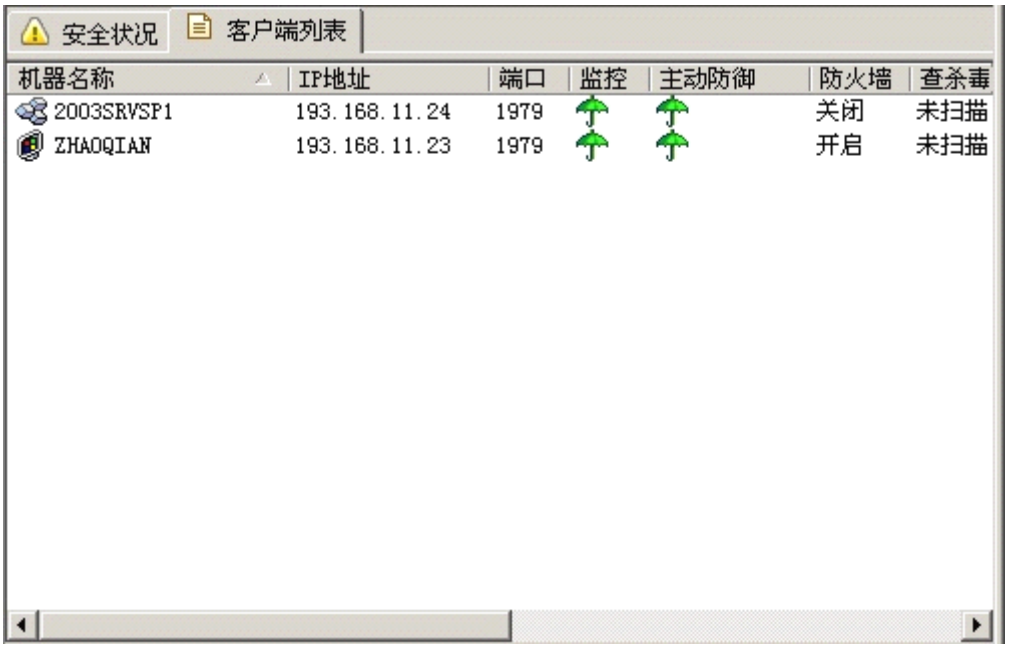

图 416

以下是对各个选项的具体说明：

【机器名称】：显示客户端计算机名称

【IP 地址】：显示客户端 IP 地址

【端口】：显示客户端打开的端口号

【监控】：显示监控状态，其中绿色 图标代表所有监控全部开启，红色 图标代表所有监控全部禁用，黄色 图标代表部分监控没有开启，如果没有图标显示，则说明此客户端的监控服务未启动或未安装监控组件

【主动防御】：显示主动防御状态，其中绿色 图标代表所有主动防御功能全部开启，红色 图标代表所有主动防御功能全部关闭，黄色 图标代表部分防御功能没有开启，如果没有图标显示，则说明此客户端的监控服务未启动或未安装主动防御组件

【防火墙】：显示防火墙状态

【查杀毒状态】：显示查杀毒状态，其中包括的状态有未扫描、正在扫描（远程查杀）、本地查杀

- 未扫描表示当前没有扫描事件
- 正在扫描（远程查杀）表示通过系统中心对客户端进行的扫描
- 本地查杀表示客户端进行的查杀

【当前版本】：显示当前网络版版本

【连接状态】：显示连接状态，包括两种：激活和未激活

【系统类型】：显示操作系统版本

4.1.1.2.5 日志栏

便于用户通过日志查看当前网络安全状态和安全历史记录。日志栏位于管理控制台界面的下方，包含五个标签页：【病毒日志】、【事件日志】、【主动防御日志】、【IP 事件日志】、【运行日志】，可以通过单击不同的标签查看指定类型的日志，默认状态显示【运行日志】。在日志信息上单击右键，可以删除所选的日志信息。

说明：在高级企业版默认显示【IP 事件日志】项；高级企业专用版在购买时定制了防火墙功能的情况下，显示【IP 事件日志】项；网吧版、中小企业版、企业版和企业专用版中无此项。

图 417

4.1.1.2.6 状态栏

显示状态信息，其中信息包括当前显示客户端数量、当前系统中心 IP、端口和版本。

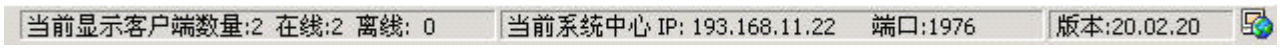

图 418

4.1.2 远程管理

远程管理功能主要是使网络管理员进行远程操作，这些操作包括为当前系统中心及其任意客户端或下级系统中心及其任意客户端进行查杀病毒、漏洞扫描、开启/关闭实时监控、开启/关闭主动防御、远程诊断客户端信息等操作。

4.1.2.1查杀病毒

在管理控制台上可以任选一台或多台计算机进行远程查杀病毒。

在计算机列表栏中选择需要查杀的计算机，单击右键，在右键菜单中选择【查杀病毒】（或单击工具栏中的  按钮，或【操作】菜单下的【查杀病毒】）后，弹出查杀选项设置界面。先在下拉列表中选择查杀路径，然后单击【开始扫描】即按照默认设置开始远程查杀病毒。若需要对查杀选项进行详细设置，单击【高级选项】按钮，在出现的页面中可以设置查杀文件类型、优化选项、对查杀病毒出现的各种不同情况的处理方式、查杀优先级、报告查杀进度时间间隔等。

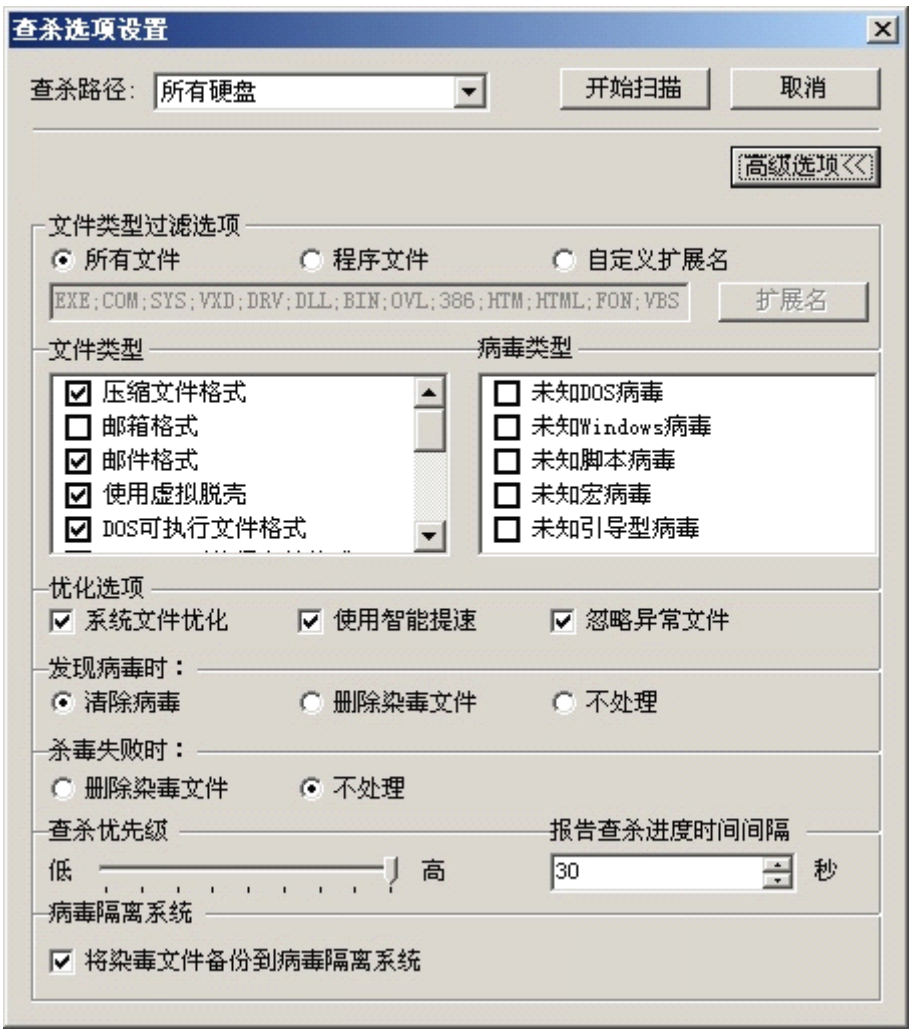

图 419

4.1.2.2漏洞扫描

说明：在企业专用版和高级企业专用版中，购买时可以定制该功能；网吧版中没有该功能；中小企业版、企业版和高级企业版中有该功能。

在管理控制台上可以任选一台或多台计算机进行漏洞扫描。管理员可以通过立即执行漏洞扫描的方式，及时的了解客户端漏洞情况。

第一步：在计算机列表栏中，选中准备进行扫描的计算机，单击  按钮或选择【操作】/【扫描漏洞】，或在选定计算机上单击右键，弹出的菜单中选择【扫描漏洞】。

第二步：在弹出的漏洞扫描设置对话框中完成扫描设置。用户可以在【扫描系统漏洞】和【扫描不安全设置】选项前的复选框中勾选或取消勾选，扫描后会根据用户的选择显示相应的扫描信息。当扫描“不安全设置”时可以选择是否自动修复，勾选【自动修复不安全设置】将修复可以自动修复的“不安全设置”，对于不能自动修复的“不安全设置”需要用户手动修复。单击【严重级别】下拉按钮可以选择不同级别对系统漏洞和不安全设置进行扫描，分为全部、最高、中级以上、低级以上四种，用户可根据需求设置扫描级别。单击【开始扫描】进行漏洞扫描。

图 420

注意：选择【自动修复不安全设置】选项可能会导致客户端的系统设置被修改，此项默认不勾选，请慎重操作！

第三步：在管理控制台中会显示漏洞扫描详细信息，用户可以查看结果并进行修复漏洞等操作。下面是在既选择系统漏洞又选择了不安全设置的情况下查看漏洞结果。

单击【客户端】标签，扫描结果将按客户端分类显示。选中某个计算机，在下面漏洞信息列表中选择某项漏洞信息，单击右键选择【安装补丁程序】可以通知选中计算机安装此漏洞的补丁程序；选择某项不安全设置，单击右键选择【修复不安全设置】可以为选中计算机修复此项不安全设置。

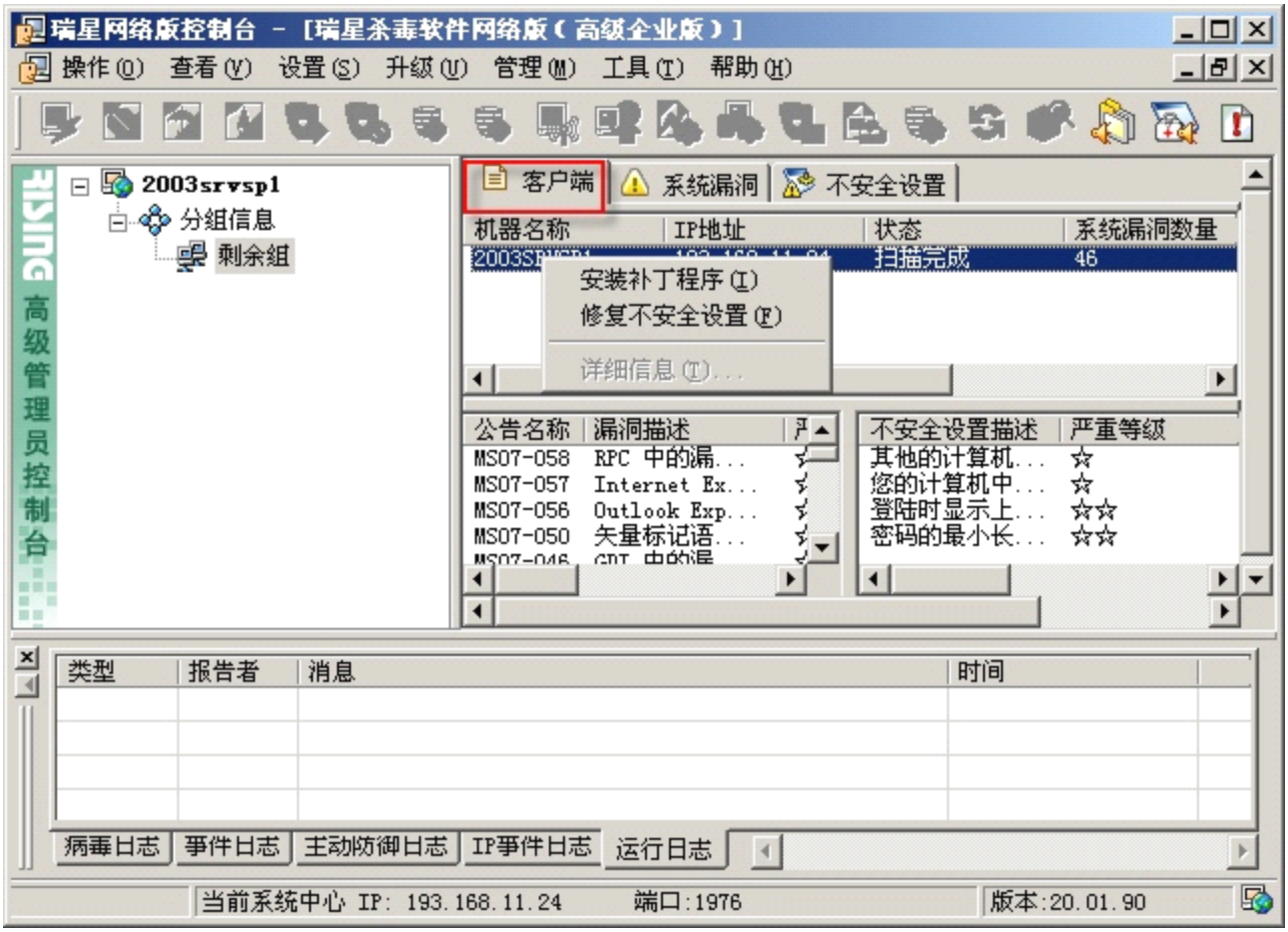

图 421

在漏洞扫描界面中会显示扫描状态和结果，在扫描结果列表中双击某项或在右键菜单中选【详细信息】，会显示该项漏洞的详细信息。

图 422

单击【系统漏洞】标签，扫描结果将按漏洞分类并显示，选择某个漏洞后可显示该漏洞的分布状况，可查看哪些客户端存在此漏洞。双击某项系统漏洞或在右键菜单中选择【详细信息】，会显示该项漏洞的详细信息及补丁下载路径。

在漏洞区域选中某个系统漏洞，在下面存在此漏洞的计算机列表中，选择准备安装补丁的计算机，单击右键选择【安装补丁程序】将通知所选择的计算机安装此漏洞的补丁程序。如果直接在漏洞信息上单击右键选择【安装补丁程序】，则通知下面列表中所有存在此漏洞的计算机安装此漏洞补丁程序。

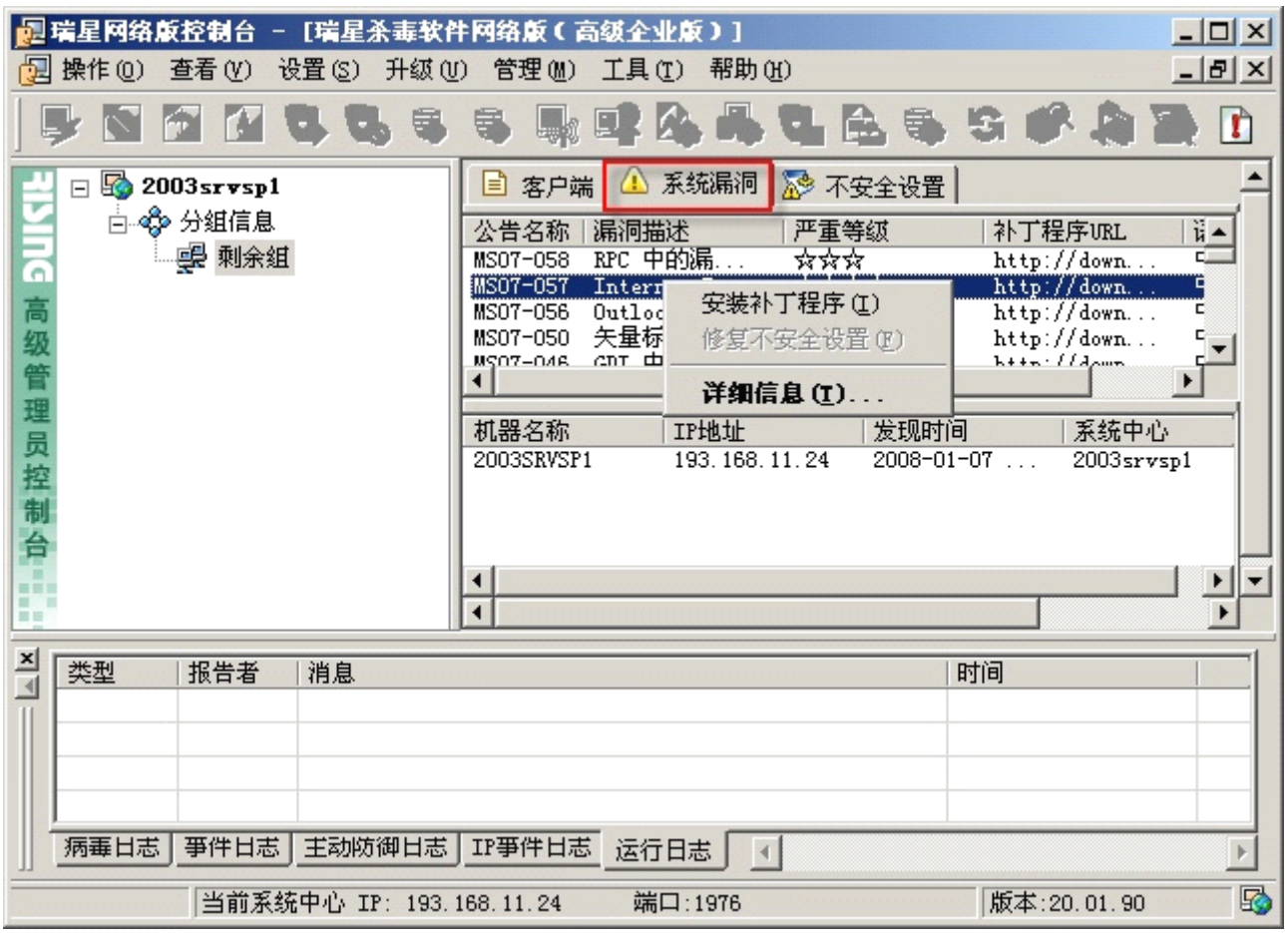

图 423

单击【不安全设置】标签，扫描结果将按不安全设置分类并显示，选择某个不安全设置后显示该不安全设置的分布状况，可查看哪些客户端存在此不安全设置。双击某项不安全设置或在右键菜单中选【详细信息】，会显示该项不安全设置的详细信息。

在不安全设置区域选中某个不安全设置，在下面存在此不安全设置的计算机列表中，选择需要进行修复的计算机，单击右键选择【修复不安全设置】将通知所选择的计算机进行修复。如果直接在不安全设置信息上单击右键选择【修复不安全设置】，则对下面列表中所有存在此不安全设置的计算机进行修复。

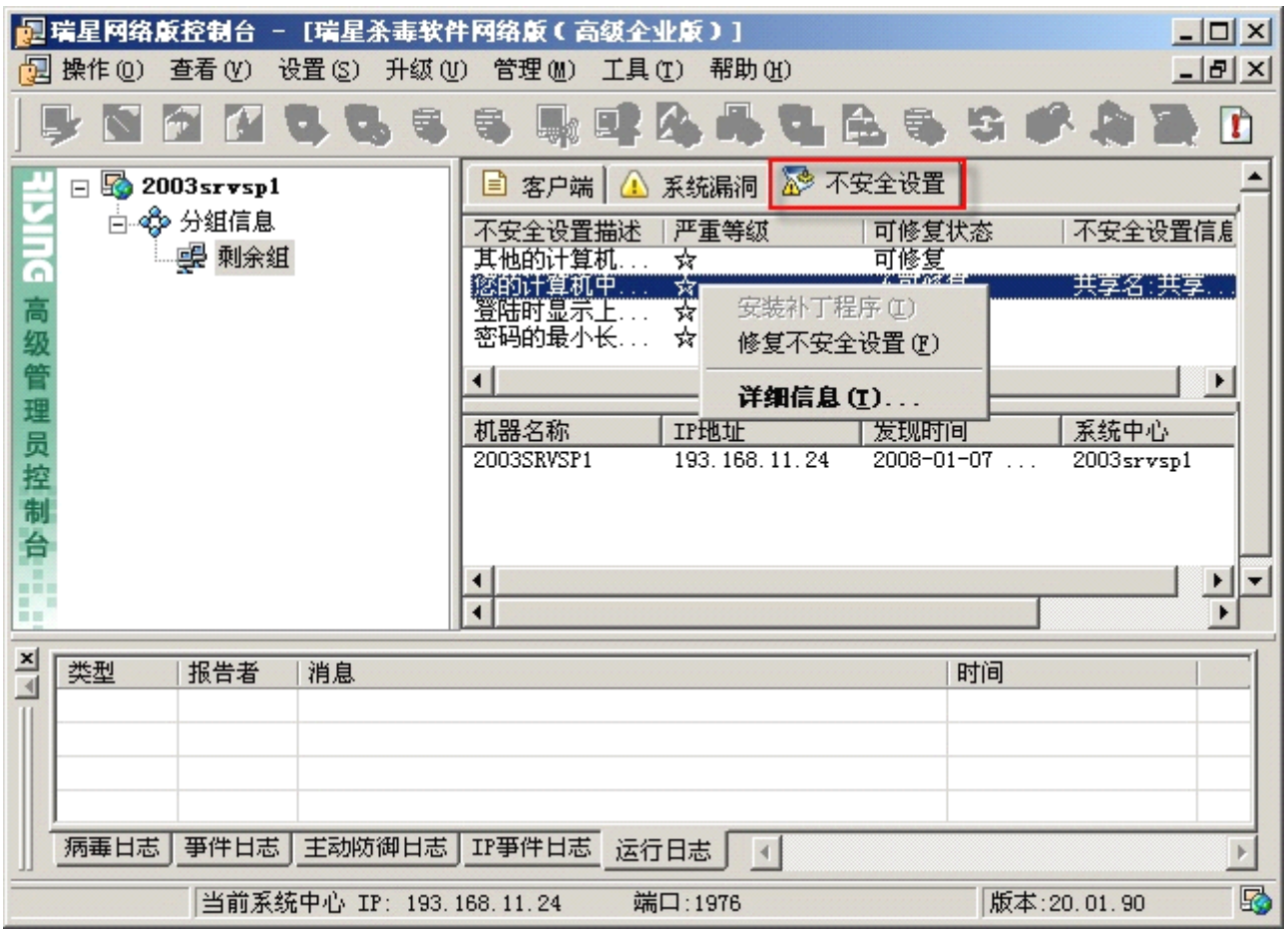

图 424

第四步：漏洞扫描后需要为客户端安装漏洞补丁，具体设置如下：

1．首先通知系统中心下载补丁程序，可以在漏洞信息管理工具中选择【操作】/【通知瑞星下载中心下载补丁程序】则系统中心会下载补丁程序。如果不希望通过手动方式通知系统中心下载客户端需要的补丁程序，可以在心 4.1.3.6.5 漏洞扫描设置勾选【自动下载漏洞补丁程序】，这样系统中心会自动进行补丁程序的下载。

2．通知客户端安装补丁程序。在漏洞信息管理工具中选择【操作】/【通知安装补丁程序】则通知选中的客户端会安装补丁程序。如果不希望通过手动方式通知客户端安装补丁程序，可以在 4.1.3.6.5 漏洞扫描设置勾选【自动通知客户端修复已下载的补丁程序】，当系统中心下载完补丁程序后，则会自动通知客户端安装补丁程序。当客户端收到通知后，如果 4.1.3.3.7 漏洞扫描设置勾选了【自动安装补丁程序】，则客户端会及时修复其漏洞。若没有勾选该项则客户端托盘程序会弹出提示，告知用户某些漏洞在系统中心已有对应补丁，需要用户手动选择安装补丁程序。

为了方便管理，管理员可以设置定期进行漏洞扫描并及时为客户端安装补丁程序。具体设置可以参考 4.1.3.3.7 漏洞扫描设置。

注意：

1.瑞星杀毒软件网络版将通过不断的升级来增加和完善漏洞信息，为保证可以扫描到最新的漏洞信息，请及时从瑞星网站更新瑞星杀毒软件网络版。

2.由于操作系统特性不同，更新补丁后可能要求重新启动系统。

3.瑞星杀毒软件网络版只提供补丁文件的管理和分发功能，所有补丁程序均由微软公司提供，补丁的安装过程也由微软程序完成，由于安装补丁程序或修复不安全设置引起的系统功能异常和配置修改等问题请向微软公司咨询。

4.在扫描结果中，会出现某些补丁程序无法下载的情况，这是由于此类漏洞的修补只能利用微软公司提供的 Windows Update 来完成，微软公司并没有单独对此漏洞提供公用的补丁程序，对于此类漏洞请通

过 Windows Update 功能进行更新。

4.1.2.3发送广播消息

说明：网吧版中无此功能。

管理员可以通过管理控制台上的广播功能对所有或指定的客户端发布文本消息。此项功能实现了管理员对客户端的文字化交流，使得管理更加周密和高效。

发送广播的步骤如下：

第一步：在计算机列表栏选中需要接受广播的用户，单击【操作】菜单，选择【发送广播消息】，或者在选中用户的右键菜单中选择【发送广播消息】。

第二步：在弹出的【发送广播消息】窗口中输入文本信息，单击【发送】。

图 425

第三步：目标客户端将弹出消息窗口，读取完消息后，单击【清除】按钮即可清除该消息，单击【保存】，可将该广播消息保存为 *.txt 文件。

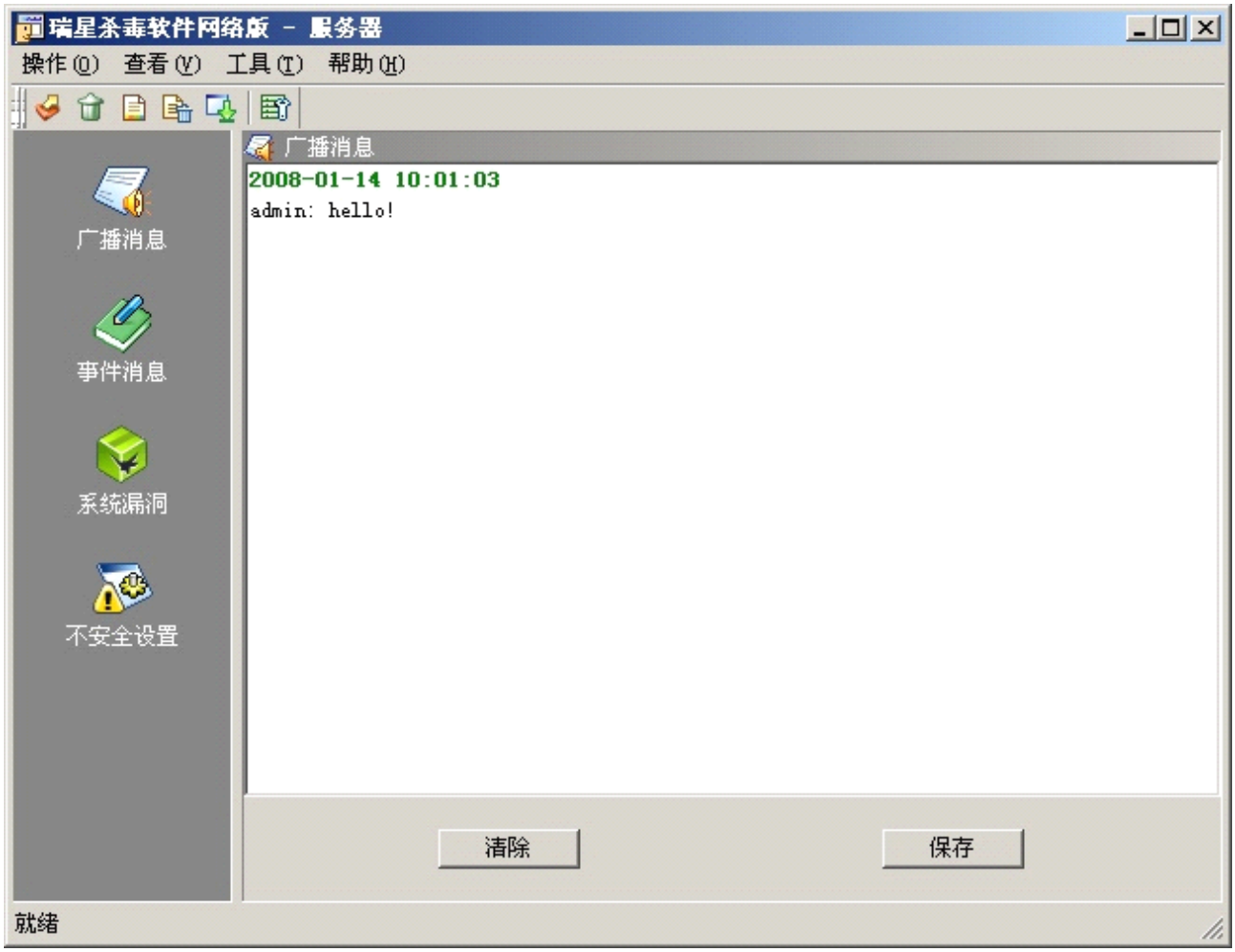

图 426

4.1.2.4开启/关闭实时监控

便于设置指定计算机打开或关闭实时监控的所有功能或部分功能。

在管理控制台上可以任选一台或多台计算机，选择【操作】/【打开实时监控】或【关闭实时监控】，或者单击工具栏中的  （或  ）按钮，或者单击右键选择【打开实时监控】或【关闭实时监控】，即可开启或关闭选中计算机的实时监控。

注意：该操作仅对处于“激活”状态的客户端有效。

4.1.2.5开启/关闭主动防御

便于设置指定计算机打开或关闭主动防御的所有功能或部分功能。

在管理控制台上可以任选一台或多台计算机，选择【操作】/【打开主动防御】或【关闭主动防御】，或者单击工具栏中的  （或  ）按钮，或者单击右键选择【打开主动防御】或【关闭主动防御】，即可开启或关闭选中计算机的主动防御。

注意：

1. 该操作仅对处于“激活”状态的客户端有效。

2. Windows 9X、NT 和所有 64 位操作系统不支持主动防御功能。对于不支持主动防御功能或没有安装主动防御的客户端，操作菜单中的【打开主动防御】或【关闭主动防御】为灰色不可用状态。

4.1.2.6开启/关闭自我保护

便于设置指定计算机打开或关闭自我保护功能。

在管理控制台上可以任选一台或多台计算机，选择【操作】/【开启自我保护】或【关闭自我保护】，则可以打开或关闭自我保护功能。

注意：

1. 该操作仅对处于“激活”状态的客户端有效。
2. 自我保护功能是主动防御功能的组成部分，Windows 9X、NT 和所有 64 位操作系统不支持主动防御功能。对于不支持主动防御功能或没有安装主动防御的客户端，操作菜单中的【开启自我保护】或【关闭自我保护】为灰色不可用状态。

4.1.2.7开启/关闭防火墙

说明：在高级企业版有此功能；在高级企业专用版中，购买时定制了防火墙的情况下有此功能；网吧版、中小企业版、企业版和企业专用版中无此功能。

便于设置指定计算机打开或关闭防火墙功能。

在管理控制台上可以选择一台或多台计算机，选择【操作】/【开启防火墙】或【关闭防火墙】用以远程启动和关闭防火墙功能。

注意：该操作仅对处于“激活”状态的客户端有效。

4.1.2.8远程诊断客户端信息

当客户端存在安全问题或防病毒软件运行不正常时，管理员可以通过管理控制台远程提取到客户端诊断信息，以便分析客户端的安全情况或防病毒系统工作不正常的原因，并针对不安全状况和防毒软件异常情况采取相应的措施。客户端能够提取的诊断信息主要分为六大类，分别是当前进程列表、系统启动项、已安装的软件列表、IE 资源插件、IE 工具条和文件关联项。系统默认选择系统启动项、加载已安装软件列表和文件关联项，管理员也可以根据自己的需要进行选择。

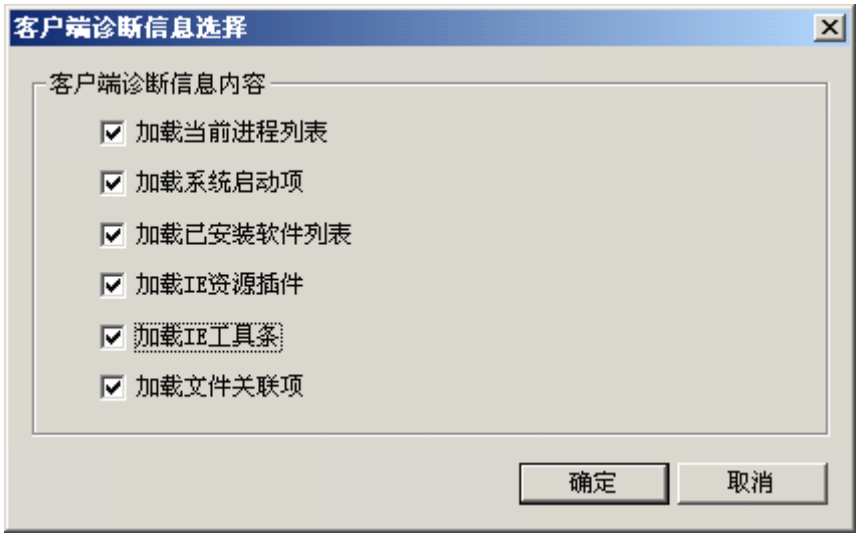

图 427

当管理员选择“确定”按钮后，控制台会弹出加载进度窗口。若加载客户端诊断信息失败，管理员可以选择【重试】按钮重新加载诊断信息，也可以选择【取消】退出。

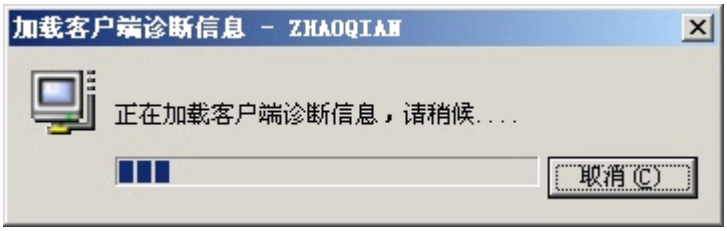

图 428

如果加载信息成功，管理控制台则根据管理员选择的具体诊断信息类别来显示诊断结果。

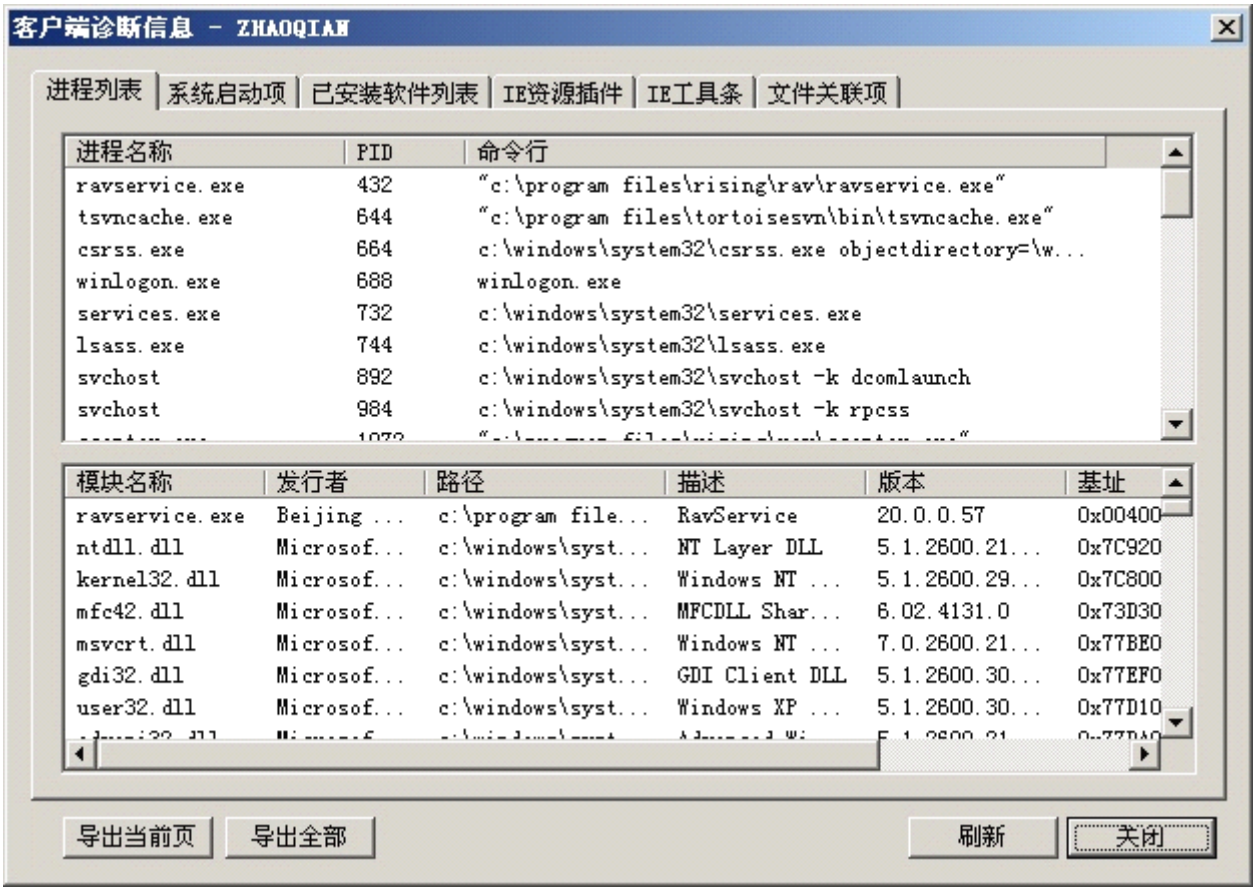

图 429

注意：对于“激活”状态的客户端能够提取其诊断信息，对于“未激活”状态的客户端则会无法提取诊断信息。

4.1.3 配置

在管理控制台中系统管理员可以为网络中的系统中心和客户端进行各种设置，实施各种安全策略。为客户端设置包括防毒策略、客户端选项、主动防御规则等策略，通过有效、合理的策略设置保障各网络在安全的环境中运行。

4.1.3.1关于设置对象的说明

瑞星杀毒软件网络版的策略包括防毒策略、客户端选项、主动防御规则和防火墙策略等，以下关于设

置对象的说明适用于这些策略的操作。

说明：仅在高级企业版有防火墙策略；在高级企业专用版定制了防火墙功能情况下有防火墙规则设置；网吧版、中小企业版、企业版和企业专用版中无防火墙规则设置。

如果在组管理界面上选中某个组，则对组设置策略；如果在组管理界面上选中系统中心则对本级系统中心及下属所有客户端进行统一设置（若要同时将设置应用到下级中心，可以勾选【应用到所有下级中心】）；如果在计算机列表中选中某个客户端，则修改指定计算机的策略。

当用户在组管理界面选择某个组、系统中心或【分组信息】设置策略时，对其包含的“已激活”的客户端该策略会被立即应用，对于“未激活”的客户端激活后也会自动应用该策略；而当用户在客户端列表中选中某个客户端进行设置时，策略将即时生效，且只能应用于已激活的客户端，对离线客户端无效。

4.1.3.2设置防毒策略

管理员对于客户端进行防毒策略的设置以及控制客户端对于防毒策略的更改权限。

【只应用已修改选项】：只应用修改选项，可以减少客户端同步策略的网络传输量

【导入】：单击此按钮弹出“导入缺省配置”和“从文件中导入”两种导入方式，可以导入缺省配置，将设置还原为出厂设置，还可以将*.ccf 格式文件导入，用于还原备份的配置，能够快速应用相同设置，避免手工设置的麻烦

【导出】：单击此按钮将设置窗口内所有参数信息导出为*.ccf 格式文件，作为当前配置的备份

其中各个设置页面均有“红锁”和“绿锁"，对于这两项在此给予解释：

红锁/绿锁：“红锁”代表该选项已经被管理员锁定，“绿锁”代表该选项未被管理员锁定，如果管理员锁定了该选项，客户端将无法在本地更改选项，直到远程管理员将该选项解锁，这样管理员可以控制客户端对于选项的更改。

4.1.3.2.1 实时监控设置页面

用户可以为选中的客户端设置开机启用文件监控、网页监控、邮件监控功能。

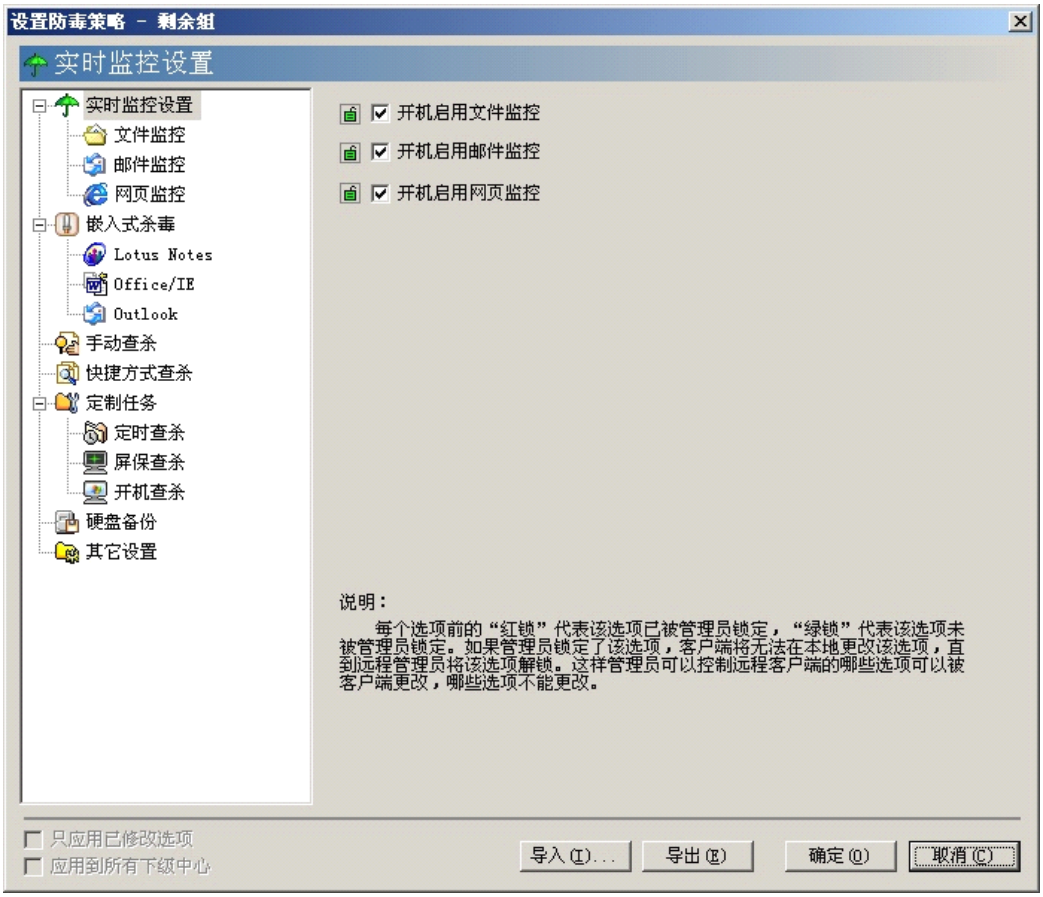

图 430

4.1.3.2.2 文件监控页面

用户可以为选中的客户端设置文件监控功能，具体内容如下：

设置文件类型：可以通过【文件类型过滤选项】自定义文件类型。并可以在文件类型和病毒类型中勾选不同类型的文件进行监控。

设置优化选项：可以通过系统文件优化、使用智能提速和忽略异常文件三种方式优化和提高查杀病毒速度并且提高引擎的稳定性。

设置发现病毒、杀毒失败和备份失败时的处理方式。

还可以设置是否启用智能监控和强杀文件、是否提示杀毒结果以及对话框自动关闭时间、是否显示监控超时后提示和是否记录日志等。

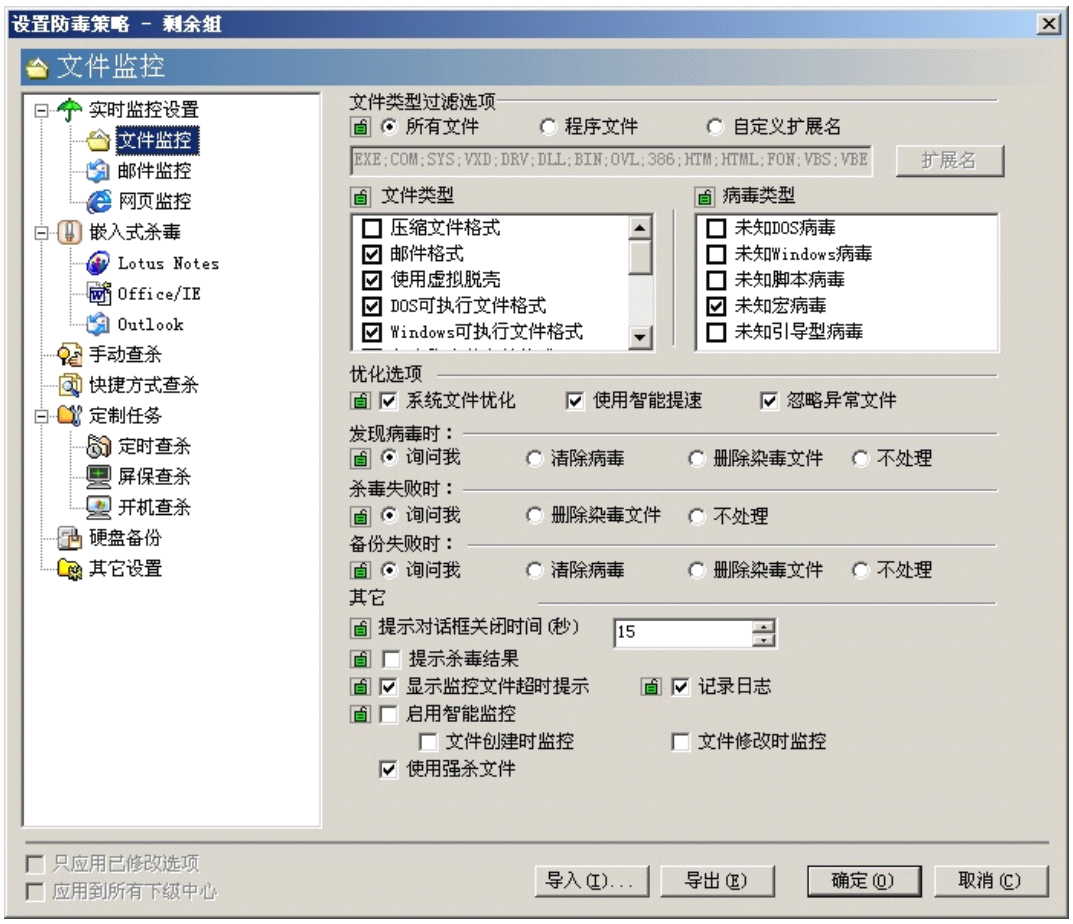

图 431

注意：当系统管理员锁定文件类型、病毒类型和优化选项任意项的时候，在客户端通过设置高、中、低级别的滑块设置级别时，仅修改未被锁定的选项，已经被锁定的选项则不能被修改。

4.1.3.2.3 邮件监控页面

说明：在企业专用版和高级企业专用版中，购买时定制了邮件监控功能的情况下可以设置邮件监控；网吧版中无邮件监控功能，故无此设置页面；中小企业版、企业版和高级企业版中有该设置页面。

在邮件监控设置界面，用户可以为选中客户端设置邮件监控功能，具体内容如下：

设置文件类型：可以通过【文件类型过滤选项】自定义文件类型。并可以在文件类型和病毒类型中勾选不同类型的文件进行监控。

端口设置：设置邮件监控的监控端口。

设置发现病毒、杀毒失败和备份失败时的处理方式。

还可以设置是否隐藏邮件收发进度提示窗口、是否提示杀毒结果、对话框自动关闭时间和是否记录日志等。

图 432

注意：当系统管理员锁定文件类型、病毒类型和优化选项任意项的时候，在客户端通过设置高、中、低级别的滑块设置级别时，仅修改未被锁定的选项，已经被锁定的选项则不能被修改。

4.1.3.2.4 网页监控页面

提供设置网页监控界面。用户可以为选中的客户端设置网页监控发现病毒时的处理方式，还可以设置对话框自动关闭时间和是否记录日志等。

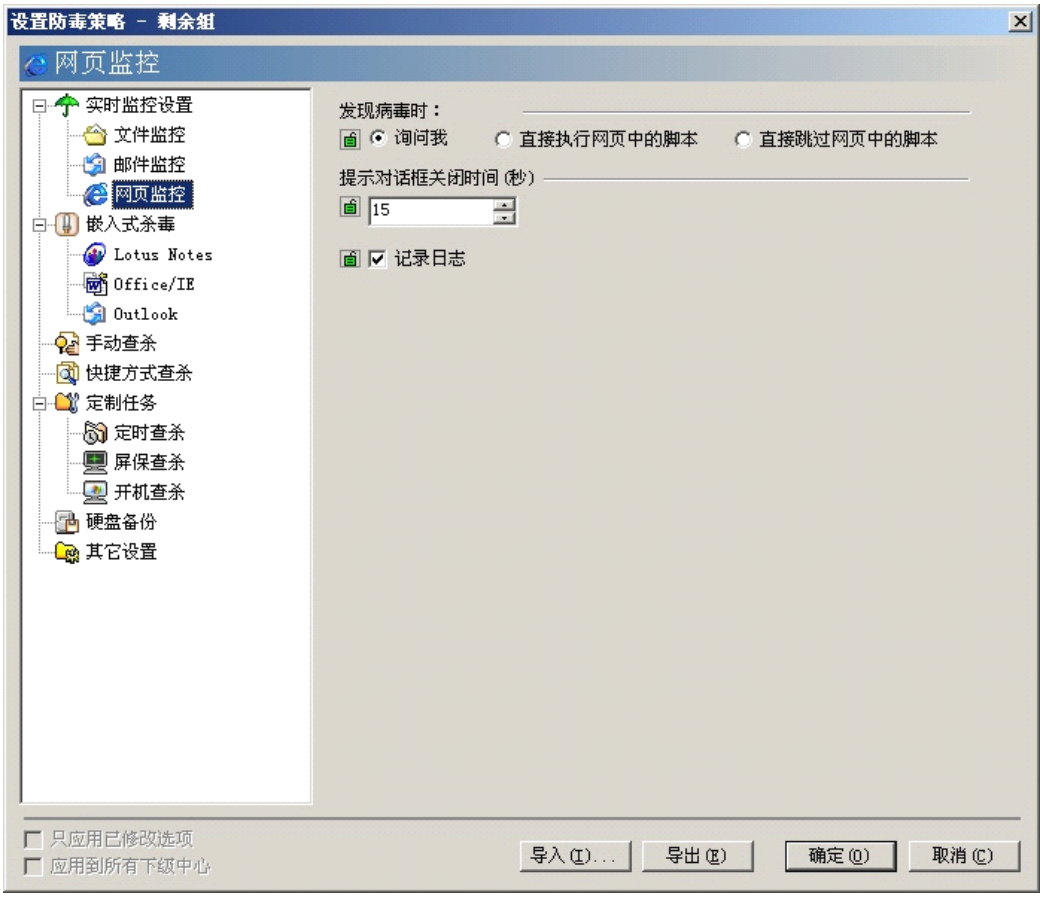

图 433

4.1.3.2.5 嵌入式杀毒页面

在嵌入式杀毒设置界面，用户可以为客户端设置是否使用 Lotus Notes 嵌入式杀毒、Office/IE 嵌入式杀毒、OutLook 嵌入式杀毒监控功能。

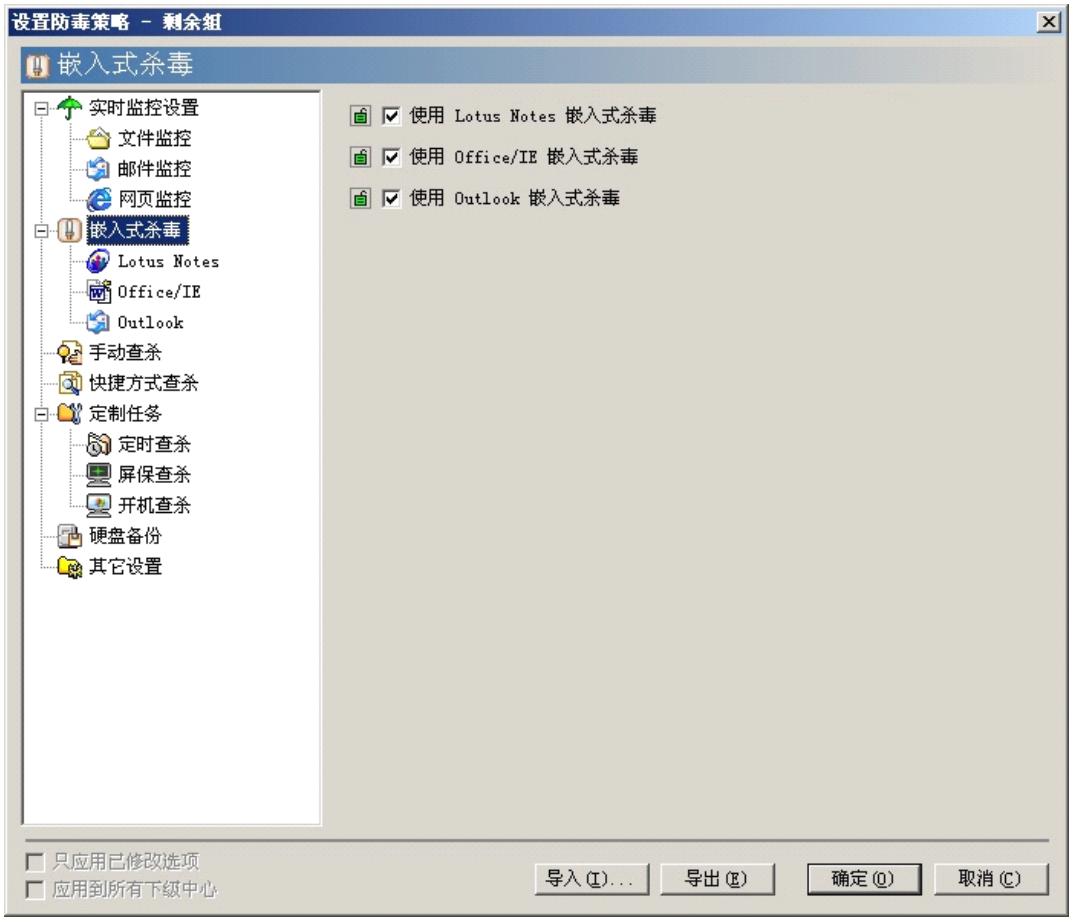

图 434

4.1.3.2.6 Lotus Notes 页面

说明：在企业专用版和高级企业专用版中，购买时定制 Lotus Notes 嵌入式杀毒功能的情况下有此设置页面；网吧版中无 Lotus Notes 嵌入式杀毒功能，故无此设置页面；中小企业版、企业版和高级企业版中有此设置页面。

用户可以设置 Lotus Notes 嵌入式杀毒，具体内容如下：

设置文件类型：可以通过【文件类型过滤选项】自定义文件类型。并可以在文件类型和病毒类型中勾选不同类型的文件。

设置在“接收邮件时”还是在“发送邮件时”进行查杀病毒操作，还可以设置发现病毒、杀毒失败和隔离失败时的处理方式。

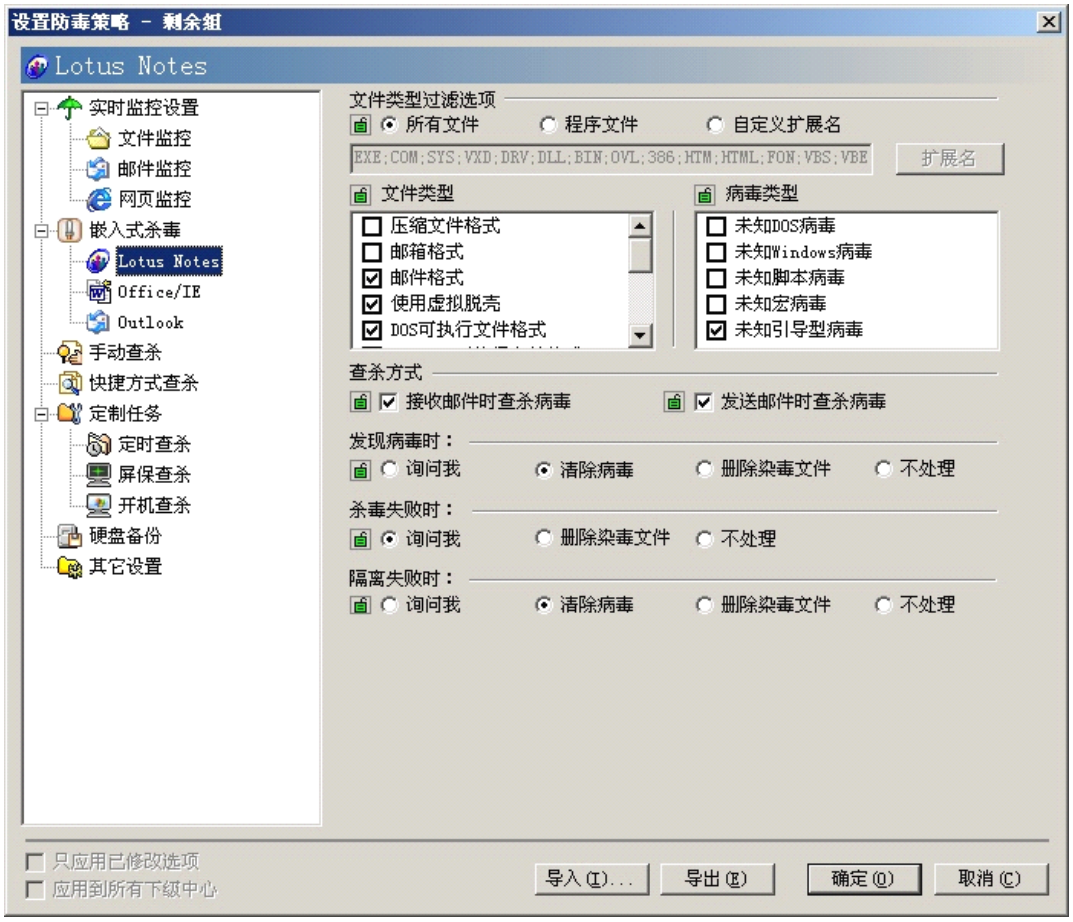

图 435

注意：当系统管理员锁定文件类型或者病毒类型的时候，在客户端通过设置高、中、低级别的滑块设置级别时，仅修改未被锁定的选项，已经被锁定的选项则不能被修改。

4.1.3.2.7 Office/IE 页面

说明：在企业专用版和高级企业专用版中，购买时定制 Office/IE 嵌入式杀毒功能的情况下有此设置页面；网吧版中无 Office/IE 嵌入式杀毒功能，故无此设置页面；中小企业版、企业版和高级企业版中有此设置页面。

用户可以设置 Office/IE 嵌入式杀毒，具体内容如下：

设置文件类型：可以通过【文件类型过滤选项】自定义文件类型。并可以在文件类型和病毒类型中勾选不同类型的文件，并且设置发现病毒、杀毒失败和隔离失败时的处理方式。

图 436

注意：当系统管理员锁定文件类型或者病毒类型的时候，在客户端通过设置高、中、低级别的滑块设置级别时，仅修改未被锁定的选项，已经被锁定的选项则不能被修改。

4.1.3.2.8 OutLook 页面

用户可以设置 OutLook 嵌入式杀毒，具体内容如下：

设置文件类型：可以通过【文件类型过滤选项】自定义文件类型。并可以在文件类型和病毒类型中勾选不同类型的文件，并且设置发现病毒、杀毒失败和隔离失败时的处理方式。

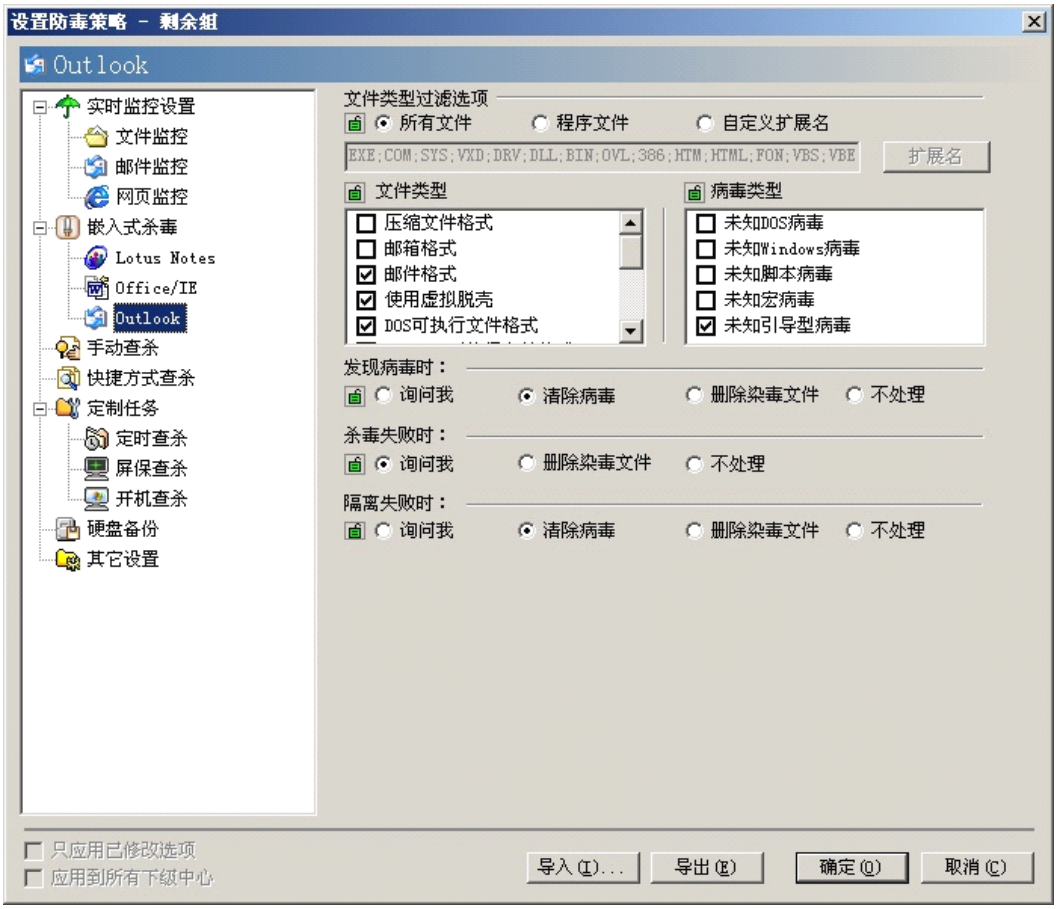

图 437

注意：当系统管理员锁定文件类型或者病毒类型的时候，在客户端通过设置高、中、低级别的滑块设置级别时，仅修改未被锁定的选项，已经被锁定的选项则不能被修改。

4.1.3.2.9手动查杀页面

用户可以为选中的客户端设置手动查杀功能，具体内容如下：

设置文件类型：可以通过【文件类型过滤选项】自定义文件类型。并可以在文件类型和病毒类型中勾选不同类型的文件。

设置优化选项：可以通过系统文件优化、使用智能提速和忽略异常文件三种方式优化和提高查杀病毒速度并且提高引擎的稳定性。

设置发现病毒时、杀毒失败时、杀毒结束后和隔离失败时的处理方式，还可以设置是否提示杀毒结果 。

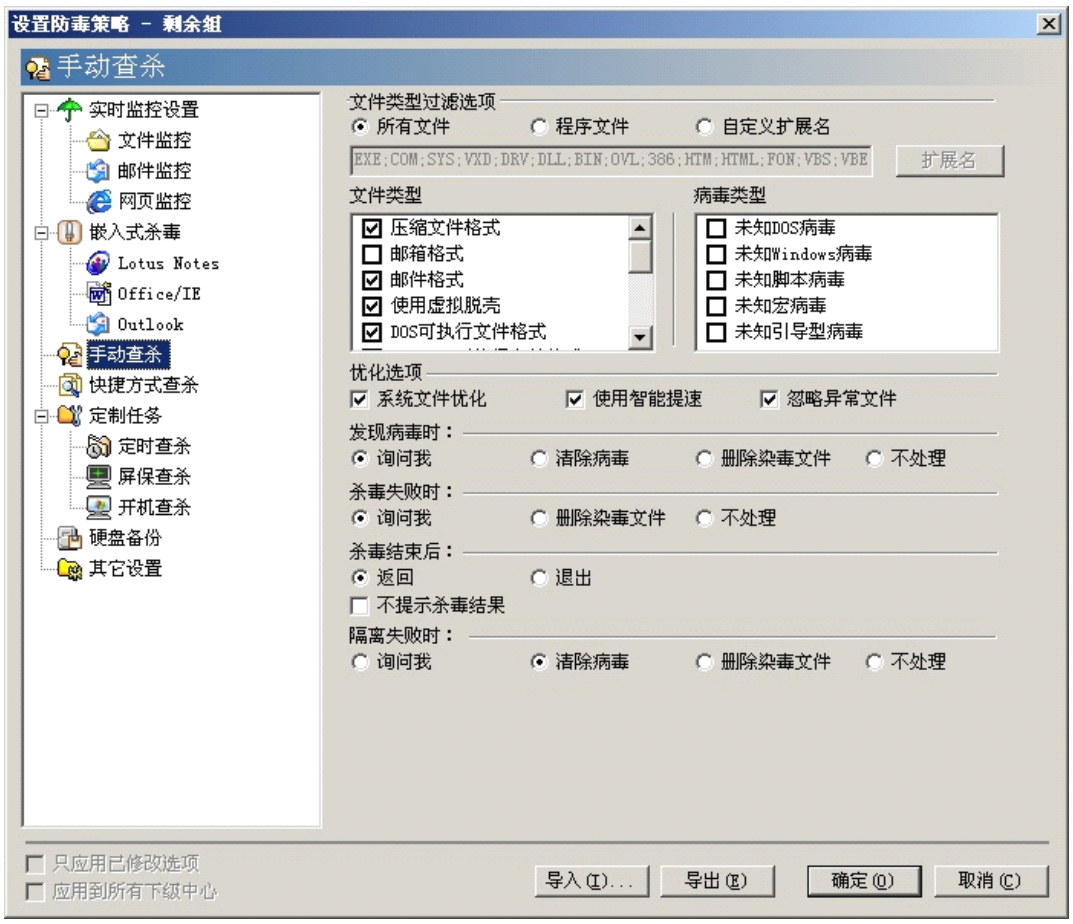

图 438

4.1.3.2.10 快捷方式查杀页面

用户可以为选中的客户端设置快捷方式查杀功能，具体内容如下：

设置文件类型：可以通过【文件类型过滤选项】自定义文件类型。并可以在文件类型和病毒类型中勾选不同类型的文件。

设置优化选项：可以通过系统文件优化、使用智能提速和忽略异常文件三种方式优化和提高查杀病毒速度并且提高引擎的稳定性。

设置发现病毒时、杀毒失败时、杀毒结束后和隔离失败时的处理方式，还可以设置是否提示杀毒结果。

图 439

4.1.3.2.11 定制任务页面

用户为选中的客户端设置是否使用定时查杀、屏保查杀和开机查杀功能。

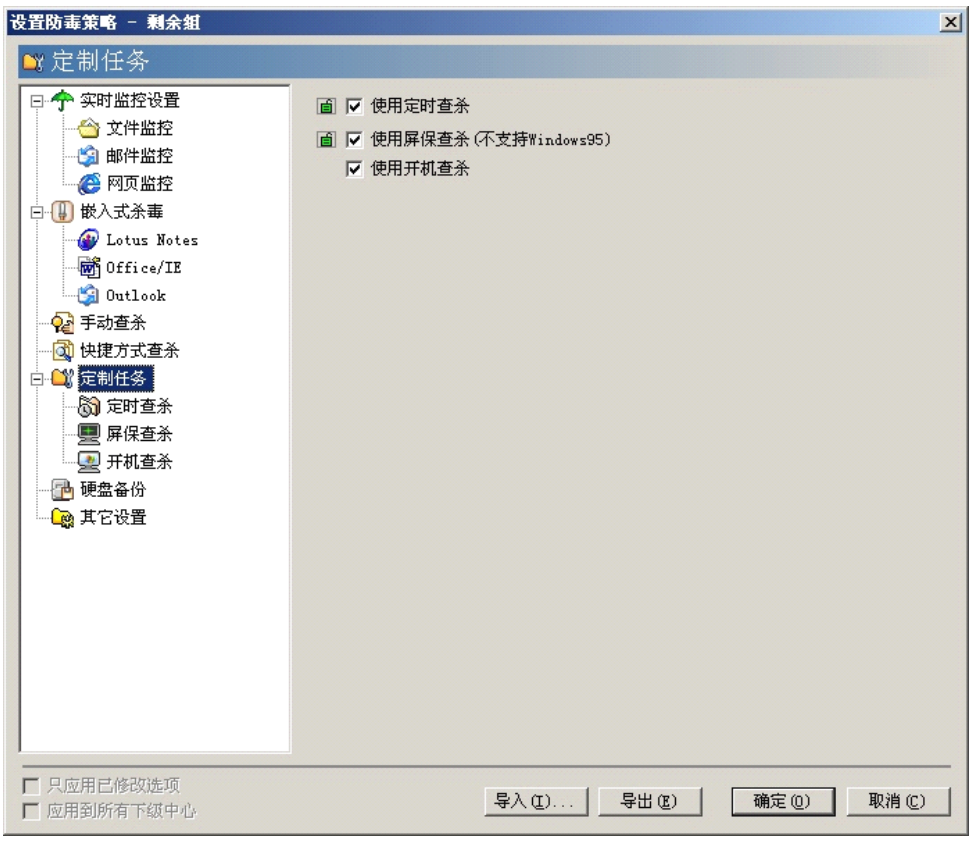

图 440

4.1.3.2.12 定时查杀页面

用户可以为选中的客户端设置定时查杀功能，具体内容如下：

设置文件类型：可以通过【文件类型过滤选项】自定义文件类型。并可以在文件类型和病毒类型中勾选不同类型的文件。

设置优化选项：可以通过系统文件优化、使用智能提速和忽略异常文件三种方式优化和提高查杀病毒速度并且提高引擎的稳定性。

设置发现病毒时、杀毒失败时、杀毒结束后和隔离失败时的处理方式，还可以设置是否提示杀毒结果。

设置定时查杀频率：可以选择每小时、每天、每周和每周期四种频率定时查杀病毒。

定时查杀检测对象：可以选择引导区、内存、邮箱和全部硬盘四种检测对象。

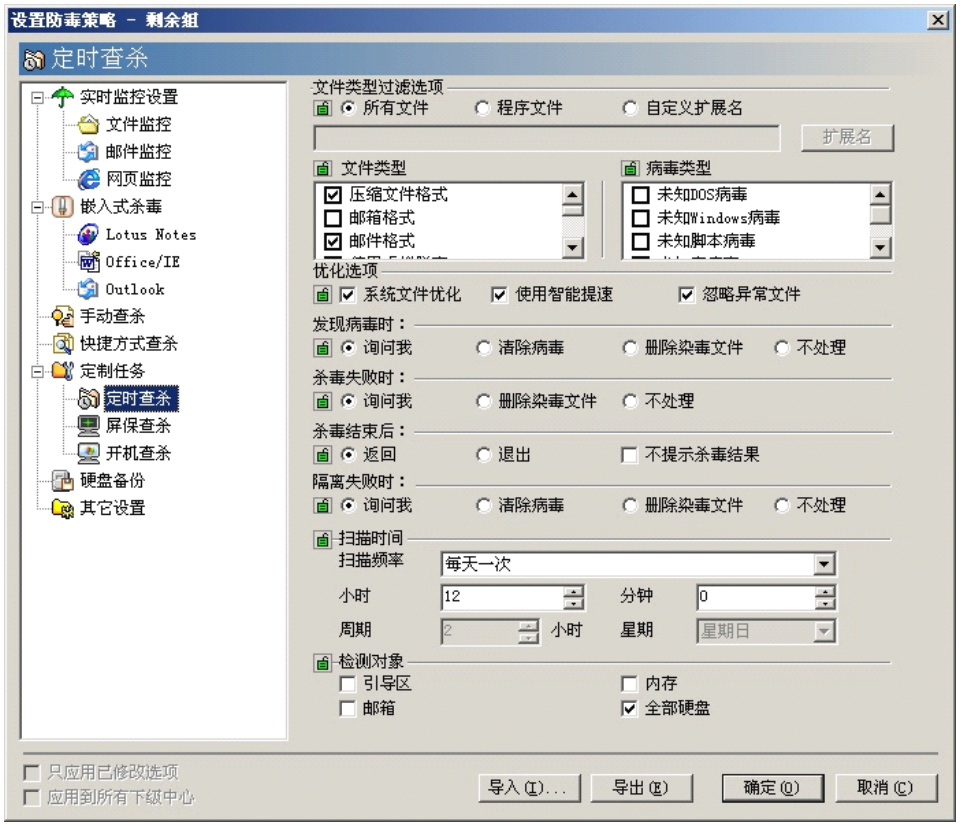

图 441

注意：当系统管理员锁定文件类型、病毒类型和优化选项任意项后，客户端用户通过设置高、中、低级别的滑块设置级别时，仅能修改未被锁定的选项，已经被锁定的选项则不能被修改。

4.1.3.2.13 屏保查杀页面

用户可以为选中的客户端设置屏保查杀功能，具体内容如下：

设置文件类型：可以通过【文件类型过滤选项】自定义文件类型。并可以在文件类型和病毒类型中勾选不同类型的文件。

设置优化选项：可以通过系统文件优化、使用智能提速和忽略异常文件三种方式优化和提高查杀病毒速度并且提高引擎的稳定性。

设置发现病毒时、杀毒失败时、杀毒结束后和隔离失败时的处理方式。

屏保查杀检测对象：可以选择引导区、内存、邮箱和全部硬盘四种检测对象。

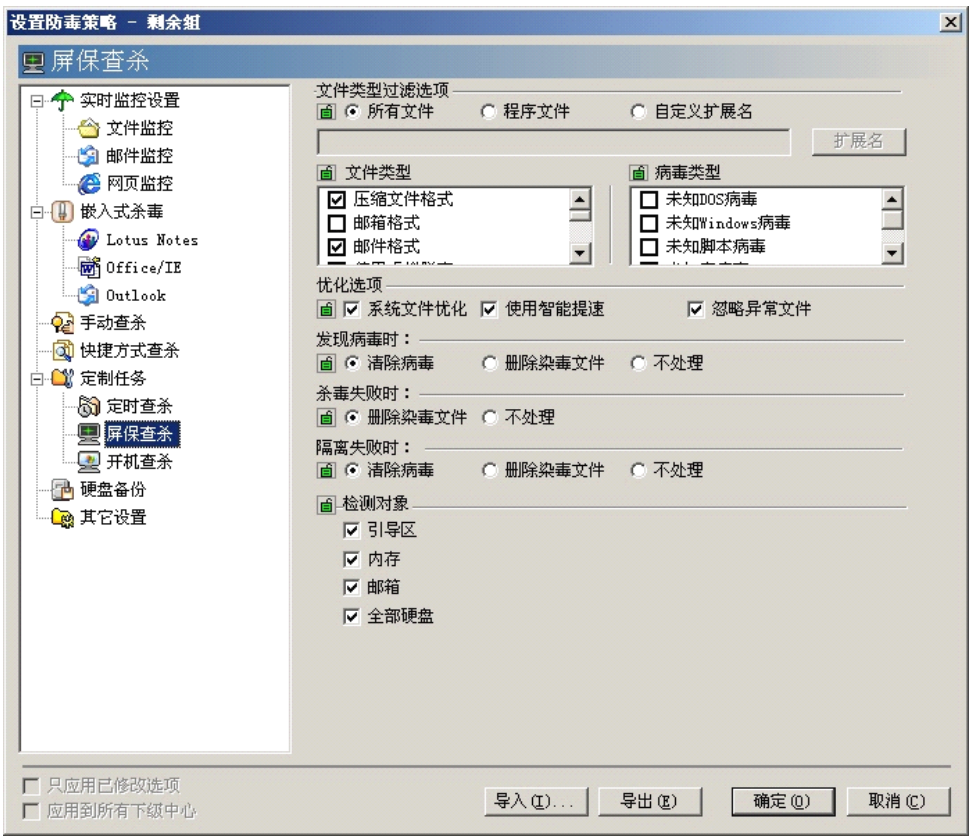

图 442

注意：当系统管理员锁定文件类型、病毒类型和优化选项任意项的时候，在客户端通过设置高、中、低级别的滑块设置级别时，仅修改未被锁定的选项，已经被锁定的选项则不能被修改。

4.1.3.2.14 开机查杀页面

用户可以为选中的客户端设置开机查杀的指定位置，分别为系统盘、Windows 系统目录、所有的硬盘、所有的服务和驱动四种。

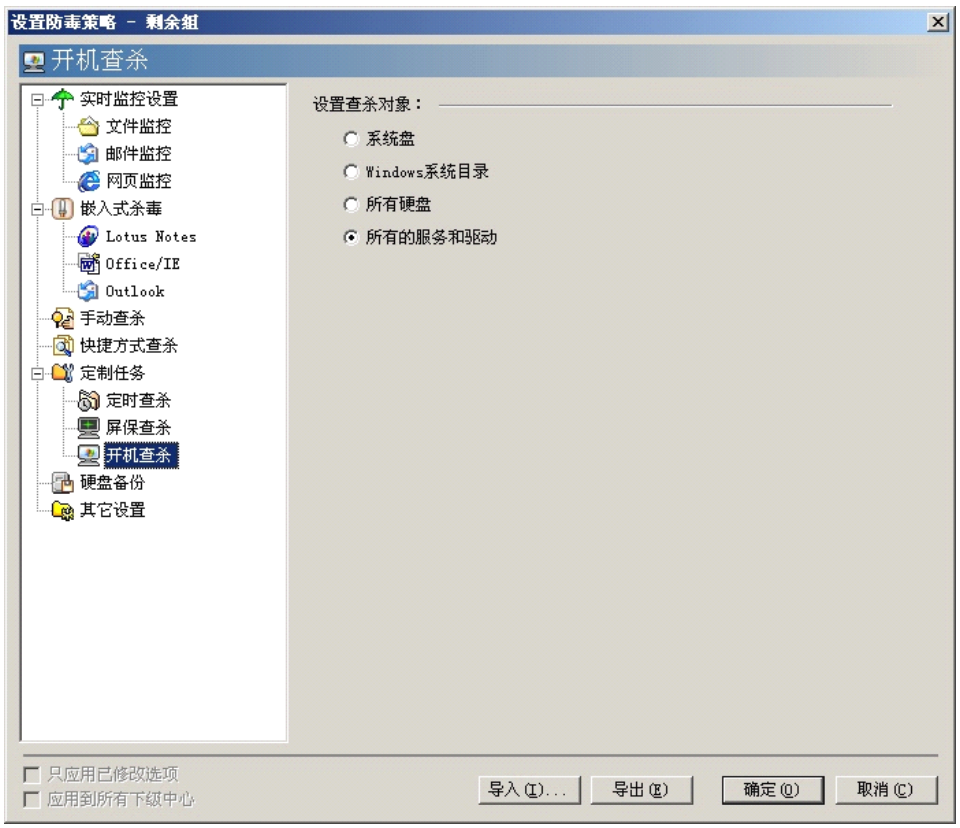

图 443

4.1.3.2.15 硬盘备份页面

说明：在企业专用版和高级企业专用版中，购买时定制了硬盘备份功能的情况下有此设置页面；网吧版中无硬盘备份功能，故无此设置页面；中小企业版、企业版和高级企业版中有此设置页面。

用户可以在此设置硬盘备份频率，分别为不备份、每小时一次、每天一次、每周一次和每周期一次五种。

图 444

4.1.3.2.16其它设置页面

说明：在企业专用版和高级企业专用版中，购买时定制了瑞星助手功能的情况下有【显示瑞星助手】设置项；网吧版中无瑞星助手功能，故无此设置项；中小企业版、企业版和高级企业版中有此设置项。

在其它设置页面中，用户可以为选中的客户端设置使用声音报警、保存历史记录、日志记录天数、向瑞星病毒疫情监测网上报查杀记录、显示瑞星助手（小狮子卡卡）、将染毒文件备份到病毒隔离系统、显示信息中心、多扩展名提示、U 盘监控和在登录系统前显示监控状态等。其中，向瑞星病毒疫情监测网上报查杀记录、将染毒文件备份到病毒隔离系统、在登录系统前显示监控状态三项为带锁选项，系统管理员可以通过设置，防止客户端用户对这几项随意修改。

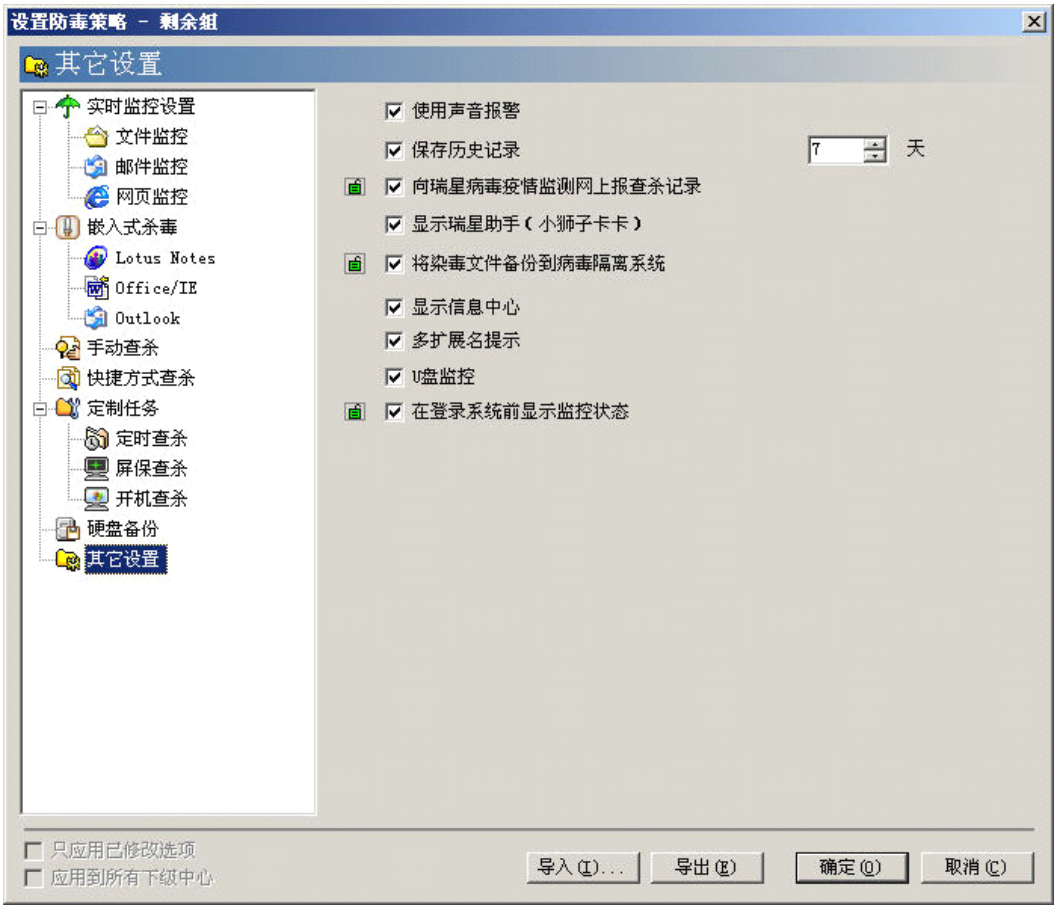

图 445

4.1.3.3设置客户端选项

打开管理控制台，选中一个设置对象，然后选择【操作】/【设置客户端选项】（或在工具栏上单击  按钮，或在设置对象上单击右键选择【设置客户端选项】），弹出【设置客户端选项】界面。

设置客户端选项对话框包含八个标签：【基本设置】、【日志上报设置】、【报告防火墙事件设置】、【定时升级设置】、【下载中心设置】、【漏洞扫描设置】、【升级代理设置】和【其它设置】。

【应用到所有下级中心】：勾选此项将设置同时应用到所有下级中心

【只应用已修改选项】：只应用修改选项，可以减少客户端同步策略的网络传输量

【导入】：单击此按钮弹出“导入缺省配置”和“从文件中导入”两种导入方式，可以导入缺省配置，将设置还原为出厂设置，还可以将*.ocf 格式文件导入，用于还原备份的配置，能够快速应用相同设置，避免了手工设置的麻烦

【导出】：单击此按钮将设置窗口内所有参数信息导出为*.ocf 格式文件，作为当前配置的备份

4.1.3.3.1 基本设置

为了避免客户端用户人为地关闭实时监控程序或卸载杀毒程序，防止客户端随意更改管理员设置的查杀策略，造成整体防毒体系的漏洞，可以在客户端基本设置页面为客户端设置保护密码。在基本设置页面还可以指定系统中心 IP 和端口。如需绑定 RavService 端口范围，在该选项前的复选框中勾选，输入端口范围。

图 446

4.1.3.3.2 日志上报设置

在日志上报设置页面中，可以设置日志上报方式，包括实时上报和每隔 X 分钟上报，这样管理员便可以实时地得到病毒和主动防御信息，并及时处理。其中上报的日志包括病毒日志和主动防御日志。

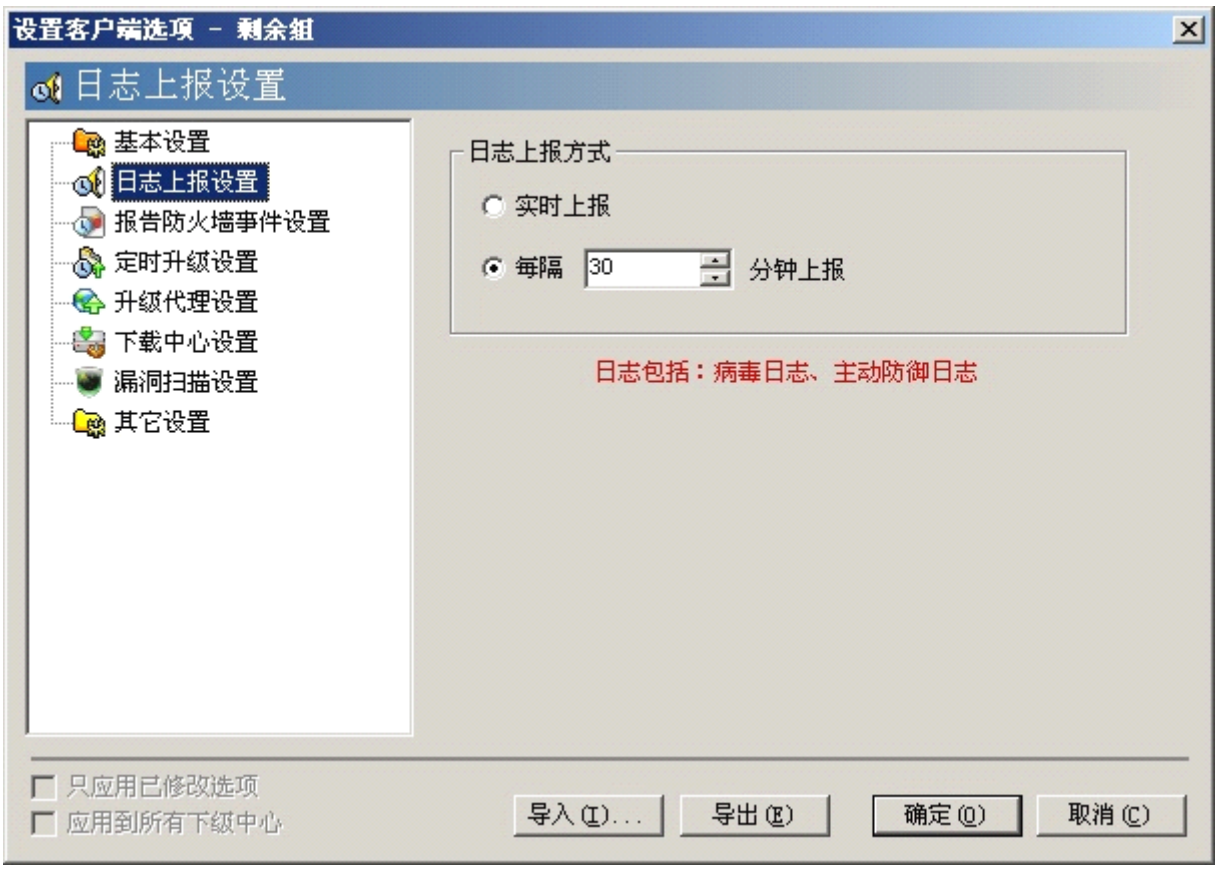

图 447

4.1.3.3.3 报告防火墙事件设置

说明：在高级企业版中可以设置报告防火墙事件；在高级企业专用版中，购买时定制了防火墙功能的情况下可以设置报告防火墙事件；网吧版、中小企业版、企业版和企业专用版中没有此设置页面。

在报告防火墙事件设置页面中，可以设置定时报告事件的频率，分别为实时报告、每天、每周和每月。

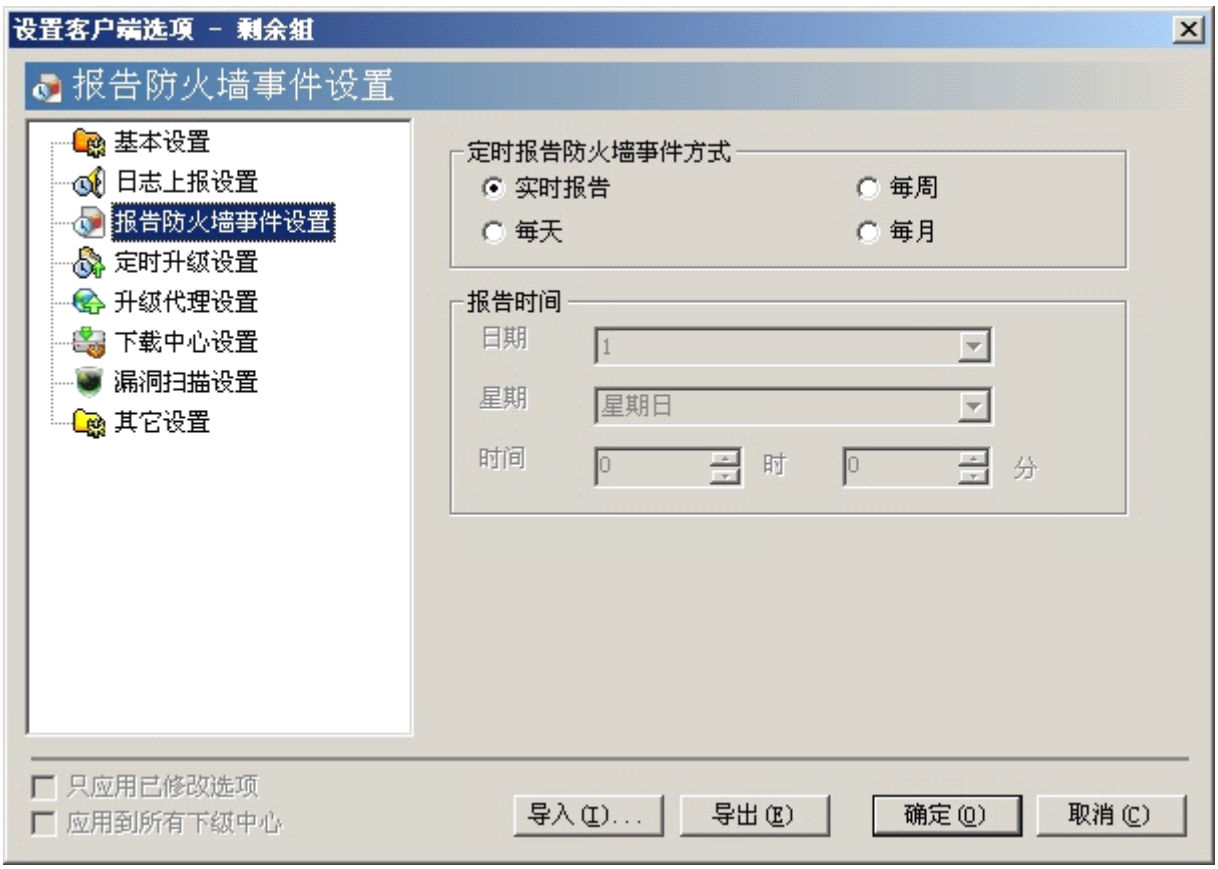

图 448

4.1.3.3.4 定时升级设置

在该页面可以设置该客户端的升级频率及升级时间，可以选择【只升级病毒特征库】及【静默升级模式】。选择【只升级病毒特征库】则只是升级病毒特征库，选择【静默升级模式】则使得客户端在不影响用户正常工作的情况下进行升级。

图 449

4.1.3.3.5升级代理设置

用户指定了升级代理后，当客户端进行升级的时候，会按照升级代理列表中的顺序寻找升级代理，即首先找第一个升级代理，如果该升级代理不能使用时候则寻找下一个升级代理，依此类推，直到找到一个可以使用的升级代理。如果找不到任何升级代理，便从系统中心进行升级。如何添加升级代理请参考 4.1.7.2 客户端升级中的通过代理升级。

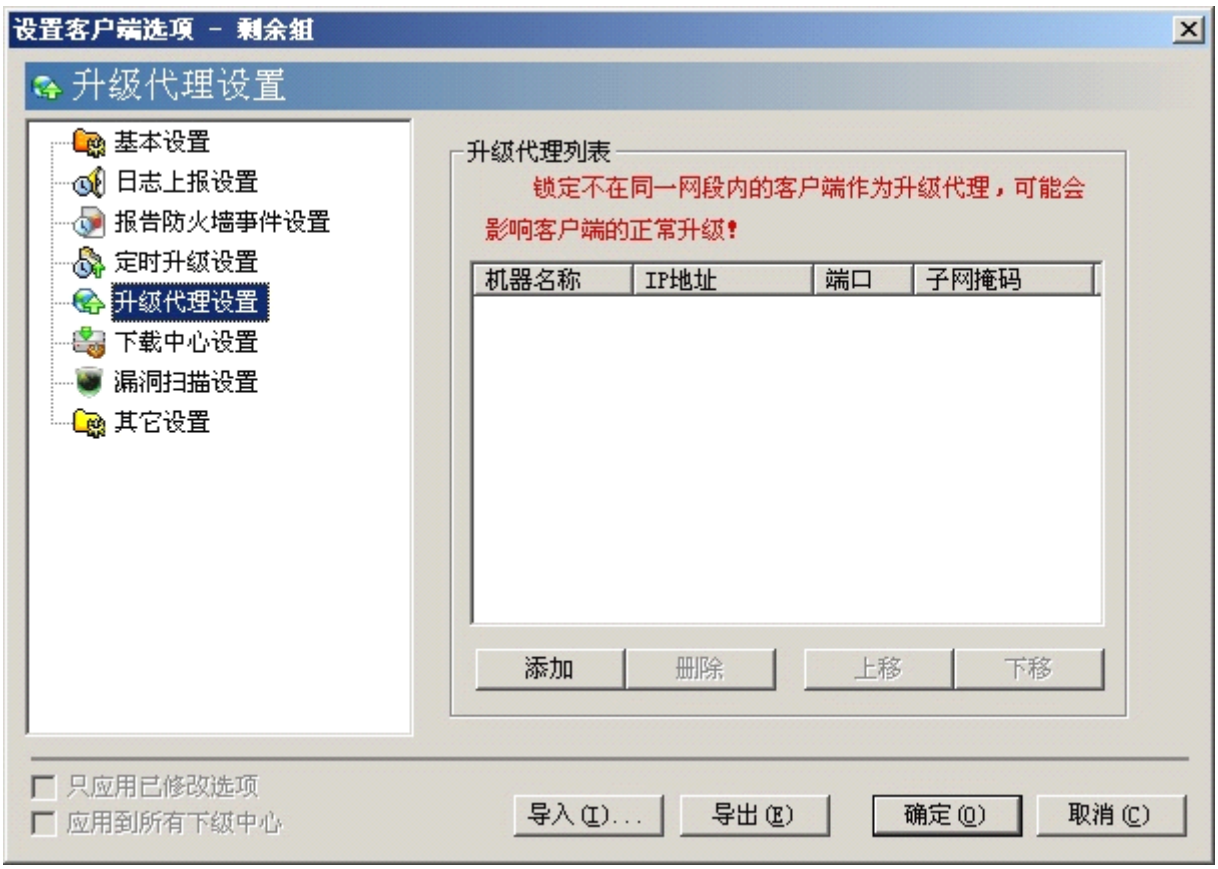

图 450

4.1.3.3.6 下载中心设置

在下载中心设置页面，可以设置下载中心的清理频率、具体清理时间，还可以通过设置升级文件保留组件的版本数及漏洞补丁文件最大使用硬盘空间的大小来避免无用文件占用过多硬盘空间，从而减少磁盘空间的占用。

图 451

4.1.3.3.7 漏洞扫描设置

说明：在企业专用版和高级企业专用版中定制漏洞扫描功能的情况下有此设置页面；网吧版没有漏洞扫描功能，故无此设置项；中小企业版、企业版和高级企业版中有此设置页面。

在漏洞扫描设置页面，用户可以设置是否启用定时漏洞扫描并且设置扫描频率、设置扫描漏洞的严重级别和是否自动安装补丁程序等。勾选【自动安装补丁程序】客户端将自动运行漏洞补丁程序，未勾选此项则需要在客户端的【系统漏洞】提示框中单击【安装漏洞补丁包】按钮进行手动安装。此项默认为不选中。

当选择【自动安装补丁程序】后，可以选择是否采取静默安装的方式，勾选【静默安装】则可在不干扰用户正常工作的情况下自动进行安装。

图 452

4.1.3.3.8 其它设置

在其它设置页面中，可以对客户端向系统中心报告状态的时间间隔、数据包大小、超时时间设置、消息框显示方式进行设置。

通过数据包大小设置，可以任意调整数据包大小（最大 64K），此功能能够方便窄带网络用户客户端和下级中心的升级。数据包大小设置建议：10M 以上带宽建议设置为 65535 字节，64K 至 10M 之间带宽建议设置为 4096 字节，64K 以下带宽建议设置为 512 字节。

超时时间设置：设置客户端与其它模块的通讯超时时间，根据网络状况设置适当的通讯超时时间保障通讯质量。

勾选【记录应用程序在自我诊断级别的运行日志】选项，将记录应用程序的所有级别的运行日志，当瑞星网络版杀毒软件在使用中发生异常时，使用日志打包工具将日志打包后上报给瑞星公司，便于分析人员解决问题。关于如何打包日志，请参见“4.2.7 日志打包工具”。

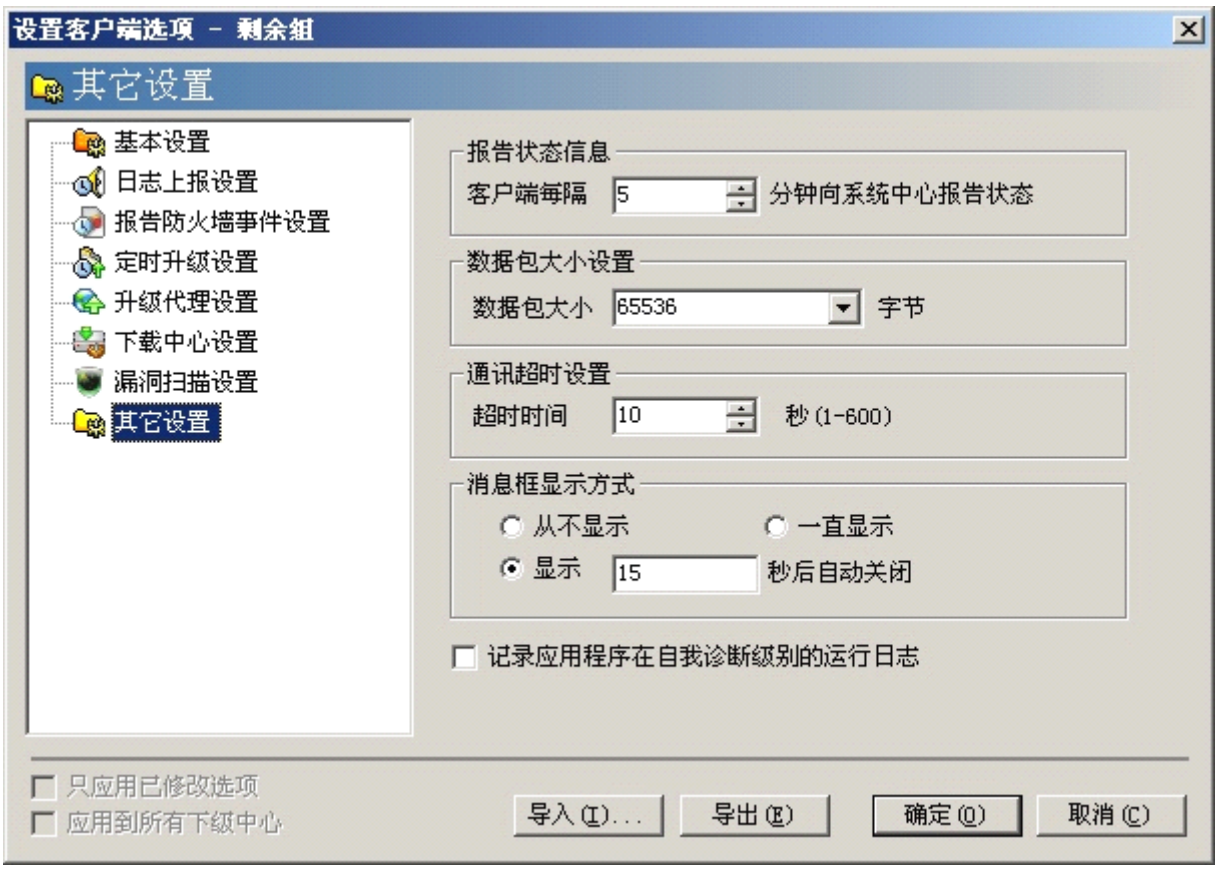

图 453

4.1.3.4设置主动防御规则

管理员可以通过管理控制台远程查看、设置客户端的主动防御选项，设置主动防御组策略，并且上报、查询、统计主动防御的日志。对于可信任的程序，可将其添加到主动防御白名单中。对于已有的主动防御规则，通过【导出】备份规则设置，当客户端需要配置主动防御规则时，也可以通过【导入】/【导入缺省配置】或【从文件中导入】快速导入主动防御规则设置。

红锁/绿锁：“红锁”代表该选项已经被管理员锁定，“绿锁”代表该选项未被管理员锁定，如果管理员锁定了该选项，客户端将无法在本地更改选项，直到远程管理员将该选项解锁，这样管理员可以控制客户端对于选项的更改。

管理员通过管理控制台设置的主动防御规则为被锁定的规则，客户端无法修改。对于客户端用户自定义的规则，可以在客户端被修改，系统管理员在管理控制台只能够开启或者关闭客户端用户设置的规则，不可以修改该规则。

注意：Windows 9X、NT 和所有 64 位操作系统不支持主动防御功能。对于不支持主动防御功能或没有安装主动防御的客户端，该功能设置项无效。

【应用到所有下级中心】：勾选此项将设置同时应用到所有下级中心，此项设置只有对系统中心进行设置时才生效。

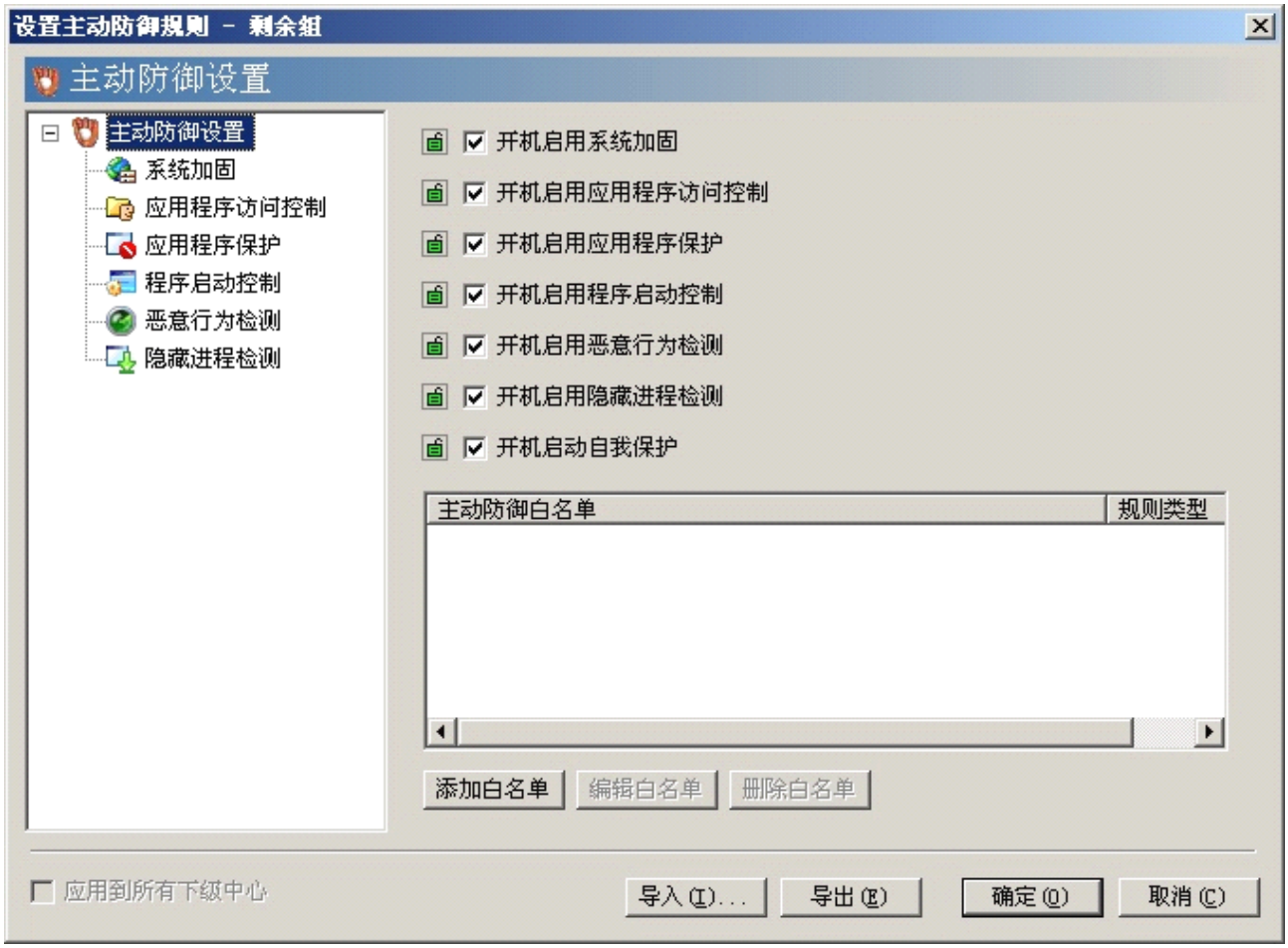

图 454

注意：具体规则设置参见 5..9.3 设置主动防御规则。

4.1.3.4.1 系统加固

系统加固是通过对系统动作监控、注册表监控、关键进程保护和系统文件保护，防止未知程序对系统进行破坏。用户还可以选择是否记录日志、当触发规则时提示用户的界面是详细信息还是简要信息。点击页面上方的【锁定系统加固】项，将锁定系统加固设置，此时绿锁会变成红锁，客户端将没有更改该功能的权限。

具体规则设置参见 5.9.3.1 系统加固设置。

图 455

注意：当系统管理员在管理控制台锁定系统动作监控、注册表监控、关键进程保护和系统文件任意项的情况下，客户端通过系统加固的【自定义级别】按钮可以查看锁定项设置的情况，被锁定的项前面带“灰色的锁”图标，故无法对右侧对应的规则进行设置，也将不会出现设置级别的滑块。未被锁定的项前面没有“灰色的锁”图标，用户可以通过【自定义级别】按钮进行设置其右侧对应的规则。

4.1.3.4.2 应用程序访问控制

应用程序访问控制是对用户指定的应用程序进行监控，一方面可以限制其访问范围，另一方面可以对重要的服务程序进行加固。指定应用程序可以设置为用户认为可疑的应用程序，通过规则设置了解其访问计算机资源情况，调查其是否包含恶意代码。

具体规则设置参见 5.9.3.2 应用程序访问控制设置。

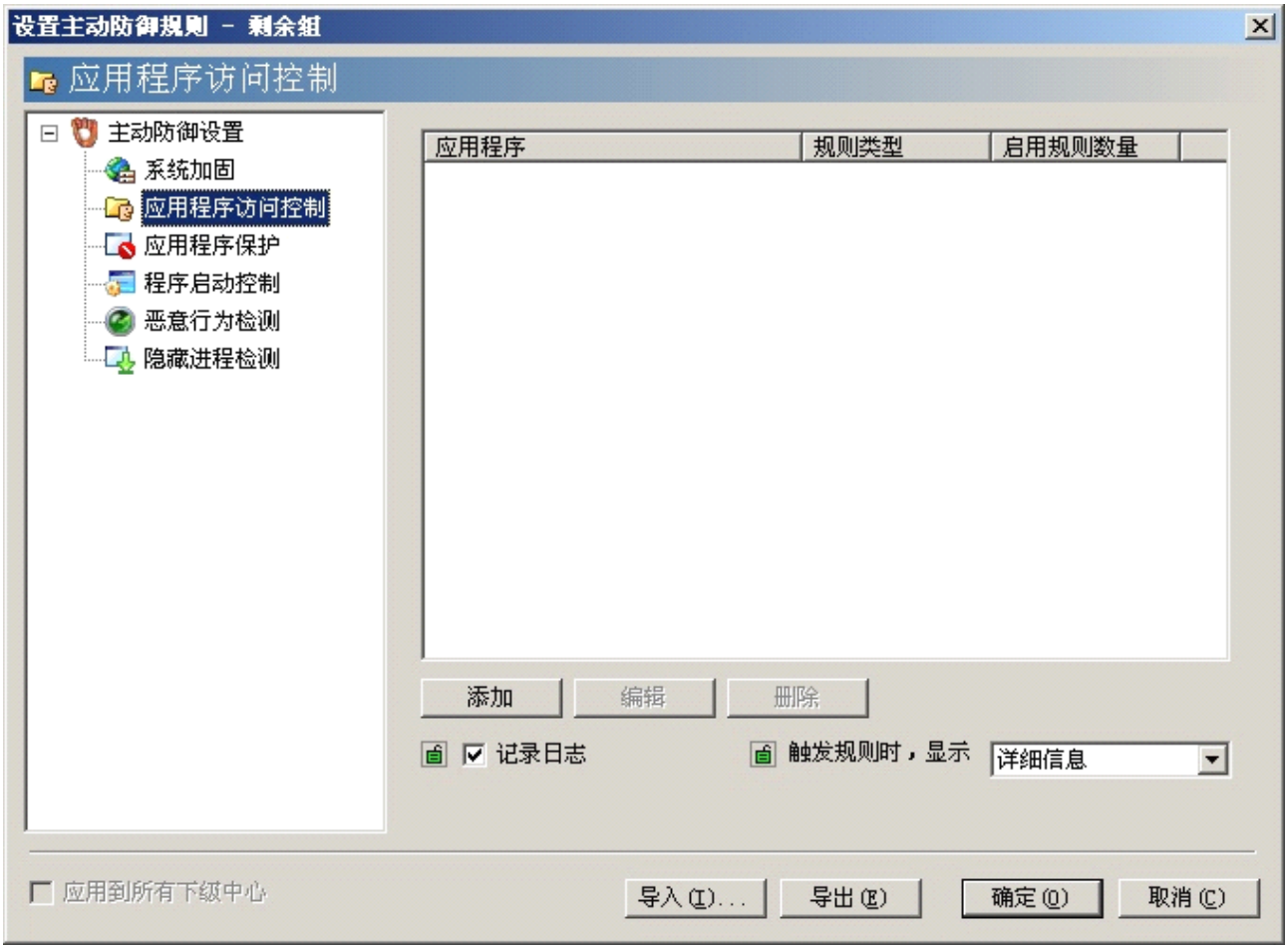

图 456

单击【添加】按钮，打开【应用程序访问控制-添加规则】页面，如图：

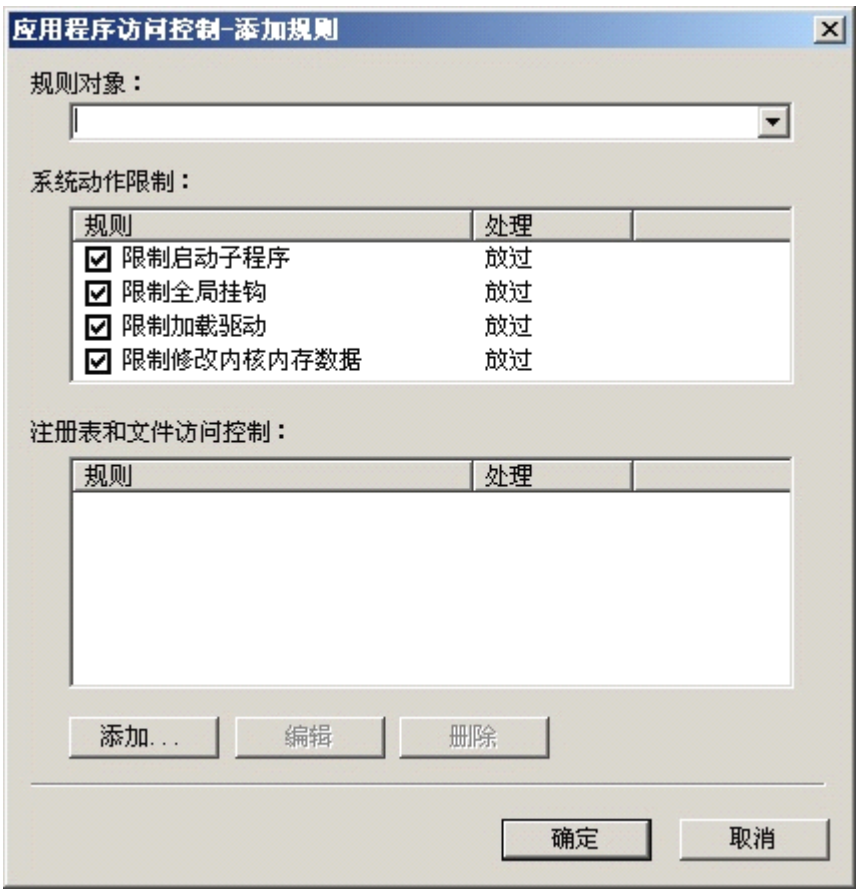

图 457

注意：用户选择规则对象时，会提供给用户一些宏路径的选择，具体含义如下：

宏路径	含义
*	所有目录和文件
%WINDIR%	windows 目录
%SYSDIR%	system32 目录
%PROGRAMDIR%	系统安装文件目录
%COMMONDIR%	安装文件目录的公共目录，例如c:\Program Files\Common Files
%FIRSTPART%	操作系统第一个分区
%DOMINODATA%	domino 数据目录
%DOMINODIR%	domino 安装目录
%NOTESDIR%	notes 的安装目录

4.1.3.4.3 应用程序保护

应用程序保护可以保护指定的应用程序不被恶意程序攻击。用户可以添加游戏软件、即时通讯软件等，对它们进行保护。勾选【被保护的程序启动时提示】，当被保护的程序启动时提示用户。

具体规则设置参见 5.9.3.3 应用程序保护设置。

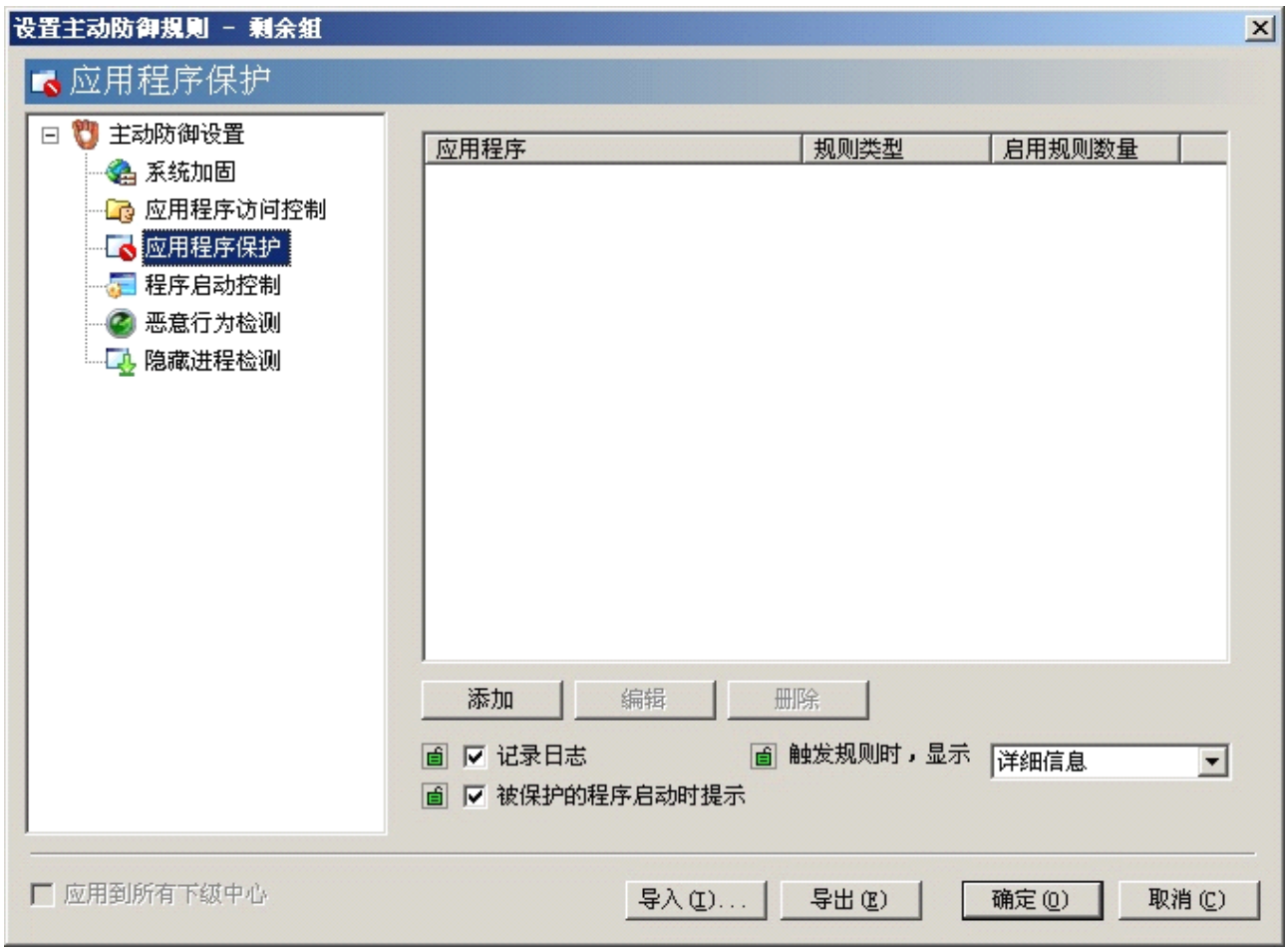

图 458

4.1.3.4.4 程序启动控制

程序启动控制功能允许用户监控指定可疑程序的启动过程，有助于阻止并截获未知恶意程序，并用于发现指定的应用程序是否被篡改。

具体规则设置参见 5.9.3.4 程序启动控制设置。

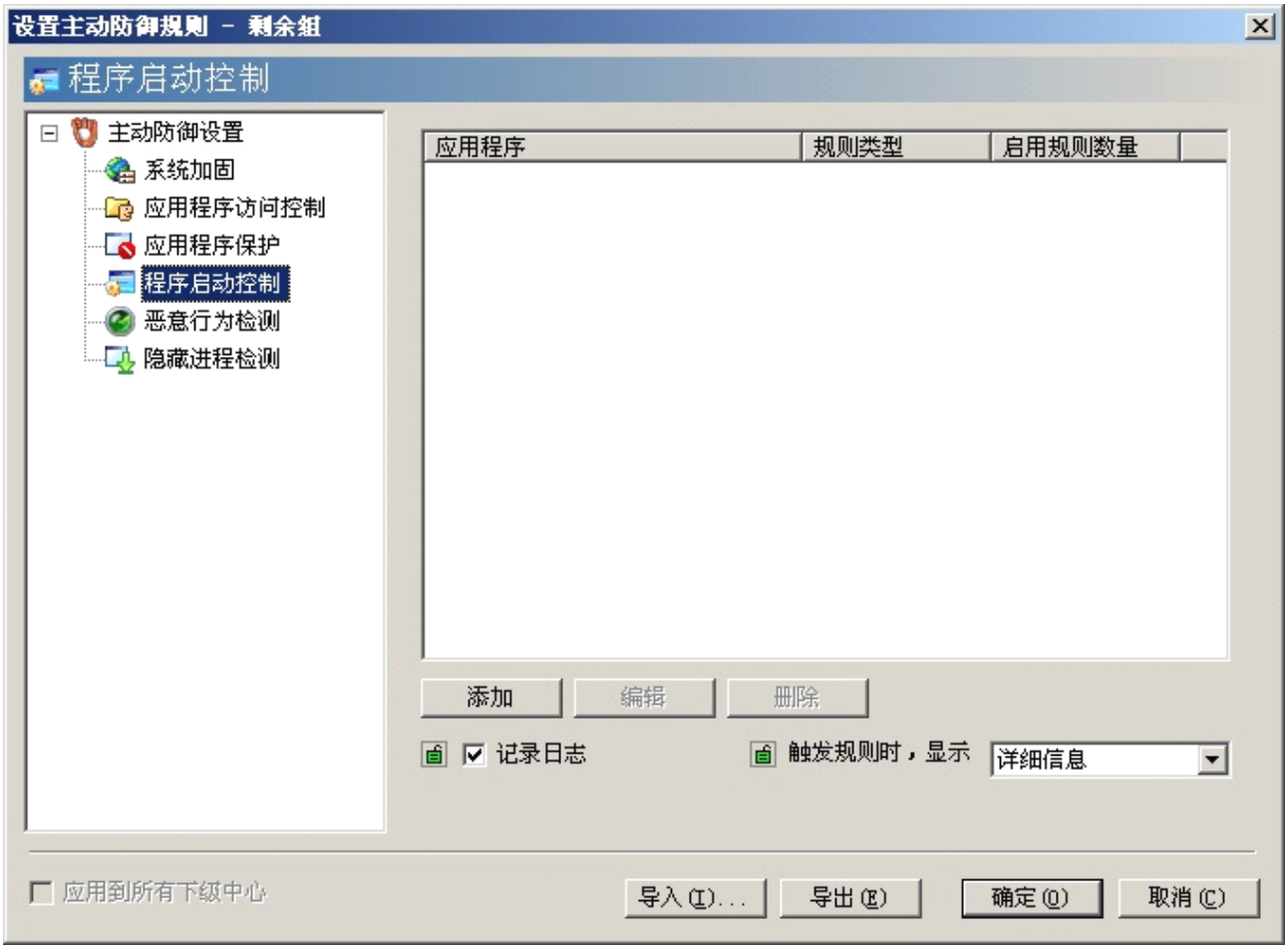

图 459

4.1.3.4.5 恶意行为检测

恶意行为检测能够对系统中的程序进行监控，根据行为检测报告发现可能包含恶意代码的应用程序。用户可以设置恶意行为启发式检测敏感度、发现程序检测恶意行为时的处理方式、是否记录日志、在进程退出时是否进行家族病毒 DNA 扫描。

具体规则设置参见 5.9.3.5 恶意行为检测设置。

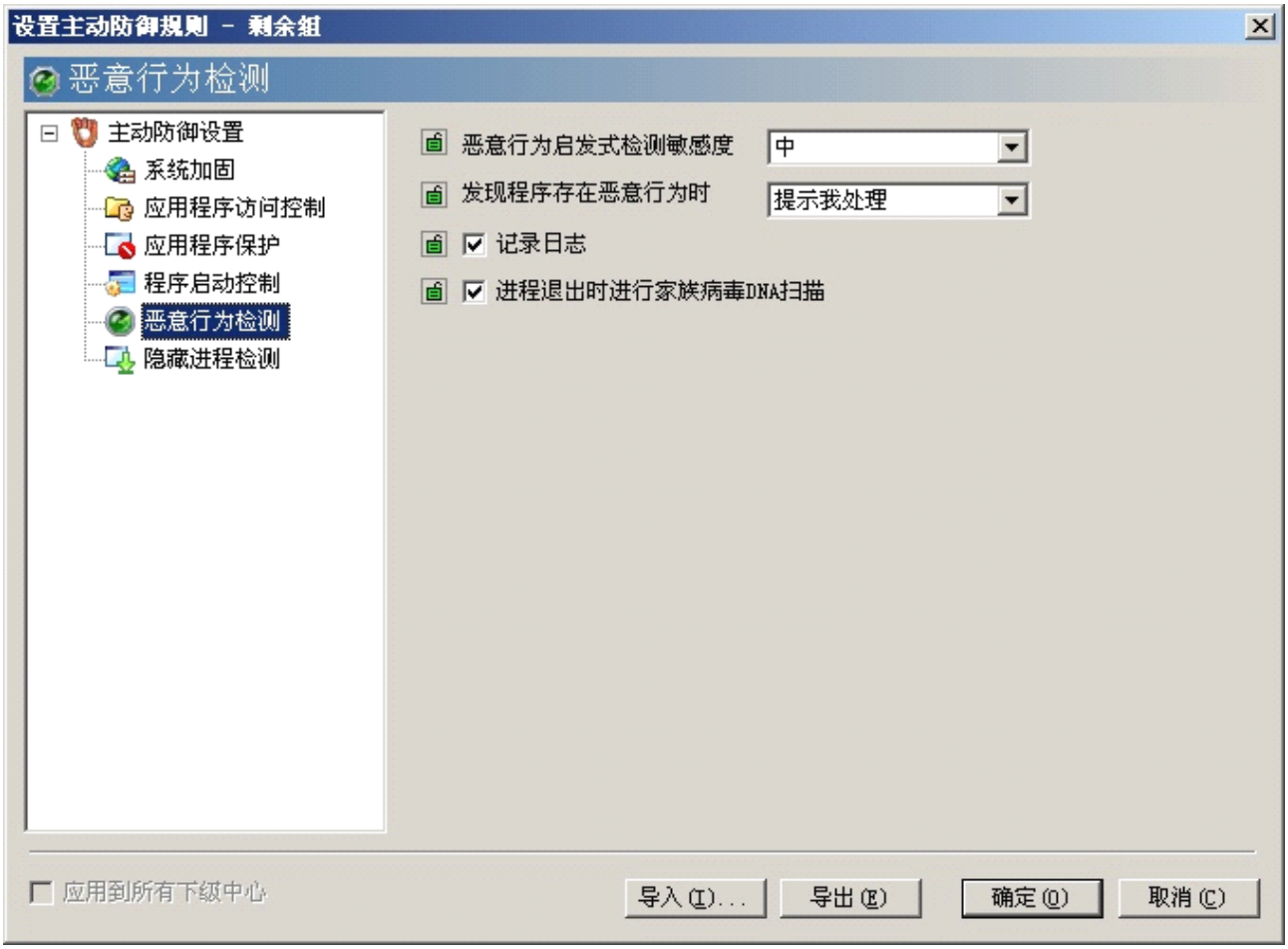

图 460

4.1.3.4.6 隐藏进程检测

隐藏进程检测可以检测“任务管理器”中无法查看的进程，被隐藏的进程很有可能是包含恶意代码的应用程序。用户可以设置自动检测间隔、是否记录日志和发现隐藏进程时是否显示警告信息。

具体规则设置参见 5.9.3.6 隐藏进程检测设置。

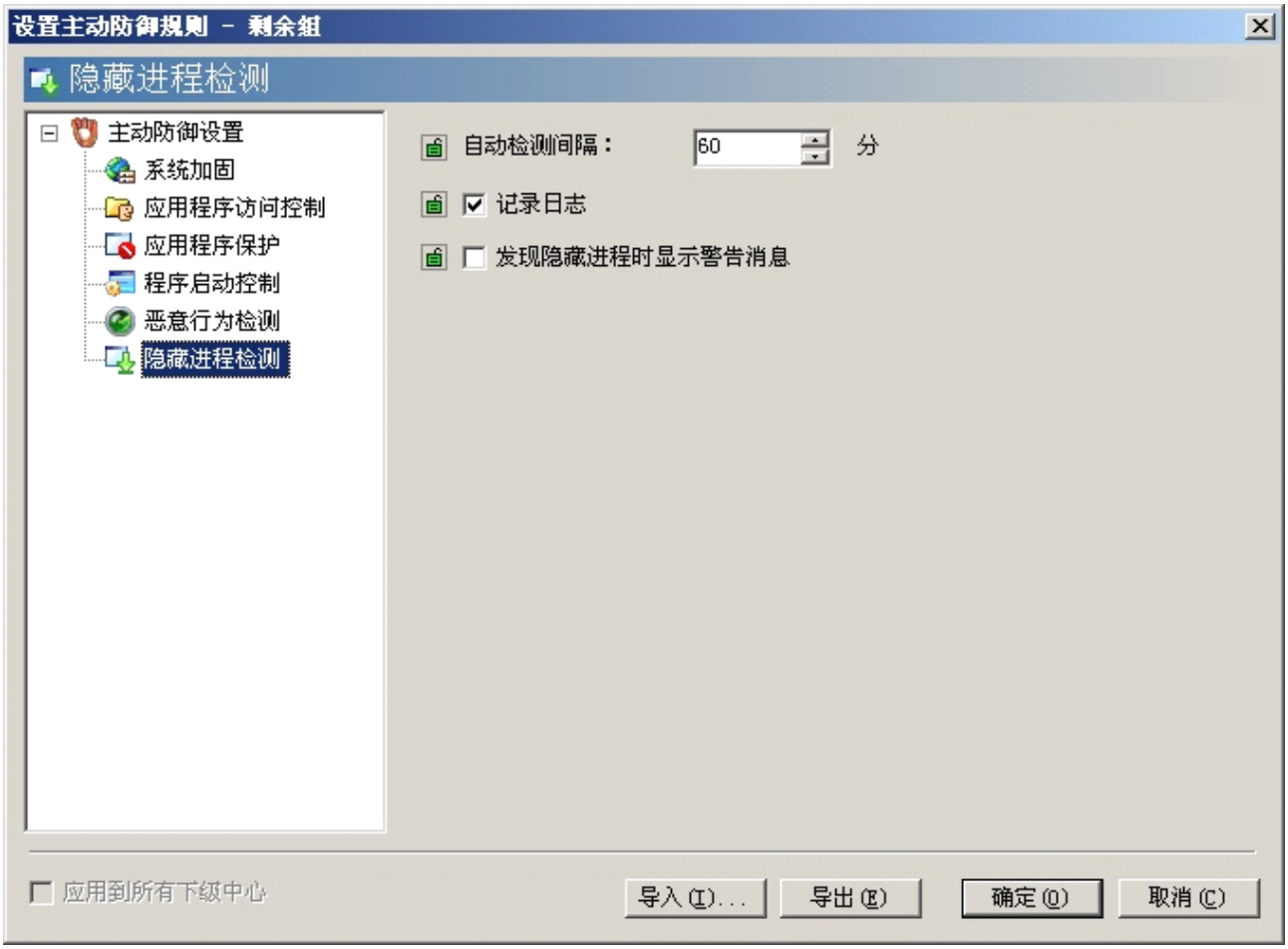

图 461

4.1.3.5防火墙规则设置

说明：在高级企业版中可以设置防火墙规则；在高级企业专用版中定制了防火墙功能的情况下能够设置防火墙规则；网吧版、中小企业版、企业版、企业专用版中无此设置页面。

在防火墙规则设置页面可以为指定的客户端设置 IP 规则以及是否开机后启用防火墙功能。

4.1.3.5.1IP 规则

在 IP 规则页面中可以为选中的客户端设置 IP 规则，其中可以通过下列的按钮添加、删除、插入、编辑、上移和下移规则。

图 462

4.1.3.5.2 选项

在选项页面中可以为指定客户端设置是否开机启用防火墙，但是首先必须在管理控制台远程开启客户端防火墙后该设置才生效。

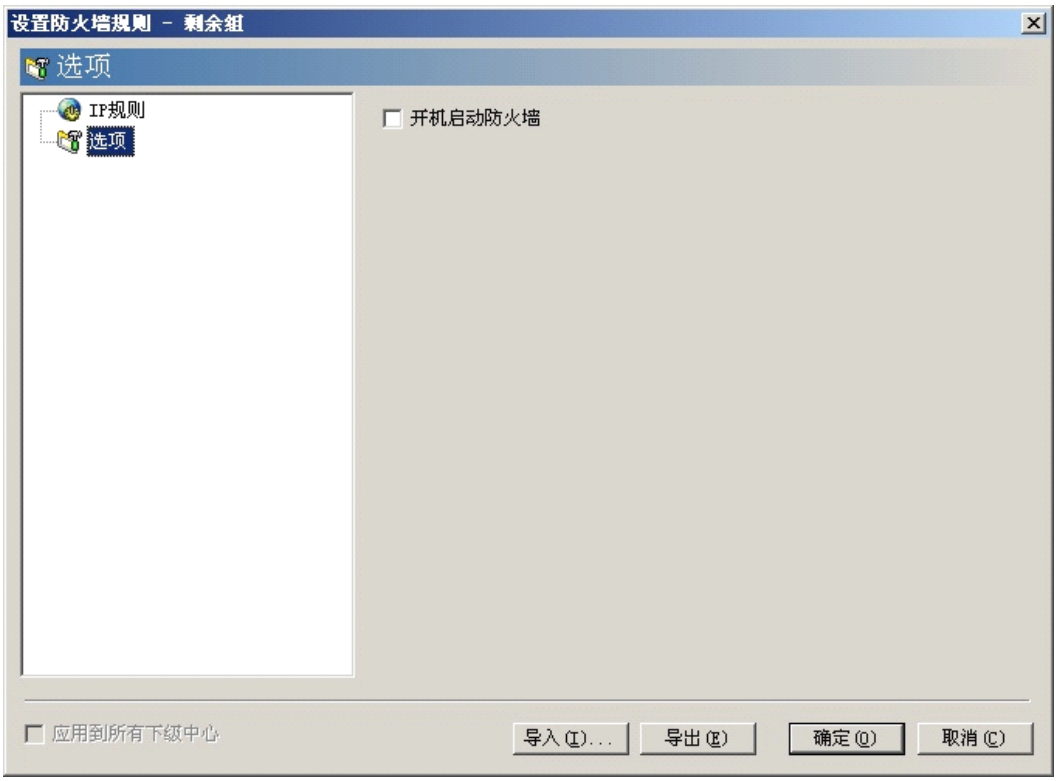

图 463

4.1.3.6系统中心设置

在管理控制台的组管理界面上选中一个系统中心，单击右键选择【系统中心设置】，弹出【系统中心设置】界面。

系统中心设置包含以下标签：【系统中心设置】、【网络设置】、【升级设置】、【黑白名单设置】、【漏洞扫描设置】、【对象端口设置】。

4.1.3.6.1 系统中心设置

在系统中心设置页面中，可以设置是否指定系统中心 UDP 监听 IP，当系统中心有多个 IP 地址，只想要管理一个网段上的客户端，则使用此项设置，单击下拉按钮选择想要监听的 IP 地址，则只有该 IP 地址所在网段内的客户端能够通过发 UDP 数据包找到此系统中心。

为了提高软件性能，节约硬盘空间，建议定期清理系统中心日志信息，在此页可以设置使用自动清除病毒日志、事件日志、漏洞信息、防火墙事件日志和主动防御日志功能，在相应的选项前勾选后，可以设定日志时间范围。用户还可以选择自动清除长时间未激活的客户端信息，以及修改系统中心显示名称。

说明：在高级企业版中“自动清除防火墙事件日志信息”设置项有效；在高级企业专用版定制了防火墙功能的情况下该设置项生效；网吧版、中小企业版、企业版和高级企业版中此设置无效。

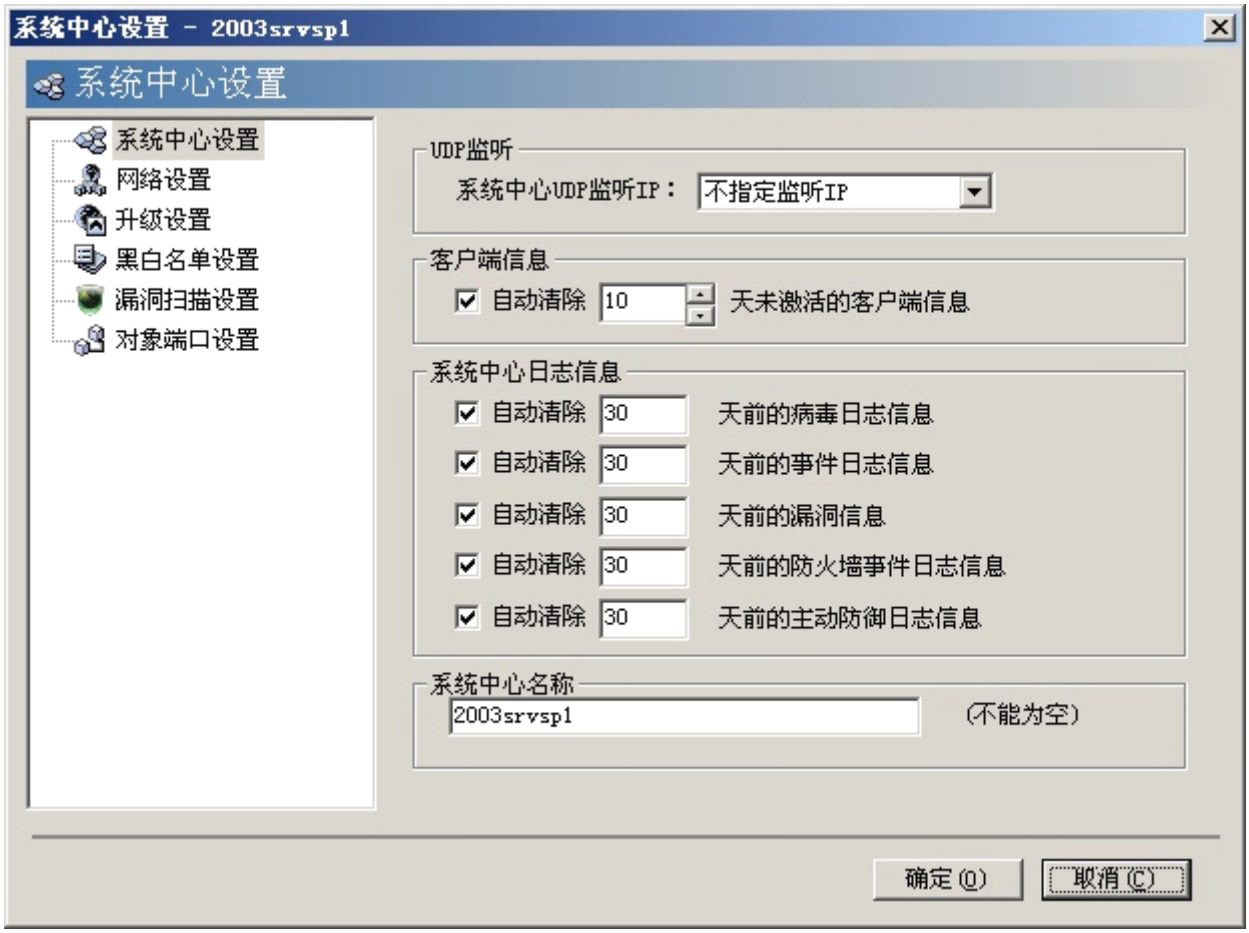

图 464

4.1.3.6.2 网络设置

在网络设置页面中，可以选择系统中心连接 Internet 的方式，包括不能连接 Internet、局域网（LAN）或专线上网、通过代理服务器（Proxy）上网三种方式。若选择【通过代理服务器（Proxy）上网】，还需要输入进一步配置代理服务器，当需要验证时，可以在此处设置用户名和密码。

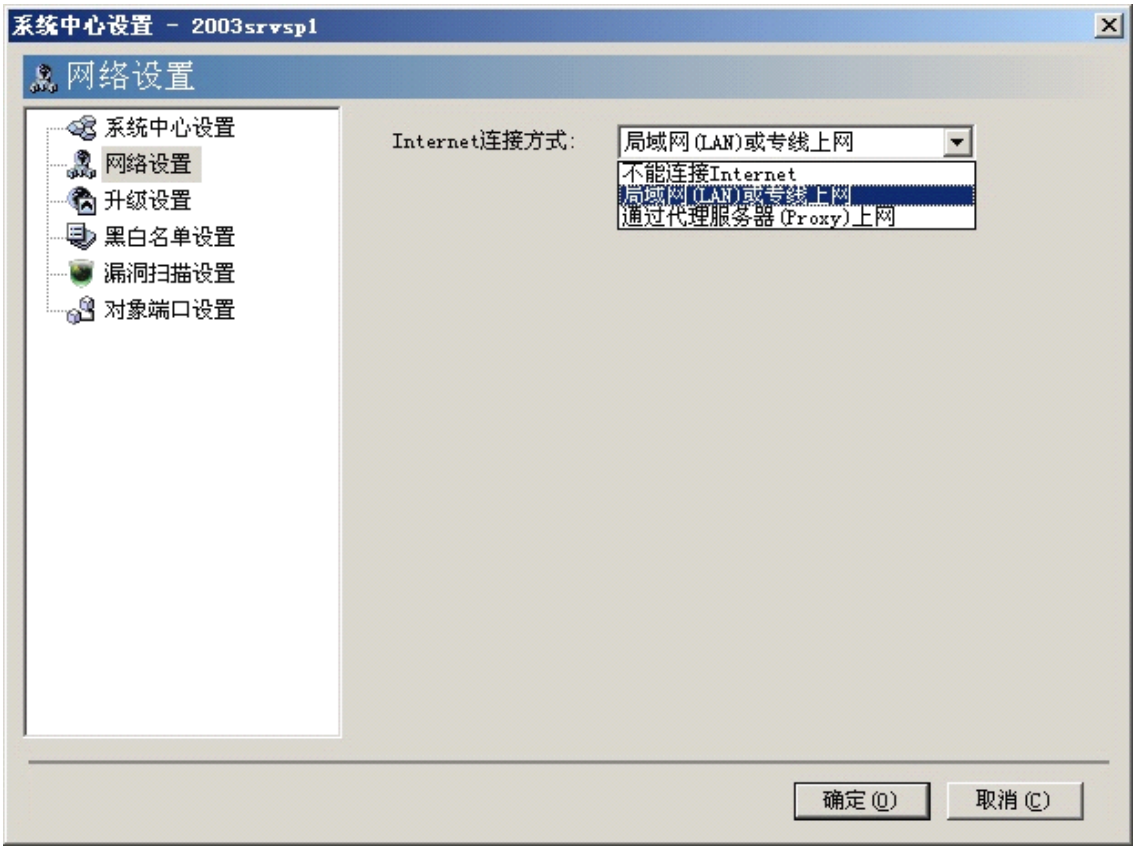

图 465

4.1.3.6.3 升级设置

在升级设置页面中，可以设置用户 ID、系统中心升级方式、升级频率、指定升级时间、选择是否使用静默升级、是否启用客户端作为升级代理功能、是否启用自动生成升级文件的智能压缩文件。

用户 ID 设置：在进行升级之前需设置用户 ID，用户同样可以在管理控制台的【管理】/【设置本中心用户信息】/【设置用户 ID】进行设置。

升级方式：

用户还可以对系统中心升级方式进行设置，选项包括自动升级、从上级中心升级、从网站智能升级、从网站下载手动升级包。

- 自动升级：先尝试从上级中心获取升级文件，如果没有上级系统中心将从网站上获取升级文件；
- 从上级中心升级：系统中心从上级中心获取升级文件，不尝试其它升级方式，多级系统中心和超级系统中心架构的所有下级系统中心适合采用此种升级方式；

- 从网站智能升级：系统中心直接通过 Internet 获取升级文件，此种方式适用于系统中心能方便的连接互联网的情况；
- 从网站下载手动升级包：先从网站上获取手动升级包，然后通过手动升级操作升级。如果选择从网站下载手动升级包，则需要选择手动升级包的保存位置。若勾选【下载完后运行手动升级包】，升级包下载完成后将自动运行；

用户还可以选择定时升级方式升级，勾选【启用定时升级】选项启用定时升级功能。系统中心将在设定的具体时间内升级，此方法不影响管理员的正常工作，更为方便、快捷、自动化。

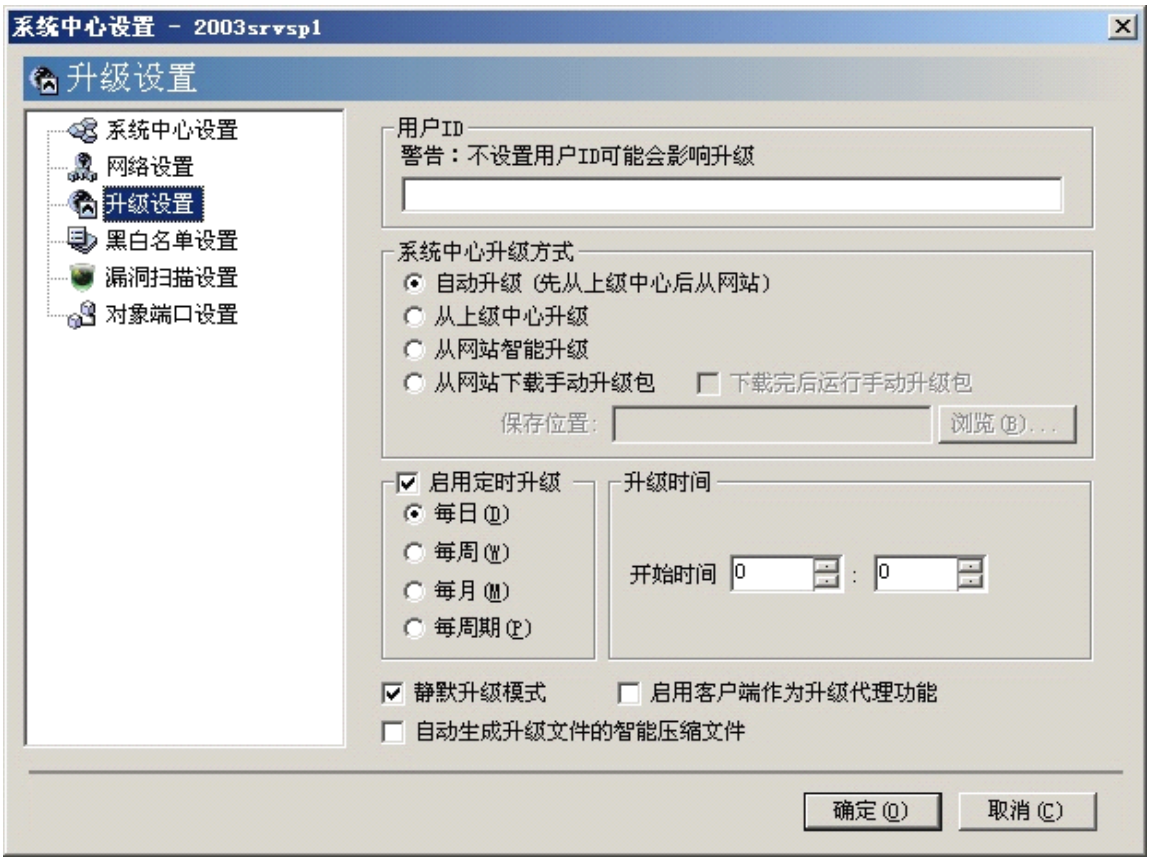

图 466

静默升级是指在升级过程中不显示升级界面，在不干扰用户的情况下自动升级到最新版本。

启用客户端作为升级代理功能：当客户端通过窄带网络从系统中心进行升级时，可以选择客户端作为升级代理。要启用此功能，首先在【启用客户端作为升级代理功能】前面勾选，单击【确定】保存设置，然后在管理控制台上计算机列表中选择要设为升级代理的客户端，单击右键，选择【开启客户端作为升级代理】即可。具体操作详见：4.1.7.2 客户端的升级。

自动生成升级文件的智能压缩文件：勾选此选项后，每次升级时，将把通过增量升级合成的智能压缩文件放到相关目录下，当客户端采用智能升级方式升级时，可以直接从系统中心获取相应的智能压缩文件，从而减少系统中心访问网络的流量。

4.1.3.6.4 黑白名单设置

在黑白名单设置页中，可指定允许或禁止在系统中心注册的 IP 地址。为防止某些非法客户端在本系统

中心注册，本系统中心可把这些非法客户端的 IP 添加到黑名单列表中。

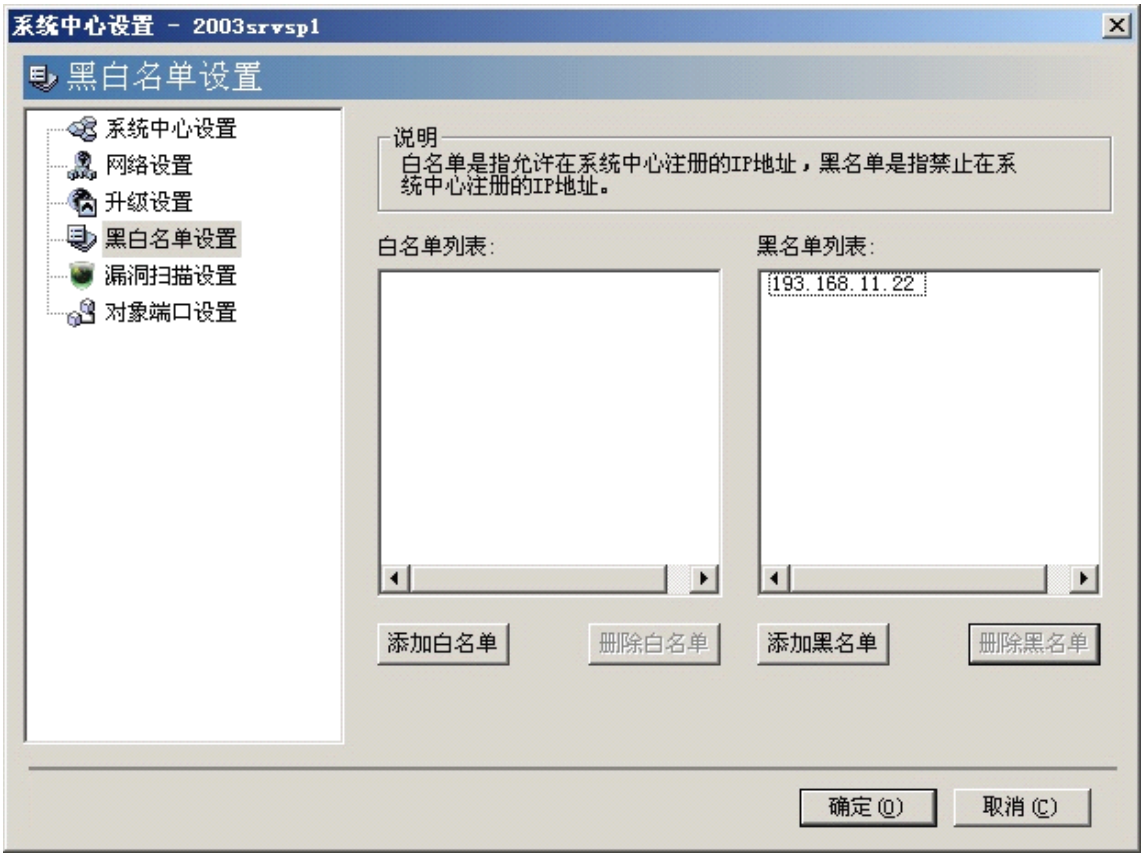

图 467

黑白名单判断逻辑关系说明：若白名单为空，则程序根据黑名单来判断是否允许注册；若白名单存在，先查看对象是否在白名单中，如果不在白名单中，则拒绝注册，如果在白名单中同时不在黑名单中则接受注册，如果在白名单中同时又在黑名单中，则拒绝注册。

4.1.3.6.5 漏洞扫描设置

在漏洞扫描设置页面中，可以对以下选项进行设置：自动下载漏洞补丁程序、自动通知客户端修复已下载的补丁程序。

自动下载漏洞补丁程序：根据漏洞扫描结果，系统中心自动下载相应补丁程序，并保存在补丁共享目录下（通常是\Rav\Patch 目录）；

自动通知客户端修复已下载的补丁程序：当系统中心下载完成某个补丁程序，自动提示具有该漏洞的客户端到系统中心获取补丁程序进行安装。

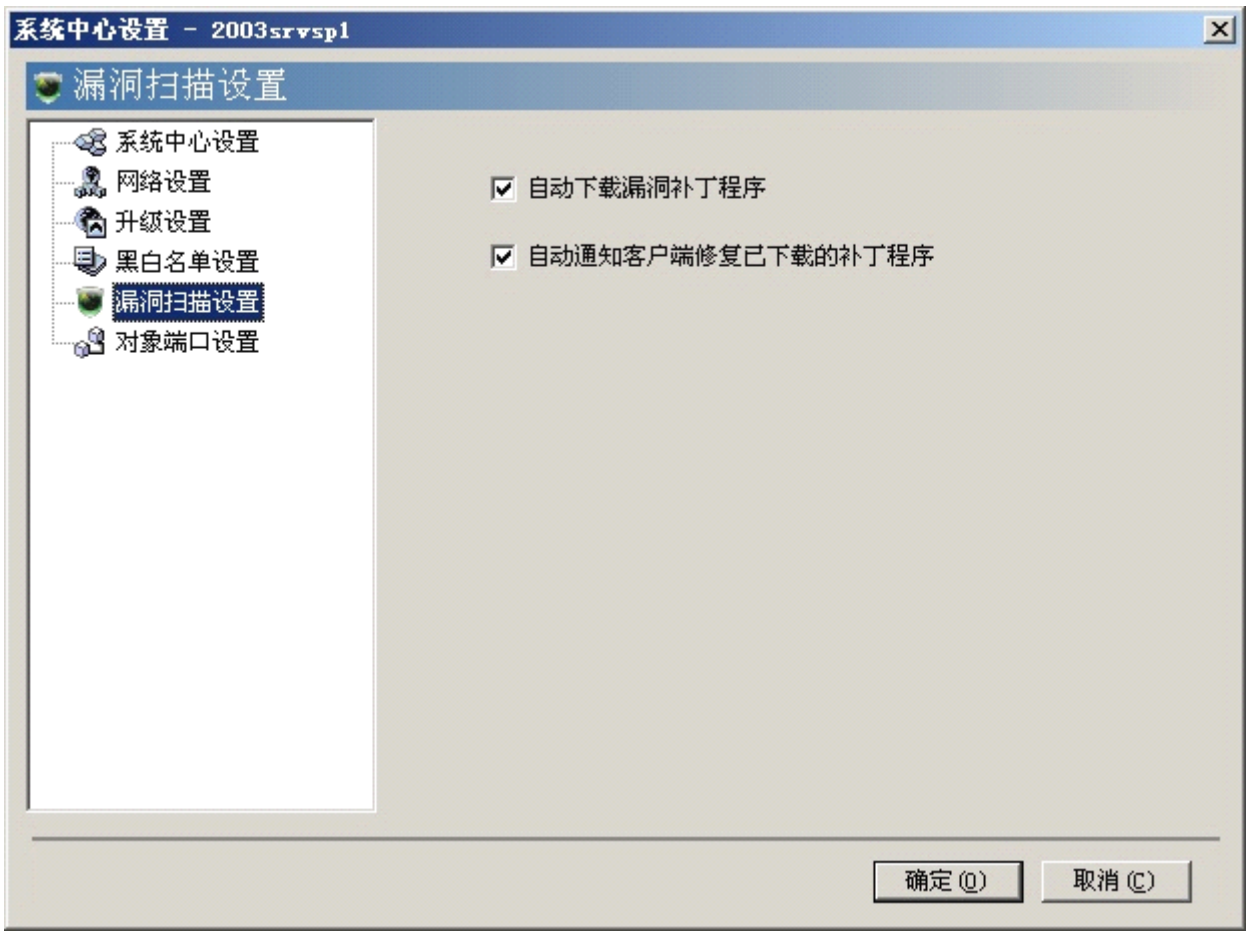

图 468

4.1.3.6.6对象端口设置

设置瑞星程序的监听端口，规范对象端口的使用，使瑞星杀毒软件网络版的通讯数据顺利地通过。

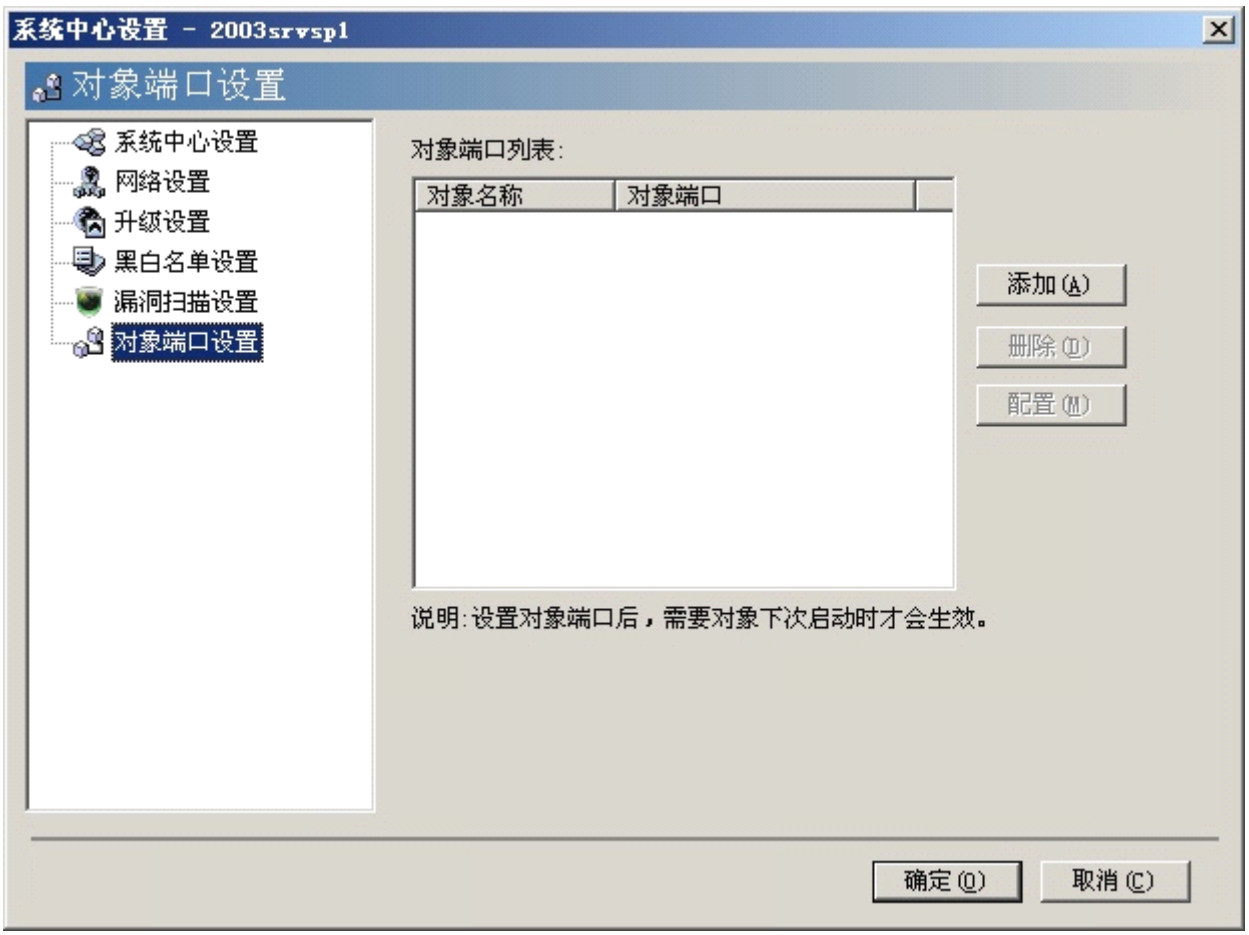

图 469

在对象端口设置页面中，单击【添加】按钮弹出【指定对象绑定端口】窗口，单击【对象名称】下拉箭头可以选择对象名称，在下面输入端口号，或勾选【端口范围】，输入对象端口的绑定范围（起始端口和终止端口）。选中列表中某条对象端口信息，单击【配置】按钮可以修改信息。

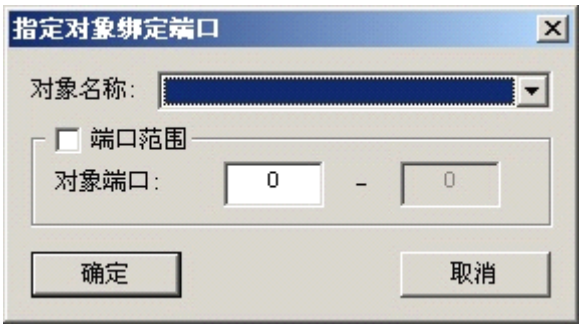

图 470

注意：设置对象端口后，需要对象下次启动时才会生效。

4.1.4 分组管理

通过管理控制台能够实现分组管理操作。

4.1.4.1添加组

方法一：在管理控制台组管理界面上，单击鼠标右键，在右键菜单中选择【添加组】，即可添加新的组。

方法二：在管理控制台上，选择【管理】/【添加组】，即可添加新的组。

4.1.4.2重命名组

方法一：在管理控制台组管理界面上，选中需要重命名的组，单击鼠标右键，选择【重命名组】。

方法二：在管理控制台上，选中需要重命名的组，在【管理】菜单中选择【重命名组】。

4.1.4.3删除组

方法一：在管理控制台组管理界面上，选中需要删除的组，单击鼠标右键，选择【删除组】，即可删除指定的组。

方法二：在管理控制台上，选中需要删除的组，在【管理】菜单中选择【删除组】，即可删除指定的组。

注意：组删除后，组所属的客户端自动归入剩余组中。

4.1.4.4客户端分组

方法一：在管理控制台上，单击【剩余组】，将显示剩余组中的计算机列表，用鼠标把列表中选中的计算机拖拽到指定的组中，即可把用户添加到指定的组中，组和组间也可以通过鼠标拖拽的方式实现客户端的分组。

注意：若在组管理界面上选中系统中心或分组信息，则无法进行分配客户端的拖拽操作。

方法二：设置自动分组规则，客户端能够自动按照分组规则划分到符合规则的组中。用户可以手动添加分组规则，也可以使用分组导入工具自动生成分组规则。

在管理控制台上选择【管理】/【分组规则管理】，弹出【分组规则管理】对话框。对话框左侧显示了分组信息，右侧显示已设置的规则信息。

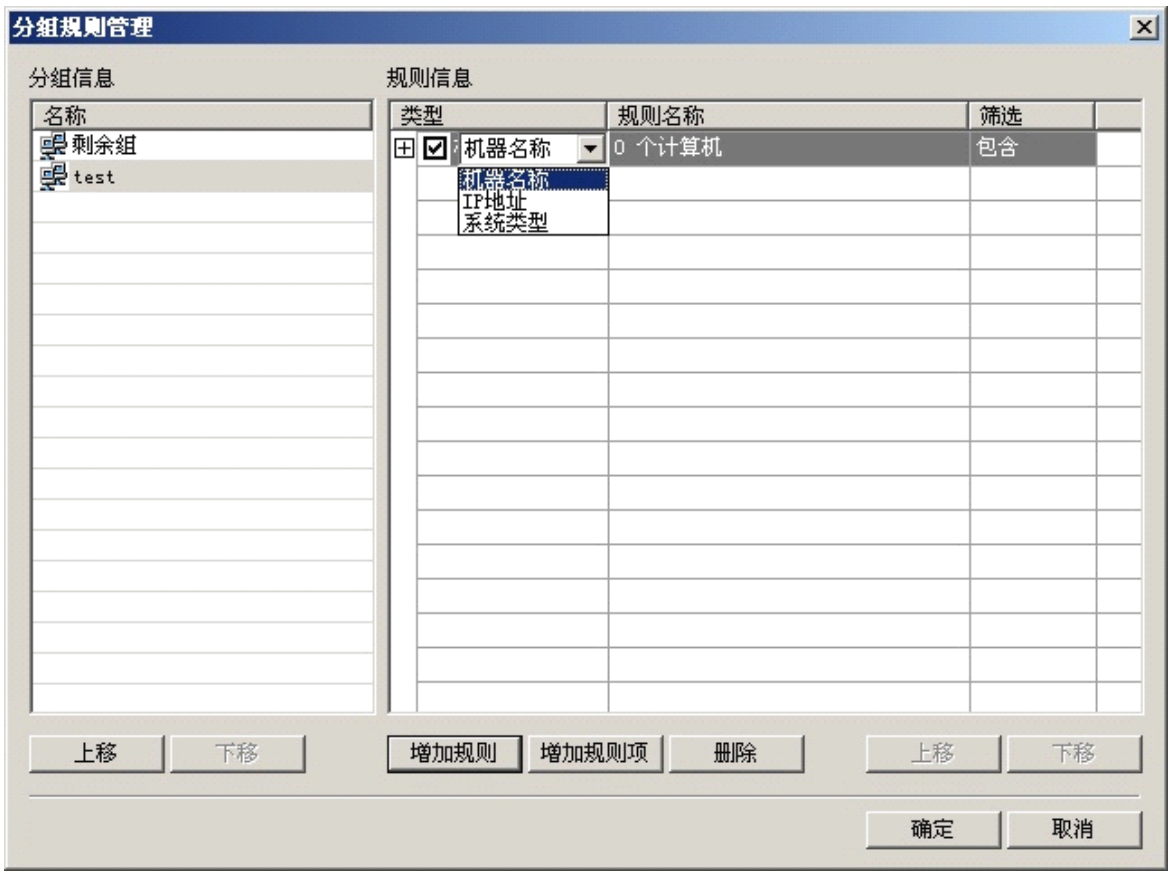

图 471

当用户需要增加分组规则时，可以单击【增加规则】按钮，用户可选择的规则类型包括机器名称、IP地址和系统类型三类，选择规则类型后，单击【增加规则项】输入具体的规则，单击【确定】按钮即可。

注意：

1、 分组信息及规则信息按自上而下的优先顺序执行。用户可以通过【上移】或【下移】按钮调整顺序。

2、 勾选规则信息前面的复选框表示该条规则有效，否则该规则不生效。

3、 立即应用分组规则：在组管理界面上右键单击【剩余组】，选择【立即应用自动分组规则】，剩余组中的客户端将按照分组规则自动加入对应组中。

4.1.5 管理员管理

通过管理员管理对话框可以新建、删除管理员，并为管理员分配客户端。

注意：超级管理员为 admin 只有一个，具有最高管理权限，可以新建操作管理员和审计管理员。

4.1.5.1管理员职责分类

根据企业用户的网络管理需求，将管理员分为三个类别：超级管理员、审计管理员和操作管理员。

管理员类别	管理员职责
超级管理员	能管辖本级中心和所有下级中心，对网络版的所有客户端都有管理权限。
操作管理员	可管理本级系统中心的客户端，并支持按组添加可管理的客户端，对管辖的客户端有全

	部的操作权限，但没有对系统中心的设置和组策略设置的权限并且不能删除日志。
审计管理员	只能管辖本级系统中心的所有客户端，可以查看并导出客户端信息、查询并统计病毒、事件、运行和主动防御日志。

4.1.5.2添加管理员

这项功能可以实现管理员的多级化，实现管理的分级化，既减轻了超级管理员的管理负担，又可以使各个管理员根据实际的网络情况和查杀需求进行配置。

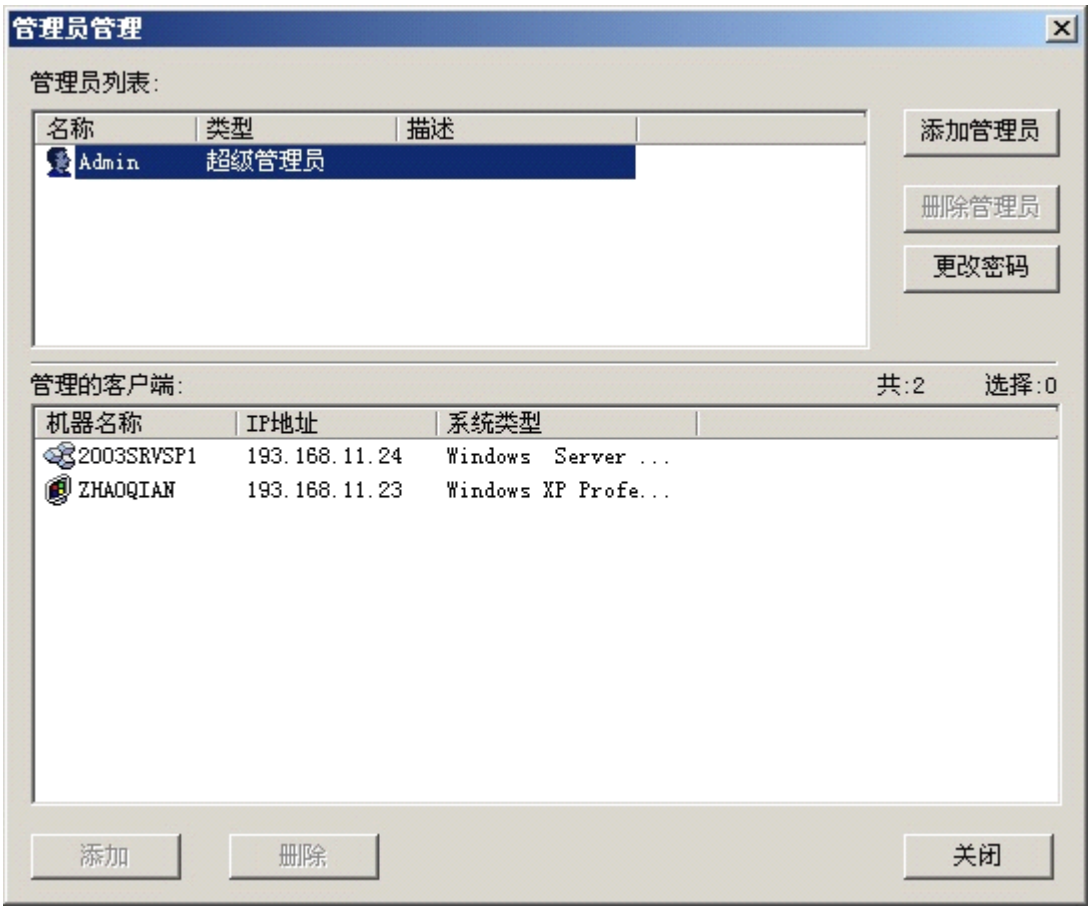

图 472

- 添加管理员：使用超级管理员登录，有添加或删除管理员的权限，单击【添加管理员】按钮可添加管理员。
- 删除管理员：该按钮用于删除选中的管理员。
- 更改密码：该按钮用于为选中的管理员更改密码。

注意：添加审计管理员时系统会自动将所有的客户端分配给其管理，超级管理员不可以再添加或删除客户端。

4.1.5.3为管理员分配客户端

在管理员列表中选择一个管理员，在下面客户端栏中将显示此管理员所管理的客户端。单击【添加】按钮，可以为此管理员添加管理的客户端；相反，单击【删除】按钮，删除选中的客户端。

4.1.6 授权计数管理

在管理控制台组管理界面中，选中某一系统中心，在管理控制台中选择【管理】/【授权计数管理】，打开【授权计数管理】对话框，用户可以查看授权计数信息。

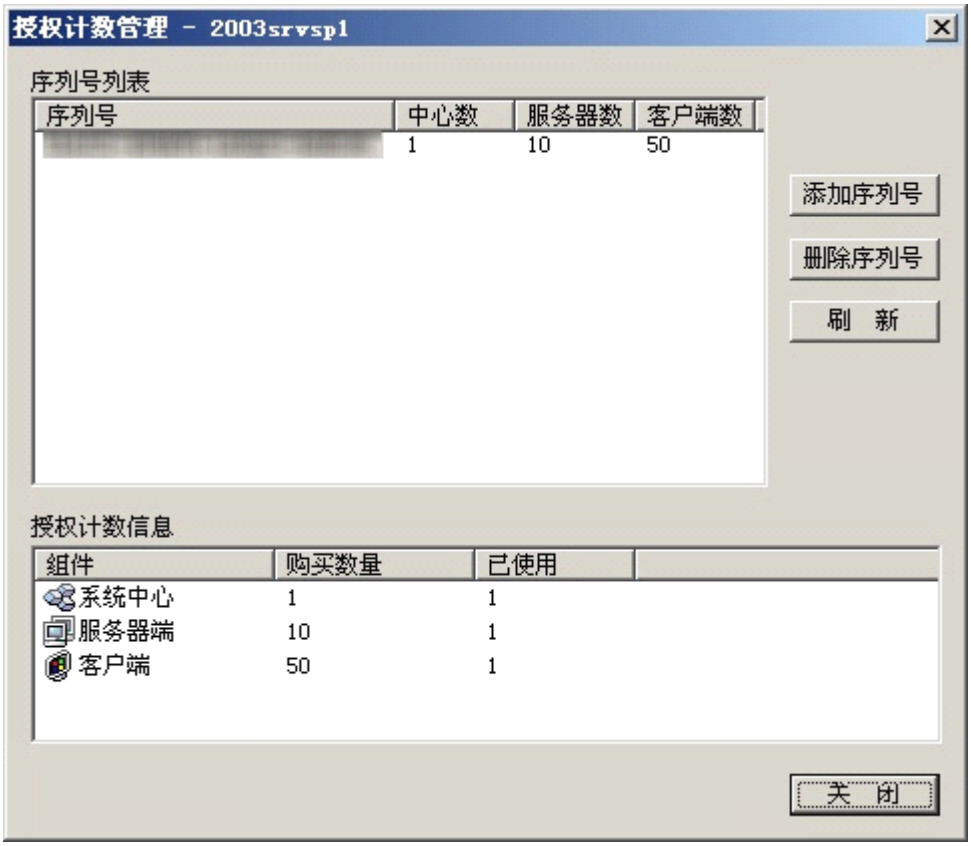

图 473

当需要增加瑞星杀毒软件网络版的服务器端或客户端数量时，可以向瑞星公司购买一定数量的授权许可（即扩容序列号）进行扩容。单击【添加序列号】按钮，在弹出的窗口中输入扩容序列号，然后单击【添加】。

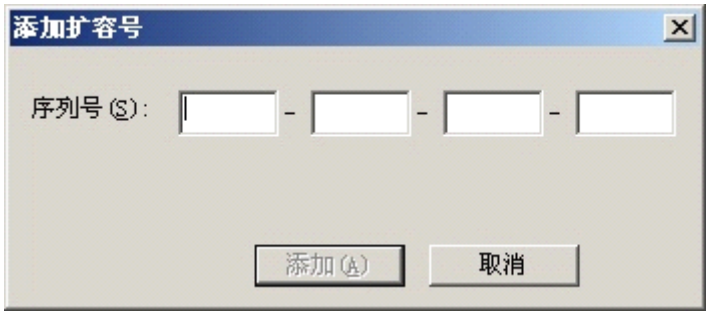

图 474

删除序列号时，选中将要删除的序列号，单击【删除序列号】即可。

注意：

1. 不能删除包含系统中心授权的序列号；
2. 添加扩容授权许可可以在局域网上任何一台安装有管理控制台的计算机上进行。

4.1.7 升级管理

为使瑞星杀毒软件网络版用户能够快速便捷地升级，瑞星杀毒软件网络版全面支持增量升级（包括系统中心从网站升级、客户端从系统中心升级、下级中心从上级中心升级），以减少升级时带来的网络流量;系统中心和客户端可设置升级周期和升级时间范围，保证及时升级，并允许用户根据自身业务的要求调整升级时间，避免升级时占用网络带宽影响用户正常业务的通讯。

4.1.7.1系统中心的升级

系统中心升级前的准备工作：设置系统中心的网络设置（具体操作详见 4.1.3.6.2 网络设置）和设置系统中心的升级方式（具体操作详见 4.1.3.6.3 升级设置）。

系统中心升级操作有三种：

方法一：打开管理控制台，在组管理界面上选中准备进行升级操作的系统中心，单击【升级】菜单，选择【通知系统中心立即升级】，程序即通知选中系统中心进行自动升级。

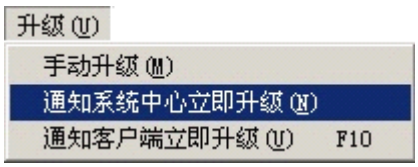

图 475

方法二：打开管理控制台，在组管理界面上选中准备进行升级操作的系统中心，单击右键，选择【通知系统中心立即升级】，升级过程如图 476。

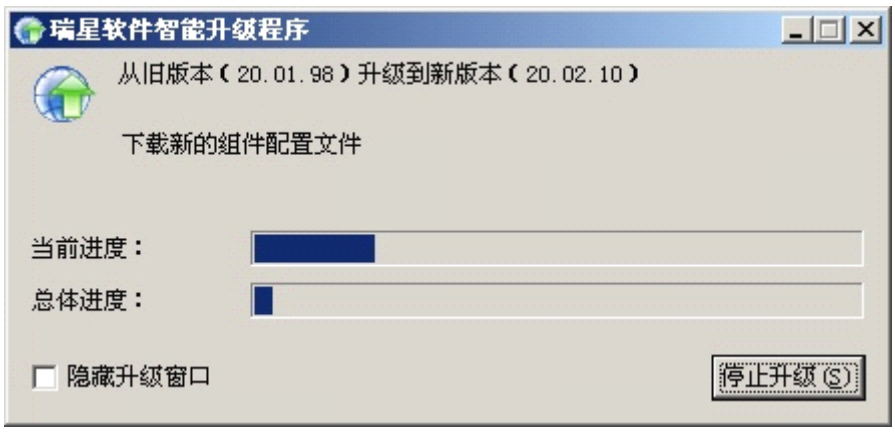

图 476

方法三：选择手动升级前，要首先从网站上下载手动升级包，下载完毕后，在管理控制台上单击【升级】菜单，选择【手动升级】，在弹出的对话框中选择瑞星杀毒软件网络版手动升级程序，单击【打开】按钮后将显示提示信息，如图 477。

图 477

开始安装手动升级包，完成系统中心的升级过程，如图 478。

图 478

注意：

1. 上述升级方法除手动升级方式外均适用于多中心的情况，如需通知下级中心进行升级，只要在管理控制台上选中下级中心作为操作对象即可；
2. 使用手动升级前，需先在瑞星网站上下载手动升级包。

4.1.7.2客户端的升级

客户端升级前的准备工作：设置客户端的升级设置，具体操作详见：4.1.3.3.4 定时升级设置。

- **客户端从系统中心升级**

默认情况下，客户端会自动从系统中心进行升级，如需人为进行升级操作方法有四种：

方法一：在管理控制台上，选中需要通知升级的客户端，单击【升级】菜单，选择【通知客户端立即

升级】，程序将通知客户端进行升级。

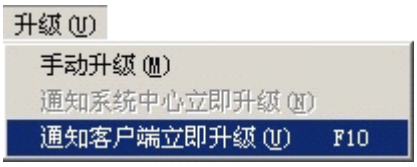

图 479

方法二：在管理控制台上，选中需要通知升级的客户端，单击右键，在弹出的菜单中选择【通知客户端立即升级】。

方法三：在管理控制台上，选中需要通知升级的客户端，单击工具栏上的  按钮或按 F10 键。

方法四：在客户端托盘程序上单击右键，选择【立即升级】，升级程序如图 480。

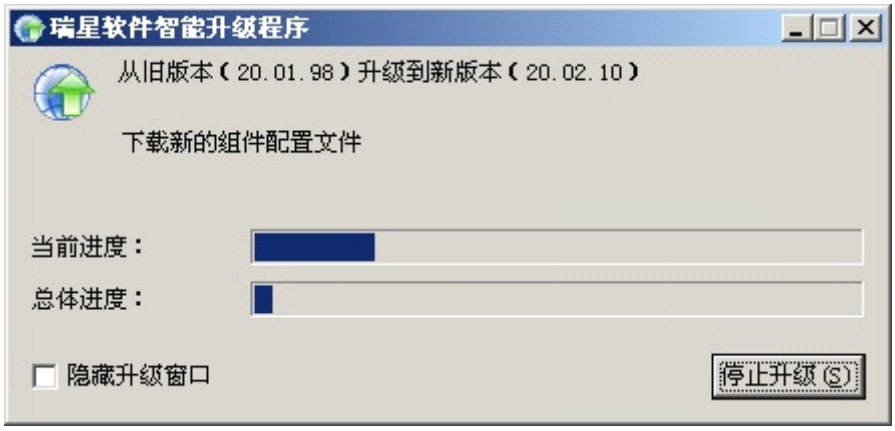

图 480

- **客户端通过代理升级**

当系统中心管辖的客户端较多时，可以设置客户端升级代理来分担系统中心升级时的负荷。开启升级代理功能后，非升级代理客户端升级时，会优先从本网段的升级代理客户端升级。升级代理客户端直接从系统中心升级。这样可以缓解系统中心的压力，提高整个系统的升级效率。

在【系统中心设置】页面的【升级设置】中，勾选页面下方的【启用客户端作为升级代理功能】选项，开启升级代理功能。此时会弹出如下图所示对话框，提示管理员是否自动生成升级代理。若系统中心所管辖的客户端较多，管理员手动挑选作为升级代理的客户端工作量比较大，管理员可以点击【是】，系统中心会把当前所有的客户端按网段划分，每网段会自动生成一个升级代理；如果管理员点击【否】，系统中心不会自动生成升级代理，此后，管理员需要手动选择客户端作为升级代理。

图 481

同一网段内，可以设置多个客户端作为升级代理，方法如下：在管理控制台上选择要设置为升级代理的客户端，单击右键，选择【开启客户端作为升级代理】选项，该客户端将成为升级代理。

锁定升级代理：为了适应各种网络拓扑结构，产品提供了锁定升级代理的功能。管理员可以根据具体网络布局，调整客户端的升级途径，锁定客户端所使用的升级代理。

方法如下：选中需要调整升级途径的客户端后，单击右键选择【设置客户端选项】，在打开的对话框

中选择【升级代理设置】。

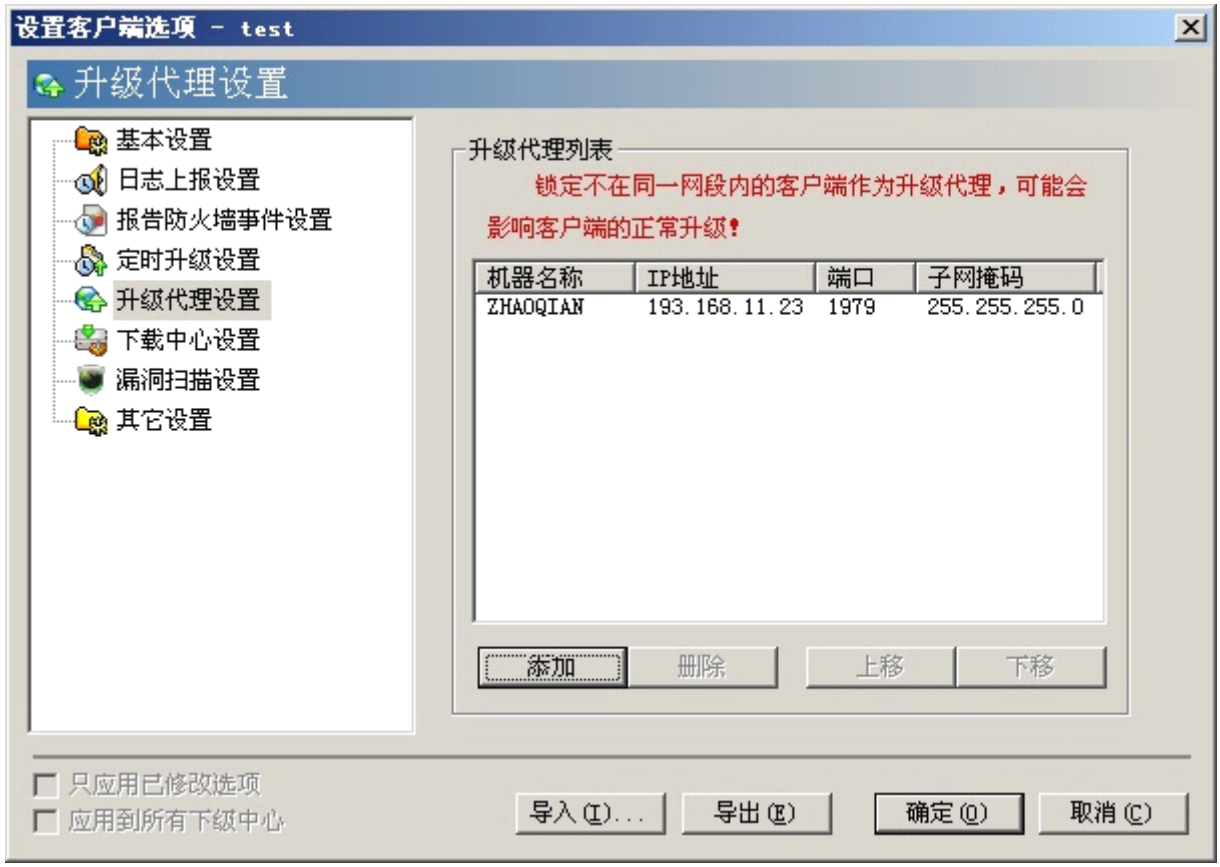

图 482

单击【添加】按钮，选择本客户端要使用的升级代理，单击【确定】即可锁定本客户端的升级代理。（即本客户端此后升级只从锁定的升级代理升级）。

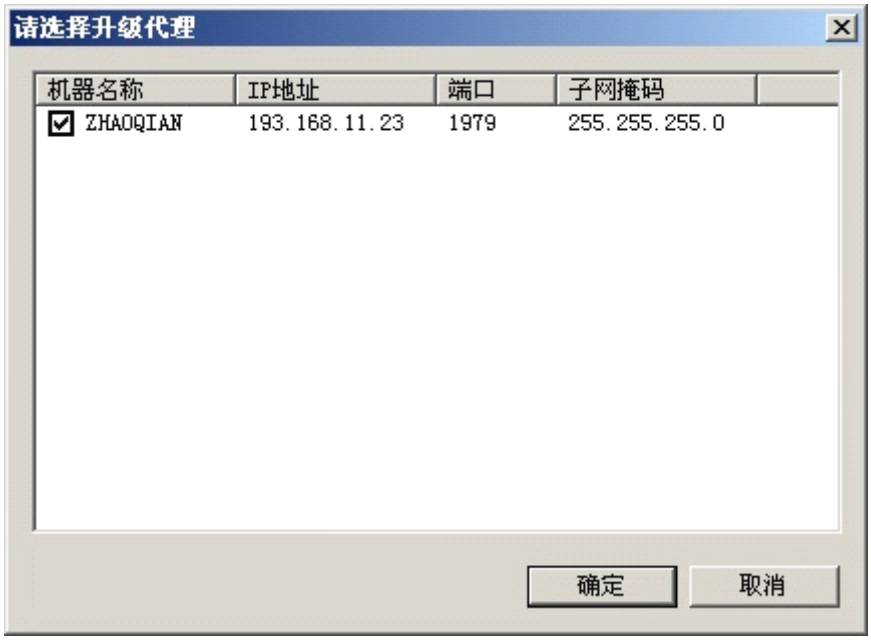

图 483

注意：

1. 若要对一个组所有客户端锁定升级代理，管理员只需选中一个组，单击右键选择【设置客户端选项】即可。

2. 上述升级描述对于多级中心也同样适用，管理员可以对下级中心的任何一个客户端或一组客户端进行升级操作，只需在操作时注意选择的操作对象即可。
3. 锁定了多个升级代理后，当非升级代理客户端进行升级的时候，会按照从上到下的顺序寻找升级代理，即首先尝试从第一个升级代理升级，如果该升级代理因某种原因不能使用（例如关机）则寻找下一个升级代理，依此类推，直到找到一个可以使用的升级代理。如果所有锁定的升级代理均不可用，就直接从系统中心进行升级。

4.1.7.3Unix 客户端升级

瑞星杀毒软件网络版支持对 Unix 客户端的集成管理。为方便 Unix 客户端升级，瑞星杀毒软件网络版在管理控制台中设置了【Unix 客户端升级工具】菜单，用户通过此工具对 Unix 客户端升级。具体步骤如下：

第一步：用户通过登录瑞星网站（http://www.rising.com.cn）升级页面，下载升级文件；

第二步：打开管理控制台，单击【工具】菜单，选择【Unix 客户端升级工具】，弹出【unixcopy】界面，单击【添加升级文件】按钮，选中已下载的升级文件，单击【打开】，随即开始复制文件到瑞星安装目录下的 UnixUpdate 文件夹中，复制结束后，在该工具的信息列表中将会显示已加入升级文件的相关信息，并且会弹出文件被成功加入的提示；

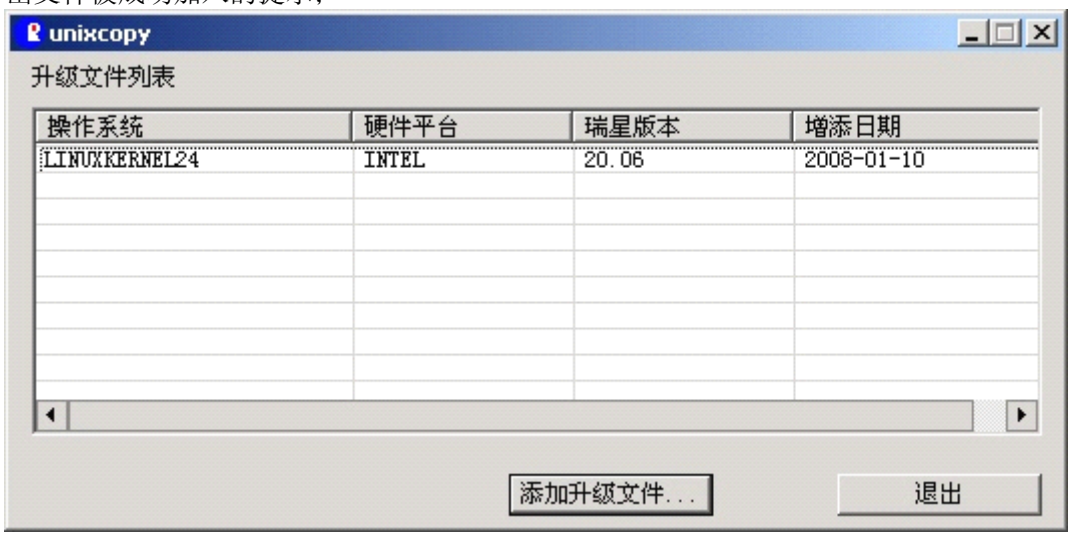

图 484

第三步：客户端程序会自动完成升级。Unix 客户端会每 15 分钟检测一次是否有新的版本，如果有新版本的话就自动升级。

注意：本工具只能在系统中心本机上使用。

4.2 管理工具

为用户提供全方位的管理工具，包括 Unix 序列号管理工具、通讯代理管理工具、日志管理工具、漏洞信息管理工具、Unix 客户端升级工具、下载中心管理工具、日志打包工具、客户端配置工具、报警插件配置工具、系统中心数据备份工具、客户端搜索工具、分组导入工具和客户端安装包制作工具。

4.2.1 Unix 序列号管理

单击【Unix 序列号管理】标签进入页面，提供给管理员查看 Unix 序列号列表的功能。管理员可以查看和删除 Unix 序列号。

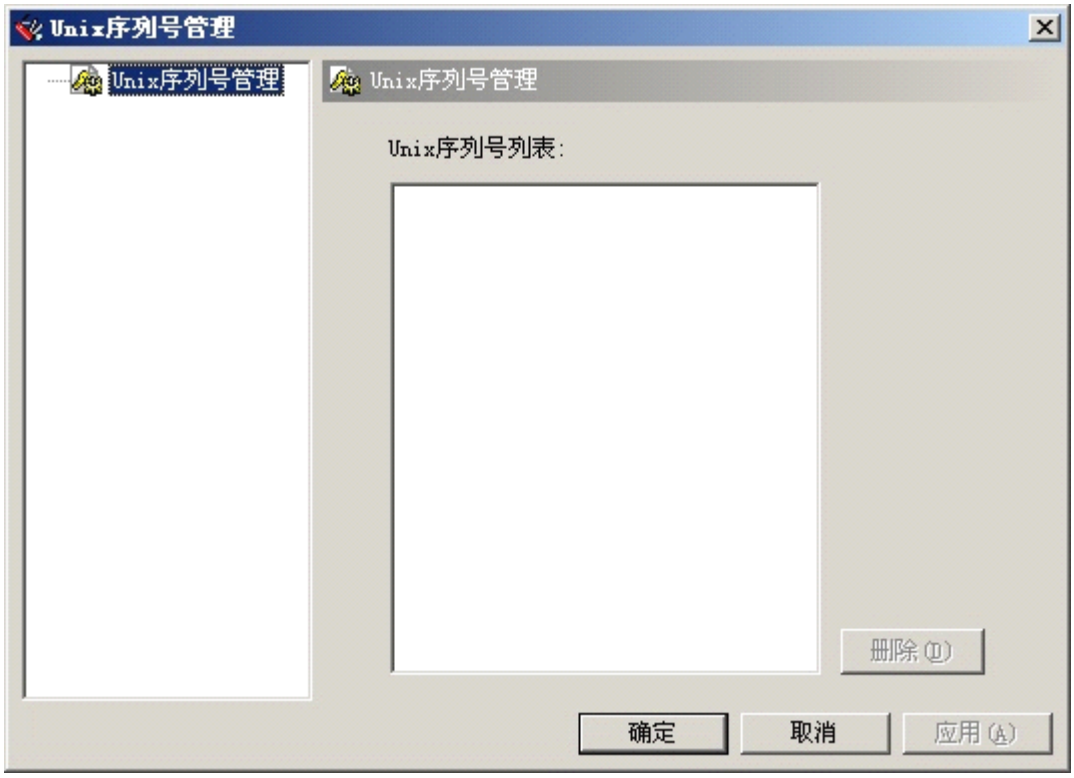

图 485

4.2.2 通讯代理管理

4.2.2.1 Sender（下级通讯代理）的设置

传递上/本级中心下发给下级中心的命令，并将下级中心 RavReceiver 返回的结果/数据传递给本级中心的相应对象。

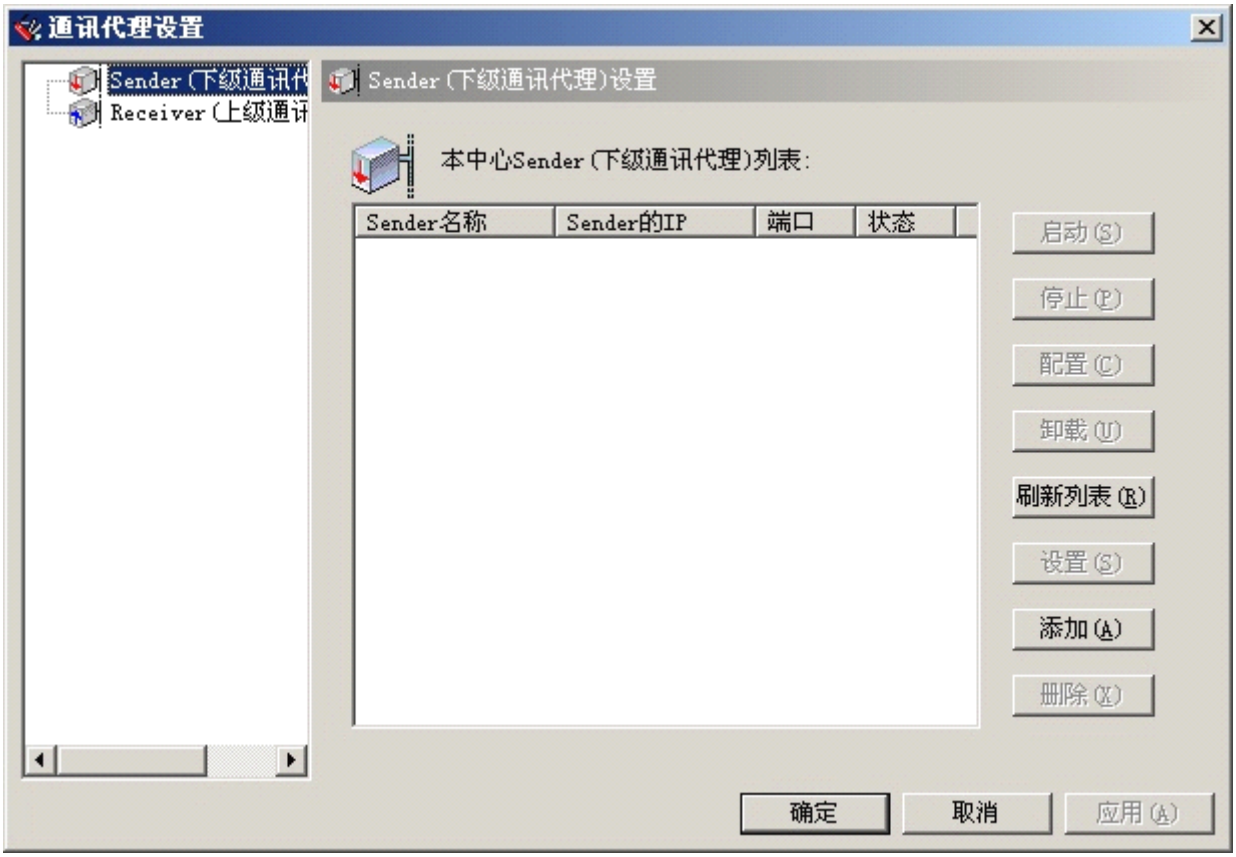

图 486

单击【添加】按钮添加下级通讯代理。在下级通讯代理列表里面选中需要进行设置的下级通讯代理，单击【设置】按钮打开黑白名单对话框。

白名单是指允许在 Sender 注册的 Receiver 所在系统中心的 IP 地址，黑名单是指禁止在 Sender 注册的 Receiver 所在系统中心的 IP 地址。可以通过【添加】或【删除】按钮对黑白名单进行编辑。

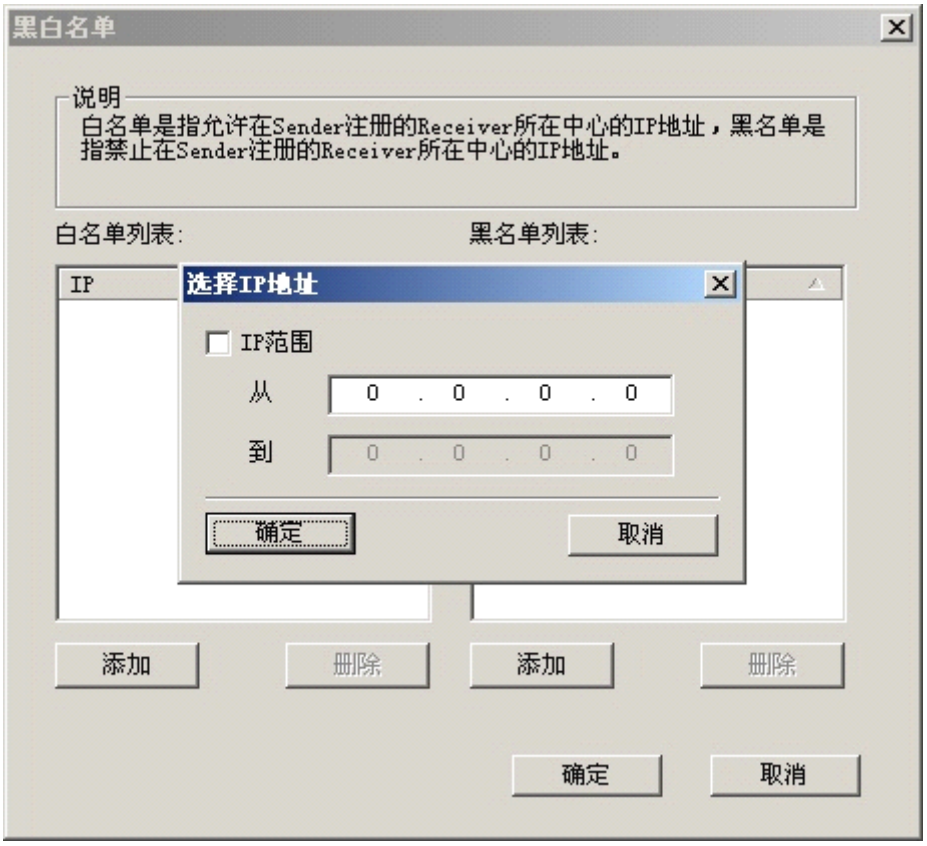

图 487

4.2.2.2Receiver（上级通讯代理）的设置

负责将上级中心的命令和数据转发给本中心的相关组件，并将本中心的数据转发给上级中心。一个中心只能有一个 Receiver。

输入 Receiver 所在的计算机的 IP 地址和 Receiver 指向 Sender 地址，单击【安装】即可。

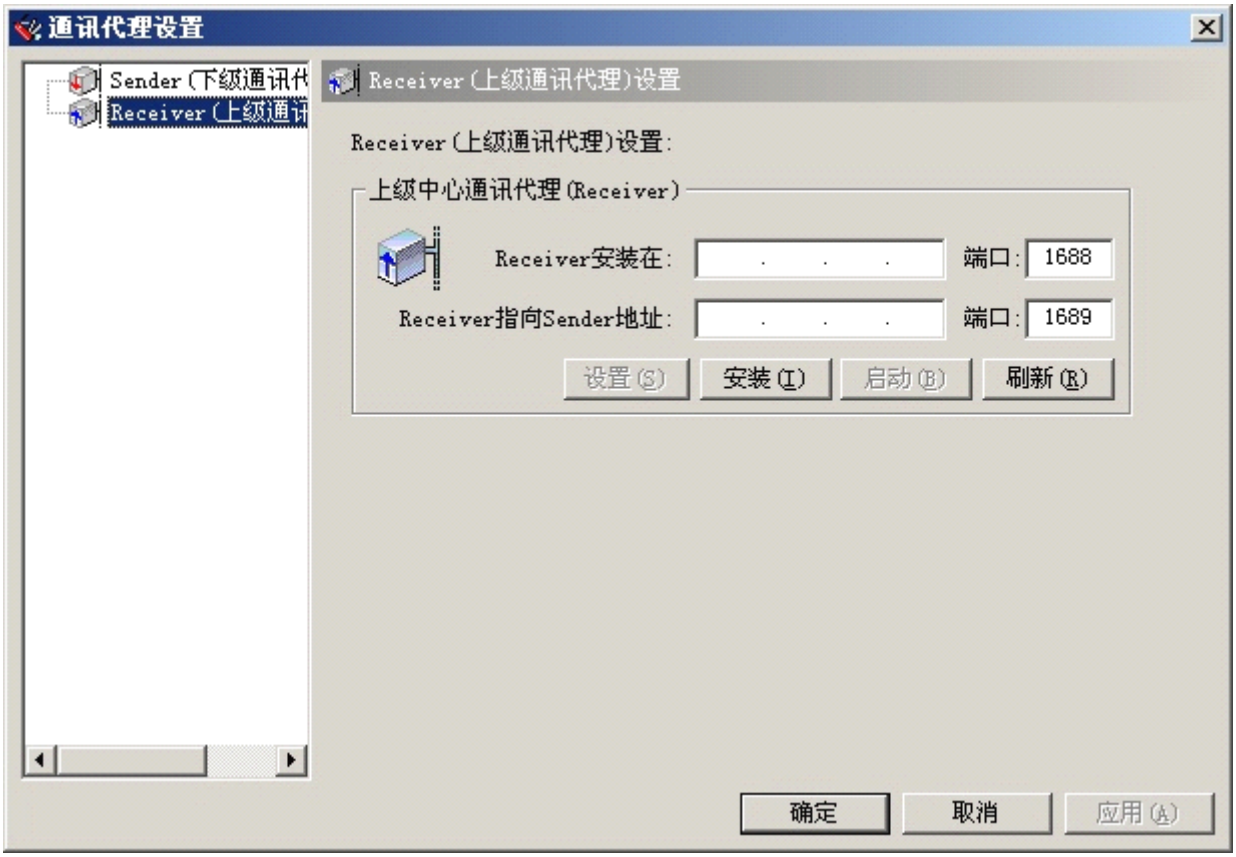

图 488

单击【设置】打开【设置 Receiver】页面，如图：

图 489

4.2.3 瑞星日志管理工具

4.2.3.1 日志查询和统计

通过瑞星日志管理工具，管理员可对病毒、事件、主动防御和防火墙的日志进行查询统计。选择【开始】/【程序】/【瑞星杀毒软件】/【瑞星日志管理工具】，或在管理控制台上单击【工具】菜单，选择【日志管理工具】，弹出日志管理工具界面。

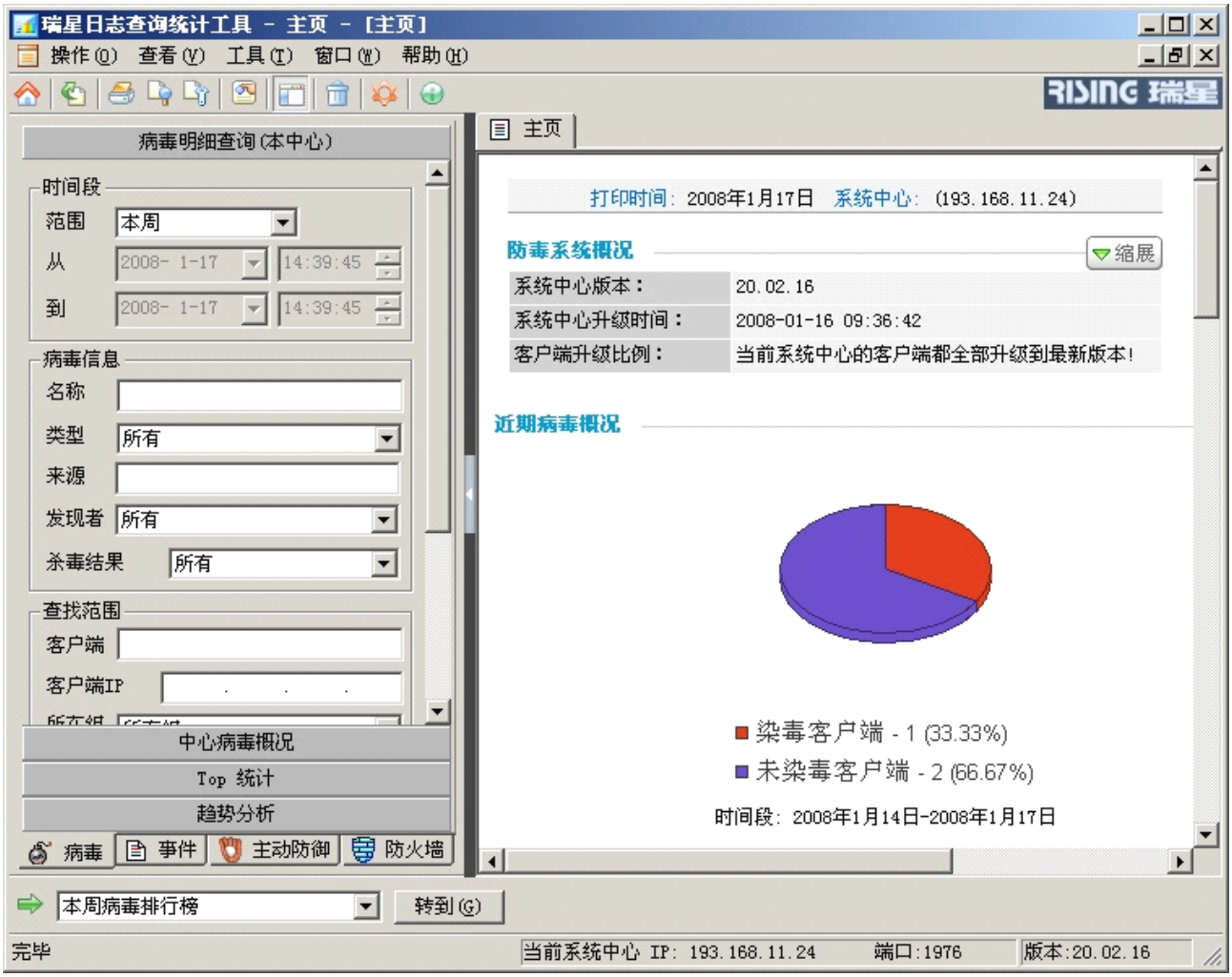

图 490

注意：瑞星日志管理工具可以以不同种类的帐号登陆，超级管理员对瑞星日志管理工具有完全的操作权限，而以操作管理员或审计管理员帐号登录此工具时，对于工具中的【日志删除】和【计划任务管理】都没有权限使用。

瑞星日志管理工具界面的左侧是项目栏，包括【病毒】、【事件】、【主动防御】和【防火墙】四个标签页，可以选择查询不同类型的日志信息。用户限定查询条件后，单击页面下方的【查询】或【统计】按钮，日志查询统计工具就会给用户最清晰的结果显示。现在以病毒日志和事件日志查询为例介绍瑞星日志管理工具的具体操作。

- **病毒日志的管理**

病毒日志的管理共包括四部分：【病毒明细查询（本中心）】、【中心病毒概况】、【Top 统计】和【趋势分析】。针对【病毒明细查询（本中心）】功能，用户需要输入查询条件，单击【查询】按钮，将显示查询数据结果，包括病毒名称、病毒类型、发作次数、客户端名称、客户端 IP 和查杀结果等信息。

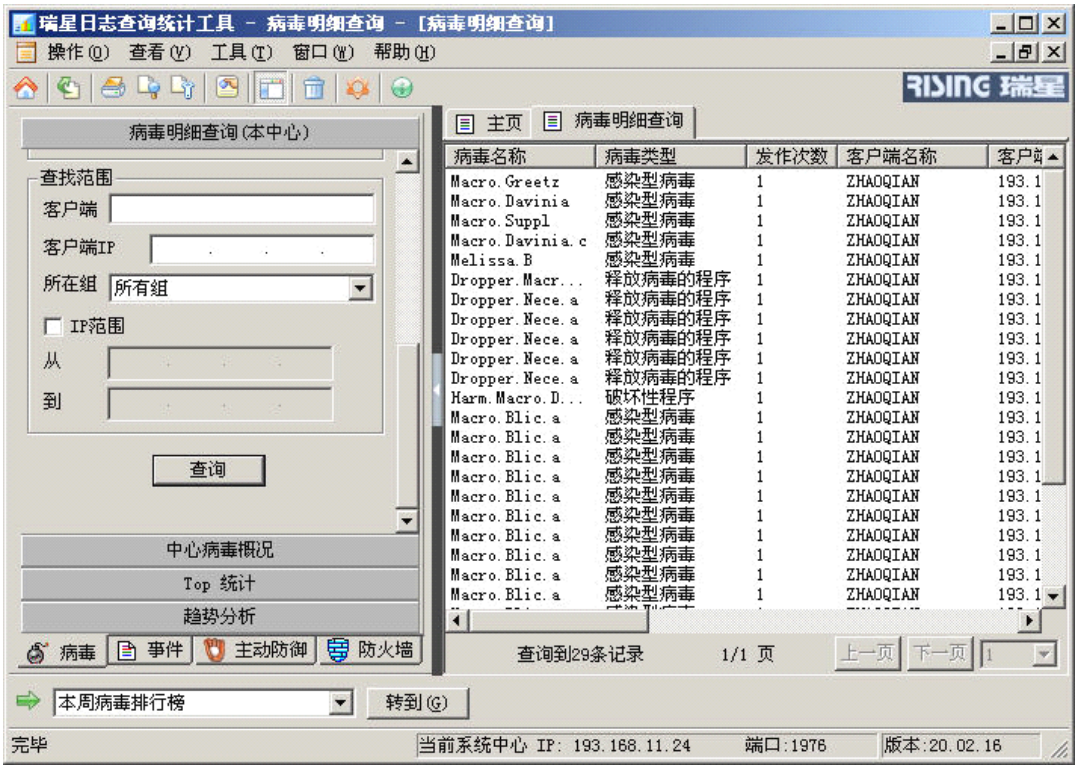

图 491

注意：病毒明细查询功能不支持查询下级中心的病毒明细功能。

针对【中心病毒概况】查询，输入查询条件后，单击【查询】按钮后，将显示结果。

图 492

用户通过【Top 统计】功能，可以查询病毒排行、本中心客户端排行、本中心组排行和中心排行，选择要统计的内容后，单击【统计】按钮后，显示统计结果，以查询本周病毒排行为例。

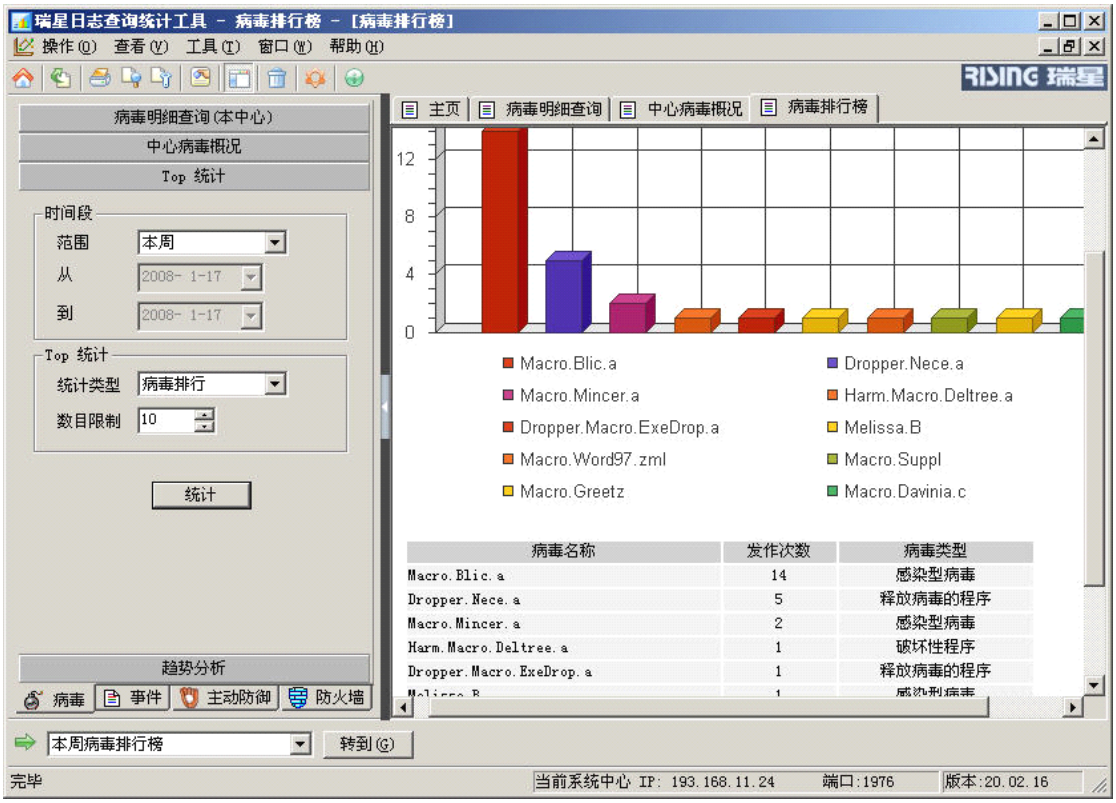

图 493

注意：在【Top 统计】中，统计类型分为：病毒排行、本中心客户端排行、本中心组排行和中心排行，其中，“本中心客户端排行”和“本中心组排行”不支持查询下级中心的内容，“病毒排行”和“中心排行”支持对下级中心的查询。

【趋势分析】功能提供分析某一时间段内某一客户端或病毒的染毒趋势，及时的预防病毒的侵害。以本周某一客户端病毒感染趋势为例，输入限定条件后单击【分析】按钮后，显示趋势图。

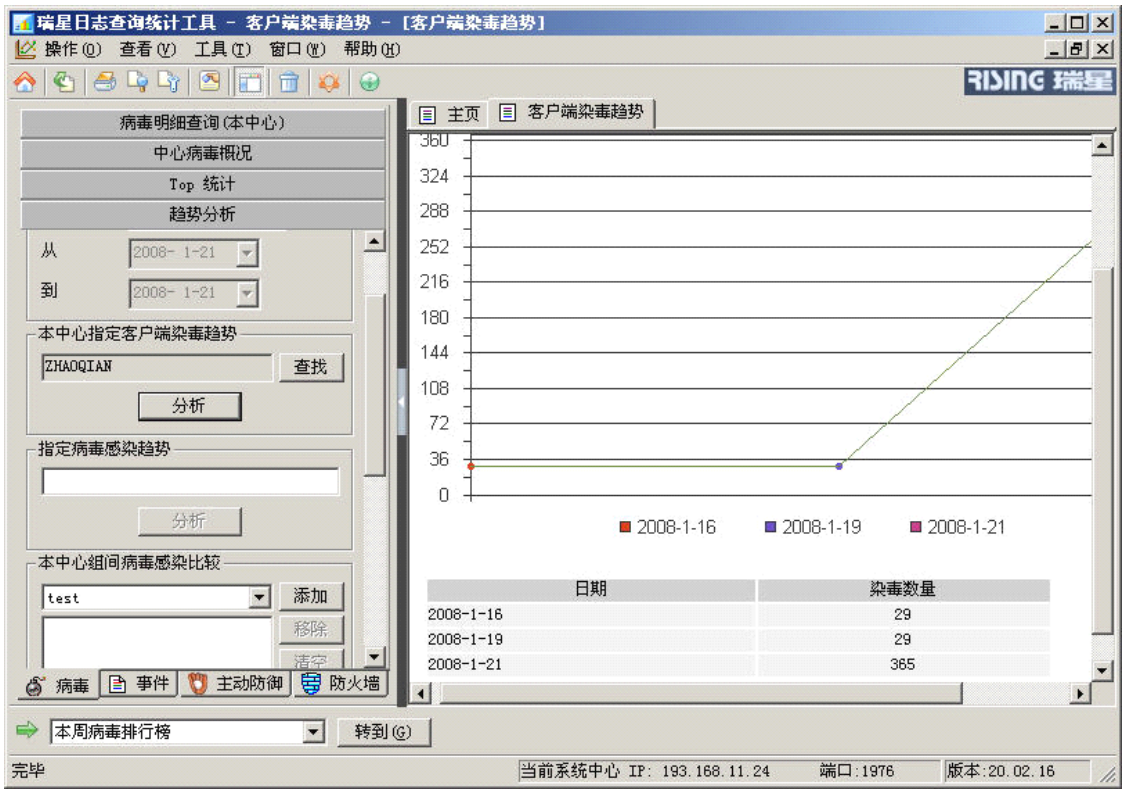

图 494

注意：在【趋势分析】中，“本中心指定客户端染毒趋势”和“本中心组间病毒感染比较”的分析不支持对下级中心的分析，但是“指定病毒感染趋势”和“中心间染毒比较”则支持。

- **事件日志的管理**

瑞星日志管理工具可以对事件日志进行查询，在左面的查询栏中输入查询条件后，单击【查询】按钮即可显示查询结果。

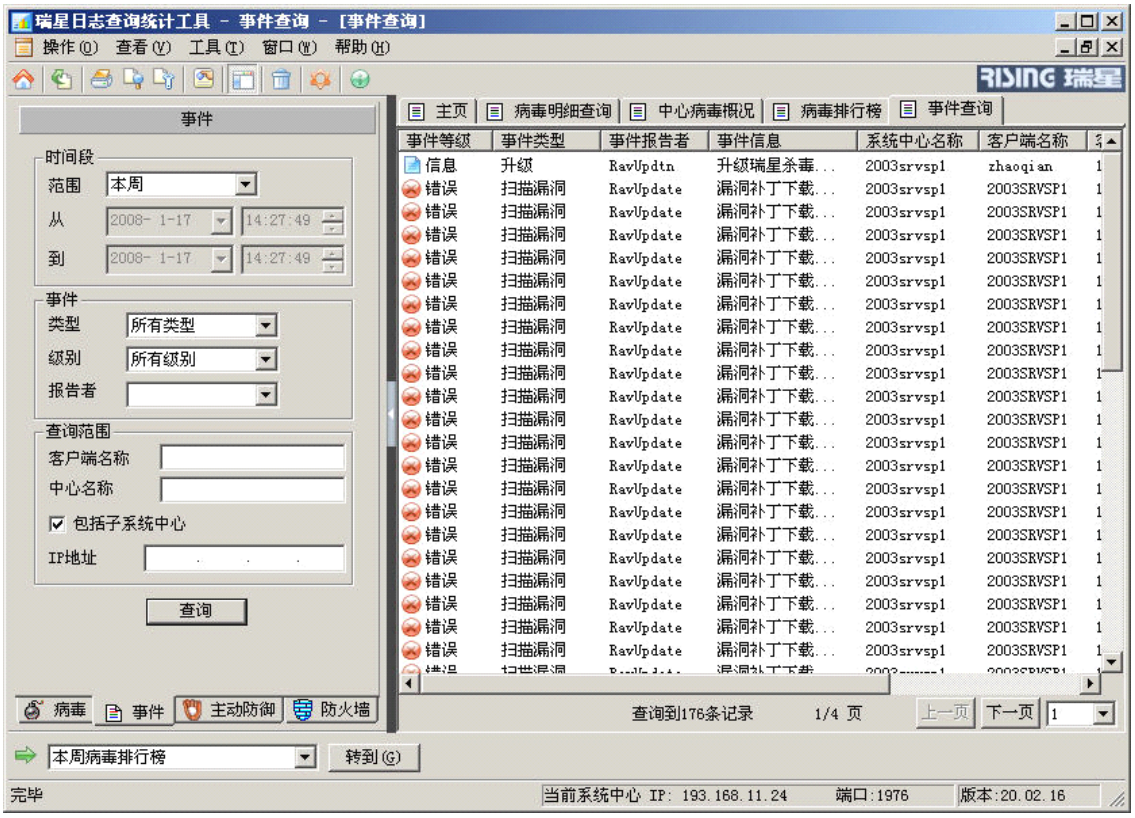

图 495

注意：事件日志和防火墙日志查询支持对下级中心的查询，主动防御日志的查询不支持对下级中心的主动防御日志的查询。

如果管理控制台上更改了组、下级中心或客户端信息时，可以通过瑞星日志管理工具的【操作】菜单的【从系统中心同步信息】选项来刷新信息而不需要重新启动瑞星日志工具。

4.2.3.2计划任务管理

此工具可以为系统管理员提供查看所关注的日志信息功能。添加任务后将定期向系统管理员发送所关注的病毒或事件等统计报表，系统管理员通过添加新任务设置发送报表中的详细内容。

在日志查询统计工具中，单击菜单栏【工具】，选择【计划任务管理】打开计划任务管理页面。用户可以添加计划任务，根据用户的设置，定期发送邮件到指定邮箱中。添加新任务完毕，在计划任务管理工具中将显示任务的具体设置项。

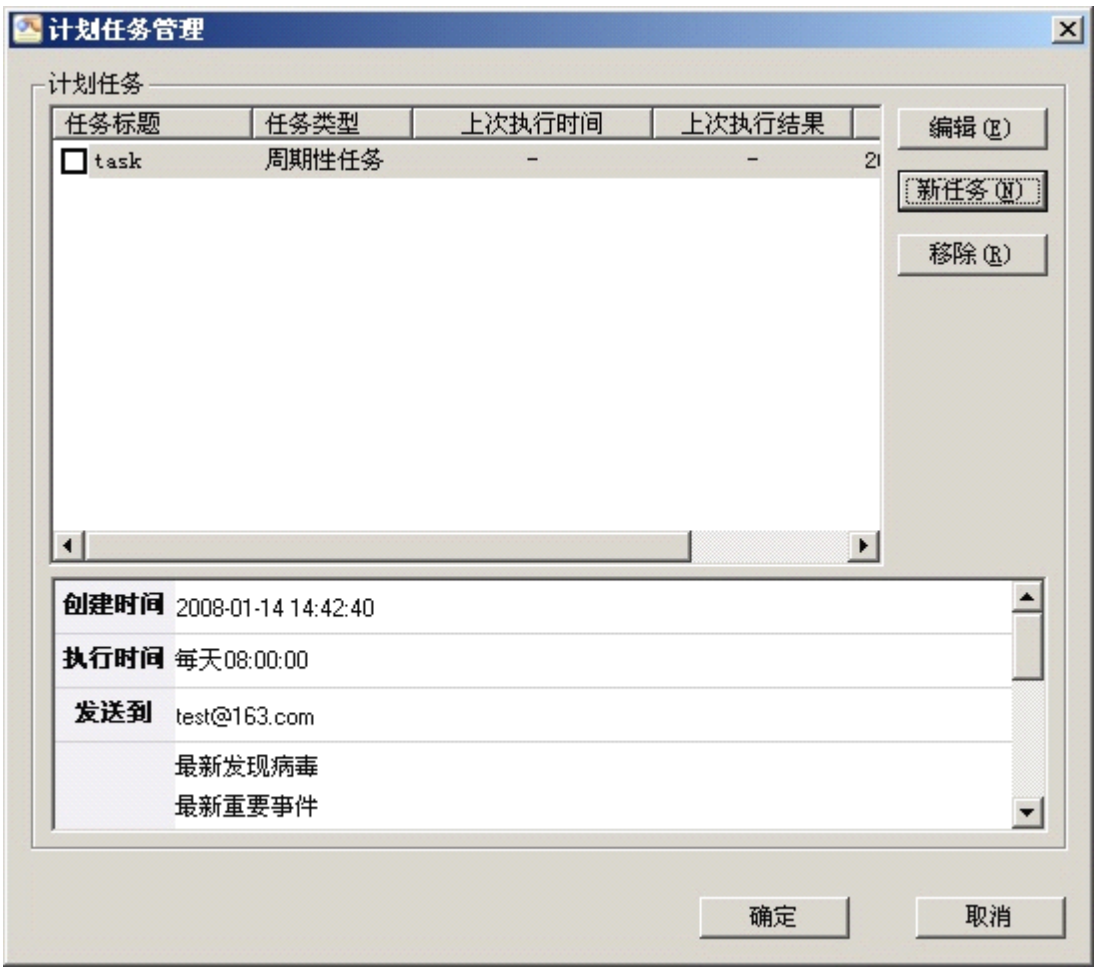

图 496

添加新任务的步骤如下：

第一步：单击【新任务】按钮，进入【设置标题和种类】页面。在该页面中需要输入任务标题，单击【下一步】继续。

图 497

第二步：进入【发送内容】页面，设置要发送的计划任务的详细内容，下拉列表中选择发送报表的详细内容，单击【添加】按钮将添加该内容到计划任务中。选中某条信息后单击【编辑】按钮，可以打开该

信息的具体设置页面，单击【移除】按钮，删除该信息，单击【清空】按钮，清空发送信息列表。单击【下一步】继续。

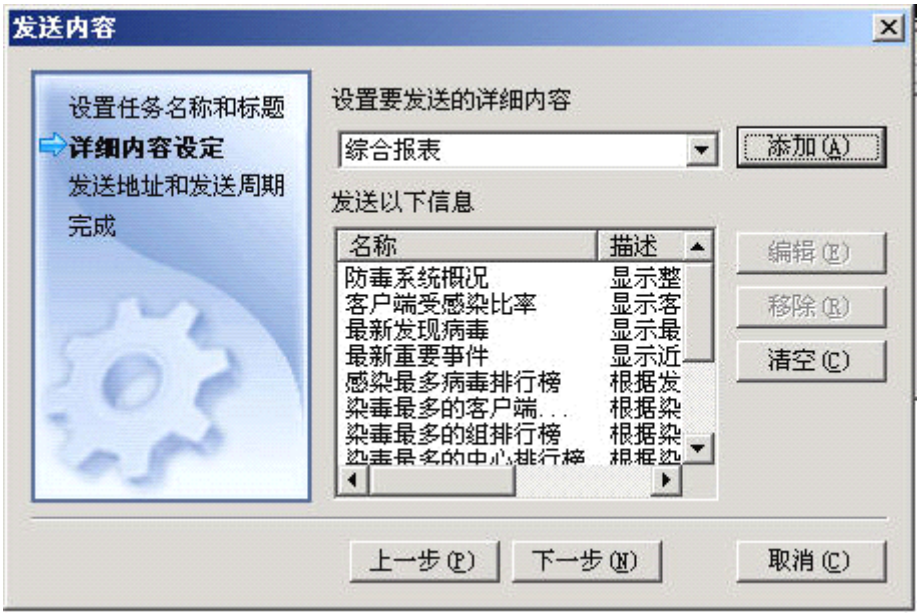

图 498

第三步：进入【发送地址和发送周期】页面，选择发送地址和周期，可以选择该任务是一次性任务还是周期性任务；在发送地址中单击【添加】按钮，双击可编辑区输入要发送的邮箱地址，确认后单击【下一步】继续。

图 499

第四步：进入【完成】页面，显示添加的计划任务的描述信息。确认无误后单击【完成】按钮，完成新任务的添加。

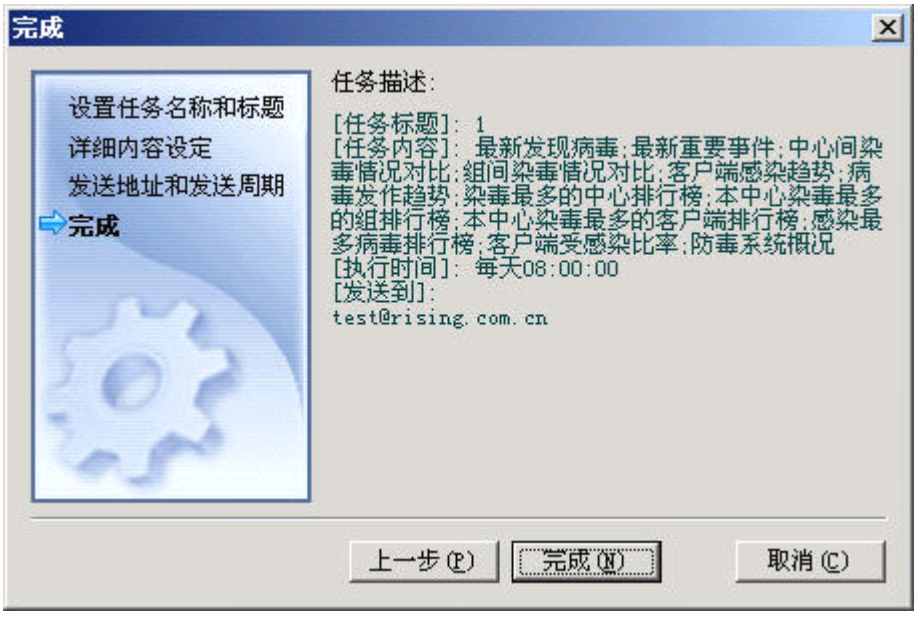

图 4100

4.2.3.3日志删除

打开瑞星日志查询统计工具，单击【工具】菜单中的【日志删除】选项，删除指定时间段内指定类型的日志，单击【细节】按钮显示详细信息。

图 4101

4.2.3.4选项

在日志管理工具中的【工具】菜单中，单击【选项】打开选项页面。在【综合设置】页面中，提供给用户自动清除日志功能，用户可以设置自动清除若干天的日志信息，并且可以设置数据库查询超时时间和每页的数据行数。勾选【星期天是一周的第一天】，将在查询结果中，把星期天算做是一周的第一天来统计日志信息。

说明：在高级企业版中“自动清楚 X 天前的防火墙事件日志信息”设置项有效；在高级企业专用版定制了防火墙功能的情况下该设置项生效；网吧版、中小企业版、企业版和高级企业版中此设置无效。

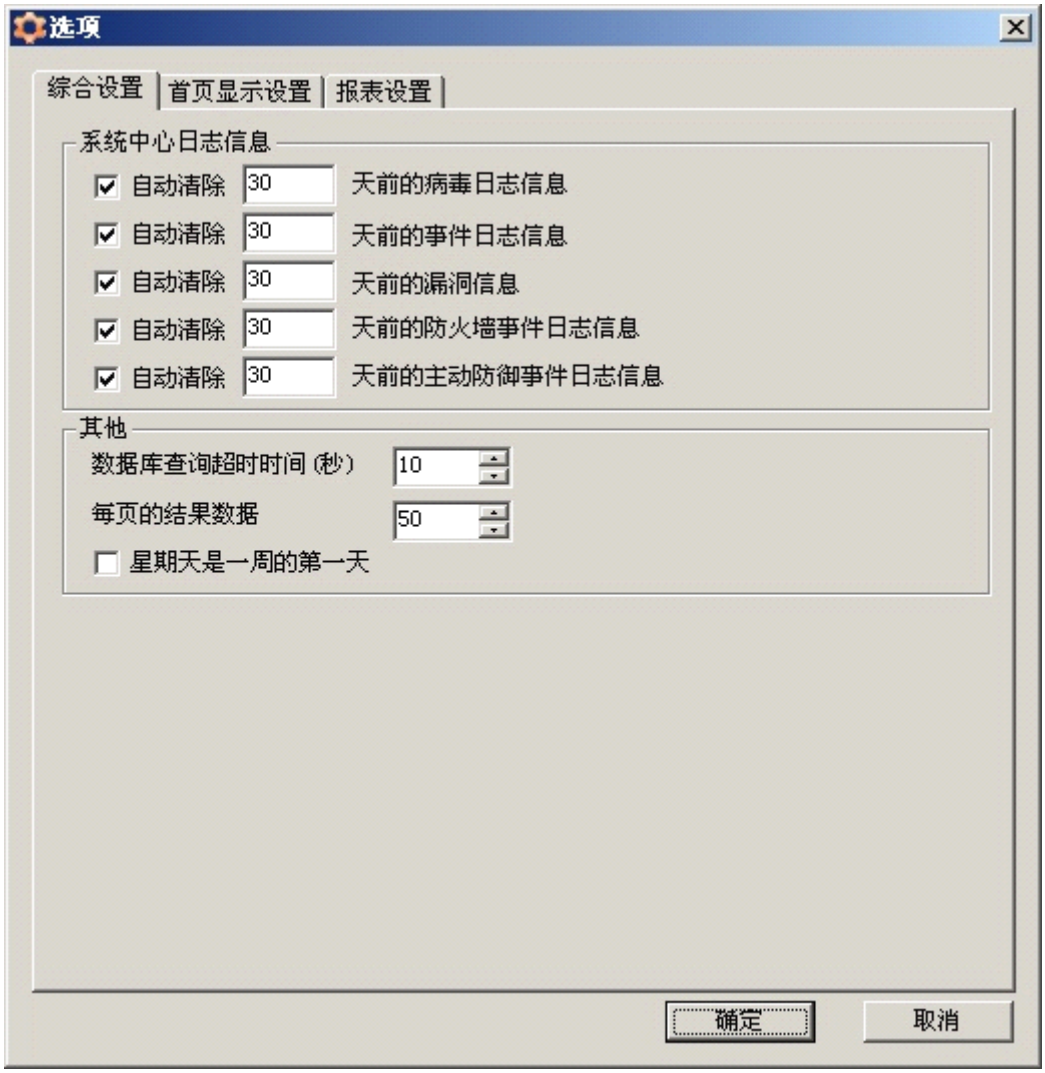

图 4102

注意：如果是以操作管理员或审计管理员的帐号登录的瑞星日志管理工具，则没有设置自动清除若干天的日志信息的权限。

在【首页显示设置】页面中，用户可以选择在日志查询统计工具的主页上显示的项目。

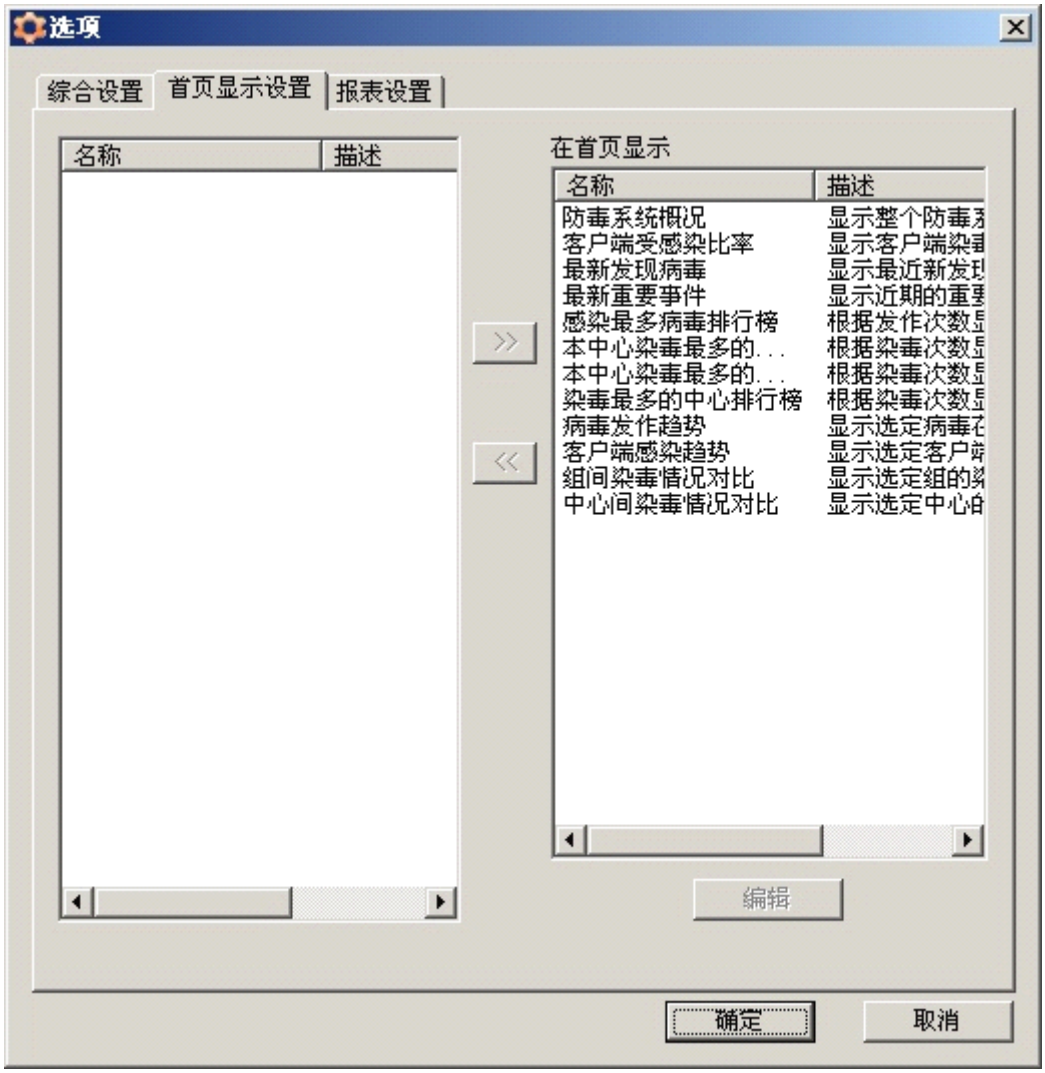

图 4103

选中某项后，单击【编辑】按钮，进行设置。

图 4104

在【报表设置】页面中，用户可以设置收集日报表和月报表的频率、时间，控制下级中心向上级中心上报病毒的频率和时间、设置 SMTP 服务器的 IP 地址和端口等。

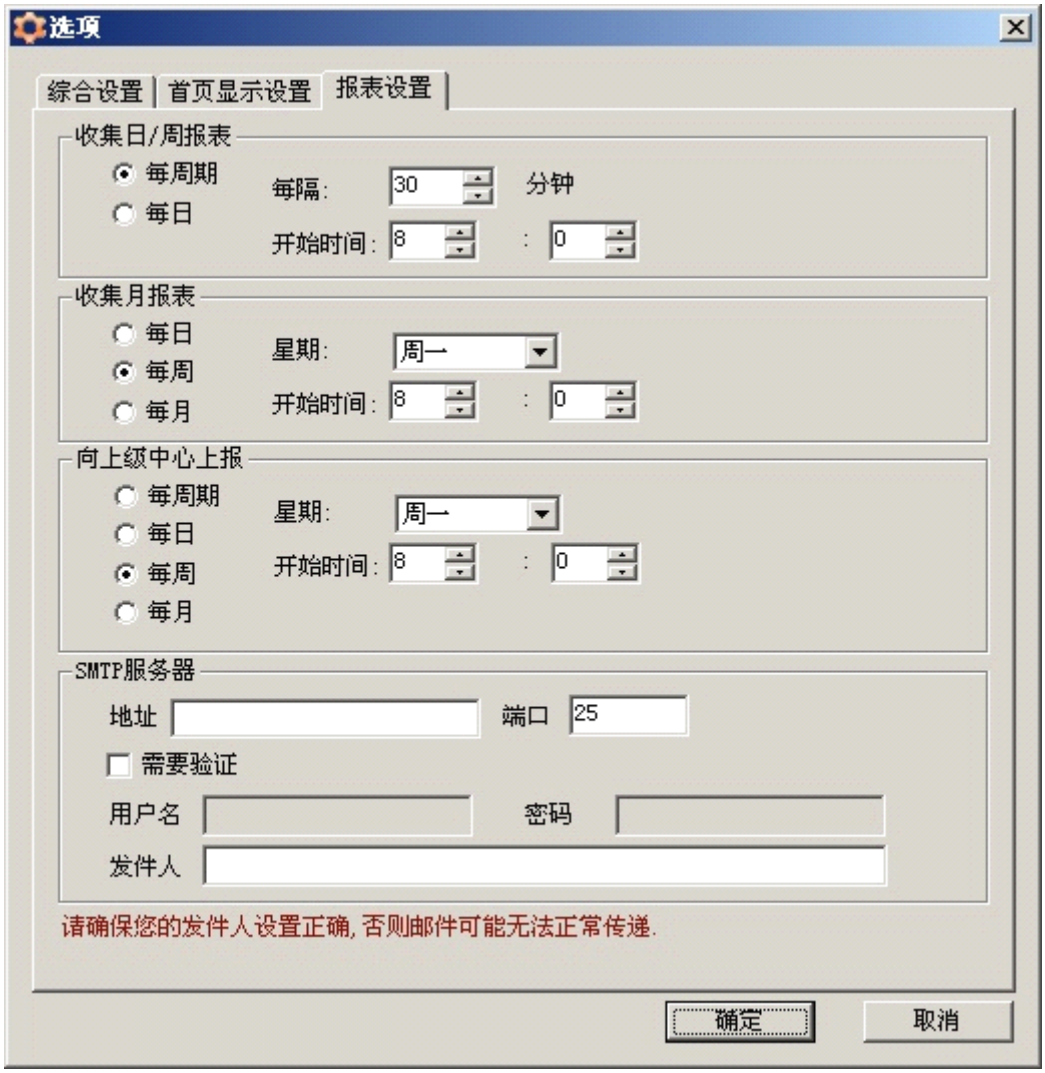

图 4105

注意：如果是以操作管理员或审计管理员的帐号登录的瑞星日志管理工具，则不显示【报表设置】这一界面。

4.2.3.5导出数据

导出日志是日志管理工具常用的功能之一。

第一步：完成日志查询或统计操作后，单击工具栏上  按钮或单击【操作】菜单，选择【导出】，在弹出的对话框中选择导出的记录范围，单击【确定】。

第二步：在弹出的保存对话框中，用户可以选择保存路径、文件名以及保存类型。最后单击【保存】按钮。

4.2.3.6打印日志

日志管理工具还提供了打印日志的功能。用户可以单击【操作】菜单选择【打印】，或单击  按钮进行打印。

4.2.4 漏洞管理工具

对于大型网络远程扫描系统漏洞是一个较漫长的过程，远程安装补丁程序更是一个耗费时间的工程，瑞星漏洞信息管理工具给网络管理员提供了一个便捷的途径，使网络管理员在短时间内做好整个网络系统的安全防范工作。

4.2.4.1界面说明

打开管理控制台，单击【工具】菜单，选择【漏洞管理工具】，弹出漏洞信息管理工具界面；也可以通过单击【开始】/【程序】/【瑞星杀毒软件】/【漏洞信息管理工具】打开漏洞信息管理工具，界面包括菜单栏、工具栏、查询栏和状态栏。

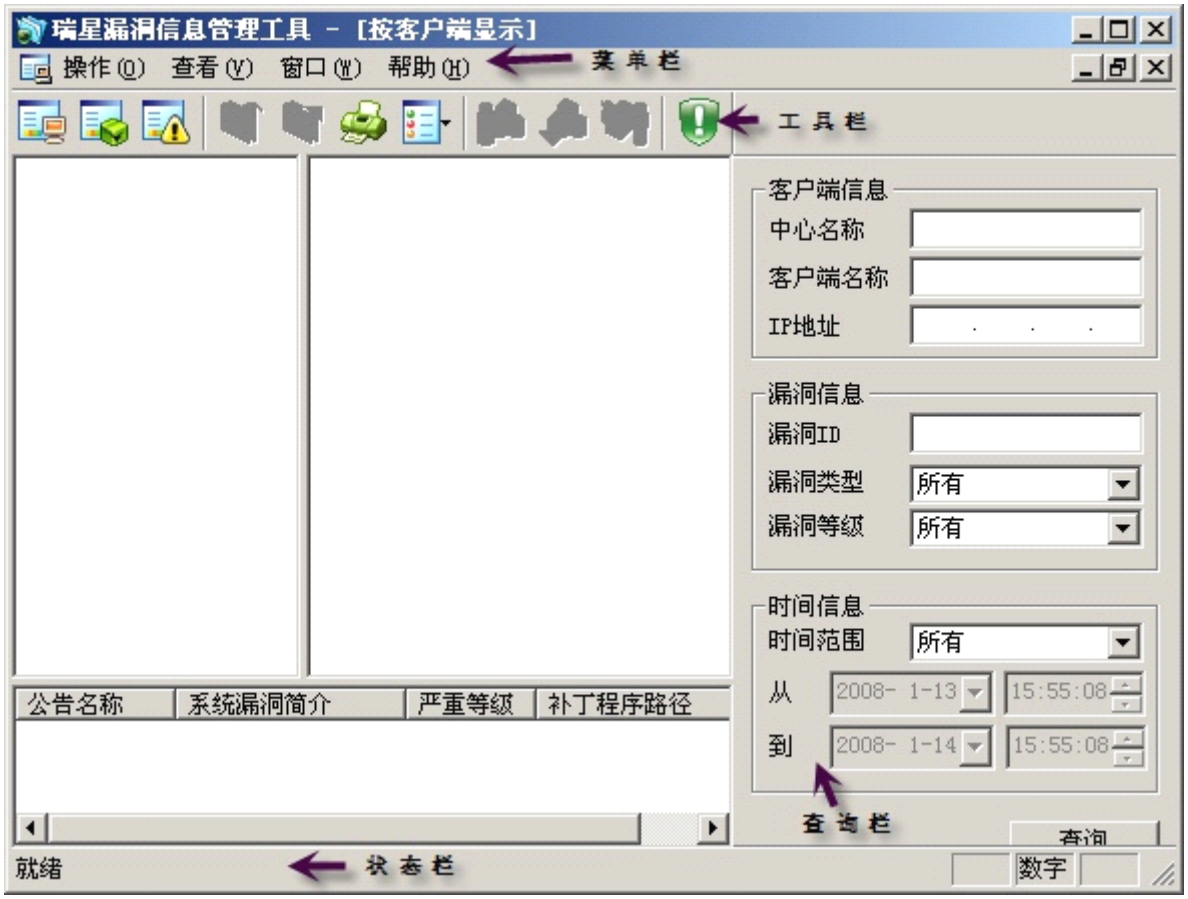

图 4106

当选择不同的查询方式来显示结果时，操作菜单的内容会有所不同。下面以【按系统漏洞显示】为例介绍漏洞管理工具的具体使用方法。用鼠标单击工具栏中的【按系统漏洞显示】按钮，显示扫描结果，如图 4111。选中某一漏洞信息后，单击鼠标右键，可以选择查看系统漏洞详细信息、手动导入补丁程序、通知瑞星下载中心下载补丁程序和通知安装补丁程序，如图 4 107。

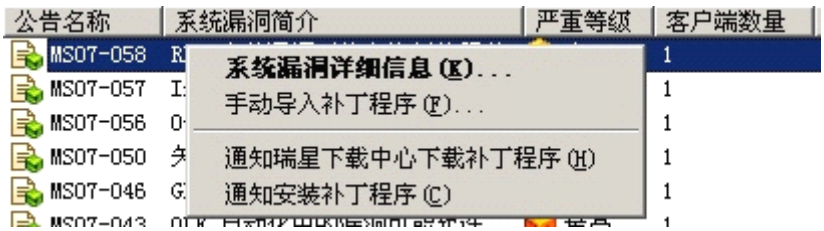

图 4107

漏洞扫描后需要为客户端安装漏洞补丁，具体设置如下：

1．首先通知系统中心下载补丁程序，可以在漏洞信息管理工具中选中某一漏洞信息后，单击鼠标右键选择【通知瑞星下载中心下载补丁程序】或在【操作】菜单中选择【通知瑞星下载中心下载补丁程序】则系统中心会下载补丁程序。如果不希望通过手动方式通知系统中心下载客户端需要的补丁程序，可以在4.1.3.6.5 漏洞扫描设置勾选【自动下载漏洞补丁程序】，这样系统中心会自动进行补丁程序的下载。

2．通知客户端安装补丁程序。注意：当系统中心已经存在补丁程序时，选择【通知安装补丁程序】即可。在漏洞信息管理工具中选择【操作】/【通知安装补丁程序】则通知选中的客户端会安装补丁程序。如果不希望通过手动方式通知客户端安装补丁程序，可以在 4.1.3.6.5 漏洞扫描设置勾选【自动通知客户端修复已下载的补丁程序】，当系统中心下载完补丁程序后，则会自动通知客户端安装补丁程序。当客户端收到通知后，如果 4.1.3.3.7 漏洞扫描设置中勾选了【自动安装补丁程序】，则客户端会及时修复其漏洞。若没有勾选该项则客户端托盘程序会弹出提示，告知用户某些漏洞在系统中心已有对应补丁，需要用户手动选择安装补丁程序。

为了方便管理，管理员可以设置定期进行漏洞扫描并及时为客户端安装补丁程序。具体设置可以参考4.1.3.3.7 漏洞扫描设置。

在【操作】菜单中选择【导出数据】选项，导出漏洞扫描的数据，用户选择保存类型、保存的信息和保存的路径，如图 4108。单击【选项】还可以选择客户端访问补丁共享目录的方式，有根据机器名称和机器 IP 两种方式，如图 4109。

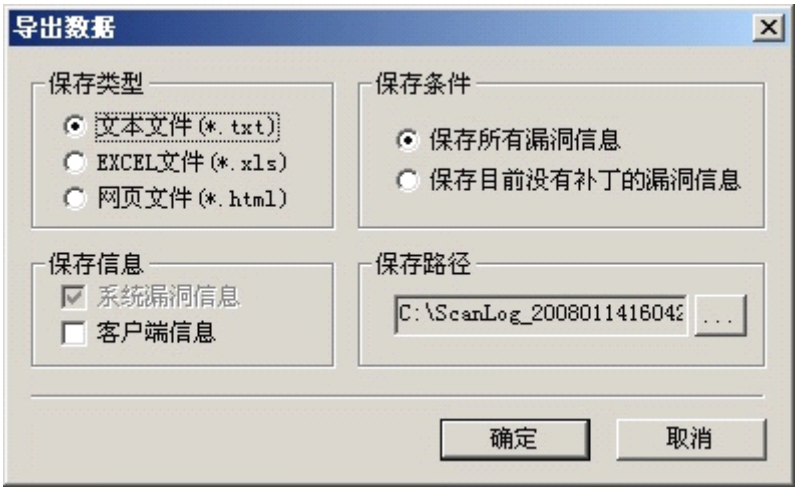

图 4108

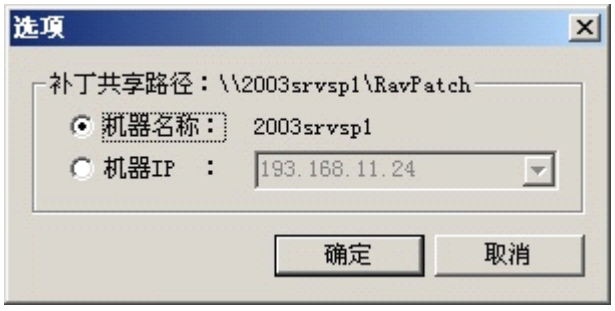

图 4109

当系统中心不能连接网络时，管理员可以通过导入补丁的方式导入漏洞补丁程序，当批量导入补丁程序时，可以选择【操作】菜单的【导入补丁程序】，在打开的浏览文件夹中选择已有的补丁程序；当只针对某个漏洞时，选择【操作】菜单的【手动导入补丁程序】导入即可。

4.2.4.2工具栏

界面菜单的下面是工具栏，为方便用户操作提供了以下快捷按钮：

 ：单击此按钮将按客户端显示所有漏洞信息；

 ：单击此按钮将按照系统漏洞显示信息；

 ：单击此按钮将按照不安全设置显示信息；

 ：单击此按钮导出数据，用户可以设置保存类型、保存条件及保存路径；

 ：当系统漏洞信息按照系统漏洞显示时，单击此按钮导入补丁程序；

 ：单击此按钮打印系统漏洞信息；

 ：单击此按钮选择查看方式，包括图标、列表、详细信息；

 ：单击此按钮通知客户端安装系统漏洞补丁程序，实现此操作也可以单击【操作】菜单，选择【通知安装补丁程序】；

 ：单击此按钮通知瑞星下载中心下载补丁程序，实现此操作也可以单击【操作】菜单，选择【通知瑞星下载中心下载补丁程序】；

 ：单击此按钮通知客户端修复不安全设置，实现此操作也可以单击【操作】菜单，选择【通知修复不安全设置】；

 ：关于瑞星漏洞信息管理工具的版本和版权信息。

按客户端显示所有漏洞信息时，在系统漏洞信息上双击左键或单击右键选择【系统漏洞详细信息】，可以查看该漏洞的详细信息，包括补丁下载路径信息。在不安全设置信息上双击左键或单击右键选择【不安全设置详细信息】，可以查看此项不安全设置的详细信息。

图 4110

按照系统漏洞显示信息时，在系统漏洞区域单击某一条系统漏洞信息，将显示此系统漏洞的分布情况，用户可以查看存在此漏洞的客户端。在系统漏洞信息上双击左键或单击右键选择【系统漏洞详细信息】，可以查看该漏洞的详细信息，包括补丁下载路径信息。

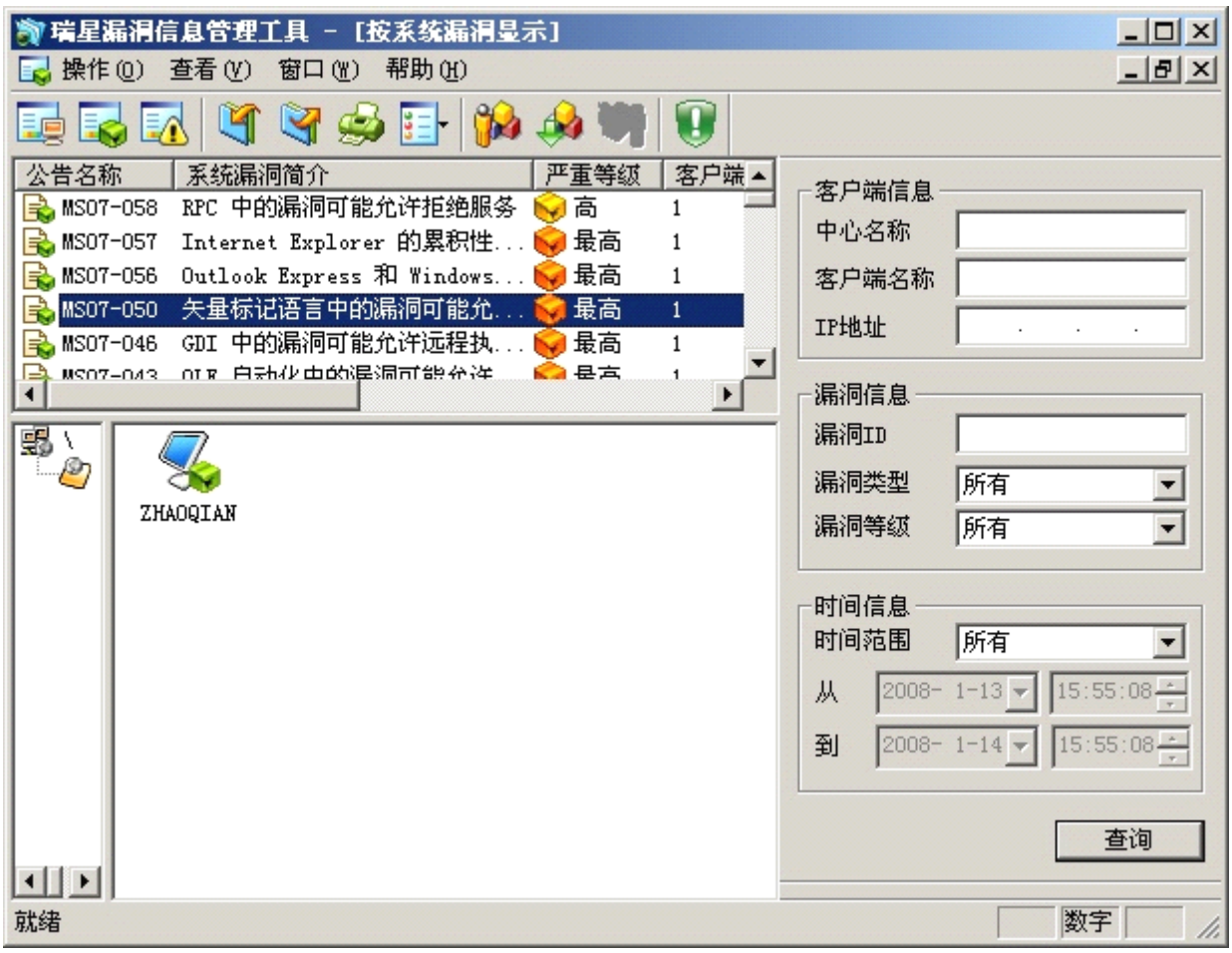

图 4111

按照不安全设置显示信息时，在不安全设置区域单击某一条不安全设置信息，将显示此不安全设置的分布情况，用户可以查看存在此不安全设置的客户端。在不安全设置信息上双击左键或单击右键选择【不安全设置详细信息】，可以查看此项不安全设置的详细信息。

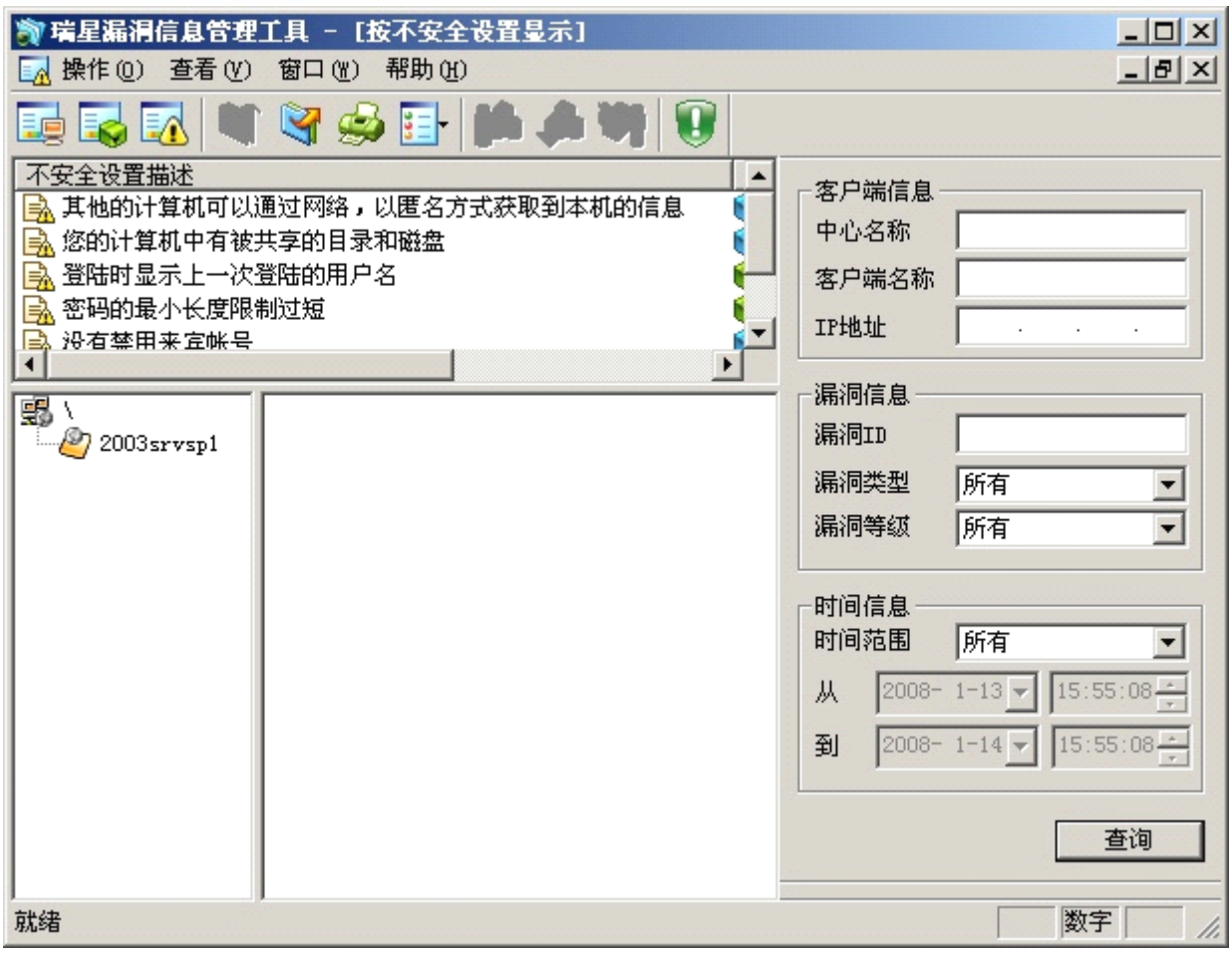

图 4112

4.2.4.3查询栏

在瑞星漏洞信息管理工具的右侧是查询栏，提供了按照客户端信息、漏洞信息、时间信息等多种查询条件，管理员可以输入相应查询条件，单击【查询】按钮对漏洞扫描结果进行查询。如果不输入任何查询条件直接单击【查询】，则会显示所有漏洞信息。

4.2.4.4状态栏

在瑞星漏洞信息管理工具的最下方是状态栏，显示当前程序运行状态以及按钮提示信息。

图 4113

4.2.5 Unix 客户端升级工具

瑞星杀毒软件网络版支持对 Unix 客户端的集成管理。为方便 Unix 客户端升级，瑞星杀毒软件网络版在管理控制台中设置了【Unix 客户端升级工具】菜单。具体的升级过程详见 4.1.7.3Unix 客户端升级。

4.2.6 下载中心管理工具

下载中心管理工具通过对下载中心目录（Rising\Rav\DLCenter）的清理和修复管理控制下载中心目录，也可以查看和管理本机的下载请求队列，对于正在下载的任务，用户可以通过删除操作改变下载任务的优先级。

在 Windows 界面上，单击【开始】/【程序】/【瑞星杀毒软件】/【瑞星工具】/【下载中心管理工具】，弹出瑞星下载中心管理控制台界面。

4.2.6.1清理设置

管理员可以设置升级文件保留组件的版本数，设定漏洞补丁文件最大使用硬盘空间的大小，避免无用文件占用过多硬盘空间，从而减少磁盘空间的占用。勾选【启用定时清理】，设置定时清理频率、具体清理时间。

在瑞星下载中心管理控制台界面上，单击  按钮或单击【文件】菜单，选择【设置】，打开【清理设置】对话框。

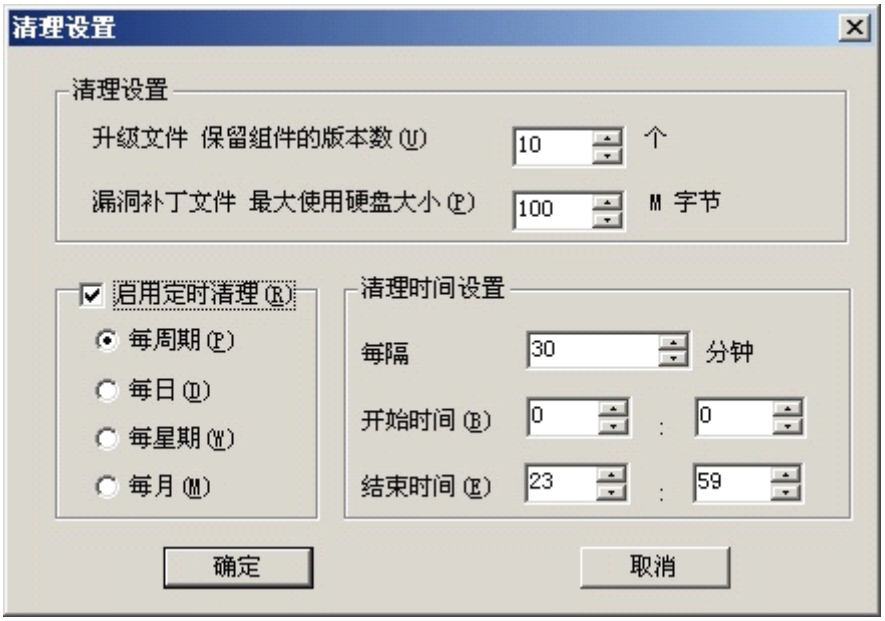

图 4114

注意：对硬盘上的升级文件删除过多也会影响升级速度，建议使用出厂默认设置以保证客户端升级的效率和速度。

4.2.6.2修复目录

当下载中心的文件损坏或丢失时，为了保证客户端正常下载文件，提供修复目录的功能，保证用户的正常下载。在下载中心管理工具中，单击【工具】\【修复目录】开始修复，如图：

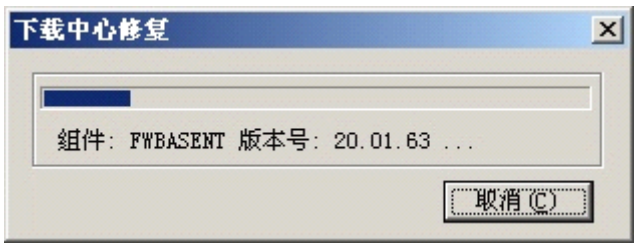

图 4115

4.2.6.3正在下载页

单击【正在下载】，打开正在下载页，当用户的计算机上装有 Update、Sender 或 Receiver 模块时，用户可以看到这些模块的下载队列列表。列表中显示出每项下载请求任务所请求的 URL、发出请求的 IP、请求的时间、状态等。在请求信息上单击右键，用户可以选择【删除任务】，程序将自动通知发出请求的对象该任务取消。

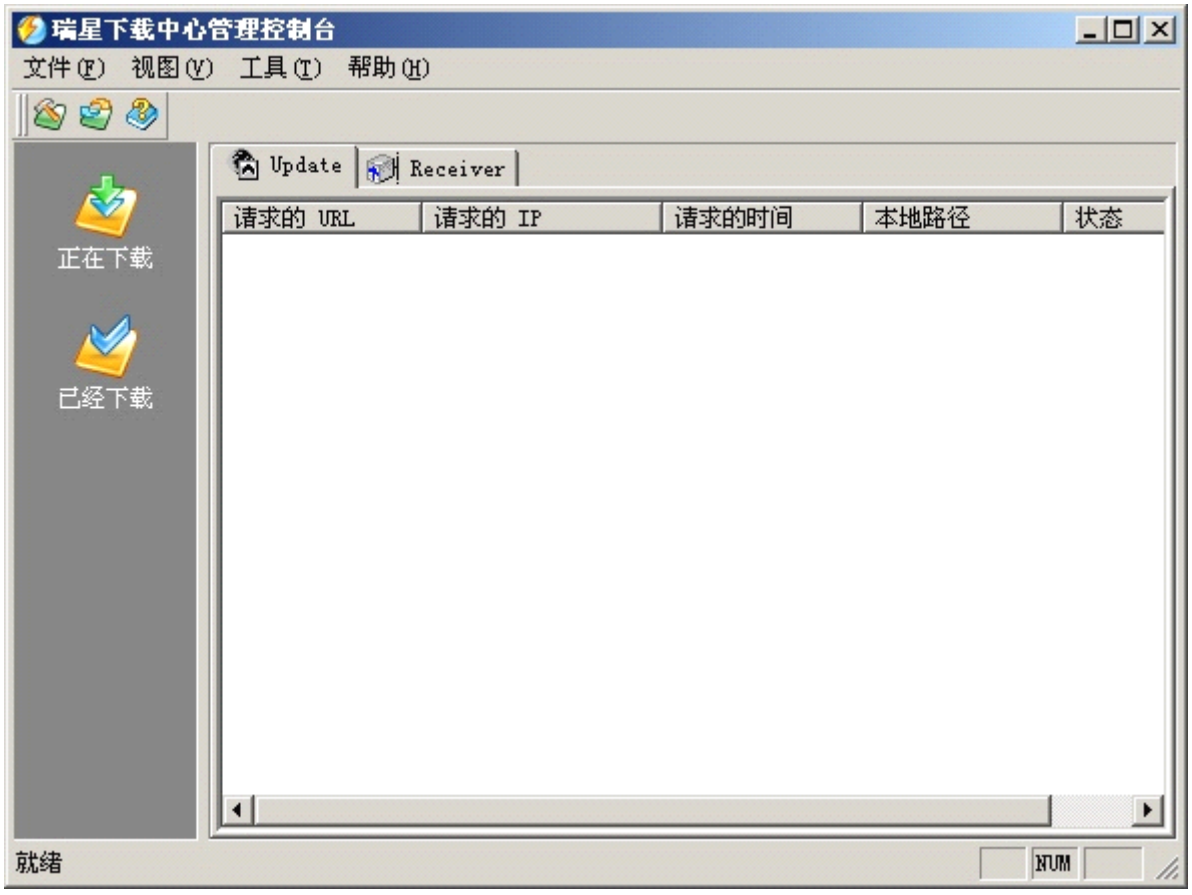

图 4116

4.2.6.4已经下载页

单击【已经下载】，打开已经下载页，用户可以在此处设置升级文件保留组件版本的个数、设定漏洞补丁文件最大使用硬盘空间的大小。单击【清理】按钮，按照当前设置分别对无用的升级文件和漏洞补丁文件进行清理。

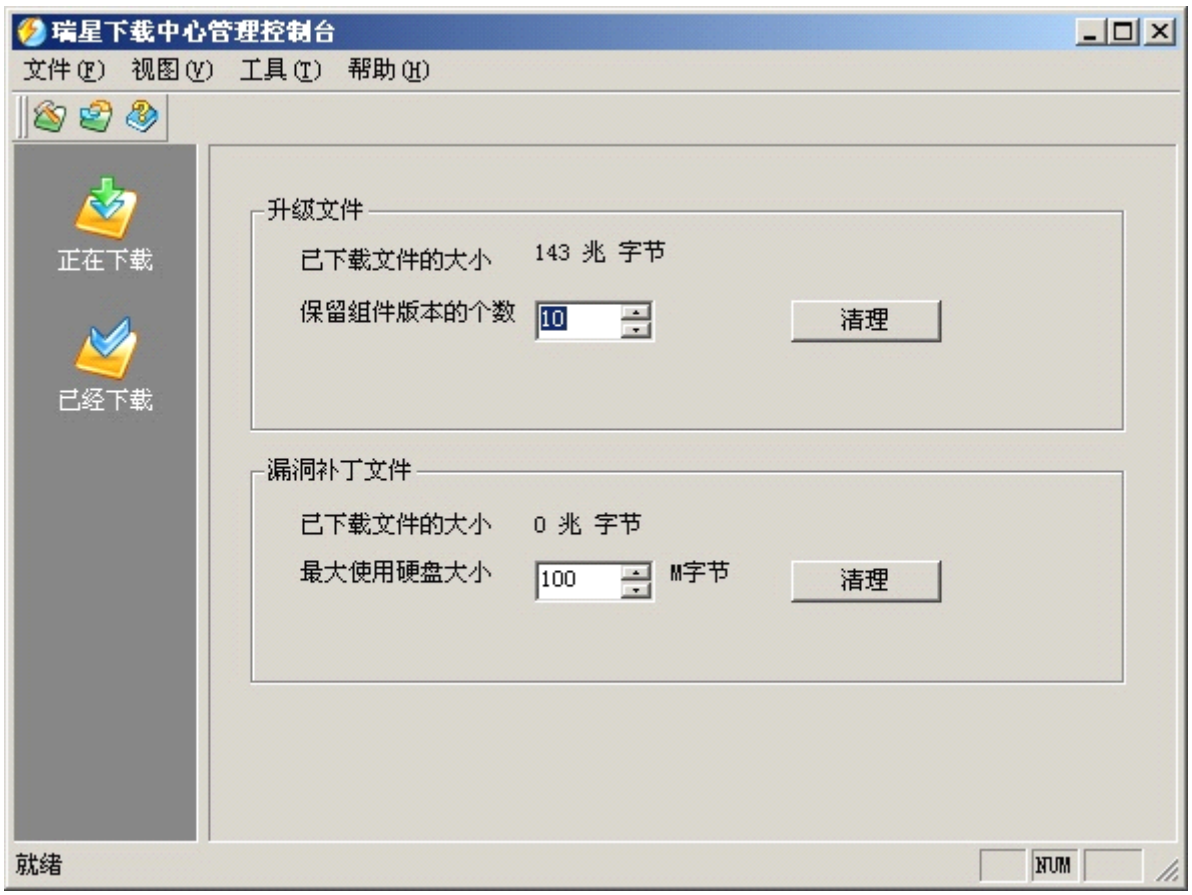

图 4117

4.2.7 日志打包工具

瑞星日志打包工具是一个收集瑞星产品运行过程中所产生信息，并输出一个标准的 Zip 格式压缩包的工具，用户将此压缩包反馈给瑞星公司以便于技术支持人员对用户在使用瑞星产品过程中产生的问题进行分析，并进一步提供最佳解决方案。

日志打包步骤如下：

第一步：在 Windows 界面上，单击【开始】/【程序】/【瑞星杀毒软件】/【瑞星工具】/【日志打包工具】，弹出瑞星日志打包工具界面。

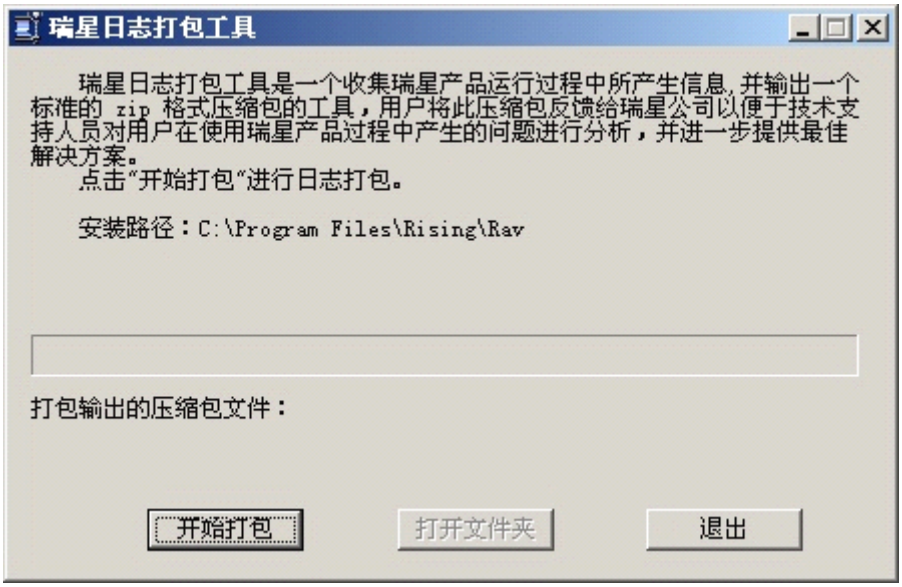

图 4118

第二步：单击【开始打包】按钮，在弹出的窗口中选择打包输出的压缩包文件的保存路径，输入文件名称，然后单击【保存】按钮开始打包。

第三步：打包完成后，瑞星日志打包工具提示“打包已经完成!”。

单击【开始打包】，重新打包日志；单击【打开文件夹】，打开日志压缩包所在的文件夹；单击【退出 】，关闭瑞星日志打包工具。

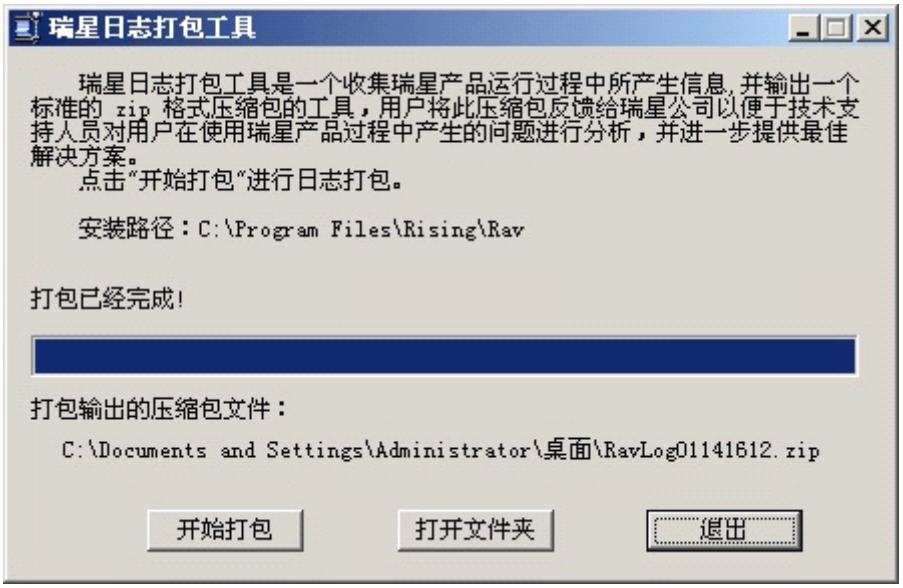

图 4119

4.2.8 客户端配置工具

通过客户端配置工具，用户可以完成对客户端系统选项、升级选项、漏洞扫描及其它内容的设置，并且能够查看本级系统中心及所属客户端范围内的升级代理列表。

打开客户端配置工具的方法：

方法一：在 Windows 界面上，单击【开始】/【程序】/【瑞星杀毒软件】/【瑞星工具】/【客户端配置工具】，打开客户端配置工具界面。

方法二：右键单击瑞星客户端托盘程序图标，在右键菜单中选择【选项】，打开客户端配置工具界面。

图 4120

说明：在高级企业版有“防火墙设置”此项功能；在高级企业专用版中，购买时定制了防火墙的情况下有此功能；网吧版、中小企业版、企业版和企业专用版中无此功能。

注意：对与通讯代理设置，RavSender 和 RavReceiver 配置页面，只有在本机上安装了通讯代理 RavSender 和 RavReceiver 后，才会在瑞星网络版客户端配置工具中有所体现。如果没有安装通讯代理 RavSender 和 RavReceiver，将不显示通讯代理设置页面。

4.2.8.1 系统设置

对客户端的系统设置进行设置，可以设置系统中心信息、客户端向系统中心注册的时间间隔和扫描病毒线程的优先级。

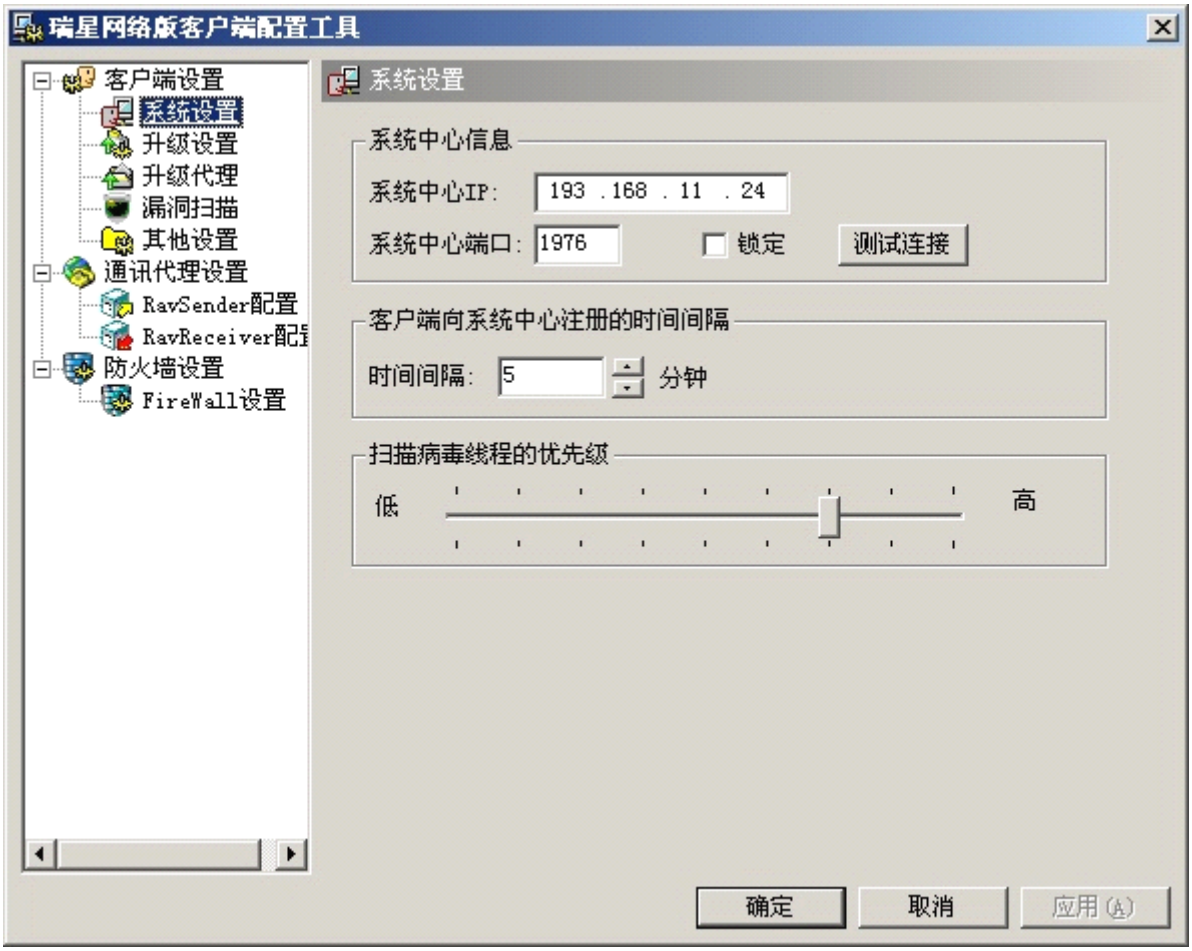

图 4121

勾选【锁定】选项，该客户端会锁定到这个系统中心所在的 IP 地址。单击【测试连接】按钮，测试客户端是否与系统中心连接，并显示提示信息。

【客户端向系统中心注册的时间间隔】：每 X 分钟向系统中心发送一次注册信息。

【扫描病毒线程的优先级】：值越大，扫描速度越快，同时占用系统资源也越多。

4.2.8.2升级设置

设置客户端的升级设置，用户可以选择升级的时间、频率和升级的方式。

图 4122

勾选【启用定时升级】按钮，将启用定时升级功能。勾选【静默升级】选项，每次升级将采用静默升级的方式。【只升级病毒特征库】选项客户端不可自主设置，只有系统中心可以设置。

4.2.8.3升级代理

查看和调整客户端的升级代理，在列表中显示管理员设置的升级代理。通过升级代理列表可以查看客户端所在网段范围内的升级代理或管理员指定的升级代理。通过【上移】和【下移】按钮改变升级代理的优先级别。

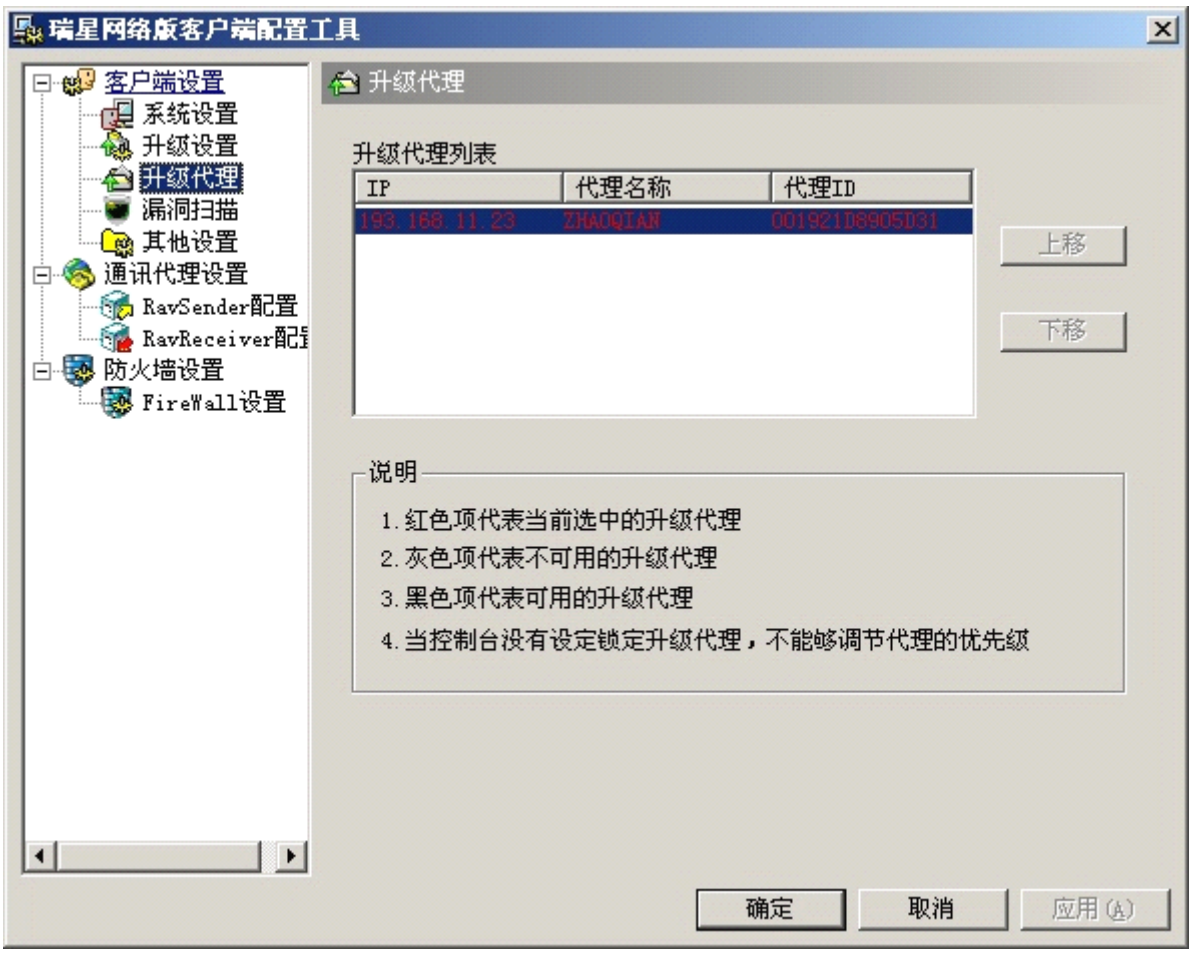

图 4123

4.2.8.4漏洞扫描

说明：在企业专用版和高级企业专用版中，在定制了漏洞扫描功能的情况下有此设置；网吧版中没有漏洞扫描功能，故无此设置；中小企业版、企业版和高级企业版中可以设置漏洞扫描功能。

设置客户端的漏洞扫描设置。勾选【启用定时扫描】，启用定时扫描功能。用户可以设置漏洞扫描的频率和时间、扫描的对象、扫描的严重级别。当系统中心通知客户端有补丁后，如果勾选【自动安装补丁程序】选项，则会立即安装补丁。用户可以选择是否静默安装，勾选【静默方式】选项将不提示用户自动安装。

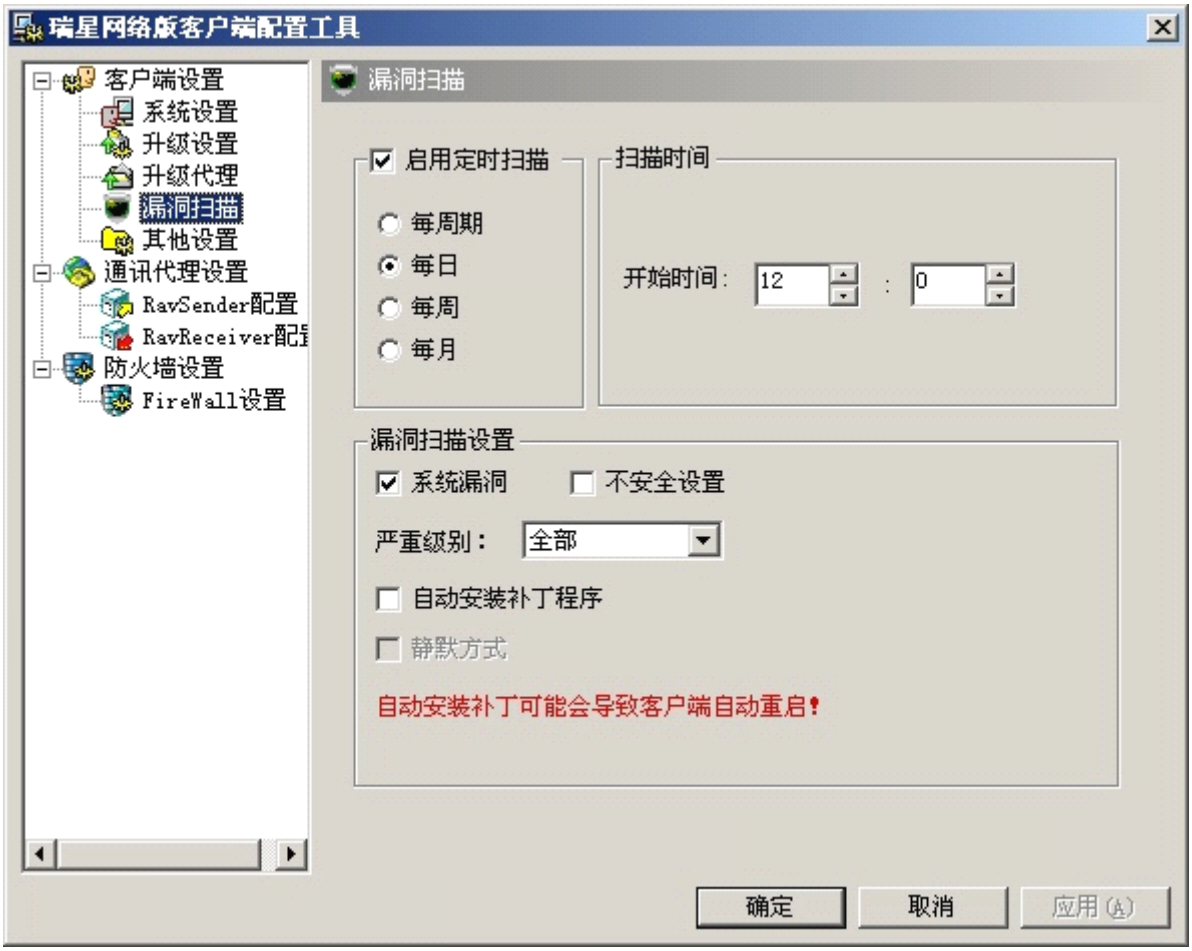

图 4124

4.2.8.5其他设置

在【其他设置】页面中可以设置消息的显示级别、显示的方式、通讯超时设置和数据包大小。勾选【记录应用程序在自我诊断级别的运行日志】选项，将记录应用程序的所有级别的运行日志，当瑞星网络版杀毒软件在使用中发生异常时，使用日志打包工具将日志打包后上报给瑞星公司，便于分析人员解决问题。关于如何打包日志，请参见“4.2.7 日志打包工具”。

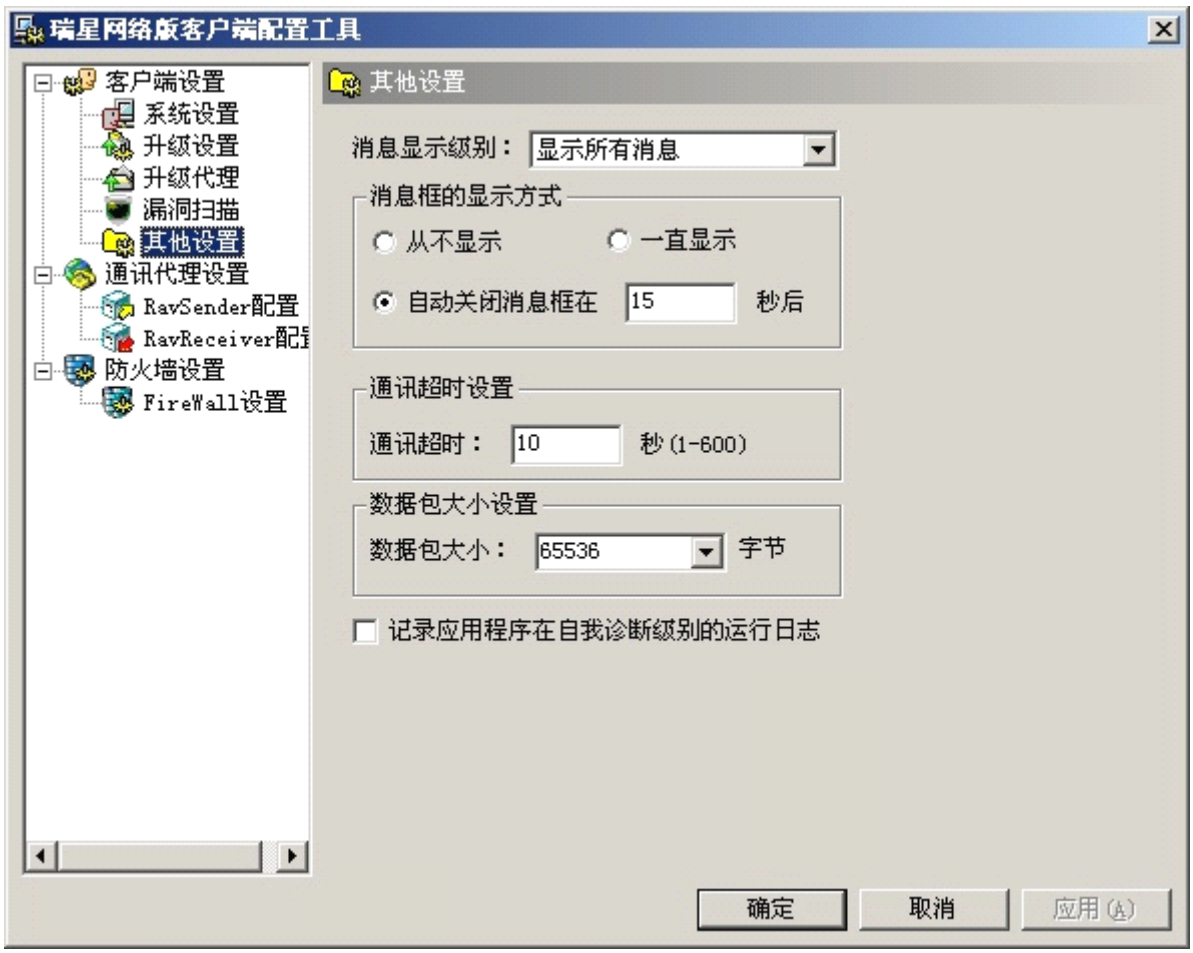

图 4125

- 消息框设置

双击任务栏托盘图标  将弹出一个窗口，为客户端消息框。当客户端收到消息时，此框将自动弹出，在【消息显示级别】选择中用户可以选择显示的消息内容范围，以及显示的方式，若选择自动关闭项，可以设置保留消息框的时间，默认时间为 15 秒。

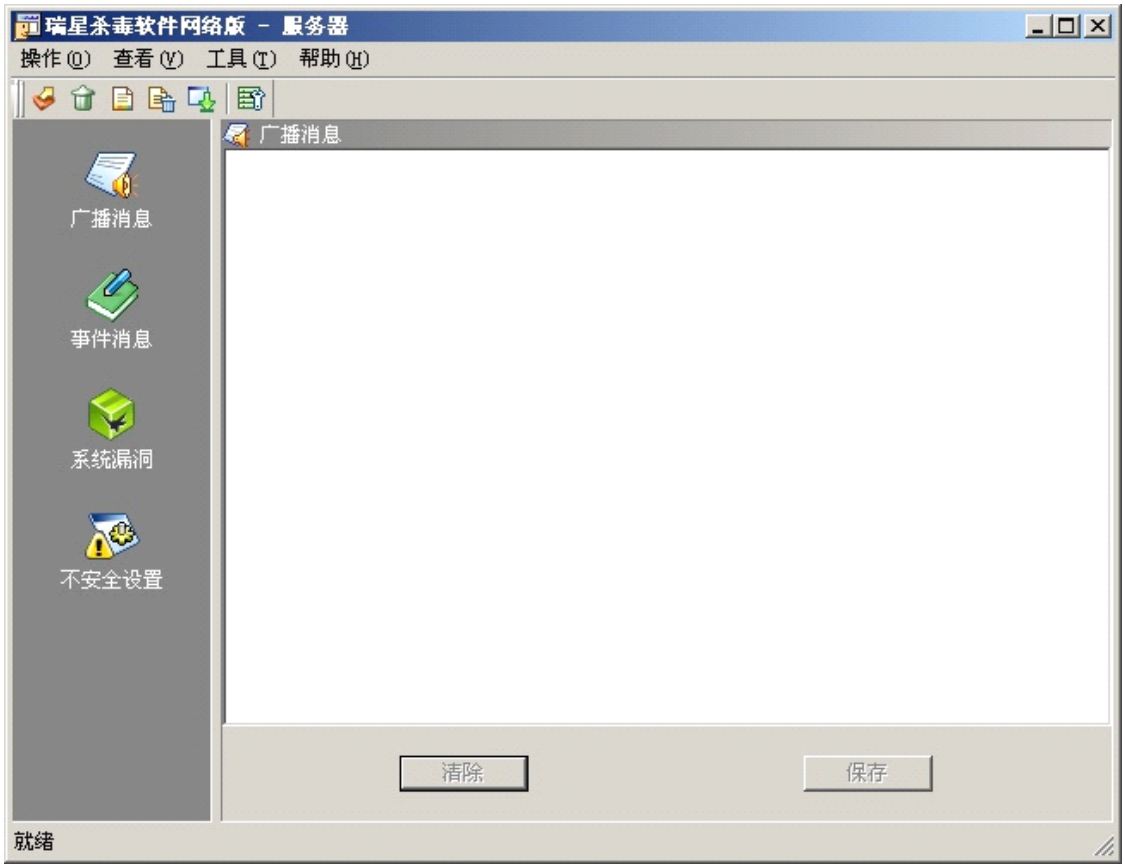

图 4126

- 通讯超时设置

通讯超时设置的时间范围是 1-600 秒，默认为 10 秒，用户可以根据网络状态更改超时设置。当网络状态不好时，需延长通讯等待时间，用户可以将通讯超时时间设置增长。

- 通讯包大小设置

为了保证客户端与系统中心正常通讯，根据网络状态的需要，用户可以调整数据包的大小。当用户的网络状态不好时，用户可以减小数据包大小。一般情况下，使用默认值 65536 字节。

注意：数据包如果设置得太小可能导致升级速度慢。

4.2.8.6RavSender 配置

当Sender通讯时用的默认端口被占用时，通过此项设置可以改变监听端口，从而保证通讯正常。

客户端向上级中心报告病毒、漏洞等信息的时候，要通过通讯代理，通讯代理内部会把这些报告排成队列，最大长度指的就是这个队列的最大长度，如果通讯阻塞，导致队列积攒过多，超过最大长度的就被忽略掉。默认为10000条记录。

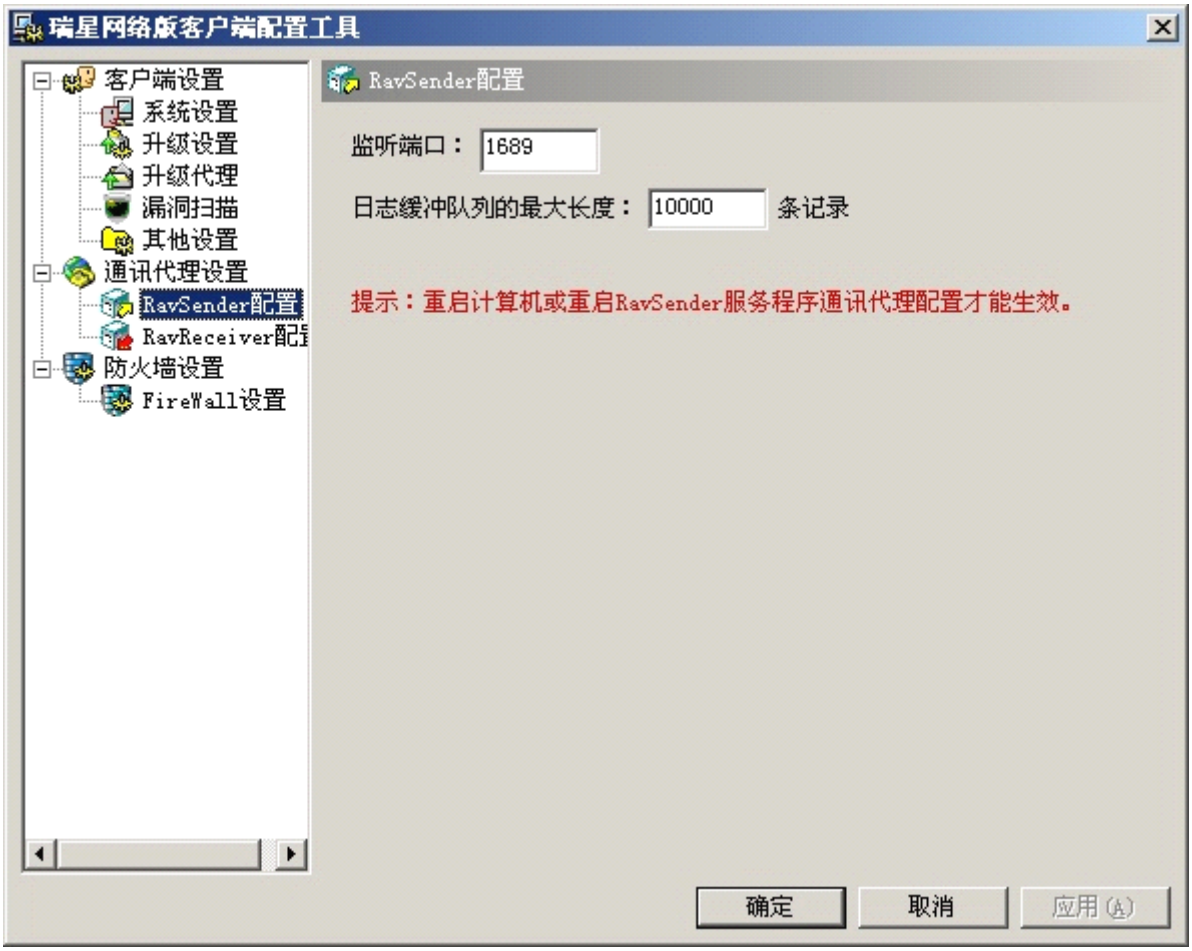

图 4127

注意：对 RavSender 的配置只有在重新启动计算机或重新启动 RavSender 服务程序后才生效。

4.2.8.7RavReceiver 配置

配置 Receiver（上级通讯代理）。用户可以设置监听端口、RavReceiver 指向的 RavSender 的信息和从上级中心获取防病毒策略的间隔时间。

当 Receiver 通讯时用的默认端口被占用时，通过这个设置可以改变监听端口，从而保证通讯正常。在此还可以查看并修改 RavReceiver 指向的 RavSender 的信息。

从上级中心获取防病毒策略的间隔时间：每若干分钟，会从上级中心获取防病毒策略。默认是 3 分钟，可以选择时间范围：1-60 分钟。

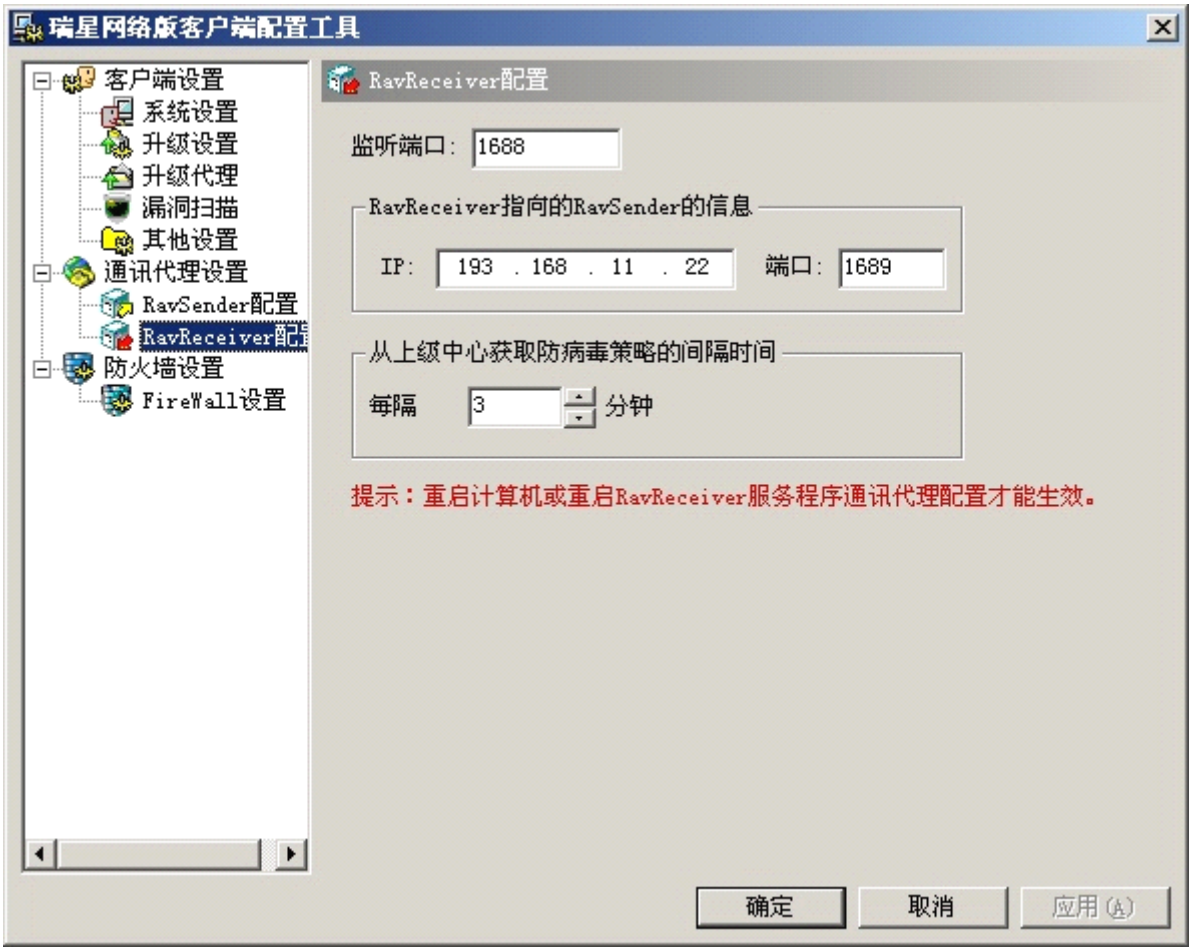

图 4128

注意：对 Receiver 的配置只有在重新启动计算机或重新启动 RavReceiver 服务程序后才生效。

4.2.8.8防火墙设置

说明：在高级企业版中有此设置页面；在高级企业专用版中购买时定制了防火墙功能的情况下有此设置页面；网吧版、中小企业版、企业版、企业专用版无此设置页。

在防火墙设置页面中可以设置防火墙事件的上报频率，分别为实时上报、每周期、每天、每周和每月。

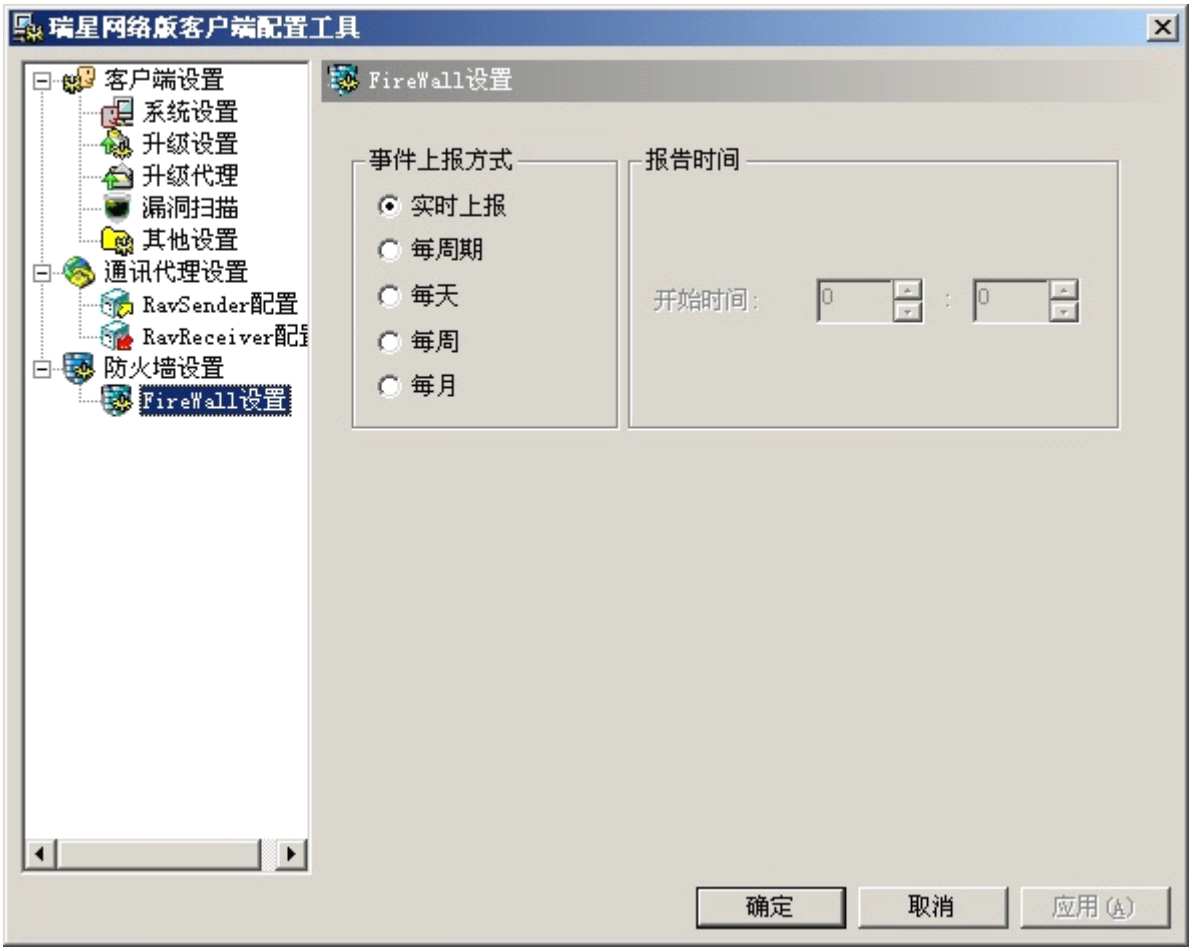

图 4129

4.2.9 报警插件配置工具

报警插件用于把病毒日志、漏洞扫描日志、事件日志、主动防御日志、防火墙事件日志定时或实时上报给指定的接收者。通过报警插件配置工具，用户可以配置报警插件，为插件设置报警内容。

在 Windows 界面上，选择【开始】/【程序】/【瑞星杀毒软件】/【报警插件配置工具】，即可打开报警插件配置工具界面。

注意：报警插件配置工具只能安装在系统中心所在计算机上，客户端无此工具。

图 4130

在报警插件配置工具的界面上，用户可以看到几种系统默认的报警插件，包括瑞星控制台报警插件、瑞星邮件报警插件、瑞星 SNMP 陷阱报警插件、瑞星消息框报警插件、瑞星 NT 日志报警插件、瑞星上级中心报警插件和瑞星系统日志报警插件。其中瑞星控制台报警插件和瑞星上级中心报警插件默认状态下已经含有报警内容，其它插件需要用户自己添加报警。报警插件配置工具还提供了病毒日志二次开发接口，除使用系统默认的七种报警插件外，用户还可以根据自己企业的需要对报警插件进行二次开发并添加插件。

下面分别对默认的几种插件进行简单介绍。

1. 瑞星控制台报警插件：把病毒日志、事件日志、主动防御日志和防火墙日志定时或实时上报给管理控制台，通过管理控制台的日志栏或日志查询统计工具可以查看报警信息。说明：在高级企业版中有防火墙日志报警插件；在高级企业专用版中购买时定制了防火墙功能的情况下有防火墙日志报警插件；网吧版、中小企业版、企业版、企业专用版中无此报警插件。

2. 瑞星上级中心报警插件：把漏洞扫描日志、事件日志和防火墙日志定时或实时上报给上级中心，上级中心通过管理控制台的日志栏或日志查询统计工具可以查看报警信息。说明：在高级企业版中有防火墙日志报警插件；在高级企业专用版中购买时定制了防火墙功能的情况下有防火墙日志报警插件；网吧版、中小企业版、企业版、企业专用版中无此报警插件。

3. 瑞星邮件报警插件：以发邮件的形式把病毒日志、事件日志定时或实时上报给指定邮件接收者。

4. 瑞星 SNMP 陷阱报警插件：把病毒日志、事件日志以发 Trap 的形式定时或实时上报给 SNMP 管理者。

5. 瑞星消息框报警插件：把病毒日志、事件日志通过 Messenger 服务定时或实时发送给指定计算机。注意：接收者必须启用 Messenger 服务才能接收到报警信息。

6. 瑞星 NT 日志报警插件：把病毒日志、事件日志定时或实时记录到系统中心所在计算机的操作系统应用程序日志中，通过系统中心所在计算机的事件查看器查看。

7. 瑞星系统日志报警插件：把病毒日志、事件日志按照 SysLog 协议定时或实时发送给系统日志服务器。

- **添加报警的步骤如下：**

以邮件报警插件为例介绍如何添加报警项目。

第一步：单击【添加报警】按钮，进入【请选择报警内容】页面。在描述栏中输入信息，并选择报警内容，单击【下一步】继续。

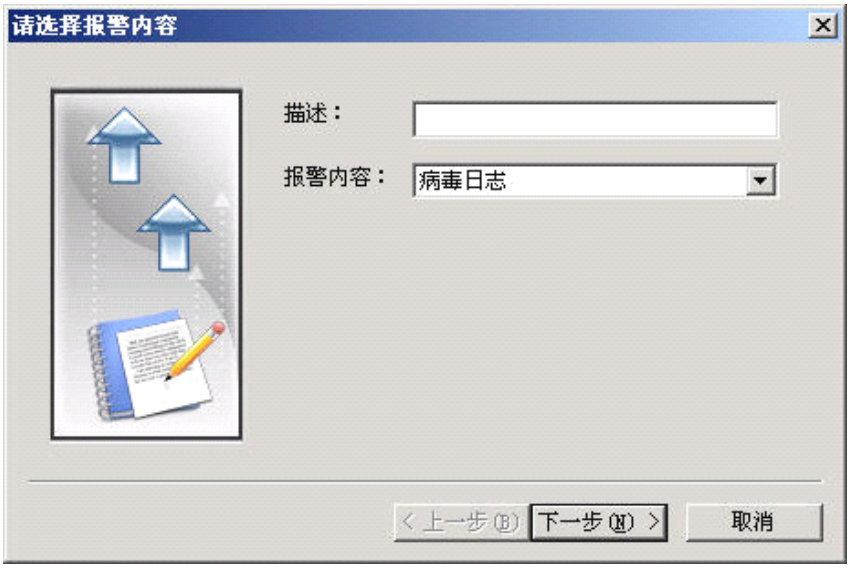

图 4131

第二步：进入【报警定时设置】页面，用户可以选择报警方式。单击【下一步】继续。

图 4132

第三步：进入【报警限制设置】页面，勾选【限制报警上限】选项，输入时间间隔和报警条数上限。在设置的时间间隔内，如果报警信息条数超过了报警条数上限时，报警插件会忽略后面的报警。单击【下一步】继续。

图 4133

第四步：进入【SMTP 设置】页面，按要求输入 SMTP 服务器地址、报警邮件接收者地址、邮件发送人地址，如 SMTP 服务器需要身份验证，需要勾选此项输入用户名和密码，单击【下一步】继续。

图 4134

第五步：进入【配置完成】页面，询问用户是否需要报告添加该报警之前的所有日志。单击【完成】按钮完成添加报警过程。

图 4135

- 测试报警：用户可以选择某个报警进行功能测试。选中准备测试的报警，单击【报警测试】按钮，弹出报警信息对话框：

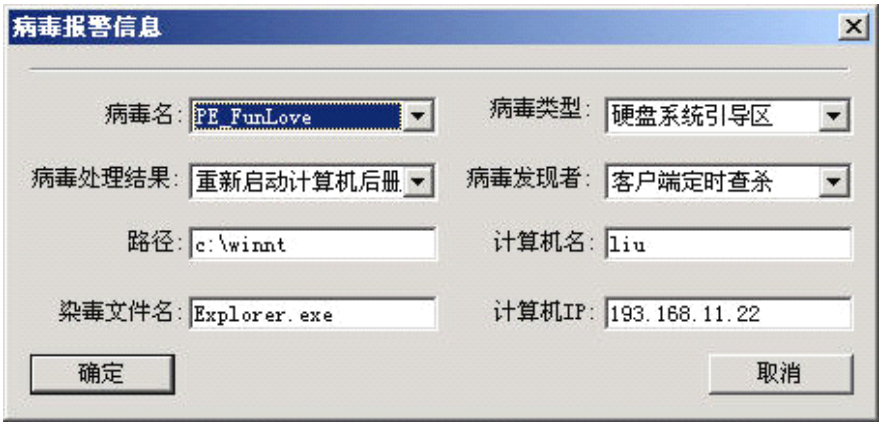

图 4136

用户可以对测试用的信息进行简单选择和修改，单击【确定】后，报警信息将根据此报警的设置发给指定的接收者。用户可以通过对应的方式，查看报警信息是否能够准确发送和接收。

- 删除报警：选中准备删除的报警，单击【删除报警】按钮即可。
- 修改报警：选中准备修改的报警，单击【修改报警】按钮，可以对报警内容、时间参数等选项进行修改。
- 添加/卸载插件：单击【添加插件】按钮，选择二次开发的插件程序添加新的插件；选中准备删除的插件，然后单击【卸载插件】按钮即可删除插件。

注意：此操作完成后需要重新启动瑞星网络版报警代理服务（Rav Net Alert）或重新启动计算机后才可以生效。

4.2.10 系统中心数据备份工具

通过系统中心数据备份工具，可以将系统中心的计算机列表、分组信息、授权信息、管理员信息、组策略、黑白名单、升级设置等重要数据和设置信息保存并导出为 IDF 格式的文件，当重新安装瑞星杀毒软

件网络版系统中心时，用户可以直接导入备份数据文件，简化了重新安装系统中心后的设置操作。

图 4137

4.2.10.1 导出数据

操作步骤如下：

在 Windows 界面中，选择【开始】/【程序】/【瑞星杀毒软件】/【瑞星工具】/【系统中心数据备份工具】，在打开的工具界面上选择【导出】，然后单击【下一步】，选择保存路径并输入保存文件名，选择要导出的系统中心数据类型，单击【下一步】开始导出系统中心数据，单击【完成】按钮结束。

图 4138

4.2.10.2 导入数据

在 Windows 界面中，选择【开始】/【程序】/【瑞星杀毒软件】/【瑞星工具】/【系统中心数据备份工具】，选择【导入】，然后单击【下一步】，选择要导入的系统中心数据文件和系统中心数据类型，单击【下一步】开始导入系统中心数据，单击【完成】按钮结束。

4.2.11 客户端搜索工具

客户端搜索工具能够扫描指定网段或网络邻居的客户端是否安装了瑞星杀毒软件或其它厂商的杀毒软件。

在 Windows 界面中，选择【开始】/【程序】/【瑞星杀毒软件】/【瑞星工具】/【客户端搜索工具】，打开客户端搜索工具界面。对话框左侧显示了网络邻居，右侧显示扫描结果列表。

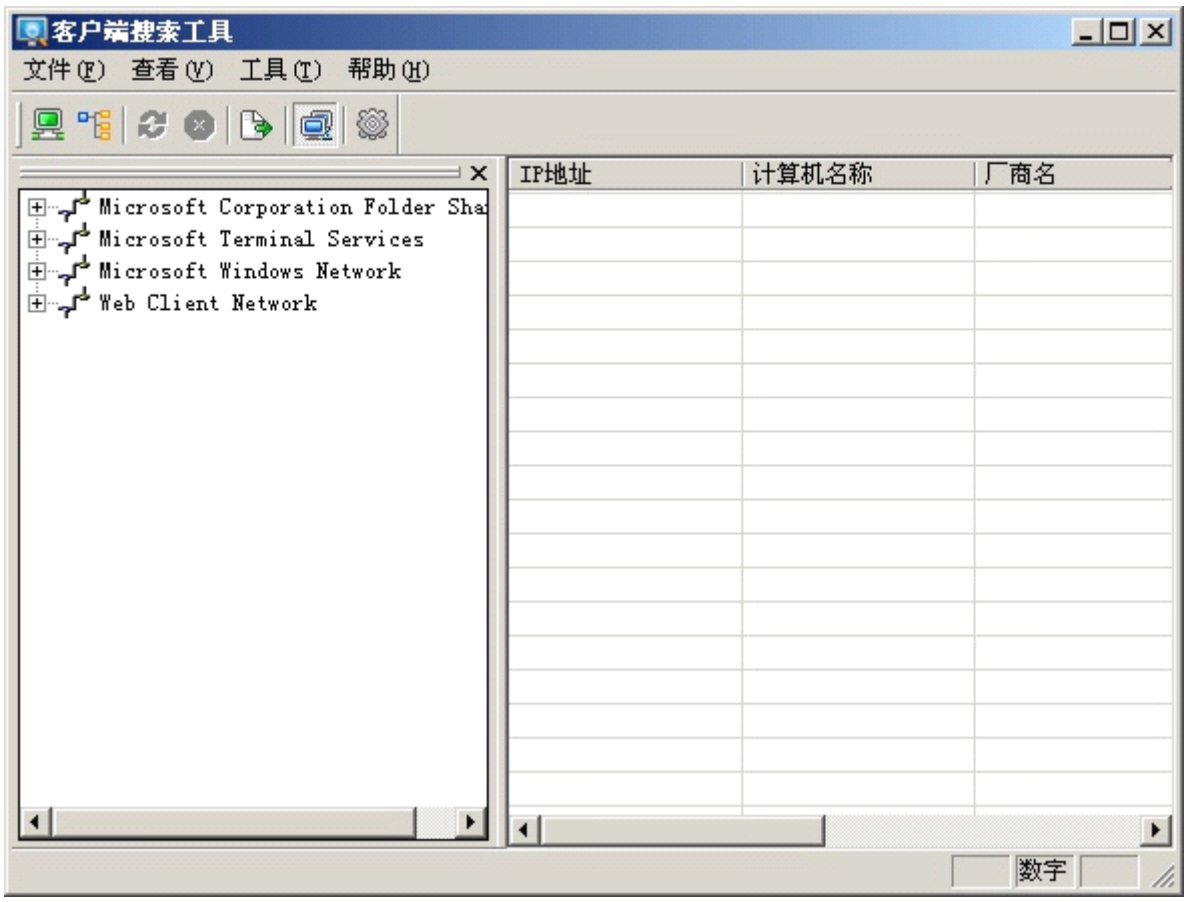

图 4139

4.2.11.1 扫描选项设置

选择【工具】/【选项】，或者单击工具栏上的  按钮，弹出【扫描选项】对话框，可以对扫描客户端的各项参数进行设置。

扫描线程数：值越大，扫描速度越快，同时占用系统资源也越多。

Ping 选项：

1、 ICMP Ping 超时：默认为 1000 毫秒，建议使用默认值；

2、 解析计算机名：勾选此项，能够根据 IP 地址解析出计算机名或根据计算机名解析出 IP 地址；

3、 即使 Ping 失败仍继续检测：默认不勾选。

瑞星选项：选择检测瑞星杀毒软件单机版或网络版，可多选。

1、如果勾选了检测单机版，在扫描时会弹出【远程管理员帐户】对话框要求输入指定客户端的帐户名和密码。

2、如果勾选了检测网络版，用户可以自己指定 TCP 端口范围，在【TCP 端口范围】前面勾选，输入端口范围；也可以不指定，不勾选【TCP 端口范围】即可。此项默认不勾选。

检测其他厂商的杀毒软件：勾选此项可以检测指定客户端是否安装了瑞星以外的其它厂商的杀毒软件，单击【编辑】按钮可以选择检测哪些杀毒软件，通过【添加】按钮可以自己配置其它杀毒软件。

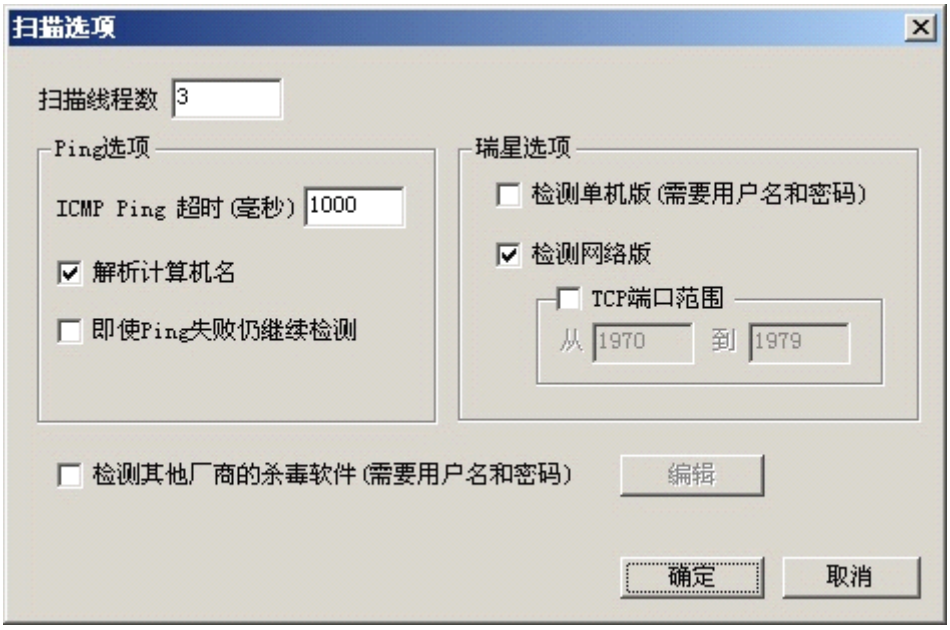

图 4140

4.2.11.2 扫描客户端

扫描组：在左侧网络邻居中选中准备扫描的组后，可以通过选择菜单【文件】/【扫描组】，或单击 按钮，或在该组上单击右键选择扫描此组。

扫描网段：可以通过选择菜单【文件】/【扫描网段】，或单击 按钮，输入要进行扫描的 IP 地址范围。

停止扫描：在对客户端进行扫描时，若想停止扫描，点击工具栏上的 按钮即可。

4.2.11.3 导出

通过选择菜单【文件】/【导出】或单击工具栏中的按钮 ，可以将客户端搜索工具的扫描结果导出为*.dat 格式的文件。

4.2.12 分组导入工具

此工具可以从活动目录或网上邻居获取计算机分组信息自动生成分组规则。

在 Windows 界面中，选择【开始】/【程序】/【瑞星杀毒软件】/【瑞星工具】/【分组导入工具】。

操作步骤如下：
第一步：【登录瑞星网络版系统中心】界面中输入管理员帐号和口令，单击【登录】按钮。

注意：超级管理员和操作管理员可以登录本工具，审计管理员不可以登录本工具。

第二步：若要从活动目录服务器获取计算机分组信息生成分组规则，选择【活动目录】，单击【下一

步】进入第三步；若要从网上邻居获取计算机分组信息生成分组规则，选择【网上邻居】，单击【下一步】进入第五步。

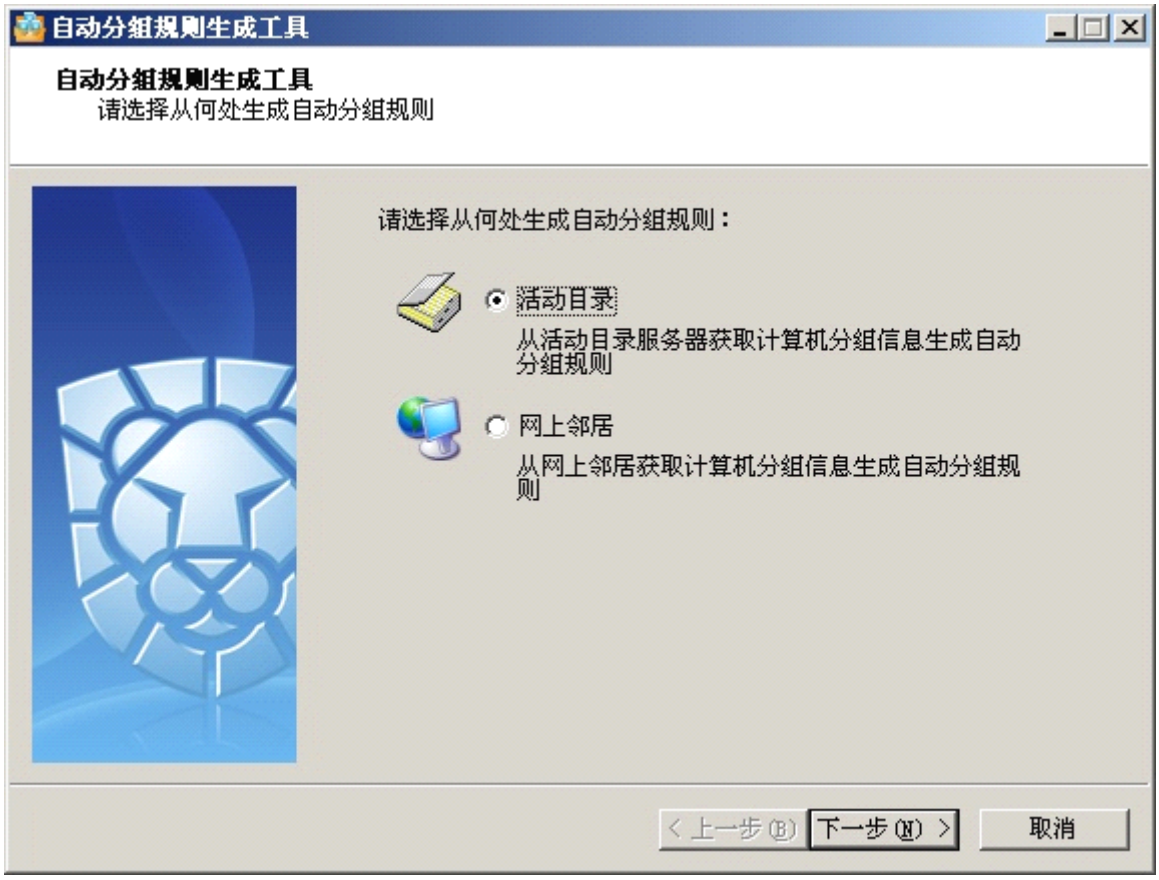

图 4141

第三步：输入活动目录服务器、用户名和密码，单击【下一步】继续。

图 4142

第四步：在界面左侧的活动目录上选择组织单元，单击移动按钮，添加到右边的分组规则列表中。单击【完成】按钮生成自动分组规则。

注意：通过单击界面右下角的【向上】或【向下】按钮可以调整生成的分组规则的顺序。

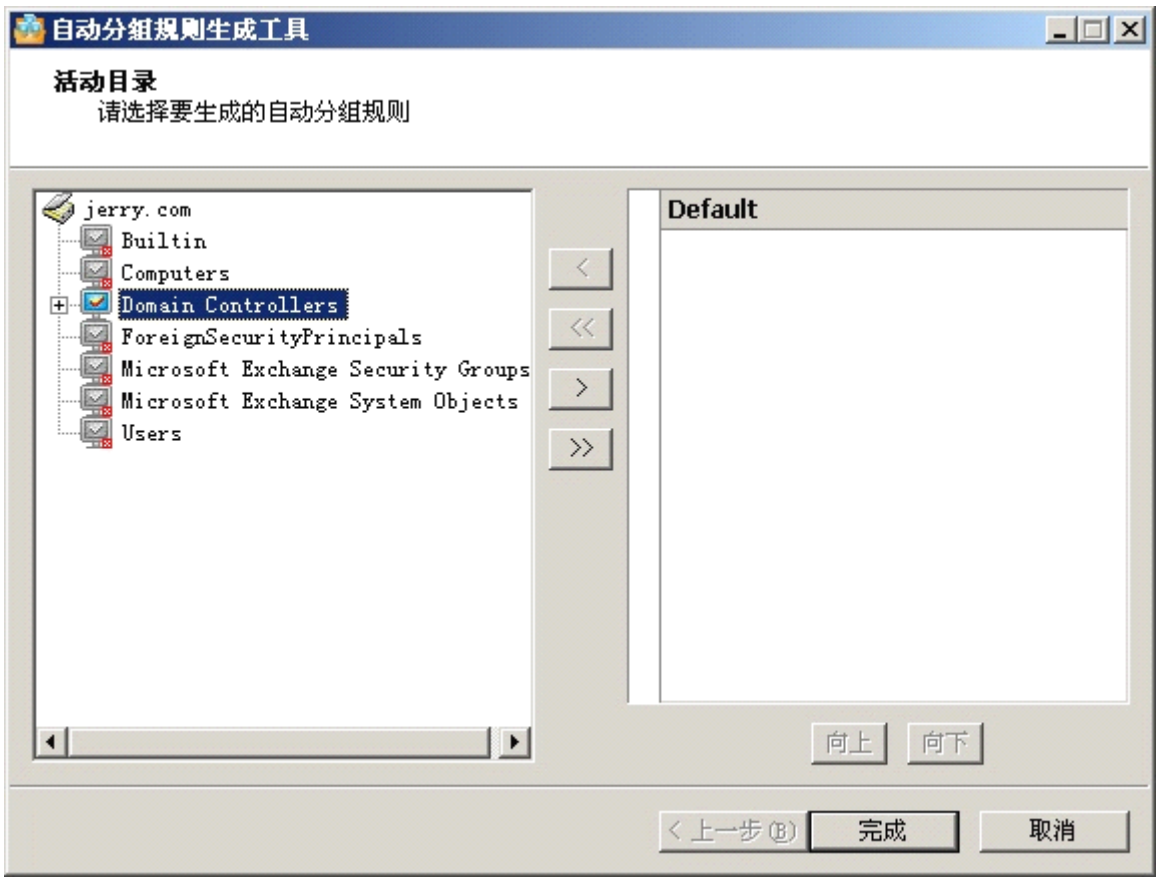

图 4143

第五步：若在第二步中选择了【网上邻居】，在界面左侧选择工作组，单击移动按钮，添加到右边的分组规则列表中。单击【完成】按钮生成自动分组规则。

注意：通过单击界面右下角的【向上】或【向下】按钮可以调整生成的分组规则的顺序。

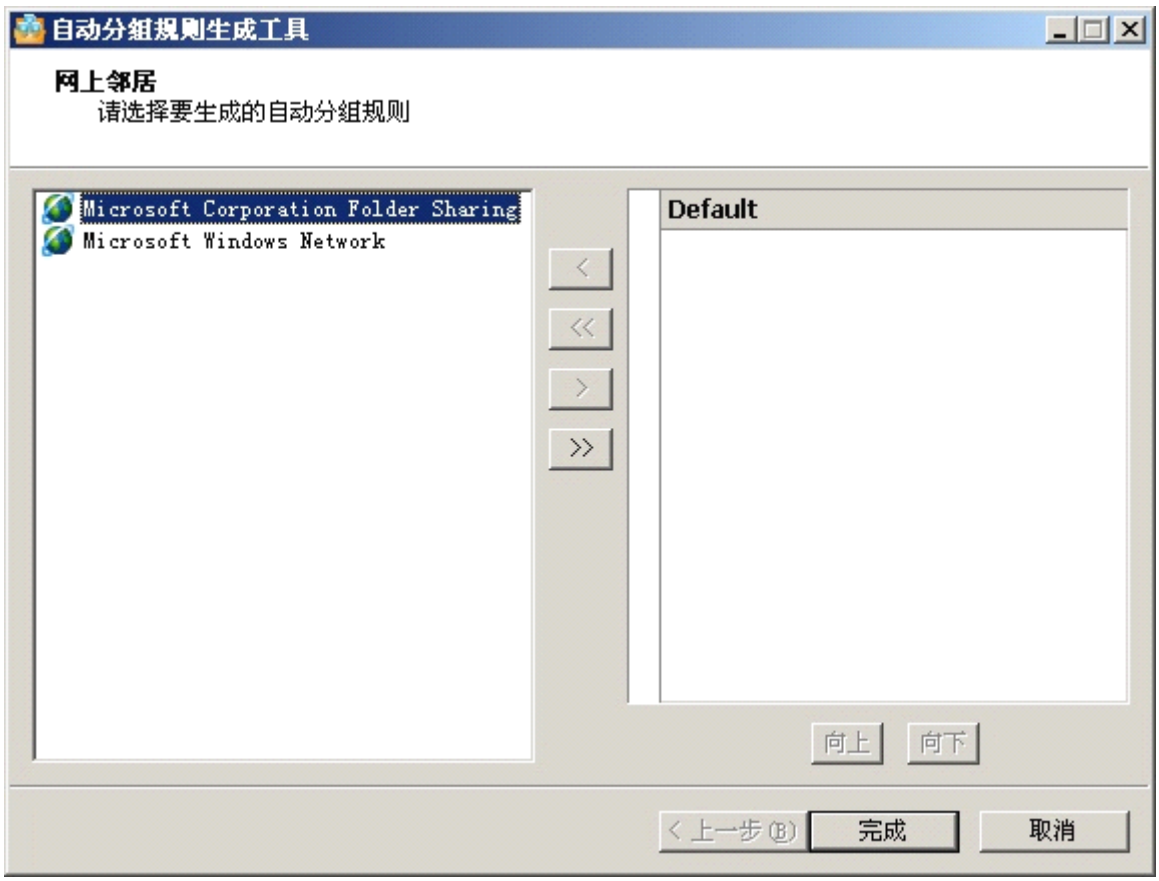

图 4144

生成分组规则后，用户可以通过以下步骤立即应用分组规则：在组管理界面上右键单击【剩余组】，选择【立即应用自动分组规则】，剩余组中的客户端将按照分组规则自动加入对应组中。

4.2.13 客户端安装包制作工具

客户端安装包制作工具利用系统中心上瑞星安装目录下的文件，制作出相应版本的客户端安装包，避免客户端利用光盘安装后需要升级才能达到最新版本的繁琐操作。具体如何使用请参见 3.2.5 通过客户端安装包制作工具定制的安装程序安装。

5 客户端本地杀毒软件的使用

瑞星客户端本地杀毒软件承担为客户机防病毒的任务，它由查杀病毒、实时监控、主动防御、瑞星工具、电脑安检和网络通讯模块等几部分组成，保障用户计算机在安全的环境中运行。杀毒软件可以在发现病毒后及时对病毒进行处理；利用实时监控功能监控文件、邮件和网页病毒，有目的的针对这几类病毒进行处理；同时能够及时发现含有恶意行为的程序，阻止其对计算机进行恶意攻击，做到提前为用户预防病毒，也为分析人员提供了更多的发现恶意程序的依据；另外，对计算机定期进行安全检测，可以使用户尽早发现漏洞或不安全设置并且及时补救，使得计算机免遭病毒侵袭；用户还可以利用各种工具进行杀毒操作；杀毒软件会定期上报所有日志到系统中心，为系统管理员分析整个网络中的安全情况提供大量的依据。总之，杀毒软件利用其有效的病毒查杀、可控的危险行为防御、及时的电脑安全检测、定期的日志上报和分析，全方位地保障用户计算机以及整个网络的安全。

5.1 启动瑞星杀毒软件主程序

通过以下几种方式，用户可以快速启动瑞星杀毒软件主程序：

双击 Windows 桌面上的瑞星杀毒软件快捷方式图标	
双击 Windows 任务栏中的瑞星杀毒软件图标	
单击 Windows 快速启动栏中的瑞星杀毒软件图标	
用鼠标左键单击瑞星杀毒软件图标，在显示菜单中选择【启动瑞星杀毒软件】	
选择【开始】/【程序】/【瑞星杀毒软件】/【瑞星杀毒软件】	

5.2 主程序界面说明

5.2.1 瑞星主程序界面说明

瑞星杀毒软件主程序界面是用户使用的主要操作界面，此界面为用户提供了瑞星杀毒软件所有的功能

和快捷控制选项。

图 51

菜单栏：

菜单栏包括【操作】、【视图】、【设置】和【帮助】四个菜单选项。

图 52

标签页：

瑞星杀毒软件提供了六个标签页面，分别是首页、杀毒、监控、防御、工具、安检。

图 53

首页：

在瑞星杀毒软件的首页中，显示了操作日志、瑞星信息中心和操作按钮三部分信息，具体功能如下：

操作日志：提供给用户主要的操作日志信息。

信息中心：提供给用户最新的安全信息。

操作按钮：提供给用户快捷的操作方式。

图 54

杀毒：

提供给用户自主选择的杀毒方式，用户在对象栏中可以选择查杀目标和快捷方式，也可以方便地在设置栏中对病毒的处理方式和隔离区空间大小等进行设置。

图 55

监控：

此界面显示了瑞星监控及其状态。包括的监控有：文件监控、邮件监控和网页监控。用户可以通过单击【开启】或【关闭】按钮控制监控状态。

图 56

防御：

主动防御是一种阻止恶意程序执行的技术。瑞星的主动防御技术提供了更开放的高级用户自定义规则的功能，用户可以根据自己系统的特殊情况，制定独特的防御规则，使主动防御可以最大限度的保护系统 。

主动防御功能包括：系统加固、应用程序访问控制、应用程序保护、程序启动控制、恶意行为检测、隐藏进程检测和自我保护等功能。具体说明详见 5.6 主动防御。

图 57

工具：

此界面包含病毒隔离系统、其它嵌入式杀毒等瑞星工具，显示工具名、版本信息、帮助、简单介绍等信息。单击某项标题，这些工具可以按照工具名称、大小、版本信息进行排序。单击【运行】可以打开相

应工具。在界面底部，单击【检查更新】按钮，程序将连接系统中心下载最新的工具包，提供给用户最新的安全工具。如果用户在使用中有不理解的地方，单击【帮助】链接到瑞星帮助文件了解帮助信息。

图 58

安检：

为用户提供全面的评测日志，方便用户了解当前计算机的安全等级及系统状态。并根据用户计算机的情况推荐用户进行相应的操作，提高计算机的安全等级。用户可以单击【详细报告】了解检查项目具体细节。

图 59

5.2.2 菜单说明

5.2.2.1【操作】菜单说明

【操作】菜单包含瑞星杀毒软件基本操作，此菜单中除了可以对查杀目标进行【查杀】、【停止】和【退出】操作外，还可以通过此菜单中的【历史记录】查看并管理以往用户使用瑞星杀毒软件的所有操作记录。

图 510

5.2.2.2【视图】菜单说明

用户可在【视图】菜单中对首页、杀毒、监控、防御、工具和安检六个标签页进行切换。

图 511

5.2.2.3【设置】菜单说明

【设置】菜单包含各种功能设置选项，包括详细设置、监控设置、防御设置、切换皮肤、切换语言和上报可疑文件。具体设置详见 5.9 设置。

图 512

5.2.2.4【帮助】菜单说明

瑞星杀毒软件提供了细致周到的帮助功能。通过【帮助文件】，可以打开瑞星的帮助文件，有助于用户快速了解产品或解决在使用过程中遇到的疑难问题，用户在任何界面的显示页中按“F1”键也可以看到相应的帮助；选择【官方网站】登录瑞星官方网站；选择【卡卡社区】进入卡卡社区；还可以选择【关于瑞星】查看瑞星杀毒软件的相关信息。

图 513

5.3 首页

操作日志：为用户提供多方位的操作日志信息，包括程序版本、上次在线升级日期、病毒库发布日期和上次全盘查杀日期。

信息中心：提供最新的安全信息，用户可以及时的了解到安全资讯。

操作按钮：提供给用户快捷方便的操作方式，分别为：电脑安检、全盘杀毒和在线服务。

【电脑安检】：功能详见 5.8 安检。

【全盘杀毒】：功能详见 5.4 杀毒。

【在线服务】：提供给用户一个与瑞星反病毒专家在线沟通的平台。

5.4 杀毒

在左侧的对象栏中用户可以得到方便快捷的查杀病毒方式，用户可以在查杀目标或快捷方式页面切换。单击设置栏中的【开始查杀】按钮，即开始查杀所选目标，发现病毒时程序会采取用户选择的处理方法。查杀过程中可随时选择【暂停查杀】按钮暂停查杀过程，按【继续查杀】可继续查杀病毒，也可以选择【停止查杀】按钮结束当前操作。

如果用户需要对某一文件杀毒，也可以拖拽该文件到瑞星杀毒软件的主界面上，或者在该文件上单击右键，选择【瑞星杀毒】，此时瑞星杀毒软件将转到杀毒标签页，并显示杀毒结果。

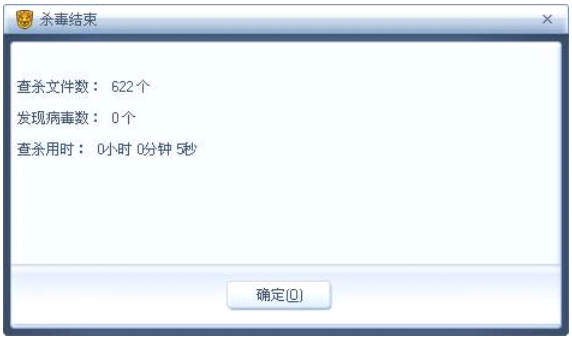

图 514

当发现病毒时，会在【更多信息】页面下方的病毒列表中详细的列出病毒所在的文件名、全路径、病

毒名和处理结果。

病毒列表：若瑞星杀毒软件发现病毒，则会将文件名、所在文件夹、病毒名称和处理结果显示在此窗口中。在每个文件名称前面有图标标明病毒类型，各图标含义如下：

	未知病毒		引导区病毒		未知宏
	Dos 下的 com 病毒		Windows 下的 le 病毒		未知脚本
	Dos 下的 exe 病毒		普通型病毒		未知邮件
	Windows 下的 pe 病毒		Unix 下的 elf 文件		未知 Windows
	Windows 下的 ne 病毒		邮件病毒		未知 Dos
	内存病毒		软盘引导区		未知引导区
	宏病毒		硬盘主引导记录		
	脚本病毒		硬盘系统引导区		

在病毒列表中，用鼠标右键单击某项，选择【病毒信息】，可连接到瑞星反病毒资讯网了解此病毒的病毒分类、传播途径、行为类型以及相应的解决方案等详细信息。

5.4.1 对象

5.4.1.1查杀目标

在瑞星杀毒软件主程序中，用户可以通过“查杀目标”选择查杀对象，针对查杀对象进行病毒的扫描和清除功能。综合大多数普通用户的通常使用情况，瑞星杀毒软件已预先作了合理的默认设置。因此，普通用户在通常情况下无需改动任何设置即可进行病毒查杀。

5.4.1.2快捷方式

用户可以从“快捷方式”中直接选择查杀目标，也可以通过【添加】、【删除】和【修改】按钮管理现有的快捷查杀目标。

5.4.2 设置

- 发现病毒时的处理方式：询问我、清除病毒、删除染毒文件和不处理。
- 显示信息：清除病毒前，自动备份到病毒隔离系统，当前隔离系统的剩余空间大小。
- 设置空间大小：设置隔离区空间大小。
- 杀毒结束时的处理方式：返回、退出、重启和关机
- 开始查杀：单击【开始查杀】按钮，将对选择的查杀目标进行查杀病毒，在页面底部的信息栏中将显示当前扫描的文件数、病毒数和扫描百分比。
- 停止查杀：单击【停止查杀】按钮，停止查杀操作。
- 查杀设置：功能同 5.9.1.1 手动查杀和 5.9.1.2 快捷方式查杀。
- 更多信息：单击【更多信息】，显示扫描病毒的进度信息，单击【返回上层】，返回【杀毒】标签页。如果扫描发现病毒，会在窗口的列表栏中详细列出病毒的名称、文件名、文件路径和处理结果。

5.5 监控

瑞星监控包括文件监控、邮件监控、网页监控，拥有这些功能，瑞星杀毒软件能在用户打开陌生文件、收发电子邮件和浏览网页时，查杀和截获病毒，全面保护计算机不受病毒侵害。

5.5.1 监控状态

瑞星监控的监控状态提供了对文件、邮件和网页监控状态的显示。同时在【监控状态】页面中，用户可以随时开启或关闭相应的监控。

图 515

5.5.2 文件监控

文件监控用于实时的监控系统中的文件操作，在操作系统对文件操作之前对文件查毒，从而阻止病毒运行，保护系统安全。用户可以设置文件白名单和目录白名单，避免对于确定安全的文件或者目录频繁访问，具体设置见 5.9.2.2 文件监控设置。

文件监控在工作中发现病毒时，会对用户进行提示：用户可以选择【清除病毒】、【删除染毒文件】或【不处理】。如果超过一定时间用户没有做出选择，那么文件监控将会对此病毒采取当前选择的处理方式。

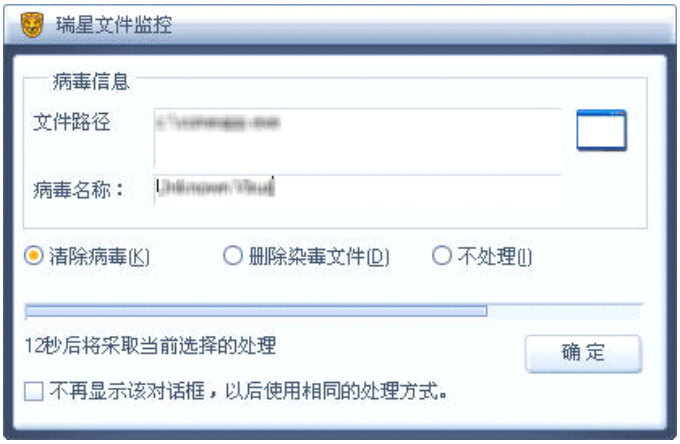

图 516

超时文件提示：当文件监控在查杀大容量压缩文件时，会占用较多的系统资源，造成系统效率降低。瑞星杀毒软件的文件监控，在遇到此类情况时能够提示用户进行操作。用户可以在提示的对话框中选择跳过对该文件的查杀，避免文件监控长时间占用系统资源，减少对系统的影响。

图 517

5.5.3 邮件监控

说明：在企业专用版和高级企业专用版中，购买时可以定制邮件监控功能；网吧版无此功能。

用户在接收或发送邮件时，邮件监控可以对接收和发送的邮件进行病毒扫描，防止病毒通过邮件传播，感染计算机。

邮件监控功能支持所有符合 SMTP 和 POP3 协议的邮件客户端，如：Foxmail、Outlook 等。

当用户选择发送和接收邮件的时候，邮件监控会自动进行扫描工作。此时，如果用户在【设置】/【监控设置】/【邮件监控】的高级设置选项页面中，取消勾选【隐藏邮件收发进度提示窗口】将显示发送或接收邮件的进度。

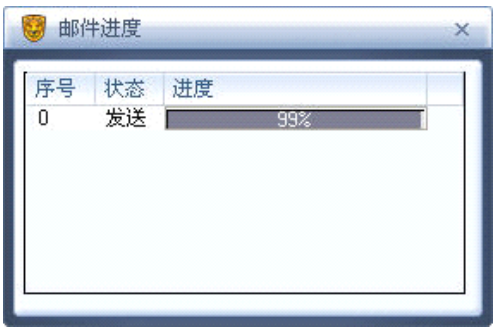

图 518

发送和接收的邮件中，邮件监控扫描到附件携带病毒时，会显示以下界面提示用户发现病毒，为用户提供处理病毒的操作方式，分别为【清除病毒】、【删除染毒文件】和【不处理】，或者在设定时间到达后按当前选择的设置进行处理。

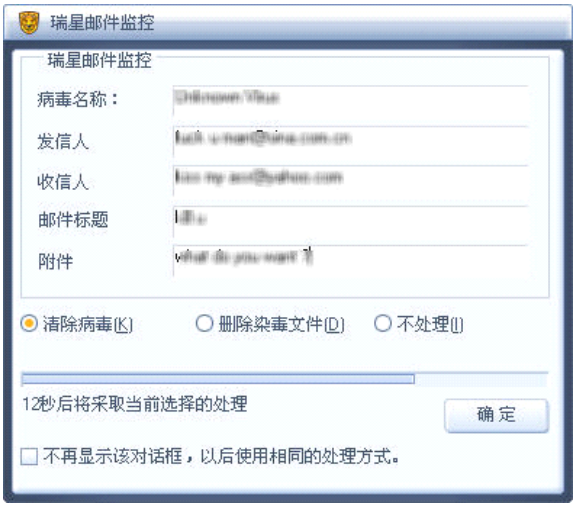

图 519

5.5.4 网页监控

网页监控是通过监控网页脚本来检测恶意网页内容的，在脚本执行之前会先检查网页脚本是否存在问题，若检查到可疑网页脚本，网页监控会提示用户进行处理。

当用户设置发现网页病毒的提示方式为【询问我】时，网页监控检测到有已知网页病毒会提示用户，用户点击【确定】按钮则直接跳过网页中的病毒。

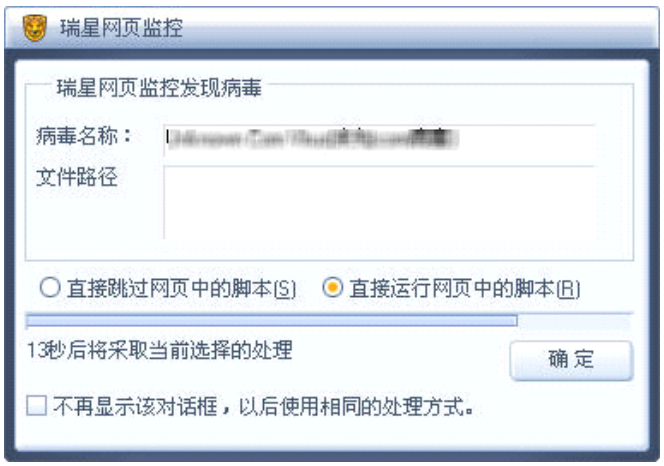

图 520

注意：当网页监控发现是未知病毒时，则提示用户的对话框中为用户提供两种方式【直接跳过网页中的脚本】和【直接运行网页中的脚本】处理该未知病毒。

5.6 主动防御

主动防御是一种阻止恶意程序执行的技术。瑞星的主动防御技术提供了更开放的高级用户自定义规则的功能，用户可以根据自己系统的特殊情况，制定独特的防御规则，使主动防御可以最大限度的保护系统 。

主动防御是瑞星杀毒软件的一项新功能，其在功能设计方面脱离了病毒库，以往杀毒软件只是发现应用程序类似病毒就去病毒库中进行验证，这样判断病毒都是已经发现的病毒，对于新病毒便失去了防御作用。主动防御具有独特的功能设计，它是瑞星公司根据多年判断病毒的经验制定了一系列的规则，通过规则过滤应用程序，当发现其存在恶意行为的时候，便告知用户，这样将处理此恶意行为的权力交给用户，由用户决定放过还是拒绝此类危险动作，从而可以达到主动预防病毒的作用。即使遇到一个病毒库里面没有记录的新病毒，瑞星杀毒软件可以提前帮助用户发现它。在病毒肆虐的网络中，主动防御功能在病毒与计算机之间又设置了一道屏障，将病毒置之门外。

主动防御由系统加固、应用程序访问控制、应用程序保护、程序启动控制、恶意行为检测和隐藏进程保护、自我保护等功能组成。

注意：Windows 9X、NT 和所有 64 位操作系统不支持主动防御功能。

选择瑞星杀毒软件主界面的防御界面，可以应用和设置主动防御的各项功能。

图 521

5.6.1 系统加固

系统加固针对恶意程序容易利用的操作系统脆弱点进行监控、加固，以抵御恶意程序对系统的侵害。

系统加固为用户预先设置了规则，并提供规则的应用对象，这些规则对象主要由容易被病毒利用的操作系统脆弱点构成，并且针对对象是否启用规则，为用户量身制定了高、中、低、自定义四种安全级别，由用户根据系统情况自由选择。

系统加固对系统动作、注册表、关键进程和系统文件进行监控，从而防止恶意程序对操作系统进行修改系统进程，操作注册表，破坏关键进程和系统文件等危险行为。

注意：系统加固功能中的规则范围是瑞星杀毒软件设置的，用户无法添加或者删除，但可以设置是否启用系统加固的各项规则。用户可以使用瑞星软件默认的使用级别，也可以对其进行设置，具体设置请参考 5.9.3.1 系统加固设置。

在瑞星杀毒软件主界面中选择【防御】页面中的系统加固，设置状态为开启，系统加固规则主要有四种类型，下面对触发系统动作监控规则的情况举例。

触发系统动作监控规则（系统动作包括挂全局钩子、加载驱动、修改内核内存数据三项）

注意：提示用户对话框有两种方式：简要信息和详细信息。瑞星杀毒软件默认的设置为显示详细信息提示框。

当有程序触发全局挂钩规则，如果弹出详细信息的对话框，对话框中显示该程序和规则的详细信息，并且可以通过【更多信息】显示更多相关信息。用户可以选择拒绝或者放过程序的动作。

图 522

5.6.2 应用程序访问控制

应用程序访问控制是对用户指定的应用程序进行系统资源监控，一方面可以限制其访问范围，另一方面可以对重要的服务程序进行加固。指定应用程序可以设置为用户认为可疑的应用程序，通过规则设置了解其访问计算机资源情况，调查其是否包含恶意代码。

注意：此功能是由用户先进行设置，选择指定的进程，再进行应用程序访问控制规则的设置，设置完毕后，当开启此功能时候，应用程序访问控制的功能生效。如何设置请参考 5.9.3.2 应用程序访问控制设置。

应用程序访问控制规则有以下几种类型，分别为：

- 限制加载驱动
- 限制全局挂钩
- 限制启动子程序
- 限制修改内核内存数据
- 文件规则
- 注册表规则

瑞星杀毒软件会根据用户设置提示相应的对话框，下面只举一例，说明有程序触发用户设置的规则的情况。

用户设置安装钩子规则后，当有程序触发规则的时候，提示详细信息对话框，用户可以选择拒绝或者放过程序的动作。

图 523

5.6.3 应用程序保护

应用程序保护可以保护指定的应用程序不被恶意程序攻击。用户可以添加游戏软件、即时通讯软件等，对它们进行保护。

注意：此功能是由用户先进行规则对象设置，选择自己需要保护的进程，如：游戏软件、即时通讯软件等，再进行应用程序保护规则设置，设置完毕后，当在【防御】页面开启此功能时候，应用程序保护的功能生效。如何设置请参考 5.9.3.3 应用程序保护设置。

当用户已经设置了应用程序保护规则，并且在设置规则页面中勾选了【启用应用程序保护提示】项，具体设置请参考 5.9.3.3 应用程序保护设置，运行被保护的程序的时候，托盘会有以下提示：

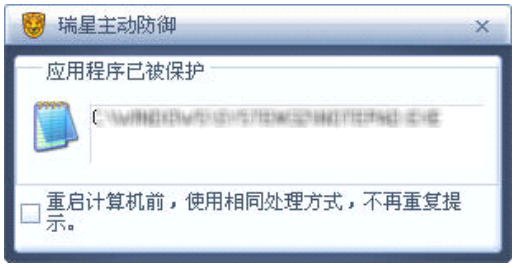

图 524

当有程序触发应用程序保护规则的时候，会显示相应的提示对话框提示用户，下面以触发防止被注入 DLL 规则为例。

当有程序触发防止被注入 DLL 规则后，提示用户详细信息对话框，用户可以选择拒绝或者放过程序的动作。

图 525

5.6.4 程序启动控制

程序启动控制功能允许用户监控指定可疑程序的启动过程，有助于阻止并截获未知恶意程序，并可以用于发现指定的应用程序被篡改。

注意：此功能是由用户先进行设置，选择启动者和目标程序，再进行程序启动控制规则的设置，设置完毕后，当开启此功能时候，程序启动控制功能生效。如何设置请参考 5.9.3.4 程序启动控制设置。

下面举例说明，当有程序触发程序启动控制规则时候，提示用户的情况。

当有程序触发程序启动控制规则的时候，提示详细信息对话框，用户可以选择拒绝或者放过程序的动作。

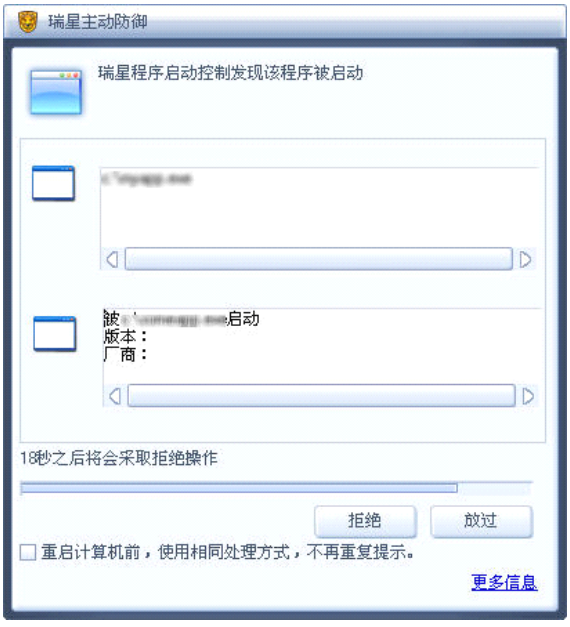

图 526

5.6.5 恶意行为检测

恶意行为检测能够对系统中的程序进行监控，用户可以根据行为检测报告发现可能包含恶意代码的应用程序。

注意：此功能是瑞星杀毒软件提供内置规则，用户可以进行相关设置，当开启此功能时，恶意行为检测功能生效。如何设置请参考 5.9.3.5 恶意行为检测设置。

若用户设置发现恶意行为后的处理方法为【提示我处理】时，则会提示用户选择【隔离并删除文件】或【放过文件】两种方式处理此程序。

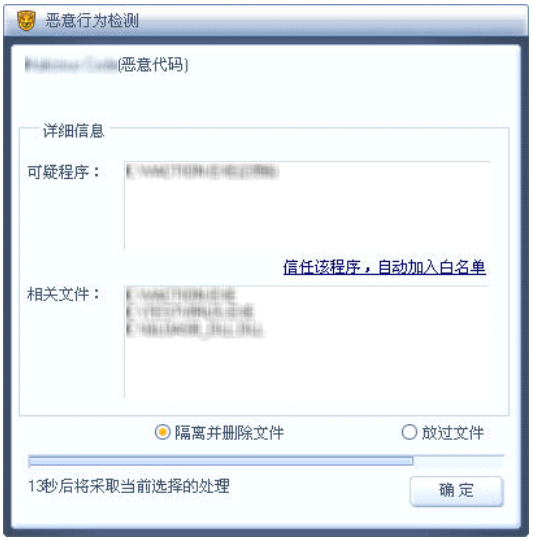

图 527

5.6.6 隐藏进程检测

隐藏进程检测可以检测“任务管理器”中无法查看的进程，被隐藏的进程很有可能是包含恶意代码的应用程序。

当用户已经启用隐藏进程检测功能，并且在 5.9.3.6 隐藏进程检测设置规则页面中勾选了【发现隐藏进程时提示用户】项，当发现有隐藏进程的时候，托盘会有以下提示：

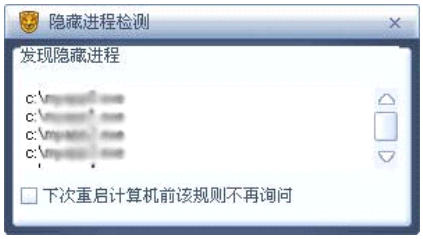

图 528

5.6.7 自我保护

瑞星杀毒软件提供自我保护功能，防止恶意程序破坏瑞星杀毒软件。如果有破坏瑞星杀毒软件的情况出现，计算机右下方会有相应提示：

图 529

可以在主动防御设置页面设置是否启动自我保护功能。

5.7 工具

瑞星杀毒软件为用户提供了以下工具，分别为：病毒隔离系统、硬盘数据备份、漏洞扫描、其它嵌入式杀毒和瑞星助手。点击【检查更新】，下载最新的工具。

图 530

5.7.1 瑞星助手

说明：在企业专用版和高级企业专用版中，购买时可以定制瑞星助手功能；网吧版无此功能。

瑞星助手可以帮助用户使用瑞星杀毒软件。鼠标双击瑞星助手图标，启动瑞星杀毒软件主程序界面。

单击右键有五种操作：鼠标跟随、音效开、动画效果、连续播放动画和退出。

图 531

5.7.2 其它嵌入式杀毒

瑞星杀毒软件嵌入式杀毒工具是在用户使用即时通讯软件（如 MSN Messenger）、压缩工具（如 WinZip）和下载工具（如 FlashGet）时，会自动调用瑞星杀毒软件对接收的文件进行病毒扫描，防止病毒通过外来文件感染本地计算机。

瑞星杀毒软件嵌入式杀毒工具目前支持的软件有：

- MSN Messenger
- AOL Messenger
- FlashGet
- NetAnts
- NetVampire
- WinZip
- WellGet
- WinRAR

图 532

5.7.3 硬盘数据备份

说明：在企业专用版和高级企业专用版中，购买时可以定制该功能；网吧版无此功能。

瑞星硬盘数据备份，只备份了整个硬盘的重要信息（而非所有信息）。数据备份功能与操作系统提供的系统还原等传统备份、恢复功能有很大差别。

瑞星杀毒软件在安装后默认不启用定时备份硬盘数据，用户可以进入【详细设置】/【硬盘备份】中更改此项设置。

当用户在遇到数据文件丢失的时候，可尝试进行数据恢复，为避免数据恢复过程中出现意外，进行恢复之前请务必先对硬盘现有的数据进行备份后再使用数据恢复功能，恢复后的硬盘不保证操作系统能够正常运行。

数据恢复操作是一项有很大风险且无法保证成功的操作，请谨慎使用，当用户不确定是否要采用此操

作时，请致电瑞星客户服务中心进行咨询。

5.7.3.1手动备份

方法一：在瑞星杀毒软件主程序界面中，选择【工具】/【硬盘数据备份】/【运行】，选择【开始备份】按钮；

方法二：在 Windows 画面中，选择【开始】/【程序】/【瑞星杀毒软件】/【瑞星工具】/【瑞星硬盘数据备份】，选择【开始备份】按钮。

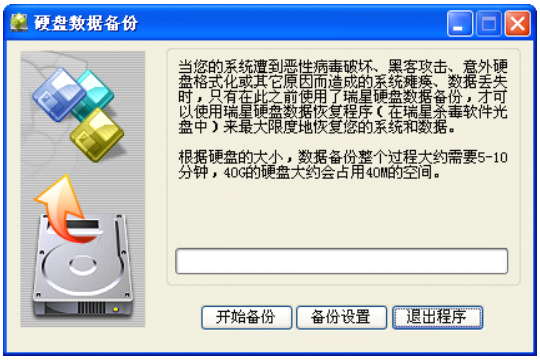

图 533

5.7.4 漏洞扫描

说明：在企业专用版和高级企业专用版中，购买时可以定制该功能；网吧版无此功能。

瑞星漏洞扫描是对 Windows 系统存在的“系统漏洞”和“安全设置缺陷”进行检查，并提供相应的补丁下载更新和安全设置缺陷修补的工具。

5.7.4.1启动瑞星漏洞扫描工具

方法一：在瑞星杀毒软件主程序界面中，选择【工具】标签页/【漏洞扫描】/【运行】；

方法二：选择【开始】/【程序】/【瑞星杀毒软件】/【瑞星工具】/【瑞星漏洞扫描】，启动系统漏洞扫描程序。

图 534

5.7.4.2漏洞扫描的使用

勾选【安全漏洞】和【安全设置】选项，单击【开始扫描】进行系统漏洞扫描。

5.7.4.3阅读扫描报告

扫描结束后自动显示扫描报告。内容包括扫描时间、发现的安全漏洞、未修复的安全设置。单击【查看详细】，可以分别查看扫描到的安全漏洞和未修复的安全设置的详细信息。

图 535

5.7.4.4安全漏洞

选择【扫描报告】/【发现的安全漏洞】/【查看详细】选项可以查看详细的安全漏洞信息，也可直接进入【安全漏洞】页进行查看。

在该页中漏洞扫描给出了每个漏洞信息的详细解释和漏洞的安全级别，★的多少将用于表示此漏洞对用户的系统造成的危害程度，★越多表示危害程度越高。

在需要修复的漏洞前面勾选，然后单击【修复选择的漏洞】，漏洞扫描可以自动连接网络下载相关补

丁文件，页面最下面显示了补丁保存目录，用户也可以单击【更换目录】更改补丁保存目录。

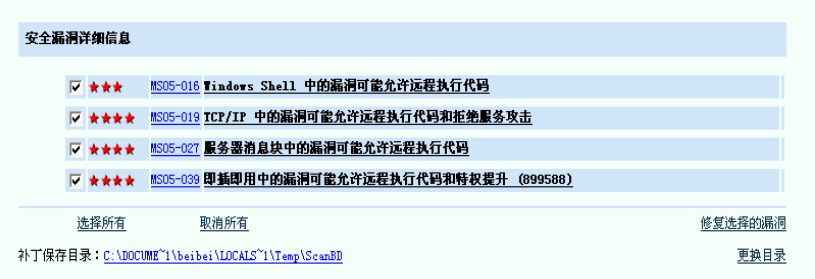

图 536

系统漏洞扫描程序会直接运行下载到计算机的补丁文件，进行系统漏洞的修复。

注意：微软公司为了确保其补丁程序的有效执行，因此在更新的过程中可能要求重新启动计算机。

5.7.4.5安全设置

选择【扫描报告】/【未修复的安全设置】/【查看详细】选项可以查看详细的未修复的安全设置信息，也可直接进入【安全设置】页进行查看。

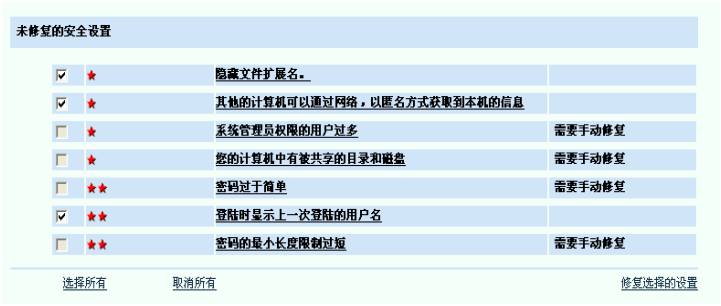

图 537

在需要修复的设置前面勾选，然后单击右下角【修复选择的设置】，即可对所选的安全设置进行修复。

对由于用户的设置而造成的系统的不安全隐患，漏洞扫描已经给出了相应的解释，对于某些设置，漏洞扫描是可以进行自动修补的，而对无法自动修复的设置，则需要用户的参与。比如：不安全的共享、过多的管理员帐户、系统管理员帐户的密码为空等。这些情况需要用户手动更改解决。

5.7.4.6扫描结果的导入和导出

当扫描完成后，进入【扫描报告】页。选择页面右上角的【导出报告】按钮后，显示报告导出路径。

程序会以操作系统时间的形式自动命名导出文件，文件名也可以由用户自定义，文件格式是*.slo 文件 。

对于扫描信息的导入，直接在【瑞星系统安全漏洞扫描】页面上单击【导入报告】，显示要导入文件的选择路径。

选定要导入的扫描结果后，选择【打开】，漏洞扫描会将扫描结果导入，并显示当前的情况，用户可以查看导入后的报告。

5.7.4.7漏洞扫描使用时出现的问题的解决

1. 漏洞扫描是对系统不安全性向用户提出警告并引导用户下载补丁程序的工具，但由于补丁程序的修补过程完全是由微软公司提供的补丁程序来完成的，所以如果出现补丁程序在修补完成后造成

系统某些设置的更改，请咨询微软公司。

2. 在扫描结果中，会出现某些补丁程序无法下载的情况，这是由于此条漏洞的修补只能利用微软公司提供的 Windows Update 来完成，微软公司并没有单独对此漏洞提供公用的补丁程序，此时瑞星漏洞扫描会将此漏洞信息直接连接到微软网站的 Windows Update 来进行在线更新。

5.7.5 病毒隔离系统

病毒隔离系统将安全隔离并保存染毒文件的备份，用户可以从中对染毒文件进行恢复。此功能为了防止异常错误给用户造成文件的损失，为用户提供一个统一的病毒文件恢复机制。

5.7.5.1启动病毒隔离系统

方法一：在瑞星杀毒软件主程序界面中，选择【工具】/【病毒隔离系统】/【运行】。

方法二：在 Windows 画面中，选择【开始】/【程序】/【瑞星杀毒软件】/【病毒隔离系统】)。

如果用户在瑞星杀毒软件主程序界面中，选择【设置】/【详细设置】/【其它设置】，在显示的对话框中勾选【将染毒文件备份到病毒隔离系统】，则病毒隔离系统将保存染毒文件的备份，并且在必要时，用户可以恢复备份的染毒文件副本。

5.7.5.2设置隔离区存储空间

为避免由于备份文件过多而占用大量磁盘空间，用户可以设置病毒隔离系统占用存储空间的大小。当隔离区空间已满时，用户可以选择【空间自动增长】或使用【替换最老的文件】处理。方法是：启动【病毒隔离系统】，选择【工具】/【设置空间】，在【设置】对话框中选择后，单击【确认】保存设置。

图 538

操作选项：操作（恢复、恢复为、删除、清空、关闭病毒隔离系统）

选择选项：全部选定、反向选择、相同时间保存的文件、相同路径保存的文件、被相同病毒感染的文件

查看选项：工具栏、状态栏、刷新列表、排列项目（按日期、按原位置、按名称、按路径、按大小）

工具选项：设置空间

帮助选项：帮助、关于隔离系统

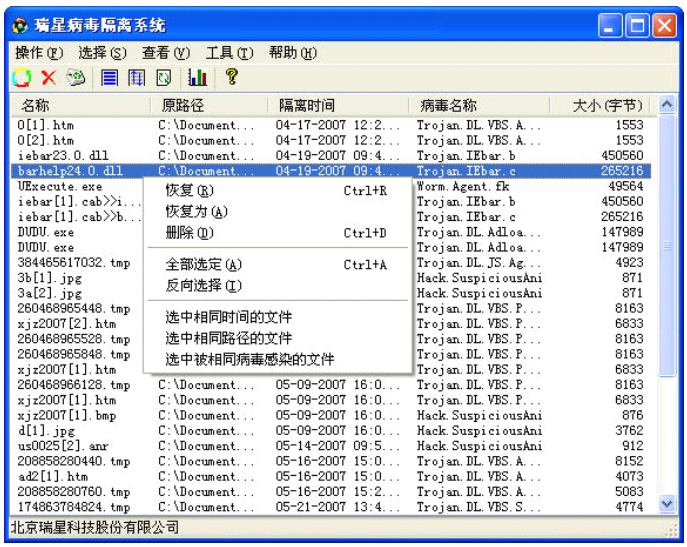

图 539

针对被隔离文件的操作：（右键操作）

- 恢复
- 恢复为
- 删除
- 全部选定
- 反向选择
- 选中相同时间的文件
- 选中相同路径的文件
- 选中被相同病毒感染的文件

5.7.6 账号保险柜

账号保险柜能够将瑞星杀毒软件支持的软件自动加入到应用程序保护功能中，减少了在主动防御的应用程序保护中手动添加规则的步骤。

启动账号保险柜方式：

- 在桌面双击“账号保险柜”图标
- 在【工具】页中运行【账号保险柜】
- 在安检的详细报告中，双击【账号保险柜】

则进入瑞星账号保险柜：

图 540

当用户的计算机中安装了相应的软件的时候，则用户可以勾选选项，按【应用】按钮，将其添加到应用程序保护规则中，若账号保险柜支持该软件，但由于未找到对应的路径而导致列表中该项图标为灰色的情况下，用户还可以点击【修改路径】按钮选择需要保护的应用程序。

注意：只有客户端用户可以在账号保险柜中设置客户端规则，若用户设置的规则与在管理控制台中已存在的应用程序保护规则相同，在客户端用户无法设置；若系统管理员在控制台中设置的应用程序保护规则与已存在的用户在账号保险柜中设置的规则相同，应用程序保护规则覆盖客户端用户在账号保险柜设置的规则并且生效。

5.7.7 专杀工具

专杀工具是快速应对流行恶性病毒单独发布的程序包，通过【工具】页面的【检查更新】，可以及时获取最新的版本，并自动下载到本地。

5.8 安检

为用户提供全面的检测日志，方便用户了解当前计算机的安全等级及系统状态。并根据用户计算机的情况，为用户提出专家建议。用户可以更加方便地选择提高安全等级的方法。

图 541

电脑安全检测结果：

- 当前电脑安全等级：显示当前计算机的安全等级。
- 详细报告：单击【详细报告】显示详细报告内容。

专家建议：

- 立刻全盘查杀：用户单击此项可以立刻扫描全盘。
- 扫描系统漏洞并升级补丁：用户单击此项可以进行扫描系统漏洞并升级补丁。
- 开启实时监控：用户单击此项打开瑞星实时监控设置页面。
- 开启主动防御：用户单击此项打开主动防御设置页面。
- 将检测到的可疑文件上报：用户单击此项则可以在发现可疑文件后将其进行上报。

单击【详细报告】会进入下一页面：

图 542

评测总结：

- 当前计算机的安全等级：显示当前计算机的安全等级。
- 详细报告：内容包括检查项目、状态信息和条件三项。
- 检查项目：显示检查项目的名称。
  - 病毒库升级：显示病毒库升级情况。
  - 全盘杀毒：双击此项则进行全盘查杀病毒。
  - 漏洞扫描：双击此项则进行漏洞扫描。
  - 实时监控：双击此项则打开实时监控设置页面。
  - 主动防御：双击此项则打开主动防御设置页面。
  - 可疑文件检测：检测可疑文件是否上报到瑞星。
  - 账号保险柜：双击此项则打开账号保险柜页面。
- 状态信息：显示检测的状态信息。
- 条件：显示是否符合检测标准。

5.9 设置

5.9.1 详细设置

5.9.1.1手动查杀

手动查杀为用户提供了手动查杀病毒的设置界面，用户可以根据自己的实际需求，对手动查杀时的病毒处理方式和查杀文件类型进行不同的设置，也可以使用滑块调整查杀级别。在【自定义级别】中，用户同样可以对安全级别进行设置，单击【默认级别】将恢复瑞星杀毒软件的出厂设置，单击【应用】或【确定】按钮保存用户的全部设置，以后程序在扫描时即根据此级别的相应参数进行病毒扫描。

如果用户需要对某一文件杀毒，也可以拖拽该文件到瑞星杀毒软件的主界面上，此时瑞星杀毒软件将转到【杀毒】标签页下的查杀目标页面，并显示杀毒结果。

图 543

处理方式：

- 发现病毒时：【询问我】、【清除病毒】、【删除染毒文件】和【不处理】；
- 杀毒失败时：【询问我】、【删除染毒文件】和【不处理】；
- 隔离失败时：【询问我】、【清除病毒】、【删除染毒文件】和【不处理】；
- 杀毒结束后：【返回】、【退出】、【重启】和【关机】。

查杀文件类型：

- 所有文件；
- 仅程序文件（Exe、Com、Dll、Eml 等可执行文件）；
- 自定义扩展名（多个扩展名需用英文状态的分号隔开）。

勾选【隐藏杀毒结果】后，杀毒软件主程序查杀病毒时，不显示杀毒结果。

图 544

5.9.1.2快捷方式查杀

用户可以根据自己的实际情况，对快捷扫描方式进行不同参数的设置。也可以通过勾选参数项自定义高、中、低扫描级别。当用户对某一文件怀疑存有病毒时，可以选中此文件后，单击鼠标右键对其查杀病毒；也可以拖动文件到瑞星杀毒软件的主界面中，进行查杀病毒，此时，瑞星杀毒软件转到【杀毒】标签页下的快捷方式页面，并显示杀毒结果。查杀设置选项同 5.9.1.1 手动查杀。

图 545

5.9.1.3定制任务

提供定时查杀、屏保查杀和开机查杀的统一使用开关界面。

5.9.1.3.1 定时查杀

在瑞星杀毒软件主程序界面中，选择【设置】/【详细设置】，在显示的详细设置对话框中，选择【定制任务】/【定时查杀】。

图 546

在对病毒的【处理方式】中有以下几种：

- 发现病毒时：用户可以根据需要选择【询问我】、【清除病毒】、【删除染毒文件】、【不处理】；
- 杀毒失败时：用户可以根据需要选择【询问我】、【删除染毒文件】和【不处理】；
- 隔离失败时：用户可以根据需要选择【询问我】、【清除病毒】、【删除染毒文件】、【不处理】；
- 杀毒结束后：用户可以根据需要选择【返回】、【退出】、【重启】、【关机】。

在【查杀文件类型】中可选择要扫描的文件类型：

- 所有文件；
- 仅程序文件（Exe、Com、Dll、Eml 等可执行文件）；
- 自定义扩展名（多个扩展名需用英文状态的分号隔开）。

在【查杀频率】中：

- 查杀频率：【每周期一次】、【每周一次】、【每天一次】和【每小时一次】。
- 查杀时刻：【小时】、【分钟】、【周期】和【星期】。

在【检测对象】中，可指定需要定时查杀的对象。

当系统时钟到达所设定的时间，瑞星杀毒软件会自动运行，开始查杀预先指定的对象。瑞星杀毒界面会自动显示，用户可以随时查阅查毒的情况。

注意：当系统管理员在管理控制台锁定文件类型、病毒类型和优化选项任意项的时候，在客户端通过设置高、中、低级别的滑块设置级别时，仅修改未被锁定的选项，已经被锁定的选项则不能被修改。

5.9.1.3.2 屏保查杀

在 Windows 进入屏幕保护程序时，瑞星杀毒软件随即开始查杀病毒，充分利用计算机的空闲时间。

在瑞星杀毒软件主程序界面中，选择【设置】/【详细设置】，在显示的详细设置界面中选择【定制任务】/【屏保查杀】选项卡，进行查杀设置。

图 547

具体设置选项详见“定时查杀”的相应选项。

注意：当系统管理员在管理控制台锁定文件类型、病毒类型和优化选项任意项的时候，在客户端通过设置高、中、低级别的滑块设置级别时，仅修改未被锁定的选项，已经被锁定的选项则不能被修改。

5.9.1.3.3 开机查杀

开机查杀功能，能够在用户刚开机且 Windows 未启动时，优先加载瑞星杀毒程序，扫描所有硬盘、系统盘、Windows 系统目录和所有服务和驱动，可以有效地清除 RootKit 和具有自我防护能力的恶意程序、流氓软件。按任意键开始杀毒，按<ESC>键退出。

图 548

在【详细设置】/【开机查杀】页面，可以选择查杀对象：所有硬盘、系统盘、Windows 系统目录和所有的服务和驱动。

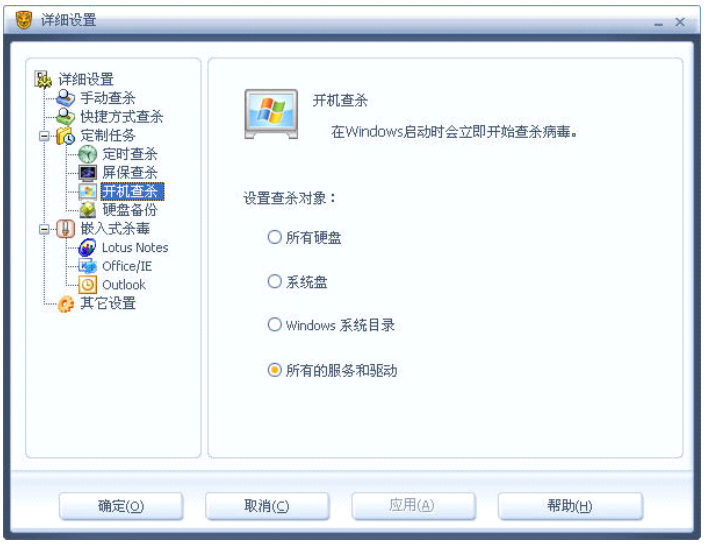

图 549

注意：开机查杀功能只在 Windows 2000 以上版本的操作系统中适用。

5.9.1.3.4 硬盘备份

说明：在企业专用版和高级企业专用版中，购买时可以定制硬盘数据备份功能，未定制的情况下无此设置页面；网吧版无硬盘备份功能，故无此设置页面。

硬盘备份为用户提供可定制时间、周期的自动化的硬盘数据备份功能。

- 备份频率：【不备份】、【每周期一次】、【每周一次】、【每天一次】和【每小时一次】。
- 备份时刻：【小时】、【分钟】、【周期】和【星期】。

图 550

5.9.1.4嵌入式杀毒

提供 Office/IE、Outlook 和 Lotus Notes 嵌入式杀毒统一使用开关界面，并且可以通过“设置其它嵌入式杀毒”连接到“其它嵌入式杀毒”工具的设置窗口。具体操作设置选项详见 5.7.2 其它嵌入式杀毒的相关设置选项。

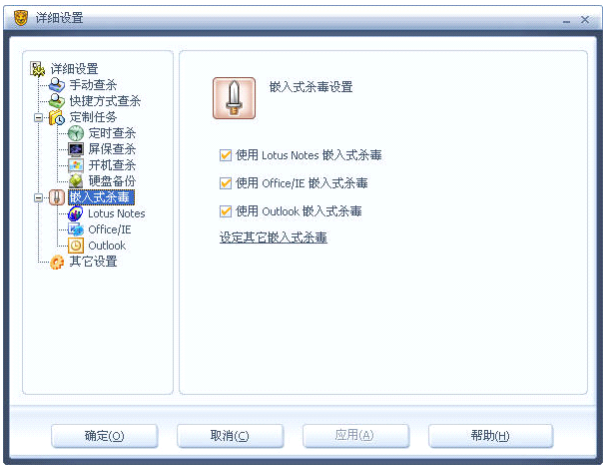

图 551

说明：在企业专用版和高级企业专用版中，Lotus Notes、Office/IE 嵌入式杀毒功能在购买时可以被定制，未定制这两项功能的情况下，该页面无此两项设置；网吧版没有 Lotus Notes、Office/IE 嵌入式杀毒功能，故没有这两项设置。

5.9.1.5其它设置

提供使用声音报警、保存历史记录、向瑞星病毒疫情监测网上报查杀记录、将染毒文件备份到病毒隔离系统、查杀时排除指定的目录、显示信息中心、多扩展名提示、U 盘监控、在登录系统前显示监控状态和显示瑞星助手的统一开关界面。

图 552

说明：在企业专用版和高级企业专用版中，瑞星助手功能购买时可以定制，未定制的情况下没有显示瑞星助手设置项；网吧版无瑞星助手功能，故无此项设置。

日志记录默认记录 7 天以内的日志，当用户输入错误时会显示提示框提示用户输入 1-60 之间的整数。若用户勾选了【查杀时排除指定的目录】选项，可以单击【设置】按钮设置相应的目录。

图 553

5.9.2 监控设置

5.9.2.1计算机监控设置

监控设置页面显示文件监控、邮件监控和网页监控的防御级别信息，并且用户可以设置下次计算机重新启动后杀毒软件是否启用这三项功能。

图 554

5.9.2.2文件监控设置

文件监控设置页面为用户提供文件监控引擎查杀级别的设置、病毒的处理方式的设置，文件监控方式的设置，以及提示框的时间设置和是否记录操作日志等。

在左侧的瑞星监控中心，选中文件监控，右侧则显示文件监控的各项设置，用户可以根据需要进行各种设置。

图 555

按钮或选项：

文件监控引擎查杀级别设置：

- 用户可以选择瑞星软件提供的高、中、低三种级别。
- 设置排除目标：用户单击此按钮显示文件白名单设置页面，用户可以设置白名单，避免文件被频繁访问时文件监控的干扰，提高效率。
- 自定义级别：用户单击此按钮，显示引擎的设置参数页面，用户可以通过勾选选项自定义参

数或者重置级别。

- 默认级别：按此按钮设置为默认级别，即中级。

注意：当系统管理员在管理控制台锁定文件类型、病毒类型和优化选项任意项的时候，在客户端通过设置高、中、低级别的滑块设置级别时，仅修改未被锁定的选项，已经被锁定的选项则不能被修改。

常规设置：

- 发现病毒时：用户可以选择【询问我】、【清除病毒】、【删除染毒文件】、【不处理】四种方式处理病毒。
- 杀毒失败时：用户可以选择【询问我】、【删除染毒文件】、【不处理】三种方式处理病毒。
- 备份失败时：用户可以选择【询问我】、【清除病毒】、【删除染毒文件】、【不处理】四种方式处理病毒。
- 提示对话框关闭时间：用户可以设置提示对话框的关闭时间。
- 记录日志：用户可以勾选此项设置是否记录日志。
- 提示杀毒结果：用户可以勾选此项来设置是否提示杀毒已经完成。

高级设置：

单击右侧中的【高级设置】，用户可以通过勾选选项来设置压缩文件扫描超时是否提示用户，以及是否启用智能监控功能和强杀文件功能。

图 556

- 显示监控文件超时提示：用户勾选此项设置压缩文件扫描超时是否询问用户。
- 启用智能监控：用户可以勾选此项开启智能监控功能。

  智能监控介绍：是指在文件被修改、创建和执行三种情况下对其进行查毒。智能监控是为了提高文件监控效率。

  当用户勾选【启用智能监控】项后，一方面开启了智能监控功能，另外则是文件在被执行情况下对其监控，查杀病毒。

  - 文件修改时监控：默认出厂设置是不勾选此项，用户可以根据需要选择是否勾选。
  - 文件创建时监控：默认出厂设置是勾选此项。

注意：智能监控下对于本地文件是可以在修改、创建和执行三种情况下进行查毒，而对于网络文件只是在执行时候进行查毒。

- 使用强杀文件：当前正在被系统调用或其它程序使用的文件是不能被删除的。若这些文件是病毒，使用瑞星杀毒软件的强杀文件的功能可以强制删除这类文件。

文件监控白名单设置：

用户可以设置文件白名单和目录白名单，当访问确定安全的文件或者目录时，不监控相关操作。

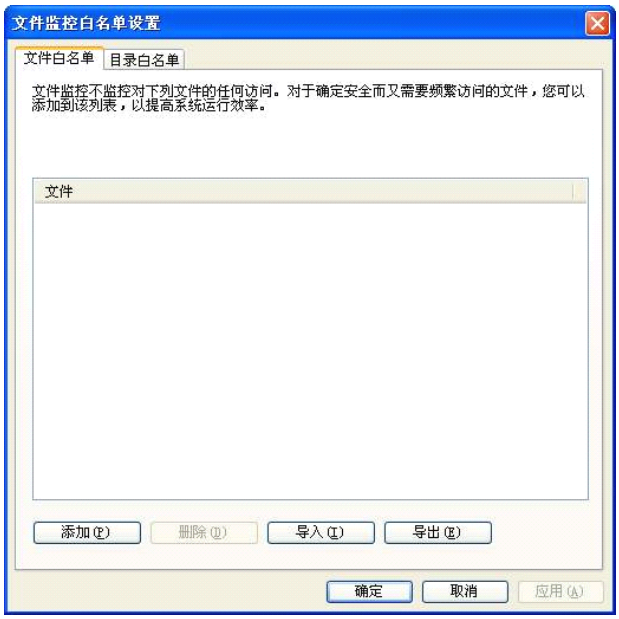

图 557

用户可以添加和删除文件或目录名单，也可以导入和导出文件或目录名单。

5.9.2.3邮件监控设置

说明：在企业专用版和高级企业专用版中，购买时可以定制邮件监控功能，未定制该功能的情况下无此设置页面；网吧版无邮件监控功能，故无此设置页面。

邮件监控设置页面为用户提供多端口设置、病毒处理方式的设置，以及提示框的时间设置和是否将操作记录日志等。

在瑞星监控中心的左侧，选中邮件监控，右侧则显示邮件监控的各项设置，用户可以根据需要进行设置。

图 558

按钮或选项：

- 邮件监控引擎查杀级别设置：
  - 用户可以选择瑞星软件提供的高、中、低三种级别。
  - 设置端口：用户单击此按钮显示设置端口页面，可以设置接收以及发送邮件的端口。
  - 自定义级别：用户单击此按钮，显示引擎的设置参数页面。用户可以通过勾选选项自定义参数或者重置级别。
  - 默认级别：按此按钮设置为默认级别，即中级。

注意：当系统管理员在管理控制台锁定文件类型、病毒类型和优化选项任意项的时候，在客户端通过设置高、中、低级别的滑块设置级别时，仅修改未被锁定的选项，已经被锁定的选项则不能被修改。

常规设置：

- 发现病毒时：用户可以选择【询问我】、【清除病毒】、【删除染毒文件】、【不处理】四种方式处理病毒。
- 杀毒失败时：用户可以选择【询问我】、【删除染毒文件】、【不处理】三种方式处理病毒。
- 备份失败时：用户可以选择【询问我】、【清除病毒】、【删除染毒文件】、【不处理】四种方式处理病毒。
- 提示对话框关闭时间：用户可以设置提示对话框的关闭时间。
- 记录日志：用户可以勾选此项设置是否记录日志。
- 提示杀毒结果：用户可以勾选此项来设置是否提示杀毒已经完成。

单击右侧中的【高级设置】选项页，则会显示邮件监控设置界面由用户通过勾选选项设置是否显示邮件收发进度提示窗口。

图 559

端口设置：

用户在端口设置页面点击【添加】按钮，可以增加端口号（0-65535）和协议，其中协议为 POP3 和 SMTP 两种：

图 560

注意：在此可以设置多个端口，进行多端口监控。

5.9.2.4网页监控设置

网页监控设置页面为用户提供发现网页病毒时的处理方式，设置提示框关闭时间和是否记录日志等。

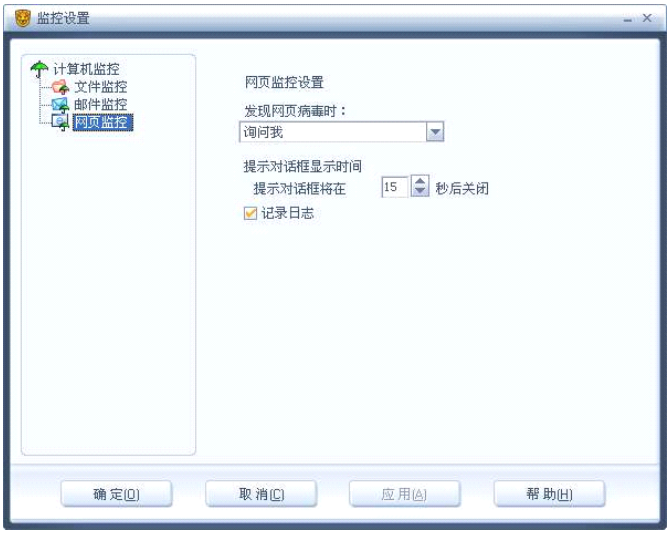

图 561

5.9.3 主动防御设置

主动防御设置界面综合显示主动防御所包括的功能的总体概况，为用户提供了系统加固、应用程序访问控制、应用程序保护、程序启动控制、恶意行为检测和隐藏进程检测的当前状态或者规则信息，以及开启自我保护功能的选项，并且提供设置下次计算机重新启动后杀毒软件是否启用这些功能。

图 562

选择【设置】/【防御设置】进入主动防御设置页面，用户可以勾选【开机启用】来设置下次计算机重新启动后开启相应的功能。同时可以设置瑞星自我保护功能的开启或关闭。如果用户确定一些程序为安全程序则可以在主动防御设置页面中设置【主动防御白名单】，放过确定安全的程序或者程序模块。

注意：当系统管理员在管理控制台的【主动防御规则设置】/【主动防御设置】页面锁定了开机启用主动防御任意功能项的时候，则在客户端相应的项前面出现一个“灰色的锁”表示用户对该规则只能查看，不可以修改设置。

按钮:

【确定】：保存用户设置并且退出主动防御设置。
【取消】：不保存用户设置并且退出主动防御设置。
【应用】：保存用户设置并且立即生效。
【帮助】：通过【帮助】按钮或者 F1 键浏览主动防御帮助详细信息。

可以在右侧查看相应功能的状态信息，具体内容如下：

- 系统加固：显示当前系统加固的安全级别。
- 应用程序保护：显示当前用户启用的规则数。
- 应用程序访问控制：显示当前用户启用的规则数。
- 程序启动控制：显示当前用户启用规则数。
- 恶意行为检测：显示当前恶意行为检测级别。
- 隐藏进程检测：显示当前隐藏进程检测功能是否运行。
- 自我保护：显示自我保护的状态。

设置主动防御白名单：

为了防止确定安全的应用程序被主动防御功能频繁报告，可以将此程序加入到白名单。在主动防御设置界面点击【主动防御白名单】按钮进入此页面。

图 563

用户可以通过【添加】、【删除】、【导入】、【导出】按钮设置白名单。点击【添加】进入规则应用对象页面添加白名单项；需要删除时，选中需要删除的项，按【删除】按钮将其删除；为了避免多次重复设置主动防御白名单，可以通过【导出】按钮导出为文件，作为备份；另外，单击【导入】按钮导入存在的白名单文件。

用户在上图中点击【添加】按钮进入此页面，用户可以在树状程序列表中选择规则应用对象，将该对象增加到主动防御白名单中。

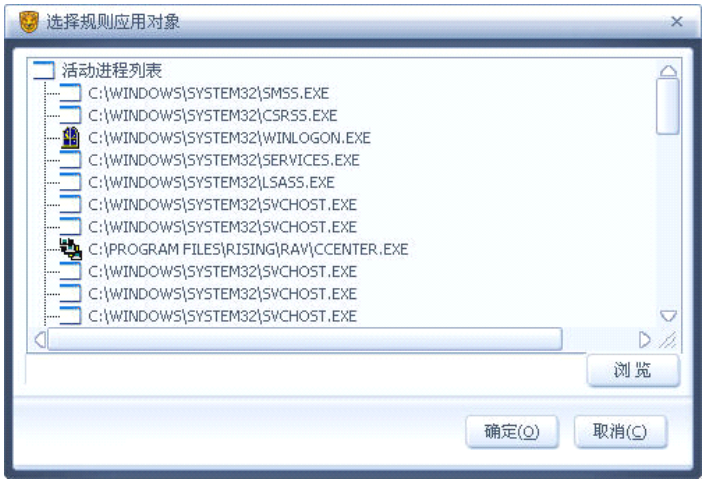

图 564

注意：瑞星杀毒软件白名单提供的规则对象，既包括应用程序又包括应用程序模块。

5.9.3.1 系统加固设置

系统加固设置页面为用户提供设置系统加固的级别，其中可以是瑞星软件提供的高、中、低三种级别，还可以由用户自己定义系统加固级别，并且设置当有程序触发规则的时候，提示用户的信息界面是简要信息界面还是详细信息界面以及是否记录日志。

图 565

用户可以选择瑞星杀毒软件提供的高、中、低级别来进行设置，其中中级为默认的推荐级别。还可以点击【自定义级别】按钮自定义系统加固的安全级别；另外，还可以勾选【记录日志】将发现的程序的操作记录到历史记录中，便于日后查看和分析。

触发规则时，显示方式有【详细信息】和【简要信息】两种。用户下拉此框来设置应用程序触发规则时候，提示用户的界面是简要信息界面还是详细信息界面。

注意：

1. 对于大多数普通用户，可以直接使用瑞星杀毒软件提供的默认设置，默认级别为中级。
2. 对于了解计算机和病毒知识的用户，可以自定义系统加固设置。
3. 当系统管理员在管理控制台锁定系统动作监控、注册表监控、关键进程保护和系统文件保护任意一项的情况下，客户端通过系统加固的【自定义级别】按钮可以查看锁定项设置的情况，被锁定的项前面带“灰色的锁”图标，故无法对右侧对应的规则其进行设置，也将不会出现设置级别的滑块。未被锁定的项前面没有“灰色的锁”的图标，用户可以通过【自定义级别】按钮进行设置其右侧对应的规则。

系统加固主要包括四个方面：系统动作监控、注册表监控、关键进程保护和系统文件保护。下面分别对这四个方面的设置进行介绍。

5.9.3.1.1 系统动作监控

在图 565 中，单击【自定义级别】按钮会显示下面的页面，左侧是系统加固包括的四项监控，选中系统动作监控，右侧则显示系统动作监控包括的挂接全局钩子、加载驱动、修改内核内存数据，用户可以勾选选项决定规则是否生效。

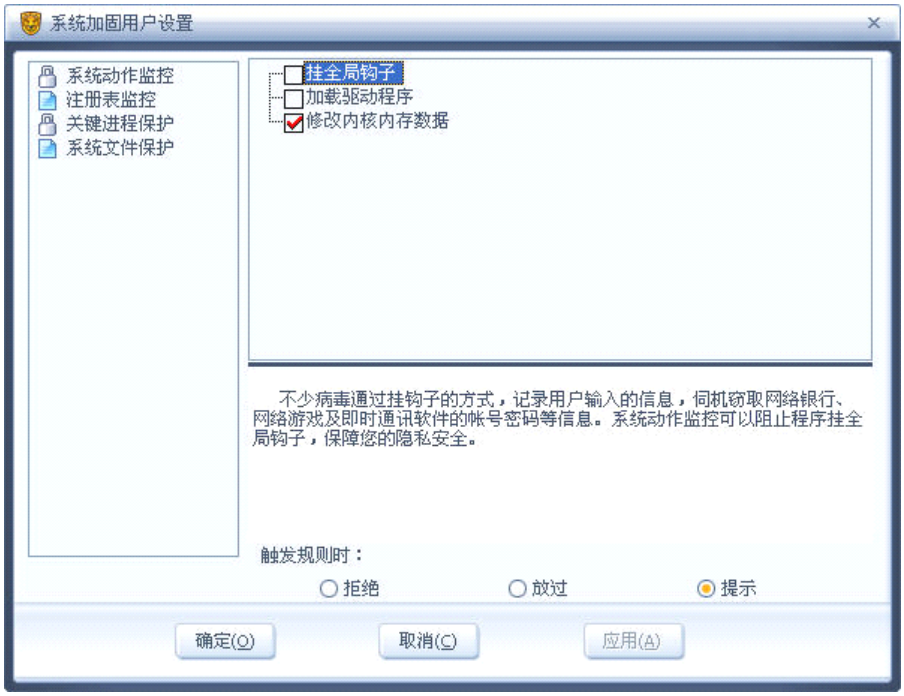

图 566

- 挂全局钩子：用户可以勾选挂接全局钩子使此功能生效。
- 加载驱动程序：用户可以勾选加载驱动程序使此功能生效。
- 修改内核内存数据：用户可以勾选修改内核内存数据使此功能生效。

用户可以选择拒绝、放过和提示三种操作方式设置未知程序触发此规则所采取的操作方式。

5.9.3.1.2 注册表监控

在左侧的系统加固树状列表中选择注册表监控，右侧则显示系统重要注册表键，用户可以勾选注册表键值来设置是否操作此键时候，提示用户有程序触发注册表规则。

- 系统关键文件的注册表项：用户可以勾选注册表项启用相应的规则。
- 触发规则：用户可以选择拒绝、放过和提示三种操作方式中的一种设置未知程序触发此规则时用户可以采取的操作方式。

5.9.3.1.3 关键进程保护

在左侧的系统加固树状列表中选择关键进程保护，右侧则显示系统重要进程，用户可以勾选进程来设置是否保护选定的进程。

- 关键进程列表：用户可以勾选来设置启用相应关键进程保护规则。
- 触发规则：用户可以选择拒绝、放过和提示三种操作方式中的一种设置未知程序触发此规则所采取的操作方式。

5.9.3.1.4 系统文件保护

在左侧的系统加固树状列表中选择系统文件保护，右侧则显示系统重要文件，瑞星杀毒软件提供用户的选择为系统关键目录和系统文件，用户可以勾选选项来设置需要保护的文件或文件夹。

当有程序触发规则时，用户可以选择拒绝、放过和提示三种中的一种操作方式设置未知程序触发此规则所采取的操作方式。

5.9.3.2应用程序访问控制设置

应用程序访问控制设置页面显示了用户已经设置的规则的信息，并且可以添加、编辑和删除这些规则，当有程序触发这些规则时可以选择是否记录日志以及提示用户的信息类型。

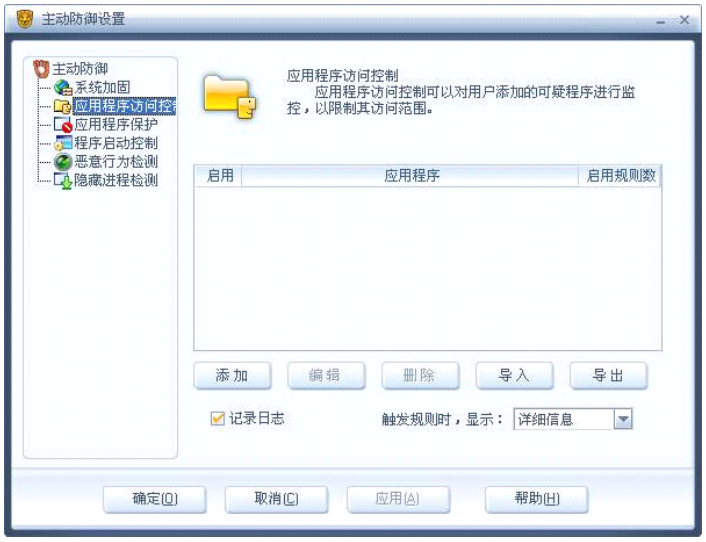

图 567

在此页面中，可以勾选【启用】项来启用设置的规则，并且可以查看当前启用的规则数。另外，还可以勾选【记录日志】将发现的程序操作记录到历史记录中，便于日后查看和分析。

触发规则时，显示方式有【详细信息】和【简要信息】两种。用户下拉此框来设置应用程序触发规则时候，提示用户的界面是简要信息界面还是详细信息界面。

注意：当系统管理员在管理控制台设置规则后，则在客户端前面为一个“灰色的锁”表示用户对该规则只能查看，不可以修改或删除。客户端用户添加规则后，会在前面出现带“绿勾的锁"，表示用户可以修改该规则。

当系统管理员在管理控制台的【主动防御规则设置】/【应用程序访问控制】页面锁定了记录日志等设置项，则在客户端相应的项前面出现一个“灰色的锁”表示用户对该规则只能查看，不可以修改设置。

各个按钮功能如下：

【添加】：单击此按钮进入添加规则界面设置规则。
【编辑】：单击此按钮进入编辑规则界面编辑规则。
【删除】：单击此按钮删除选中的规则。
【导入】：单击此按钮导入之前备份的规则文件。
【导出】：单击此按钮导出当前规则作为备份，避免今后频繁设置规则。

应用程序访问控制功能主要是针对了解计算机和病毒知识的用户设计的，瑞星杀毒软件仅提供规则，没有为用户设置规则应用对象，应用程序访问控制功能无法生效，需要用户自己设置。具体设置如下：

首先，设置规则应用的对象，在设置规则页面中，选择【添加】按钮，提示用户选择应用程序。

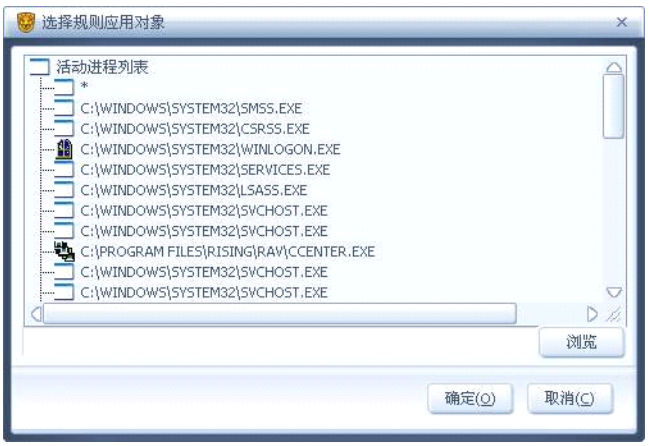

图 568

注意：列表中显示的是正在运行的进程，选择【浏览】按钮可以设置所有的程序。如果选择“*”，则为选中所有的进程，从而对它们进行设置，一般情况下，主要在设置注册表和文件规则时候，应用对象选择“*”。

其次，为设定的对象启用规则，瑞星杀毒软件为用户提供的规则类型包括限制启动子程序、限制全局挂钩、限制加载驱动、限制修改内核内存数据、文件和注册表。其中对于限制启动子程序，限制全局挂钩、限制加载驱动、限制修改内核内存数据，用户可以设置是否启用以及处理方式是提示、放过还是拒绝。对于文件和注册表用户可以添加、编辑和删除规则。

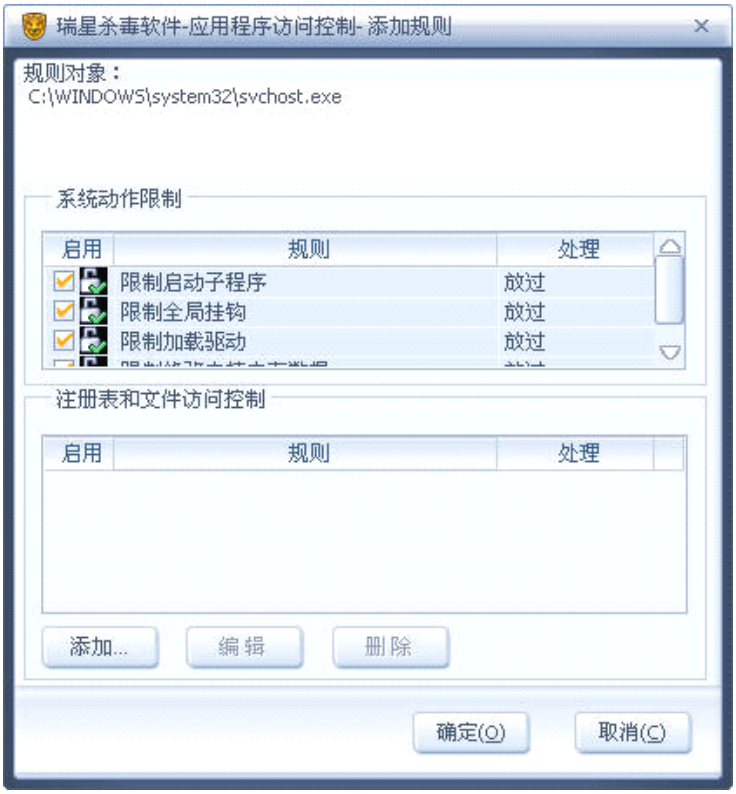

图 569

用户可以设置限制启动子程序、限制全局挂钩、限制加载驱动、限制修改内核内存数据、注册表和文件规则，选择触发规则时候的处理方式，分别为【提示】、【放过】、【拒绝】，如果需要添加、修改或者删除规则可以通过【添加】、【编辑】和【删除】三个按钮实现；勾选【启用】项则启用所设置的规则。

5.9.3.2.1 文件规则的设置

在文件和注册表规则页面中，单击【添加】按钮，会提示文件和注册表两项，选择文件则会显示以下页面，用户可以设置该规则。

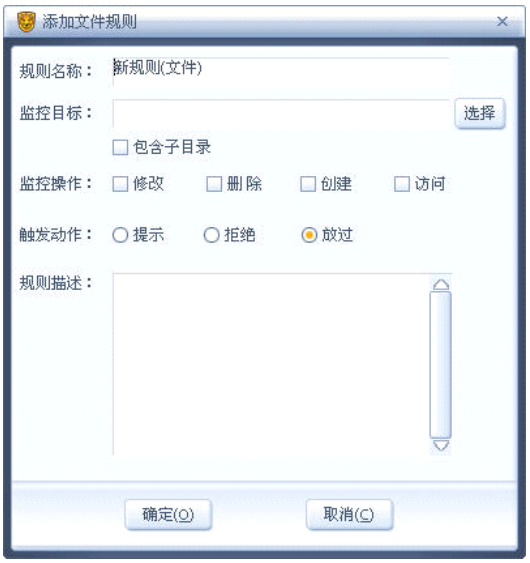

图 570

在此页面，用户可以进行以下设置：

- 规则名称：用户输入规则名称。
- 监控目标：输入或者选择监控目标。
  - 选择：点此按钮浏览监控目标。
  - 包含子目录：勾选此项将包括监控目标包含的子目录。
- 监控操作：用户选择监控未知程序的操作方式，包括创建、修改、删除、访问四项。
- 触发时的动作：用户选择未知程序触发此规则时的动作，包括提示、拒绝和放过三种动作。
- 规则描述：用户对此规则输入对规则的描述。

5.9.3.2.2 注册表规则的设置

在文件和注册表规则页面中，单击【添加】按钮，会提示文件和注册表两项，若选择注册表则会显示以下页面，用户可以设置该规则。

图 571

在此页面，用户可以进行以下设置：

- 规则名称：用户输入规则名称。
- 监控目标：输入或者选择监控目标。
  - 选择：单击此按钮显示注册表项菜单供用户选择。
  - 监控键：当用户创建一个当前系统还未存在的键的时候，勾选此项。
  - 包含子键：勾选此项将包括监控目标包含的子项。
- 监控操作：用户选择监控未知程序的操作方式，包括修改、删除和创建三项。
- 键名称：当用户勾选了监控操作中的创建时，此项则可编辑，输入用户需要监控的键名称，否则默认为键值。
- 触发时的动作：用户选择未知程序触发此规则时的动作，包括提示、拒绝和放过三种动作。
- 规则描述：用户对此规则输入自己的描述。

单击【选择】按钮，进入下一页面，浏览注册表项。

设置完毕后，会在应用程序保护控制页面显示该规则信息，用户可以选中规则对其进行编辑或者删除 。

5.9.3.3应用程序保护设置

应用程序保护设置页面为用户显示了用户已经设置规则以及这些规则的信息，并且用户可以添加、编辑和删除这些规则，当有程序触发这些规则时候是否记录日志，提示用户的信息是简要信息还是详细信息以及是否启用被保护的程序启动时提示。

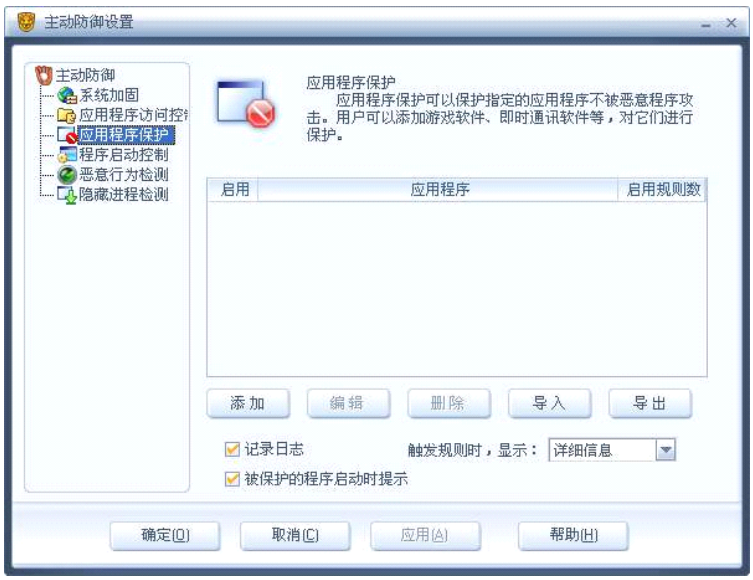

图 572

在此页面中，可以勾选【启用】项来启用设置的规则，并且可以查看当前启用的规则数。另外，还可以勾选【记录日志】将发现的程序的操作记录到历史记录中，便于日后查看和分析。

勾选【启用应用程序保护提示】，当被应用程序保护设定的程序被启动后，在计算机右下方，弹出提示框提示用户该程序已经被保护。

触发规则时，显示方式有【详细信息】和【简要信息】。用户下拉此框来设置应用程序触发规则时候，提示用户的界面是简要信息界面还是详细信息界面。

注意：当系统管理员在管理控制台设置规则后，则在客户端前面为一个“灰色的锁”表示用户对该规则只能查看，不可以修改或删除。客户端用户添加规则后，会在规则前面出现带“绿勾的锁”表示用户可以修改该规则。

当系统管理员在管理控制台的【主动防御规则设置】/【应用程序保护】页面锁定了记录日志、被保护的程序启动时提示等设置项，则在客户端相应的项前面出现一个“灰色的锁”表示用户对该规则只能查看，不可以修改设置。

各个按钮功能如下：

- 【添加】：单击此按钮进入添加规则界面设置规则。
- 【编辑】：单击此按钮进入编辑规则界面编辑规则。
- 【删除】：单击此按钮删除选中的规则。
- 【导入】：单击此按钮导入之前备份的规则文件。
- 【导出】：单击此按钮导出当前规则作为备份，避免今后频繁设置规则。

应用程序保护功能主要是针对了解计算机和病毒知识的用户设计的，瑞星杀毒软件仅提供规则，没有为用户设置规则对象，应用程序保护功能无法自动生效，需要用户自己设置。具体设置如下：

首先，设置规则应用的对象，在设置规则页面中，选择【添加】按钮，提示用户选择应用程序。

注意：列表中显示的是正在运行的进程，选择【浏览】按钮可以设置所有的程序。

选择其中的一项单击【确定】按钮或者浏览选择程序后，能够进入下面的页面进行应用程序选择。

其次，为设定的对象启用规则，用户可以设置触发规则的处理方式，分别为提示、拒绝或放过。

图 573

在【启用】项处进行勾选，则此应用生效。以下是对应用程序保护规则的介绍：

- 防注入 DLL：可以防止其它程序将动态库注入被保护进程。
- 防注入代码：可以防止其它程序将代码注入被保护进程。
- 防内存篡改：可以防止其它程序篡改被保护进程的内存。
- 防内存读取：可以防止其它程序读取被保护进程的内存。
- 防挂起：可以防止其它程序挂起被保护进程中的线程。
- 防结束：可以防止其它程序结束被保护进程中的进程和线程。
- 防模拟发送消息：可以防止其它程序向被保护进程发送消息。
- 防模拟按键：可以防止其它程序向被保护进程发送模拟的键盘输入的消息。
- 防监听键盘输入：可以防止其它程序监听被保护程序的键盘输入。

设置完毕后，会在应用程序保护设置页面显示该规则信息，用户可以选中规则对其进行编辑或者删除。

5.9.3.4程序启动控制设置

程序启动控制设置页面为用户显示了用户已经设置的规则以及这些规则的信息，并且用户可以添加、编辑和删除这些规则，当有程序触发这些规则时候是否记录日志以及提示用户的信息是简要信息还是详细信息。

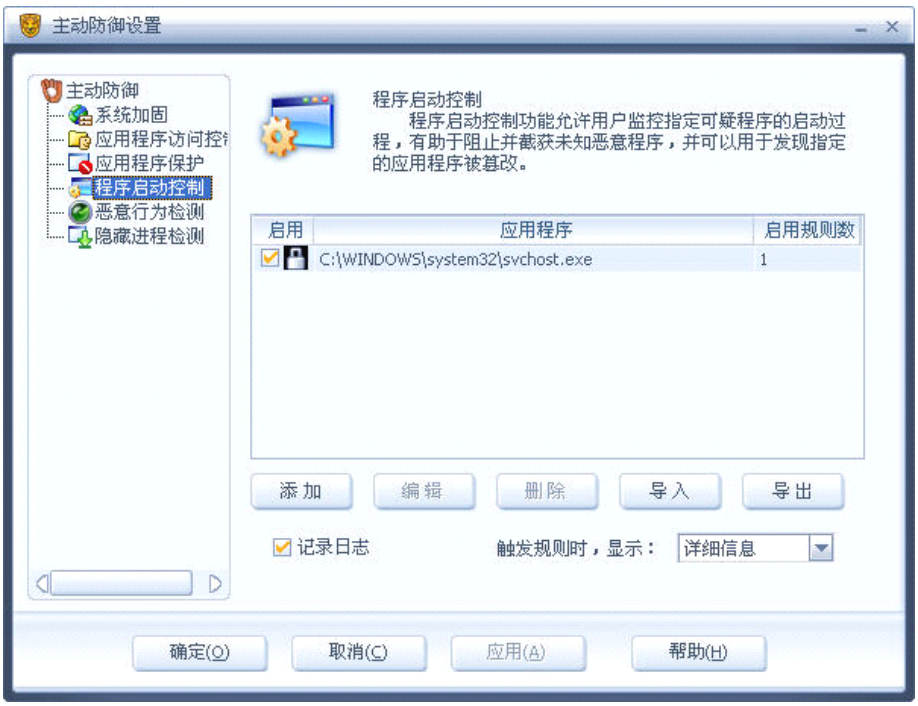

图 574

在此页面中，可以勾选【启用】项来启用设置的规则，并且可以查看当前启用的规则数。另外，还可以勾选【记录日志】将发现的程序的操作记录到历史记录中，便于日后查看和分析。

触发规则时，显示方式有【详细信息】和【简要信息】两种。用户下拉此框来设置应用程序触发规则时候，提示用户的界面是简要信息界面还是详细信息界面。

注意：当系统管理员在管理控制台设置规则后，则在客户端前面出现一个“灰色的锁”表示用户对该规则只能查看，不可以修改或删除。客户端用户添加规则后，会在规则前面出现带“绿勾的锁”表示用户可以修改该规则。

当系统管理员在管理控制台的【设置主动防御规则】|【程序启动控制】页面锁定了记录日志等设置项，则在客户端相应的项前面出现一个“灰色的锁”表示用户对该规则只能查看，不可以修改设置。

各个按钮功能如下：

- 【添加】：按此按钮进入添加规则界面设置规则。
- 【编辑】：按此按钮进入编辑规则界面编辑规则。
- 【删除】：按此按钮删除选中的规则。
- 【导入】：按此按钮导入之前备份的规则文件。
- 【导出】：按此按钮导出当前规则作为备份，避免今后频繁设置规则。

程序启动控制功能主要是针对了解计算机和病毒知识的用户设计的，瑞星杀毒软件仅提供规则，没有为用户设置规则应用对象，应用程序访问控制功能无法生效，需要用户自己设置。具体设置如下：

首先，设置规则应用的对象，在设置规则页面中，选择【添加】按钮，提示用户选择应用程序。

注意：列表中显示的是正在运行的进程，选择【浏览】按钮可以设置所有的程序。

选择其中的一项单击并且按【确定】按钮或者浏览选择程序后，能够进入下面的页面对设定的程序进行规则设置。

图 575

点击【添加】按钮，则出现如图 5-76 界面

图 576

在此页面，用户可以进行以下设置：

规则名称：输入规则名称。
启动者：弹出选择规则应用对象框供用户选择。
触发动作：提示、拒绝、放过和防篡改。
规则描述：用户输入对此规则的描述，便于当有程序触发此规则时候提示相关的信息。

注意：防篡改是将用户设置进程的校验值计算并记录下来，下次此进程启动时，进行比对校验，如果完全正确则放过，不正确则提示用户。

当选择启动者的时候，单击【选择】按钮，会弹出此页面，用户可以设置启动者，防止该启动者启动设定的应用程序。

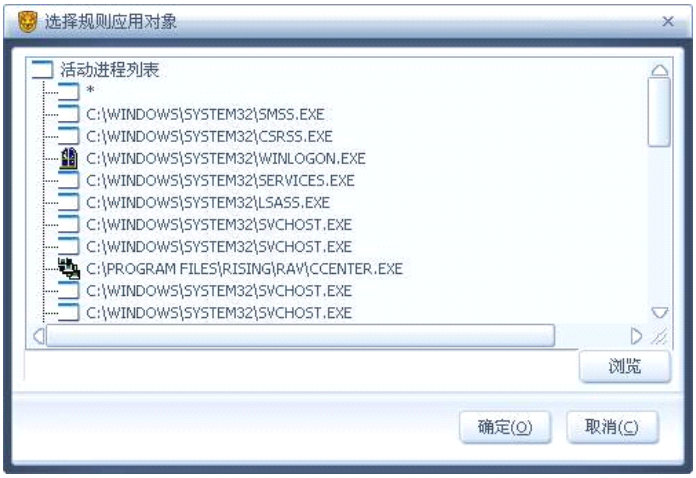

图 577

注意：列表中显示的是正在运行的进程，选择【浏览】按钮可以设置所有的程序。如果选择“*”，则会选中所有的应用程序，从而对它们进行设置。

设置完毕后，会在程序启动控制设置页中显示该规则信息，用户可以选中规则对其进行编辑或者删除 。

5.9.3.5恶意行为检测设置

瑞星杀毒软件已经为用户设置了恶意行为检测规则，用户可以启用此功能。并且可以设置通过恶意行为检测发现病毒后的处理方式是【仅报告】还是【提示我处理】。

图 578

在此页面，用户可以进行以下设置：

【恶意行为启发式检测敏感度】：用户可以拖动滑块选择敏感度级别，分别为高、中、低三种级别。

【发现程序存在恶意行为时】：用户可以选择相应的处理方式，包括【提示我处理】和【仅报告】两种方式，其中如果用户选择【仅报告】方式，该方式仅是提示用户有可疑程序但并不作处理，存在危险。

【记录日志】：勾选此项将记录日志。

【进程退出时进行家族病毒 DNA 扫描】：用户勾选此项后，当任意进程退出时，恶意行为检测会扫描这个进程是否为可疑的病毒程序。

注意：当系统管理员在管理控制台的【设置主动防御规则】/【恶意行为检测】页面锁定了记录日志、进程退出时进行家族病毒 DNA 扫描等设置项，则在客户端相应的项前面出现一个“灰色的锁”表示用户对该规则只能查看，不可以修改设置。

5.9.3.6隐藏进程检测设置

在隐藏进程检测设置页面，用户可以看到由瑞星软件检测到的进程，用户可以设置检测的间隔时间，并且可以单击【手工检测】按钮，刷新列表框中的进程。

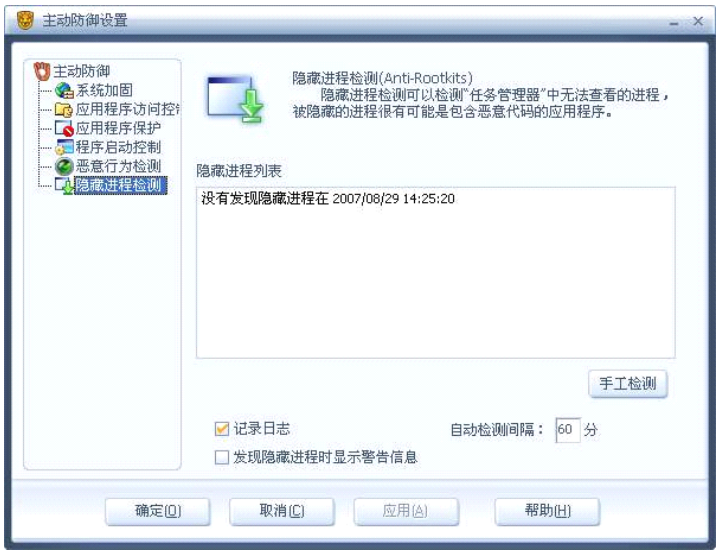

图 579

在隐藏进程列表，用户可以查看系统中存在的隐藏进程，并且对此功能用户可以进行以下设置：

- 【记录日志】：用户可以勾选此项来记录日志。
- 【自动检测间隔】：设置检测时间间隔，在用户设置的时间范围内刷新系统存在的隐藏进程列表。
- 【手工检测】：刷新系统存在隐藏进程列表，得到所有当前隐藏进程。
- 【发现隐藏进程时显示警告信息】：勾选此项当发现有隐藏进程时，托盘会弹出提示框提示用户存在隐藏进程。

注意：当系统管理员在管理控制台的【设置主动防御规则】/【隐藏进程检测】页面锁定了记录日志、发现隐藏进程时显示警告信息等设置项，则在客户端相应的项前面出现一个“灰色的锁”表示用户对该规则只能查看，不可以修改设置。

5.9.4 切换皮肤

用户可以选择不同风格的外观，包括：怀旧情调、蓝色月光、玄之魅影和古典朱红。

5.9.5 切换语言

提供软件支持语言的实时切换，满足不同用户的需要。目前瑞星可以提供四种语言的选择：中文简体 、中文繁体、English 和日文。

5.9.6 上报可疑文件

如果用户发现某个文件可能属于恶意文件，选择菜单【设置】/【上报可疑文件】，填写用户姓名以及联系方式（可以是 E-mail 地址或联系电话等），即可将通过网页将此文件上报给瑞星公司，以便检查分析可疑文件。

在扫描病毒过程中，如果发现可疑文件或者异常文件将自动提示用户上报可疑文件页面，用户可以将其上报。另外，当有可疑文件后，可以在安检页面中通过【将检测到的可疑文件上报】链接方式上报可疑文件，如图 580

图 580

5.10 文件粉碎

文件粉碎功能将废弃文件数据完全粉碎、清除，无法用常规手段恢复，保证用户隐秘资料的安全。

在准备粉碎的文件或文件夹上单击右键，选择【粉碎文件】，将显示【瑞星文件粉碎器】界面，粉碎列表中显示了用户已选择的准备粉碎的文件或文件夹。单击【添加】可以添加其它想要粉碎的文件到列表中；选中列表中某个文件或文件夹单击【移除】按钮可以把已选择的文件或文件夹从列表中删除；单击【清空】按钮将把粉碎列表清空。确定准备粉碎的文件后，单击【开始】按钮，即对列表中的所有文件执行粉碎操作。

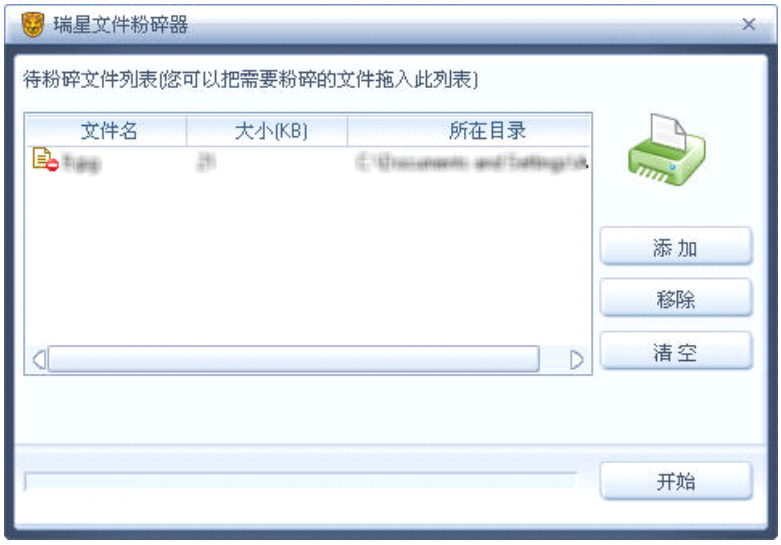

图 581

注意：粉碎文件的操作将导致被粉碎的文件无法恢复，须慎重选择，防止误操作造成数据丢失。

6 客户端本地防火墙的使用

说明：高级企业版有防火墙功能；高级企业专用版在购买时可以定制防火墙功能；中小企业版、企业版、企业专用版、网吧版无防火墙功能。

6.1 启动/关闭瑞星防火墙网络版

通过系统中心的管理控制台启动或关闭防火墙，具体方法如下：

方法一：使用超级管理员帐号登录管理控制台，选择要开启或关闭防火墙的客户端后，单击右键选择【开启防火墙】/【关闭防火墙】即可；

方法二：选择要开启或关闭防火墙的客户端后，单击管理控制台的工具按钮  或  即可开启/关闭防火墙。

6.2 主界面及菜单说明

6.2.1 防火墙主界面

双击客户端系统托盘上的防火墙图标，启动瑞星防火墙网络版主界面如图 61，共包括菜单栏、标签页、快捷按钮和状态栏。

图 61

工作状态页面

在工作状态页面中，显示具体如下信息：

- 防火墙状态：显示网络版防火墙开启或关闭的状态。
- 受攻击信息：

  1.可以显示攻击的名称，攻击者的 IP 地址、攻击的时间、攻击次数、攻击的端口。

  2.追踪位置：可以打开 http://www.ikaka.com 网站查询，根据攻击者的 IP 地址查询所在地。

  3.更多信息：可以查看防火墙日志。
- 网络状态：

  1.流量曲线：显示接收/发送数据包流量的曲线图。

  2.在曲线的左侧可以设定可显示的接收、发送数据包曲线的最高峰值。

  3.在流量曲线的右侧显示了接收、发送总的数据流量。

6.2.2 【操作】菜单

操作菜单包括：启动/停止保护、显示日志和退出，如图 62。

图 62

启动/停止保护：启动或停止防火墙，同主界面的“启动/停止保护”按钮。

显示日志：启动日志显示程序如图 63，功能同主界面的“查看日志”按钮。

图 63

退出：退出防火墙主程序。

6.2.3 【设置】菜单

详细设置：用户可以查看网络版防火墙的 IP 规则设置。

图 64

打开详细设置对话框，单击【规则设置】/【IP 规则】选项卡，查看防火墙的 IP 过滤规则，如图 65。

图 65

IP 规则：在 IP 层过滤的规则。列表中显示了规则名称、状态、协议、对方端口、本地端口和是否报警信息。

- 规则名称：每条规则都要有一个名称，用于标识这条规则。
- 执行动作：当发现匹配这条规则的数据包时进行的动作。有禁止、放行和忽略。如果是忽略的话，就传递到下面的规则进行处理；如果所有的规则都是忽略，就根据当前的安全级别确定这个数据包的处理状况。
- 协议类型：TCP、UDP、ICMP、IGMP、ALL、GRE、RDP、SKIP、ESP、AH 等。选择不同的协议类型会影响后面的选项。
- ICMP 类型：仅当协议类型为【ICMP】时可见。
  - 指定类型：指定一种单一的过滤类型。
  - 类型组合：指定多种类型进行组合，并控制方向。点击【编辑类型】进入详细设置界面，选中要控制的类型，勾选【匹配接收】、【匹配发送】，点击【应用】按钮后生效。

- 任意类型：设定对所有 ICMP 类型生效。

- 对方端口：这个数据包中对方的端口号。可设置【任意端口】、【指定端口】、【端口范围】或【端口列表】。
- 本地端口：这个数据包中本地的端口号。可设置【任意端口】、【指定端口】、【端口范围】或【端口列表】。
- 报警方式：
  - 托盘动画：防火墙的图标变成  并且闪烁。
  - 气泡通知：通过气泡窗口通知用户，气泡窗口会自动消失。
  - 弹出窗口：通过弹出窗口通知用户。
  - 记录日志：是否记录日志。
  - 声音报警：通过发出报警声音通知用户。

6.2.4 【帮助】菜单

帮助主题：在使用瑞星网络版防火墙的过程中，当用户有疑问或操作上的疑难问题时，可在帮助主题寻找答案；

官方网站：通过此选项程序可自动打开瑞星公司主页；

卡卡社区：通过此选项程序可自动进入卡卡社区；

关于瑞星：可查看瑞星防火墙网络版的相关信息。

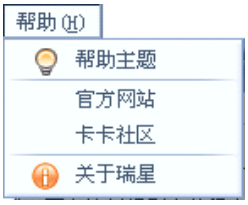

图 66

6.3 托盘图标

右键单击系统托盘中的防火墙图标，显示操作列表如图 67，包括：启动主程序、开启/停止保护、显示日志、关于和退出。用户可以根据实际需求操作。

图 67

注意：

1. 客户端没有设置防火墙的权限，只能启动或停止保护、查看日志。可以通过管理控制台开启或关闭防火墙。
2. 高级企业版中，默认安装防火墙但是不启动。
3. 高级企业专用版中，默认不安装防火墙，但可以通过专用信息码升级得到此功能，升级后默认也不启动。

附录一 北京瑞星科技股份有限公司简介

北京瑞星公司成立于 1998 年 4 月，前身为 1991 年成立的北京瑞星电脑科技开发部，是中国最早从事计算机病毒防治与研究的大型专业企业。瑞星以研究、开发、生产及销售计算机反病毒产品、网络安全产品和反“黑客”防治产品为主，拥有全部自主知识产权和多项专利技术。

目前，瑞星公司已推出基于多种操作系统的杀毒软件单机版、网络版软件产品；以及企业防毒墙、防火墙、网络安全预警系统等硬件产品，是全球第三家、也是国内唯一一家可以提供系列信息安全产品和服务专业厂商。

在公安部组织的计算机病毒防治产品评测中，“瑞星杀毒软件”单机版、网络版曾双双荣获总分第一的殊荣，并连续 5 年蝉联至今。公司拥有国内最大、最具实力的反病毒和网络安全研发队伍，并且拥有国内安全行业唯一的“电信级”呼叫服务中心和“在线专家门诊”Online 服务系统。瑞星和政府机构、商业伙伴以及媒体有着广泛深入的合作关系，借助内外部各种资源，目前已建成五大安全网络体系－－全球计算机病毒检测网、全球计算机病毒应急处理网、全国计算机病毒预报网、全国反病毒服务网以及全球疫情检测网。

瑞星公司拥有国内规模最大的反病毒研发和技术服务队伍，在反病毒和信息安全的技术研究方面已进入世界最前沿，通过与国家计算机病毒主管部门及国内、国际企业间的密切协作，承接国家信息安全研究项目，瑞星公司已为众多的政府部门、企业级用户以及个人用户提供了全方位的反病毒及信息安全解决方案，产品和服务深得用户的拥护和信赖。

通过这些年来的发展，瑞星公司已经建成国内完善的销售、服务体系，产品打入香港、日本等国际市场，瑞星公司立志成为最具价值的信息安全产品和服务提供商。

附录二 瑞星信息安全资讯网

瑞星信息安全资讯网是全球最大的中文专业信息安全网站，拥有简体中文、繁体中文、日文和英文四个版本，为个人和企业用户提供权威的反病毒和信息安全资讯服务。网站连续两年被评为中国商业网站100强，中国最优服务5佳网站。

瑞星网站是国内最权威的重大病毒和安全漏洞新闻发布平台，每当出现重大病毒及系统安全漏洞威胁用户安全时，瑞星网站将提供全面的解决方案，包括病毒新闻、最新动态、技术解决方案和免费的专杀工具。同时，网站也提供手机短信息服务，为用户提供更贴身的信息安全保护。

瑞星网站可以为个人和企业用户提供量身订制的信息安全产品和服务，个人用户可以在网站进行免费在线查毒，及时检查自己计算机中是否隐藏着病毒，下载免费杀毒工具和漏洞弥补工具；企业用户可以在网站查找适合自己的信息安全解决方案，在线定购相应产品。

瑞星信息安全资讯网是一千多万瑞星正版用户自己的网站，它是瑞星公司对正版用户的售后服务在网络上的延伸。作为反病毒领域的领先企业，瑞星公司一直致力于不断地自我完善及不断进取之中，为了让您的计算机和存储的宝贵数据高枕无忧，瑞星公司再次提醒您关注瑞星信息安全资讯网站，提醒您不断进行软件的升级更新，避免遭到病毒的侵袭。