

瑞星杀毒软件网络版 使用手册

(2005 版)

北京瑞星科技股份有限公司

重要声明

感谢您购买瑞星公司出品的瑞星杀毒软件系列产品。请在使用瑞星杀毒软件之前认真阅读配套的使用手册，当您开始使用瑞星杀毒软件时，瑞星公司认为您已经阅读了本使用手册。

本使用手册的内容将随着瑞星杀毒软件的更新而改变，恕不另行通知。从瑞星网站（www.rising.com.cn）可下载本使用手册的最新版。

请在购买软件后一周内，认真填写“用户注册卡”并以“挂号”或“快递”形式邮寄到瑞星公司客户服务中心，以便进行登记注册（注：不能在瑞星网站注册！）。注册后的产品才会得到唯一合法使用该套产品的“产品授权书”其中包括用于从瑞星网站下载升级的“用户 ID 号”。**对于自购买日起一个月后未持有“产品授权书”的使用者，瑞星公司有权拒绝提供升级程序、技术支持和售后服务，并对因未及时获得瑞星公司的产品、技术、病毒疫情和服务等信息而造成的影响不承担任何责任。**了解注册用户获得的服务，请参阅《客户服务指南》。

作为计算机病毒清除工具，瑞星杀毒软件将进行不断的升级。无论是功能的增加、性能的提高还是清除病毒种类的增加，都关系到其实际的使用价值。**所以，在使用本产品过程中应随时保持与瑞星公司的联系，以便及时获得升级程序或更新换代产品。**

注意：瑞星公司的网络版系列产品包括：大型企业版、企业版、专用版、中小企业版和网吧版等。本手册以讲述企业版内容为准。

忠告客户

(1) 请将所购产品与“产品组件册”进行核对，以确定产品的完整性。确认购买的产品为瑞星公司的正版产品；

(2) 如果自产品购买之日起一个月内未将注册卡返回瑞星公司注册，将不能得到包括升级在内的技术支持和服务；

(3) 为了避免“产品序列号”、“用户 ID 号”等机密信息泄露，保障用户的合法权益不受侵害，瑞星公司不接受除了最终用户以外的任何人或机构的代替注册；

(4) 请准确填写注册卡中的每项内容确保及时注册；

(5) 请妥善保管“产品序列号”和“用户 ID 号”，以免软件被盗用，从而影响自己的正常使用。

(6) 一旦对产品包装内物品和注册过程有疑义，请立即向该套产品的提供商或瑞星公司咨询。

(7) 任何情况下，贵单位不得在授权范围外使用本软件。

瑞星服务联系方式

如果遇到了问题，在您寻求技术支持之前，请务必先仔细阅读本使用手册，或者直接访问瑞星网站中的客户服务频道寻找您遇到的问题和解决办法，我们将尽力帮助您解决问题。若您所遇到的问题仍然没有解决，请发送电子邮件或拨打瑞星公司客户服务电话。

客户服务：(010) 82616666

电子邮件：（请从瑞星网站“服务与支持”栏目内发送）

网址：<http://www.rising.com.cn>

中文网址：瑞星

邮政编码：100080

通信地址：北京市海淀区中关村大街 22 号·中科大厦 1305 室

2005 年 3 月 北京·中国

目录

重要声明.....	2
忠告客户.....	2
瑞星服务联系方式.....	3
第一章 认识网络版.....	10
1.1 产品组成.....	10
1.2 文件清单.....	10
1.3 应用环境.....	10
第二章 网络版概述.....	12
2.1 瑞星杀毒软件网络版体系结构.....	12
2.2 瑞星杀毒软件网络版工作原理.....	12
2.3 瑞星杀毒软件网络版防病毒管理.....	13
2.4 瑞星杀毒软件网络版的特点.....	14
第三章 安装与卸载.....	16
3.1 安装.....	16
3.1.1 系统中心的安装.....	16
3.1.2 服务器端和客户端的安装.....	22
3.1.2.1 脚本安装.....	22
3.1.2.2 远程安装.....	24
3.1.2.3 本地安装.....	24
3.1.2.4 Web安装.....	25
3.2 卸载.....	27
附表 1.....	28
附表 2.....	28
附表 3.....	28
第四章 客户端本地杀毒.....	29
4.1 瑞星杀毒软件网络版客户端的主要特性与功能.....	29
4.2 客户端本地杀毒软件的启动.....	31
4.3 客户端本地杀毒软件主程序界面及菜单说明.....	32
4.3.1 主程序界面说明.....	32
4.3.2 【操作】菜单说明.....	34
4.3.3 【视图】菜单说明.....	34

4.3.4	【设置】菜单说明	35
4.3.5	【帮助】菜单说明	35
4.4	用瑞星杀毒软件杀毒	35
4.4.1	在默认状态下快速查杀病毒	35
4.4.2	快速启用右键查杀	36
4.4.3	根据设定的安全防护级别进行查杀	37
4.4.4	按文件类型进行查杀	37
4.4.5	定制任务	38
4.4.5.1	定时扫描	38
4.4.5.2	开机扫描	39
4.4.5.3	屏保扫描	40
4.5	瑞星监控中心	40
4.5.1	启动瑞星监控中心	41
4.5.2	退出瑞星监控中心	42
4.5.3	文件监控	42
4.5.3.1	启动文件监控	42
4.5.3.2	文件监控设置说明	42
4.5.3.3	文件监控在工作中的提示	42
4.5.3.4	禁止文件监控	43
4.5.4	内存监控	43
4.5.4.1	启动内存监控	43
4.5.4.2	内存监控设置说明	43
4.5.4.3	内存监控在工作中的提示	43
4.5.4.4	禁止内存监控	44
4.5.5	邮件监控	44
4.5.5.1	启动邮件监控	44
4.5.5.2	邮件监控设置说明	44
4.5.5.3	邮件监控在工作中的提示	45
4.5.5.4	禁止邮件监控	46
4.5.5.5	垃圾邮件过滤	46
4.5.6	网页监控	46
4.5.6.1	启动网页监控	47
4.5.6.2	网页监控设置说明	47
4.5.6.3	网页监控在工作中的提示	47
4.5.6.4	禁止网页监控	47
4.5.7	引导区监控	47
4.5.8	注册表监控	48
4.5.9	漏洞攻击监控	49

4.6 嵌入式杀毒	50
4.6.1 使用Lotus Notes嵌入式杀毒	50
4.6.1.1 启用Lotus Notes 监控功能	50
4.6.1.2 Lotus Notes监控工作中的提示	51
4.6.1.3 关闭Lotus Notes监控功能	51
4.6.2 使用Office/IE嵌入式杀毒	51
4.7 使用黑名单列表	52
4.8 使用嵌入式杀毒工具	53
4.9 病毒隔离系统	54
4.9.1 启动病毒隔离系统	54
4.9.2 设置隔离区存储空间	55
4.10 硬盘数据备份与恢复	55
4.10.1 手动备份	55
4.10.2 硬盘数据恢复	56
4.11 制作瑞星DOS杀毒工具盘	56
4.11.1 制作启动软盘	56
4.11.2 制作USB启动盘	57
4.12 设置密码	57
4.13 瑞星漏洞扫描工具	58
4.13.1 启动瑞星漏洞扫描工具	58
4.13.2 漏洞扫描的使用	59
4.13.3 阅读扫描报告	59
4.13.4 查看安全漏洞信息	59
4.13.5 查看安全设置信息	60
4.13.6 获取系统漏洞的补丁包	60
4.13.7 进行漏洞的更新	61
4.13.8 “安全设置”漏洞的修补	61
4.13.9 扫描结果进行导入和导出	61
4.13.10 漏洞扫描使用时出现的问题的解决	62
4.14 注册表修复工具	62
4.14.1 启动注册表修复工具	62
4.14.2 使用注册表修复工具	63
4.14.3 注册表修复工具的风格	63
4.14.4 注册表修复工具列表栏的使用	64
4.15 瑞星短信通	65
4.15.1 启动瑞星短信通	65
4.15.2 使用瑞星短信通	66
4.15.2.1 【手机注册】	66

4.15.2.2 【登录瑞星短信通】	67
4.15.2.3 【发送短信】	67
4.15.2.4 【通讯录】	68
4.15.2.5 【短信传情】	68
4.15.2.6 【密码查询】	68
4.16 添加删除、修复和卸载	69
4.17 瑞星DOS杀毒工具使用指南	69
4.17.1 启动瑞星DOS杀毒工具	70
4.17.1.1 用软盘启动	70
4.17.1.2 用瑞星光盘启动	70
4.17.1.3 用USB盘启动	70
4.17.2 用瑞星DOS杀毒工具杀毒	71
4.17.3 用瑞星DOS杀毒工具恢复硬盘数据	72
4.17.4 用瑞星DOS杀毒工具提取硬盘引导区信息	73
第五章 全网安全管理	75
5.1 瑞星管理控制台概述	75
5.2 管理控制台的启动	75
5.3 瑞星管理控制台界面说明	76
5.3.1 菜单说明	77
5.3.2 组管理界面	83
5.3.3 计算机列表栏	83
5.3.4 病毒信息列表栏	84
5.3.5 消息窗口	84
5.4 远程控制	85
5.4.1 远程查杀	85
5.4.2 远程设置	85
5.4.2.1 策略的分发	85
5.4.2.2 选项设置	86
5.4.3 远程安装	89
5.4.3.1 远程安装管理控制台	89
5.4.3.2 远程安装瑞星杀毒软件（网吧版无此功能）	89
5.4.4 远程启动/关闭客户端监控	90
5.4.5 远程报警	90
5.4.6 远程全网查杀	91
5.5 用户管理	91
5.5.1 组管理	91
5.5.1.1 建立组	91

5.5.1.2 为指定的组添加用户	92
5.5.1.3 删除组	92
5.5.2 管理员管理	92
5.6 日志信息	92
5.6.1 病毒日志	93
5.6.2 瑞星病毒日志查询统计工具	93
5.6.3 事件日志	94
5.7 其他	94
5.7.1 广播的应用	94
5.7.2 删除客户端	96
5.7.3 记数统计	96
5.7.4 瑞星配置工具的使用	96
第六章 升级与扩容	102
6.1 升级配置	102
6.2 网络设置	102
6.3 产品序列号和用户 ID 号绑定注意事项	103
6.4 UNIX客户端升级	103
6.5 升级瑞星DOS杀毒工具	104
6.6 产品扩容	104
附录：使用过程中的故障问题解决	104
第七章 多级中心系统使用说明	106
前言	106
7.1 安装	107
7.1.1 安装前的准备	107
7.1.2 安装环境	108
7.1.3 关于上级通讯代理和下级通讯代理设置的特别说明	108
7.1.4 上级通讯代理的安装	108
7.1.4.1 上级通讯代理的安装条件	109
7.1.4.2 上级通讯代理的安装过程	109
7.1.5 下级通讯代理的安装	112
7.1.5.1 下级通讯代理的安装条件	112
7.1.5.2 下级通讯代理的安装过程	112
7.2 卸载	114
7.3 多级中心系统的网络安全管理	114
7.3.1 概述	114
7.3.2 操作与管理	114

7.3.2.1 对下级系统中心的查杀毒	114
7.3.2.2 对下级系统中心的实时监控	115
7.4 升级	115
第八章 客户服务	116
附录一 瑞星信息安全资讯网	117
附录二 如何有效防范病毒	117
附录三 如何降低由病毒破坏所引起的损失	118
附录四 瑞星全线产品列表	118
附录五 瑞星杀毒软件网络版产品系列	119
附录六 北京瑞星科技股份有限公司简介	120

第一章 认识网络版

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组件：

1. 光盘：包含瑞星杀毒软件网络版所有程序(支持光盘启动进行 DOS 查杀病毒)。
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》：本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，请填写并挂号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. 产品组件册：用于核对产品组件，以确定产品的完整性。

1.2 文件清单

光盘

序号	文件名	说明
1	RavSetup.exe	瑞星杀毒软件网络版安装程序
2	Ravscript.exe	脚本登录安装程序
3	RavCheck.exe	瑞星杀毒软件网络版辅助安装程序
4	Autorun.inf	光盘自启动配置文件
5	Autorun.exe	光盘自动运行程序

1.3 应用环境

瑞星杀毒软件网络版是专门为 Windows NT/2000 网络环境开发的计算机病毒防护系统。

➤ 它支持的服务器操作系统有：

- ❖ Windows NT 4.0 Server 简体中文版，繁体中文版，英文版
- ❖ Windows 2000 Server 简体中文版，繁体中文版，英文版

- ❖ Windows 2000 Advanced Server 简体中文版，繁体中文版，英文版
- ❖ Windows 2003 Server 简体中文版，繁体中文版，英文版
- 它支持的客户机操作系统有：
 - ❖ Windows 95/98/Me 简体中文版，繁体中文版，英文版
 - ❖ Windows NT 4.0 Workstation 简体中文版，繁体中文版，英文版
 - ❖ Windows 2000 Professional 简体中文版，繁体中文版，英文版
 - ❖ Windows XP Home Edition 简体中文版，繁体中文版，英文版
 - ❖ Windows XP Professional 简体中文版，繁体中文版，英文版

第二章 网络版概述

2.1 瑞星杀毒软件网络版体系结构

瑞星杀毒软件网络版整个防病毒体系是由四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，还与另外子系统通讯，协同工作，共同完成对网络的病毒防护工作。

一、系统中心

系统中心是瑞星杀毒软件网络防病毒系统信息管理和病毒防护的自动控制核心。它实时记录防护体系内每台计算机上的病毒监控、检测和清除信息。根据管理控制台的设置，实现对整个防护系统的自动控制。其他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。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。详细内容，请参阅“3.1.1 系统中心的安装”节

二、服务器端

服务器端是专门为可以应用为网络服务器的操作系统设计的防病毒子系统。

三、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。它承担着对当前工作站上病毒的实时监控、检测和清除任务，同时自动向系统中心报告病毒监测情况。

四、管理控制台

管理控制台是为网络管理员专门设计，对网络防病毒系统进行设置、使用和控制的操作系统平台。利用管理控制台可以集中管理网络上所有已安装有瑞星杀毒软件网络版客户端的计算机，保障每个纳入瑞星杀毒软件防护网络的计算机时刻处于最佳的防病毒状态。它既可以安装到服务器上，也可以安装到客户机上，视网络管理员的需要，可自由安装。所以，它又被称为“移动管理控制台”。

2.2 瑞星杀毒软件网络版工作原理

瑞星杀毒软件网络版安装到服务器和客户机上后，通过“系统中心”、“服务器端”、“客户端”和“管理控制台”四个子系统的协同工作，实现了对网络上病毒的实时监控、定时扫描、手动扫描、自动或手动升级、信息管理等功能。同时提供了用户合法身份认证结构，保障用户利益。（如图 1）

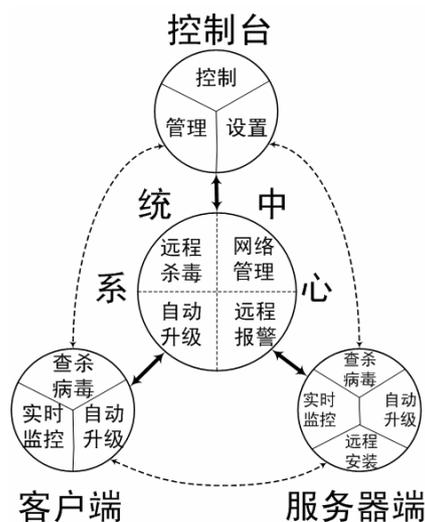


图 1

2.3 瑞星杀毒软件网络版防病毒管理

当一个计算机网络安装瑞星杀毒软件网络版后，必须将防病毒管理纳入日常工作。只有通过网络系统管理员、瑞星杀毒软件网络版和瑞星公司的客户服务中心三方努力下才能真正实现整个网络安全的目的。针对瑞星杀毒软件网络版提供的功能和特点，建议网络系统管理员进行如下的管理：

► 确立病毒防护原则

在通过瑞星杀毒软件网络版、企业自身技术人员（多指网络管理员）和瑞星公司客户服务工程师建立起网络的防病毒体系后，还必须确立该体系运转的工作原则。视每个企业的网络状况、技术人员状况和其他实际情况，瑞星公司提出以下建议：

- ❖ 所有计算机均应安装瑞星杀毒软件，避免形成防护体系的薄弱环节。在购买产品时，网络版授权安装的服务器和客户机数量应大于或等于实际的数量。
- ❖ 强制每台计算机开启瑞星实时监控功能。
- ❖ 在每台服务器和客户机上设定合理的定时扫描频率。
- ❖ 每次手动查杀病毒时，选择扫描所有文件。
- ❖ 在重要服务器或客户机上选中【杀毒时备份染毒文件到病毒隔离系统】选项。
- ❖ 系统管理员通过管理控制台获得某台服务器或客户机染毒信息后，应针对该计算机进行专门处理。

► 病毒防护信息管理

系统中心对防护体系内所有计算机的病毒监控、检测，以及处理情况均有记录。对这些信息的有效监控、利用和管理会使整个防病毒工作更加有效。网络管理员应根据网络的实际运行状况和工作需要制定切实可行的管理方案。

► 监控、检测和清除病毒

该项管理是网络防病毒管理的核心，利用瑞星杀毒软件网络版提供的各项功能可实现对所有计算机设计具体的管理方案。如对实时监控、扫描、清除时间、周期等设置。

➤ 未知病毒侦测管理

由于新病毒的不断出现，反病毒软件也要随之更新。只有建立一套完整可行的新病毒侦测和捕获方案才能实现这一过程的良性循环和周期的缩短。这也是维护整个网络安全必不可少的环节。一旦发现异常现象，及时与瑞星公司联系。

➤ 版本升级更新管理

彻底解决新病毒的办法是保证杀毒软件的不断升级更新。为此，网络管理员应充分利用瑞星公司提供的各种升级方式，结合自身具体情况，制定合理的升级管理办法，并组织实施。

➤ 与瑞星公司的信息交流

与瑞星公司的信息交流是保证病毒防护体系不断完善的最佳途径。

2.4 瑞星杀毒软件网络版的特点

2.4.1 国际领先的杀毒技术

瑞星杀毒软件采用了瑞星新一代病毒扫描引擎技术，继承并发扬瑞星公司十余年的反病毒经验，可全面处理各种 DOS 病毒、Windows 3.x 病毒、Windows 9x 病毒、宏病毒、网络病毒和黑客程序等。

2.4.2 远程化管理

- ❖ 远程杀毒：网络管理员只需通过一台安装有管理控制台的计算机，就可以对全网的所有计算机同时进行病毒检测和清除工作。（注意：网吧版不支持此功能）
- ❖ 远程报警：局域网中任何一台计算机上发现病毒时，瑞星杀毒软件自动将病毒信息传递给网络管理控制台。
- ❖ 远程设置：网络管理员只需通过一台安装有管理控制台的计算机，就可以对全网所有瑞星杀毒软件客户端进行统一或个性化设置。

2.4.3 自动化管理

- ❖ 自动安装：整个局域网只需在一台计算机上安装瑞星杀毒软件，即可实现对所有计算机的自动安装。
- ❖ 自动升级：系统中心自动从瑞星网站下载最新升级版本，安装有瑞星杀毒软件的各节点计算机自动请求升级，实现全网统一升级。

2.4.4 功能强大，操作简便

针对以往网络版杀毒软件设置复杂，操作繁琐的弊病，瑞星杀毒软件网络版采用智能化的底层优化技术，在保持功能强大的前提下，实现了界面简洁、操作便利的目标，最大限度地减少了用户操作难度和工作量。

2.4.5 集中式管理、分布式杀毒

- ❖ 系统中心结合移动管理控制台实现全网智能化管理

局域网内任意一台计算机均可设置为移动管理控制台。网络管理员通过帐号和口令使用移动管理控制台，即可清楚地掌握整个网络环境中各个节点的病毒监测状态，对局域网进行远程集中式安全管理。

❖ 先进的分布式管理技术

瑞星杀毒软件采用先进的分布式管理技术，调用每个节点各自的杀毒软件对该计算机上所有文件进行全面查杀病毒，解决了以往网络版杀毒软件只能查杀共享文件的缺陷。由于不在网络上传输文件，既保障了每个节点使用者的隐私，又大大提高了全网查杀病毒的效率。

2.4.6 完备的服务与技术支持

瑞星公司拥有完备的病毒跟踪系统，能够及时发现各种流行和新生病毒并提供解决方案。同时，通过互连网站提供 24 小时不间断升级服务。网络管理员可自行设置升级方式，通过瑞星杀毒软件网络版与网络的无缝连接，以及瑞星公司自行开发的断点续传技术，使得升级既迅速及时，又安全可靠。

瑞星公司客户服务中心为用户提供全天候技术咨询和支持，并利用遍布全国各地的服务网开展救助服务，满足用户各种需求。

第三章 安装与卸载

3.1 安装

瑞星杀毒软件网络版是由四个相互关联的子系统组成。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”。安装首先是在服务器上安装“系统中心”，然后才能进行其他三个模块的安装。

3.1.1 系统中心的安装

系统中心简介

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

提示：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。

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) 可方便上网：瑞星杀毒软件网络版具有自身更新、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。

提示：系统中心不要求一定安装在域控制器上，请用户在安装瑞星杀毒软件网络版时考虑现有网络中的资源分配。

系统中心的安装过程

首先确定准备安装瑞星杀毒软件网络版系统中心的服务器，对操作系统的需求请参阅本章附表1。

安装步骤如下：

第一步：进入操作系统；

第二步：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，安装即开始（如图2）；

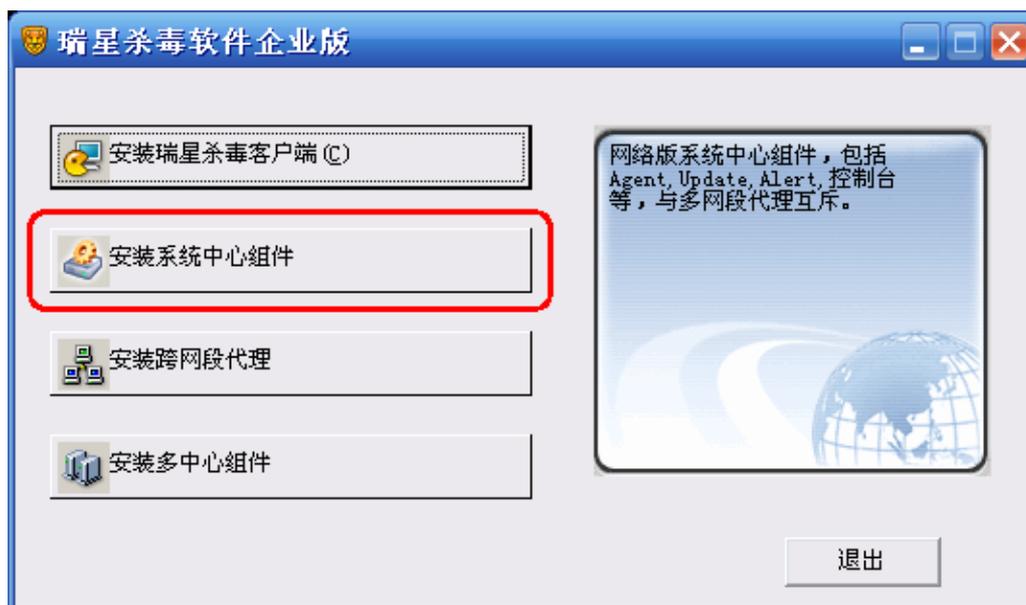


图2

提示：瑞星杀毒软件网络版安装光盘内容见本章附表2。

第三步：进入欢迎安装程序界面，点击【下一步】按钮继续（如图3）；

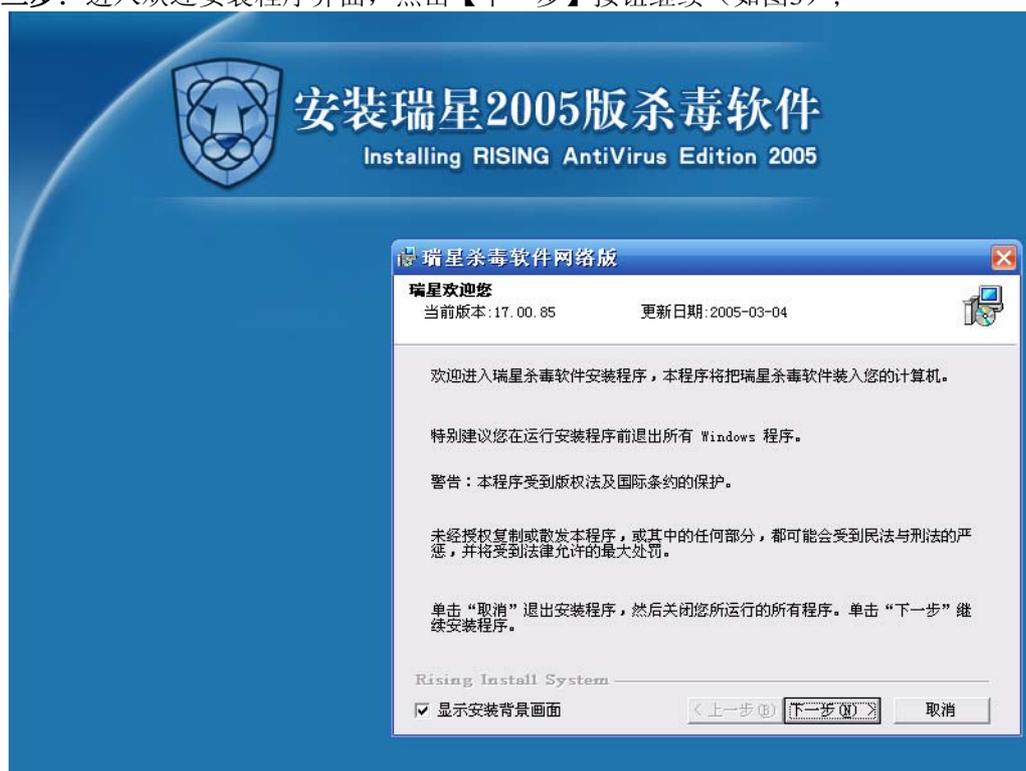


图3

第四步：随即弹出【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，请单击【我接受】选项，选择【下一步】继续安装。如不接受该协议，单击【我不接受】退出安装程序（如图4）；

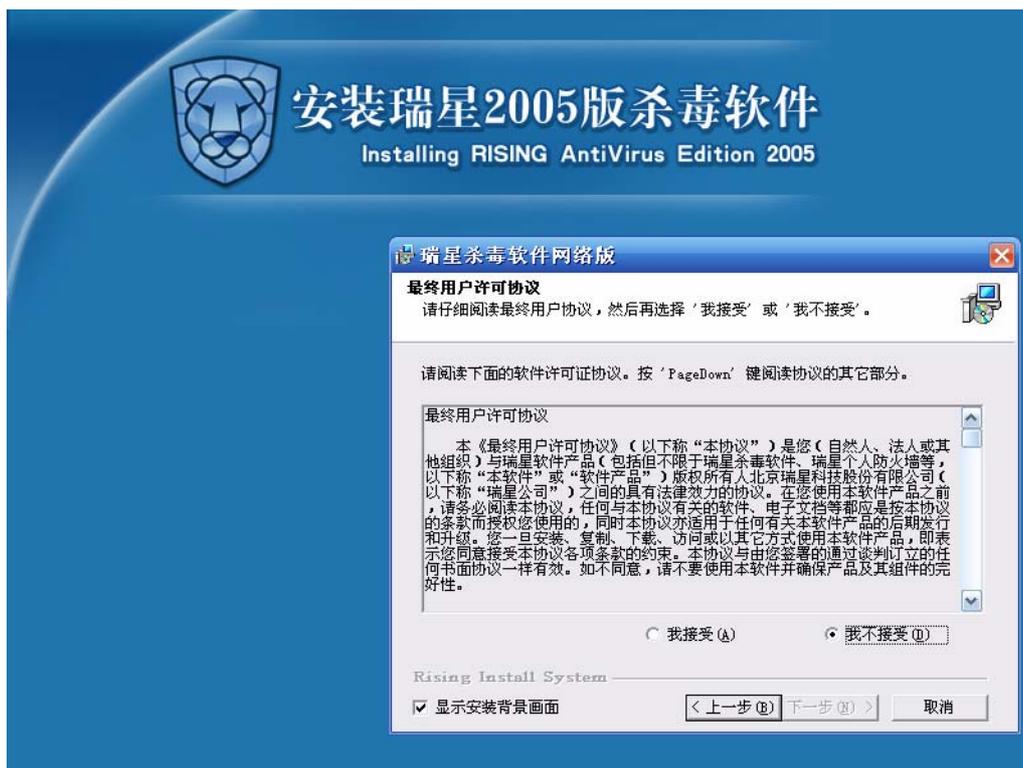


图4

第五步：安装【系统中心】组件，点击【下一步】继续安装（如图5）；

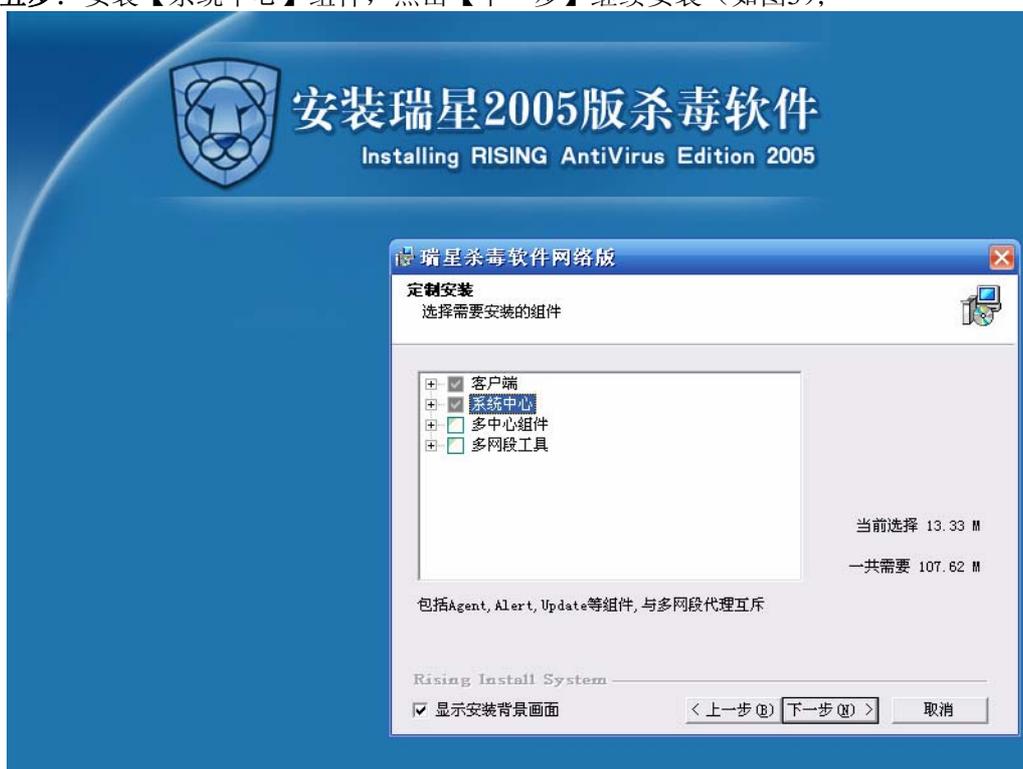


图5

第六步：输入瑞星杀毒软件网络版产品序列号（如图6）；

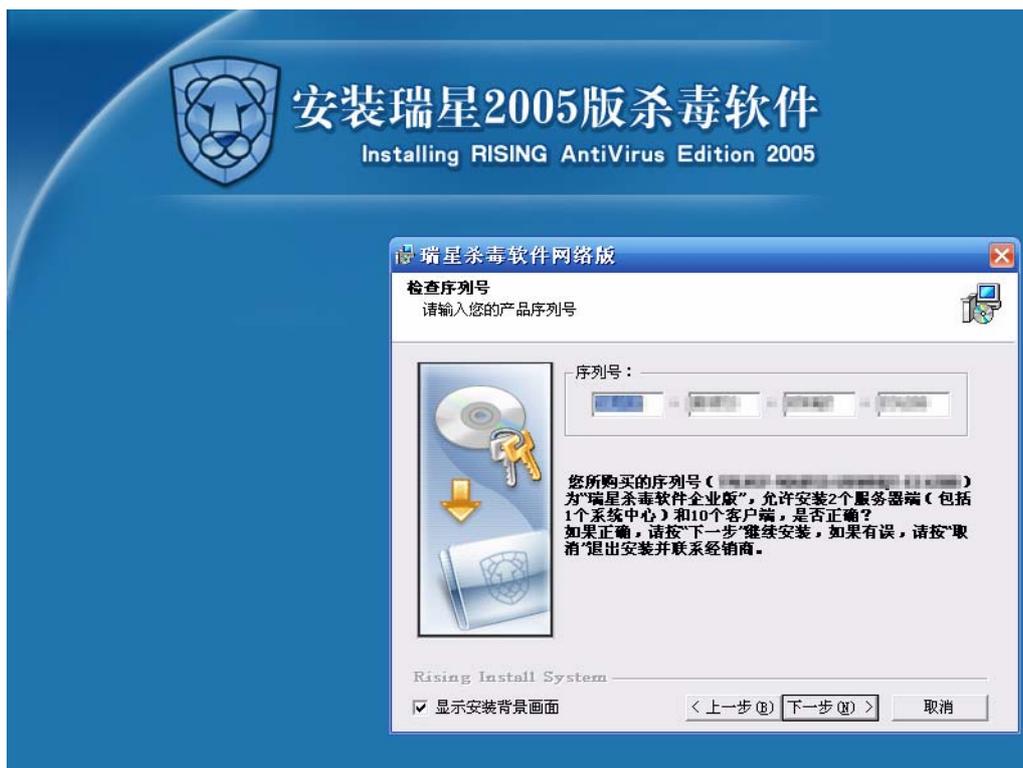


图6

提示：正确输入产品序列号后，立即显示服务器端和客户端允许安装的数量。

第七步：确认【选择安装目录】，选择【下一步】继续安装（如图7）；

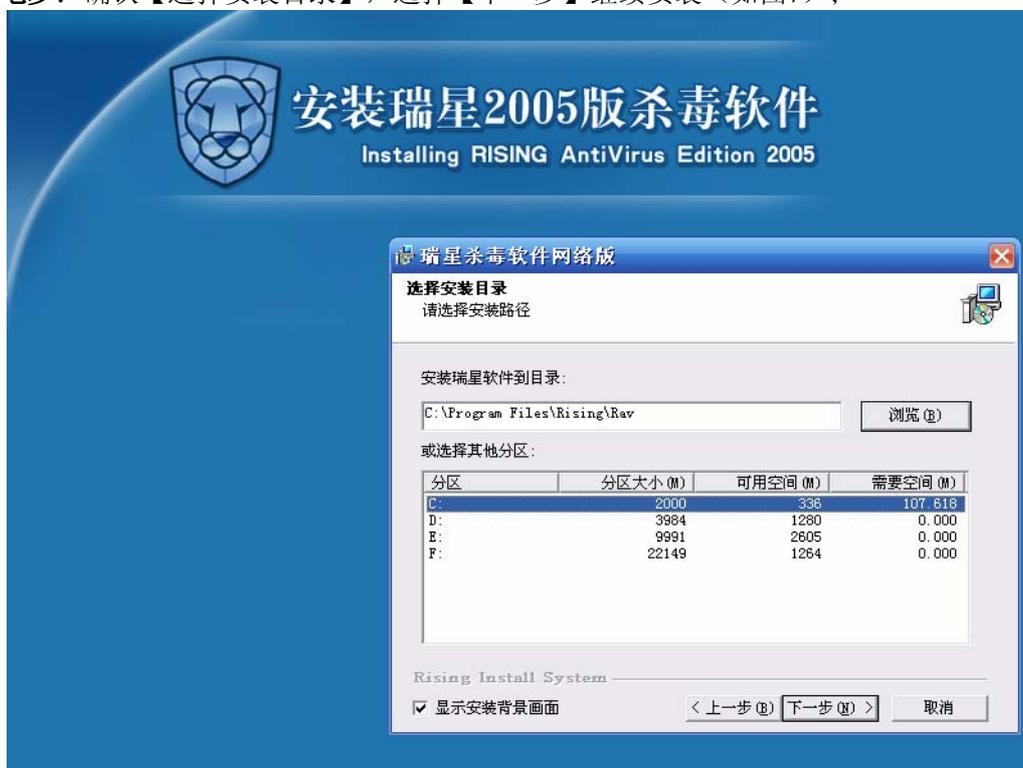


图7

第八步：确认【设置补丁包共享目录】，选择【下一步】继续安装（如图8）；

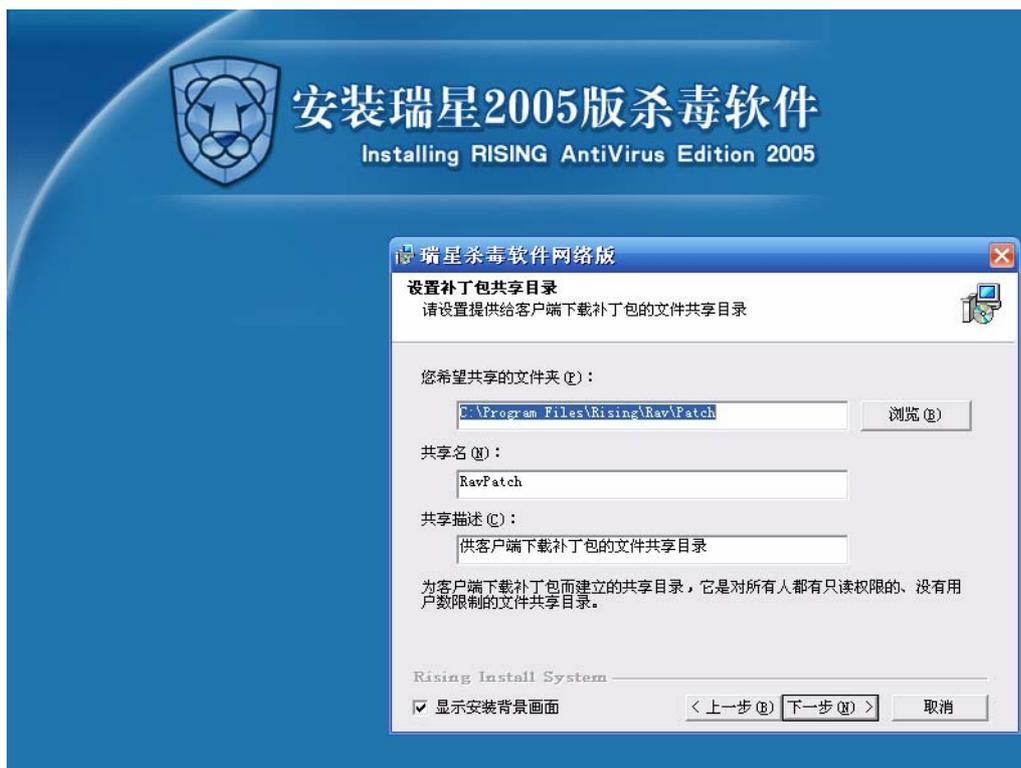


图8

第九步：确认【程序组】的名称，选择【下一步】继续安装（如图9）；

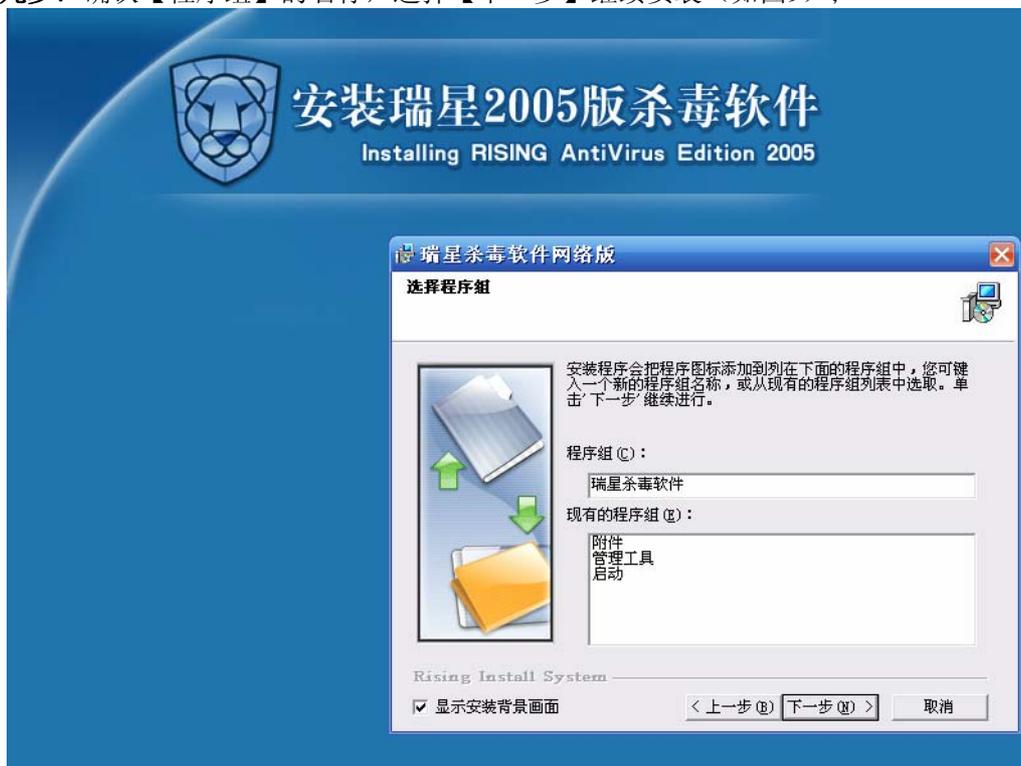


图9

第十步：安装程序将进行安装前的系统内存查毒，建议完成系统内存查毒操作后才开始复制文件，选择【下一步】开始复制文件（如图10）；

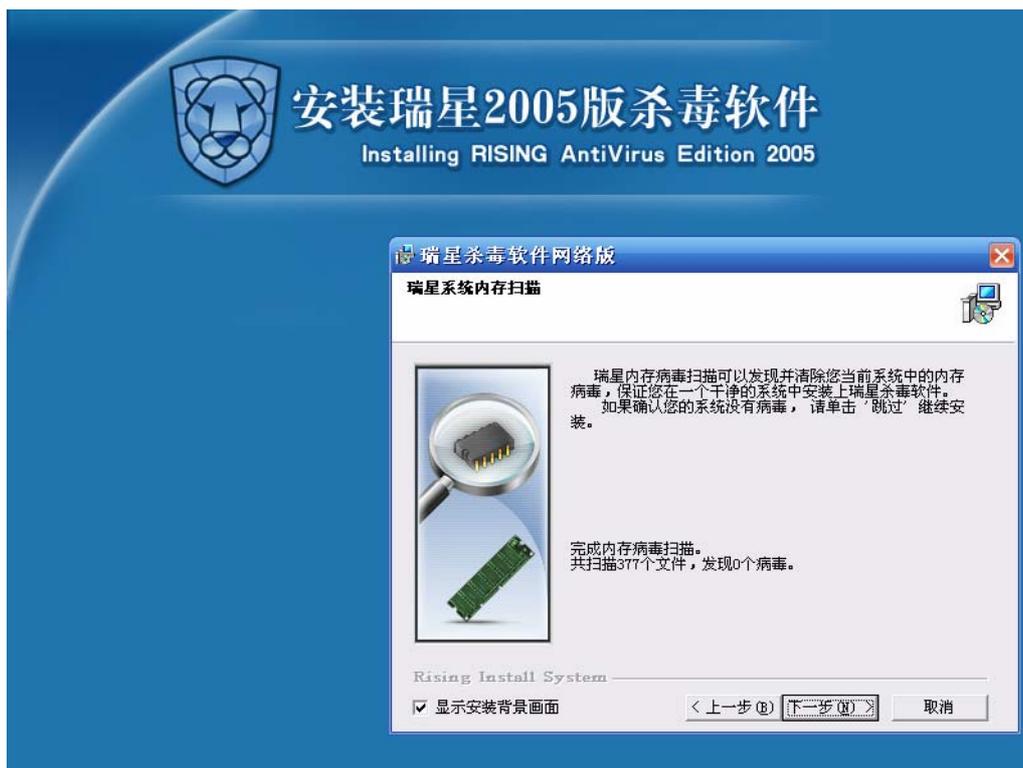


图10

第十一步：文件复制结束后，选择【完成】结束安装（如图11）。

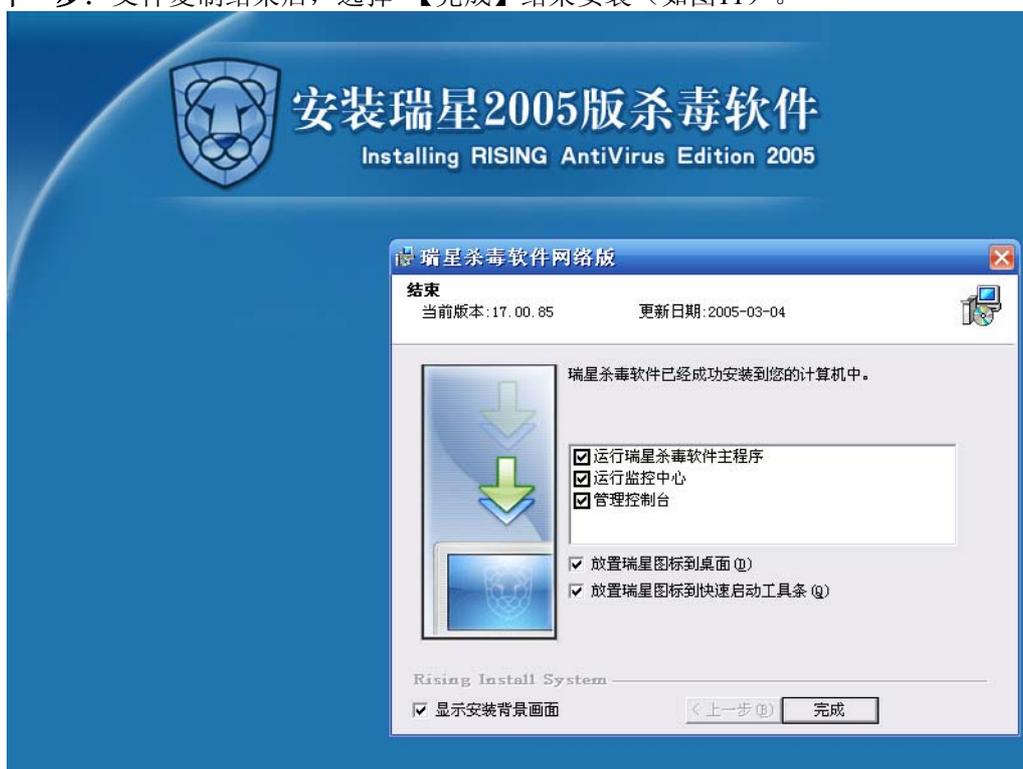


图11

3.1.2 服务器端和客户端的安装

服务器和客户端采用的安装方式包含脚本安装、远程安装、本地安装和 Web 安装，各个操作系统支持的安装方式详情参阅本章末的附表 3。

3.1.2.1 脚本安装

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。当用户登录到系统中心所在域时，实现自动为其安装瑞星杀毒软件网络版。

在域服务器上的脚本安装

第一步：将瑞星杀毒软件网络版光盘放入本机的光驱内，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】按钮，安装程序即开始。

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（如图 12）所示的安装向导界面；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。



图 12

注意：添加脚本请选【添加瑞星用户】，卸载脚本请选【删除瑞星用户】；添加脚本和卸载脚本的以下步骤相同。

第三步：在用户列表框中单击选择要安装或卸载脚本的用户（如图13）



图 13

第四步：出现如图 14 所示的界面后脚本安装完成。



图 14

在客户端的设置，以配合脚本方式安装。

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。

第一步：进入【Microsoft 网络用户属性】界面，选择登录到域；（如图 15）

注意：下图以 Windows 98 为例，瑞星杀毒软件网络版支持的其他操作系统的具体设置请参考相关操作系统使用手册；

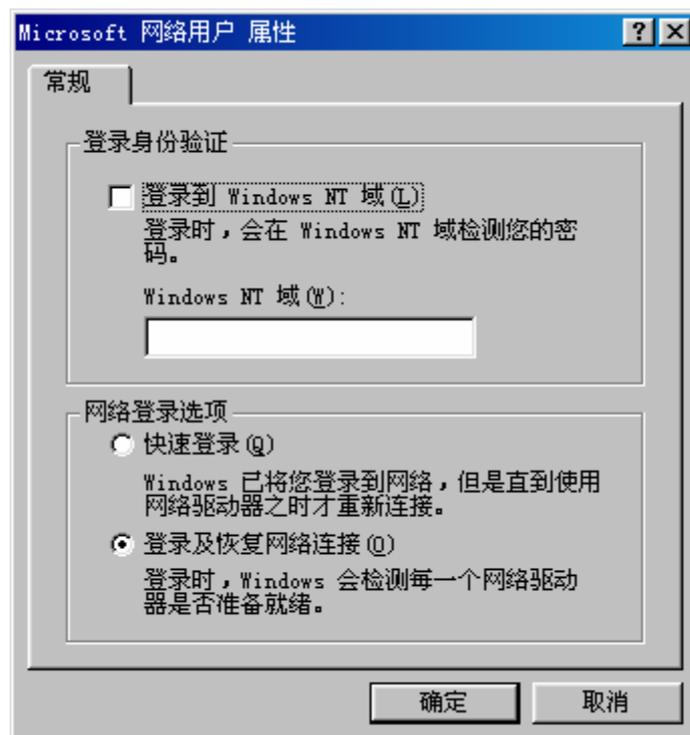


图 15

第二步：重新启动计算机，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。

提示：

1、脚本登陆安装需要被安装计算机人员的参与以完成所有的安装步骤。详细情况请参阅“3.1.2.3 本地安装”小节。

2、对于 Windows NT、Windows 2000、Windows XP、Windows 2003 操作系统，登录计算机的域用户需要具有被登陆计算机的本地管理员权限。

3.1.2.2 远程安装

远程安装是实现瑞星杀毒软件网络版快速自动安装的另一种重要方法。主要操作是在瑞星管理控制台上完成的；（详细操作请参阅“5.4.3 远程安装”）

注意：远程安装功能对操作系统的要求请参阅本章附表 3。

3.1.2.3 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端都可以采取本地安装的方式。

安装步骤如下：

第一步：运行光盘中的 Autorun，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），选择【安装瑞星杀毒客户端】按钮；

第二步：进入安装程序欢迎界面，点击【下一步】按钮继续安装；

第三步：随即弹出【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，请单击【我接受】选项，选择【下一步】继续安装。如不接受该协议，单击【我不接受】退出安装程序；

第四步：程序将自动检测本机的操作系统，根据附表 1 的规则提示安装瑞星程序，选择【客户端】

组件，按【下一步】继续安装；

第五步：确认【程序组】的名称，选择【下一步】继续安装；

第六步：安装程序将进行安装前的系统内存查毒，建议完成系统内存查毒操作后才开始复制文件，选择【下一步】开始复制文件；

第七步：文件复制结束后，选择【完成】结束安装。

注意：瑞星程序会自动识别需要安装跨网段代理程序的计算机。安装完毕后，跨网段代理同其他瑞星程序一样驻留在后台运行，并在 Windows 操作系统的状态栏中显示图标，在双击图标弹出的窗体上显示系统中心的 IP 地址，并可重新指向系统中心的 IP 地址。

3.1.2.4 Web 安装

Web 安装是指用户通过浏览指定位置的网页来实现网络版的安装。

第一步：指定网络内的一台机器提供 Web 安装功能，首先确定这台机器已经安装了 Internet 信息服务（IIS）组件；

第二步：运行 RavWebSetup.exe 程序，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 C:\Inetpub\wwwroot\ravweb），点击【安装】按钮开始安装，完成后点击【确定】结束安装（如图 16）；



图 16

第三步：选择【开始】/【控制面板】/【管理工具】/【Internet 信息服务】/【本地计算机】/【网站】，用鼠标右键点击【默认网站】，在右键菜单中点击【属性】，在【默认网站属性】对话框中选择【网站】标签，指定【IP 地址】和【TCP 端口】；

第四步：选择【主目录】标签，选中【此计算机上的目录】单选钮，再指定【本地路径】（默认路径是 C:\Inetpub\wwwroot\ravweb）（如图 17）；

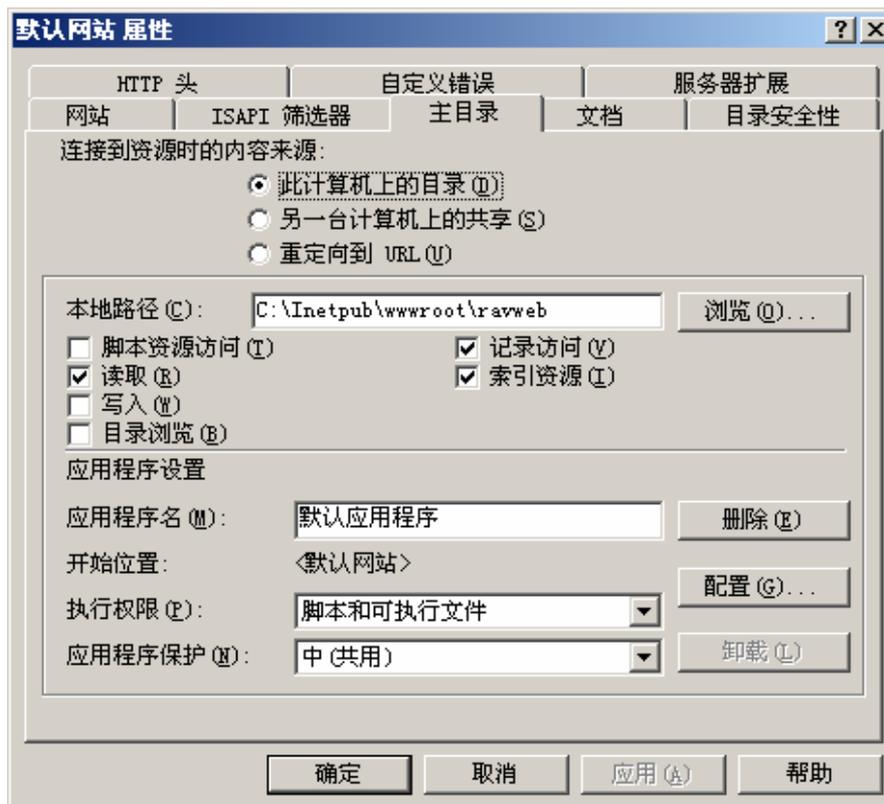


图 17

第四步：选择【文档】标签，确认 RavWeb.htm、Default.htm、Default.asp、index.htm 和 iisstart.asp 等项已经添加，选中【启用默认文档】复选框；

第五步：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 安装功能的机器的 IP 地址，显示【瑞星杀毒软件网络版 Web 安装】页面，点击【立即下载】按钮，将安装包下载至本地进行安装（如图 18）。

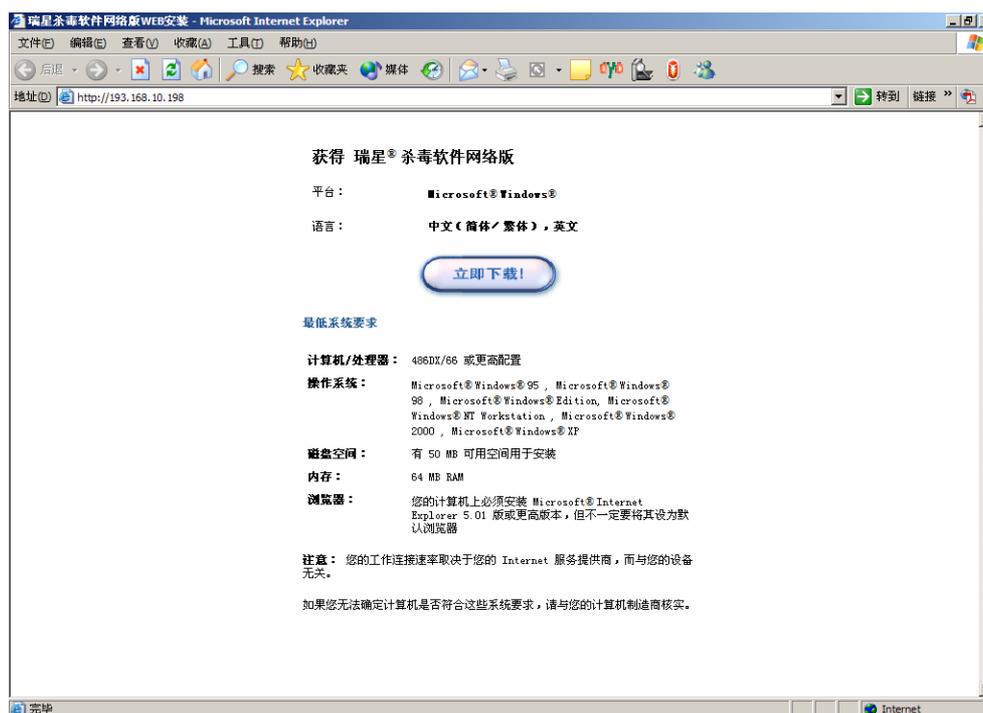


图 18

3.2 卸载

瑞星杀毒软件网络版提供了两种卸载方法：

方法一：在 Windows 画面中，选择【开始】/【程序】/【瑞星杀毒】/【卸载瑞星软件】（如图 19），随即开始卸载瑞星杀毒软件。



图 19

方法二：在 Windows 画面中，选择【开始】/【设置】/【控制面板】/【添加/删除程序】/【瑞星杀毒软件】/【更改/删除】，随即开始卸载瑞星杀毒软件。（如图 20）



图 20

附表 1

系统中心、服务器端和客户端在安装时所需操作系统

	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 2003 Server	√	√	

附表 2

瑞星安装光盘内容

序号	文件名	功能介绍
1	RavSetup.exe	瑞星杀毒软件网络版安装程序
2	Ravscript.exe	登录脚本安装程序
3	Autorun.exe	瑞星杀毒软件网络版安装主界面
4	Autorun.inf	光盘自启动配置文件
5	RavCheck.exe	瑞星杀毒软件网络版辅助安装程序

附表 3

本地安装、脚本安装和远程安装所需的操作系统

	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 Hoem Edition	√		√
	Windows XP Professional	√	√	√
服务器端	Windows NT Server	√	√	√
	Windows 2000 Server	√	√	√
	Windows 2000 Advanced Server	√	√	√
	Windows 2003 Server	√	√	√

注意：网吧版不支持远程安装客户端瑞星杀毒软件。

第四章 客户端本地杀毒

4.1 瑞星杀毒软件网络版客户端的主要特性与功能

4.1.1 首创智能解包还原技术，支持族群式变种病毒查杀

采用瑞星独创的智能解包还原技术，解决了杀毒软件无法有效查杀因使用各种公开、非公开的自解压程序对病毒进行压缩打包而产生大量变种病毒的世界性技术难题，彻底根治此类变种病毒造成的危害。

4.1.2 增强型行为判断技术，防范各类未知病毒

瑞星首创的”行为判断查杀未知病毒”技术再次实现突破，不仅可查杀 DOS、邮件、脚本以及宏病毒等未知病毒，还可自动查杀 Windows 未知病毒。在国际上率先使杀毒软件走在了病毒前面，并将防病毒能力拓展到防范 Windows 新病毒。

4.1.3 一体化监控

文件监控、邮件监控、内存监控、网页监控、注册表监控、引导区监控和漏洞攻击监控协同工作，提供全方位的防护。支持多种软件的嵌入式杀毒工具，为经常上网的用户提供方便。

4.1.4 创新的网络黑名单列表

能够识别出网络上的病毒感染来源，并通过网络黑名单功能阻止病毒攻击。特别对于企业局域网用户提供了防止病毒通过网络传播感染的最佳方法。

4.1.5 注册表监控管理列表

当有程序试图修改注册表项，注册表监控会自动进行拦截，并提示用户是否同意修改。通过注册表监控管理列表，用户可了解修改注册表项的进程名称、注册表项及其处理结果，方便用户了解和管理哪些程序对注册表造成了影响。

4.1.6 垃圾邮件过滤

针对日趋泛滥的垃圾邮件，瑞星杀毒软件 2005 版新增了垃圾邮件过滤功能，它采用贝叶斯算法对邮件进行判断，若发现垃圾邮件，瑞星垃圾邮件过滤程序会在邮件的主题中标注该邮件是垃圾邮件，无需用户打开浏览邮件，节约用户的时间和精力。

4.1.7 三重病毒分析过滤技术

瑞星杀毒软件在秉承传统的特征值扫描技术的基础上，又增加了瑞星独有的行为模式分析

(BMAT) 和脚本判定 (SVM) 两项查杀病毒技术。检测内容经过三重检测和分析, 既能通过特征值查出已知病毒, 又可以通过程序分析出未知的病毒。三个杀毒引擎相互配合, 从根本上保证了系统的安全。

4.1.8 多引擎杀毒技术

瑞星杀毒软件采用国际领先的 VST II 病毒扫描引擎技术, 该技术是一项多引擎技术, 可快速、全面地查杀 DOS、Windows 3.x/9x/Me/NT/2000/XP/2003 等操作系统平台上的病毒。在公安部举行的杀毒软件评测中, 瑞星杀毒软件名列第一, 在很大程度上归功于此技术。

4.1.9 屏幕保护程序杀毒, 充分利用计算机的空闲时间

通过屏保杀毒功能, 计算机会在运行屏幕保护程序的同时, 启动瑞星杀毒软件进行后台杀毒, 充分利用计算机空闲时间。

4.1.10 内嵌信息中心, 及时为您提供最新的安全信息和病毒预警提示

在 Internet 连接状态下, 程序的主界面会自动获取瑞星网站公布的最新信息。诸如重大病毒疫情预警、最新安全漏洞和安全资讯等信息, 用户能及时做好相应的预防措施。

4.1.11 瑞星注册表修复工具, 安全修复系统故障

瑞星最新提供的注册表修复工具, 可以帮助您快速修复被病毒、恶意网页篡改的注册表内容, 排除故障, 保障系统安全稳定。

4.1.12 光盘启动系统, 直接查杀病毒

使用瑞星杀毒软件的光盘即可引导系统, 直接查杀病毒, 并能够自动寻找和使用硬盘中的最新版本进行病毒查杀。

4.1.13 支持多种压缩格式

瑞星杀毒软件支持 DOS、Windows、UNIX 等系统的几十种压缩格式, 如 ZIP, GZIP, ARJ, CAB, RAR, ZOO, ARC 等, 使得病毒无处藏身, 并且支持多重压缩以及对 ZIP、RAR、ARJ、ARC、LZH 等多种压缩包内文件的杀毒。

4.1.14 Windows 共享文件杀毒

瑞星杀毒软件成功地解决了正在运行的程序不能被修改的共享冲突难题, 在染毒程序运行的情况下, 也可以清除程序文件中的病毒。

4.1.15 实现在 DOS 环境下查杀 NTFS 分区

瑞星公司以领先的技术, 突破了 NTFS 文件格式的读写难题, 解决了在 DOS 下对 NTFS 格式分区文件进行识别、查杀的问题。瑞星杀毒软件可以彻底、安全地查杀 NTFS 格式分区下的病毒, 免

除了因 NTFS 文件系统感染病毒带来的困扰。

4.1.16 瑞星系统漏洞扫描

当前用户系统上存在大量安全漏洞和不安全设置，这种情况给系统造成了大量的不安全隐患，用户可以利用瑞星系统漏洞扫描工具检查系统当前存在的漏洞和不安全设置，并及时修复这些情况。

4.1.17 瑞星安全助手

瑞星安全助手可以在 Office 2000（及其以上版本）的文档在打开之前对该文件进行查毒，将宏病毒封杀在宏启动之前。同时，瑞星安全助手还可以对 IE 5（及其以上版本）下载的控制件在本地运行之前先行查毒，杜绝恶意代码通过 IE 下载的控制件进行传播。

4.1.18 瑞星短信通

瑞星短信通是一个即时短信工具，用户可以通过瑞星短信通方便的进行短信的发送，使发送短信变得快捷方便。

4.1.19 可疑文件上报

如果用户觉得某个文件比较可疑，可将此文件上报给瑞星公司，我们将竭诚为您检查分析可疑文件。

4.1.20 个性化界面风格，全面提高易用性

采用最新流行的 Windows XP 界面，可随时更换不同的风格和语言，充分体现瑞星软件的个性化与易用性。

4.1.21 自动语言配置

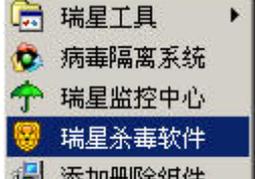
根据用户系统采用的默认语言，瑞星杀毒软件能自动进行语言配置，以显示相应语言的界面。同时还实现了实时转换界面语言的功能，在菜单中进行语言选择后，无须下次启动主程序即可立即显示相应语言的界面了。

4.1.22 针对 Intel Pentium 处理器进行全面优化，大幅提升查杀毒及实时监控效率。

4.2 客户端本地杀毒软件的启动

通过以下几种方式，您可以快速启动瑞星杀毒软件主程序：



双击 Windows 任务栏中的瑞星计算机监控图标;	
单击 Windows 快速启动栏中的瑞星杀毒软件图标;	
用鼠标左键点击瑞星计算机监控图标, 在弹出菜单中选择【启动瑞星杀毒】;	
用鼠标左键点击瑞星助手小狮子图标, 在弹出菜单中选择【启动瑞星程序】;	
选择【开始】/【程序】/【瑞星杀毒软件】/【瑞星杀毒软件】。	

4.3 客户端本地杀毒软件主程序界面及菜单说明

4.3.1 主程序界面说明

瑞星主程序界面是您使用的主要操作界面，此界面为您提供了瑞星杀毒软件所有的控制选项。通过简单、易操作和友好的操作界面，您无需掌握丰富的专业知识即可轻松的使用瑞星杀毒软件（如图 21）。



图 21

菜单栏：用于进行菜单操作的窗口，包括【操作】、【视图】、【设置】和【帮助】四个菜单选项。

查杀目录栏：用于选择查杀目标，具体的文件夹、磁盘、内存、引导区、邮件。

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、病毒名称和状态显示在此窗口中。在每个文件名称前面有图标标明病毒类型，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 Ie 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		

新功能：在病毒列表中，用鼠标右键点击某项，选择【病毒详细信息】，可连接至瑞星网站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。

查毒状态栏：在此状态栏中显示了当前查杀的文件名、已查杀文件数和病毒数以及相应的处理进度，通过进度条的显示，用户可以一目了然地掌握查杀毒的进展情况。

瑞星工具栏：为方便使用，用户可在查杀目录和瑞星工具两个界面间来回切换。点击瑞星工具，随即切换到瑞星工具界面，此界面包含的瑞星工具有：瑞星助手、嵌入式杀毒工具、瑞星 DOS 杀毒工具、硬盘备份、计算机监控、注册表修复工具、漏洞扫描、瑞星短信通和病毒隔离系统等（如图 22）。



图 22

4.3.2 【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【杀毒】、【停止】和【退出】操作外，还可以通过此菜单中的【历史记录】查看并导出以往查杀毒的记录（如图 23）。



图 23

4.3.3 【视图】菜单说明

用户可在主界面中选择显示查杀目录和工具列表两种界面（如图 24）。



图 24

4.3.4 【设置】菜单说明

【设置】菜单包含各种功能设置选项（如图 25）。第一次启动瑞星杀毒软件时程序的功能设置是默认的。当然，您也可以在【详细设置】菜单中根据自身需要进行相应的设置（详见设置介绍）。选择【密码】，用户可以设置和修改密码，以防其他用户未经许可修改设置和关闭瑞星计算机监控。



图 25

为满足不同用户的喜好，用户可以通过【外观选择】选择不同风格的界面。除界面选择之外，用户还可以选择不同的语言，目前瑞星杀毒软件提供简体中文、繁体中文、英文和日文四种语言。

如果用户觉得某个文件比较可疑，点击【上报可疑文件】项可将此文件上报给瑞星公司，我们将为您检查分析可疑文件。

4.3.5 【帮助】菜单说明

瑞星杀毒软件提供了细致周到的帮助功能（如图 26）。通过【帮助】菜单，可以打开【帮助】快速入门或解决在使用过程中遇到的疑难问题；选择【瑞星主页】登录瑞星公司主页；选择【瑞星社区】进入瑞星虚拟社区；还可以选择【关于瑞星...】查看瑞星公司的相关信息。



图 26

4.4 用瑞星杀毒软件杀毒

4.4.1 在默认状态下快速查杀病毒

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须改动其他任何设置即可进行病毒查杀。

第一步：启动瑞星杀毒软件；

第二步：在【查杀目录】栏中显示了待查杀病毒的目标，默认状态下，所有硬盘驱动器、内存、引导区和邮件都为选中状态（如图 27）；



图 27

第三步：单击瑞星杀毒软件主程序界面上的【查杀病毒】按钮，即开始扫描所选目标，发现病毒时程序会提示用户如何处理。扫描过程中可随时选择【暂停杀毒】按钮暂停当前操作，按【继续杀毒】可继续当前操作，也可以选择【停止杀毒】按钮停止当前操作。对扫描中发现的病毒，病毒文件的文件名、所在文件夹、病毒名称和状态都将显示在病毒列表窗口中。

注意：在清除病毒过程中，若出现【删除失败】提示时，即表示该文件可能正在被使用。您可以使用瑞星 DOS 杀毒工具制作软盘或 USB 盘启动计算机（具体操作请参阅 4.11 小节 制作瑞星 DOS 杀毒工具盘），用瑞星 DOS 杀毒工具清除该病毒（具体操作请参阅 4.17 小节 瑞星 DOS 杀毒工具使用指南）。

4.4.2 快速启用右键查杀

当您遇到外来陌生文件时，为避免外来病毒的入侵，您可以快速启用右键查杀功能，方法是：用鼠标右键点击该文件，在弹出的右键菜单中选择【瑞星杀毒】（如图 28），即可启动瑞星杀毒软件专门对此文件进行查杀毒操作。



图 28

4.4.3 根据设定的安全防护级别进行查杀

瑞星杀毒软件为用户设定了高、中、低三个安全防护级别，用户可以根据自己的实际情况设定不同的级别。此外，为了让用户更方便、灵活地使用计算机资源，用户还可以自定义三套安全防护级别。高、中、低三个级别是软件预先设置好的，其中各项设置用户不可更改，只有在用户自定义的状态下才可以对各项设置进行修改。用户保存好安全防护级别后，以后程序在扫描时即根据此级别的相应参数进行扫描病毒了（如图 29）。



图 29

4.4.4 按文件类型进行查杀

在默认设置下，瑞星杀毒软件是对所有文件进行查杀病毒的。为节约时间，您可以有针对性地指定文件类型进行查杀病毒，步骤是：在瑞星杀毒软件主程序界面中，选择【设置】/【详细设置】/【手动扫描】，在【查杀文件类型选项】中指定文件类型，按【确定】，即可对指定文件类型的文件进行查杀病毒了（如图 30）：



图 30

查杀文件类型选项:

所有文件: 选择后将扫描任何格式的文件, 此时扫描范围最全面, 但扫描时间花费最多;

仅程序文件: 只扫描程序文件, 如 EXE、COM、SYS、VXD、DRV、DLL、BIN、OVL、386、SRC、HTM、HTML、FON、VBS、VBE、DOC、DOT、XLS、XLT、PPT、BAT、ASP、HTT、HTA、JS、JSE、CSS、WSH、SCT、OCX、CPL、LNK 等文件, 此时扫描具有一定针对性, 可节约部分扫描时间;

自定义扩展名: 选择后可在提供的输入栏中输入文件扩展名, 瑞星杀毒软件即可对在文件名称中以此类文件扩展名结尾的文件进行杀毒; 或在下拉菜单中选择以某类文件扩展名结尾的文件进行杀毒。按扩展名扫描同样具有一定针对性, 可节约部分扫描时间。

快捷扫描: 用鼠标右键点击查杀目标, 在弹出菜单中选择【瑞星杀毒】, 或者用鼠标将查杀目标拖放到桌面上的【瑞星杀毒软件】快捷方式图标上, 或者拖放到瑞星杀毒软件主程序窗口中, 即可调用瑞星杀毒软件对此目标进行专门查杀病毒。用户同样可以指定文件类型进行查杀。

4.4.5 定制任务

4.4.5.1 定时扫描

在瑞星杀毒软件主程序界面中, 选择【设置】/【详细设置】/【定时扫描】选项卡 (如图 31);



图 31

在【扫描频率】中，您可以根据需要选择【不扫描】、【每天一次】、【每周一次】、【每月一次】等不同的扫描频率。在【扫描内容设定】中，可指定需要定时扫描的磁盘或文件夹，并可选择查毒还是杀毒以及要扫描的文件类型。当系统时钟到达所设定的时间，瑞星杀毒软件会自动运行，开始扫描预先指定的磁盘或文件夹。瑞星杀毒界面会自动弹出显示，用户可以随时查阅查毒的情况。在【高级设置】中，您可以设置【定时扫描高级设置】。

定时杀毒为用户提供了自动化的、个性化的杀毒方式。例如，对上班族而言，可利用午餐时间对系统进行自动杀毒。可以这样设置：在瑞星杀毒软件主程序界面中，选择【设置】/【详细设置】/【定时扫描】，将【扫描频率】设为【每天一次】，将【扫描时刻】设为 12:00，再按【确定】保存设置。以后每天 12:00 时，瑞星杀毒软件即可自动查杀病毒了。另外一种方法就是在启动“屏保杀毒”功能，充分利用计算机的空闲时间。

4.4.5.2 开机扫描

在 Windows 系统启动后随即开始扫描病毒（如图 32）。



图 32

4.4.5.3 屏保扫描

在 Windows 进入屏幕保护程序时，随即开始调用瑞星杀毒软件扫描病毒，充分利用计算机的空闲时间（如图 33）。



图 33

4.5 瑞星监控中心

瑞星监控中心包括文件监控、内存监控、邮件监控、网页监控、引导区监控、注册表监控和漏洞攻击监控。拥有这些功能，瑞星杀毒软件能在您打开陌生文件、收发电子邮件和浏览网页时，查

杀和截获病毒，全面保护您的计算机不受病毒侵害。

4.5.1 启动瑞星监控中心

方法一：在 Windows 窗口中，选择【开始】/【程序】/【瑞星杀毒软件】/【瑞星监控中心】，即可启动瑞星监控中心程序（如图 34）：

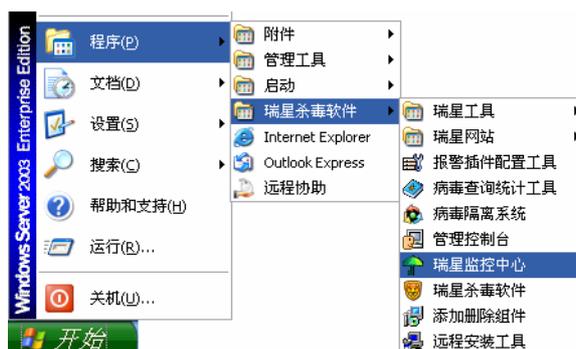


图 34

启动瑞星监控中心后，随即在系统托盘区（位于桌面任务栏右侧显示时钟的区域）出现小雨伞标志（）。“绿色打开”代表所有监控均处于有效状态，“黄色打开”代表部分监控处于有效状态，“红色收起”代表所有监控均处于关闭状态。

方法二：在瑞星杀毒软件主程序界面中，选择【设置】/【详细设置】/【计算机监控】，在【启动计算机时自动启动计算机监控】选项前打勾（如图 35），按【确定】按钮保存设置，即可在以后开机时同时启动瑞星计算机监控中心了。



图 35

4.5.2 退出瑞星监控中心

在系统托盘区中，用鼠标右键点击【瑞星计算机监控】程序图标（形状如绿色小雨伞），在弹出的右键菜单中选择【退出】，即可退出瑞星监控中心程序（如图 36）。



图 36

4.5.3 文件监控

文件监控用于实时的监控系统文件操作，在操作系统对文件操作之前对文件查杀毒，从而阻止病毒运行，保护系统安全。

4.5.3.1 启动文件监控

方法一：在系统托盘区中，用鼠标右键点击【瑞星计算机监控】程序图标（形状如绿色小雨伞），在弹出的右键菜单中选择【监控控制中心】/【文件监控】/【开启监控】，即可启动文件监控。

方法二：在瑞星杀毒软件主程序界面中，选择【设置】/【详细设置】/【计算机监控】，在【使用文件监控】选项前打勾，再按【确定】按钮保存设置，即可在监控中心启动时打开文件监控功能了。

4.5.3.2 文件监控设置说明

在瑞星杀毒软件主程序界面中，选择【设置】/【详细设置】，弹出【瑞星设置】窗口，再选择【计算机监控】选项卡。

如前所述，【使用文件监控】用于用户设置在监控中心启动时是否启动文件监控功能。用户还可以通过【计算机监控】/【文件监控】/【提示对话框关闭时间】来设置文件监控在工作中发现病毒时自动关闭询问对话框的时间长短。

强烈建议：请在【启动计算机时自动启动计算机监控】、【使用文件监控】、【使用内存监控】、【使用邮件监控】、【使用引导区监控】、【使用网页监控】、【使用注册表监控】和【使用漏洞攻击监控】选项前打勾，这样瑞星计算机监控就始终处于开启状态，一旦发现病毒就会及时报警。

4.5.3.3 文件监控在工作中的提示

文件监控在工作中发现病毒时的提示（如图 37）：您可以选择【杀毒】、【忽略】和【删除】。如果您不选择，文件监控会在一定时间后自动清除该病毒。



图 37

4.5.3.4 禁止文件监控

在系统托盘区中（位于 Windows 窗口任务栏中显示时钟的区域），用鼠标右键点击的【瑞星计算机监控】图标（绿色小雨伞标志），选择【监控控制中心】，点选【文件监控】/【关闭监控】，此时瑞星文件监控被关闭，计算机监控中心仍然运行，您可以选择【开启监控】来启动文件监控功能。

4.5.4 内存监控

内存监控用于监控关键的操作系统调用，并判定是不是病毒活动并且阻止病毒活动。内存监控对于通过系统漏洞传播的病毒效果良好。

4.5.4.1 启动内存监控

方法一：在系统托盘区中，用鼠标右键点击【瑞星计算机监控】程序图标（形状如绿色小雨伞），在弹出的右键菜单中选择【监控控制中心】/【内存监控】/【开启监控】，即可启动内存监控。

方法二：在瑞星杀毒软件主程序界面中，选择【设置】/【详细设置】/【计算机监控】，在【使用内存监控】选项前打勾，再按【确定】按钮保存设置，即在监控中心启动时启动内存监控功能了。

4.5.4.2 内存监控设置说明

在瑞星杀毒软件主程序界面中，选择【设置】/【详细设置】，弹出【瑞星设置】窗口，再选择【计算机监控】标签。在【计算机监控】选项卡中，【使用内存监控】用于用户设置监控中心启动时是否启动内存监控功能。

4.5.4.3 内存监控在工作中的提示

内存监控在工作中发现病毒时的提示（如图 38）：包括内存病毒的详细信息，如病毒所在路径，病毒进程 ID，病毒名称和处理结果等信息。



图 38

4.5.4.4 禁止内存监控

在系统托盘区中（位于 Windows 窗口任务栏中显示时钟的区域），用鼠标右键点击的【瑞星计算机监控】图标（绿色小雨伞标志），选择【监控控制中心】/【内存监控】/【关闭监控】。

4.5.5 邮件监控

邮件监控分为邮件接收监控和邮件发送监控。

邮件接收监控在用户接收邮件的时候，对邮件进行查杀毒。邮件接收监控不需要对用户的邮件程序做出任何修改。目前邮件接收监控只支持 POP3 协议，不能监控 IMAP，MAPI 和通过 WEB 接收的邮件。

邮件发送监控有两个功能：

- 1、支持所有使用 SMTP 协议的邮件客户端。
- 2、对于发送的邮件进行病毒扫描，若发现邮件带毒则按照【邮件监控】/【高级设置】/【发现病毒时】设置的处理方式进行处理，防止病毒扩散。

邮件发送监控目前只支持 SMTP 协议，不支持 MAPI 和通过 Web 发送的邮件。

4.5.5.1 启动邮件监控

方法一：在系统托盘区中，用鼠标右键点击【瑞星计算机监控】程序图标，选择【监控控制中心】/【邮件发送监控】/【开启监控】，或者【邮件接收监控】/【开启监控】，即可启动邮件监控；

方法二：在瑞星杀毒软件主程序界面中，选择【设置】/【详细设置】/【计算机监控】，在【使用邮件监控】选项前打勾，即可在监控中心启动时启动邮件监控。

4.5.5.2 邮件监控设置说明

在瑞星杀毒软件主程序界面中，选择【设置】/【详细设置】/【计算机监控】/【邮件监控】，即可设置【邮件监控选项】。

监控中心启动时打开邮件监控：每次运行瑞星计算机监控时，自动启动邮件监控程序。

使用 POP3 监控：选中此项，可在接收邮件时监控邮件是否带毒；

使用 SMTP 监控：选中此项，可在发送邮件时监控邮件是否带毒；

指定 POP3 端口：默认邮件端口是 110，某些时候这个端口会被其它程序占用（例如代理程序或者其它杀毒软件），您可以通过指定其它端口解决这个问题。

指定 SMTP 端口：默认邮件端口是 25，某些时候这个端口会被其它程序占用（例如代理程序或者其它杀毒软件），您可以通过指定其它端口解决这个问题。

提示对话框关闭时间：当邮件监控发现病毒或可疑文件，而用户在高级设置中选择的是“询问后处理”时，则会弹出对话框询问用户处理方式。如果用户未进行选择，对话框 15 秒后会自动关闭，邮件可以继续接收。

4.5.5.3 邮件监控在工作中的提示

(1) 发送邮件提示

当您选择发送邮件的时候，邮件监控会自动进行扫描工作，显示发送邮件进度（如图 39）。



图 39

(2) 接收邮件提示

当您选择接收邮件的时候，邮件监控会自动进行扫描工作，显示接收邮件进度。

(3) 发现病毒的提示

邮件监控如果在发送邮件时发现病毒，瑞星邮件监控将会拦截该邮件并将其存放到【发送失败的邮件列表】中，并告知用户无法发送此邮件的原因。发送和接收的邮件中如果发现病毒会弹出提示窗口（如图 40）。用户可以自己选择如何处理该邮件，或者在设定时间到达后按默认设置进行处理。



图 40

(4) 发现未知程序发送邮件的提示

当发现未知程序发送邮件时，瑞星邮件监控会立刻报告用户，让用户选择是同意该程序发送该邮件，还是拒绝该程序发送该邮件（如图 41）：

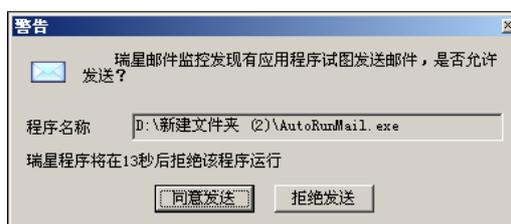


图 41

4.5.5.4 禁止邮件监控

方法一：用鼠标右键点击系统托盘区中的【瑞星计算机监控】程序图标，选择【监控控制中心】，再选择【邮件发送监控】或【邮件接收监控】后点击【关闭监控】，即可禁止邮件监控。

方法二：在瑞星杀毒软件主程序界面中，选择【设置】/【详细设置】/【计算机监控】，在【使用邮件监控】选项前取消打勾，按【确定】按钮保存设置，即可在监控中心启动时禁止邮件监控功能了。

4.5.5.5 垃圾邮件过滤

垃圾邮件（Spam）是指未经请求而发送的电子邮件，常见内容譬如成人广告、商业广告、推销信息、赚钱信息、电子杂志、连环信或者个人网站广告等。垃圾邮件的泛滥严重影响了网络的运行效率，浪费了收件人的时间和精力。2004 年 9 月初，据中国互联网协会发布的《第三次中国反垃圾邮件市场研究报告》显示，2003 年垃圾邮件致使国内生产总值损失高达 48 亿元人民币。

针对日趋泛滥的垃圾邮件，瑞星杀毒软件 2005 版新增了垃圾邮件过滤功能，它采用贝叶斯算法对邮件进行判断，若判断是非垃圾邮件，则正常接收邮件；若判断是垃圾邮件，则瑞星垃圾邮件过滤程序会在邮件的主题中标注该邮件是垃圾邮件，无需用户打开浏览邮件，节约用户的时间和精力。

启动或关闭垃圾邮件过滤的步骤是：在系统托盘区中，用鼠标右键点击【瑞星计算机监控】程序图标（形状如绿色小雨伞），在弹出的右键菜单中选择【监控设置】/【邮件监控】/【高级设置】，在【过滤垃圾邮件】复选框中打勾，即可启动垃圾邮件过滤功能；取消打勾，即可关闭垃圾邮件过滤功能。

4.5.6 网页监控

网页监控是通过脚本控件，在脚本执行之前先检查脚本是不是有威胁，若检查到具有威胁的脚本，网页监控会提示用户跳过执行脚本。

4.5.6.1 启动网页监控

方法一：在系统托盘区中，用鼠标右键点击【瑞星计算机监控】程序图标（形状如绿色小雨伞），在弹出的右键菜单中选择【监控控制中心】/【网页监控】/【开启监控】，即可启动网页监控。

方法二：在瑞星杀毒软件主程序界面中，选择【设置】/【详细设置】/【计算机监控】，在【使用网页监控】选项前打勾，再按【确定】按钮保存设置，即可在监控中心启动时打开网页监控功能了。

4.5.6.2 网页监控设置说明

在瑞星杀毒软件主程序界面中，选择【设置】/【详细设置】，弹出【瑞星设置】窗口，再选择【计算机监控】标签。在【计算机监控】选项卡中，【使用网页监控】用于用户设置是否启动网页监控功能。

4.5.6.3 网页监控在工作中的提示

在您浏览的网页中存在可疑的脚本时，脚本监控程序会给您一个详细的报告，其中包括哪个程序在启动哪一个网页、网页中包含哪些可疑的动作等。您可以根据这些信息决定是否要运行这个网页中的脚本。建议您使用默认的【跳过代码】选项，一般不会影响您浏览网页（如图 42）。



图 42

4.5.6.4 禁止网页监控

方法一：用鼠标右键点击系统托盘区中的【瑞星计算机监控】程序图标，选择【监控控制中心】，再选择【网页监控】/【关闭监控】，即可禁止网页监控；

方法二：在瑞星杀毒软件主程序界面中，选择【设置】/【详细设置】/【计算机监控】，在【使用网页监控】选项前取消打勾，按【确定】按钮保存设置，即可在监控中心启动时禁止网页监控功能了。

4.5.7 引导区监控

引导区监控是在用户访问软驱的时候，检查软盘是否感染了引导区病毒，防止引导区病毒通过感染软盘来传播破坏。

启动或关闭引导区监控

方法一：在系统托盘区中，用鼠标右键点击【瑞星计算机监控】程序图标（形状如绿色小雨伞），在弹出的右键菜单中选择【监控控制中心】/【引导区监控】，点击【开启监控】或【关闭监控】按钮，即可启动或关闭引导区监控。

方法二：在瑞星杀毒软件主程序界面中，选择【设置】/【详细设置】/【计算机监控】，在【使用引导区监控】选项前打勾（或不打勾），再按【确定】按钮保存设置，即可在监控中心启动时开启（或关闭）引导区监控功能。

引导区监控在工作中的提示

在开启引导区监控的情况下，当用户访问软盘时，若发现引导区感染病毒，则会弹出如下提示框（如图 43）：



图 43

注意：此功能在 Windows 9x 下禁用。

4.5.8 注册表监控

注册表监控对系统注册表的操作进行监控，对于特定的注册表项的操作报告并提示用户，防止恶意网页和恶意脚本对注册表的修改。

启动或关闭注册表监控

方法一：在系统托盘区中，用鼠标右键点击【瑞星计算机监控】程序图标（形状如绿色小雨伞），在弹出的右键菜单中选择【监控控制中心】/【注册表监控】，点击【开启监控】或【关闭监控】，即可启动或关闭注册表监控。

方法二：在瑞星杀毒软件主程序界面中，选择【设置】/【详细设置】/【计算机监控】，在【使用注册表监控】选项前打勾或不打勾，再按【确定】按钮保存设置，即可在监控中心启动时开启或关闭注册表监控功能了。

注册表监控在工作中的提示

在开启注册表监控的情况下，若有程序试图修改注册表项，则会弹出如下提示框：



图 44

4.5.9 漏洞攻击监控

漏洞攻击监控是为防止病毒利用系统漏洞进行攻击而提供的解决方案。在某些操作系统没有安装补丁程序的情况下，瑞星漏洞攻击监控可以轻易地化解病毒通过系统漏洞进行攻击的潜在危险。

在互联网日益普及的今天，越来越多的计算机连接到互联网，甚至某些计算机保持“始终在线”的连接，这样的连接使他们暴露在病毒感染、黑客入侵、拒绝服务攻击以及其他可能的风险面前。

当风险来临之际，面对攻击用户不必感到束手无策，此时瑞星漏洞攻击监控就会发挥它的强大威力，保护您的计算机不受到攻击，并向用户提示系统漏洞攻击的信息，在可能的情况下用户应该报告计算机管理员，这是“外治”。

对大多数公司而言，一个计算机管理员或者普通用户具有的良好习惯就是及时给操作系统打补丁程序，您可以使用 Windows Update 进行更新，也可以使用瑞星杀毒软件中的系统漏洞扫描工具进行扫描、下载和更新，这是“内补”。

有了“外治”加“内补”的解决之道，相信您不再受到系统崩溃、资料丢失或者机密信息泄漏的困扰。

启动或关闭漏洞攻击监控

在系统托盘区中，用鼠标右键点击【瑞星计算机监控】程序图标（形状如绿色小雨伞），在弹出的右键菜单中选择【监控控制中心】/【漏洞攻击监控】，点击【开启监控】或【关闭监控】，即可启动或关闭漏洞攻击监控。

漏洞攻击监控工作中的提示

漏洞攻击监控功能启用后，一旦发现系统正在受到攻击，则弹出提示框警告用户，并列出具体的监控信息，包括：漏洞所在路径、漏洞进程 ID、漏洞名称、源地址和目标地址等。若用户不采取操作，则程序在 15 秒后会采取默认处理，如图 45。



图 45

注意：此功能在 Windows 9x 下禁用。

4.6 嵌入式杀毒

4.6.1 使用 Lotus Notes 嵌入式杀毒

如果您安装了 Lotus Notes，您就可以使用瑞星杀毒软件来对 Lotus Notes 进行监控了。

4.6.1.1 启用 Lotus Notes 监控功能

启用 Lotus Notes 监控功能的方法是：在瑞星杀毒软件主程序界面中，选择【设置】/【详细设置】/【嵌入式杀毒】，在【使用 Lotus Notes 嵌入式杀毒】选项前打勾（如图 46）：



图 46

只要在【使用 Lotus Notes 嵌入式杀毒】选项前打勾，在运行 Lotus Notes 时也同时启用了 Lotus Notes 监控功能，该功能监控 Lotus Notes 邮件附件是否带有病毒。

在【Lotus Notes 监控】设置中，选中【发送邮件时扫描】和【接收邮件时扫描】，即可在 Lotus Notes 中在发送接收带有附件的邮件时进行病毒扫描了。在【查杀文件类型选项】中，您还可以对邮件附件指定文件类型进行监控。为尽可能地减小病毒的侵害、让病毒无藏身之地，请选中【所有文件】选项。

4.6.1.2 Lotus Notes 监控工作中的提示

发送邮件的提示：在发送邮件时，若附件带有病毒，则会弹出【瑞星 Lotus Notes 实时监控程序---发现病毒】的提示画面（如图 47）：



图 47

接收邮件的提示：在接收邮件时，若附件带有病毒，则会弹出【瑞星 Lotus Notes 实时监控程序---发现病毒】的提示画面。

发现病毒后，在提示画面中显示有【病毒信息】和供选择的【处理方法】，您可以在【清除病毒】、【删除带毒附件】和【忽略】三种处理方法中任选一种方法来处理病毒。

4.6.1.3 关闭 Lotus Notes 监控功能

在瑞星杀毒软件主程序界面中，选择【设置】/【详细设置】/【嵌入式杀毒】，取消选中【使用 Lotus Notes 嵌入式杀毒】，在以后运行 Lotus Notes 时就不会启用 Lotus Notes 监控功能了。

4.6.2 使用 Office/IE 嵌入式杀毒

每次当您打开 Office 文档时或者用 Internet Explorer 浏览网页时，瑞星嵌入式杀毒系统会自动保护您系统的安全。

注：瑞星 Office/IE 安全助手只有在您使用 Office 2000 及以上版本或者 IE 5 及以上版本时才起作用。

如果您安装了 Office 2000 或 IE 5.0 版本以上的浏览器，则在瑞星杀毒软件安装完毕后，瑞星 Office/IE 的安全助手就处于有效状态。

在瑞星 Office/IE 安全助手处于有效状态时，如果您启动了 Office 或 IE 会看到瑞星安全助手的启动 Logo 画面（如图 48）。



图 48

如果您启动的 Office 2000 文件中有病毒存在，安全助手会发出警告（如图 49）。



图 49

用户可以根据自己的需要选择相应的操作，如【直接清除】、【删除文件】和【忽略，继续扫描】等。如果清除病毒失败，安全助手会让用户选择清除失败后的处理方式。

如果您不想在启动 Office 和 IE 时启动瑞星 Office/IE 安全助手，则须进行以下设置：在瑞星杀毒软件主程序界面中，选择【设置】/【详细设置】/【嵌入式杀毒】，取消选中【使用 Office/IE 嵌入式杀毒】。

4.7 使用黑名单列表

病毒的传播方式多种多样，如软盘光盘传输、电子邮件、网页浏览和硬盘共享等，其中硬盘共享最有威胁，一旦病毒（如 Nimda，尼姆达病毒）入侵局域网中的某一台电脑，便尝试向局域网中的其它电脑传播，并为其所有盘符创建网络共享，从而越传越多，造成网络通信阻塞、计算机系统资源耗尽等严重后果。

针对泛滥成灾的网络病毒，瑞星杀毒软件 2005 版提供了更全面、更高效的反病毒解决方案——黑名单列表。此功能属于瑞星实时监控系统的功能模块，它一旦发现其它计算机正在通过网络向本机释放病毒，便截获此病毒，并将发送病毒的计算机名称和 IP 地址记录到黑名单中，阻止其通过网络共享访问本机。

注意：一旦计算机被加入到黑名单之后，这台计算机就不能访问本机的共享文件夹了，只有从

黑名单中删除之后，这台计算机才能够继续访问本机的共享文件夹。

打开黑名单列表的步骤是：在系统托盘（在 Windows 任务栏中显示系统时钟的区域）中，用鼠标右键点击“瑞星计算机监控”图标（形状如小雨伞），在右键菜单中选择“网络黑名单”，即可打开黑名单列表（如图 50）。



图 50

4.8 使用嵌入式杀毒工具

随着网络的日益普及，越来越多的用户通过网络进行实时通讯和下载文件，而这也越来越成为病毒传播的主要途径之一。为此，瑞星杀毒软件专门提供了嵌入式杀毒工具。

瑞星杀毒软件嵌入式杀毒工具是在用户使用实时通讯软件（如 MSN Messenger）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查杀病毒，防止病毒通过外来文件传播到本地。

瑞星杀毒软件嵌入式杀毒工具目前支持的软件有：

- 1、MSN Messenger
- 2、Yahoo! Messenger
- 3、AOL Messenger
- 4、FlashGet
- 5、NetAnts
- 6、NetVampire
- 7、WinZip

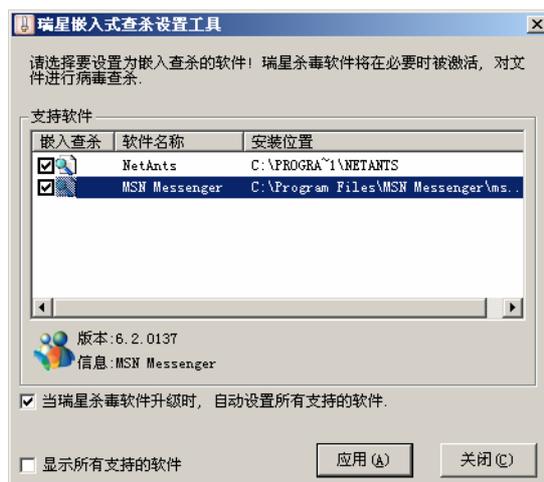


图 51

4.9 病毒隔离系统

4.9.1 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【瑞星工具】/【病毒隔离系统】。

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】（如图 52）。

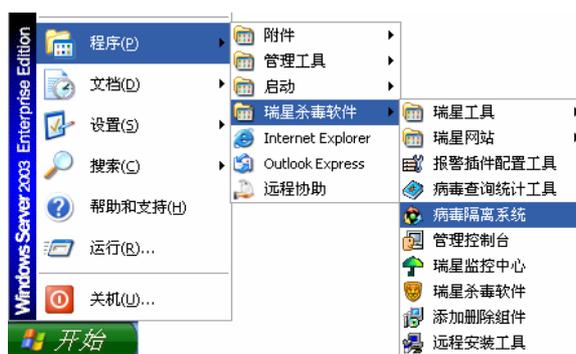


图 52

如果您选择备份染毒文件到病毒隔离系统的方式，方法是：在瑞星杀毒软件主程序界面中，选择【设置】/【详细设置】/【手动扫描】，在【将染毒文件备份到病毒隔离系统】复选框中打勾，则病毒隔离系统将保存染毒文件的备份，当然您也可以恢复备份。

4.9.2 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，病毒隔离系统还可以设置隔离区存储空间。您可以选择文件替换策略，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【替换最老的文件】，再按【确定】保存设置（如图 53）。



图 53

4.10 硬盘数据备份与恢复

如果硬盘数据被破坏或者硬盘被格式化，在大多数情况下，您都可以通过硬盘恢复工具将丢失的硬盘数据恢复回来。此时，硬盘数据备份就显得必不可少。您可以手动备份或定时备份硬盘数据。

4.10.1 手动备份

方法一：在瑞星杀毒软件主程序界面中，选择【瑞星工具】/【硬盘备份】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】/【瑞星硬盘备份】，选择【开始备份】按钮（如图 54）。

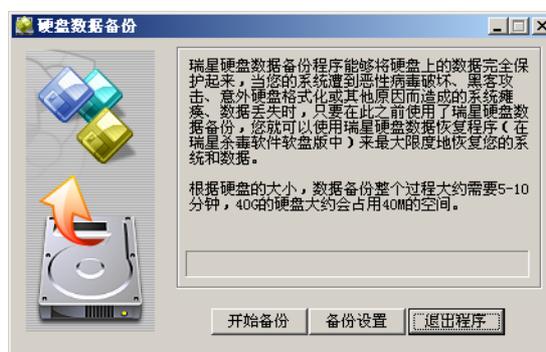


图 54

4.10.2 硬盘数据恢复

用瑞星 DOS 杀毒工具软盘启动，进入 DOS 查杀病毒程序。选择【实用工具】，再选择【硬盘数据恢复】，即可对您最近一次的硬盘数据备份进行恢复了（具体操作请参阅 3.3）。

警告：此过程可能需要较长时间，如果您的硬盘数据没有被破坏，请不要使用此工具。

4.11 制作瑞星 DOS 杀毒工具盘

瑞星杀毒软件提供制作 DOS 杀毒工具软盘和 USB 盘的功能。通过该功能，用户可以自行制作与当前计算机中安装的瑞星杀毒软件版本相一致的 DOS 杀毒工具，它既能启动系统，又能进行杀毒操作、恢复硬盘数据和提取引导区信息等（具体使用请参阅 4.18 小节 瑞星 DOS 杀毒工具使用指南）。

4.11.1 制作启动软盘

制作瑞星 DOS 杀毒工具软盘的两种方法：

方法一：在瑞星杀毒软件主程序界面中，选择【瑞星工具】/【瑞星 DOS 杀毒工具】，弹出【瑞星 DOS 启动盘制作工具】对话框，选择【制作启动软盘】选项；

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 DOS 杀毒工具】，弹出【瑞星 DOS 启动盘制作工具】对话框，选择【制作启动软盘】选项（如图 55）。



图 55

提示：制作瑞星 DOS 杀毒工具软盘版需要多张空白软盘，依照制作顺序，建议将制作好的软盘按 A、B、C... 进行编号，以便后续的使用。

4.11.2 制作 USB 启动盘

随着 USB 盘使用的普及,越来越多的用户希望通过 USB 盘启动系统查杀病毒,瑞星杀毒软件 2005 版让这部分用户的希望成为了现实。

将启动型 USB 盘接入计算机 USB 端口,并能让操作系统正常识别此设备。启动瑞星杀毒软件主程序,在【瑞星工具】界面中,选择【瑞星 DOS 杀毒工具】,弹出【瑞星 DOS 启动盘制作工具】对话框,选择【制作 USB 启动盘】选项,按【下一步】继续(如图 56);再指定 USB 盘(如图 57)。



图 56



图 57

提示:请在计算机 BIOS 设置中,先将计算机的第一启动设备设为 USB-ZIP (若是 USB 闪存盘,请选择 USB-ZIP 方式;若是 USB 移动硬盘,请选择 USB-HDD 方式。具体方法详见计算机的相关使用说明),才能使用 USB 盘启动系统查杀病毒。

4.12 设置密码

在瑞星杀毒软件主程序界面中,选择【设置】/【密码】,进入【设置密码】对话框(如图 58);

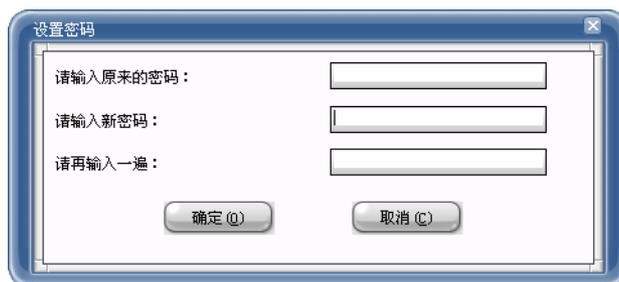


图 58

设置密码的目的在于防止未经许可的情况下，擅自关闭瑞星计算机监控程序或者修改【详细设置】，这在单机多用户的情况下尤其有用。密码设置完成后，每次退出瑞星计算机监控程序或修改【详细设置】时均要求输入密码。若输入密码不正确，则不能关闭瑞星计算机监控程序或修改【详细设置】。

4.13 瑞星漏洞扫描工具

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和安全设置缺陷自动修补的工具。

4.13.1 启动瑞星漏洞扫描工具

启动瑞星漏洞扫描工具可以从【开始】/【程序】/【瑞星杀毒软件】/【瑞星工具】/【瑞星漏洞扫描】，选择漏洞扫描工具后，出现【瑞星系统安全漏洞扫描】对话框，如图 59。

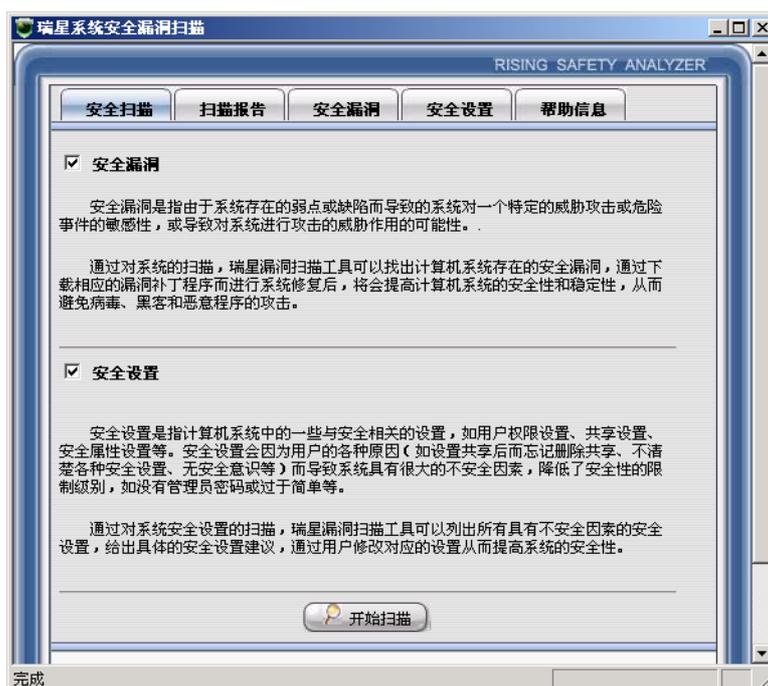


图 59

4.13.2 漏洞扫描的使用

选择『安全漏洞』和『安全设置』选项，点击【开始扫描】进行系统漏洞扫描。

4.13.3 阅读扫描报告

如图 60，该扫描结果页显示了被扫描计算机名称、扫描时间、发现的安全漏洞数量、发现的安全设置数量、已修复安全漏洞数量、可自动修复的不安全设置的数量等信息。



图 60

4.13.4 查看安全漏洞信息

选择【查看安全漏洞】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（如图 61）。

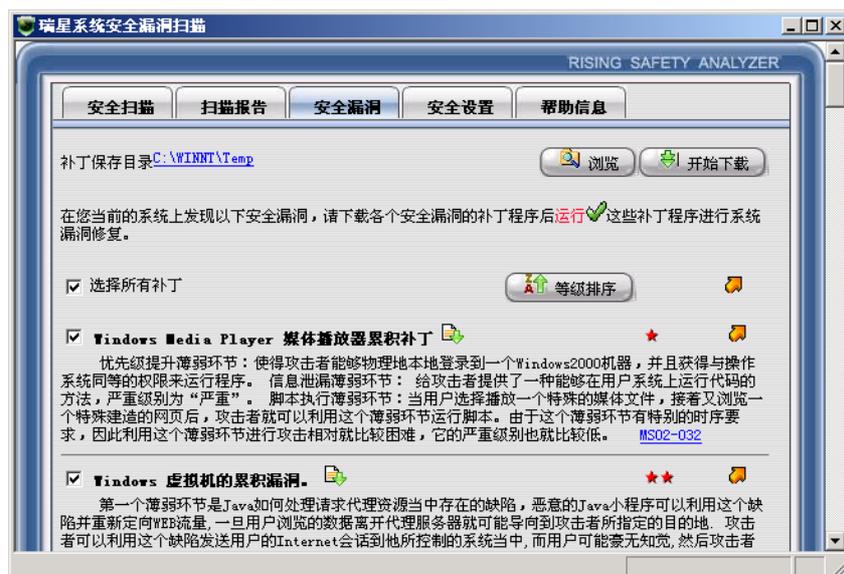


图 61

4.13.5 查看安全设置信息

选择【查看安全设置】选项，可以查看详细的安全设置信息，也可以直接进入【安全设置】页进行查看，如图（图 62）。

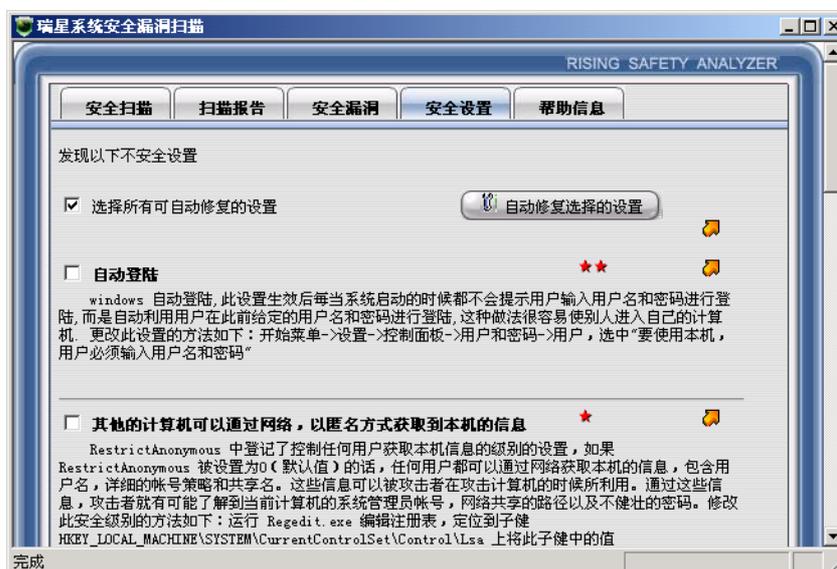


图 62

4.13.6 获取系统漏洞的补丁包

在对系统进行扫描完成后，进入【安全漏洞】页，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，*****表示此漏洞对您的系统造成的危害最高，****表示此漏洞的危害性为次之。对于每个漏洞信息，可以左键点击每条漏洞信息前的键，漏洞扫描可以自动下载相关补丁文件。

4.13.7 进行漏洞的更新

当漏洞信息的相关补丁文件下载到本地后，可以直接运行补丁文件，进行系统文件的更新。在更新的过程中更新程序可能要求系统重新启动计算机，这些步骤都是微软根据补丁程序的需要进行的必要操作！

4.13.8 “安全设置”漏洞的修补

对于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，而对于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，系统管理员的密码为空等。这些情况需要用户手动更改解决。

4.13.9 扫描结果进行导入和导出

当扫描完成后，进入【扫描报告】页。选择了【导出报告】按钮后，弹出报告导出路径（如图63）。

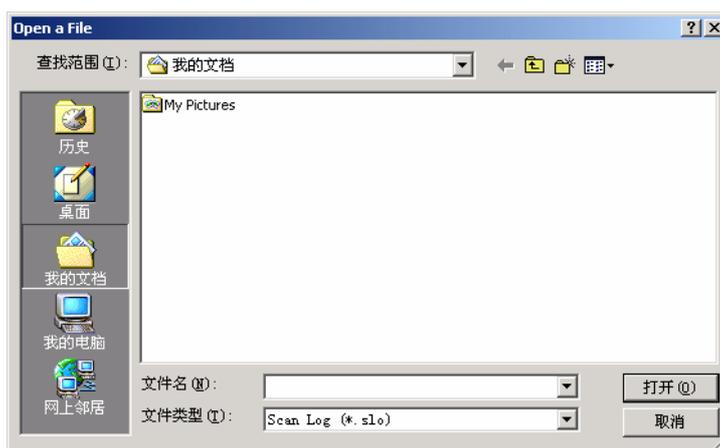


图 63

程序会自动命名导出文件，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，进入【扫描报告】，选择【扫描报告】中的【导入报告】按钮，弹出要导入文件的选择路径。

在选定了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，用户可以继续利用 4.14.4 叙述的内容进行查看。

4.13.10 特殊的系统漏洞处理

- ① 由于漏洞扫描是对系统不安全性进行警告和引导用户下载补丁的工具，补丁的修补过程完全是由微软提供的补丁包来完成的，所以如果出现补丁包在修补完成后造成系统某些设置的更改，请到微软网站进行了解和咨询；
- ② 在扫描结果中，会出现某些补丁无法下载的情况，这是由于此条漏洞的修补只能利用微软的 Windows Update 来完成，微软并没有单独对此漏洞提供公用的补丁包，此情况下，“瑞星漏洞扫描”会将此漏洞信息直接连接到微软的 Windows Update 来进行更新。

4.14 注册表修复工具

注册表修复是对于由病毒或某些恶意程序给系统注册表造成损坏，导致系统的某些重要功能被更改，而提供给用户的工具。专门检测、修复与系统运行息息相关的重要的注册表的内容。尤其是对于遭病毒侵害后的系统注册表，注册表修复工具提供了快捷的修复方式。

4.14.1 启动注册表修复工具

选择【开始】/【程序】/【瑞星杀毒软件】/【瑞星工具】/【注册表修复工具】，启动注册表修复工具（如图 64）。

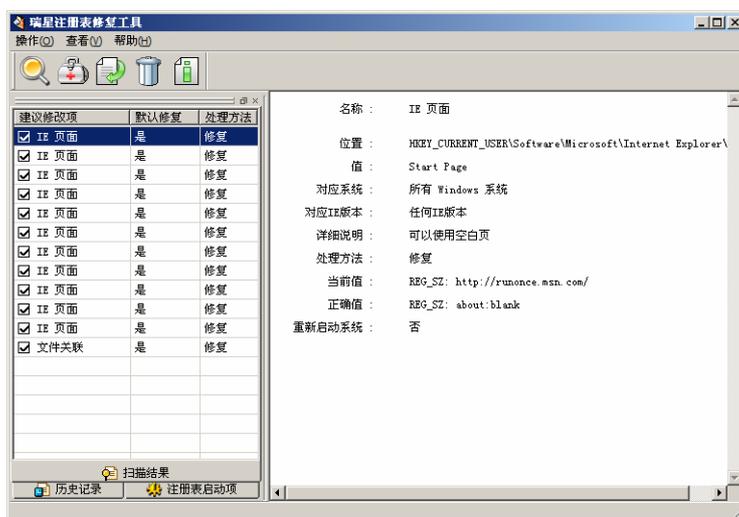


图 64

在启动注册表修复工具的同时，注册表修复工具会自动检测系统注册表的内容，如果您的注册表没有被修改，注册表修复工具将报出“未发现被修改的注册项”。

当如果出现被恶意更改的内容，则注册表修复工具将自动显示出被更改“建议修改项”、“默认修复”、“处理方法”。

4.14.2 使用注册表修复工具

- ① 当启动了注册表修复工具后，从菜单【操作】中选择【扫描】；
也可以选择工具栏中的键进行注册表扫描。当扫描结束后，在左侧“列表栏”中将显示出扫描结果。

高亮化“列表栏”中的扫描结果项，在右侧“扫描结果详细栏”中，将显示出详细的被更改注册表项的信息；

- ② 如何修复扫描出的出错注册表信息：当注册表修复工具扫描发现系统注册表存在异常后，选择菜单项的【操作】/【修复】项进行修复；

也可以从工具菜单选择进行注册表修复。如果存在多处需要更改的内容，请选定要修复的项，按上面介绍的进行修复，如果没有选定被修复项，则无法正常修复；

- ③ 历史记录恢复：由于某些注册表项的更改是由于用户主动更改的内容，但注册表修复工具无法判断出此项的更改是用户的个人设置还是病毒或恶意程序造成的更改。所以注册表修复工具对已经修复的设置，可以由用户自行将其重新设回修复前的状态，这样既保证了注册表的安全性，同时也给用户提供了灵活的设置方式。当修复完成后，会在注册表修复工具的“历史记录”栏中出现已修复的结果；

选择菜单中的【操作】/【恢复记录】项，则可以将高亮化的历史记录进行恢复。

也可以选择工具栏中的键进行对高亮化选定的历史记录信息进行恢复，恢复完成后继续选择扫描，修复过的注册表项将重新被扫出。

- ④ 删除记录：删除记录是指删除历史记录中的内容。用户可以删除选定的记录也可以删除所有的历史记录。通过菜单中的【操作】/【删除记录】来进行历史记录的删除。

也可以选择工具栏中的来执行删除历史记录的功能。

4.14.3 注册表修复工具的风格

注册表修复工具的列表栏是可移动风格，用户可以通过菜单【查看】/【工具栏】的选择来决定是否进行工具栏的启用。

4.14.4 注册表修复工具列表栏的使用

注册表工具栏共存在 3 个标签：**【扫描结果】**、**【历史记录】**和**【注册表启动项】**。

【扫描结果】标签是当注册表修复工具完成扫描后将结果进行显示，它包含『建议修改项』『默认修复』『处理方法』三项解释，每条扫描结果都会显示出这三种信息：

『建议修改项』是指被更改的注册表项会给系统造成某种影响，如无法关机，无法启动应用程序等；

『默认修复』是指此条扫描结果是否是用户自定义的默认键值。选择“是”注册表修复工具默认将不修补此条信息，如果选择“否”注册表修复工具将自动选择修复此条信息（如图 65）；

建议修改项	默认修复	处理方法
<input checked="" type="checkbox"/> IE 页面	是	修复
<input checked="" type="checkbox"/> IE 页面	是	修复
<input checked="" type="checkbox"/> IE 页面	否	修复
<input checked="" type="checkbox"/> IE 页面	否	修复
<input checked="" type="checkbox"/> IE 页面	是	修复
<input checked="" type="checkbox"/> IE 页面	是	修复
<input checked="" type="checkbox"/> IE 页面	是	修复
<input checked="" type="checkbox"/> IE 页面	是	修复
<input checked="" type="checkbox"/> IE 页面	是	修复
<input checked="" type="checkbox"/> IE 页面	是	修复
<input checked="" type="checkbox"/> IE 页面	是	修复
<input checked="" type="checkbox"/> 文件关联	是	修复

扫描结果

历史记录 注册表启动项

图 65

『处理方法』是指对于出现的注册表错误项，处理的方式有删除或修复：

- ① 删除：是指此注册表信息属于病毒或恶意程序写入的垃圾信息，这些信息会直接导致系统功能受损，对于这样的注册表信息，此工具采用删除的方法；
- ② 修复：是指由于用户设定或其他程序更改，造成系统某些键值被更改。对系统造成功能损坏这样的情况，注册表修复工具采用恢复系统默认值的办法来解决。

【历史记录】页记录修复信息的内容。对于被修复信息，会在历史记录页显示『修改项』和『修改时间』两种信息。

『修改项』是指此条注册表项会给系统造成的某种影响，如系统无法关机，禁止运行等。

『修改时间』是指此条注册表信息是什么时候被修复为正常值的。高亮化一条历史记录，在详细信息栏将显示出此条记录的详细内容。

【注册表启动项】注册表启动项是指对于在中曾经设置过的启动项，可以通过选择是否启动来重新设置启动项（如图 66）



图 66

当勾选了某个启动项目后，在相应的注册表位置将会出现此启动项的注册表值，当不选择启动项时，启动项在注册表中的相应键值将被删除。这样有利于用户判别在启动项中是否存在异常的启动项，并可以有选择的设置启动的内容。

4.15 瑞星短信通

4.15.1 启动瑞星短信通

选择【开始】/【程序】/【瑞星杀毒软件】/【瑞星工具】/【瑞星短信通】来启动短信通程序（如图 67）。



图 67

瑞星短信通启动后出现登录界面（如图 68）



图 68

注意：瑞星短信通的注册和发送、密码查询是联机在线进行的，您使用的过程中需要保持联网状态。

4.15.2 使用瑞星短信通

使用瑞星短信通需要输入您的手机号码和登录平台的密码，如果您是初次使用瑞星短信通，则需要您进行手机注册。

4.15.2.1 【手机注册】

- ① 首先运行瑞星短信通，在显示框内点击『注册向导』；
- ② 选择手机注册后，进入注册界面（如图 69）；

图 69

- ③ 在注册的第一步需要您仔细阅读相关的许可协议和相关条款，如果您继续注册而没有仔细阅读相关条款时，瑞星将认为您已经阅读并同意了各项条款内容，选择【短信服务条款】进行各项条款的阅读；
- ④ 在阅读完【短信服务条款】后，将您的有效手机号和真实联系邮箱，填入相应的位置，选择【确定】，大约 1 分钟左右，您将收到注册确认短信。



图 70

注意：输入手机号码提交后，会在 1 分钟左右（视电信网络状况，时间略有差异）收到确认短信。此时您就可以按照短信内容回复订阅信息，经确认后即可获得登陆密码的短信通知。保存好此密码，在以后的登录中将需要用到。

4.15.2.2 【登录瑞星短信通】

- ① 启动瑞星短信通，输入手机号和登录密码到相应栏位，点击【登录】；
- ② 当登录成功后会进入瑞星短信通主界面。



图 71

4.15.2.3 【发送短信】

登录成功后，在接收人一栏中填写接收短信方的手机号码，并填写短信内容。



图 72

在短信内容中输入想发送的文字（短信内容栏必须填写内容），然后点击『发送』就可以发送短信了。

4.15.2.4 【通讯录】

瑞星短信通提供通讯录功能，用户可在通讯录中添加、查询、修改和保存通讯录信息，方便用户发送短信。

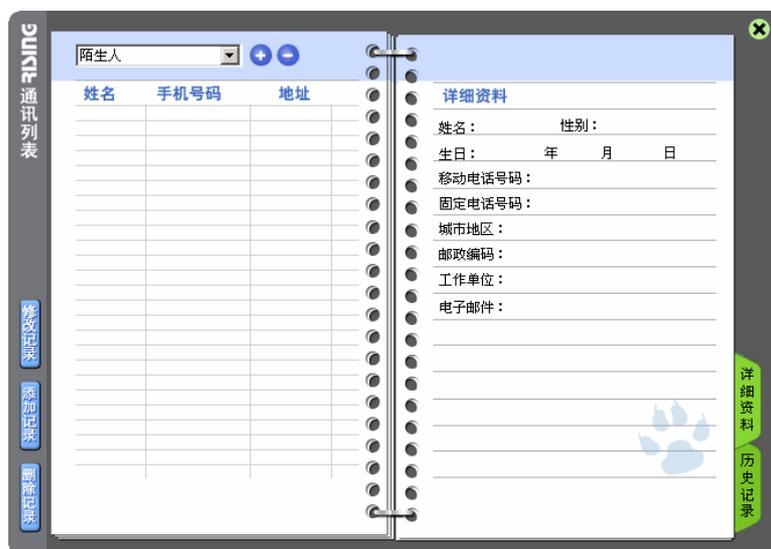


图 73

4.15.2.5 【短信传情】

瑞星短信通提供内容丰富的短信，用户可快速挑选到自己喜爱的短信内容，传递亲情友情等。



图 74

4.15.2.6 【密码查询】

如果您在注册后由于各种原因，忘记了密码，可以在瑞星短信通的登录状态下选择『忘记密码』

进行密码的查询。

在登录了密码查询界面后，填入要查询的手机号，点击【确定】，很快您的手机就可以收到密码。

4.16 添加删除、修复和卸载

为方便用户更灵活、更方便和更稳定地使用瑞星杀毒软件，瑞星杀毒软件 2005 版新增了添加删除、修复和卸载软件功能。

在 Windows 画面中，选择【开始】/【程序】/【瑞星杀毒软件】/【添加删除组件】，弹出【选择安装方式】窗口：



图 75

【添加/删除】：选中此项后，用户可根据自身需要，添加或删除瑞星杀毒软件的组件，便于用户更灵活、更有效地使用资源；

【修复】：选中此项后，程序会自动进行修复安装，检查并修复已安装的瑞星杀毒软件的完整性，便于用户更稳定地使用瑞星杀毒软件；

【卸载】：选中此项后，程序会自动卸载瑞星杀毒软件。

4.17 瑞星 DOS 杀毒工具使用指南

瑞星杀毒软件提供制作 DOS 杀毒工具软盘和 USB 盘的功能。您可以使用该功能自行制作和当前计算机中安装的瑞星杀毒软件版本一致的瑞星 DOS 杀毒工具，用于软盘或 USB 盘引导系统杀毒（带瑞星 DOS 杀毒工具的软盘和 USB 盘的具体制作方法，请阅读 4.11 小节 制作瑞星 DOS 杀毒工具盘）。

使用带瑞星 DOS 杀毒工具的软盘或 USB 盘启动系统后，即可在 DOS 状态下查杀病毒、恢复硬盘数据和提取引导区信息了。

4.17.1 启动瑞星 DOS 杀毒工具

4.17.1.1 用软盘启动

先将计算机启动顺序设为软盘启动（具体方法详见计算机的相关使用说明）。

- (1) 将事先做好的瑞星 A 号盘插入软盘驱动器；
- (2) 打开计算机电源或重新启动计算机，由软盘引导启动计算机；
- (3) 按照提示，取出 A 号盘，再依次插入 B 号、C 号盘；
- (4) 启动后自动进入瑞星杀毒软件 DOS 界面（如图 76）；



图 76

4.17.1.2 用瑞星光盘启动

先将计算机启动顺序设为光盘启动（具体方法详见计算机的相关使用说明）。

将瑞星光盘放入光驱，重新启动计算机，即可由瑞星光盘引导计算机到瑞星杀毒软件 DOS 状态下，接下来您就可以查杀病毒、恢复硬盘数据和提取硬盘引导区信息了。

注意：用瑞星光盘启动，只能引导计算机到光盘出厂时的版本。

4.17.1.3 用 USB 盘启动

请在计算机 BIOS 设置中，先将计算机的第一启动设备设为 USB-ZIP（若是 USB 闪存盘，请选择 USB-ZIP 方式；若是 USB 移动硬盘，请选择 USB-HDD 方式。具体方法详见计算机的相关使用说明）。

将事先制作好的瑞星 DOS 杀毒工具启动型 USB 盘接入计算机 USB 端口，重新启动计算机即可进入 DOS 进行查杀病毒（制作 USB 启动盘的方法详见 4.11.2 小节）。

4.17.2 用瑞星 DOS 杀毒工具杀毒

- (1) 进入瑞星 DOS 杀毒工具的杀毒界面；
- (2) 选择需要查毒的目录（默认状态下为扫描本机所有硬盘）；
- (3) 用鼠标点击【查毒】按钮，或按“TAB”键将光标移至【查毒】按钮再按“Enter”键，即可开始查毒；
- (4) 用鼠标点击【杀毒】按钮，或按“TAB”键将光标移至【杀毒】按钮再按“Enter”键，即可直接杀毒；
- (5) 在查杀病毒过程中，按【暂停】按钮可暂停查杀病毒，再次按【继续】按钮可继续查杀病毒，按【终止】按钮可终止查杀病毒；（如图 77）



图 77

- (6) 如果要对查杀病毒功能进行设置，则选择【功能设置】。您可用“上/下”方向键移动光标再按空格键或用鼠标点击每项前面的方框对选项进行选定/取消；（如图 78）



图 78

各个选项的说明如下：

仅查程序文件：选定后仅扫描程序文件，取消后将扫描所有文件。

查杀未知 Windows 病毒：选定后增加对未知 Windows 病毒的扫描（默认为选定）。

查压缩文件：选定后增加对压缩文件的扫描。

备份病毒有关文件：选定后在杀毒过程中会备份带毒文件，您可在瑞星杀毒软件中恢复备份文件。（默认为选定）

查引导区：选定后查引导区病毒。（默认为选定）

查杀未知 DOS 病毒：选定后查未知 DOS 病毒。

杀毒前询问用户：选定后在杀毒前将要求用户确认。（默认为选定）

- (7) 按【完成】按钮完成本次查杀病毒，在【查杀结果】中会显示本次查杀病毒的结果；
- (8) 按鼠标、“TAB”键或“上/下/左/右”方向键，选择其他驱动器或路径进行查杀病毒；
- (9) 按【退出】按钮退出瑞星杀毒软件【瑞星软盘版】程序。

4.17.3 用瑞星 DOS 杀毒工具恢复硬盘数据

如果您在 Windows 下做了硬盘备份工作（具体操作请参阅 4.10），则当硬盘数据被破坏时，您可用瑞星杀毒软件 DOS 杀毒工具恢复硬盘数据。此工具将为您查找此备份，并通过此备份修复您的硬盘数据（此过程可能需要比较长的时间）。在【实用工具】选项卡中，选择【硬盘数据恢复】（如图 79），随即弹出窗口询问用户是否继续，选择【是】即可开始恢复硬盘数据。（如图 80）



图 79



图 80

★ 警告：如果您的硬盘数据没有被破坏，请勿使用此工具。

4.17.4 用瑞星 DOS 杀毒工具提取硬盘引导区信息

如果您认为您的硬盘引导区有问题，或者怀疑有病毒感染，您可以通过此工具提取您的硬盘引导区信息，再将保存有硬盘引导区信息的软盘寄送到瑞星公司。瑞星公司将为您分析您的硬盘引导区是否被病毒感染。在【实用工具】选项卡中，选择【提取硬盘引导区信息】（如图 80），随即弹出窗口提示用户插入软盘，选择【确定】即可开始提取硬盘引导区信息到软盘中。（如图 81）

第五章 全网安全管理

5.1 瑞星管理控制台概述

瑞星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。通过瑞星管理控制台可以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、查杀毒和当前版本等状态。管理控制台能对远程计算机安装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。管理员通过管理控制台的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面坚实的网络病毒防护系统。

5.2 管理控制台的启动

启动已经安装瑞星管理控制台的机器，依次进入【开始】/【程序】/【瑞星杀毒软件】/【管理控制台】（如图 82），或者双击桌面【管理控制台】图标，进入登录界面。

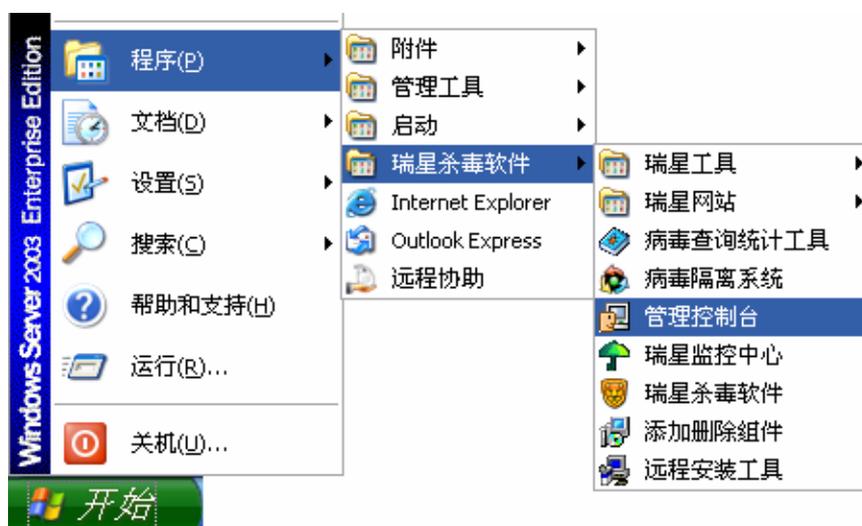


图 82

在【管理员登录】界面中（如图 83），输入帐号和口令后（初次登录帐号为 Admin、口令为空），按【确定】进入瑞星管理控制台界面。



图 83

5.3 瑞星管理控制台界面说明

瑞星管理控制台（如图84）分为4个部分：功能菜单项、组管理界面、计算机列表栏、病毒信息列表栏、消息列表。

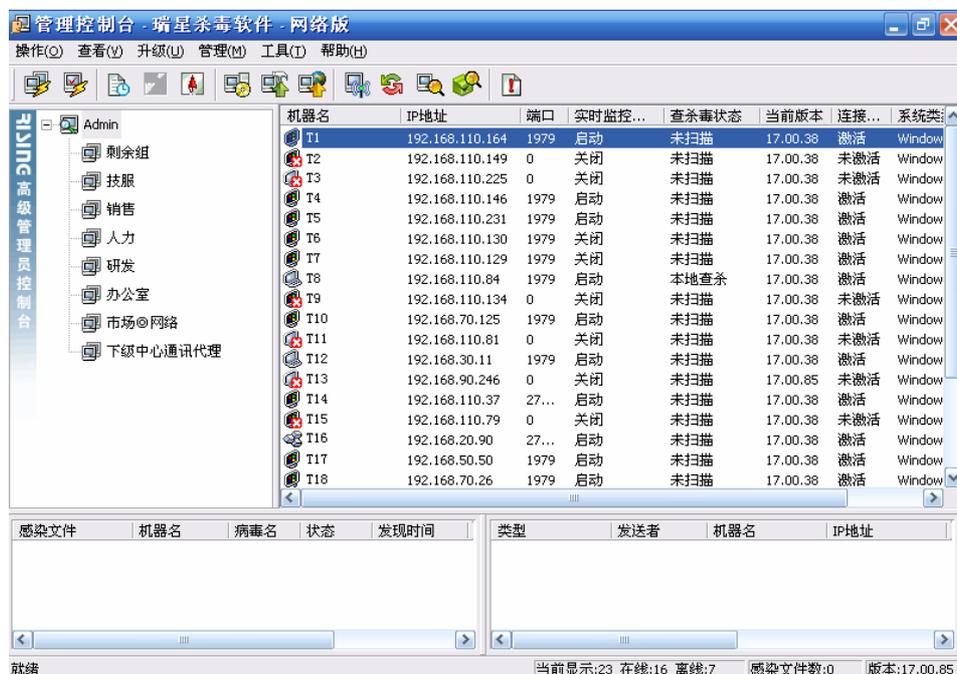


图 84

计算机列表图标识别



: 系统中心;



: 已激活的客户端;



: 未激活的客户端;



: 安装有控制台的已激活的客户端;

：安装有控制台的未激活的客户端；

：已激活的Unix客户端；

：未激活的Unix客户端。

5.3.1 菜单说明

选择功能菜单项中的各项菜单，或者点击工具栏中的快捷按钮，可完成管理控制的多项重要功能。

【操作】菜单：（如图85）

- **【全网查杀】：**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关机状态，则这些计算机在开机后即自动进行查杀病毒；（网吧版无此菜单）
- **【查杀病毒】：**对选中的一台或多台计算机进行远程查杀病毒；（网吧版无此菜单）
- **【停止查杀病毒】：**停止查杀病毒操作；
- **【扫描漏洞】：**对选中的计算机进行漏洞扫描，可以设置“最高、高、中、低”四个漏洞严重程度级别进行扫描；
- **【开启实时监控】：**对选中的计算机启动实时监控；
- **【关闭实时监控】：**对选中的计算机关闭实时监控；
- **【设置查杀策略】：**对选中的计算机进行详细的病毒查杀策略设置；
- **【立即升级】：**对选中的计算机进行程序升级；
- **【选项】：**对选中的计算机进行选项设置，具体包括“设置保护密码”、“定时升级设置”、“绑定端口”、“指定系统中心”、“漏洞扫描”和“报毒设置”等选项；
- **【日志信息】：**查看病毒日志和事件日志；
- **【发送广播消息】：**对选中的计算机发送广播消息，默认发送对象为所有计算机。
- **【卸载客户端】：**卸载客户端的杀毒软件；
- **【安装管理控制台】：**对选中的计算机进行远程安装瑞星管理控制台；
- **【卸载管理控制台】：**对选中的计算机进行远程卸载瑞星管理控制台；
- **【加入拒绝列表】：**将选中的计算机加入拒绝列表（黑名单），黑名单中的计算机不能在系统中心注册，直到此计算机从黑名单中删除；
- **【删除客户端】：**将选中的计算机从列表中删除；
- **【属性】：**查看选中计算机的属性，包括“机器名”、“实时监控状态”、“查杀毒状态”、“当前版本”、“系统类型”、“IP地址”和“端口”等详细信息；
- **【刷新客户端状态】：**选中该选项后，将重新获取整个局域网内可以管理的计算机列表信息；
- **【从系统中心获取最新数据】：**刷新系统中心的最新状态；
- **【退出】：**退出瑞星管理控制台。

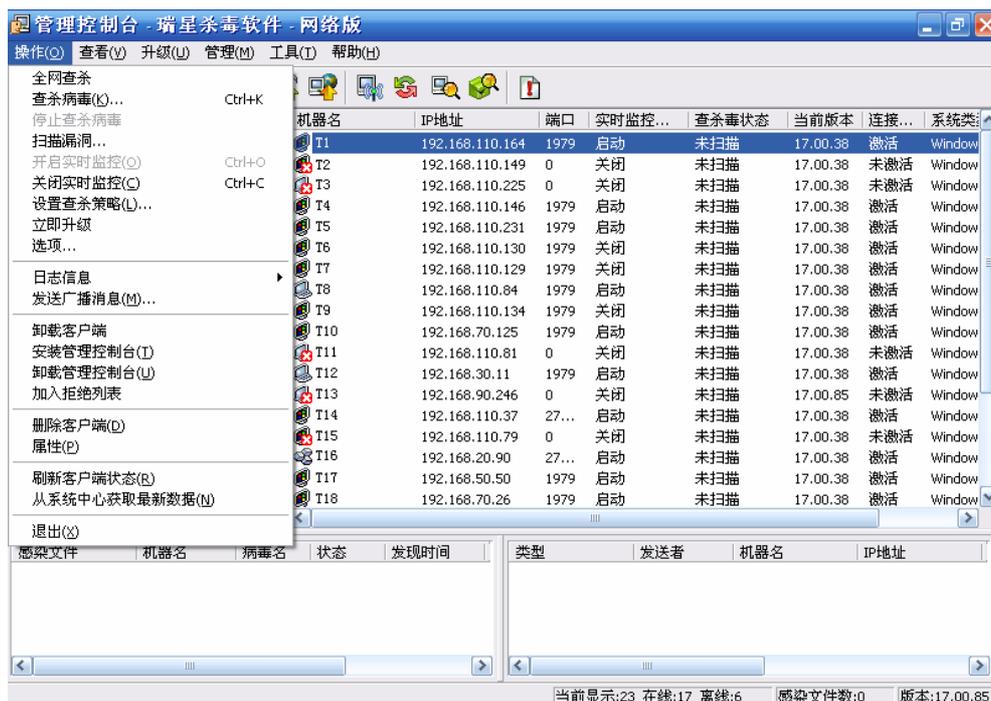


图85

【查看】菜单：（如图86）

- 【分组窗口】：选中此项将显示计算机分组信息窗口；
- 【病毒窗口】：选中此项将显示病毒信息窗口；
- 【消息窗口】：选中此项将显示消息窗口；
- 【漏洞扫描窗口】：选中此项将显示漏洞扫描窗口；
- 【工具栏】：选中该项后，会在控制台上列出一些快捷按钮，功能与各所属菜单中的作用相同；
- 【状态栏】：在病毒信息列表栏下方，显示管理控制台的当前状态信息；
- 【授权信息】：查看此软件的授权信息，包括“系统中心”、“客户端”和“服务器”的购买数量等信息；
- 【注册信息】：查看系统中心的注册信息；
- 【全部选定】：全部选中计算机列表中的机器；
- 【反向选择】：反向选择计算机列表中的机器。

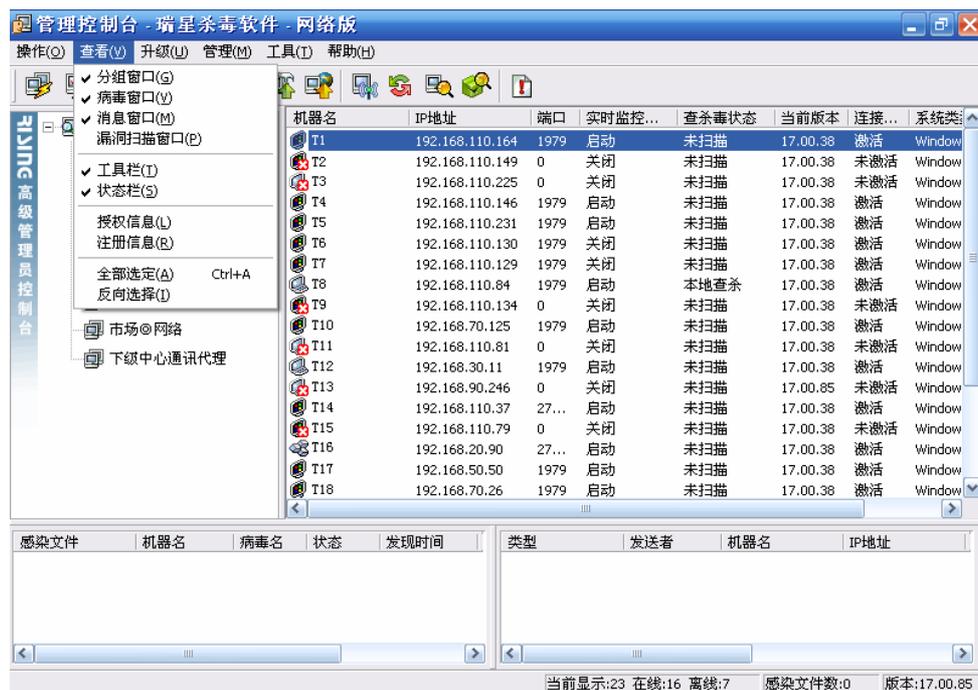


图86

【工具栏】：选中该项后，会在控制台上列出一些快捷按钮，功能与各所属菜单中的作用相同。工具栏上的快捷按钮主要有：



：对所有机器进行远程查杀毒；（网吧版无此按钮）



：对选中机器进行远程查杀毒；（网吧版无此按钮）



：查看病毒警告历史记录；



：启动选中机器上的瑞星实时病毒监控程序；



：关闭选中机器上的瑞星实时病毒监控程序；



：在选中的机器上远程安装管理控制台；



：手动升级瑞星杀毒软件网络版；



：立即升级瑞星杀毒软件网络版；



：向客户端发送广播消息；



：刷新计算机列表；



: 查找未安装杀毒软件的客户端;



: 扫描选中机器上的系统漏洞;



: 显示瑞星管理控制台的版本等信息。

【状态栏】: 在病毒信息列表栏下方, 显示管理控制台的当前状态信息。(如图 87)

就绪 当前显示:23 在线:16 离线:7 感染文件数:0 版本:17.00.85

图 87

【升级】菜单: (如图88)

- **【手动升级】:** 选中该项, 在弹出的**【打开】**对话框中选择升级包程序, 再按**【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】:** 选中该项后, 程序将通知系统中心自动进行升级。

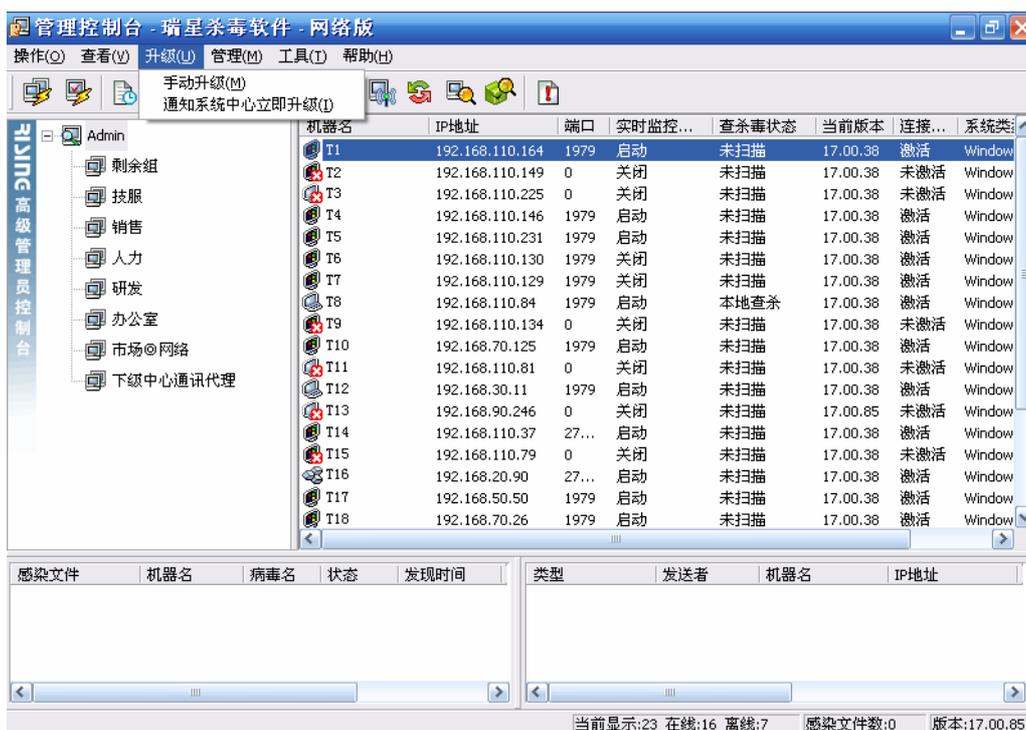


图88

【管理】菜单: (如图 89)

- **【添加组】:** 在组管理界面里添加组。
- **【删除组】:** 在组管理界面里删除组。
- **【重命名组】:** 在组管理界面里对组名重命名。
- **【管理员管理】:** 切换到管理员管理模式。
- **【添加管理员】:** 在管理模式下, 有添加或删除管理员的权限, 选中该选项后, 可添加

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，又可以实现各个管理员根据实际的网络情况和查杀需求进行配置；

- **【删除管理员】**：选中该选项后，可删除管理员。

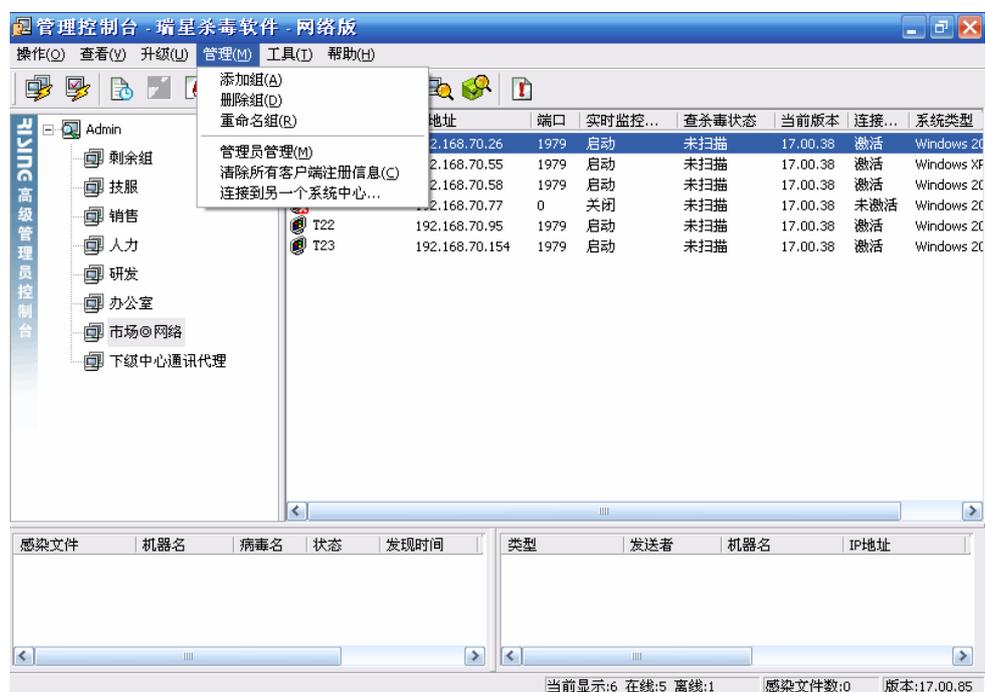


图89

【工具】菜单：（如图90）

- **【客户端安装工具】**：对客户端进行远程安装组件；
- **【瑞星配置工具】**：瑞星网络版配置工具，可对系统中心、客户端、网络设置、升级设置、黑白名单、漏洞扫描和对对象端口设置等选项进行配置；
- **【Unix客户端升级工具】**：通过此工具完成对Unix客户端的升级；
- **【添加授权数】**：对产品进行扩容；
- **【设置用户ID】**：对用户ID进行设置；
- **【更改密码】**：设置或更改当前登录用户帐号的密码。

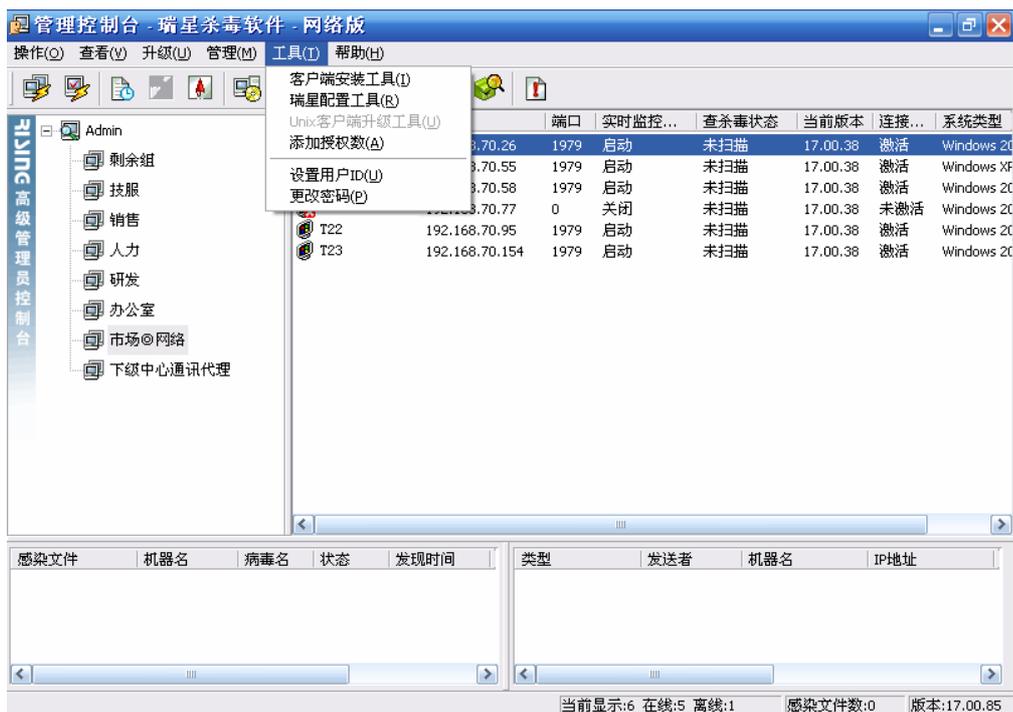


图90

【帮助】菜单:(如图91)

- 【帮助主题】: 查看瑞星杀毒软件网络版使用帮助信息。
- 【瑞星管理控制台】: 查看瑞星管理控制台版本等相关信息。

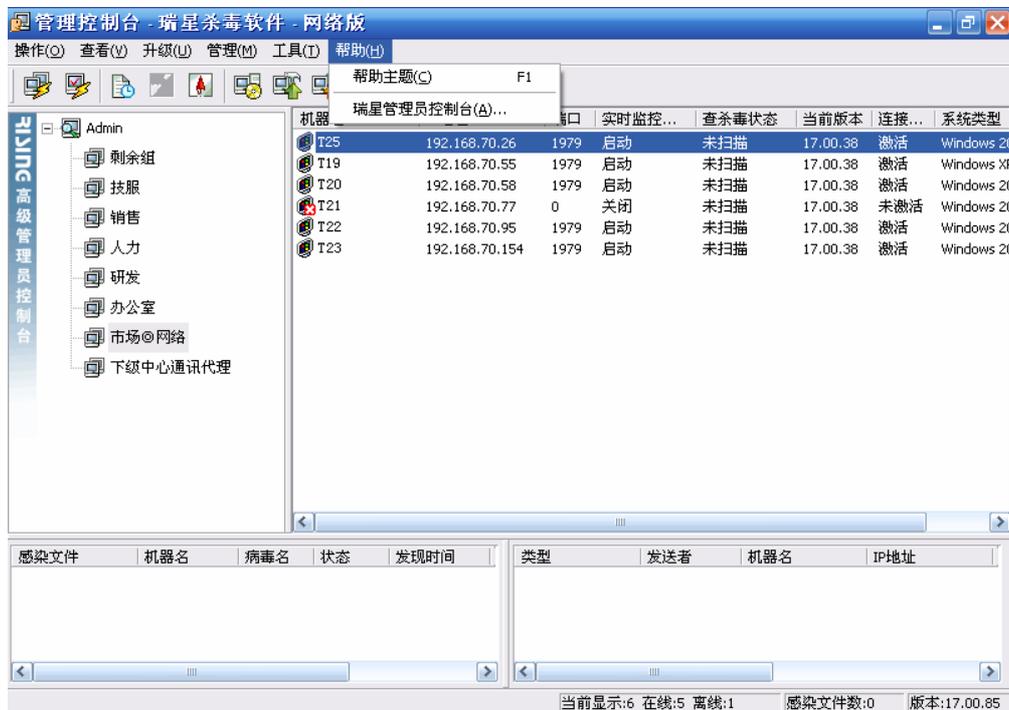


图91

5.3.2 组管理界面

一种基于用户分组管理的功能界面,在这里我们可以创建组、添加组以及添加组成员。(如图92)



图92

5.3.3 计算机列表栏

在该列表栏中(如图93),显示注册过的机器名、IP地址、端口、实时监控状态、查杀毒状态、当前版本、连接状态以及系统类型,并支持为选中的机器设置客户端口令。该列表栏支持鼠标右键功能,包括:【全部选定】、【反向选定】、【选项】等。

机器名	IP地址	端口	实时监控...	查杀毒状态	当前版本	连接...	系统类型
T1	192.168.110.164	1979	启动	未扫描	17.00.38	激活	Windows 2000 Prof...
T2	192.168.110.149	0	关闭	未扫描	17.00.38	未激活	Windows 2000 Prof...
T3	192.168.110.225	0	关闭	未扫描	17.00.38	未激活	Windows 2000 Prof...
T4	192.168.110.146	1979	启动	未扫描	17.00.38	激活	Windows 2000 Prof...
T5	192.168.110.231	1979	启动	未扫描	17.00.38	激活	Windows XP Profes...
T6	192.168.110.130	1979	关闭	未扫描	17.00.38	激活	Windows 2000 Prof...
T7	192.168.110.129	1979	关闭	未扫描	17.00.38	激活	Windows 2000 Prof...
T8	192.168.110.84	1979	启动	本地查杀	17.00.38	激活	Windows XP Profes...
T9	192.168.110.134	0	关闭	未扫描	17.00.38	未激活	Windows XP Profes...
T10	192.168.70.125	1979	启动	未扫描	17.00.38	激活	Windows 2000 Prof...
T11	192.168.110.81	0	关闭	未扫描	17.00.38	未激活	Windows 2000 Prof...
T12	192.168.30.11	1979	启动	未扫描	17.00.38	激活	Windows 2000 Prof...
T13	192.168.90.246	0	关闭	未扫描	17.00.85	未激活	Windows Server 20...
T14	192.168.110.37	27...	启动	未扫描	17.00.38	激活	Windows 2000 Prof...
T15	192.168.110.79	0	关闭	未扫描	17.00.38	未激活	Windows XP Profes...
T16	192.168.20.90	27...	启动	未扫描	17.00.38	激活	Windows 2000 Server
T17	192.168.50.50	1979	启动	未扫描	17.00.38	激活	Windows 2000 Prof...
T18	192.168.70.26	1979	启动	未扫描	17.00.38	激活	Windows 2000 Prof...
T19	192.168.70.55	1979	启动	未扫描	17.00.38	激活	Windows XP Profes...

图93

5.3.4 病毒信息列表栏

该列表栏（如图94）显示局域网内所有发现的病毒信息，包括文件名、文件所在的计算机名、文件所在的文件夹、病毒名、病毒的状态以及发现该病毒的时间。

该列表栏支持鼠标右键功能，包括：**【全部选定】**、**【反向选定】**、**【删除】**以及**【查看详细信息】**。

感染文件	机器名	病毒名	状态	发现时间

图94

5.3.5 消息窗口

该列表栏（如图95）显示局域网内所有消息，包括类型、发送者、IP地址、消息内容和时间。该列表栏支持鼠标右键功能，包括：**【全部选定】**、**【反向选定】**、**【删除】**以及**【查看详细信息】**。

类型	发送者	机器名	IP地址

图95

5.4 远程控制

5.4.1 远程查杀

在瑞星管理控制台上可以任选一台或多台计算机进行远程查杀毒，在机器列表栏选择需要查杀的

机器名，点击工具栏中的  按钮或【操作】菜单下的【查杀毒病】后，弹出查杀选项设置界面，单击【开始扫描】即可进行远程查杀毒。同时在目标客户端的系统托盘（位于 Windows 界面右下角显示时钟的区域）内将显示瑞星杀毒软件正在扫描病毒的图标，表示其正在被执行远程查杀毒操作。

5.4.2 远程设置

通过瑞星管理控制台的【设置查杀策略】菜单，管理员可以对全部机器或指定的机器设置查杀策略，使得管理员只需在控制台上就可对所有用户的设置进行统一的管理和设定。为了避免人为的关闭或卸载客户端程序，管理控制台还提供了设置客户端口令的功能。在口令的保护下，任何客户端都无法进行关闭实时监控和卸载程序的操作。

5.4.2.1 策略的分发

在计算机列表中选中全部或部分计算机，选择【操作】/【设置查杀策略】，弹出【查杀策略设置】对话框，完成设置后点击【确定】，策略便被分发到这些被选中计算机中。（如图 96）

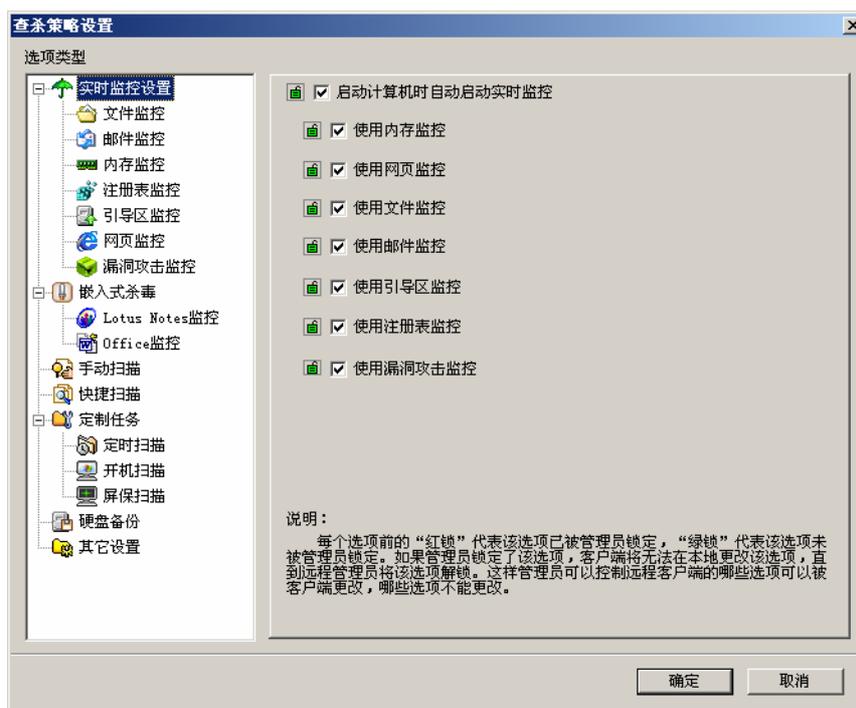


图96

5.4.2.2 选项设置

为了避免客户端用户人为的关闭实时监控程序或卸载杀毒程序，从而造成整体防毒体系的漏洞，管理员可以通过控制台程序对所有或指定的用户设置密码。管理员还可以通过选项设置，对客户端进行定时升级设置和端口绑定，也可以对组指定系统中心。

(1) 客户端设置保护密码

在计算机列表栏选中需设定密码的机器，选择【操作】/【选项】，弹出【选项设置】对话框，选择【设置保护密码】标签，在文本框中填写保护密码。（如图97）



图97

(2) 客户端设置升级方式

在计算机列表栏选中需设定升级的机器，选择【操作】/【选项】，弹出【选项设置】对话框，选择【定时升级设置】标签，为指定的客户端设置定时升级方式。（如图98）



图98

(3) 客户端设置绑定端口

在计算机列表栏选中需绑定端口的机器，选择【操作】/【选项】，弹出【选项设置】对话框，选择【绑定端口】标签，为指定的客户端绑定端口。（如图99）

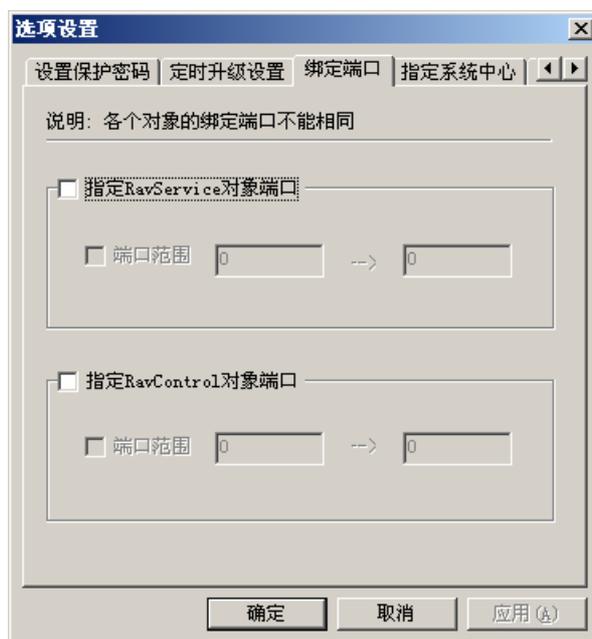


图99

(4) 指定系统中心

在计算机列表栏选中需绑定端口的机器，选择【操作】/【选项】，弹出【选项设置】对话框，选择【指定系统中心】标签，填写系统中心的IP地址和端口。（如图100）

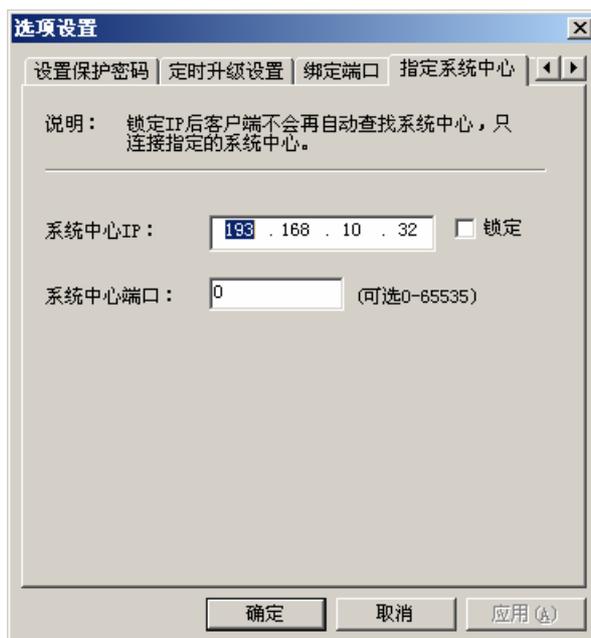


图100

(5) 漏洞扫描

在计算机列表栏选中需要扫描系统漏洞的机器，选择【操作】/【选项】，弹出【选项设置】对话框，选择【漏洞扫描】标签，在【自动安装漏洞补丁程序】复选框中打勾。(如图101)

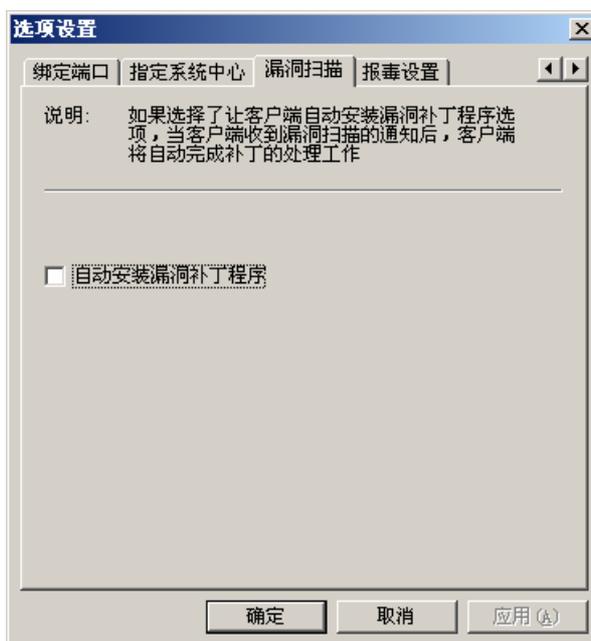


图101

(5) 报毒设置

在计算机列表栏选中需要进行病毒报告设置的机器，选择【操作】/【选项】，弹出【选项设置】对话框，选择【报毒设置】标签，设置定时报毒方式和时间。(如图102)



图102

注意：以上所有的远程设置功能，仅对处于激活状态的客户端有效。

5.4.3 远程安装

通过瑞星管理控制台，不仅可以为局域网内的所有客户端安装管理控制台，也可以为基于NT结构的操作系统远程安装瑞星杀毒软件，远程安装功能极大的方便了系统管理员的管理和安装工作。

5.4.3.1 远程安装管理控制台

系统管理员可以将瑞星管理控制台远程安装其他计算机上，安装步骤如下：

步骤一：在计算机列表栏中将要远程安装控制台的机器，单击【操作】菜单，选中【安装管

理控制台】，或在工具栏中按  快捷按钮；

步骤二：弹出【提示信息】对话框，选择【确定】按钮；完成远程安装控制台后，在计算机列表栏中相应机器的图标有所变化，表示该机器已安装控制台。

提示：不要在局域网上安装过多的瑞星管理控制台，以保障管理的统一化。

5.4.3.2 远程安装瑞星杀毒软件（网吧版无此功能）

系统管理员可以通过瑞星管理控制台，给指定的基于 Windows NT WorkStation / Windows NT Server / Windows 2000 Professional / Windows 2000 Server / Windows 2000 Advanced Server / Windows 2003 Server 系统的客户端进行远程安装瑞星杀毒软件的操作（支持远程安装的操作系统信息参阅第三章附表3），安装步骤如下：

步骤一：在瑞星管理控制台界面中，单击【工具】菜单，选择【客户端安装工具】；

步骤二：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机器，或直接输入计算机名或IP，单击【添加】按钮。（如图103）

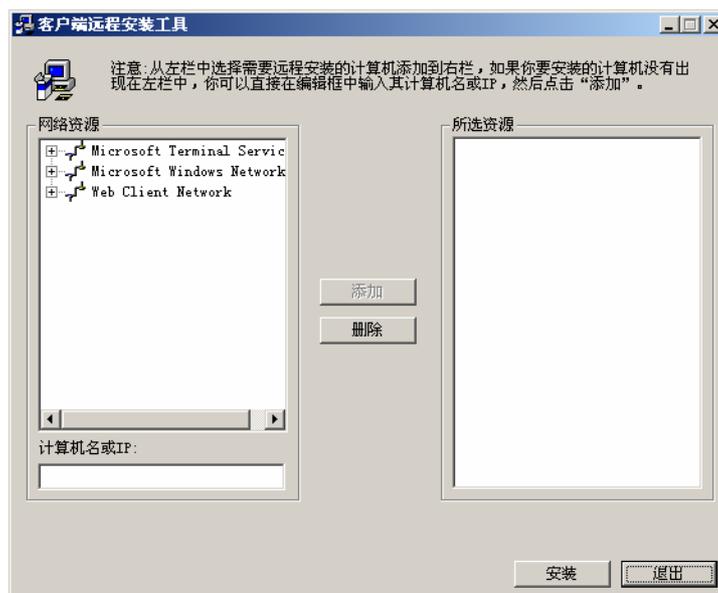


图103

步骤三: 在【输入\\XXX 的管理员密码】(XXX 为计算机名)对话框中, 输入目标计算机的用户名和密码, 单击【确定】。

步骤四: 将目标计算机被添加到【所选资源】框中后, 单击【开始安装】按钮, 随即开始为目标机器远程安装瑞星杀毒软件。

步骤五: 安装完成后, 在安装状态栏中显示【完成远程安装!】的提示。

步骤六: 被远程安装瑞星杀毒软件的客户端桌面上将显示【信使服务】的提示信息, 单击【确定】, 远程安装完成。

注意: 因操作系统的局限, 针对 Windows 9x/Me/XP 系统的客户端, 不能实现远程安装瑞星杀毒软件。

5.4.4 远程启动/关闭客户端监控

管理员可以通过管理控制台实时地查看目前所有客户端实时监控是处于启动状态还是关闭的状态, 也可以通过按工具栏中的  和  按钮来远程控制客户端的监控状态。

选中实时监控状态处于关闭(或启动)的机器, 选择【操作】/【启动实时监控】或单击工具栏中的  (或 ) 按钮, 即可对选中的计算机启动(或关闭)实时监控功能。

注意: 该操作仅对处于“激活”状态的客户端有效。

5.4.5 远程报警

在全网中, 有关瑞星杀毒软件发现的任何病毒信息和病毒处理方法的信息都将传递到系统中心,

并在管理控制台的病毒信息列表栏中显示。管理员可以通过该功能方便的了解全网的安全状况，并可根据具体情况做出相应的处理。

5.4.6 远程全网查杀

远程全网查杀是瑞星杀毒软件网络版整体保护网络安全的重要功能。远程全网查杀的特点在于整体性和实时性。即，其查杀的范围是网络中所有安装了瑞星杀毒软件网络版的计算机。这样就保障了所有客户端几乎在同一时刻进行杀毒的工作，避免了病毒交叉感染的可能。管理员可以通过控制台有计划的对网络上所有的计算机同时进行远程查杀毒操作。

进入瑞星管理控制台后，单击【操作】/【全网查杀】。

在弹出的“查杀选项设置”程序界面中单击【开始扫描】按钮。

5.5 用户管理

用户管理作为瑞星杀毒软件网络版的一个管理特色，其核心在于在一个管理控制台中可以进行多模式管理，即组的管理模式与管理员的多级管理模式。

5.5.1 组管理

启动管理控制台后，默认状态是进入到组管理模式中。

5.5.1.1 建立组

方法一：

- 1、以 Admin 身份登录进入组管理模式。
- 2、在组管理界面中点击鼠标右键。
- 3、在右键菜单中选择【添加组】，添加新的管理组。（如图 104）



图 104

方法二：

- 1、以 Admin 身份登录进入组管理模式。
- 2、选择菜单【管理】/【添加组】。

5.5.1.2 为指定的组添加用户

- 1、以 Admin 身份登录进入组管理模式。
- 2、选中【剩余组】，用鼠标把选中的计算机“拖”到指定的组中，即可把用户添加到指定的组中。

5.5.1.3 删除组

方法一：选定希望删除的组，点击鼠标右键，选择【删除组】，即可删除指定的组。

方法二：选定希望删除的组，选择菜单【管理】/【删除组】，即可删除指定的组。

5.5.2 管理员管理

在管理控制台中，选择【管理】/【管理员管理】菜单，随即显示【管理员管理】界面。（如图 105）



图 105

通过【管理员管理】，可添加管理员、删除管理员和设置管理员密码，以及查看每个管理员所管辖的客户端的机器名、IP 地址和系统类型等详细信息。

5.6 日志信息

日志信息记录了网络中计算机感染病毒的情况和事件内容，管理员可以查看网络中计算机感染病毒的情况，包括感染病毒的时间、病毒类型及分布情况等，以及事件的类型、发送者、IP 地址、

消息内容和时间。

5.6.1 病毒日志

在瑞星管理控制台中，选择【操作】/【日志信息】/【病毒日志】，进入【病毒日志】界面。

【操作】菜单：

- 【导出选定的病毒记录】：导出选定的病毒警告历史记录信息到指定的文件中。
- 【导出全部的病毒记录】：导出所有的病毒警告历史记录信息到指定的文件中。
- 【删除选定的病毒记录】：删除选定的病毒警告历史记录信息。
- 【删除所有的病毒记录】：删除所有的病毒警告历史记录信息。
- 【打印选定的病毒记录】：打印选定的病毒警告历史记录信息。
- 【打印全部的病毒记录】：打印所有的病毒警告历史记录信息。

【查看】菜单：

- 【查看指定日期病毒记录】：查看任意一天的记录；
- 【文字统计报告】：以文字方式报告感染病毒的计算机的统计信息。
- 【图表统计报告】：以图表方式报告感染病毒的计算机的统计信息。
- 【全部选定】：选定所有的记录。
- 【反向选定】：不选定任何记录。

5.6.2 瑞星病毒日志查询统计工具

通过瑞星病毒日志查询统计工具，管理员可对查杀病毒的日志进行查询统计。选择【开始】/【程序】/【瑞星杀毒软件】/【病毒日志查询统计工具】，进入【瑞星病毒日志查询统计工具】界面（如图 106）。

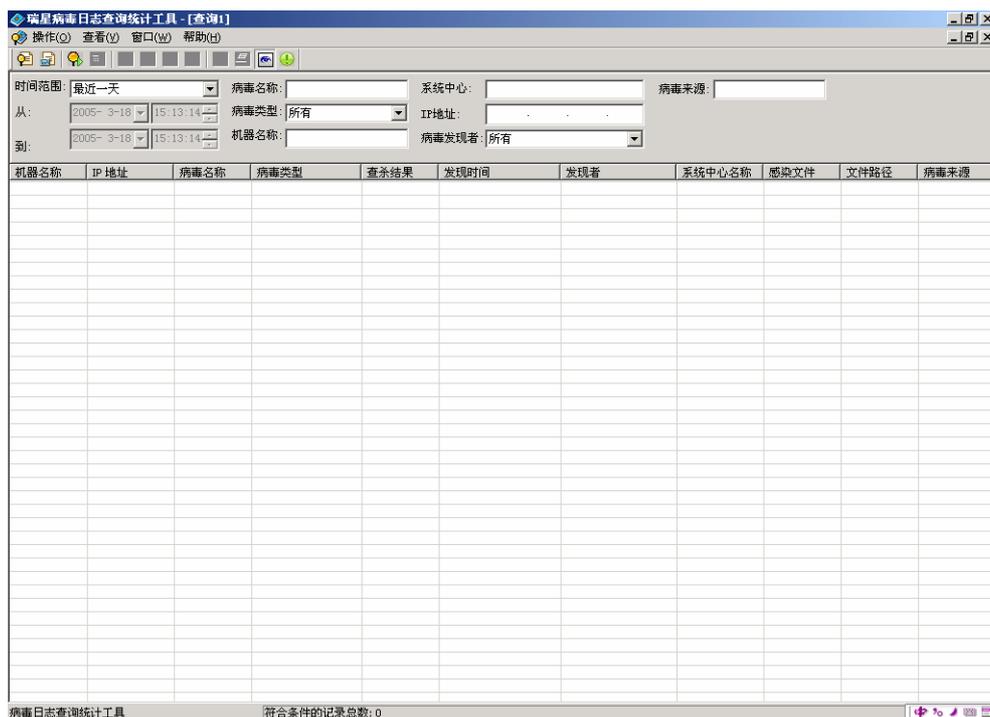


图 106

5.6.3 事件日志

在瑞星管理控制台中，选择【操作】/【日志信息】/【事件日志】，进入【事件日志】界面。

【文件】菜单：

- 【查看详细信息】：查看事件的详细信息。
- 【删除已选日志】：删除选定的日志信息。
- 【删除所有日志】：删除所有的日志信息。
- 【退出】：退出事件日志界面。

【查看】菜单：

- 【查看事件日志】：查看任意一天的事件日志。

5.7 其他

5.7.1 广播的应用

瑞星管理控制台提供广播的功能。管理员可以通过控制台对所有或指定的客户端发布文本消息，实现了远程的病毒预警功能。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：

步骤一：在机器列表栏选中需要接受广播的用户，选择【操作】/【发送广播消息】，或者单击



快捷按钮。

步骤二：在弹出的【广播窗口】中输入文本信息，单击【发送】。（如图 107）

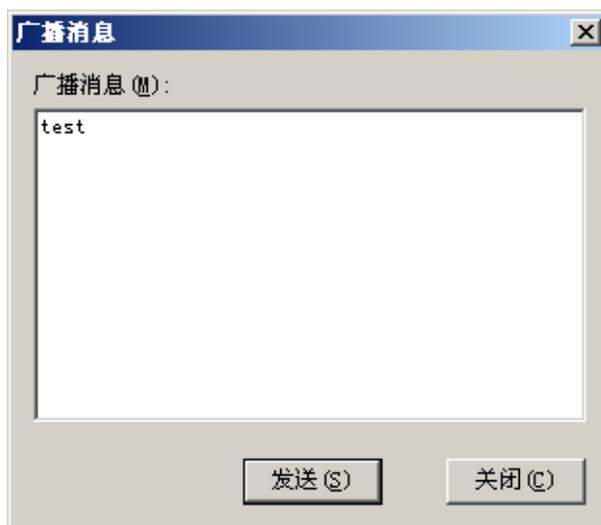


图 107

步骤三：在目标客户端将出现【客户端服务程序】提示框，读取完消息后，单击【隐藏】按钮即可关闭该窗口。（如图 108）

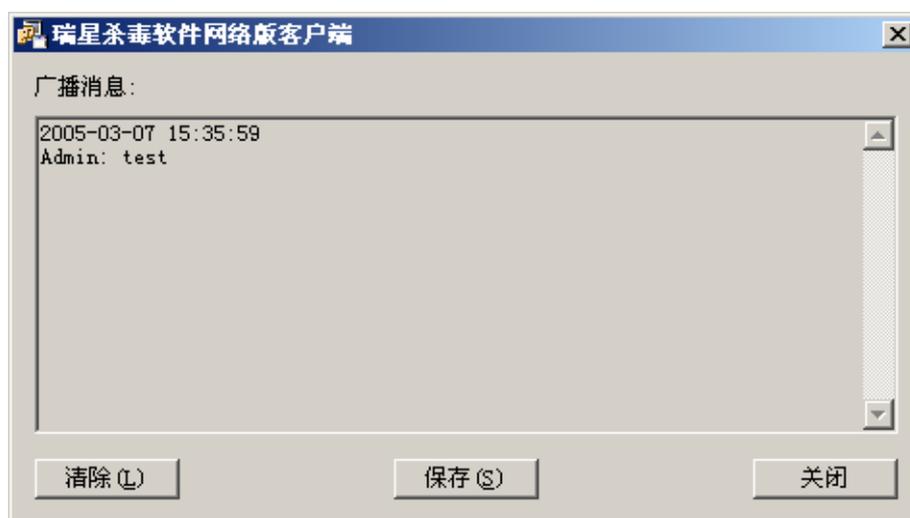


图 108

注意：当您不对接受广播的用户做出选定时，默认的是向当前所有用户发送广播。

5.7.2 删除客户端

当客户端发生诸如更换操作系统、更换 IP 地址等变化时，需要通过管理控制台释放这些机器（因为这些机器仍然占用 License 记数），以避免一台机器同时占用多个 License 记数。

删除客户端的步骤是：在管理控制台中，选中待删除的客户端，再选择【操作】/【删除客户端】菜单，在弹出的【提示信息】对话框中单击【确定】，即可删除选中的客户端，此客户端占用的 License 数即被释放。

5.7.3 记数统计

管理员可以通过管理控制台查看瑞星杀毒软件网络版授权记数的使用情况和已注册机器的统计情况。

选择【查看】/【授权信息】，随即显示本系统中心和所有系统中心的授权信息。（如图 109）

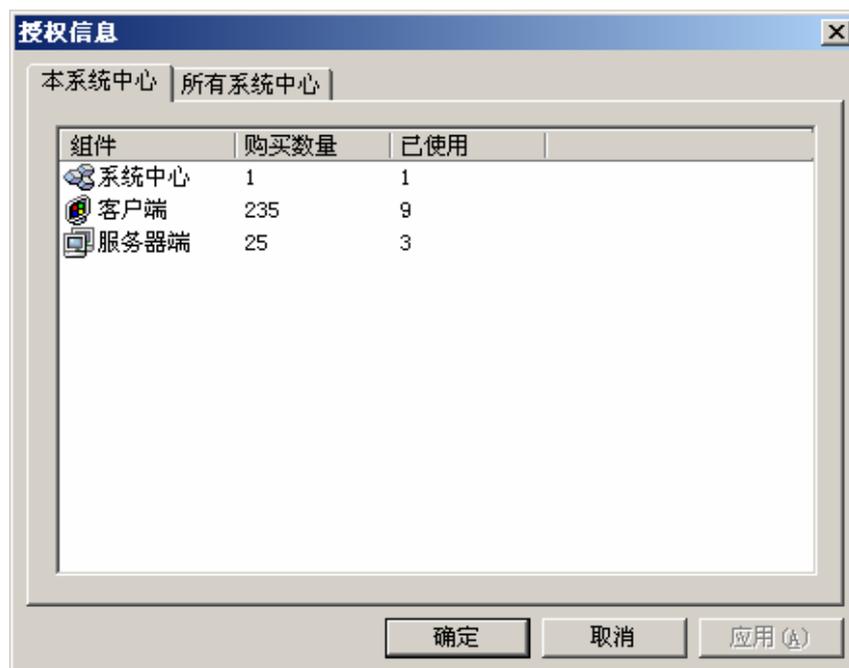


图 109

5.7.4 瑞星配置工具的使用

为了方便用户管理系统中心和客户端的配置，瑞星公司为用户开发了瑞星配置工具。

在管理控制台中，选择【工具】/【瑞星配置工具】，弹出【瑞星网络版配置工具】对话框（如图 110）；

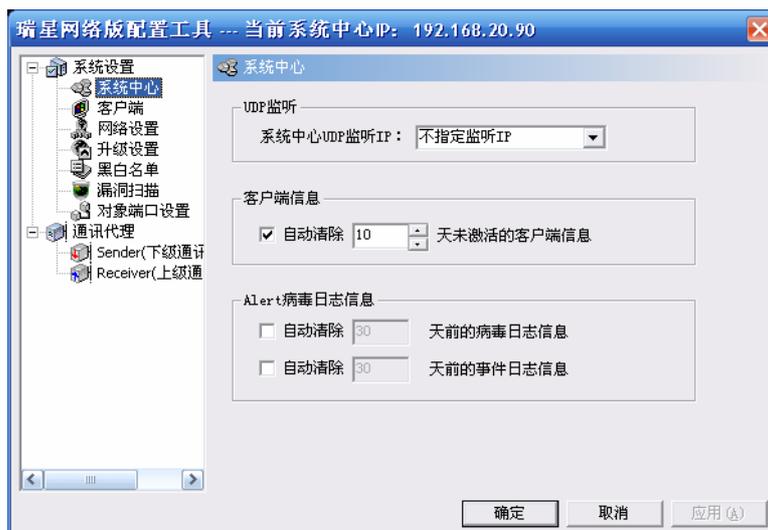


图 110

通过瑞星配置工具，管理员可对系统中心、客户端、网络设置、升级设置、黑白名单、漏洞扫描、对象端口设置和通讯代理进行设置。在任一控制台上，管理员均可通过此工具进行远程配置。

(1) 系统中心

在系统中心设置页中，管理员可对 UDP 监听 IP 地址、客户端信息和病毒日志信息三项设置进行配置。在不指定监听 IP 的情况下，是指对所有 IP 地址进行监听，可以响应本系统中心所连接网段内的所有客户端的请求。在指定监听 IP 的情况下，只响应该 IP 所在网段内的客户端的请求。

(2) 客户端

在客户端设置页中，管理员可对客户端向系统中心报告状态信息的时间间隔、客户端从上级获取数据包的大小和客户端消息框显示方式此三项进行设置（如图 111）。

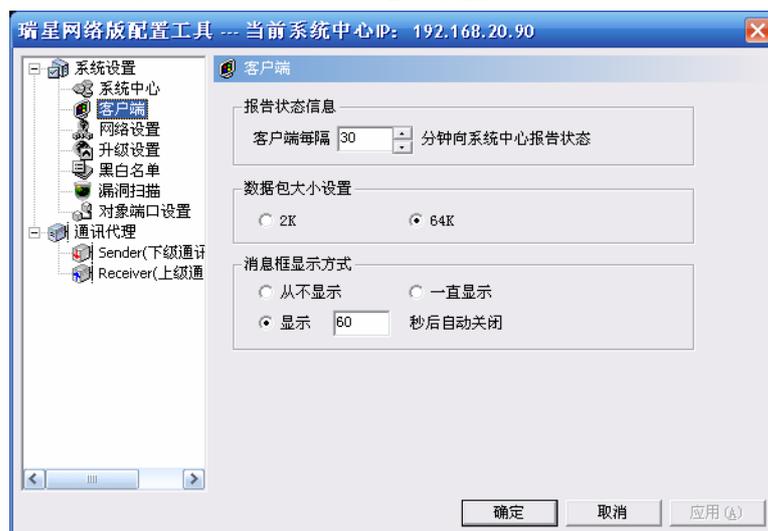


图 111

(3) 网络设置

在网络设置页中，管理员可选择三种 Internet 连接方式：局域网（LAN）或专线上网、通过代理服务器（Proxy）上网和使用拨号网络连接上网（如图 112）。

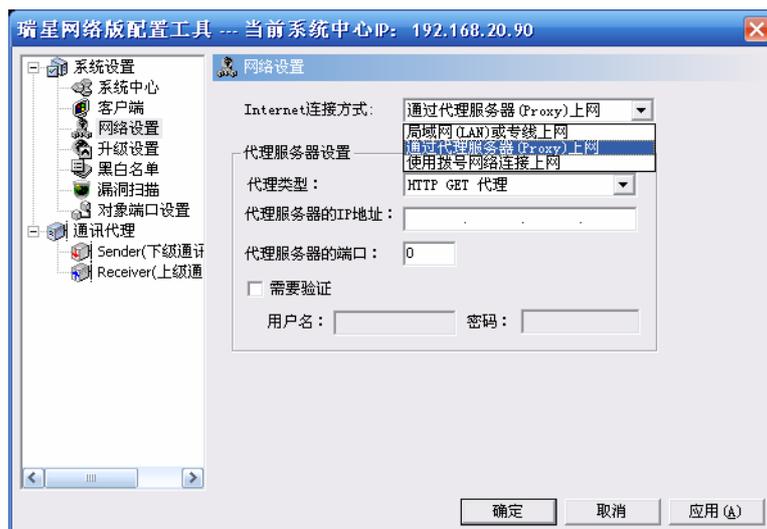


图 112

(4) 升级设置

在升级设置页中，管理员可选择四种升级方式：自动升级、从上级中心升级、从网站智能升级和从网站下载手动升级包。此外，还可对升级时间进行设置（如图 113）。

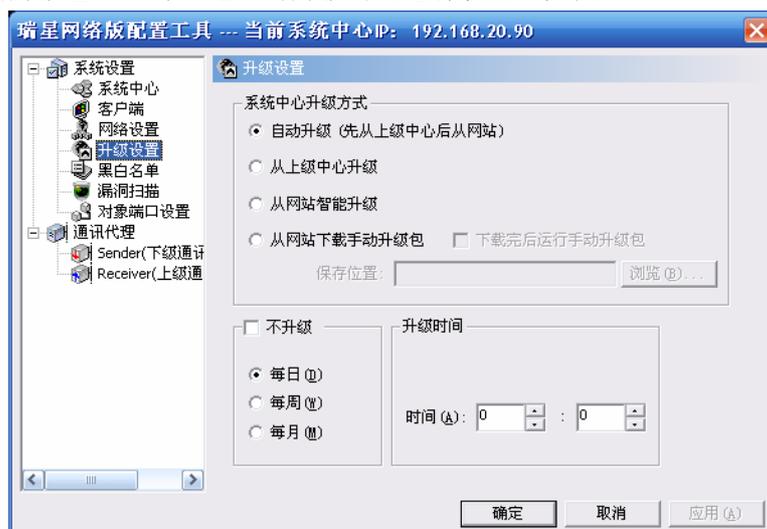


图 113

(5) 黑白名单

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（如图 114）。

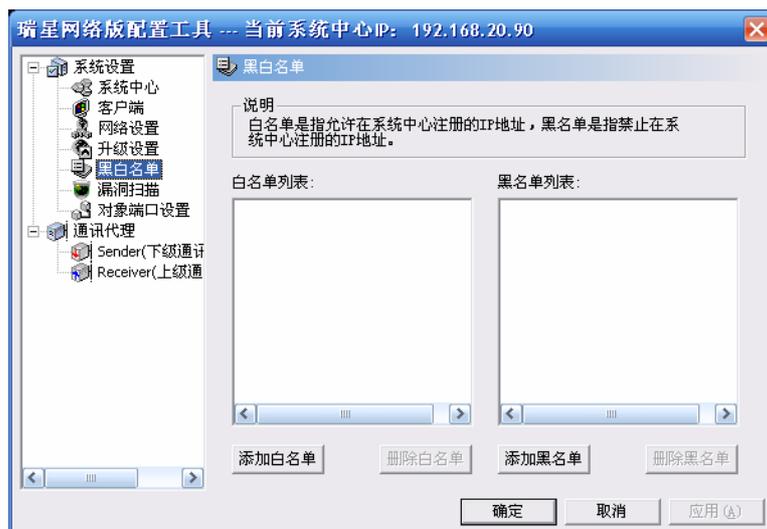


图 114

(6) 漏洞扫描

为及时让客户端安装系统漏洞补丁程序，管理员可设置客户端自动下载和安装漏洞补丁程序（如图 115）。

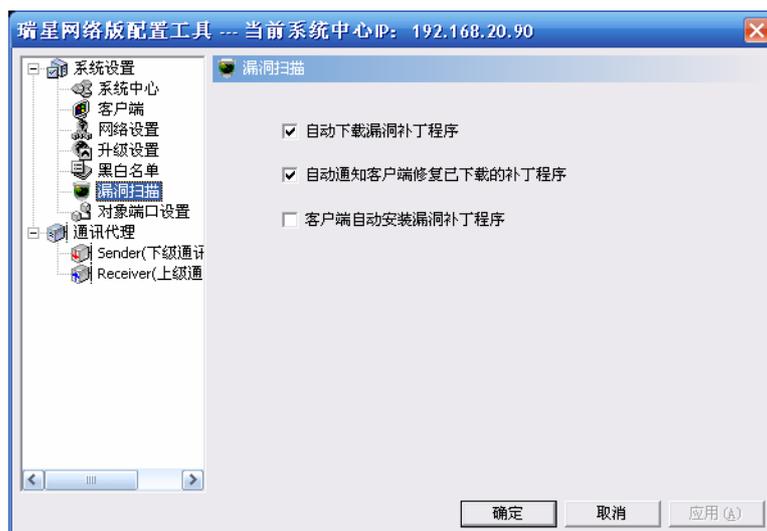


图 115

(7) 对象端口设置

为防止某些通讯端口被防火墙封闭，造成瑞星网络版程序不能正常通讯，用户需要进行固定端口设置。用户可分别选择某个程序的起始端口和终止端口（如图 116）。

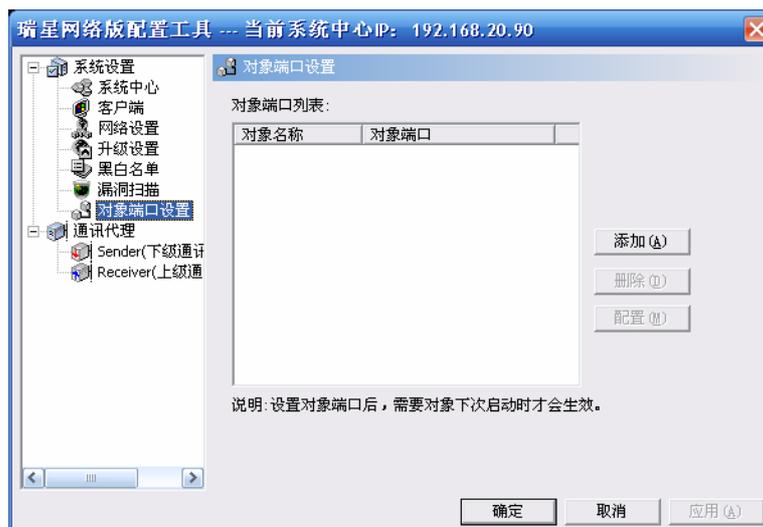


图 116

(8) 通讯代理

下级通讯代理设置:

在安装了下级通讯代理的情况下，瑞星网络版配置工具会显示此设置页。通过此设置页，管理员可查看本系统中心 Sender（下级通讯代理）的名称、IP 地址、端口和状态。

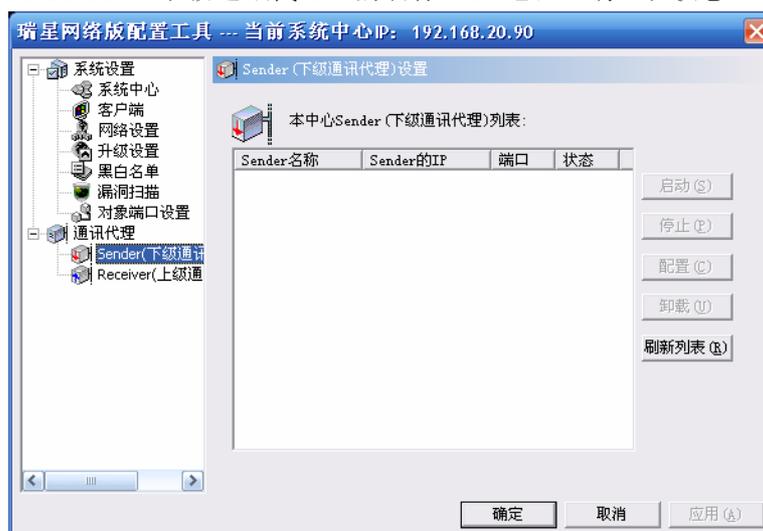


图 117

上级通讯代理设置:

在安装了上级通讯代理的情况下，瑞星网络版配置工具会显示此设置页。通过此设置页，管理员设置本级中心标识和上级通讯代理所在的 IP 地址和端口。

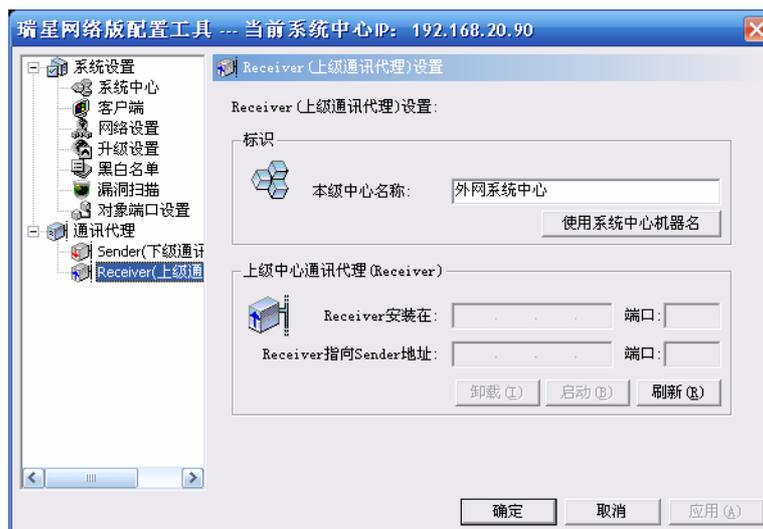


图 118

第六章 升级与扩容

当安装杀毒软件后，升级工作应该是您首要进行的重要工作。杀毒软件的特性决定了升级工作所处的重要地位。利用互联网及时更新软件的版本、自动分发升级程序到客户端是瑞星杀毒软件升级功能的特色。

提示：强烈建议您把瑞星杀毒软件升级到最新版本并进行全网杀毒，以保障当前网络处于全网安全的状况。

6.1 升级配置

在进行软件升级之前，请务必配置好网络设置。

在瑞星管理控制台中，选择【工具】/【瑞星配置工具】，随即弹出【瑞星网络版配置工具】对话框（如图 119）。瑞星杀毒软件网络版提供 4 种网络连接方式，包括自动升级、从上级中心升级、从网站智能升级和从网站下载手动升级包。

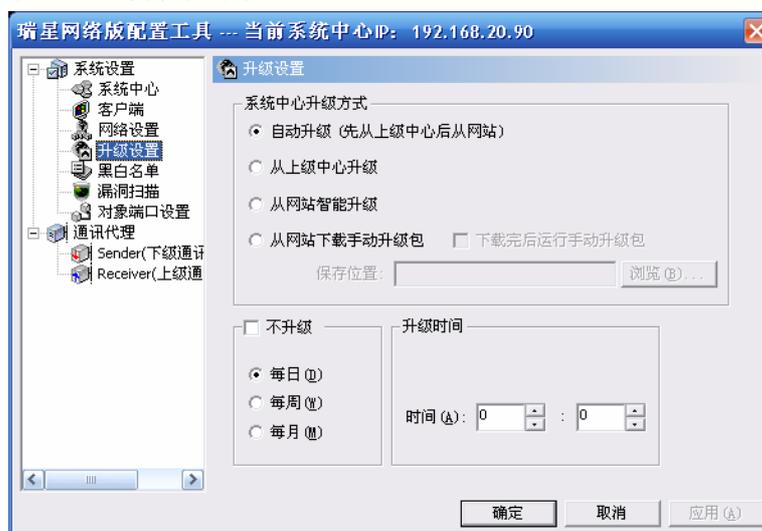


图 119

6.2 网络设置

在【网络设置】中，可设定 Internet 连接方式。

在瑞星管理控制台中，选择【工具】/【瑞星配置工具】/【网络设置】，弹出【网络设置】对话框（如图 120）；

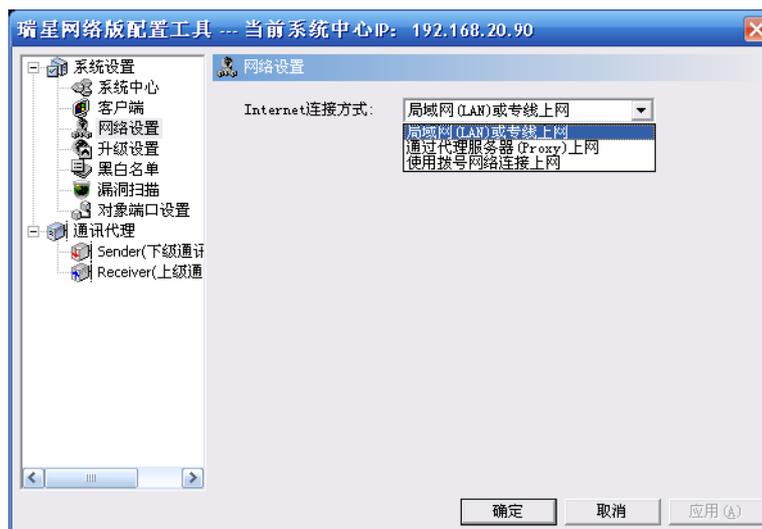


图 120

6.3 产品序列号和用户 ID 号绑定注意事项

用户在得到“瑞星网络版杀毒软件”产品后应立即正确填写“用户注册卡”，并以“挂号”或“快递”形式邮寄给瑞星公司客户服务中心。注册后，用户可以得到带有‘用户 ID’的‘用户授权书’。请在管理控制台中，选择【工具】/【设置用户 ID】菜单，然后输入用户 ID 号（如图 121），之后即可及时获得升级服务了。



图 121

注：用户注册详细信息请参阅《客户服务指南》。

6.4 Unix 客户端升级

瑞星杀毒软件网络版支持 Unix 客户端查杀毒。为方便 Unix 客户端升级，瑞星杀毒软件网络版特地在瑞星管理控制台中新增了【Unix 客户端升级工具】菜单。具体的升级过程如下：

步骤一：确认软件的当前版本信息，在主界面上即可查看版本号；

步骤二：在瑞星网站查看最新版本信息，网址<http://www.rising.com.cn>；

步骤三：比较当前的版本和瑞星网站上最新的版本，使用用户 ID 登录升级页面，找到对应的升级文件，确定要下载的升级文件；

步骤四：下载升级文件，选择【工具】/【Unix 客户端升级工具】，弹出【unixcopy】界面，选中已下载的升级文件，再选择【加入到升级清单】，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，在该工具的版本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。

步骤五：客户端程序会自动完成升级。

6.5 升级瑞星 DOS 杀毒工具

点击【开始】/【程序】/【瑞星杀毒软件】/【瑞星工具】/【瑞星 DOS 杀毒工具】，弹出【瑞星 DOS 启动盘制作工具】界面，可以选择【制作启动软盘】或【制作 USB 启动盘】两种方式升级瑞星 DOS 杀毒工具。

6.6 产品扩容

当需要增加瑞星杀毒软件网络版的服务器或客户端数量时，可以向瑞星公司购买一定数量的授权许可（即扩容序列号）进行网络扩容。

添加扩容授权许可数量可以在局域网上任何一台安装有管理控制台的机器上进行。具体步骤如下：

在管理控制台中，点击【工具】/【添加授权数】，弹出【添加扩容号】对话框，填写扩容号。（如图 122）



图 122

附录：使用过程中的故障问题解决

（1）在安装瑞星杀毒软件网络版时，系统提示“系统初始化失败”而无法继续安装。

解决：运行瑞星杀毒软件网络版安装光盘中 tools 目录中的安装程序，安装结束后重新启动计算机，再次安装瑞星杀毒软件网络版。

（2）升级过程发生意外，升级失败。

解决：A、确定您是否采用的正确的升级方法。

B、如果是手动升级，确定升级包下载正确。

C、如果是自动升级，确定网络设置是否正确。

D、及时和瑞星公司客户服务中心取得联系。

(3) 系统报告“授权计数超出，请购买更多授权”。

解决：确定安装瑞星杀毒软件的服务器端和客户端是否超出购买的授权数，如果不是，请在管理控制台中删除状态为“未激活”的计算机，以释放授权。否则，请和瑞星公司客户服务中心联系。

(4) 在安装系统中心时，安装程序总是提示“安装服务器端”杀毒软件。

解决：确定您是否安装过瑞星网络版杀毒软件，如果在同一网段中存在另一个系统中心，请把另一个系统中心卸载后再安装新的系统中心。

(5) 客户端或者服务器端在系统中心的状态为“未激活”。

解决：A、确定未激活的计算机未关机。

B、确定该计算机和系统中心所在服务器可以相互通讯。

(6) 远程杀毒时，出现某些病毒杀毒结果是“用户忽略”的情况。

解决：出现这种情况大多由于遇上了木马类病毒，需要直接删除文件才能彻底清除这类病毒。出于保护用户数据安全的目的，在没有本机用户的直接干预的情况下，远程杀毒是按照“用户忽略”的方式处理的。如果您需要彻底清除这类病毒，请在目标计算机进行本地杀毒。

第七章 多级中心系统使用说明

（注：本章内容不适用于中小企业版和网吧版）

前言

面对新的经济形势，大、中型企业纷纷踊跃地加入信息化建设，大力建设多级中心网络系统，其网络呈现出多层次、分隶属的复杂结构。如何在这些不同层级的网络中实现统一的、全面的、及时有效的计算机反病毒管理呢？

“瑞星杀毒软件网络版多级中心系统”及时地满足了大、中型企业在这方面的需求（以下简称“网络版多级中心系统”）。通过该系统，可实现反病毒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、下达版本升级提示，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，并主动向上级中心发送请求和汇报信息。可见，网络版多级中心系统支持大型的、多层次的、复杂的网络。

网络版多级中心系统是基于网络版单级中心系统进行开发的，因而既能在单网段中使用，又能在多网段中使用，能够对多网段的大型网络进行很好的统一管理。网络版多级中心系统新增加了 Receiver 上级通讯代理和 Sender 下级通讯代理两个功能模块，这两个新增加的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。

- 上级通讯代理功能模块的作用是与下级通讯代理建立对应的通讯关系，使得上级中心可以对下级中心进行管理，并上报下级中心传送过来的数据。
- 下级通讯代理功能模块的作用是发送命令给上级通讯代理。

下面，我们通过图解来说明网络版多级中心系统的管理机制，如图 123：

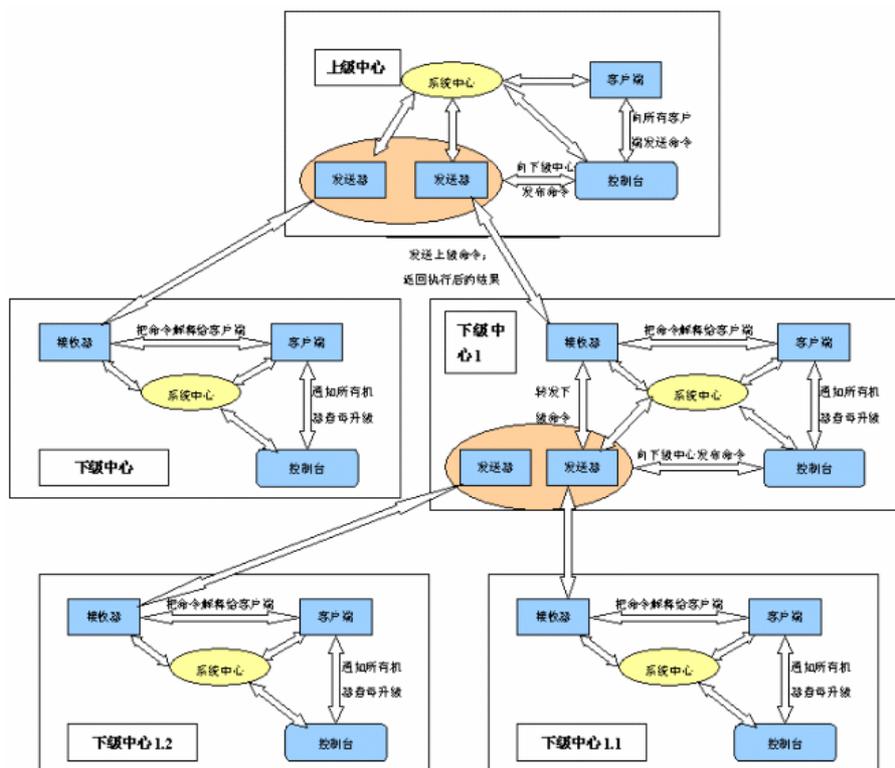


图 123: 瑞星杀毒软件网络版多级中心系统通讯结构简图

图解: 图中【发送器】是指下级通讯代理;【接收器】是指上级通讯代理。多级中心是由不同层级的中心组成的,不同层级的中心所处的隶属关系决定了该层级中心不同的拓扑结构。需要指出的是,下级通讯代理可以同时维护多个上级通讯代理程序,如果存在一个上级中心管理多个下级中心,则只需要在上级中心安装一个下级通讯代理,这个上级中心管理的下级中心,则需要每个中心都安装一个上级通讯代理与下级中心进行通讯。值得强调的是,对于一个上级中心安装的下级通讯代理有且只能有一个,而对于下级中心来说,则不限制上级通讯代理的数量。

7.1 安装

7.1.1 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,您需要做的准备工作有:

- 先安装瑞星杀毒软件网络版;
- 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上建立通讯的基础上实现的。新增的两个子系统通讯模块是建立多级系统的重要组成部分。安装对象包括"上级通讯代理的安装"和"下级通讯代理的安装"。这两个模块的安装相互独立,安装时不存在先后顺序。

7.1.2 安装环境

📖 对服务器系统资源的要求：

- ◆ Intel 奔腾 500MHz 或更快的处理器
- ◆ 工作站 64MB 以上内存，服务器 128MB 以上内存
- ◆ 显卡：标准VGA，256色显示模式以上
- ◆ 120MB 以上硬盘可用空间

📖 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 2003 Server

客户端系统：

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

📖 对通信协议的要求：

TCP/IP

7.1.3 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，您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。

7.1.4 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单中心系统的通讯，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。

在安装上级通讯代理之前必须保证已经安装了瑞星杀毒软件网络版。安装上级通讯代理的机器不必限于系统中心所在的机器，可以安装在该网段任何一个客户端上。

7.1.4.1 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机器上。
- 全天候开机：为确保正常实现多网段通讯和管理，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。

7.1.4.2 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：

- (1) 将瑞星杀毒软件网络版安装光盘放入本机的光驱内；
- (2) 进入安装程序界面，选择【安装多中心组件】（如图 124）；

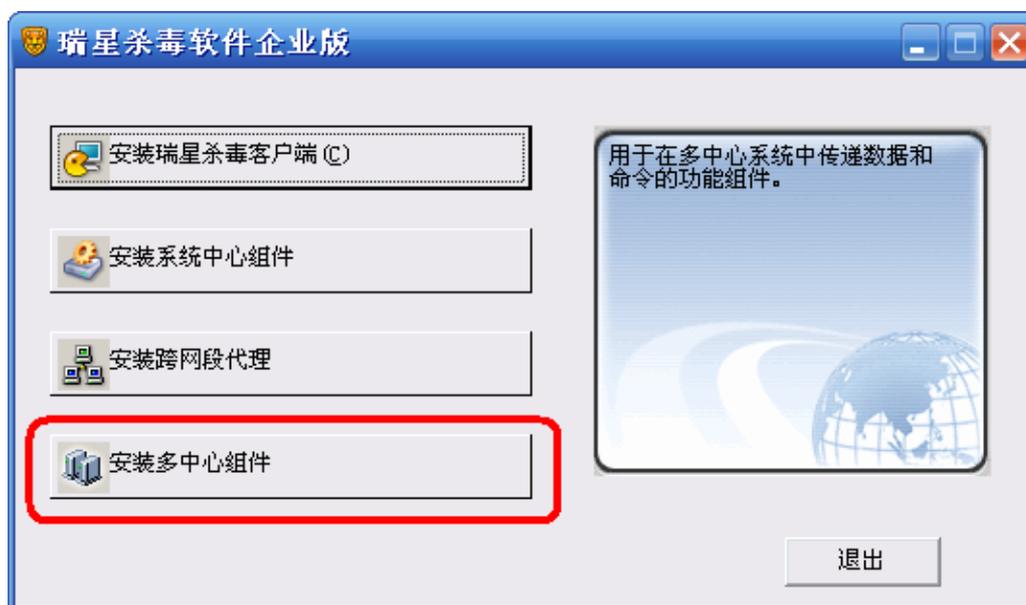


图 124

- (3) 在【定制安装】画面中，选择【上级通讯代理】，按【下一步】继续安装（如图 125）；

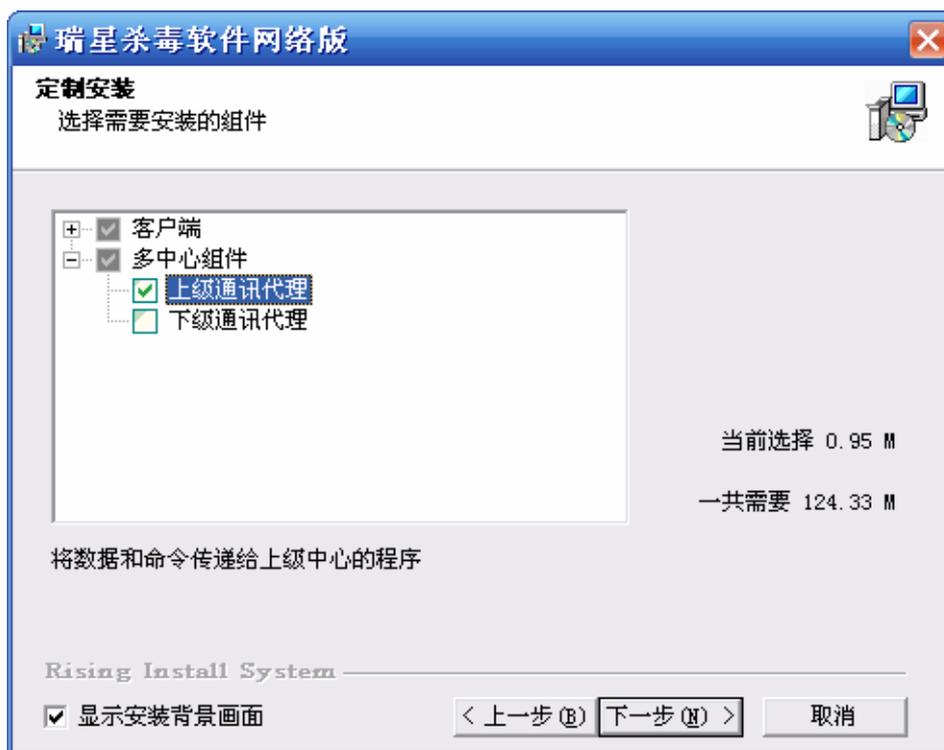


图 125

(4) 在【网络参数设置】画面中，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，按【下一步】(如图 126)；



图 126

特别提示:

- 上级通讯代理【指向的 RavSendre 端口】的配置必须与在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【监听端口】；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。

- 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。

(5) 在【准备好安装】画面中，确认【当前设置】的信息无误后，按【下一步】继续安装（如图 127）



图 127

(6) 文件复制结束后，点击【完成】按钮结束安装（如图 128）；

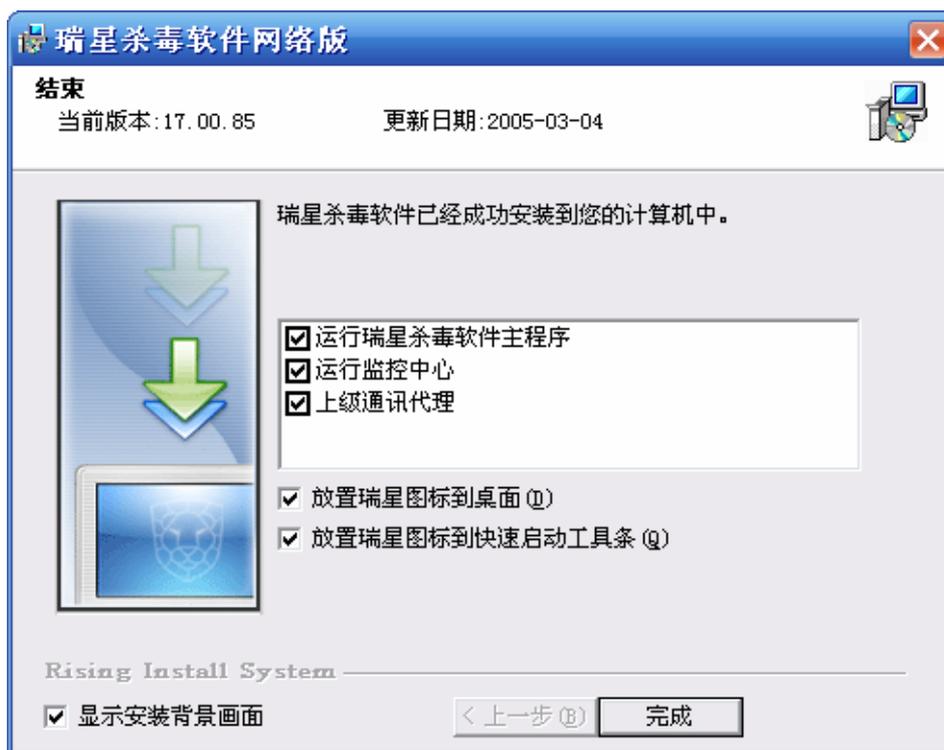


图 128

7.1.5 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机器不必限于系统中心所在机器，可以安装在该网段任何一个客户端上。

7.1.5.1 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：为确保正常实现多网段通讯和管理，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机器上。

7.1.5.2 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了，再进行以下安装步骤：

- (1) 将瑞星杀毒软件网络版安装光盘放入本机的光驱内；
- (2) 进入安装程序界面，选择【安装多中心组件】；
- (3) 在【定制安装】画面中，选择【下级通讯代理】，按【下一步】继续安装（如图 129）；

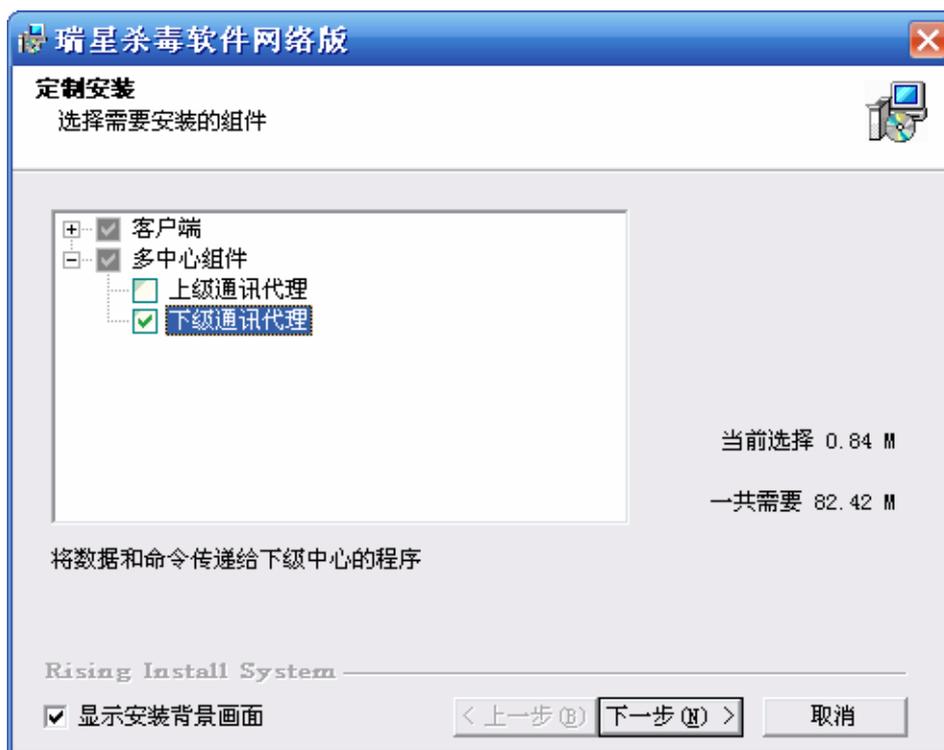


图 129

(4) 在【网络参数设置】画面中，填写下级通讯代理的监听端口，按【下一步】(如图 130)；



图 130

特别提示：

- 下级通讯代理【监听端口】的配置必须与在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。

- 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。

(5) 文件复制结束后，点击【完成】按钮结束安装。

7.2 卸载

通过瑞星杀毒软件网络版的【添加删除组件】，可以添加或者删除上级通讯代理和下级通讯代理组件。详细的卸载步骤请参阅“4.16 添加删除、修复和卸载”小节。

7.3 多级中心系统的网络安全管理

7.3.1 概述

通过上级通讯代理和下级通讯代理之间的通讯，超级管理员可以利用管理控制台对下级中心系统进行反病毒管理，实现全网统一查杀、全网实时监控统一控制、全网查杀设置统一设定，以及客户端口令统一设置。这样全网任何一台客户端的病毒信息都能反映到装有下级通讯代理的系统中心管理控制台上。瑞星杀毒软件网络版及时地反映整个网络的安全状况，真正做到了在复杂网络环境中的网络病毒防护。

7.3.2 操作与管理

网络版多级中心系统通过管理控制台进行网络安全管理操作，大体分为两部分：一部分是针对父中心所在网段内所有客户端的操作，另一部分是对下级系统中心的全局操作。对下级系统中心的操作是一种全局操作，而不支持对下级系统中心某个客户端的操作，也就是说上级中心对下级中心的操作是对下级管理的客户端的一个集体行为，比如查杀毒、开启/关闭实时监控、查看历史纪录都是对下级系统中心所有客户端的操作。

注意：管理控制台的分组管理策略不支持对上级通讯代理的操作，即上级通讯代理只能存在剩余组里，不能分组到用户新建组中。同时，上级通讯代理只能存在于管理员组里，无法被分组到新建管理员组里。

7.3.2.1 对下级系统中心的查杀毒

打开控制台，点选代表上级通讯代理的客户端，再选择工具栏里的  按钮，将会弹出查杀毒界面。

注意: 对上级通讯代理的查杀毒操作实际是针对安装下级中心所在网段的全部客户端进行操作。

7.3.2.2 对下级系统中心的实时监控

打开控制台，点选代表上级通讯代理的客户端，选择工具栏里的  按钮，将会全面启动

下级中心系统的实时监控；点击工具栏里的  按钮，将会全面关闭下级中心系统的实时监控。

注意: 对上级通讯代理的开启/关闭实时监控操作实际上是针对安装下级中心所在网段的全部客户端进行操作。

7.4 升级

当安装完瑞星杀毒软件网络版多级中心系统后，升级工作应该是您首先进行的重要工作。杀毒软件的特性决定了升级操作所处的重要地位。能够方便的利用互联网进行实时更新软件的版本，自动分发升级程序到全网段所有的客户端是瑞星杀毒软件升级系统的一大特色。

提示: 强烈建议您把您的瑞星杀毒软件升级到最新版本，并进行全网杀毒，以保障您目前的网络处于安全的状态。

有的系统中心无法从瑞星网站直接升级，而多级中心系统很好的解决了这个问题。只要最高一级的中心与 Internet 连接，则访问瑞星网站就能够直接升级到最新版本。而对下级中心而言，既可以从它的上一级中心智能升级到最新版本，又可以通过 Internet 升级到最新版本。

第八章 客户服务

本着“客户的需求就是瑞星的服务”的宗旨，瑞星提出了“以客户为中心，创瑞星服务品牌”的口号。长期以来一直以品牌化的标准不断规范和完善我们的服务工作，力图以快速、准确、完善的服务解决用户遇到的相关问题。自瑞星公司成立以来，我们以谨慎负责的工作态度，一丝不苟的工作精神博得了广大客户的信任与支持。在瑞星的眼中客户是永恒的上帝，客户需要的就是我们努力的方向。

今天，瑞星的客户服务队伍已经从最早成立的几个人发展到拥有完善的客户服务体系，专业、先进的软硬件设备和几十名资深技术工程师的专业服务队伍。这支队伍团结有序、分工明细，在不同领域满足着用户不同的需求。随着瑞星公司的不断壮大，瑞星服务体系也不断完善，服务项目不断增多，“瑞星服务”在用户心目中正在占据着越来越重要的位置。

客户的需求就是我们的服务，在瑞星公司向着国际信息安全市场全面进军的进程中，我们将一如既往地以客户为中心，不断完善、拓展我们的服务项目和服务范围，实现服务的多样化、贴身化、实用化。为您提供更加及时、专业、完整的服务，让您有限的投入换回无限的价值！

详细服务信息请参见《客户服务指南》。

附录一 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、繁体中文和英文三个版本，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，在线订购相应产品。

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，提醒您不断进行软件的升级更新，避免遭到病毒的侵袭。

瑞星社区（艾卡卡社区）是国内最热门的信息安全专业交流社区，每天有数千名热心网友在各个板块进行交流。在这里您可以反映您遇到的问题，也可以提出建议与意见，还可以同大家作朋友。

附录二 如何有效防范病毒

- 1、在计算机上安装杀毒软件和防火墙软件；
- 2、及时升级。瑞星杀毒软件目前提供每个工作日升级一次的服务，在病毒盛行期间或者病毒突发的非常时期，瑞星杀毒软件可能会每天升级一次甚至一天升级数次，以保证您的计算机受到持续地保护；
- 3、下载瑞星流行病毒专杀工具（免费）。一旦爆发恶性病毒，我们会在第一时间在瑞星网站（[Http://www.rising.com.cn](http://www.rising.com.cn)）上提供专杀工具免费下载，针对性强，速度快，防止疫情扩散；
- 4、开启瑞星计算机监控功能。系统启动后立即启用计算机监控功能，防止病毒侵入计算机（提示：瑞星计算机监控是用户实时的、多层级的病毒防御体系，关闭瑞星计算机监控将大大增加病毒侵入的风险。建议开启计算机监控并设置密码以防止别人关闭）；
- 5、定期全面扫描一次系统（建议个人计算机每周一次，服务器每天深夜全面扫描一次系统）；

- 6、复制任何文件到本机时，建议使用瑞星杀毒软件右键查杀功能进行专门查杀；
- 7、以纯文本方式阅读信件，不要轻易打开电子邮件附件，建议启用瑞星杀毒软件邮件监控功能；
- 8、从互联网下载任何文件时，请检查该网站是否具有安全认证。在通过实时通讯软件（如 MSN Messenger）传送文件或者从互联网下载文件时，建议使用瑞星杀毒软件嵌入式杀毒工具，接收文件后自动调用瑞星杀毒软件扫描病毒；
- 9、请勿访问某些可能含有恶意脚本或者蠕虫病毒的网站，建议启用瑞星杀毒软件网页监控功能；
- 10、及时获得反病毒预报警示。在病毒爆发前，用户可通过浏览瑞星反病毒资讯网站（[Http://www.rising.com.cn](http://www.rising.com.cn)）、浏览瑞星杀毒软件主界面中的信息中心或者手机短信（瑞星短信通用户）来获得病毒爆发的预报信息；
- 11、使用 Windows Update 更新操作系统，或者使用瑞星系统漏洞扫描工具及时下载并打补丁程序；
- 12、使用瑞星个人防火墙软件，防止黑客程序侵入计算机。

附录三 如何降低由病毒破坏所引起的损失

- 1、从“干净”（未感染病毒）的系统中创建应急启动盘，若 Windows 操作系统不能启动，可使用瑞星杀毒软件 DOS 杀毒工具软盘启动系统；
- 2、定期备份硬盘数据。万一发生硬盘数据损坏或丢失，可使用瑞星杀毒软件的硬盘数据备份功能恢复数据；
- 3、向瑞星客户服务中心请求支援，您可以通过电子邮件、电话或上门等方式进行求助，瑞星技术服务工程师将为您提供专业化的服务，尽量减少由病毒破坏带来的损失。

附录四 瑞星全线产品列表

■反病毒产品

- 瑞星杀毒软件单机版
- 瑞星杀毒软件网络版
 - for Windows
 - ◆ 中小企业版
 - ◆ 企业版
 - ◆ 大型企业版

- ◆ 专用版
- ◆ 网吧版
- for Unix
- for Exchange
- for Domino
- 无毒邮箱中间件
- 瑞星杀毒软件 OEM 版
- 瑞星杀毒软件 for Linux
- 瑞星杀毒软件 for PDA
- **网络安全产品**
- 瑞星个人防火墙(软件)
- 瑞星企业级防火墙(硬件)
 - 瑞星企业级千兆防火墙 RFW-1000
 - 瑞星企业级百兆防火墙 RFW-100+
 - 瑞星全功能 NP 防火墙 RFW-SME
- 瑞星企业级入侵检测系统 RIDS-100
- 瑞星网络监控系统 RNM-100
- 瑞星网络隐患扫描系统
- 瑞星 VPN 解决方案
- 瑞星防毒墙
 - 瑞星防毒墙 RSW-1000
 - 瑞星防毒墙 RSW-3000
 - 瑞星防毒墙 RSW-9000

附录五 瑞星杀毒软件网络版产品系列

根据客户网络规模的大小，瑞星公司推出了网络版系列产品，包括：大型企业版、企业版、专用版、中小企业版和网吧版。这些产品间的区别是：

- **大型企业版：**拥有网络版系列产品的所有功能，可控制下级系统中心，可直接控制下级系统中心的任一个客户端；

- **企业版:** 多个企业版可组建呈树状结构的多级系统中心, 上级系统中心可控制下级系统中心, 但不能直接控制下级系统中心的客户端, 客户端数量无限制;
- **专用版:** 与企业版属同级产品, 但在功能设计上是根据用户需求来定制的;
- **中小企业版:** 不支持多个中小企业版系统中心之间的通讯;
- **网吧版:** 与中小企业版属同级产品, 支持在 Windows 9x 操作系统下安装系统中心, 但不支持远程安装瑞星杀毒软件、远程查杀和远程设置。

附录六 北京瑞星科技股份有限公司简介

北京瑞星科技股份有限公司, 前身为北京瑞星电脑科技开发有限责任公司, 成立于 1991 年 11 月, 于 1998 年 4 月改制为股份公司, 是中国最早从事计算机病毒防治与研究的专业软件公司, 研制生产涉及计算机反病毒和信息安全相关的全系列产品, 目前已自主研发成功基于多种操作系统的瑞星杀毒软件单机版、网络版、企业级防火墙、入侵检测、漏洞扫描等系列信息安全产品。

瑞星公司是目前中国最大的提供全系列反病毒及信息安全产品的专业厂商, 软件产品全部拥有自主知识产权; 在 2000 年中国公安部组织的所有在中国境内销售的病毒防治产品统一标准评测中, “瑞星杀毒软件”单机版、网络版双双荣获总分第一的殊荣, 是中国主流的信息安全产品和服务提供商。

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。

瑞星公司针对计算机病毒的防治, 先后建立了“全球计算机病毒监测网”、“全球计算机病毒应急处理网”、“全国计算机病毒预报网”和“全国反病毒服务网”四大网络体系, 同时组建了畅通的软件销售渠道, 具备强大的市场营销能力。通过这些年来发展, 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。