网络版介绍及个性化全局策略

网络版产品介绍

- 目前瑞星网络版产品的种类
- 网络版的授权方式
- 网络版产品与单机版产品的区别

网络版产品介绍

- 目前瑞星网络版产品的种类

小型企业版

中小企业版(一年/三年)

企业版

高级企业版

企业专用版

教育专用版

高级企业专用版

瑞星网络版的产品介绍

- **小型企业版：** 专为小企业设计，成本可控，使用简便，查杀能力强。
- **中小企业版：** 易部署、易安装、易管理，适用于中小企业网络。
- **企业版：** 拥有强大的管理和木马查杀能力，适用于大中型企业网络。
- **高级企业版：** 适用于大型复杂网络环境。分层网络防毒体系， 支持跨级管理。
- **企业专用版：** 拥有强大的管理和木马查杀能力，适用于大中型企业网络（可定制）
- **教育专用版：** 针对复杂的校园网络环境需求，量身定制的专用版本。
- **高级企业专用版：** 适用于大型复杂网络环境（电信、银行等）。分层网络防毒体系，支持跨级管理。

瑞星网络版的产品线

网络版的授权方式：

1+1+100

代表

一个系统中心，一个服务器端，100个客户端授权

网络版与单机版的区别

- **架构**

系统中心、服务器端、客户端

系统中心： 网络版核心主控系统，负责管理维护服务器端与客户端的信息

服务器端： 防病毒子系统，针对微软server内核的系统

客户端： 防病毒子系统，普通的非server内核系统

瑞星网络版的安装

系统中心安装

系统环境要求:

系统中心必须安装在服务器上，此处的服务器指计算机的操作系统必须是 Windows 2000 server / 2003 server / 2008 server(NT不支持)。

硬件环境要求:

Intel 奔腾 800MHz或更快的处理器

256MB以上内存，建议512MB

显卡：标准VGA，800X600以上分辨率，16K真彩色显示模式

500MB以上硬盘可用空间

对网络通信协议的要求:

支持TCP/IP双向通讯，服务器和客户端双向能够Ping通。

瑞星网络版的安装

系统中心

1）需一个固定的IP地址，不能随意更改；

2）server内核的操作系统；

3）需与客户端互联通讯的网络环境；

瑞星网络版的安装

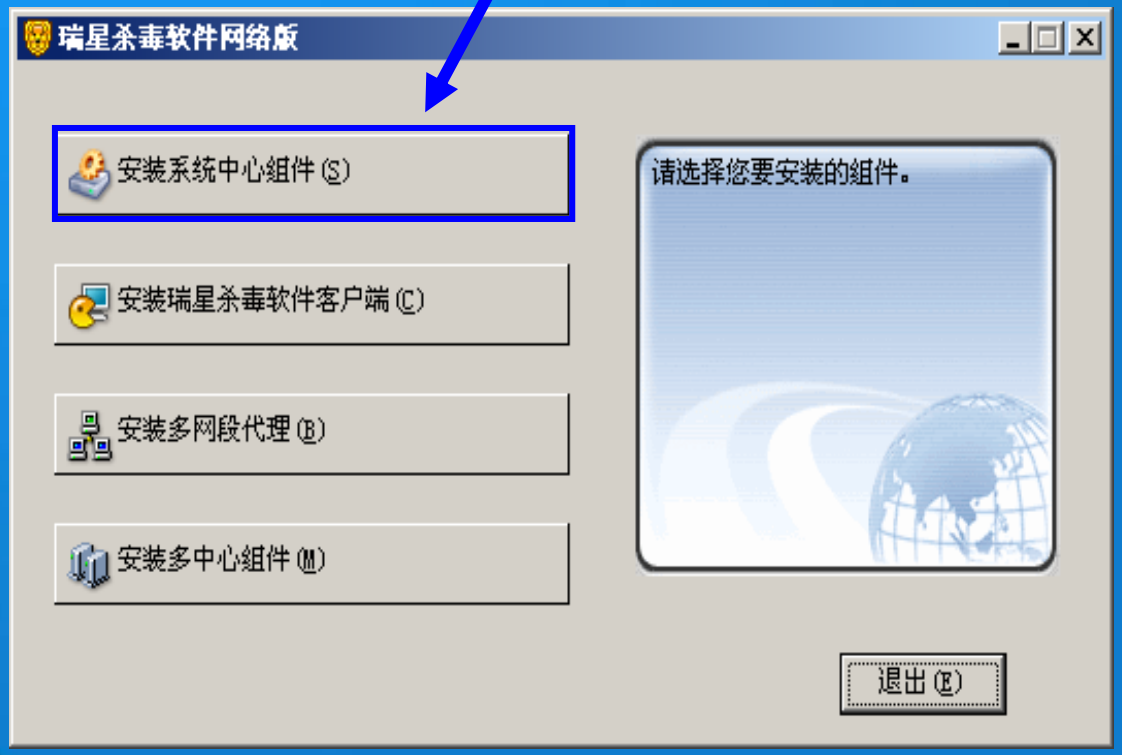
数据库安装

1）安装包里自带MSDE数据库引擎，安装后桌面右下角有SQL图标，但没绿色箭头；

2）支持SQL SERVER数据库，安装中心前需进行安装，在安装过程中选择SQL；

瑞星网络版的安装

选择安装系统中心组件



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

瑞星网络版的安装

服务器端/客户端的安装——本地安装

服务器端与客户端安装一样，根据操作系统类型智能判别

瑞星网络版的安装

客户端安装方式

1)手动本地安装

2)登陆域的脚本安装

3)WEB安装

4)远程安装（仅支持NT内核）

瑞星网络版的架构与拓朴

系统中心与服务器端及客户端属C/S架构

client端　服务器端与客户端

server端　系统中心

瑞星网络版支持多复杂网络环境，包括异网段，VPN连接等模式；

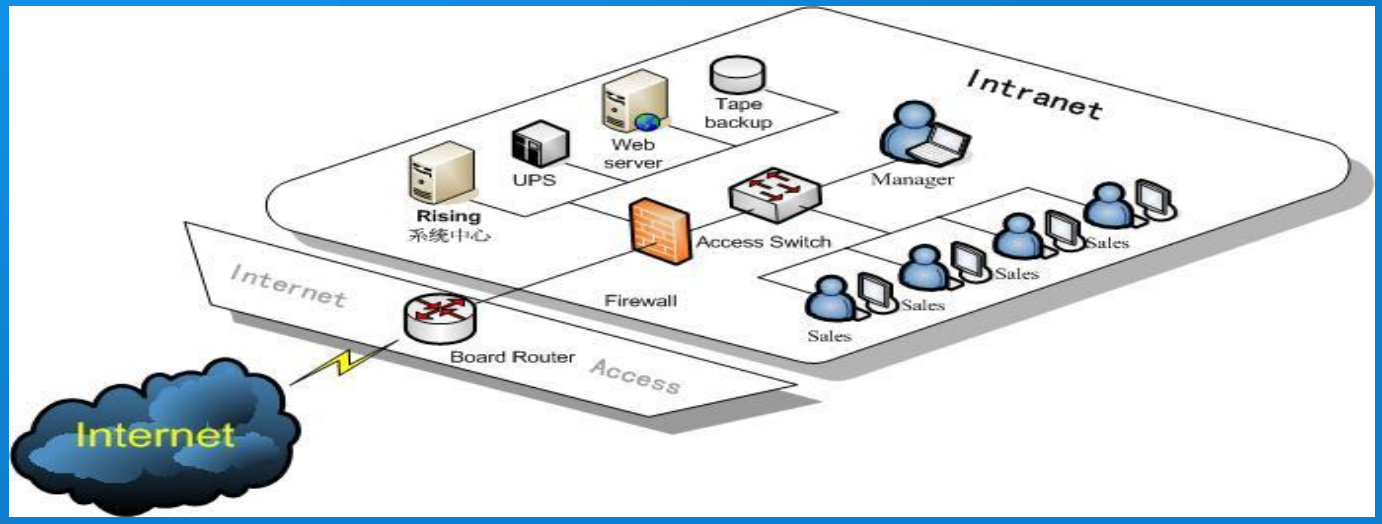
瑞星网络版的架构与拓朴

安装前注意事项　网络防火墙配置：

双向开启

TCP：（1976－1983)

UDP：（7273－7282）



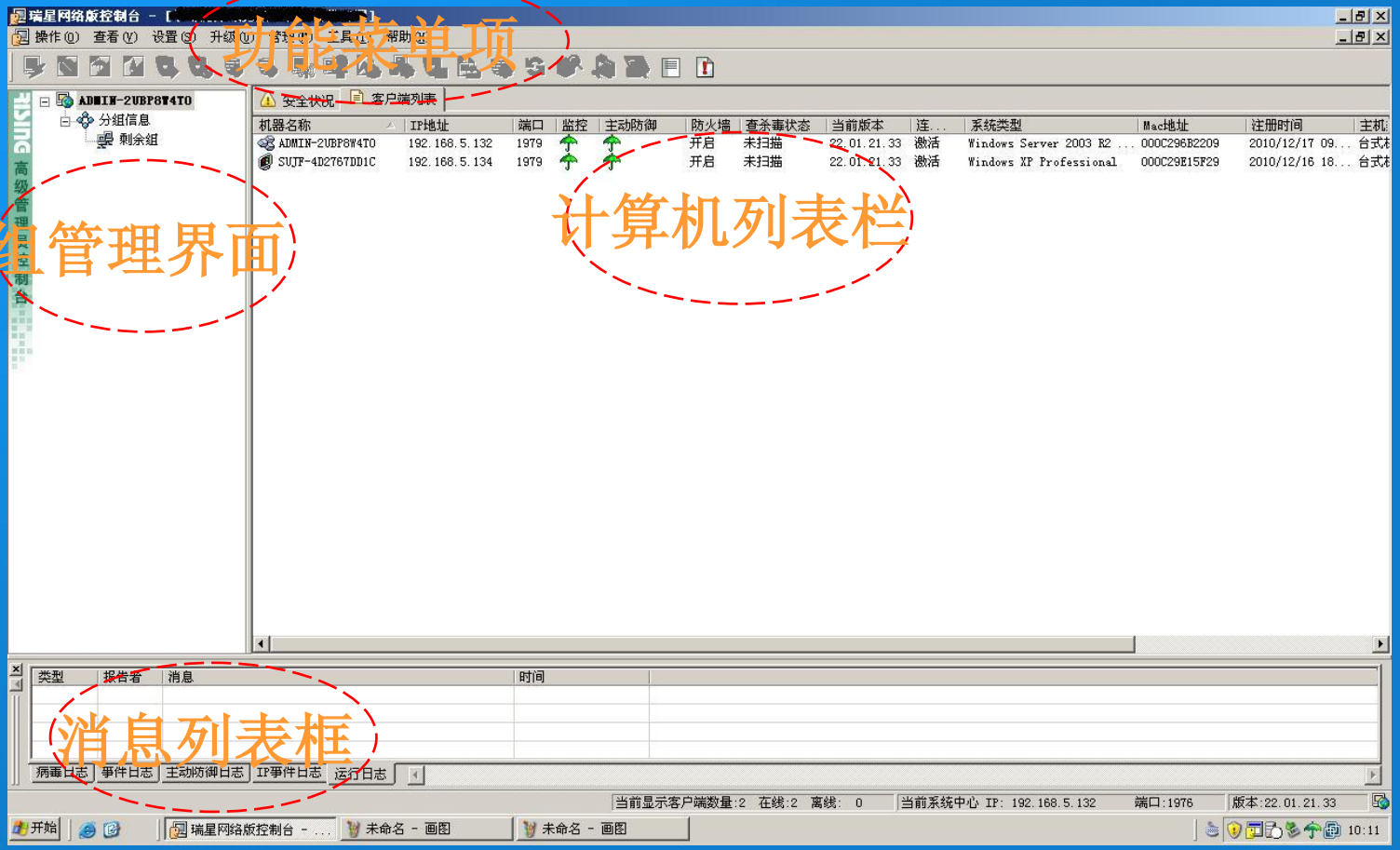
瑞星网络版使用说明

瑞星管理控制台概述

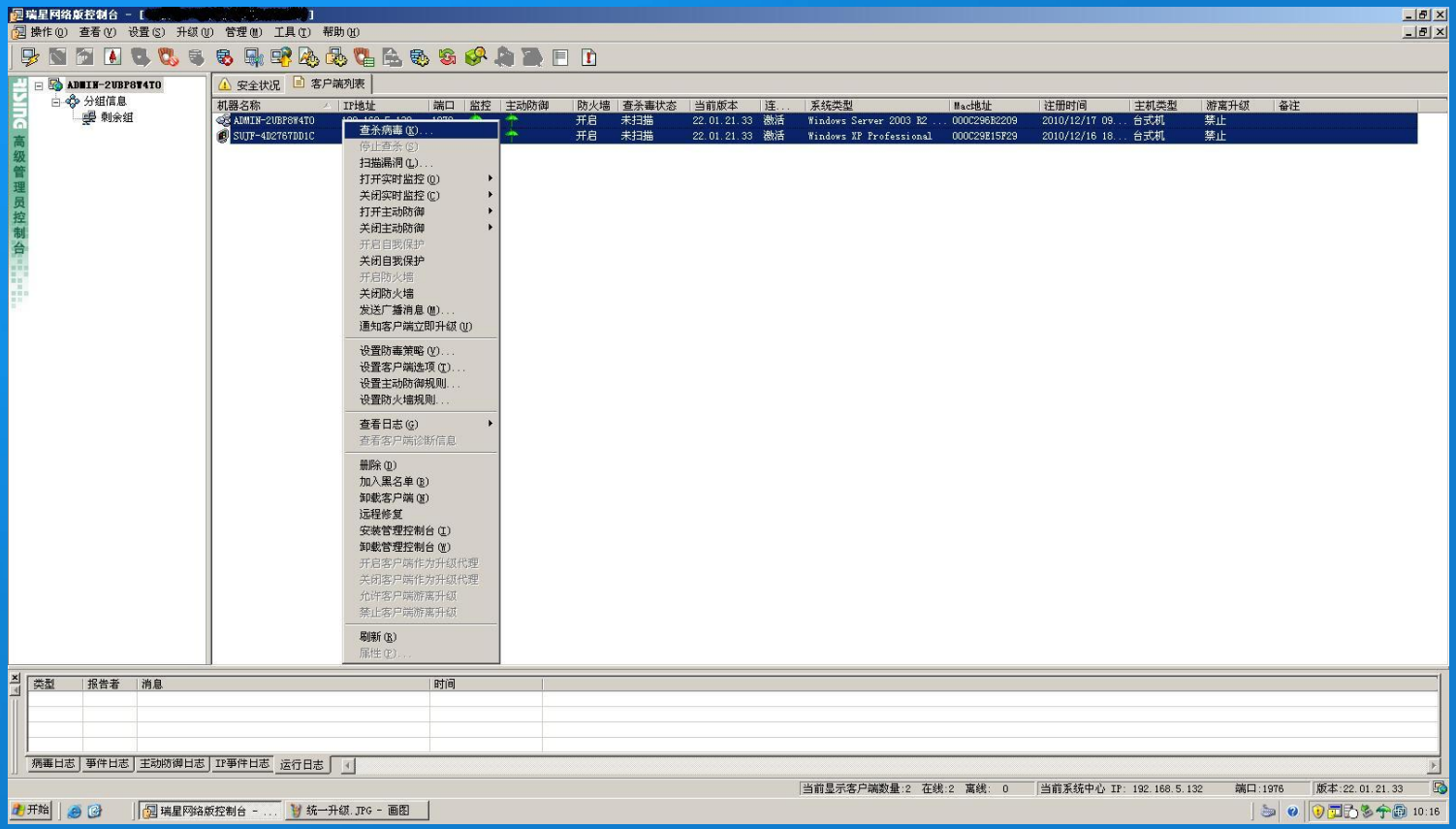
- 管理控制台是在网络上集中管理所有安装有瑞星杀毒软件网络版客户端软件的计算机的管理工具。通过管理控制台可以了解整个网络中的总体安全状况并且远程管理网络中的任何一台计算机中的瑞星杀毒软件。
- 网络上任何一台计算机的病毒警告信息都能在管理控制台得到汇总，通过管理控制台也能直观地查看网络上所有计算机当前的实时监控状态、病毒查杀情况、主动防御状态和当前版本信息等。
- 管理控制台能对远程计算机安装瑞星杀毒软件和移动管理控制台，让管理控制台自由移动到管理员认为合适的计算机上去。管理员通过对管理控制台的操作就能对网络上所有计算机进行定期、实时地查杀病毒和全网统一升级管理，真正做到在整个网络中建立起坚实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

控制台的登陆

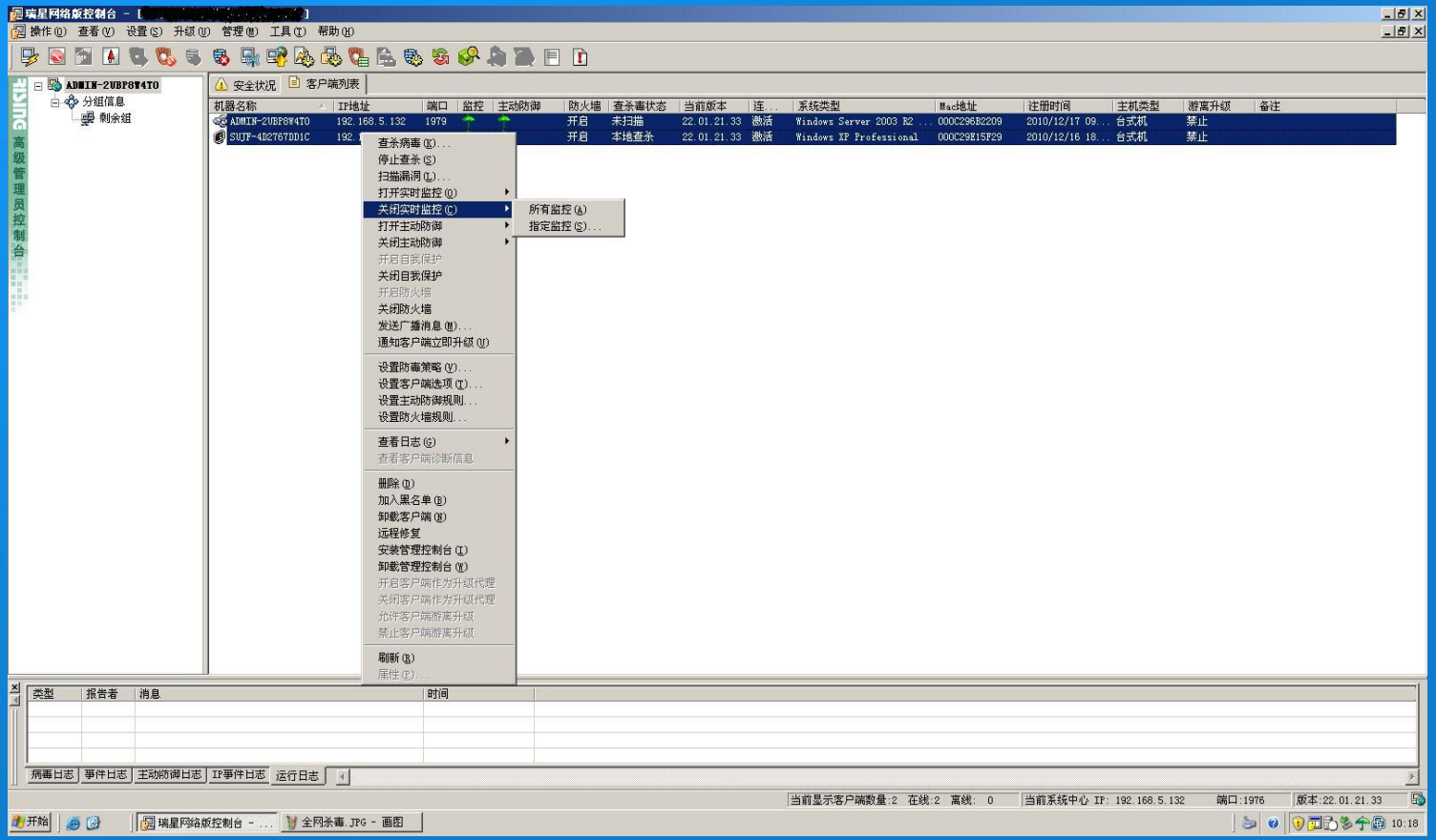
管理控制台的使用


功能菜单项
组管理界面
计算机列表栏
消息列表框
瑞星网络版控制台
操作(O) 查看(V) 设置(S) 升级(U) 工具(T) 帮助(H)
ADMIN-2UBP8W4TO
分组信息
剩余组
安全状况
客户端列表
机器名称 IP地址 端口 监控 主动防御 防火墙 查杀毒状态 当前版本 连... 系统类型 Mac地址 注册时间
ADMIN-2UBP8W4TO 192.168.5.132 1979 开启 未扫描 22.01.21.33 激活 Windows Server 2003 R2 ... 000C296B2209 2010/12/17 09... 台式
SUJF-4D2767DD1C 192.168.5.134 1979 开启 未扫描 22.01.21.33 激活 Windows XP Professional 000C29E15F29 2010/12/16 18... 台式
类型 报告者 消息 时间
病毒日志 事件日志 主动防御日志 IP事件日志 运行日志
当前显示客户端数量:2 在线:2 离线: 0
当前系统中心 IP: 192.168.5.132 端口:1976
版本:22.01.21.33
开始
瑞星网络版控制台 - ...
未命名 - 画图
未命名 - 画图
10:11

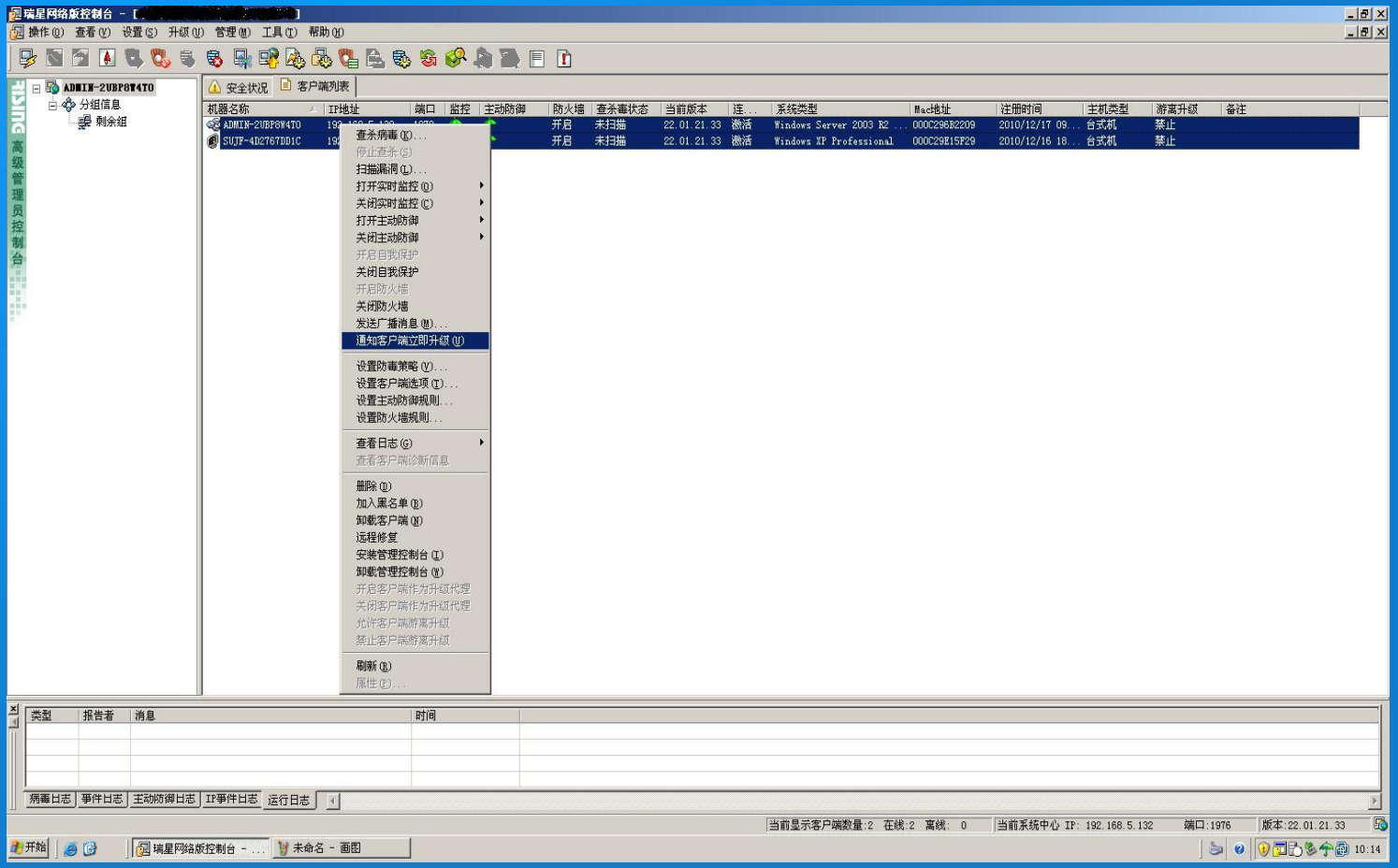
实现全网同时杀毒


瑞星网络版控制台
操作(O) 查看(V) 设置(S) 升级(U) 管理(M) 工具(T) 帮助(H)
ADMIN-2UBP8W4TO
分组信息
剩余组
安全状况
客户端列表
机器名称 IP地址 端口 监控 主动防御 防火墙 查杀毒状态 当前版本 连... 系统类型 Mac地址 注册时间 主机类型 游离升级 备注
ADMIN-2UBP8W4TO 开启 未扫描 22.01.21.33 激活 Windows Server 2003 R2 ... 000C296B2209 2010/12/17 09... 台式机 禁止
SUJF-4D2767DD1C 开启 未扫描 22.01.21.33 激活 Windows XP Professional 000C29E15F29 2010/12/16 18... 台式机 禁止
查杀病毒(E)...
停止查杀(S)
扫描漏洞(L)...
打开实时监控(O)
关闭实时监控(C)
打开主动防御
关闭主动防御
开启自我保护
关闭自我保护
开启防火墙
关闭防火墙
发送广播消息(B)...
通知客户端立即升级(U)
设置防毒策略(Y)...
设置客户端选项(T)...
设置主动防御规则...
设置防火墙规则...
查看日志(G)
查看客户端诊断信息
删除(D)
加入黑名单(B)
卸载客户端(N)
远程修复
安装管理控制台(I)
卸载管理控制台(W)
开启客户端作为升级代理
关闭客户端作为升级代理
允许客户端游离升级
禁止客户端游离升级
刷新(R)
属性(P)...
类型 报告者 消息 时间
病毒日志 事件日志 主动防御日志 IP事件日志 运行日志
当前显示客户端数量:2 在线:2 离线: 0
当前系统中心 IP: 192.168.5.132 端口:1976
版本:22.01.21.33
开始
瑞星网络版控制台 - ...
统一升级.JPG - 画图
10:16

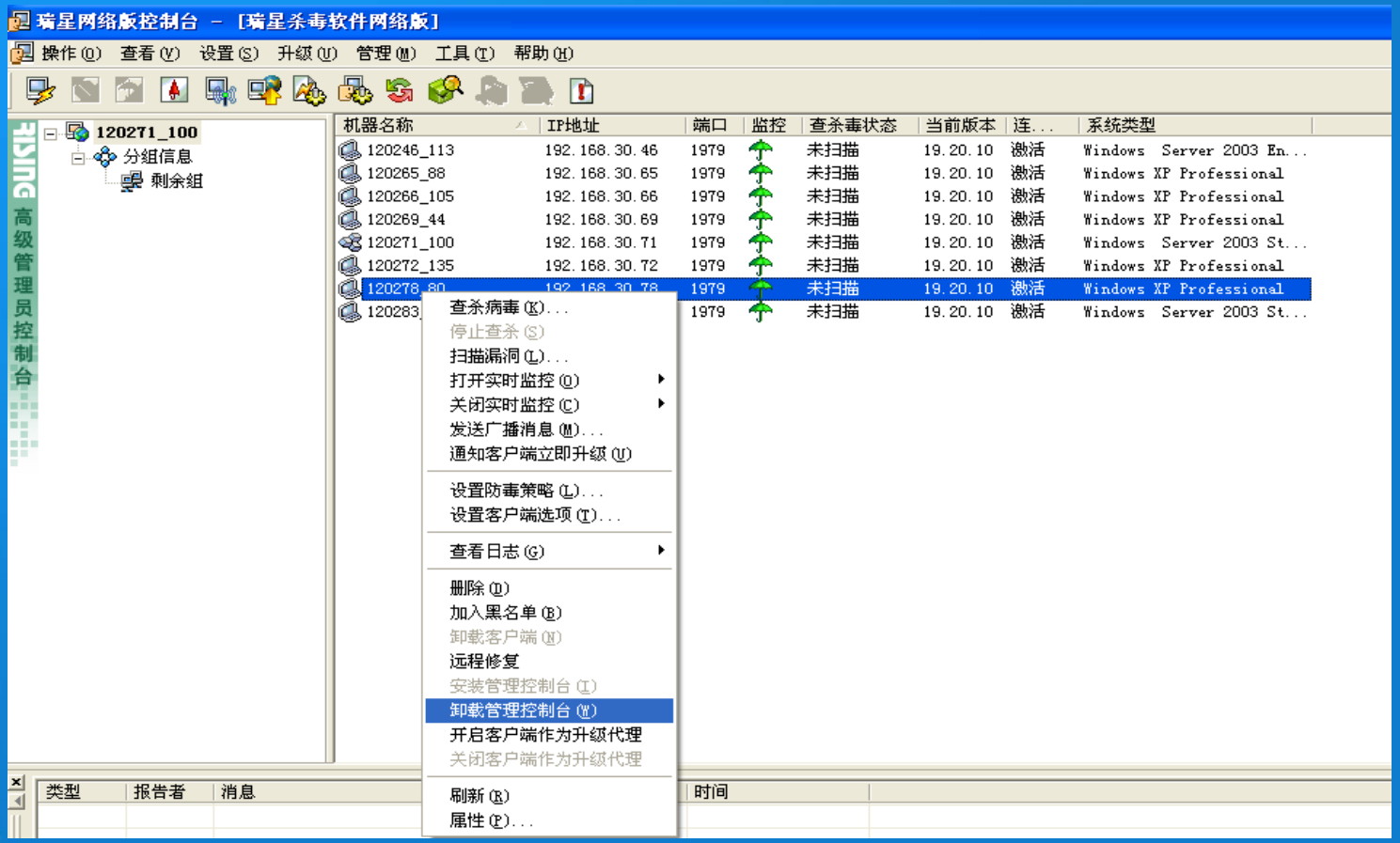
远程开启/关闭实时监控


瑞星网络版控制台
操作(O) 查看(V) 设置(S) 升级(U) 管理(M) 工具(T) 帮助(H)
高级管理员控制台
安全状况
客户端列表
机器名称 IP地址 端口 监控 主动防御 防火墙 查杀毒状态 当前版本 连... 系统类型 Mac地址 注册时间 主机类型 游离升级 备注
查杀病毒(K)...
停止查杀(S)
扫描漏洞(L)...
打开实时监控(O)
关闭实时监控(C)
打开主动防御
关闭主动防御
开启自我保护
关闭自我保护
开启防火墙
关闭防火墙
发送广播消息(M)...
通知客户端立即升级(U)
设置防毒策略(Y)...
设置客户端选项(T)...
设置主动防御规则...
设置防火墙规则...
查看日志(G)
查看客户端诊断信息
删除(D)
加入黑名单(B)
卸载客户端(M)
远程修复
安装管理控制台(I)
卸载管理控制台(W)
开启客户端作为升级代理
关闭客户端作为升级代理
允许客户端游离升级
禁止客户端游离升级
刷新(R)
属性(P)...
所有监控(A)
指定监控(S)...
类型 报告者 消息 时间
病毒日志 事件日志 主动防御日志 IP事件日志 运行日志
当前显示客户端数量:2 在线:2 离线: 0
当前系统中心 IP: 192.168.5.132 端口:1976
版本:22.01.21.33
开始
瑞星网络版控制台 - ...
全网杀毒.JPG - 画图
10:18

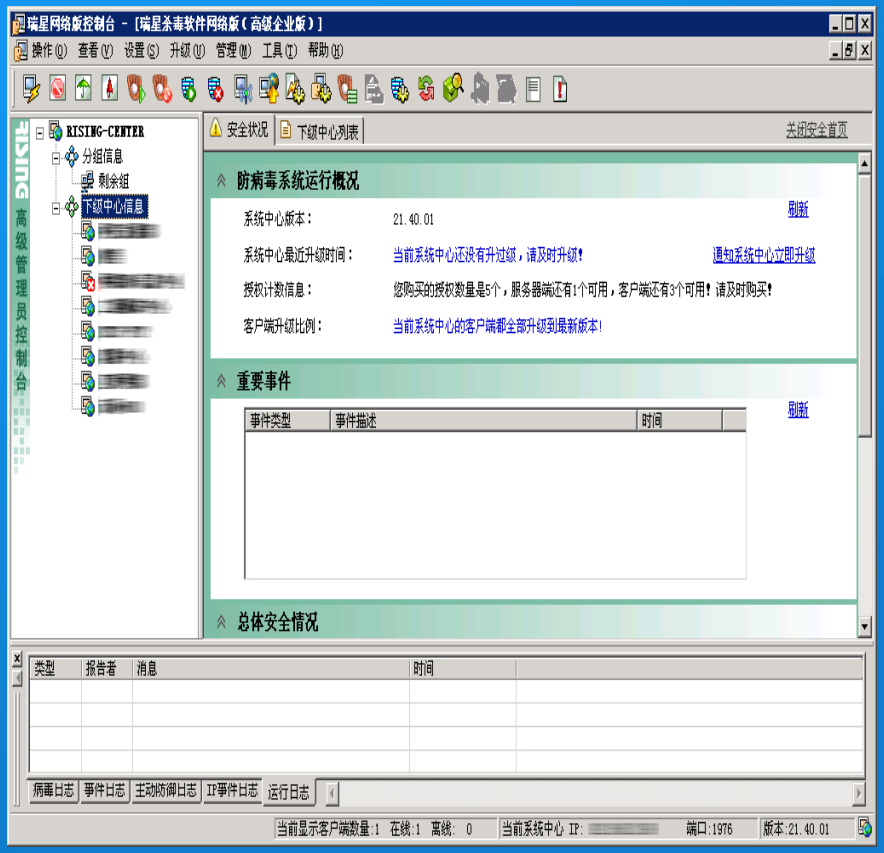
全网统一升级


瑞星网络版控制台 - [ ]
操作(O) 查看(V) 设置(S) 升级(U) 管理(M) 工具(T) 帮助(H)
ADMIN-2UBP8W4TO
分组信息
剩余组
安全状况
客户端列表
机器名称 IP地址 端口 监控 主动防御 防火墙 查杀毒状态 当前版本 连... 系统类型 Mac地址 注册时间 主机类型 游离升级 备注
ADMIN-2UBP8W4TO 开启 未扫描 22.01.21.33 激活 Windows Server 2003 R2 ... 000C296B2209 2010/12/17 09... 台式机 禁止
SUJF-4D2767DD1C 开启 未扫描 22.01.21.33 激活 Windows XP Professional 000C29E15F29 2010/12/16 18... 台式机 禁止
查杀病毒(K)...
停止查杀(S)
扫描漏洞(L)...
打开实时监控(O)
关闭实时监控(C)
打开主动防御
关闭主动防御
开启自我保护
关闭自我保护
开启防火墙
关闭防火墙
发送广播消息(M)...
通知客户端立即升级(U)
设置防毒策略(Y)...
设置客户端选项(T)...
设置主动防御规则...
设置防火墙规则...
查看日志(G)
查看客户端诊断信息
删除(D)
加入黑名单(B)
卸载客户端(N)
远程修复
安装管理控制台(I)
卸载管理控制台(W)
开启客户端作为升级代理
关闭客户端作为升级代理
允许客户端游离升级
禁止客户端游离升级
刷新(R)
属性(E)...
类型 报告者 消息 时间
病毒日志 事件日志 主动防御日志 IP事件日志 运行日志
当前显示客户端数量:2 在线:2 离线: 0
当前系统中心 IP: 192.168.5.132 端口:1976
版本:22.01.21.33
开始
瑞星网络版控制台 - ...
未命名 - 画图
10:14

远程安装卸载控制台


瑞星网络版控制台 - [瑞星杀毒软件网络版]
操作(O) 查看(V) 设置(S) 升级(U) 管理(M) 工具(T) 帮助(H)
RISING 高级管理员控制台
120271_100
分组信息
剩余组
机器名称 IP地址 端口 监控 查杀毒状态 当前版本 连... 系统类型
120246_113 192.168.30.46 1979 未扫描 19.20.10 激活 Windows Server 2003 En...
120265_88 192.168.30.65 1979 未扫描 19.20.10 激活 Windows XP Professional
120266_105 192.168.30.66 1979 未扫描 19.20.10 激活 Windows XP Professional
120269_44 192.168.30.69 1979 未扫描 19.20.10 激活 Windows XP Professional
120271_100 192.168.30.71 1979 未扫描 19.20.10 激活 Windows Server 2003 St...
120272_135 192.168.30.72 1979 未扫描 19.20.10 激活 Windows XP Professional
120278_80 192.168.30.78 1979 未扫描 19.20.10 激活 Windows XP Professional
120283 1979 未扫描 19.20.10 激活 Windows Server 2003 St...
查杀病毒(K)...
停止查杀(S)
扫描漏洞(L)...
打开实时监控(O)
关闭实时监控(C)
发送广播消息(M)...
通知客户端立即升级(U)
设置防毒策略(L)...
设置客户端选项(T)...
查看日志(G)
删除(D)
加入黑名单(B)
卸载客户端(N)
远程修复
安装管理控制台(I)
卸载管理控制台(W)
开启客户端作为升级代理
关闭客户端作为升级代理
刷新(R)
属性(P)...
类型 报告者 消息 时间

控制台安装状态



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。

网络版的升级方式

系统中心三种升级方式

1）在线智能升级

2）下载升级包手动升级

3）从上级中心升级（多中心架构）

网络版升级方式

客户端升级方式

1）根据策略自动从系统中心升级

2）通过控制台主动通知客户端升级

3）通过客户端代理中心升级

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：在高级企业版和高级企业专用版中有防火墙策略；中小企业版、企业版、企业专用版、教育专用版和小型企业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。

瑞星网络版的策略设置

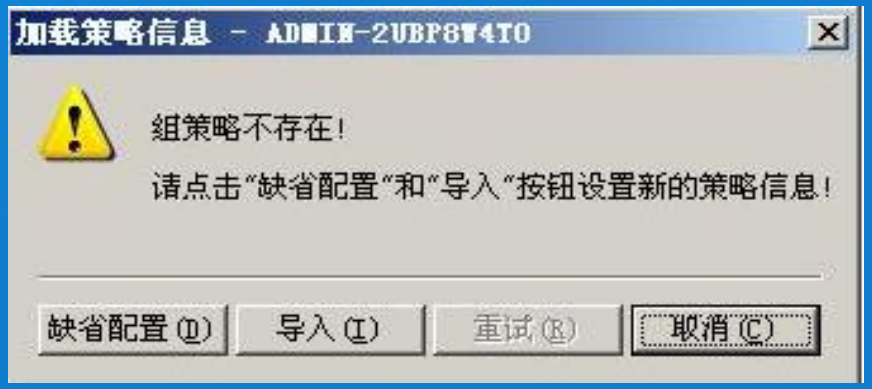
1. 如何设置防毒策略
2. 如何设置客户端选项
3. 如何设置主动防御策略
4. 如何设置防火墙规则

瑞星网络版的策略设置

设置防毒策略

- ◆病毒查杀策略（清除、删除、重启删除）
- ◆开机加载查杀任务（开机、屏保、定时）
- ◆硬盘备份分区表（不推荐使用）

重点：复合文档清除要重启，复合文件指的特定格式的压缩文件，通常由病毒制造者压缩程序使用的外壳

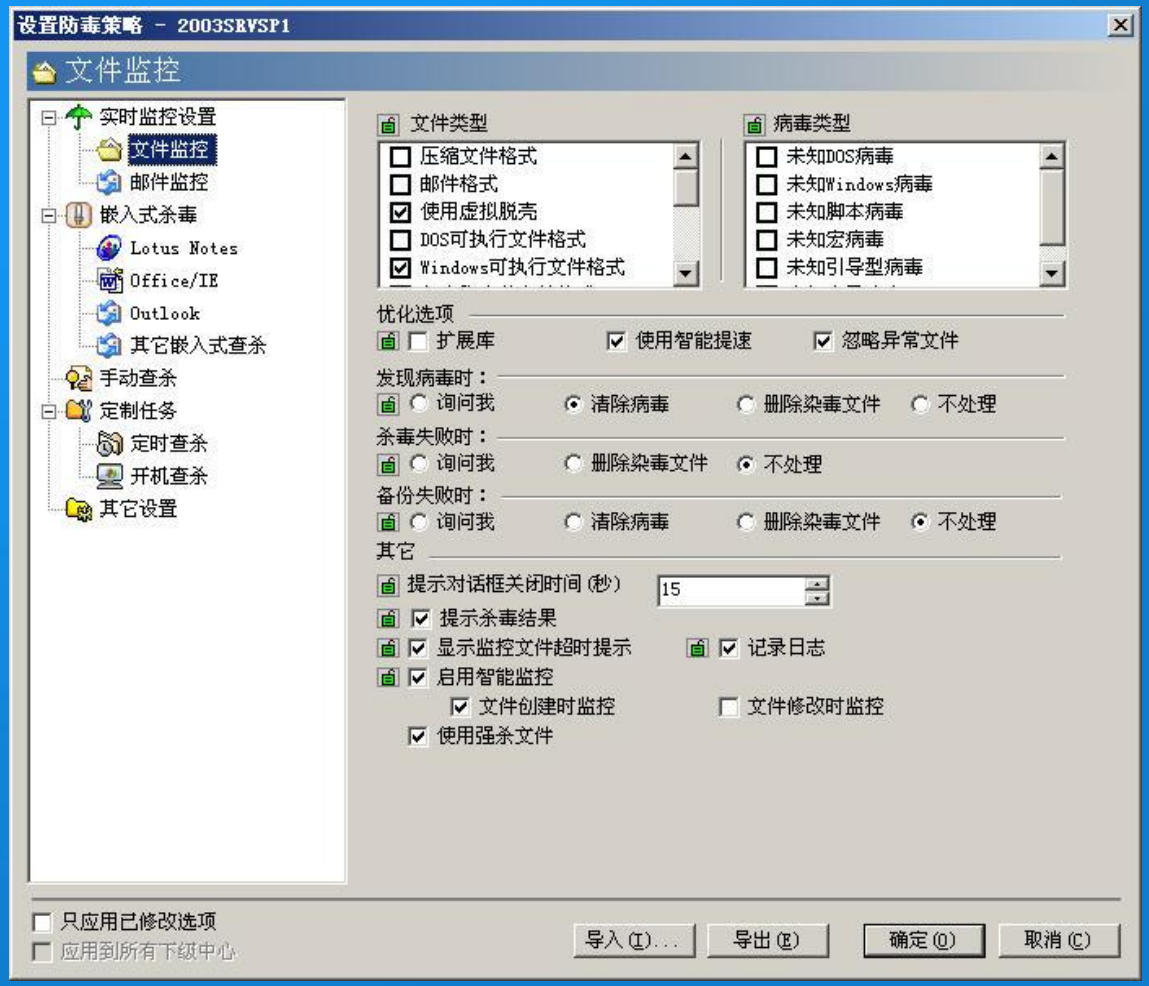


实时监控设置页面

用户可以为选中的客户端设置开机启用文件监控、邮件监控功能。

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

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：

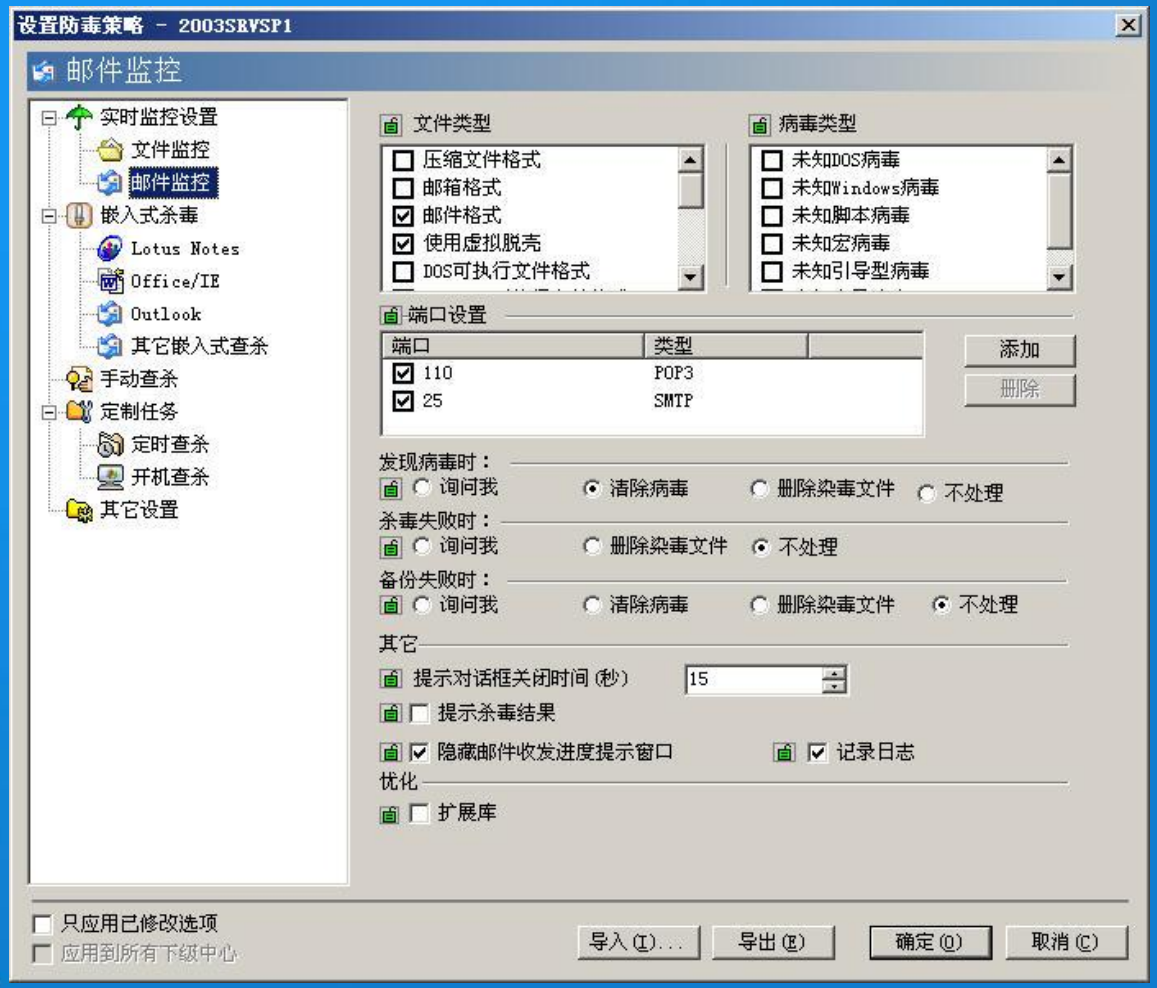
设置文件类型：可以通过【文件类型过滤选项】自定义文件类型。并可以在文件类型和病毒类型中勾选不同类型的文件进行监控。

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。

邮件监控页面



说明：中小企业版、企业版、高级企业版和小型企业版中有此设置页面；在企业专用版、高级企业专用版和教育专用版中，购买时定制了邮件监控功能的情况下有此设置页面。

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。

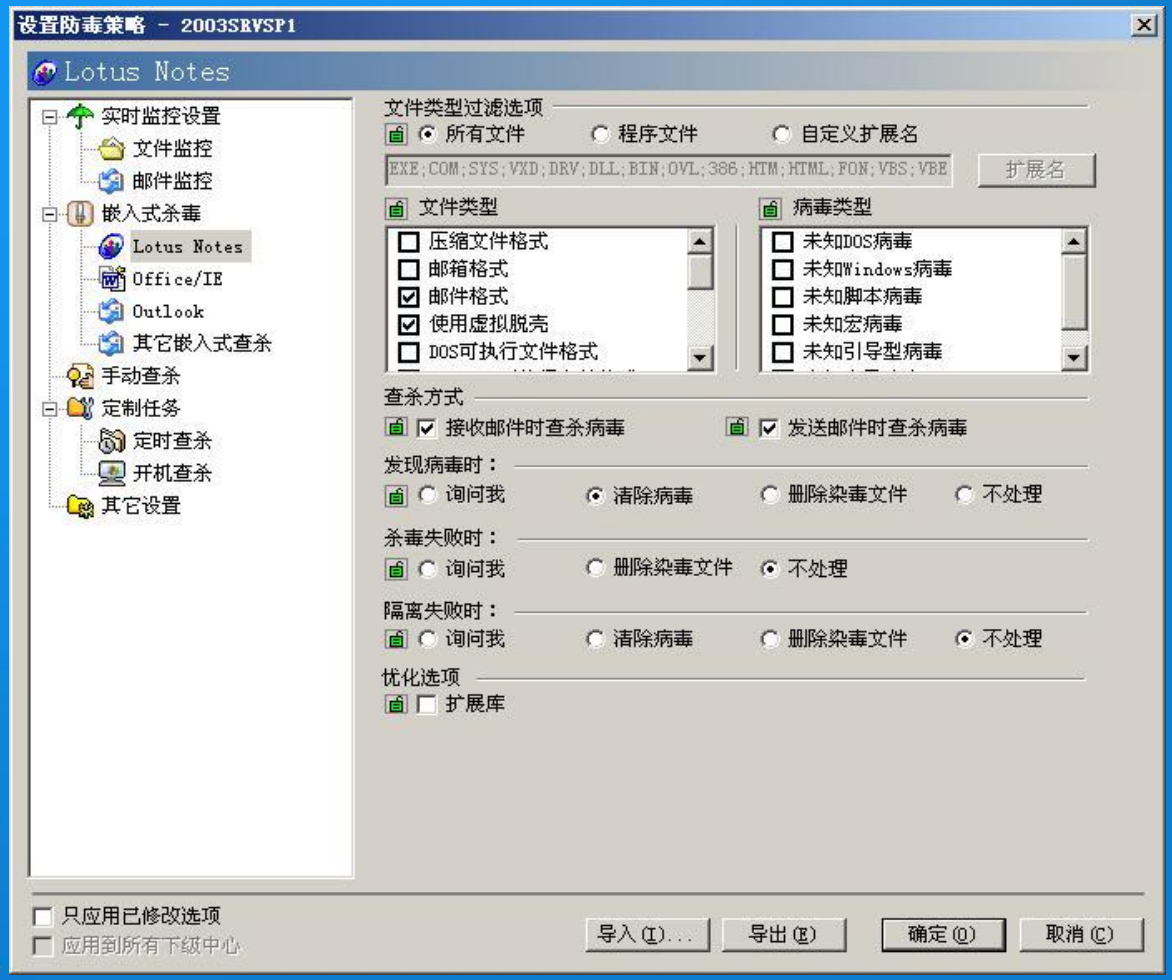
端口设置：设置邮件监控的监控端口。

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。


设置防毒策略 - ADMIN-2UBP8T4TO
嵌入式杀毒
实时监控设置
文件监控
邮件监控
嵌入式杀毒
Lotus Notes
Office/IE
Outlook
其它嵌入式查杀
手动查杀
定制任务
定时查杀
开机查杀
其它设置
使用 Lotus Notes 嵌入式杀毒
使用 Office/IE 嵌入式杀毒
使用 Outlook 嵌入式杀毒
只应用已修改选项
应用到所有下级中心
导入(I)...
导出(E)
确定(O)
取消(C)

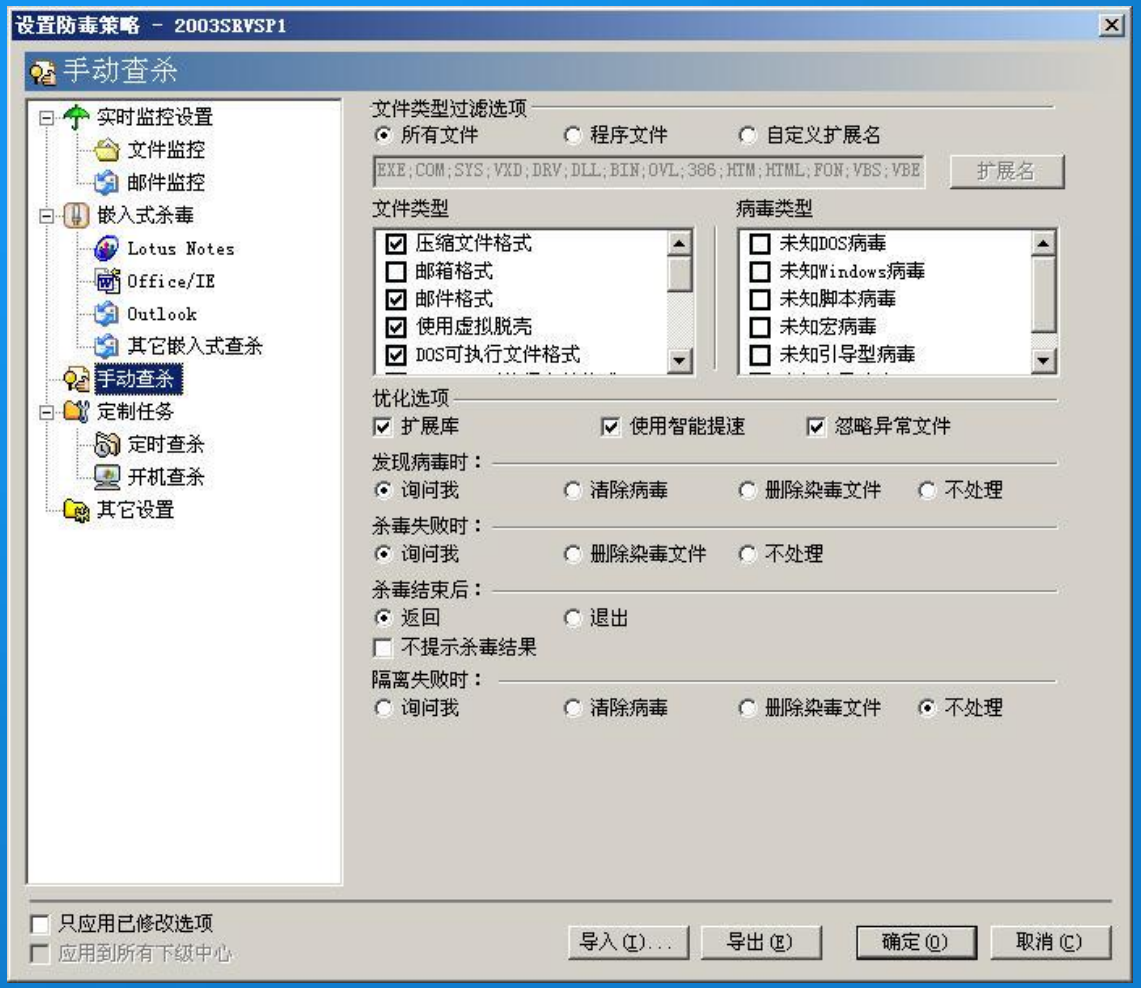
Lotus Notes页面



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。

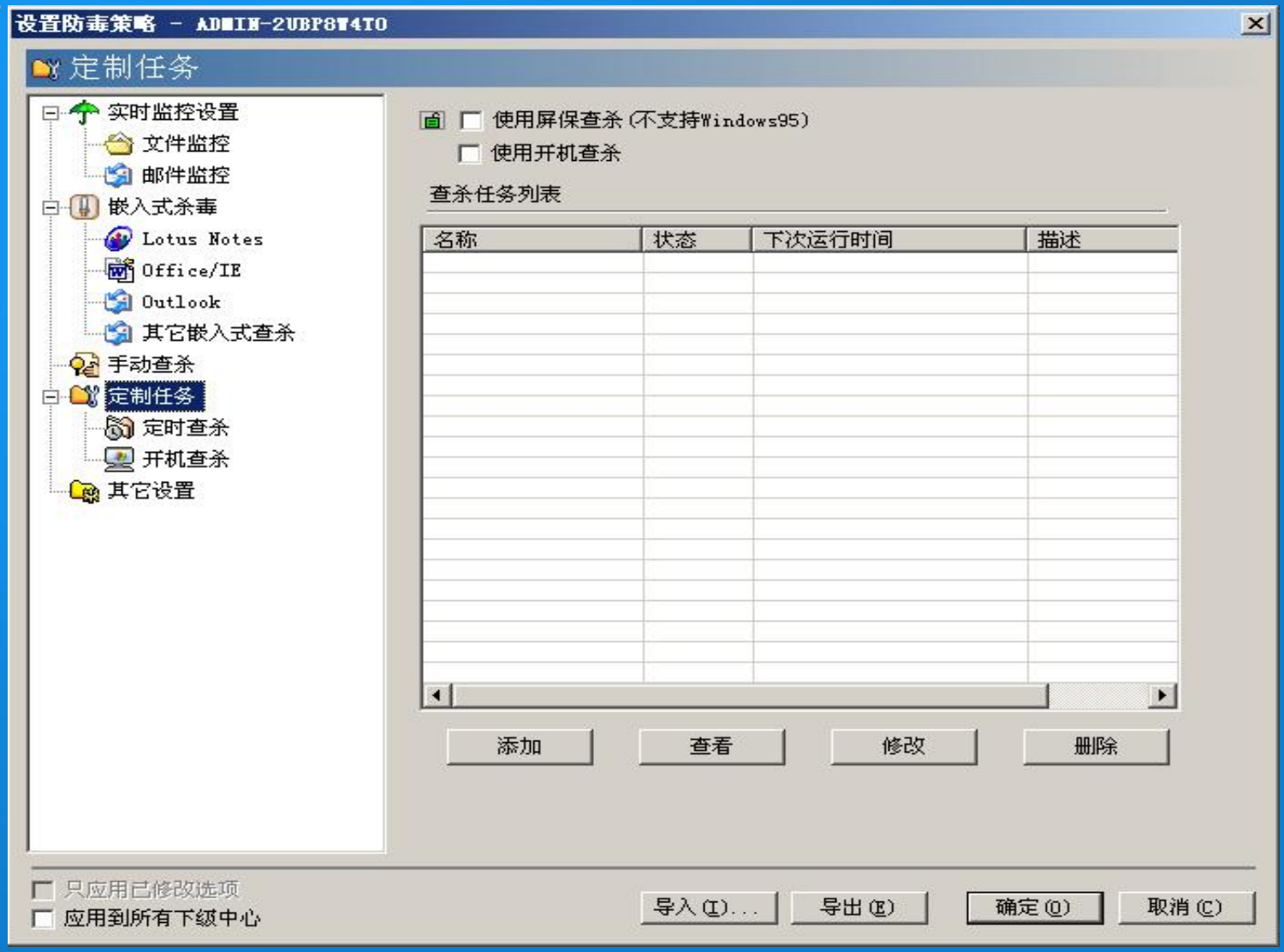
手动查杀页面



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。


设置防毒策略 - ADMIN-2UBP8W4TO
定制任务
实时监控设置
文件监控
邮件监控
嵌入式杀毒
Lotus Notes
Office/IE
Outlook
其它嵌入式查杀
手动查杀
定制任务
定时查杀
开机查杀
其它设置
使用屏保查杀(不支持Windows95)
使用开机查杀
查杀任务列表
名称
状态
下次运行时间
描述
添加
查看
修改
删除
只应用已修改选项
应用到所有下级中心
导入(I)...
导出(E)
确定(O)
取消(C)

定时查杀页面

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。


设置防毒策略 - ADMIN-2UBP8W4TO
其它设置
实时监控设置
文件监控
邮件监控
嵌入式杀毒
Lotus Notes
Office/IE
Outlook
其它嵌入式查杀
手动查杀
定制任务
定时查杀
开机查杀
其它设置
使用声音报警
保存历史记录
保留：
60
天
加入“云安全”计划
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
在登录系统前显示监控状态
只应用已修改选项
应用到所有下级中心
导入(I)...
导出(E)
确定(O)
取消(C)

瑞星网络版的策略设置

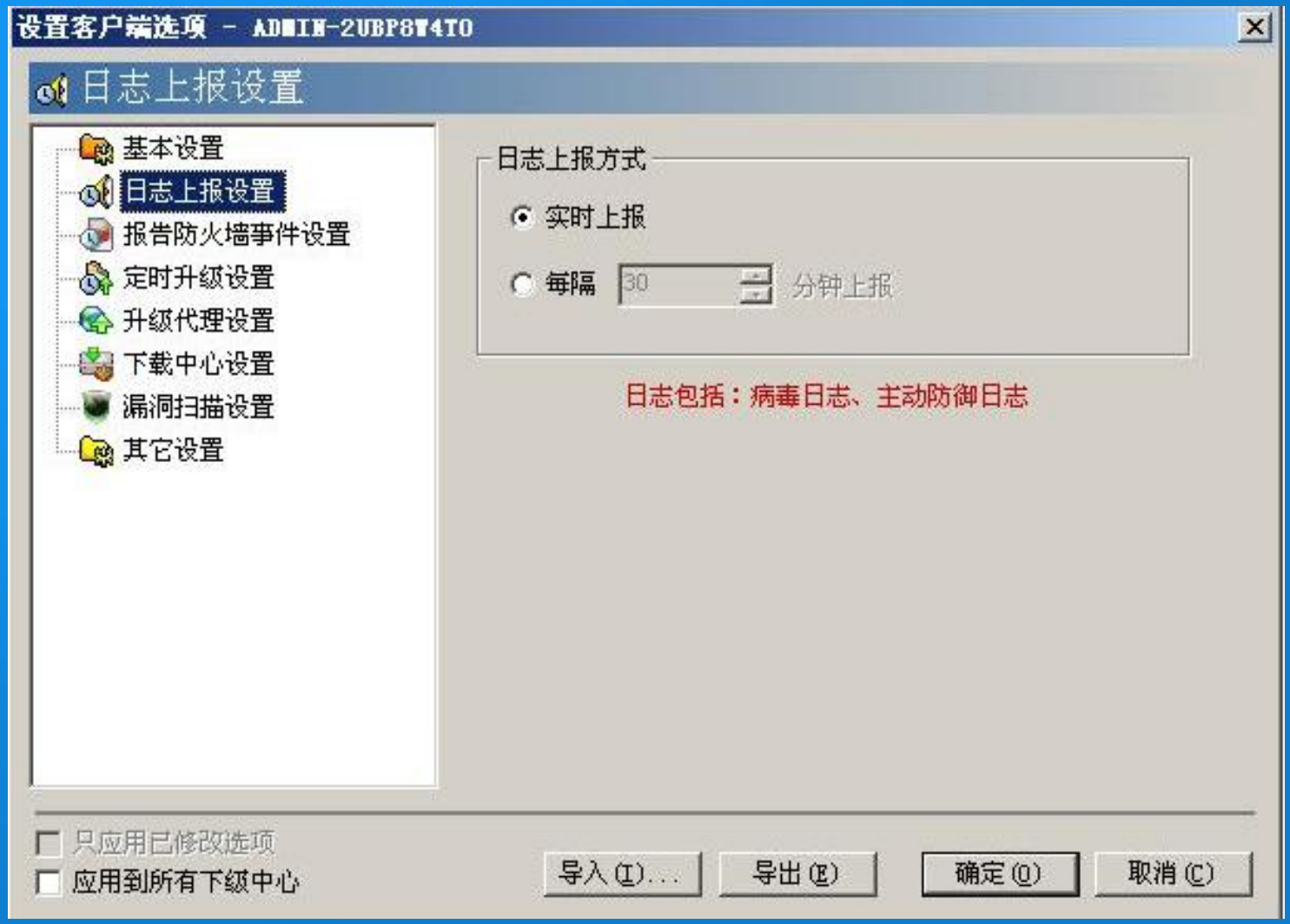
瑞星网络版的客户端选项设置

- ◆升级时间（从中心升级的时间）
- ◆密码保护（保证客户端子系统安全）
- ◆漏洞扫描（设定漏洞扫描的时间）
- ◆代理设置（指定代理升级中心的IP）

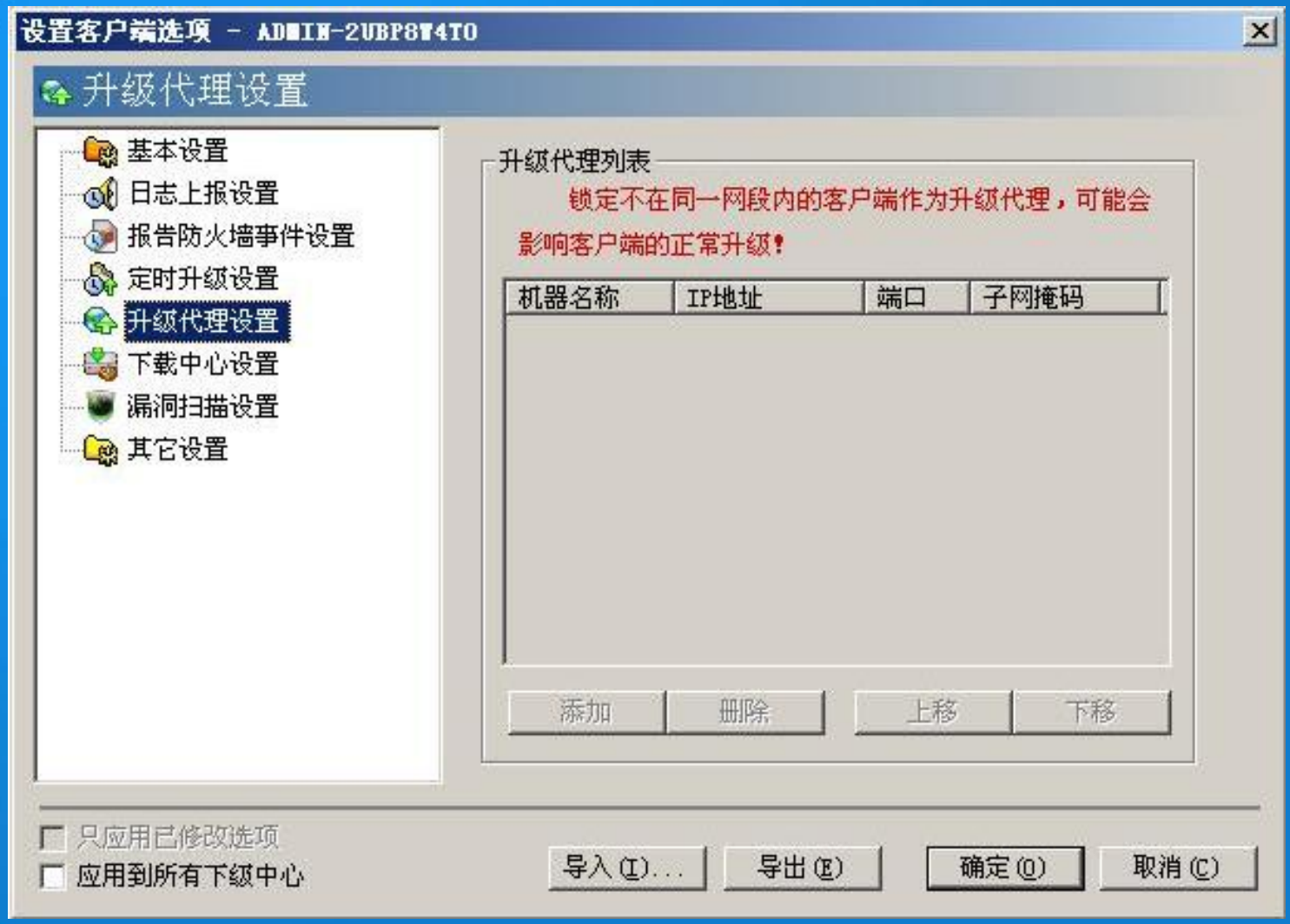
重点：密码保护，不要与控制台登录密码混淆

设置客户端选项

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。


设置客户端选项 - ADMIN-2UBP8W4TO
日志上报设置
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
升级代理设置
下载中心设置
漏洞扫描设置
其它设置
日志上报方式
实时上报
每隔
30
分钟上报
日志包括：病毒日志、主动防御日志
只应用已修改选项
应用到所有下级中心
导入(I)...
导出(E)
确定(O)
取消(C)


设置客户端选项 - ADMIN-2UBP8W4TO
定时升级设置
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
升级代理设置
下载中心设置
漏洞扫描设置
其它设置
启用定时升级
每天
每月
每周
每周期
升级时间
每隔
5
分钟升级
日期
1
星期
星期日
开始时间
0
时
0
分
结束时间
23
时
59
分
只升级病毒特征库
静默升级模式
只应用已修改选项
应用到所有下级中心
导入(I)...
导出(E)
确定(O)
取消(C)


设置客户端选项 - ADMIN-2UBP8W4TO
升级代理设置
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
升级代理设置
下载中心设置
漏洞扫描设置
其它设置
升级代理列表
锁定不在同一网段内的客户端作为升级代理，可能会影响客户端的正常升级！
机器名称
IP地址
端口
子网掩码
添加
删除
上移
下移
只应用已修改选项
应用到所有下级中心
导入(I)...
导出(E)
确定(O)
取消(C)


设置客户端选项 - 2003SRVSP1
下载中心设置
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
升级代理设置
下载中心设置
漏洞扫描设置
其它设置
启用定时清理
每天
每月
每周
每周期
清理时间
每隔
5
分钟清理
日期
1
星期
星期日
开始时间
0
时
0
分
结束时间
23
时
59
分
升级文件 保留组件的版本数
10
个
漏洞补丁文件 最大使用硬盘大小
100
兆字节
只应用已修改选项
应用到所有下级中心
导入(I)...
导出(E)
确定(O)
取消(C)

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；教育专用版和小型企业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。

其它设置

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

设置主动防御规则

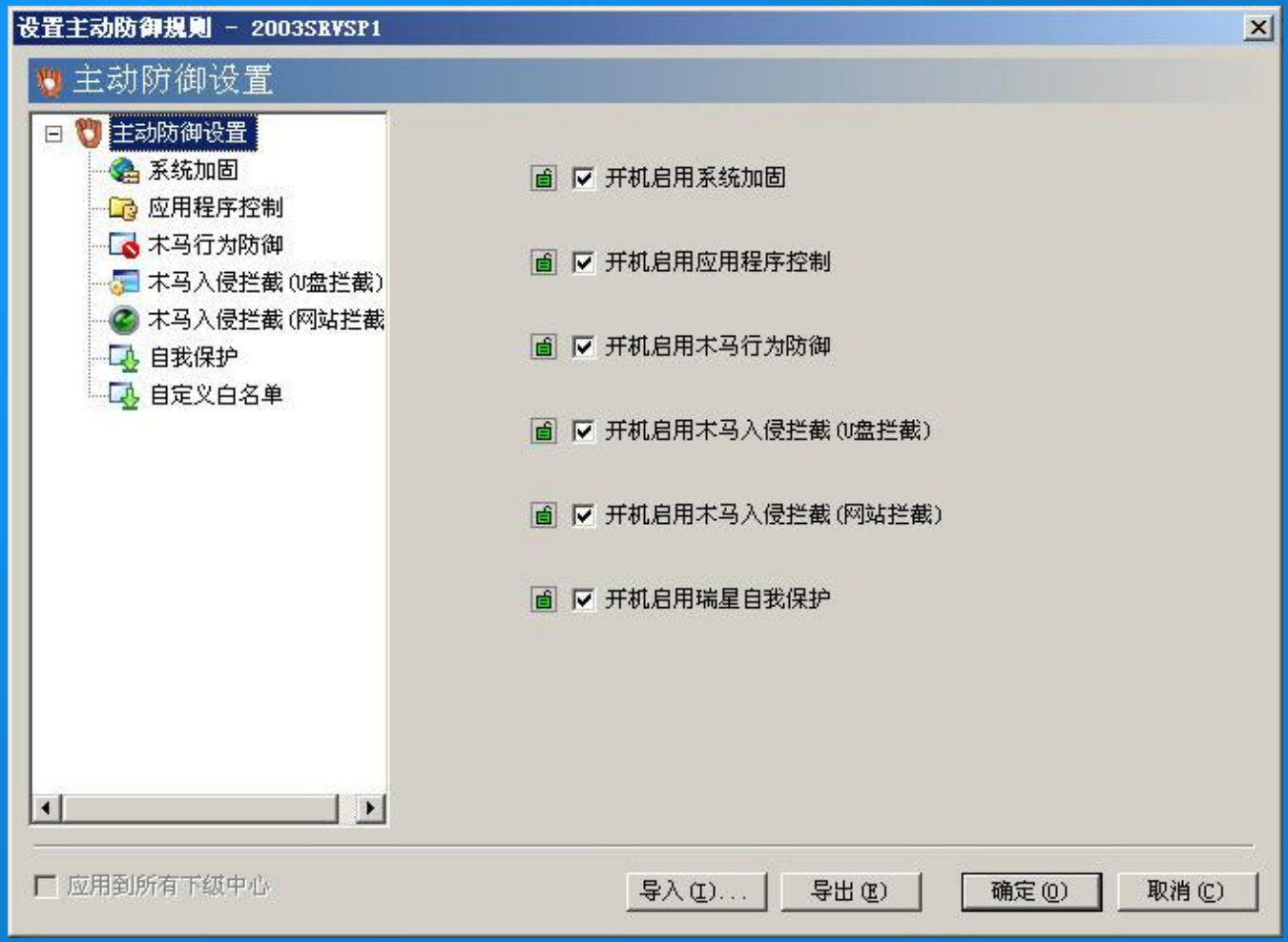
管理员可以通过管理控制台远程查看、设置客户端的主动防御选项，设置主动防御组策略，并且上报、查询、统计主动防御的日志。对于可信任的程序，可将其添加到主动防御白名单中。对于已有的主动防御规则，通过【导出】备份规则设置，当客户端需要配置主动防御规则时，也可以通过【导入】/【导入缺省配置】或【从文件中导入】快速导入主动防御规则设置。

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。

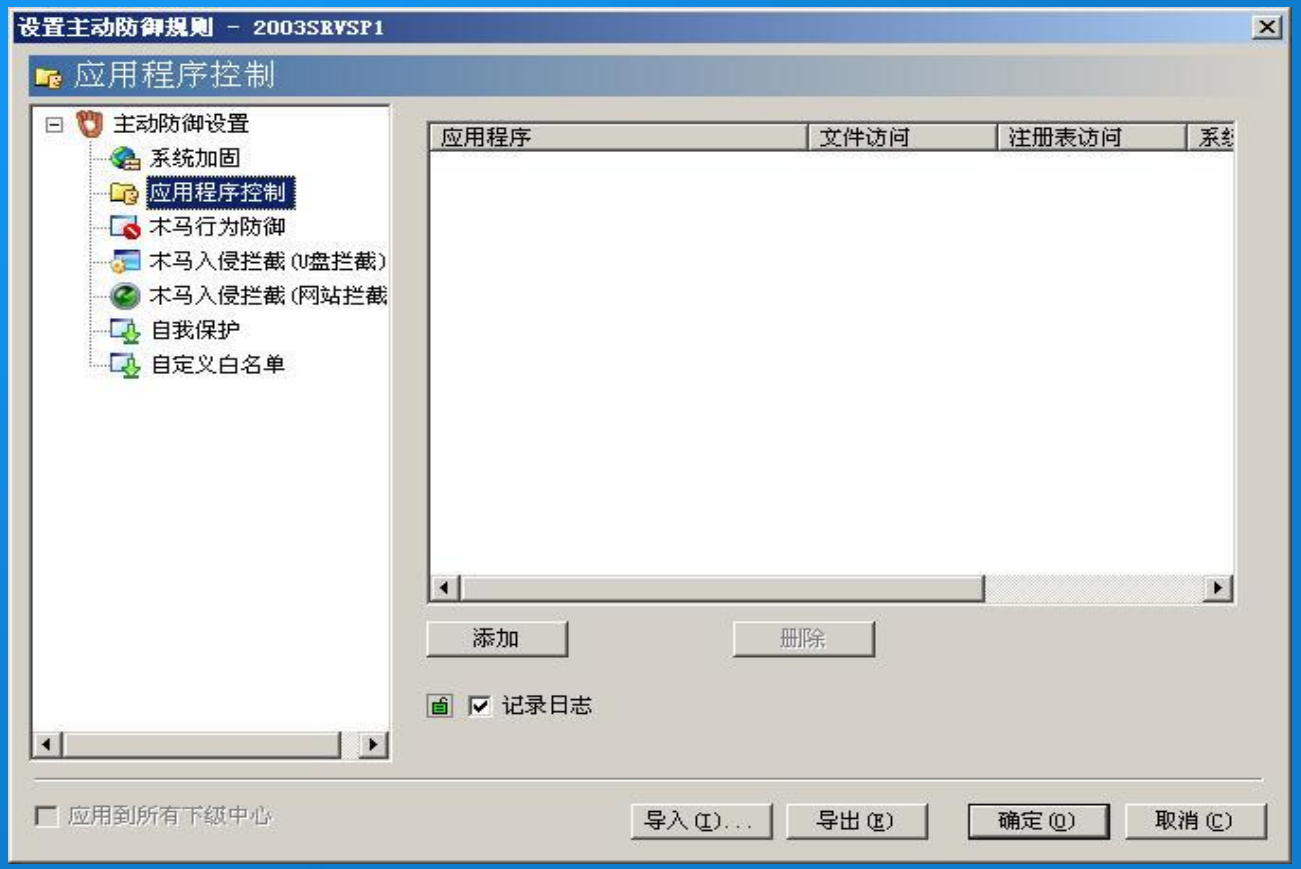
注意：所有64位操作系统不支持主动防御功能。对于不支持主动防御功能或没有安装主动防御的客户端，该功能设置项无效。

【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。


设置主动防御规则 - 2003SRVSP1
主动防御设置
主动防御设置
系统加固
应用程序控制
木马行为防御
木马入侵拦截(U盘拦截)
木马入侵拦截(网站拦截
自我保护
自定义白名单
开机启用系统加固
开机启用应用程序控制
开机启用木马行为防御
开机启用木马入侵拦截(U盘拦截)
开机启用木马入侵拦截(网站拦截)
开机启用瑞星自我保护
应用到所有下级中心
导入(I)...
导出(E)
确定(O)
取消(C)

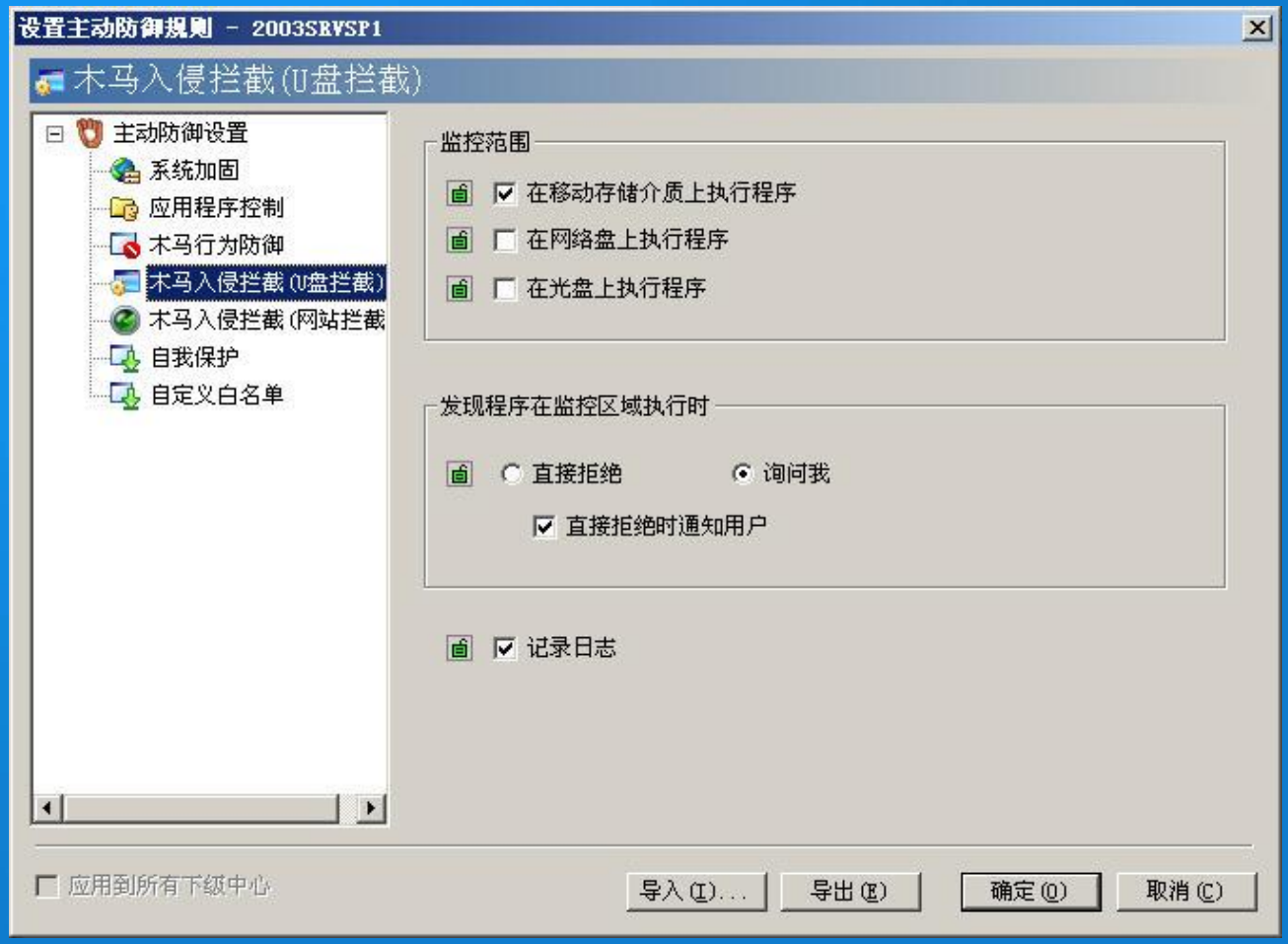

设置主动防御规则 - 2003SRVSP1
系统加固
主动防御设置
系统加固
应用程序控制
木马行为防御
木马入侵拦截(U盘拦截)
木马入侵拦截(网站拦截
自我保护
自定义白名单
系统加固
系统动作监控
注册表监控
关键进程保护
系统文件保护
系统动作监控
挂全局钩子
修改内核内存数据
加载驱动程序
修改系统日期及时间
关闭电脑
使用摄像头
安装驱动
底层磁盘访问
记录日志
应用到所有下级中心
导入(I)...
导出(E)
确定(O)
取消(C)

应用程序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。

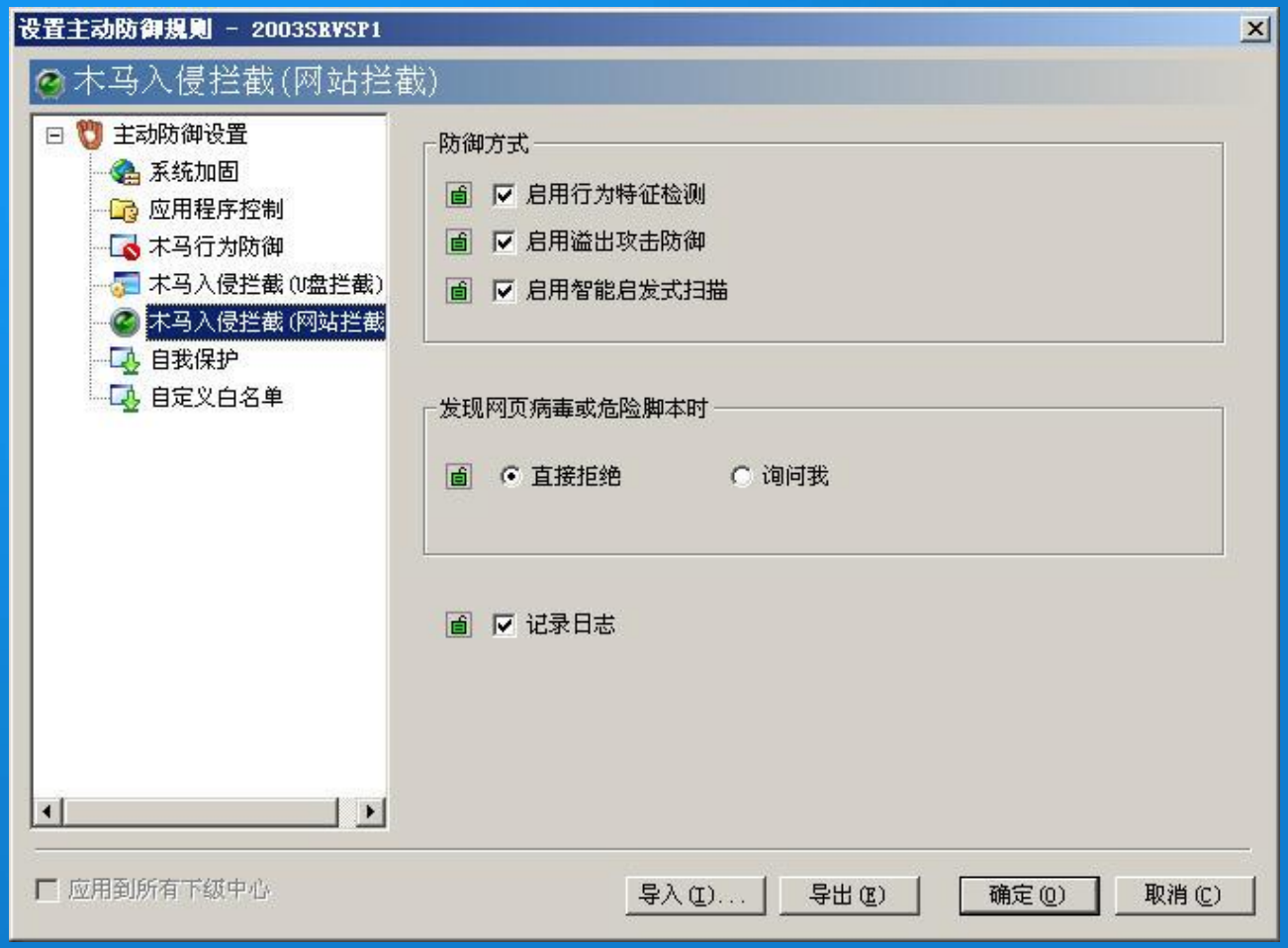


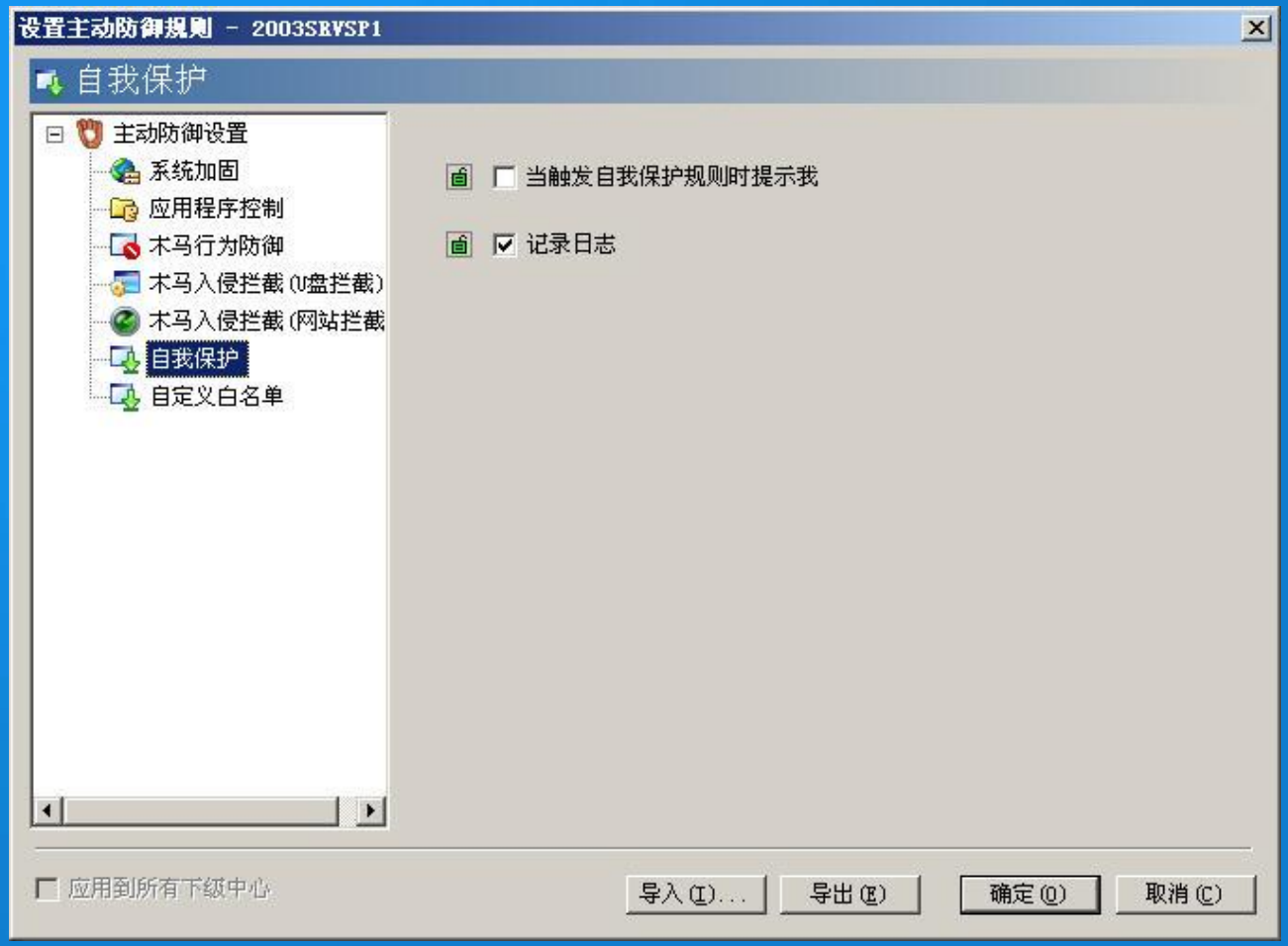
木马行为防御能够对系统中的程序进行监控，根据行为检测报告发现可能包含恶意代码的应用程序。用户可以设置恶意行为启发式检测敏感度、发现程序检测恶意行为时的处理方式、是否记录日志、在进程退出时是否进行家族病毒DNA扫描。

木马入侵拦截（U盘拦截）取代了原来的U盘监控，控制范围更广，能够更好地控制执行区域，避免外部病毒感染到主机。当木马入侵拦截（U盘拦截）范围内的程序试图自动运行或直接运行的时候，进行拦截，并提示用户。

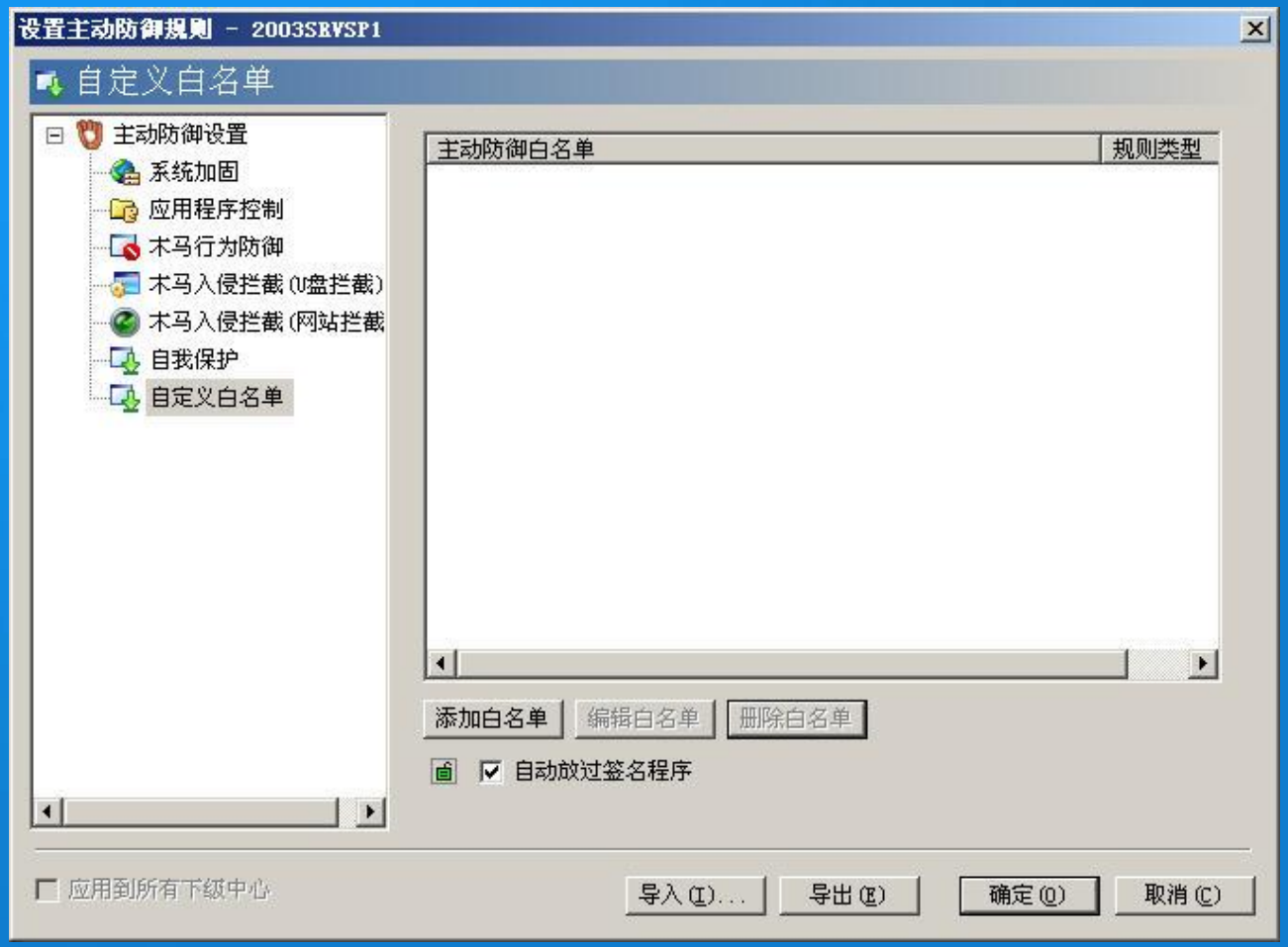


木马入侵拦截（网站拦截）突破了原来网页脚本扫描只能通过特征进行查杀的技术壁垒。解决了原网页脚本监控无法对加密变形的病毒脚本进行处理的问题。由于采用的是行为检测查杀，对于网页挂马一类的木马有很好的防御和处理能力。




设置主动防御规则 - 2003SRVSP1
自我保护
主动防御设置
系统加固
应用程序控制
木马行为防御
木马入侵拦截(U盘拦截)
木马入侵拦截(网站拦截
自我保护
自定义白名单
当触发自我保护规则时提示我
记录日志
应用到所有下级中心
导入(I)...
导出(E)
确定(O)
取消(C)

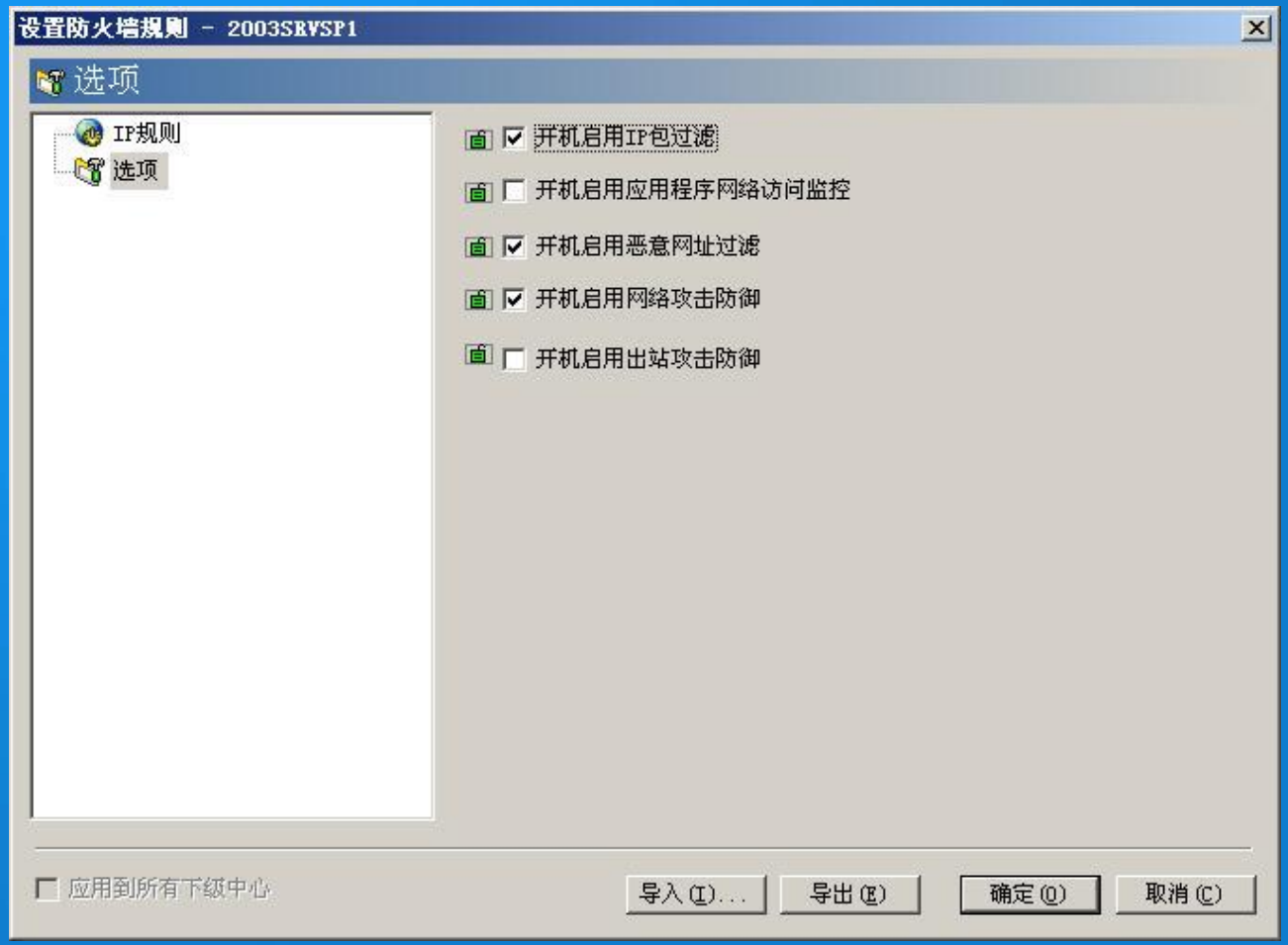
用户可以自行在智能主动防御中将信任的程序添加到自定义白名单中。添加到自定义白名单中的程序将不受智能主动防御的限制，满足用户的个性化需求



防火墙规则设置

说明：在高级企业版和高级企业专用版中可以设置防火墙规则；中小企业版、企业版、企业专用版、教育专用版和小型企业版中无此设置页面。

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。


设置防火墙规则 - 2003SRVSP1
选项
IP规则
选项
开机启用IP包过滤
开机启用应用程序网络访问监控
开机启用恶意网址过滤
开机启用网络攻击防御
开机启用出站攻击防御
应用到所有下级中心
导入(I)...
导出(E)
确定(O)
取消(C)

网络安全　源自瑞星