

瑞星企业终端安全管理系统软件 用户手册

制作本手册的目的在于指导用户使用瑞星企业终端安全管理系统软件。手册中详细介绍了瑞星企业终端安全管理系统软件的各个功能及其操 作方法。请在使用瑞星企业终端安全管理系统软件前认真阅读本手册。



重要声明

感谢您购买瑞星公司出品的瑞星安全软件系列产品。请在使用瑞星安全软件之前认真阅 读配套的使用手册,当您开始使用瑞星安全软件时,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安全软件的更新而改变,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。因使用手册对用户可能产生的影响, 瑞星公司不承担责任。

瑞星企业终端安全管理系统软件均可以通过瑞星网站在线注册,其中包括用于从瑞星网站下载升级的"服务号"。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、技术和服务等信息而造成的影响不承担任何责任。

作为内网安全管理软件,瑞星企业终端安全管理系统软件将进行不断的升级。无论是功 能的增加、性能的提高,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。

忠告用户

(1)请将所购产品与"产品组件清单"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)如果自购买日起一个月后未注册,将不能得到包括升级在内的技术支持和售后服务;

(3)为了避免"产品序列号"、"服务号"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) 请准确填写注册中的每项内容确保及时注册;

(5)请妥善保管"产品序列号"和"服务号",以免软件被盗用,从而影响自己的正常使用;

(6)如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,不得在授权范围外使用本软件。

瑞星客户服务联系方式

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,请通过以下方式与我们取得联系。

客户服务: 400-660-8866(免长途话费)

010-82678800(自费电话)

邮件服务中心: http://mailcenter.rising.com.cn

网址: http://www.rising.com.cn

邮政编码: 100190

通信地址:北京市海淀区中关村大街 22 号中科大厦 1408 室

2014年7月北京•中国

目录

重要声明	0
忠告用户	2
瑞星客户服务联系方式	
日录	
1 **	
1. 软件说明	ð
1.1 产品组成	8
1.2 应用环境	8
1.2.1 级据中心	8
1.2.2 目理中心	هه م
1.2.4 升级中心	
1.2.5 补丁下载中心	
1.2.6 客户端	
1.2.7 远程管理控制台	
2. 软件概述	
2.1 支持大型网络的多中心负载平衡系统	
2.2 安装方式	
2.2.1 智能安装	14
2.2.2 WEB 安装	14
3. 安装与卸载	
3.1 安装	
3.2 卸载	22
3.3 修复	23
4. 产品授权	24
4.1 获取授权	24
5. 系统登录	
0. 自建控制口	
0.1 女至中心	26
0.2 口芯报音 6.9.1 日主杏海	27 דכ
0.2.1 口心旦间 6.2.1 1系统事件日志	
6.2.1.2 防病毒	
6.2.1.3 漏洞扫描	
6.2.1.4 IT 资产管理	
6.2.1.4.1 硬件异动日志查询	
6.2.1.4.2 设备异动日志查询	
6.2.1.4.3 设备扫描日志查询	32

6.2.1.4.4 软件扫描日志查询	
6.2.1.4.5 软件部署日志查询	
6.2.2 报告查询	
6.2.3 定时报告	
6.2.4 综合报告查询	
6.3 计算机管理	
6.3.1 我的组织	41
6.3.1.1 菜单栏	
6.3.1.1.1 域信息	
6.3.1.1.2 子域信息	
6.3.1.1.3 策略模板	
6.3.1.1.3.1 添加策略模板	
6.3.1.1.3.2 使用己创建的模板	
6.3.1.1.4 共有策略	51
6.3.1.1.4.1 修改 IT 资产管理模板	52
6.3.1.1.4.2 修改客户端代理模板	52
6.3.1.1.4.3 修改U盘登记模板	52
6.3.1.1.4.4 修改控制台个性化模板	52
6.3.1.1.5 客户端	52
6.3.1.1.5.1 己知计算机	53
6.3.1.1.5.2 未知计算机	57
6.3.1.1.6 客户端备注	60
6.3.1.2 根管理组(普通组)	61
6.3.1.3 服务器管理	61
6.3.1.3.1 系统服务器	61
6.3.1.3.1.1 瑞星管理中心(MANAGER)	61
6.3.1.3.1.2 漏洞补丁中心(RDC)	62
6.3.1.3.1.3升级中心(RUC)	64
6.3.1.3.1.4 业务中心(BUS)	66
6.3.1.3.2 外围服务器	67
6.3.1.3.3 数据连接设置	68
6.3.1.3.4 日志数据清理	68
6.3.1.5 黑名单	70
6.4 授权管理	71
6.4.1 产品信息	71
6.4.2 授权信息	72
6.5 用户管理	73
6.5.1 创建用户	73
6.5.1.1 基本设置	74
6.5.1.2 权限设置	74
6.5.1.2.1 管理员权限	74
6.5.1.2.2 自定义权限	75
6.5.2 修改	75
6.5.3 修改密码	

	6.5.4 详情	76
7.	审计控制台	76
	7.1 平台	77
	7.1.1 客户端	77
	7.1.2 未知终端	77
	7.2 防病毒	78
	7.2.1 全网查杀	78
	7.2.2 病毒分析	80
	7.2.3 病毒详情	84
	7.2.4 系统加固	87
	7.2.5 应用加固	88
	7.3漏洞扫描	89
	7.3.1 漏洞统计	90
	7.3.2 漏洞修复	91
	7.3.3 补丁管理	93
	7.3.3.1 未在下载	93
	7.3.3.2 正在下载	94
	7.3.3.3 已下载	95
	7.4 资产管理	96
	7.4.1 禁用软件	97
	7.4.2 保护软件	98
	7.4.3 关注软件	99
	7.4.4 软件详情	102
	7.4.5 软件部署	104
	7.4.6 硬件异动	106
	7.4.7 硬件详情	107
	7.5 XP 盾	109
	7.5.1 防御概要	109
	7.5.2 攻击详情	110
8.	升级中心	. 111
	8.1 客户端安装包	111
	8.2 手动升级	113
	8.3 第三方软件	114
9.	客户端	. 115
	9.1 系统托盘	115
	9.2 客户端主界面	118
	9.2.1 瑞星杀毒	118
	9.2.1.1 病毒查杀	119
	9.2.1.2 电脑防护	124
	9.2.1.3 设置中心	128
	9.2.1.4 日志系统	131
	9.2.1.5 更多功能	135
	9.2.1.5.1 隔离区	135

9.2.1.5.2 使用教程	136
9.2.1.5.3 更多功能	137
9.2.2 漏洞修复	138
9.2.3 XP 盾	141
9.2.3.1 热补丁实时监控	142
9.2.3.2 漏洞免疫	142
9.2.3.3 发生攻击主动提醒	142
9.2.3.4 记录漏洞攻击日志	142
9.2.3.5 白名单设置	142
9.2.4 其他功能	144
9.2.4.1 杀毒日志	144
9.2.4.2 隔离中心	144
9.2.4.3 引导区工具	146
9.2.4.4 电脑修复	148
9.2.4.5 开机优化	150
9.2.4.6 进程管理	153
9.2.4.7 右键菜单管理	154
9.2.4.8 垃圾文件清理	156
9.2.4.9 隐私痕迹清理	158
9.2.4.10 使用痕迹清理	160
9.2.4.11 文件粉碎器	162
9.2.4.12 产品信息	164
9.3 漏洞补丁导入导出工具	171
9.4 日志打包工具	171
9.5数据库管理工具	172
附录一北京瑞星信息技术有限公司简介	174
附录二瑞星信息安全资讯网	175

1. 软件说明

1.1 产品组成

当您通过合法途径获得瑞星企业终端安全管理系统软件的使用权后,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企业终端安全管理系统软件所有程序。

 《用户手册》:即《瑞星企业终端安全管理系统软件用户手册》(电子版),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. 《快速使用指南》: 指导用户快速掌握软件的使用方法。

5. 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。

6. 《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 数据中心

a. 数据库

Microsoft SQL Server 2005 Microsoft SQL Server 2008 MSDE(没有上述时自动安装)

b. 网络要求

网络环境: 100M带宽以上网络, 需一个固定IP地址

c. 对通信协议的要求

TCP/IP

1.2.2 管理中心

a. 软件环境

1) 操作系统

Windows 7系统

Windows 8系统

Windows Server 2003 系列系统
Windows Server 2008 系列系统(包含 Windows Server 2008 R2 系统)
Windows Server 2012 系列系统
2) 其它
IIS 6.0以上发布版本

Microsoft.NET Framework 3.5

b. 硬件和网络要求

剩余磁盘空间: 2.0GB以上

CPU: 1.0GHz 及以上32 位 (x86) 或 64 位 (x64) 内存: 2.0GB系统内存及以上,最大支持内存4.0GB 网络环境: 100M带宽以上网络,需一个固定IP地址

c. 对通信协议的要求

TCP/IP, UDP

1.2.3 业务中心

a. 软件环境

1) 操作系统

Windows XP 系统 Windows Vista 系统 Windows 7 系统 Windows 8系统 Windows Server 2003 系列系统 Windows Server 2008 系列系统(包含Windows Server 2008 R2 系统) Windows Server 2012 系列系统

b. 硬件和网络要求

剩余磁盘空间: 2.0GB以上 CPU: 1.0GHz 及以上32 位 (x86) 或 64 位 (x64) 内存: 2.0GB系统内存及以上,最大支持内存4.0GB 网络环境: 100M带宽以上网络,需一个固定IP地址

c. 对通信协议的要求

 $\ensuremath{\mathsf{TCP}}\xspace/\ensuremath{\mathsf{IP}}\xspace$, $\ensuremath{\mathsf{UDP}}\xspace$

1.2.4 升级中心

a. 软件环境

操作系统

Windows 7系统

Windows 8系统

Windows Server 2003 系列系统

Windows Server 2008 系列系统(包含 Windows Server 2008 R2 系统)

Windows Server 2012 系列系统

2) 其它

IIS 6.0以上发布版本

Microsoft.NET Framework 3.5

b. 硬件和网络要求

剩余磁盘空间: 4.0GB以上

CPU: 1.0GHz 及以上32 位 (x86) 或 64 位 (x64)

内存: 2.0GB系统内存及以上,最大支持内存4.0GB

网络环境: 100M带宽以上网络, 需一个固定IP地址; 建议服务器可访问瑞星官网,

以方便自动升级

c. 对通信协议的要求

TCP/IP, UDP

1.2.5 补丁下载中心

a. 软件环境

操作系统
 Windows 7系统
 Windows 8系统
 Windows Server 2003 系列系统
 Windows Server 2008 系列系统 (包含 Windows Server 2008 R2 系统)
 Windows Server 2012 系列系统
 2) 其它

北京瑞星信息技术有限公司

IIS 6.0以上发布版本 Microsoft.NET Framework 3.5

b. 硬件和网络要求

剩余磁盘空间: 20GB以上

CPU: 1.0GHz 及以上32 位 (x86) 或 64 位 (x64)

内存: 2.0GB系统内存及以上,最大支持内存4.0GB

网络环境:100M带宽以上网络,需一个固定IP地址;建议服务器可访问瑞星官网,以方便自动升级

c. 对通信协议的要求

TCP/IP, UDP

1.2.6 客户端

a. 软件环境

操作系统

Windows XP 系统 Windows Vista 系统 Windows 7 系统 Windows 8系统 Windows Server 2003 系列系统 Windows Server 2008 系列系统(包含 Windows Server 2008 R2 系统) Windows Server 2012 系列系统

b. 硬件环境

剩余磁盘空间: 500MB以上

CPU: 1.0GHz 及以上

内存: 512 MB系统内存及以上

1.2.7 远程管理控制台

a. 浏览器

Microsoft Internet Explorer 7.0及以上

Google Chrome 谷歌浏览器(推荐)

Apple Safari 苹果浏览器

Mozilla Firefox 火狐浏览器

b. 其他要求

Adobe Flash 插件 9.0 及以上

2. 软件概述

瑞星企业终端安全管理系统软件是瑞星信息技术有限公司推出的企业级内网安全管理 软件产品,它为加强内网管理提供了一套统一的 IT 安全解决方案,不但提供传统的防病毒、 漏洞扫描等功能,还对网络环境中各计算机的信息、软硬件资源进行有效的管理和控制。

传统的安全解决方案,比如防病毒、入侵检测等在网络安全中起到非常重要的作用,但 很多企业在部署了这些安全产品后,还是得不到全面的安全防护,如:ARP 欺骗攻击、内部 资料泄密等。这是由于传统的安全技术和解决方案主要保证网络边界的安全,而忽视内部网 络的安全威胁。这些威胁主要表现在:移动电脑设备随意接入、非法外联难以控制、软硬件 资产滥用、网络故障频发等。瑞星企业终端安全管理系统软件产品,不仅包含传统的防病毒、 入侵检测等安全功能,还具备增强内网信息安全性的强大功能,提供给企业用户一个完整的 企业 IT 安全解决方案。可以更好的帮助企业用户解决内部信息安全问题、软硬件的运维管 理问题。从而为企业用户提高 IT 维护效率,有效降低 IT 运营成本。

瑞星企业终端安全管理系统软件产品实质上不只是一个管理平台,企业用户可以根据自 身的需求在其上布置具有不同管理功能的子产品。本软件可以满足不同企业的不同需求,有 针对性的解决企业遇到的各种安全风险,彻底改变了以往安全类软件功能过于笼统、不够灵 活的缺点。瑞星企业终端安全管理系统软件工作原理如下图:



管理中心:是对企业全网进行统一管理的交互平台,用户通过管理中心就可以完成所有管理 功能。它实时反映防护体系内每台计算机情况,为管理员管理客户端计算机的使用情况提供 了大量的依据。通过管理中心可以发布操作、升级等各项命令,统一设置安全管理的各种策 略,实现对整个防护系统的自动控制,保障整个网络安全。

远程管理控制台:管理员登录管理中心的计算机。

数据中心:用于存储软件运行过程中产生的各种数据的服务器。

业务中心:是全网客户端连接服务器的中心服务器,业务中心会按照管理员操作下发策略、 任务等管理数据给全网客户端,同时又会接收客户端的日志、状态等信息,并及时写入数据 中心,独特的负载均衡方案,使得业务中心具备更强的负载能力,突破传统方式的网络连接 瓶颈。

扩展中心:除系统必备中心(管理中心、数据中心、业务中心)之外的其它扩展中心。目前 只包括升级中心、补丁下载中心。

补丁下载中心: 主要用于存储补丁文件, 管理中心下载任务。

升级中心:用于全网部署、升级的工作

客户端:企业安装瑞星企业终端安全管理系统软件客户端的计算机。

瑞星企业终端安全管理系统软件采用分布式体系,结构清晰明了,管理维护方便。管理 北京瑞星信息技术有限公司 13 员只要拥有管理员账号和口令,就能在网络上任何一台有网页浏览器的计算机上,实现对整 个网络上所有计算机的集中管理。

2.1 支持大型网络的多中心负载平衡系统

单业务中心环境中,实际上它的处理能力总是有限的,考虑大、中型网络环境中,众多 客户端造成整个系统性能下降的问题,系统提供了增加业务(扩展)中心的方式,即整个系 统可部署1个以上的业务中心,用以提高整个系统的负载能力。

多中心的部署,对客户端连接来说是透明的,客户端对中心来说是一个逻辑的组,增加 中心也不会影响客户端的原有连接,在启用了负载平衡后,中心会根据当前的实际情况智能 分配连接,使得各中心连接相对平衡,达到最大化的优化系统,提高整体性能。

2.2 安装方式

瑞星企业终端安全管理系统软件提供多种安装方式,包括:智能安装和 WEB 安装等,通 过这些多样化的安装方式,网络管理员可以十分轻松地在最短的时间内完成整个系统的安装。 而且管理员可以通过登录升级服务器使用"制作客户端安装包"定制客户端安装包,并快速 发布。

2.2.1 智能安装

智能安装又分单服务器模式安装、单客户端模式安装和自定义模式安装。

单服务器模式,安装过程中只需要输入安装管理中心所需要的各种参数,之后的业务中 心、升级中心等参数都会自动填充,以方便在中小型网络环境下快速使用部署。

单客户端模式安装,快速部署客户端子产品,不需要选定客户端子产品即可快速使用部署。

自定义安装,用户可根据需要自由组合产品,给与用户较大的自定义自由度,方便在不同的网络环境下部署不同的产品。

2.2.2 WEB 安装

如果安装了升级中心,可上传安装包到升级中心上,也可以使用升级中心制作客户端安装包,即在内网环境下发布相应的安装包,客户端用户通过浏览指定位置的网页实现软件的 安装。

3. 安装与卸载

瑞星企业终端安全管理系统软件的基本安装对象包括管理中心(包含数据中心)、业务

中心、升级中心、补丁下载中心、客户端代理、客户端子产品——防病毒、客户端子产品——IT 资产管理、客户端子产品——漏洞扫描和客户端子产品——XP 盾。

瑞星企业终端安全管理系统软件光盘提供了三种安装模式:单服务器模式安装、单客户 端模式安装和自定义模式安装。

● 单服务器模式安装

如果您准备把中心(服务器产品)安装在同一台计算机,可以使用这种安装方式, 会最大化减少安装过程。

- 单客户端模式安装
 单独安装客户端程序包。
- 自定义模式安装

高级自定义安装模式,可实现上述两种安装模式效果。

本文档将以单服务器模式安装为例,统一介绍产品的安装与卸载,其他安装模式类似。

提示:

- 1. 安装本软件前请卸载其它安全类软件。
- 服务器端和客户端不要安装在同一电脑上,如:将服务器端安装在 Windows Server 2003
 系统中,客户端安装在 Windows XP 系统中。

3.1 安装

第一步:将瑞星企业终端安全管理系统软件光盘放入光驱内,双击瑞星企业终端安全管理系统软件的安装程序,开始安装。

自动安装制	野	- • ×
8	欢迎使用瑞星软件 ! 请稍候	
		退出(Q)

第二步:进入安装程序欢迎界面。

瑞星企业终端安 Rising Enterprise	全管理系统软件 Security Manager	: nent System	– × 2.0.1.3
开始 ➡ 设置 进行中	完成		
	次迎使用瑞	星企业终端安全	管理系统
路径:C:\Program Files\Risin	g 更改	安装试用版	导入授权
<и>✓ 我已阅读并同意 瑞星用户许	可协议		

- 1、点击【瑞星用户许可协议】浏览瑞星企业产品最终用户许可协议;
- 2、点击【更改】修改安装目录(默认为 C:\Program Files\Rising);
- 3、选择【我已阅读并同意】瑞星用户许可协议。

第三步: 点击 导入授权 ,输入基本号,导入授权证书文件,点击【确定】。
😽 瑞星企业终端安全管理系统软件 🛛 🗙
基本号:
证书文件: 选择文件 未选择文件
确定
提示:
产品安装包内置短期试用授权许可,您可以点击【确定】,直接使用此授权并进入下

- 步骤。在产品使用中,您可以通过产品授权操作,获得正式使用授权。
- 2. 产品授权操作方法,请参考本文档章节 4.产品授权。

1.

安装试用版



进入下一步安装。

第四步:点击



第五步:按照默认的组件安装,点击【下一步】。

瑞星企业 Rising Ent	终端安全管理系统软件 erprise Security Management System	– × 2.0.1.3
开始 设置 ➡ 进	行中 完成	
✓必装组件		
✓客户端代理	安装:1.0.2.81	
✓服务器子产品		
✓管理中心	安装:1.0.3.47	
✓ 业务中心	安装:1.0.0.43	
✓升级中心	安装:1.0.2.0	
✓漏洞补丁中心	安装:1.0.0.67	
		上一步下一步

第六步:进入数据库的安装界面,设置数据库的类型及相关参数。有两种数据库类型可选择,分别为【SQL SERVER】和【MSDE】。默认选择为【SQL SERVER】,在条件许可的情况下建议选择此项。若安装环境中已有 SQL SERVER 数据库,选择【SQL SERVER】,设置各项参数后,单击【下一步】。

NINC F端星端星企业终端安全管理系统软件用户手册

开始 设置 → 进行中 完」	成.
服务地址:	•
数据库类型: ● SQL Server	O MSDE
管理数据库	日志教据库
服务器:	服务器:
数据库: esmdb	数据库: esmlogdb
用户名:	用户名:
密码:	密码:
后安装环境中已有 MSDE 数据库	,可以选择【MSDE】,设置各项参数后,单击【下一
音安裝环境中已有 MSDE 数据库 瑞星企业终端安全管 Rising Enterprise Secu	F,可以选择【MSDE】,设置各项参数后,单击【下一 「理系统软件 ー Irity Management System 2.0.
古安装环境中已有 MSDE 数据库 瑞星企业终端安全管 Rising Enterprise Secu 开始 设置 → 进行中 完	F,可以选择【MSDE】, 设置各项参数后,单击【下一 「理系统软件 Irity Management System 2.0.
古安装环境中已有 MSDE 数据库 瑞星企业终端安全管 Rising Enterprise Secu 开始 设置 → 进行中 完 服务地址: 193.168.12.116	F,可以选择【MSDE】,设置各项参数后,单击【下一 行理系统软件 urity Management System 2.0.
古安装环境中已有 MSDE 数据库 瑞星企业终端安全管 Rising Enterprise Secu 平衡 设置 → 进行中 完 服务地址: 193.168.12.116 数据库类型: ○SQL Server	r,可以选择【MSDE】,设置各项参数后,单击【下一 T理系统软件 rrity Management System 2.0. 成 ● MSDE
古安装环境中已有 MSDE 数据库 瑞星企业终端安全管 Rising Enterprise Secu 形象 设置 → 进行中 完 服务地址: 193.168.12.116 数据库美型: ○SQL Server MSDE安装目录: C:\Program File	r,可以选择【MSDE】,设置各项参数后,单击【下一 r理系统软件 urity Management System 2.0. ▲ MSDE es\Rising\ESMMsde
古安装环境中已有 MSDE 数据库 瑞星企业终端安全管 Rising Enterprise Secu 田参 设置 → 进行中 完 服务地址: 193.168.12.116 数据库类型: ○SQL Server MSDE安装目录: C:\Program File MSDE数据目录: C:\Program File	r,可以选择【MSDE】,设置各项参数后,单击【下一 r理系统软件 rity Management System 2.0. ▲ MSDE es\Rising\ESMMsde es\Rising\ESMMsdeData
古安装环境中已有 MSDE 数据库 瑞星企业终端安全管 Rising Enterprise Secu 田参 设置 → 进行中 完 服务地址: 193.168.12.116 数据库类型: ○ SQL Server MSDE安装目录: C:\Program File MSDE数据目录: C:\Program File	r,可以选择【MSDE】,设置各项参数后,单击【下一 r理系统软件 rity Management System 2.0. ▲ MSDE es\Rising\ESMMsde es\Rising\ESMMsdeData
古安装环境中已有 MSDE 数据库 瑞星企业终端安全管 Rising Enterprise Secu 平参 设置 → 进行中 完 服务地址: 193.168.12.116 数据库美型: ◎ SQL Server MSDE安装目录: C:\Program File MSDE数据目录: C:\Program File	r,可以选择【MSDE】,设置各项参数后,单击【下一 行理系统软件 (inity Management System 2.0. ▲ ● MSDE es\Rising\ESMMsde es\Rising\ESMMsdeData
古安装环境中已有 MSDE 数据库 瑞星企业终端安全管 Rising Enterprise Secu 平参 设置 → 进行中 完 服务地址: 193.168.12.116 数据库美型: ◎ SQL Server MSDE安装目录: C:\Program File MSDE数据目录: C:\Program File	r,可以选择【MSDE】,设置各项参数后,单击【下一 行理系统软件 (inity Management System 2.0. ▲ ● MSDE es\Rising\ESMMsde es\Rising\ESMMsdeData
古安装环境中已有 MSDE 数据库 瑞星企业终端安全管 Rising Enterprise Secu 平始 设置 → 进行中 完 服务地址: 193.168.12.116 数据库美型: ◎ SQL Server MSDE安装目录: C:\Program File MSDE数据目录: C:\Program File	r,可以选择【MSDE】,设置各项参数后,单击【下一 行理系统软件 (inity Management System 2.0. ▲ ● MSDE es\Rising\ESMMsde es\Rising\ESMMsdeData
古安装环境中已有 MSDE 数据库 瑞星企业终端安全管 Rising Enterprise Secu 开始 设置 → 进行中 完 服务地址: 193.168.12.116 数据库类型: ◎ SQL Server MSDE安装目录: C:\Program File MSDE数据目录: C:\Program File	r,可以选择【MSDE】,设置各项参数后,单击【下一 行理系统软件 (inity Management System 2.0. ▲ ● MSDE es\Rising\ESMMsde es\Rising\ESMMsdeData
古安装环境中已有 MSDE 数据库 端星企业终端安全管 Rising Enterprise Secu 开始 设置 → 进行中 完 服务地址: 193.168.12.116 数据库类型: ◎ SQL Server MSDE安装目录: C:\Program File MSDE数据目录: C:\Program File	F. 可以选择【MSDE】,设置各项参数后,单击【下一 F理系统软件 Inity Management System 2.0. MSDE es\Rising\ESMMsde es\Rising\ESMMsdeData

图示中"ESM"或"esm"为瑞星企业终端安全管理系统软件英文名称"Enterprise Security Management"的缩写。

第七步:进入服务器站点信息设置界面,选择【服务地址】,对所选地址进行【控制台站点模式】设置。有三种站点访问模式可供选择,分别为【默认站点(HTTP)】、【自定义站点(HTTP)】和【自定义站点(HTTPS)】。选择合适模式并设置相关信息后,点击【下一步】。

服务地址:193	3.168.12.116		-
全制台站点模式:◎	默认站点(http)		
0	自定义站点(http)	http端口:12012	
• E	自定义站点(https)	http端口: 12012	
		https端口:10443	
	ht	tps访问地址:193.168.12.11	.6
访问	同示例:https://193.16	8.12.116:10443/esm	

第八步:输入【管理中心服务端口】和【业务中心服务端口】或使用默认端口。设置漏 洞补丁保存路径(默认路径为C:\Program Files\Rising\ESM\rdc\download),点击【下一步。

瑞星企业终	- 端安全管理系统软件	- ×
Rising Enter	prise Security Management System	2.0.1.3
□□ 四二 五 二 五 二 二 二 二 二 二 二 二 二 二 二 二 二 二 二		
开如 反直 🖛 进门	甲 元與	
68.5		
管理中心服务端口:	3333	
业务中心服务端口:	5555	
漏洞补丁保存路径:	C:\Program Files\Rising\ESM\rdc\downloa	选择
	□虚拟化环境	
1000 Contraction (1990)		
漏洞补丁例	存路径所属分区空间不足,小于30G,建议更改存储分	<u>26</u>

提示:漏洞补丁保存路径所属分区剩余空间建议大于 30G。

第九步:进入安装进度界面,可以点击【展开】查看安装进度明细。

开始	Rising 役置	企业终端安全管理系 g Enterprise Security M 进行中 🔶 完成	系统软件 1anagement System		2.0.1.3
	1		模映 用户可 更好的	化子产晶 按需部署, 扩展性和兼容性	
正在安業	专:核心组	件 > >展开		139	6(安装中)

第十步:安装进度完成,点击【完成】结束。



3.2 卸载

瑞星企业终端安全管理系统软件卸载有两种方式:

1、在Windows 画面中,选择【开始】/【所有程序】/【瑞星企业终端安全管理系统软

件】/【卸载】。

2、在 Windows 画面中,选择【开始】/【控制面板】/【添加/删除程序】/【瑞星企业终端安全管理系统软件】/【更改/删除】。

两种方式均会运行产品维护向导,按照界面提示操作即可完成卸载。



3.3 修复

您可以通过修复菜单,重新安装已安装的组件。在Windows 画面中,选择【开始】/【所 有程序】/【瑞星企业终端安全管理系统软件】/【修复系统】,运行产品维护向导,按照界 面提示操作即可完成修复。



4. 产品授权

用户在购买瑞星企业终端安全管理系统软件安装光盘后会得到一个基本包序列号,使用 基本包序列号到瑞星企业终端安全管理系统软件自助服务平台注册,再用下发的用户服务号 和注册密码(请牢记服务号和密码)登录自助服务平台,下载授权文件。将授权文件利用管理 控制台——授权管理导入后,瑞星企业终端安全管理系统软件即可正常使用。授权证书更新、 序列号查询、扩容充值、注销等操作均可使用此平台。

4.1 获取授权

第一步:进入瑞星官网相应版块,进行用户服务号注册。

第二步:根据网站向导提示,输入您的用户信息,产品序列号及购买信息,用户登录口 令,完成用户服务号注册。

第三步:注册成功,网站将返回用户服务号(如:E3NPSLXX)。请记录本服务号,用于 后续登录服务系统,对授权证书进行管理。

第四步:使用获得的用户服务号登录服务系统。进入【证书下载】版块,可查看当前已 北京瑞星信息技术有限公司 24 经注册的基本包序列号、子产品列表、产品服务期限及相应信息。

第五步:选择【下载】,下载授权证书文件。(如:1000086.1ic),本文件用于激活中心服务器程序,请妥善保管。

导入授权		X
基本号: 证书文件:	浏览… 未选择文件。	
		确定

第六步:进入瑞星企业终端安全管理系统软件——管理控制台,打开【授权管理】,点击【导入授权】。在导入授权对话框中,输入基本包序列号,并选择相应的授权证书文件。 点击【确定】,如上图所示。

提示:本步骤需要瑞星企业终端安全管理系统软件已经安装完成。

第七步:管理控制台提示导入成功。在授权管理的产品信息中,可以检查子产品授权状态及授权许可证号等授权信息。至此,产品授权完成。

5. 系统登录

瑞星企业终端安全管理系统软件安装完成后在桌面会自动生成瑞星企业终端安全管理 系统软件的快捷方式,点击此快捷方式即可登录瑞星企业终端安全管理系统软件——管理控 制台。

首次登录默认用户名为: admin 密码为: 123456。只有修改初始密码后才能进入系统。

瑞星企业	业终端安全自	锂系统软件		
用户名:		-		
· · · · · · · · · · · · · · · · · · · ·				
」		•		
	■ 记住密码	登录		
点击瑞星企业终端多	天全管理系结	统软件——管	會理控制	台页面上

切换至审计台 C 按钮可切换到审计控制台: 点击瑞星企业终端安全管理系统软件 切换至管控台 ●

--宙计控制台页面上方 可切换到管理控制台。

管理控制台 6.

瑞星企业终端安全管理系统软件——管理控制台是一个面向企业计算机管理员及企业 管理者的基于 Web 的管理控制界面。管理控制台使得管理员能够对网络中的所有客户端进行 有针对性的策略分配、配置管理并可以查看客户端信息以及监控计算机的使用情况,从而保 障企业资产及企业敏感信息的安全。



管理控制台主要包括【安全中心】、【日志报告】、【计算机管理】、【授权管理】和【用户 管理】五大功能。

6.1 安全中心

安全中心是管理控制台的首页,显示瑞星企业终端安全管理系统软件的运行概况及客户 端概况。在安全中心界面中主要显示【今日提醒】、【收藏夹】、【客户端在线情况】、【防病毒】、 【病毒类型统计】、【全网病毒趋势统计】和【产品授权信息】等统计情况。

今 → 账户[admin]从[193.168.11.74]登陆成功 2014-06-24 10:10 收 E 暂时没有收藏内容,常用的日志报告可以收藏起来哦~ →账户[admin]从[193.168.11.74]登陆成功 2014-06-20 11:14 藏 提 夹 醒 → 用户admin删除了组[根管理组]的策略 2014-06-17 14:25 最近24小时 🧾 3台在线 占全网100% 🔜 0台不在线 占全网0% 客户端名称 客户端IP 病毒发作次数 1/1在线 2.0.0.9 xp(412F8C64464F4F7) 193.168.12.7 1 2.0.0.7 2/2在结 病毒类型 ■ 未处理 部署更多客户端 全网升级 🔲 成功 客户端查看 域信息 策略模板 共有策略 客户端备注 没有发现新的未知客户端 立即查看 用户您好,授权状态一切正常! 授权信息如下: 🔺 收起 行为审计 200点 2013-01-21到2014-01-21 IT资产管理 2013-01-21到2014-01-21 200点

6.2 日志报告

【日志报告】主要包括【日志查询】、【报告查询】、【定时报告】和【综合报告查询】等 子功能分类的相关信息。为企业全面记录计算机的各种使用数据,保障资产安全。

6.2.1 日志查询

日志查询包括【系统事件日志】、【防病毒】、【漏洞扫描】和【IT 资产管理】四个子产品记录的客户的各种使用情况。

김) ING 瑞星瑞星企业终端安全管理系统软件用户手册

日志查询 报告查询 定时报告 综合报告查询 系统事件日志 管理中心事件查询 业务中心事件查询 客户端事件查询 升级中心日志查询 网络连接测试日志查询 客户端升级日志音询 客户端子产品统计 防病毒(XAV) 病毒扫描结果奋狗 Q 漏洞扫描(RLS) 漏洞扫描结果查询 IT资产管理(RAM) 硬件异动日志查询 设备异动日志查询 设备扫描日志查询 软件扫描日志查询 软件部署日志查询 Ħ

6.2.1.1 系统事件日志

【系统事件日志】就是系统、客户端操作记录。显示最近十条管理中心事件,包括用户 登录信息、具体操作以及具体时间等。

【系统事件日志】包括【管理中心事件查询】、【业务中心事件查询】、【客户端事件查询】、 【客户端升级日志查询】、【升级中心日志查询】、【网络连接测试日志查询】和【客户端子产 品统计】等七类相关日志信息。

6.2.1.2 防病毒

【防病毒】即【病毒扫描结果查询】。显示最新发现的十条病毒记录,包括时间、IP、 机器名、病毒名称、分类和染毒文件。

时间范围:本周 ▼	病毒扫描结果日志					[返回]	
Ж	🦻 时间	IP	机器名	病毒名称	分类	染毒文件	
到	2013/6/27 15:12:04	193.168.12.7	xp(412F8C64464F4F7)	Trojan.Win32.Generic.1468959A	木马	C:\Documents and S	l
	2013/6/27 15:07:09	193.168.12.7	xp(412F8C64464F4F7)	Trojan.Win32.Generic.1468959A	木马	C:\Documents and S	l
病毒分类: - 全部 - ▼	2013/6/27 14:33:40	193.168.12.7	xp(412F8C64464F4F7)	Trojan.Win32.Generic.153B9923	木马	E:\TDDOWNLOAD\S	l
病毒来源: - 全部 - 🔻	2013/6/27 14:33:40	193.168.12.7	xp(412F8C64464F4F7)	Trojan.Win32.Generic.153C0BDA	木马	E:\TDDOWNLOAD\S	l
处理方式: - 全部 - ▼	2013/6/27 14:33:40	193.168.12.7	xp(412F8C64464F4F7)	Trojan.Win32.Generic.1539C60A	木马	E:\TDDOWNLOAD\S	
病毒状态: - 全部 - ▼	2013/6/27 14:28:07	193.168.12.7	xp(412F8C64464F4F7)	Trojan.Win32.Generic.1565D3CE	木马	E:\TDDOWNLOAD\S	
客户端: Q	2013/6/27 14:27:44	193.168.12.7	xp(412F8C64464F4F7)	Trojan.DL.Sex8!55DC	木马	E:\TDDOWNLOAD\N	
	2013/6/27 14:16:29	193.168.12.7	xp(412F8C64464F4F7)	Trojan.Win32.Generic.156497BE	木马	E:\TDDOWNLOAD\S	
域: 我的组织 🔻	2013/6/27 14:07:32	193.168.12.7	xp(412F8C64464F4F7)	Trojan.Win32.Generic.155AA9D3	木马	E:\Downloads\softwa	
	2013/6/27 14:07:22	193.168.12.7	xp(412F8C64464F4F7)	Trojan.Win32.Generic.1519A35D	木马	E:\Downloads\softwa	
查询	2013/6/27 14:05:48	193.168.12.7	xp(412F8C64464F4F7)	VirTool.Linux.Elfwrsec.b	病毒	D:\病毒样本\ELF123\	
	2012/0/27 14:05:40	103100137		VINTE ET ENLEN KALANCE	/= =	D.\. ++++++ FI F1 22	

在左侧查询条件中输入相应条件(不输入查询条件默认搜索全部漏洞扫描结果):

时间范围:选择【时间范围】本周/上周/本月/上月或指定范围(20xx/xx/xx/xx: xx²20xx/xx/xx/xx: xx);

病毒分类:选择可疑、病毒、蠕虫、rookit、广告、木马、后门、壳。
病毒来源:选择快速查杀、全盘查杀、自定义查杀、文件监控、邮件监控。
处理方式:选择暂未处理、忽略、删除、清除、信任、上报。
病毒状态:选择未处理、成功、处理失败、备份失败、处理中。

客户端: 输入客户端名称。如果需要搜索客户端名称可以点击, 弹出查找计算机页面, 设置搜索关键字和所在组, 点击【立即查找】则可以查找到相关计算机, 选择需要的计算机名称, 再点击【确定】。

查找计算机				X
搜 索: 所在组: 组织结构范围	© ਮੇ	⊦算机名称 ◎ MAC ◎ IP	立即查找	
名称	IP	MAC	所在组	^
	任意计算	拿机		
412F8C64464F4F7	193.168.12.7	44-87-FC-A4-9C-52	根管理组	
LIUYH-PC	193.168.11.74	00-24-E8-23-9A-A2	根管理组	
				Ŧ

域:选择所在的组织。

在【病毒扫描结果】中,点击【时间】左侧 图标,在弹出的【可选列】窗口中,对显示分类进行选择,可勾选【IP】、【机器名】、【病毒名称】、【分类】、【染毒文件】、【来源】、 【处理方式】和【状态】,点击【保存】设置成功。

可选列	
 ☑ IP ☑ 机器名 ☑ 病毒名称 ☑ 分类 ☑ 分类 ☑ 公表 ☑ 型 来) ☑ 型 大态 	
保存	取消

6.2.1.3 漏洞扫描

【漏洞扫描】即【漏洞扫描结果查询】。单击【日志查询】/【漏洞扫描结果查询】/【查询】即可得到漏洞扫描结果【IP】、【机器名】、【名称】、【危险等级】、【分类】、【状态】和【描述】等信息。

名称:		漏洞扫描结果							[返回]
危险等级:	- 全部 - 🔹 🔻	🧑 IP	机器名	名称	危险等级	分类	状态	描述	
状态:	- 全部 - 🔹 🔻	193.168.12.7	xp(412F8C64464F4F7)	KB2898785	高危	IE更新	已过期	Microsoft 安全公告 MS13-097 - 严重	E Intei
		193.168.12.7	xp(412F8C64464F4F7)	KB2709162	重要	系统更新	已过期	Microsoft 安全公告 MS12-041 - 重要	₹ Win
域: 1	数的组织 ▼	193.168.12.7	xp(412F8C64464F4F7)	KB2647516	中等	IE更新	已过期	Microsoft 安全公告 MS12-010 - 严重	≣ Intei
	查询	193.168.12.7	xp(412F8C64464F4F7)	KB968537	重要	系统更新	已过期	Microsoft 安全公告 MS09-025 - 重要	문 Win
		193.168.12.7	xp(412F8C64464F4F7)	KB2570947	重要	系统更新	已修复	Microsoft 安全公告 MS11-071 - 重要	툰 Win
		193.168.12.7	xp(412F8C64464F4F7)	KB975254	重要	系统更新	未修复	Microsoft 安全公告 MS09-053 - 重要	₹用于
		193.168.12.7	xp(412F8C64464F4F7)	KB953838	高危	IE更新	已过期	Microsoft 安全公告 MS08-045 - 严重	E Intei
		193.168.12.7	xp(412F8C64464F4F7)	KB2744842	高危	IE更新	已过期	Microsoft 安全公告 MS12-063 - 严重	E Intei
		193.168.12.7	xp(412F8C64464F4F7)	KB938464	高危	系统更新	已过期	Microsoft 安全公告 MS08-052 - 严重	E GDI
		193.168.12.7	xp(412F8C64464F4F7)	KB2620712	重要	系统更新	已修复	Microsoft 安全公告 MS11-097 - 重要	₹ Win
		193.168.12.7	xp(412F8C64464F4F7)	KB2506223	重要	系统更新	已过期	Microsoft 安全公告 MS11-034 - 重要	€ Win

在左侧查询条件中输入相应条件(不输入查询条件默认搜索全部漏洞扫描结果):

名称:可以输入漏洞名称 ID。

危险等级:可以选择全部、高危、重要、中等、一般或轻微。

状态:可以选择全部、未修复、已修复、修复失败或已忽略。

域:选择所在的组织。

在【漏洞扫描结果】中,点击【IP】左侧 图标,在弹出的【可选列】窗口中,对显示分类进行选择,可勾选【机器名】、【名称】、【危险等级】、【分类】、【状态】和【描述】, 点击【保存】设置成功。



6.2.1.4 IT 资产管理

【IT 资产管理】主要包括【硬件异动日志查询】、【设备异动日志查询】、【设备扫描日 志查询】、【软件扫描日志查询】和【软件部署日志查询】等相关信息,帮助企业有效管理企 业 IT 资产。

6.2.1.4.1 硬件异动日志查询

单击【日志查询】/【硬件异动日志查询】,在打开的页面中选择【时间范围】本周/上 周/本月/上月或指定范围(20xx/xx/xx/xx: xx²0xx/xx/xx/xx: xx);在【变更类型】中选 择【全部】、【添加】、【移除】或【变更】,点击【查询】即可得到相关信息。

硬件异动日志	
吹1十7十4月日/心	

	[返回]

190	0.163	TD	扣架夕	夕街	本百米刑	1日 <i>北</i> -44田	*
6	ניונים	115	们的合	白仦	受史天主	採TF结果	
				没有符合条件	的数据		
		. 41. T 7.					
	仕 (1)	出的【彻	『件异动日志』 甲	会显示【时	间】、【IP】、【机器名】	1、【名称 】、【	7
					454		

和【操作结果】等具体信息。您也可以点击【时间】左侧 图标,在打开的【可选列】窗口中,对显示分类进行选择,可勾选【IP】、【机器名】、【名称】、【变更类型】和【操作结果】, 点击【保存】设置成功。

🔹 时间	
可选列	
 ♥IP ♥机器名 ♥名称 ♥空更类型 ♥操作结果 	
保存	取消

6.2.1.4.2 设备异动日志查询

单击【日志查询】/【设备异动日志查询】,在打开的页面中选择【时间范围】本周/上 周/本月/上月或指定范围(20xx/xx/xx/xx: xx²20xx/xx/xx/xx: xx);在【变更类型】中选 择【全部】、【添加】或【移除】,点击【查询】即可得到相关信息。

	设备界	动日志							[返回]
	9	时间	IP	机器名	设备分类	名称	变更类型	操作结果	*
					没有符合条	件的数据			
	7	在查诉	可出的	【设备异动E	志】中会显示【	时间】、【I	P】、【机器名】、【	设备分类人	【名称】、
	变	軍 拳型	リ】和	【操作结果】	等具体信息。您	也可以点	[击【时间】左侧	● 图标,	在打开的
	~.	~/~1						(1,1,1)	
I	(可)	选列】	窗口	中,对显示分	▶类进行选择,可	勾选【IP	】、【 机器名】、【	设备分类】、	【名称】、

🔅 时间	
可选列	
 ♥IP ♥机器名 ♥设备分类 ♥名称 ♥空更类型 ♥操作结果 	
保存	取消

6.2.1.4.3 设备扫描日志查询

【变更类型】和【操作结果】,点击【保存】设置成功。

单击【日志查询】/【硬件扫描日志查询】,在【设备分类】一栏中输入需查询的设备分 类名称,且分类名称只支持完整查询,不支持缩略查询,点击【查询】即可得到相关信息。

提示:【设备分类】中不输入任何硬件分类名称即默认查询全部硬件扫描日志。

WHITH HID

2番扫描日志	ā		[返回]
🦻 IP	机器名	设备分类	名称	-
193.168.1	1.74 LIUYH-P	C DVD/CD-ROM 驱动器	DTSOFT Virtual CdRom Device	
193.168.11	1.74 LIUYH-P	C DVD/CD-ROM 驱动器	PLDS DVD-ROM DH-16D5S ATA Device	
193.168.11	1.74 LIUYH-P	C IDE ATA/ATAPI 控制器	ATA Channel 0	-
193.168.11	1.74 LIUYH-P	C IDE ATA/ATAPI 控制器	Intel(R) ICH10 Family 2 port Serial ATA Storage Controller 2 - 3A26	
193.168.11	1.74 LIUYH-P	C IDE ATA/ATAPI 控制器	Intel(R) ICH10 Family 4 port Serial ATA Storage Controller 1 - 3A20	_
193.168.11	1.74 LIUYH-P	C IDE ATA/ATAPI 控制器	ATA Channel 1	
193.168.11	1.74 LIUYH-P	C IDE ATA/ATAPI 控制器	ATA Channel 0	

.

	,		
193.168.11.74 LIUYH-PC	IDE ATA/ATAPI 控制器	ATA Channel 1	
193.168.11.74 LIUYH-PC	IDE ATA/ATAPI 控制器	ATA Channel 0	
193.168.11.74 LIUYH-PC	IDE ATA/ATAPI 控制器	ATA Channel 1	
193.168.11.74 LIUYH-PC	人体学输入设备	USB 输入设备	
193.168.11.74 LIUYH-PC	图像设备	Canon MF4400 Series	
193.168.11.74 LIUYH-PC	声音、视频和游戏控制器	Realtek High Definition Audio	
193.168.11.74 LIUYH-PC	声音、视频和游戏控制器	Intel(R) High Definition Audio HDMI	
193.168.11.74 LIUYH-PC	处理器	Pentium(R) Dual-Core CPU E5200 @ 2.50GHz	
193.168.11.74 LIUYH-PC	处理器	Pentium(R) Dual-Core CPU E5200 @ 2.50GHz	
193.168.11.74 LIUYH-PC	存储卷	通用卷	
193.168.11.74 LIUYH-PC	存储卷	通用卷	
•		III	Þ

共164条记录,1/4页 ◀ ▶ 50 ▼

在查询出的【设备扫描日志】中会显示【IP】、【机器名】、【设备分类】和【名称】等具

体信息。您也可以点击【IP】左侧 图标,在打开的【可选列】窗口中,对显示分类进行 选择,可勾选【机器名】、【设备分类】和【名称】,点击【保存】设置成功。



6.2.1.4.4 软件扫描日志查询

单击【日志查询】/【软件扫描日志查询】, 在【软件名称】和【软件厂商】中输入中文 或英文相关信息,点击【查询】即可。

提示: 在【软件名称】和【软件厂商】中不输入任何信息即默认查询全部软件扫描日 志。

软件扫描日志

[返回]

🧽 IP	机器名	软件名称	版
193.168.11.74	LIUYH-PC	Microsoft Windows SDK for Visual Studio 2008 Win32 Tools	6.:
193.168.11.74	LIUYH-PC	Microsoft SQL Server Compact 3.5 CHS	3.!
193.168.11.74	LIUYH-PC	Adobe Reader XI (11.0.07) - Chinese Simplified	11
193.168.11.74	LIUYH-PC	搜狗拼音输入法 6.7正式版	6.7
193.168.11.74	LIUYH-PC	FAST 无线USB网卡 驱动	1.:
193.168.11.74	LIUYH-PC	腾讯QQ2013	1.9
193.168.11.74	LIUYH-PC	Microsoft Visual Studio Team System 2008 Team Suite - 简体中文	
193.168.11.74	LIUYH-PC	Microsoft SQL Server Compact 3.5 for Devices CHS	3.!
193.168.11.74	LIUYH-PC	Microsoft Visio Premium 2010	14
193.168.11.74	LIUYH-PC	Crystal Reports Basic Simplified Chinese Language Pack for Visual Studio 2008	10
193.168.11.74	LIUYH-PC	FlashFXP v3.6 Final	5.1
193.168.11.74	LIUYH-PC	Microsoft SQL Server Desktop Engine (RSESM)	8.(
193.168.11.74	LIUYH-PC	MSXML 4.0 SP3 Parser (KB2758694)	4.:
193.168.11.74	LIUYH-PC	TortoiseSVN 1.4.1.7992 (32 bit)	1.4
193.168.11.74	LIUYH-PC	瑞星软件部署系统	23
193.168.11.74	LIUYH-PC	Microsoft SOAP Toolkit 3.0	3.(
•		III	•

共101条记录 , 1/3页 🛛 🚺 50 👻

在查询出的【软件扫描日志】中会显示【IP】、【机器名】、【软件名称】、【版本】和【软件厂商】具体信息。您也可以点击【IP】左侧 图标,在打开的【可选列】窗口中,对显示分类进行选择,可勾选【机器名】、【软件名称】、【版本】和【软件厂商】,点击【保存】 设置成功。



6.2.1.4.5 软件部署日志查询

单击【日志查询】/【软件部署日志查询】,在【状态】栏通过下拉列表选择需要查询的 条件,点击【查询】即可。

软件部署日志						[返回]				
	9	时间	IP	机器名	软件名称	软件厂商	软件分类	状态	软件版本	*
						没有符合条件的数据				

在查询出的【软件部署日志】中会显示【时间】、【IP】、【机器名】、【软件名称】、【软件

厂商】【软件分类】、【状态】和【软件版本】具体信息。您也可以点击【时间】左侧 🔅 图标,在打开的【可选列】窗口中,对显示分类进行选择,可勾选【IP】、【机器名】、【软件名称】、【软件厂商】、【软件分类】、【状态】和【软件版本】,点击【保存】设置成功。

🔅 时间	
可选列	
 ☑ IP ☑ 机器名 ☑ 软件名称 ☑ 软件厂商 ☑ 软件分类 ☑ 状态 ☑ 软件版本 	
保存	取消

6.2.2 报告查询

【报告查询】主要是把分散的日志、信息等按照一定的规则进行统计、分析。包括【系 统事件报告】、【防病毒】和【IT资产管理】三个子产品收集反馈的相关信息统计。

系统事件报告:即【客户端子产品统计】。

防病毒:即【病毒趋势统计】。

IT 资产管理:包括【设备异动趋势统计】、【设备类型统计】和【装机软件统计】三大 类信息。
AISING 瑞星。 瑞星企业终端安全管理系统软件用户手册

日志查询 报告	查询 定时报告 综合报告查询		
系统事件报告			·
客户端子产品统;	ł		
防病毒(XAV)			
肉毒趋势统计			E
IT资产管理(RAM)			
设备异动趋势统计	设备类型统计	装机软件统计	

选择不同的报告类型查看相关信息时,查询方式及界面会有所不同,但是与【日志查询】 中的操作基本相同。下面以【IT资产管理】/【设备异动趋势分析】为例介绍报告查询。

单击【日志查询】/【报告查询】/【设备异动趋势统计】/【查询】即可得到硬件异动 趋势图表。

在左侧查询条件中输入相应条件(不输入查询条件默认搜索本周硬件异动信息):

时间范围:可以选择本周/上周/本月/上月或指定范围(20xx/xx/xx/xx: xx²20xx/xx/xx/xx: xx)。



上图中折线图部分展示的是硬件【添加】/【移除】的趋势,折线图的下面数据表则以 详细数据的形式展示某一时间段【添加】/【移除】硬件的总数。

在【硬件异动趋势统计】中,点击【时间】左侧 整图标,在弹出的【可选列】窗口中,

对显示分类进行选择,可勾选【增加的硬件总数】和【移除的硬件总数】,点击【保存】设置成功。



6.2.3 定时报告

【定时报告】是某一种或几种类型且经过一定条件过滤的统计分析报告在规定的时间发送至管理人员邮箱,使其能够方便有效的了解到相关信息。

单击【日志查询】/【定时报告】/【查询】即可得到报告的定时报告【标题】、【类型】、 【创建时间】和【操作】等信息。

V	日志查询	报告查询	定时报告	综合报告	查询			
报告类型:	全部	•	标题		类型	创建时间	操作	*
	查询					没有符合条件的数据		
d.								
								Ŧ
			新建定时报	告				

在左侧查询条件中输入相应条件(不输入查询条件默认搜索全部定时报告):

报告类型:可以自十五种统计方式中选择,包括全部、存储设备统计、客户端操作系统 统计、客户端聊天统计、客户端网址访问统计、客户端文件打印趋势、客户端文件访问趋势、 杀毒软件统计、设备类型统计、设备异动趋势、网址访问统计、网址审计结果统计、文档审 计结果统计、文档审计统计和装机软件统计。

▶ 新建定时报告

在此页面可以新建定时报告,点击页面左下角 新建定时报告 按钮会弹出新建定时报 告窗口。

		保存 取消
报告标题:	新建定时报告	
报告类型:	病毒趋势统计	
功能介绍:	统计一段时间内,病毒查杀的数量,以折线图表现	
接收人Email:		
时间计划:	每天 🔻 发送时间: 9:00	
过滤条件:	此报告无设置参数	

报告标题: 输入报告名称。

报告类型: 可选择多种类型:

- 病毒趋势统计:统计一段时间内,病毒查杀的数量,以折线图表现。
- 存储设备统计:统计一段时间内,移动存储设备被审计的数量。
- 客户端操作系统统计:统计全网所有客户端所装操作系统的种类与数量。
- 客户端聊天统计:统计一段时间内全网内各客户端聊天记录的数量,以柱状图
 形式按从多到少的顺序展示。
- 客户端网址访问统计:针对指定的客户端统计其一段时间之内访问网址的数量
 趋势,以折线图表现。
- 客户端文件打印趋势:针对指定的客户端统计其一段时间之内文件打印数量趋势,以折线图表现。
- 客户端文件访问趋势:针对指定的客户端统计其一段时间之内文件访问的数量
 趋势,以折线图表现。
- 杀毒软件统计:统计全网所有客户端所装杀毒软件的种类与数量。
- 设备类型统计:按类别统计全网所有客户端硬件数量。
- 设备异动趋势:统计全网所有客户端硬件随时间的增减变化趋势,以双折线图表现。
- 网址访问统计:按 URL 统计一段时间内,客户端上网访问网址的审计次数。
- 网址审计结果统计:统计一段时间内,全网客户端上网被允许与被拒绝的比例。

- 文档审计结果统计:统计一段时间内,全网客户端访问文件被允许与被拒绝的 比例。
- 文档审计统计: 按文件名统计一段时间内, 客户端访问文件审计次数。
- 装机软件统计:统计全网所有客户端安装软件的种类与数量。

功能介绍:主要介绍各个报告类型的作用,帮助管理员建立正确的符合需要的定时报告。 **接收人 Email:** 输入本报告邮件接收人的电子邮箱。

提示:本功能需事先在【服务器管理】/【外围服务器】/【邮件服务器设置】中对 SMTP 服务器进行设置。

时间计划:在此可以设置报告发送的,每天的任意时间点/每周某天或某几天任意时间 点/每月某一的任意时间点。

过滤条件:

- 时间范围:最近 X 天
- 审计结果:可以选择全部、允许或拒绝
- 统计数目:统计前 X 名移动存储设备被审计事件

当完成以上设置后,点击【保存】定时报告即添加成功。

6.2.4 综合报告查询

【综合报告查询】是根据不同的查询条件,生成一个综合性的报告,集各种风险于一体 展示给用户。

综合报告可以打印或者导出 pdf 文件,还可以保存并收藏,下次可以进行快速查询,或 者在安全中心的收藏夹直接查看收藏的日志报告。

日志查询 报告查询 定时报告 综合报告查询 选择报告 快速查询 默认 -类型: 防病毒 受病毒感染的计算机 保护不完整的计算机 防毒系统病毒库升级概况 计算机病毒扫描 病毒检测数量分布 病毒趋势分析 按病毒来源分布 主动防御系统加固报表 主动防御ATP应用防护报表 系统加固检测 ATP应用防护检测 终端查询条件 时间: 过去24 本周 本月 上周 上月 本年 上年 指定日期 从 2013-06-25 🛗 到 2013-06-25 🛗 ● 计算机名称 ○ IP地址 ○ MAC 终端: 在线状态:不限 已登录 未登录 **直**级条件 🔥 日志查询条件へ 生成报告 快速查询: 保存 保存并收藏

选择报告类型:可以自十一种统计方式中选择,包括受病毒感染的计算机、保护不完整的计算机、防毒系统病毒库升级概况、计算机病毒扫描、病毒检测数量分部、病毒趋势分析、按病毒来源分布、主动防御系统加固报表、主动防御 ATP 应用防护报表、系统加固检测、ATP 防护检测。

终端查询条件:查询条件包含时间、终端、在线状态、高级条件、以及针对报告类型的 其他查询条件。

6.3 计算机管理

计算机管理为瑞星企业终端安全管理产品最核心的内容,可实现对管理域内客户端计算 机的审计与控制管理。可对客户端计算机进行分组管理,并且可以通过配置、下发不同的策 略使管理更具操作性、个性化和针对性,真正做到为企业的内部资产安全建立起一个可靠的 监控管理体系。

RISING 瑞星瑞星企业终端安全管理系统软件用户手册

域信息 子	域信息 策略模板 客户端 著	客户端备注			Q隐藏搜索区
	搜索: 登录状态: 全部 ▼	所在组: 维	 ●计算机名称 ● い算机名称 ● い 	/IAC◎IP◎版本]	查询
黑名单	□ 名称	策略来源 IP	版本 所在组	连接业务中心 静态授权	所属域 ^
	🔲 💻 xp(412F8C64464F4F7)	继承 193.168.12.7	2.0.0.7 根管理组	193.168.11.74 否	我的组织
	🔲 💻 LIUYH-PC	继承 193.168.11.74	2.0.0.7 根管理组	193.168.11.74 否	我的组织
	🔲 💻 PC_YY	继承 193.168.11.72	2.0.0.9 根管理组	193.168.11.74 否	我的组织
4					
۰ III ۲	移动到 删除静态授权 客户端命令	在线客户端:3台		共3条记录,1/1页 🛛 🖌	▶ 50 ▼

김〉INC 瑞星瑞星企业终端安全管理系统软件用户手册

在计算机管理界面左侧显示的是组管理界面,其中包括:

- 我的组织:即"域"的概念。域包括当前网络环境中所有被发现的客户端的集合。
- 根管理组:即普通组,是指可正常下发策略,接受审计与管控管理的客户端的 集合。也可以根据需要建立不同的子组,进行有针对性的分组管理。
- 服务器管理:即各中心所使用的服务器,包括瑞星软件部署升级中心(RUC)、 瑞星业务中心(BUS)、系统数据中心、补丁下载中心以及管理中心(即管理平 台自身服务器)。
- 未知计算机:客户端已经被程序发现,但并未被划归至任意根管理组/黑名单的计算机的集合。未知计算机不可下发策略,而且可能并没有安装相应的客户端软件。
- 黑名单:不想进行管理的客户端的集合。加入黑名单的客户端,系统无法对其 下发策略或其他命令。

6.3.1 我的组织

我的组织,指企业网络中所有被发现的客户端的域,是最高级别的管理域。点击【计算 机管理】打开的页面即为【我的组织】页面,主要包括菜单栏、搜索区、客户端列表和操作 栏四部分内容。 其中搜索区功能最为简单,在此做简单介绍。由于功能类似,以后不再说明。此功能主 要用于当客户端较多时,实现快速查找。

设置相关信息:

计算机名称/MAC/IP/版本:可输入计算机名称、MAC 地址、IP 或版本,作为过滤条件。 登录状态:可选择全部、已登录、未登录。

所在组:可选择根管理组或具体子组(只有在根管理组,此功能可选,其它组均为默认, 不可选)。

设置完成后点击【查询】即可。

6.3.1.1 菜单栏

菜单栏主要包括【域信息】、【子域信息】、【策略模板】、【客户端】和【客户端备注】五个功能分区,在这里可以查看管理我的组织的基本信息、客户端和策略等相关内容。

域信息 子域信息 策略模板 客户端 客户端备注 Q 隐藏搜索区

6.3.1.1.1 域信息

在【域信息】可以修改"我的组织"的名称并可以添加对"我的组织"的描述信息。 单击【计算机管理】/【域信息】进入界面。

域信息			保存
域名称:	我的组织		
描述信息:			
1 10 1410+11	https://193.168.11.74:10443	(下級访问地址)	
RUBIE:		(上級访问地址)	
验证码:			
已连父域:	否连接		
保存			

6.3.1.1.2 子域信息

在【子域信息】可以连接在这个域下的子域。

单击【计算机管理】/【子域信息】进入界面。连接在这个域下的子域

域信息	子域信息 策略模板 芬	共有策略 客户端 客户端备注			
▲ 我的组织 ● 與根管理组	连接子域				
。服务器管理 未知计算机 黑名单	域名称	描述	地址	操作	*

点击【连接子域】,输入站点地址和验证码,点击【连接】即可。

连接子域		х
站点地址	如 : http://192.168.0.1:80]
验证码		连接

6.3.1.1.3 策略模板

登录管理控制台, 依次点击【计算机管理】/【我的组织】/【策略模板】, 进入策略设

置界面。

选择子产品: IT资产管理							
IT资产管理 (RAM) 防病毒 (XAV) 客户端代理 (EP) 漏洞扫描 (RLS) 软件部署组件 (RUA)		IT资产管理子产品。			添加	口策略相	莫板
策略模板							
名称: 瑞星网络安全管理 出厂设置 描述: 产品: 网络安全管理(RSM) [安全管理策略	8]						
			详情	分配	复制	删除	导出

【策略模板】安全管理平台自带的预先设置的策略配置,企业可以根据自身需要选用、 编辑或创建合适的模板并可统一分配至根管理组(普通组),以实现策略的快速统一分配。 目前策略模板包括【IT资产管理(RAM)】、【防病毒(XAV)】、【客户端代理(EP)】、【漏洞扫 描(RLS)】和【软件部署(RUA)】五个策略模板。

IT资产管理(RAM)

IT 资产管理属于企业的精细化管理范畴。

该子产品策略分为两部分内容【IT 资产管理-默认策略】和【IT 资产管理-软件部署策略】。用于扫描并记录客户端计算机的硬件信息,同时对硬件资产的变更也做详细的记录, 通过单一控制台即可掌握整个企业的 IT 硬件资产信息;并且可以保护指定的软件、进程、 以及服务,防止终端中运行的这些服务、进程被登录的用户强杀、删除、停止服务。这样可 以做到企业内部的某些关键应用可以被有效的保护起来,而不被终端登录用户手动停止,或 者第三方程序强制停止。

防病毒(XAV)

属于日常维护性管理范畴,能够在客户端计算机进行工作、上网等活动时,有效保护用户的个人数据不会被恶意程序窃取以及破坏。

客户端代理(EP)

该策略是基础性子产品,是其它子产品插件的基础。客户端代理不允许设置策略,本文 档将不再详细介绍。

漏洞扫描 (RLS)

该策略是负责扫描并修补客户端上的系统漏洞与应用程序漏洞。可为您提供全面的漏洞 管理服务,可以帮助您杜绝主机层面或网络层面的威胁,从而阻止非法侵入或窃取,保障您 的系统安全。

软件部署组件 (RUA)

该策略是基础性子产品,负责更新升级客户端上的其它子产品。

6.3.1.1.3.1 添加策略模板

依次点击【计算机管理】/【策略模板】/【添加策略模板】打开添加模板界面。

添加策略模板	

	770-00-07
住な	HV:当
NV 13	-10/13

策略名称:	17资产管理 策略模板
对应产品:	IT资产管理(RAM) - 默认策略 ▼
描述信息:	
70776	
已分配组	
策略内容:	IT资产管理
	● □启用硬件异动扫描
	禁用软件列表 添加
	• 🗌 触犯规则后上报日志 🗐 触犯规则后提示用户
	当前没有列表项,请添加。
	保护软件列表 添加
	• 🗏 触犯规则后上报日志 🗏 触犯规则后提示用户
	当前没有列表项,请添加。
	软件保护白名单 添加
	● 当前没有列表项,请添加。
	进程管理
	• □记录进程启动历史

保存取消

在添加界面包括五方面的内容:

- 策略名称:为添加的模板确定名称。若不输入,在选择对应产品时名称会自动 变更。
- 对应产品:即选择瑞星提供的子产品中的一个。
- 描述信息: 描述创建模板的目的之类的信息。
- 已分配组:通过此信息可防止重复建立或分配模板。
- 策略内容:展示模板的主要功能。

提示:可重复建立基于任何一个子产品的模板。

6.3.1.1.3.1.1 创建 IT 资产管理策略模板

一、 IT 资产管理-默认策略

依次点击【计算机管理】/【策略模板】/【添加策略模板】打开添加模板界面。

在对应产品中选择【IT 资产管理-默认策略】并输入【策略名称】/【描述信息】/【已 分配组】等相关信息再设置策略内容。

策略内容:

- IT 资产管理:勾选【启用硬件异动扫描】对客户端机器上的硬件进行扫描,记录
 硬件异动、设备插拔变化并且发送到系统中心汇总处理。管理员可以查看相关审计
 日志。
- 禁用软件列表:点击添加启动添加规则页面,分别对软件库、服务以及自定义进程 进行规则设定,达到软件禁用目的。可勾选【触犯规则后上报日志】、【触犯规则后 提示用户】。
- 保护软件列表:点击添加启动添加规则页面,分别对软件库、服务以及自定义进程 进行规则设定,达到软件保护目的。可勾选【触犯规则后上报日志】、【触犯规则后 提示用户】。
- 软件保护白名单:点击添加启动添加规则页面,分别对软件库、服务以及自定义进程进行规则设定。
- 进程管理:勾选记录进程启动历史。

点击【保存】模板为创建成功;点击【取消】为不保存。

二、IT 资产管理-软件部署策略

依次点击【计算机管理】/【策略模板】/【添加策略模板】打开添加模板界面。

在对应产品中选择【IT资产管理-软件部署策略】并输入【策略名称】/【描述信息】/ 【已分配组】等相关信息再设置策略内容。

点击^{添加}启动添加规则页面,可通过【软件库中推荐软件】和【自定义软件】两种方式 设置需要部署软件的下载源、版本号、注册表等信息以达到第三方软件部署的目的。

6.3.1.1.3.1.2 创建防病毒策略模板

依次点击【计算机管理】/【策略模板】/【添加策略模板】打开添加模板界面。

在对应产品中选择【防病毒-默认策略】并输入【策略名称】/【描述信息】/【已分配 组】等相关信息后再设置【策略内容】。

策略内容

策略内容包括【公共设置】、【扫描设置】、【文件监控设置】和【邮件监控设置】四方面内容。

- A. 公共设置
 - 白名单、排除列表:可分别对文件、目录及扩展名设置为白名单,扫描和监控默认 不扫描
 - 云查杀相关设置:可对 CPU 占用率、云连接测试时间间隔、是否启动公有云及私 有云相关设置
 - 隔离区:设置杀毒时是否备份原文件、空间不足的处理方式、隔离失败时的处理方式、大文件的处理方式
 - 启动病毒跟踪功能:方便管理员了解病毒爆发的起始时间、机器、数量等情况
 - 启用 U 盘监控:防止病毒从 U 盘进入电脑
 - 启用内存模式病毒库:可以加快病毒扫描的速度
 - 加载木马库:可以更快速,更全面的扫描木马
 - 记录病毒日志:方便管理员查询病毒日志
- B. 扫描设置
 - 启动定时全盘扫描:提供【开机】、【每天】、【每周】三种扫描时机设置,管理员可 根据自身需求进行定时设置
 - 启动定时快速扫描:提供【开机】、【每天】、【每周】三种扫描时机设置,管理员可
 根据自身需求进行定时设置

引入ING 瑞星瑞星企业终端安全管理系统软件用户手册

- 扫描文件类型:设置扫描的文件类型
- 普通扫描引擎:提供【启发式扫描】、【仅扫描流行病毒】和【启动压缩包扫描】三
 种扫描方式
- 启用云扫描引擎:通过云端引擎进行扫描
- 发现病毒处理方式: 自定义病毒处理方式
- C. 文件监控设置
 - 开机是否默认不开启:设置开机是否默认开启文件监控功能
 - 锁定不允许客户端关闭监控: 勾选后客户端用户无法手动关闭文件监控
 - 启动智能监控:启动后监控效率提高
 - 通知处理结果:弹出提示框提示用户
 - 扫描文件类型:设置扫描的文件类型
 - 普通扫描引擎:提供【启发式扫描】、【仅扫描流行病毒】和【启动压缩包扫描】三
 种扫描方式
 - 启动云扫描引擎:通过云端引擎进行扫描
 - 发现病毒处理方式: 自定义病毒处理方式
- D. 邮件监控设置
 - 开机是否默认不开启:设置开机是否默认开启邮件监控功能
 - 锁定不允许客户端关闭监控: 勾选后客户端用户无法手动关闭邮件监控
 - 通知处理结果:弹出提示框提示用户
 - 扫描文件类型:设置扫描的文件类型
 - 普通扫描引擎:提供【启发式扫描】、【仅扫描流行病毒】和【启动压缩包扫描】三
 种扫描方式
 - 启动云扫描引擎:通过云端引擎进行扫描
 - 发现病毒处理方式: 自定义病毒处理方式

部分设置项存在锁定模式,如果设为锁定,客户端用户无法在本地修改相关设置,下发 的策略与本地冲突时,管理员下发的策略优先生效;如果未设锁定,下发的策略与本地冲突 时,本地设置的策略优先生效。

点击【保存】模板创建成功;点击【取消】不保存。

6.3.1.1.3.1.3 创建客户端代理策略模板

客户端代理策略是基础性策略,是其它功能策略的基础。

依次点击【计算机管理】/【策略模板】/【添加策略模板】打开添加模板界面。

在对应产品中选择【客户代理-默认策略】并输入【策略名称】/【描述信息】/【已分 配组】等相关信息再设置策略内容。

- 客户端托盘:设置退出密码以及是否隐藏客户端托盘
- 客户端重连时间:提供5分钟、10分钟、20分钟、30分钟四种时间间隔,默认为5
 分钟间隔
- 流量控制:提供不限制、10kb/s、100kb/s、200kb/s、500kb/s五种方式,默认为
 不限制
- 客户端日志清理:对个产品日志提供多种不同方式的清理条件,管理员可根据自身 需求合理设置不同的清理条件

6.3.1.1.3.1.4 创建漏洞扫描策略模板

策略模板中策略名称、对应产品、描述信息和已分配组只要按实际填写即可,主要需设置:

- 扫描时机:开机扫描、每天某一时刻或每周某一时刻
- 扫描后处理:可勾选扫描后自动修复漏洞
- 修复漏洞级别:可勾选全部、最高级、中级以上或低级以上
- 修复产品范围:可勾选系统、微软产品和第三方产品
- 补丁下载服务器:在选定原始下载地址或指定补丁服务器后填写相关地址
- 补丁下载方式:可勾选顺序下载或并行下载
- 修复后处理:可勾选修复后删除补丁文件

6.3.1.1.3.1.5 创建软件部署组件策略模板

依次点击【计算机管理】/【策略模板】/【添加策略模板】打开添加模板界面。

在对应产品中选择【软件部署组件-默认策略】并输入【策略名称】/【描述信息】/【已 分配组】等相关信息再设置【策略内容】。

策略内容

● 部署子产品:可分别对 IT 资产管理(RAM)、防病毒(XAV)和漏洞扫描(RLS)三

个子产品的安装进行设置,提供安装、不安装和不限制三种选择。

- 升级策略:时间频率可以选择每天的任意时间点/每周的某一天/某几天的任意时间 点/手动。
- 网络连接:提供使用 IE 设置、直接连接和通过代理三种连接方式
- 代理设置:
 - 1) 输入代理服务器的 IP 地址和端口。
 - 2) 若启用验证则填写代理服务器的账号和密码。
- 升级源:获取升级文件的目的地。
 - 1) 瑞星官方网站: http://www.rising.com.cn
 - 2) 指定共享路径: 输入路径地址。
 - 3) 其它升级中心:输入其它中心地址。

点击【保存】模板为创建成功;点击【取消】为不保存。

6.3.1.1.3.2 使用已创建的模板

模板创建完成后,会以列表的形式展示在【策略模板】界面,点击相应的子产品会显示 基于此子产品创建的模板。下面以【IT资产管理】为例介绍模板的用法。

依次点击【计算机管理】/【策略模板】/【IT资产管理】会显示已创建模板。

选择子产品: IT资产管理							
IT资产管理 (RAM) 防病毒 (XAV) 客户端代理 (EP) 漏洞扫描 (RLS) 软件部署组件 (RUA)		IT资产管理子产品。			添加	口策略楨	莫板
策略模板							
名称:瑞星网络安全管理 出厂设置 描述: 产品:网络安全管理(RSM) [安全管理策略	各]						
			详情	分配	复制	删除	导出

- 点击【详情】会在打开的窗口中显示此模板在之前设置的详细信息,也可以在此对 策略模板进行修改。
- 2. 点击【分配】会弹出【分配策略】窗口。

分配策略	X
请选择策略[瑞星II资产管理 出厂设置]的分酉对象: (灰色项表示已分配过或该组开启了继承不允许从模板分配策略)	
 ▼ □	

策略只可分配到根管理组(普通组),而黑名单组和未知计算机组不接受分配。目前在 根管理组(普通组)有两个子组:测试组和开发组。其中开发组可勾选而测试组是灰色的拒 绝勾选,因为测试组开启了【继承策略】而开发组未开启【继承策略】所以有此差别。

设置完成后,点击【确定】策略就分配到相应的组织。

继承策略:当子组具有父组的情况下才有此功能,继承就是把父组的策略内容同步下来, 这样在子组也就可以使用这些策略,继承时不继承任务的应用对象,只是继承任务内容本身。

父组:即子组的上级组(例如:根管理组是父组,测试组和开发组是子组)。

复制策略	X
新策略名:	
瑞星II资产管理 出厂设置 副本	
	确定

3. 点击【复制】会弹出【复制策略】窗口。

在新策略名中输入需要名称(如果不输入名称,系统会自动为副本编号如:副本 1/副本 2;若复制的是副本,复制几次名称中会自动增加几个"副本"),点击【确定】即可。

提示:复制策略模板功能的主要作用在于,当新建策略模板较为复杂且存在相似模板 时,复制此模板后在【详情】中做简单修改即可。

- 4. 点击【删除】,将不需要的策略模板删除。
- 5. 点击【导出】,将弹出【导出策略】窗口。

正在打开 PolicyTemplate.xml
您选择了打开:
PolicyTemplate.xml
哪个是: HTML Document (901 字节)
来源: https://193.168.11.74:10443
您想要 Firefox 如何处理此文件 ?
◎ 打开方式(<u>O</u>) Internet Explorer (默认) ▼
○ 保存文件(S) ■ 桌面 浏览
以后自动采用相同的动作处理此类文件。(A)
确定 取消

6.3.1.1.4 共有策略

共有策略是子产品策略的全局配置,配置共有策略后,子产品策略模板、策略的部署才 能生效。共有策略是策略模板内容之外配置给所有客户端使用的策略,对共有策略的修改会 影响到所有客户端。

依次点击【计算机管理】/【共有策略】打开界面。

國共有策略	
辛品:瑞星客户端代理 (共有策略) 跟踪:已下发客户端 3 个,尚未下发 0 个 [详情]	
¥	羊情
□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□	
跟踪:此策略仅中心使用,无需下发至客户 端	
۴ ۲	羊情
←品:U盘登记 (共有策略)	
跟踪:此策略仅中心使用,无需下发至客户 端	
¥ ۲	并情
空制台个性化	
兑明:定制个性化控制台信息	
۴ ب	¥情

1. 点击模板名称【详情】查看分配信息

策略跟踪			x
已下发	IP	计算机名	~
~	193. 168. 11. 72	pc_YY	1
✓	193, 168, 12, 7	412F8C64464F4F7	
✓	193, 168, 11, 74	LIUYH-PC	

6.3.1.1.4.1 修改 IT 资产管理模板

依次点击【计算机管理】/【共有策略】/【IT资产管理】/【详情】打开修改界面。 在关注软件列表输入相关软件名称(每行一个软件),点击【保存】设置完成。

提示:策略名称不可修改。

6.3.1.1.4.2 修改客户端代理模板

依次点击【计算机管理】/【共有策略】/【客户端代理】/【详情】打开修改界面。

在【策略内容】/【子网网段】输入网段内容,点击【保存】设置完成。

提示:点击右侧【增加】可无限增加输入栏;点击【删除】时可以删除输入框但至少 保留一个。

6.3.1.1.4.3 修改 U 盘登记模板

依次点击【计算机管理】/【共有策略】/【U盘登记】/【详情】打开修改界面。

在【策略内容】/【关注 U 盘列表】中点击【增加】出现 U 盘描述列表。

输入 U 盘标识和描述信息,点击【保存】设置完成。

提示:此策略仅中心查询时使用,策略无需下发至客户端

6.3.1.1.4.4 修改控制台个性化模板

依次点击【计算机管理】/【共有策略】/【控制台个性化】/【详情】打开修改界面。

在【自定义标题名称】输入标题名称,在【自定义页面图标】选择要上传的图片,点击 【提交】完成设置。

6.3.1.1.5 客户端

点击【计算机管理】打开的界面中即显示管理中心已发现的所有客户端(不包括黑名单)。 客户端列表展示的是客户端名称、策略来源、IP、版本、所在组、连接业务中心、静态授权 和所属域等信息。

		"病 各户嫡首注						Q 隐藏措	捜索区
↑ 我的组织 ● ● 根管理组 ● 服务器管理 ★和计算机	搜索: 登录状态: 全部	▼ 所在组:	: 组织结	● 计 纳范围	算机名称 [◎] N	IAC◎IP◎版本]		一查道	D
黑名单	□ 名称	策略来源	IP	版本	所在组	连接业务中心	静态授权	所属域	*
	🔲 💻 xp(412F8C64464	F4F7) 继承	193.168.12.7	2.0.0.7	根管理组	193.168.11.74	否	我的组织	
	🔲 💻 LIUYH-PC	继承	193.168.11.110	2.0.0.7	根管理组	193.168.11.74	否	我的组织	
đ						世2名记录	1//17.5	50	·

RISING 瑞星。 瑞星企业终端安全管理系统软件用户手册

点击【名称】或【策略来源】时,分为已知计算机(除黑名单、未知计算之外的计算机) 和未知计算机(除已知计算机、黑名单之外的计算机)两种情况。下面将做详细介绍。

6.3.1.1.5.1 已知计算机

6.3.1.1.5.1.1 情形一

点击任意一个已知客户端的名称,打开界面。

0	组信息	组策略	组命令	子组	客户端	客户端备注	
🔒 我的组	织	412F8	3C64464F4F	7 的详细信	息		返回
 	管理组 我的小组 器管理	基本	信息				~
未知计算机 黑名单	机	产品	信息				*
	硬件	信息				~	
		软件	信息				*
6		网络	设备信息				*
		系统	信息				*
		返					

此界面显示的是此客户端的详细信息包括:基本信息、产品信息、硬件信息、软件信息、 网络设备信息以及系统信息等六方面的内容,可以分别打开,查看具体信息。

一、 组信息

点击【组信息】在打开的界面中会列出父组、组名、最大容量和描述信息等信息。

RISING 瑞星 瑞星企业终端安全管理系统软件用户手册

N T V			
组信息	组策略 组命令 子	组 客户端 客户端备注	
會 我的组织	组信息		保存 返回
 ・ ・<	父组:	-	
■ 服务器管理	组名:	根管理组	
未知计算机 黑名单		☑允许添加新客户端□开启继承	
	最大容量:	0 (0为不限制)	
		已添加客户端2台,当前在线2台	
	描述信息:		
			_
1	瓜记录于2014/06/17	9:55:43回建。	
	保存返回		

其【组名】可以修改,也可以勾选其下方的:

- 允许添加新客户端:可以添加新的组成员。
- 开启继承:开启后,当父组有新的策略时会自动继承下来。

提示:最大容量没有限制,输入数字0为不做限制。

二、组策略

点击【组策略】会显示分组已经分配有的策略。

0	组信息	组策略	组命令	子组	客户端	客户端备注					
🔒 我的组	织	当前	街:根管理4	1							
 · · ·	产品跟踪	: IT资产管理 : 已下发客户	- - [默认策略 •端 2 个 ,	3] (私有策略) 尚未下发 0 ⁻	^ [详情]						
	π								详情	转为私有	删除
		产品跟踪	: 防病毒 [默] : 已下发客户	认策略] (私 9端 2 个 ,	ム有策略) 尚未下发 0 ⁻	↑[详情]					
			الا بنديد مح						详情	转为私有	删除
		产品:客户 跟踪:已下	:客户嫡代理 :已下发客户	2 [默认策略 9端 2 个,	創 (分配副本) 尚未下发 0 ⁻	个[详情]					
					ric I ala hitemites				详情	转为私有	删除
		武時	: 漏洞扫描 [] ::已下发客户	就认录哈] 端2个,	(松有東哈) 尚未下发 0 1	个 [详情]					
			+与14、+7997/2		reales (≤1 → keter	100			详情	转为私有	删除
		广品	 : 軟件部書組 : 已下发客户 	iff [默认穿 9端 2 个,	『略] (私有策) 尚未下发 0 1	☞) 个 [详情]					
									详情	转为私有	删除
		添加	加组策略								

将鼠标放在策略上会显示出操作菜单。

详情:可以查看策略内容,也可以修改策略。

转为私有:策略来源可分为分配副本、继承副本和私有策略三种,只有策略为分配副本的时候可转为私有。转为私有以后,点击【详情】可修改策略。

删除:只有策略为【私有策略】时,【删除】按钮才有效。

添加组策略

点击界面左下角【添加组策略】可以为小组补充新的策略。

添加方法请参考本文档章节 6.1 添加策略模板

三、组命令

命令客户端立即执行的内容。包括 IT 资产管理、软件部署组件、瑞星漏洞扫描和客户 端基础平台等命令。

组信息	组策略 组命令	子组 客户端	客户端备注		
 ▲ 我的组织 ● ● 報告 ● ● 我的小组 ● 服务器管理 未知计算机 黒名単 	当前组:根管理组 IT资产管理(RAM) 扫描硬件) 扫描软件	扫描进程	重新部署第三方软件	×
i.	软杆部督组杆(RU) 立即升级	A) 立即修复 5)	立即卸载		E
	客户端基础平台(E 立即同步策略	P)	立即申请授权	远程执行	

四、子组

在本组名下的下级组织。本界面下方会出现【添加组】、【移动到】、【修改】和【删除】 等操作按钮。

组信息 组	目策略 组命令 子组	客户端 客户端备注			
⑥ 我的组织	□ 名称	描述	开启继承	允许添加客户端	*
日	□ 我的小组	工作组		\checkmark	
未知计异机 黑名单					
4					
					Ψ.
	添加组 移动到	8改 删除		共1条记录,1/1页	▲ ▶ 50 ▼

添加组:添加组的界面和组信息的界面是一致的,设置完【组名】、【最大容量】和【描述信息】之后点击【追加】即可。

移动到:将本组整体移动到其它组织,作为其下级组织存在。转移后,前若已勾选【开 启继承】原策略失效,将全盘接受上级组织的策略;若未勾选【开启继承】将保留组原策略。

移动组	x
请选择将[我的小组]移动到:	
 ▼ → 我的组织 ▼ → 根管理组 → 我的小组 	
	确定

修改:打开的是组信息界面,在这里可以修改组基本信息。

删除:将组整体删除,但并不删除客户端。

五、客户端

点击【客户端】会显示客户端所在组织的所有客户端列表。在此界面可以对客户端进行

【移动到】、【删除】、【静态授权】和【客户端命令】等操作。

勾选具体客户端后:

移动到:将选中的客户端批量移动到其它组织并接受其它组织的策略。

删除:将所选客户端删除,被删除的客户端将移动到未知计算机组中。

静态授权:由于每个子产品的授权点数是有限的,在客户端多于授权点数的情况下,会存在后上线客户端无剩余授权数可用的情况。为保证某些重要客户端可以独占授权数登录,保证策略下发有效,可以给这些客户端预先分配产品静态授权(可用授权总数相应减少)。

客户端产品静态权限设置	x
请选择要设置的产品:	
II资产管理	
III XP盾	
□ 防病毒	
□ 漏洞扫描	
	确定

客户端命令: 请参考本文档章节 6.3.1.1.5.1 已知计算机 三、组命令

6.3.1.1.5.1.2 情形二

返回根管理组界面,点击任意已知计算机【策略来源】按钮.

例如:点击【继承】打开客户端的计算机策略界面,会显示本客户端已有的策略。点击 界面左下角【添加】按钮可以为客户端添加新的策略。具体操作请参考本文档章节 6.3.1.1.3.1 添加策略模板

6.3.1.1.5.2 未知计算机

新安装本产品后,新增的客户端系统认为是未知计算机,所以会被自动显示在客户端一 一未知计算机列表中,管理员可以通过设定的扫描策略和入组策略将客户端分配至其相应组 织中。考虑默认情况下就能使用,自动入组策略里有一项配置开关"未匹配计算机加入到根 管理组",默认是开启的,即这些新加入的未知计算机会自动移动到根管理组去,如果还是 有其它需要管理的未知计算机,就需要手动分配。

点击客户端列表中任意未知计算机组的客户端计算机名,会打开此计算机详细信息界面。 此界面显示的是此客户端的详细信息包括:基本信息、产品信息、硬件信息、软件信息、网 络设备信息以及系统信息等六方面的内容,可以分别打开,查看具体信息。还可以点击界面 上方自动入组策略、扫描策略和未知计算机分别查看或设置未知计算机组信息。

一、未知计算机

点击【未知计算机】打开界面。

瑞星企业终端	端安全管理系统软	次件 - 管理控	制台(体验版)		日刷新	你好	:admin 🖞	<u> 改密码 帮助</u> ▼	退
安全中心	计算机管理	日志报告	授权管理	用户管理			切换	至审计台	0
未知计算机	自动入组策略 扫描	苗策略 客户端行	昏注						
會 我的组织	□ 名称		IP	MAC		版本	静态授权	所属域	•
			193.168.12.74	00-50-56-92	-0B-93	未安装	否	我的组织	
未知计算机			193.168.12.39	00-50-56-7A	-22-63	未安装	否	我的组织	
黑名单			193.168.12.24	28-6E-D4-88	-C6-7B	未安装	否	我的组织	
			193.168.12.221	90-B1-1C-10	-41-0B	未安装	否	我的组织	1
			193.168.12.88	D4-AE-52-C1	L-33-7B	未安装	否	我的组织	
			193.168.12.20	D4-3D-7E-D	1-EB-B2	未安装	否	我的组织	
			193.168.12.137	00-50-56-92	-0B-97	未安装	否	我的组织	
			193.168.12.222	A4-BA-DB-2I	E-D6-F9	未安装	否	我的组织	
			193.168.12.236	00-50-56-A4	-41-6C	未安装	否	我的组织	
			193.168.12.220	B8-AC-6F-9B	3-04-71	未安装	否	我的组织	
			193.168.12.205	00-1A-4D-0A	-9A-35	未安装	否	我的组织	
			193.168.12.3	44-37-E6-67	-6E-F2	未安装	否	我的组织	
			193.168.12.252	28-6E-D4-88	-B4-52	未安装	否	我的组织	
			193.168.12.132	00-50-56-B7	-1C-E3	未安装	否	我的组织	
			193.168.12.61	52-54-00-5F	-C4-C8	未安装	否	我的组织	
			193.168.12.225	00-22-19-D6	-00-C6	未安装	否	我的组织	
			193.168.12.90	00-1E-90-B3	-0B-37	未安装	否	我的组织	
			193.168.12.1	00-16-C8-A6	-33-00	未安装	否	我的组织	
	_						_		v
•	移动到删除					共75条记	录,1/2页	50	•

显示内容为未知客户端的列表。可以选择一定的客户端点击界面左下角【移动到】按钮,单个或批量的将客户端转移到其他分组。

二、自动入组策略

确定一定的 IP 规则,当有符合条件的客户端登录时,自动将其分配到预先设置的组织中。此功能根据【扫描策略】的扫描结果匹配 IP,分配客户端。有两种 IP 规则即 IP 匹配规则和网上邻居扫描匹配规则。

IP 匹配规则

IP 匹配规则是设置一定 IP 范围,再选择【等于】、【不等于】、【包含于】和【不包含于】 选项,当有 IP 符合规则时自动将其分配到预先设置的组中。

引入INC 计学会瑞星企业终端安全管理系统软件用户手册

瑞星企业终端	耑安全管理系统 转	次件 - 管理控制	制台(体验版)		С 刷新	你好:admin <u>修改密码 帮助</u> ▼ 退出
安全中心	计算机管理	日志报告	授权管理	用户管理		切换至审计台 ●
未知计算机	自动入组策略 扫扰	苗策略 客户端备	注			
我的组织 现 我管理组 最好器管理 未知计算机	IP匹配规则 添加到普通组 ▼	▼ 不等于 我的组织\根管理组	▼ ^{193.168.12.7}			
黑名单						删除上移下移
4						
	添加保存	导入 导出				

网上邻居扫描匹配规则

网上邻居扫描匹配规则:预设一个 IP,当有 IP 符合规则时,此功能根据【扫描策略】 的扫描结果匹配 IP,分配客户端。

三、扫描策略

扫描策略,可以配置服务器扫描客户端的 IP 段,使业务中心服务器主动发现网络内客户端。

点击【扫描策略】打开界面。

点击界面左下角【添加】按钮, 创建 IP 地址输入栏(可无限添加, 方便分段精细扫描), 输入 IP 地址范围, 点击【保存】设置成功。

C 刷新 你好:admin | <u>修改密码</u> | <u>帮助</u> ▼ | 退出 **瑞星企业终端安全管理系统软件 - 管理控制台**(体验版) 切换至审计台 ● 安全中心 计算机管理 日志报告 授权管理 用户管理 未知计算机 自动入组策略 扫描策略 客户端备注 🏫 我的组织 IP包含于: 193.168.12.0 _ 193.168.12.255 📃 根管理组 🔓 服务器管理 删除上移下移 未知计算机 黑名单 添加 保存 导入导出

6.3.1.1.6 客户端备注

客户端备注功能可以使管理员更加直观快捷的对客户端进行管理。页面信息包括: IP 地址、机器名、MAC地址和备注。在【备注】栏中修改备注名称后,点击【保存】即可。

域信息	子域信息 策略模板	共有策略 客户端 客	户端备注		
は信息 ● 我的组织 ● 我的组织 ● 我的理想 ● 服务器管理 未知计算机 黒名单	子域信息 策略模板	共有策略 客户端 客 412F8C64464F4F7 1 LIUVH-PC ・ PC_YY・	中端备注 MAC地址 44-87-FC-A4-9C-52 00-24-E8-23-9A-A2 44-37-E6-12-C4-60	备注 xp LIUYH-PC	

客户端备注支持批量修改,也可以将现有备注资料导出备份。

김১///С 這這是端星企业终端安全管理系统软件用户手册

导入: 上传 XML 格式文件, 当其满足 IP 地址相同、计算机名称相同和 MAC 地址相同中 任意一个条件时, 备注即可成功导入。

导出:导出已有备注资料进行备份。

6.3.1.2 根管理组(普通组)

详情请参考本文档章节 6.3.1.1.5.1 已知计算机

6.3.1.3 服务器管理

各中心所使用的服务器,包括瑞星管理中心(即管理平台自身服务器)、漏洞补丁中心、 升级中心和业务中心。服务器按照系统可划分为系统服务器、外围服务器。系统服务器是安 装有瑞星软件中心系统的服务器,外围服务器是没有安装瑞星软件起辅助管理作用的服务器。

6.3.1.3.1 系统服务器

系统服务器目前包括【瑞星管理中心】、【漏洞补丁中心】、【升级中心】和【业务中心】, 以后可能会增加其它扩展中心,但操作基本一致。

点击【系统服务器】右侧的倒三角,可以选择不同中心的服务器。

事	<u> </u>	端安全管理系统	🕑 刷新	你好:adm	in <u>修改密码</u>	<u>帮助</u> ▼ 退			
	安全中心	日志报告	计算机管理	授权管理	用户管理		t	切换至审论	†台 0
	系统服务器 👻	外围服务器 数 瑞星管理中心	対据连接设置 日志	数据清理					
▲ 我的组织 ● 報告報	思想	漏洞补丁中心 漏洞补了 升级中心	「中心(RDC)]						
一 日 振务器 未知计算机	管理	业务中心PC	193.168	8.11.74	版本:2.0.0.7	✔ 已绑定授权	✔ 已获取授权	<u>况四条数</u>	谷谷
黑名单								汉旦罗奴	549AE121X

6.3.1.3.1.1 瑞星管理中心(MANAGER)

依次点击【服务器管理】/【系统服务器】 🚩/【瑞星管理中心】打开界面。

YAERSA YERSA YERBAS YERBAS YERBAS Edata Edata

设置参数

点击【设置参数】可以修改管理中心配置参数。在弹出的界面中,用户可以重新设置服 务器的【名称】,【服务器 IP】、【类型】、【配置信息】等均为默认设置,不可修改。

编辑服务器		保存 返回
服务器IP:	192.168.20.95	
名称:	DFFGH-A666A5D1C	
美型:	管理中心 🔻	
	管理表同步定时器:900 秒	
副 男/c自 .	客户表同步定时器: 600 秒	
	日志同步定时器:500秒	
	日志版本检查时间:500 秒	

6.3.1.3.1.2 漏洞补丁中心(RDC)

김১///С 這是瑞星企业终端安全管理系统软件用户手册

依次点击【服务器管理】/【系统服务器】▼/【漏洞补丁中心】打开界面。

		_							
-	系统服务器 🔻	外围服务器	数据连接设置	日志数据清理					
會 我的组	织	服务器列表 [漏洞]补丁中心(RDC)]						
■ 根管 ■ 服务	理组 器管理	LIUYH-PC	1	93.168.11.74	版本:2.0.0.7	✔ 已绑定授权	✔ 已获取授权		
未知计算机 黑名单							设置参数	绑定授权	
4									
		共2个授权,已绑	定1个				共1条记录 , 1/1]	5	50 🕶

主要有【设置参数】、【绑定授权】两个内容。

AISING 瑞星瑞星企业终端安全管理系统软件用户手册

1. 设置参数

点击【设置参数】可以修改补丁下载中心配置参数。在弹出的界面中用户可以重新设置 服务器【名称】和升级源,而【服务器 IP】、【类型】为默认设置,不可修改。

	系统服务器 👻 外围服务器 数据连接设置 日志数据清理	
编辑服务器		保存 返回
服务器IP:	193.168.11.74	
名称:	LIUYH-PC	
类型:	漏洞补丁中心 🔻	
	升级源	
配置信息:	+ 增加-移除	
	原始下载地址 ▼	

保存返回

- 服务器 IP: 显示当前补丁下载中心服务器的 IP 地址。
- **名称:**设置服务器名称。
- **类型:**显示当前服务器类型(即补丁下载中心)。
- **配置信息:**分为原始下载地址和指定补丁服务器。

完成后点击【保存】即可。

2. 绑定授权

点击【绑定授权】打开【服务器授权绑定】。



绑定授权功能,使管理员有针对性的将授权许可绑定至经过管理员认可的服务器,以防 止网络内由于部署等问题意外出现未知服务器抢占授权点数。这样,管理员便可确定本台服 务器产品授权的正常性和有效性。

提示:在服务器安装的数目在授权数目内时,服务器会自动绑定授权,即正常使用时 (没有安装超过正常授权总数服务器个数),默认可以省去这个步骤。

6.3.1.3.1.3 升级中心(RUC)

依次点击【服务器管理】/【系统服务器】 / 【升级中心】打开界面。

服务器列表 [升级中心(RUC)]				
	193.168.11.74 版本	\$: 2.0.0.7	✔ 已绑定授权 ✔ 已获取	授权
病毒库 版本:25.21.01.02 更新:2014-07-01 13:05	聚意网址库 版本:24.00.25.10 更新:2014-07-01 12:05	漏洞库 版本:1.0.0 更新:201-	0.6 4-06-17 10:53	
子产品	当前版本	发布时间	更新时间	
管理中心(MANAGER)	1.0.3.55	2014-07-17 09:37	2014-07-17 16:34	
核心组件(COMMON)	1.0.2.46	2014-07-15 10:08	2014-07-17 16:34	
反病毒引擎(RSV)	1.0.0.4	2013-03-04 13:36	2014-07-17 16:34	
设备管理基础(RDF)	1.0.0.19	2014-05-22 14:58	2014-07- <mark>1</mark> 7 16:34	
监控组件(CLIENTCOMM)	1.0.1.6	2014-06-13 16:25	2014-07-17 16:34	
升级中心(RUC)	1.0.2.1	2014-07-04 09:47	2014-07-17 16:34	
软件部署组件(RUA)	1.0.3.17	2014-07-17 09:37	2014-07-17 16:34	
业务中心(BUS)	1.0.0.44	2014-07-15 10:08	2014-07-17 16:34	
XP盾(RXP)	1.0.0.10	2014-07-11 10:38	2014-07-17 16:34	
IT资产管理(RAM)	1.0.0.92	2014-02-26 16:52	2014-07-17 16:34	
防病毒(XAV)	1.0.2.67	2014-07-12 10:48	2014-07-17 16:34	
客户端代理(EP)	1.0.2.82	2014-07-11 10:38	2014-07-17 16:34	
恶意网址库(FWLIB)	1.0.0.3	2014-02-26 16:52	2014-07-17 16:34	
安全助手(RSA)	1.0.0.4	2014-04-16 10:15	2014-07- <mark>1</mark> 7 16:34	
漏洞补丁中心(RDC)	1.0.0.67	2014-06-11 16:40	2014-07-17 16:34	

主要有【设置参数】、【绑定授权】、【制作安装包】、【上传升级包】、【立即升级】和【上传第三方软件包】。

1. 设置参数

服务器 IP:显示当前软件升级部署中心服务器的 IP 地址。

名称:设置服务器名称。

类型:显示当前服务器类型(即软件升级部署中心)。

配置信息:分为升级策略、网络连接、代理设置、升级源、数据连接配置和网络配置六部分。

- 升级策略:频率可设置为每天的任意时间点/每周某一天或几天的任意时间点/
 手动/间隔。
- 网络连接:设置使用 IE 设置,直接连接或通过代理。
- 代理设置:输入代理服务器的 IP 和端口。若勾选启用验证,则输入代理服务器的登录账号和密码。
- 升级源:升级源可以选择瑞星官方网站、指定共享路径或其它升级中心,但都 需要输入准确的升级路径地址。升级源可以点击右侧【增加】/【删除】项任意 添加或删除,删除时至少保留一个升级源。
- 数据连接配置:设置连接池最小,最大连接数。
- 网络配置:设置 TCP 服务端口号、搜索范围,负载均衡最大连接数。
 完成后点击【保存】即可。

2. 绑定授权

点击【绑定授权】打开【服务器授权绑定】。

服务器授权绑定	X
☑ 为服务器 [LIUYH-PC] 绑定产品静态授权	
	确定

绑定授权功能,使管理员有针对性的将授权许可绑定至经过管理员认可的服务器,以防 止网络内由于部署等问题意外出现未知服务器抢占授权点数。这样,管理员便可确定本台服 务器产品授权的正常性和有效性。

提示: 在服务器安装的数目在授权数目内时,服务器会自动绑定授权,即正常使用时 (没有安装超过正常授权总数服务器个数),默认可以省去这个步骤。

3. 制作安装包

客户端软件由多个子产品构成,不同子产品以及客户端会有所更新。根据部署的需要, 可以有选择性的将组合子产品制作成为安装包,并发布至升级中心服务器。客户机便可通过 升级中心服务器下载最新版本的客户端安装包安装,方便计算机管理员的部署工作。

4. 上传升级包

上传升级包,提供了手动上传服务器升级包的途径。可通过瑞星技术支持获得更新的完整升级程序,并上传至 RUC 服务器。以便后续 RUC 服务器以及业务中心、客户端升级使用。 下载最新的升级程序,并上传至升级中心服务器即可完成上传。

5. 立即升级

点击立即升级,升级中心服务器将按照升级源设置对自身进行升级部署。

6. 上传第三方软件包

上传第三方软件包功能是为了方便管理员统一分发部署相关文件;部署软件的相关名称、 软件包路径、规则检查、命令均可统一成一套模板上传至 RUC 平台上,管理员在分发时只需 选择相应的软件即可完成分发操作。

6.3.1.3.1.4 业务中心(BUS)

依次点击【服务器管理】/【系统服务器】 ▼/【业务中心】打开系统服务器列表界面。

-	系统服务器 ▼	外围服务器	数据连接设置	日志数据清理					
會 我的组	1织								_
■ 根管	理组	服务器列表 [业务	中心(BUS)]						
🛃 服务 未知计算	器管理 1机	LIUYH-PC		193.168.11.74	版本:2.0.0.7	✔ 已绑定授权	✔ 已获取授权		
黑名单								设置参数	绑定授权
u .									
		雨新土亨配罢	±2个括权 =	9			共1条记录 , 1/1]	页 ◀ ▶	50 🕶
			774 H 191X / L	JORAET I					

主要有【设置参数】、【绑定授权】两个内容。

1. 设置参数

点击	【设置参数】打开设置参数界面。	
	系统服务器 マ 外围服务器 数据连接设置 日志数据清理	
编辑服务器		保存 返回
服务器IP:	193.168.11.74	
名称:	LIUYH-PC	
类型:		
配置信息:	数据连接配置 连接池最小连接数: 6 连接池最大连接数: 10 网络配置 TCP服务端口号: 5555 TCP端口搜索范围: 5555 至 5555 至 5555 至 5555 至 5555 至 5555 1000 	

保存返回

服务器 IP:显示当前业务中心服务器的 IP 地址。

名称: 输入服务器名称。

类型:显示当前服务器类型(即瑞星业务中心)。

配置信息:分为数据连接配置和网络配置两方面。

数据连接配置:输入连接池最小连接数和连接池最大连接数。连接池数高,响应的速度 越快,但由于数据库连接池数有限,请合理分配资源。如不确定如何设置,可保留默认值。

网络配置:输入 TCP 服务端口号、TCP 端口搜索范围以及负载均衡最大数。负载均衡最 大数是指服务器所能承受的最大客户端连接数。在【更新共享配置】选项页中,如果勾选【负 载均衡】功能,业务中心会自动根据各业务中心服务器的负载均衡最大连接数,按负载均衡 最大连接数比例自动分配连接,达到调节服务器负载,合理利用服务器资源的目的。

2. 绑定授权

点击【绑定授权】打开【服务器授权绑定】。

服务器授权绑定	x
☑ 为服务器 [LIUYH-PC] 绑定产品静态授权	
	确定

6.3.1.3.2 外围服务器

外围服务器可配置邮件服务器设置。

管理平台中的日志报告等功能,需要使用业务管理平台发送相应报告邮件。因此,在邮件服务器设置页,可设置管理平台发送邮件所需的 SMTP 服务器参数。参数生效后,服务器才可发送日志报告邮件。

依次点击【服务器管理】/【外围服务器】打开设置界面。

系统服务器	▼ 外围服务器 数据连接设置 日志数据清理
會 我的组织	
🖳 根管理组	SMTP服务器设置
服务器管理 未知计算机	服务器信息
黑名单	IP/域名:
	发件人:
	身份认证
	用户名: admin
	密 码: •••••••••• (若不修改请留空)
4	保存

在服务器信息中输入 IP/域名或端口、发件人;若需要身份认证则输入用户名和密码。 点击【保存】设置成功。

6.3.1.3.3 数据连接设置

设置就是登陆数据库的信息。

依次点击【服务器管理】/【数据连接设置】打开界面。

🔒 我的组织	数据连接设置	
🖳 根管理组		
🖥 服务器管理	业务数据库服务器	
未知计算机	数据库实例: 193.168.11.74\RSESM,7 库名: esmdb	
黑名单	数据库用户: sa 密码: 123456	
	日志数据库服务器	
	数据库实例: 193.168.11.74\RSESM,7 库名: esmlogdb	
	数据库用户: sa 密码: 123456	
	数据库用户: sa 密码: 123456	

在此界面可分别对业务数据库服务器和日志数据库服务器的数据库实例、库名、数据库 用户以及用户密码进行设置。

提示:数据库参数为 SQL Server 数据库参数,修改后必须重新登录。

6.3.1.3.4 日志数据清理

日志清理设置是定期清理日志条数,避免旧日志占用太大的空间,导致系统运行缓慢或 其他异常。

依次点击【服务器管理】/【日志数据清理】打开界面。

北京瑞星信息技术有限公司

김) INC 瑞星瑞星企业终端安全管理系统软件用户手册

系统服务器	外围服务器 数据连接证	设置 日志巻	如据清理			
1 我的组织	日志清理设置					•
■ 根管理组 ■ 服务器管理	共享访问日志	保留 60	天 🔻	◎并且◎或者	超过条记录	
未知计算机	软件流量监控日志	保留 60	天 🔻	◎并且◉或者	超过 条记录	
黑名单	存储控制日志	保留 60	天 🔻	◎并且◎或者	超过 条记录	
	终端流量监控日志	保留 60	天 🔻	◎并且◎或者	超过 条记录	
	信息审计日志	保留 60	天 🔻	◎并且◎或者	超过 条记录	
	信息审计统计	保留 60	天 🔻	◎并且◎或者	超过 条记录	
	ARP事件日志	保留 60	天 🔻	◎并且◎或者	超过 条记录	
4	开机时间日志	保留 60	天 🔻	◎并且◎或者	超过 条记录	
·	计算机操作日志	保留 60	天 🔻	◎并且◎或者	超过 条记录	
	IP防篡改日志	保留 60	天 👻	◎并且◉或者	超过 条记录	
	网络隔离日志	保留 60	天 🔻	◎并且◎或者	超过 条记录	
	恶意网址查杀日志	保留 60	天 🔻	◎并且◎或者	超过 条记录	
	客户端升级日志	保留 60	र र	◎并且◎或者	超过 条记录	
	升级中心升级日志	保留 60	天 👻	◎并且◉或者	超过 条记录	E
	病毒查杀事件	保留 60	天 🔻	◎并且◉或者	超过 条记录	
	病毒查杀记录	保留 60	天 🔻	◎并且◎或者	超过 条记录	
	病毒跟踪	保留 60	र र	◎并且◎或者		
< <u> </u>	保存 返回					•

在此可以设置以下日志的保留期限,单位可选天/月。

- 业务中心日志
- 客户端事件日志
- 终端日志
- 控制台操作日志
- 硬件异动日志
- 设备异动日志
- 进程启动日志
- 软件禁用日志
- 软件保护日志
- 网页浏览日志
- 客户端外联日志
- 文件审计日志
- 文件打印日志
- 聊天审计日志
- 网络 IP 访问日志
- 邮件审计日志
- 联网程序审计日志

- 网络数据包审计日志
- 出站攻击日志
- 代理审计日志
- 共享访问日志
- 软件流量监控日志
- 存储控制日志
- 终端流量监控日志
- ARP 事件日志
- 开机时间日志
- 计算机操作日志
- IP 防篡改日志
- 网络隔离日志
- 客户端升级日志
- 升级中心升级日志
- 病毒查杀事件
- 病毒查杀记录
- 病毒跟踪
- 6.3.1.4 未知计算机

详情请参考本文档章节 6.3.1.1.5.2 未知计算机

6.3.1.5 黑名单

在已知/未知计算机中不希望对其进行管理的计算机。

点击【黑名单】打开界面,显示的是黑名单列表。界面下方包括【移动到】和【删除】 两个按钮。

黑名单 计算机备注 Q隐藏搜索区 **會**我的组织 搜索: ●计算机名称◎MAC◎IP◎版本 🖳 根管理组 查询 🔓 服务器管理 全部 ▼ 黑名单 * 登录状态: 所在组: 未知计算机 黑名单 🗌 名称 IP 版本 MAC地址 黑名单源 静态授权 所属域 🔲 💻 PC_YY 193.168.11.72 44-37-E6-12-C4-60 2.0.0.9 手工入组 否 我的组织 共1条记录,1/1页 50 ▼ 移动到删除

김〉ING 瑞星瑞星企业终端安全管理系统软件用户手册

6.4 授权管理

授权管理主要是管理瑞星企业终端安全管理产品各个子产品的使用授权,检查使用期限、 授权数量以及更新子产品。主要包括产品信息和授权信息两方面内容。

6.4.1 产品信息

点击【授权管理】打开的就是产品信息界面,【子产品】列表会列出所有安装的子产品 并显示各个子产品的【代号】、【授权】、【总授权点数】等信息。点击任一子产品在【子产品】 列表下方会显示此子产品的【授权许可号】、【有效期限】、【授权点数】和【状态】等信息。
			产品信息	授权信息	L		
子产品	f	号	授权		总授权点数		~
Ⅲ资产管理	R	AM	至 2014-01-21		300		
XP盾	R	XP	未安装		0		
防病毒	х	AV	至 2014-01-21		300		
漏洞补丁中心	R	DC	至 2014-01-21		2		
漏洞扫描	R	LS	至 2014-01-21		300		
升级中心	R	UC	至 2014-01-21		2		
网络安全管理	R	SM	至 2014-01-21		300		
信息内容审计	R	MI	至 2014-01-21		300		
授权许可号	有效期限				授权点数	状态	~
JY83P-JTNB7-XM4XA-6DF63-D88VN	2013-01-21	至 2014-01-21			200	有效	
PUXL3-QX7AR-358B7-HLNJQ	2013-01-21	至 2014-01-21			100	有效	
							\sim

导入授权

6.4.2 授权信息

依次点击【授权管理】/【授权信息】打开界面。

产品信息 授权信息					
授权许可号	产品	有效期限	授权点数	状态	
JY83P-JTNB7-XM4XA-6DF63-D88VN	行为审计	2013-01-21 至 2014-01-21	200	有效	
JY83P-JTNB7-XM4XA-6DF63-D88VN	IT资产管理	2013-01-21 至 2014-01-21	200	有效	
JY83P-JTNB7-XM4XA-6DF63-D88VN	防病毒	2013-01-21 至 2014-01-21	200	有效	
JY83P-JTNB7-XM4XA-6DF63-D88VN	漏洞扫描	2013-01-21 至 2014-01-21	200	有效	
JY83P-JTNB7-XM4XA-6DF63-D88VN	信息内容审计	2013-01-21 至 2014-01-21	200	有效	
JY83P-JTNB7-XM4XA-6DF63-D88VN	升级中心	2013-01-21 至 2014-01-21	1	有效	
JY83P-JTNB7-XM4XA-6DF63-D88VN	漏洞补丁中心	2013-01-21 至 2014-01-21	1	有效	
JY83P-JTNB7-XM4XA-6DF63-D88VN	业务中心	2013-01-21 至 2014-01-21	1	有效	
JY83P-JTNB7-XM4XA-6DF63-D88VN	网络安全管理	2013-01-21 至 2014-01-21	200	有效	Ш
PUXL3-QX7AR-358B7-HLNJQ	行为审计	2013-01-21 至 2014-01-21	100	有效	
PUXL3-QX7AR-358B7-HLNJQ	网络安全管理	2013-01-21 至 2014-01-21	100	有效	
PUXL3-QX7AR-358B7-HLNJQ	IT资产管理	2013-01-21 至 2014-01-21	100	有效	
PUXL3-QX7AR-358B7-HLNJQ	防病毒	2013-01-21 至 2014-01-21	100	有效	
PUXL3-QX7AR-358B7-HLNJQ	漏洞扫描	2013-01-21 至 2014-01-21	100	有效	
PUXL3-QX7AR-358B7-HLNJQ	信息内容审计	2013-01-21 至 2014-01-21	100	有效	
PUXL3-QX7AR-358B7-HLNJQ	升级中心	2013-01-21 至 2014-01-21	1	有效	
PUXL3-QX7AR-358B7-HLNJQ	漏洞补丁中心	2013-01-21 至 2014-01-21	1	有效	
PUXL3-QX7AR-358B7-HLNJQ	业务中心	2013-01-21 至 2014-01-21	1	有效	-

导入授权 共 18 个正在使用的授权许可

此界面显示的是各个子产品的授权基本号、有效期限、授权数量和状态等信息。

提示:导入授权和产品信息中的操作一致。

6.4.3 导入授权

导入授权主要用于激活产品、增加授权计数或延长授权使用期限,是合法使用本软件的 标志。从瑞星得到的授权包括基本号和证书文件两部分。

点击【导入授权】打开【导入授权】界面。

导入授权		Х
基本号:		
证书文件:	浏览… 未选择文件。	
		确定

输入【基本号】导入【证书文件】,点击【确定】即可。

6.5 用户管理

在用户管理界面主要是用户列表的内容,为了方便对管理对象的权限设定。

【用户管理】主要包括【创建用户】、【修改】、【修改密码】和【详情】等子功能。

用户列表						
	用户名:admin(我的组织) 上次登录:2013-06-26 09:46:31 备 注:维护系统的正常运行	登录IP : 193.168.11.74		多改	修改密码	详情
创建用户			共1条记录,1/1	页(50 🔻

用户列表展示的是所有己建用户信息,包括用户名、类型、上次登录时间、登录 IP 和 备注等。其中 admin(具有超级管理员权限)为内置用户,其他用户只可查看详情不可进行 修改、删除和修改密码等操作。此用户可以建立与之拥有相同权限的用户,数量不限。

6.5.1 创建用户

创建用户分为基本设置和权限设置。

6.5.1.1 基本设置

基本设置主要是设置用户的基本信息,包括登录名、全名、电子邮件、验证方式和登录 控制。

基本设置 权限设置	返回保存
基本信息	
登录名	
admin	
全名	
维护系统的正常运行	
电子邮件	
24774-8	
按此方式	
● 密码永不过期	
○ 密码将在以下天数后过期: 7 天	
登录控制	
管理员登录尝试失败次数达到 3 次后,系统会锁定帐户 5 分钟	
☑ 帐户锁定时向管理员发送邮件	

提示:用户名不可重复;密码可为数字、英文字母或其组合且不限字符数:密码不可 为空且英文字母区分大小写。

6.5.1.2 权限设置

要创建用户有四种可选权限:超级管理员、管理员、审计员和自定义。

基本设置	权限设置						返回	保存	
权限定义 ●超级管	建员 〇管理	長 〇审计员							

- 超级管理员:具有超级管理员权限的用户拥有管理员的所有权限。创建此用户
 不需要手工分配权限,其自动拥有管理员的所有权限。
- 管理员:具有管理员权限的用户可以登录本软件的管理控制台和审计控制台。
 创建此用户可以按照权限需要自定义权限。
- 审计员:具有审计员权限的用户可以登录本软件的管理控制台和审计控制台, 仅拥有查看审计控制台的各个客户端操作日志的权限。创建此用户不需要手工 分配权限,其自动拥有审计控制台的查看权限。
- **自定义权限**: 创建此用户可以按照权限需要自定义权限。

6.5.1.2.1 管理员权限

管理员权限用于设置管理员对各个组织的写权利,包括删除、修改。

基本设置权限设置			返回	保存
基本设置 权限设置 V限定义 ●管理员 ●超级管理员 ●管理员 ●超级管理员 ●管理員 ● ●管理員 ● ●	3 〇南计员 〇百定义 『写 『写 『写 『写 『写 『写 『写 『写 『写 『写		送回	保存

6.5.1.2.2 自定义权限

自定义权限用于设置用户对各个组织与功能的写权利,包括删除、修改。

基本	设置权限设置					返回	保仔
权限	定义						
(◎超级管理员 ◎管理员	◎ 审计员 ◎ 自定	义				
	▼ ■ 型 我的组织 ■ ■ 根管理组		平台	软件部署			
	□ 🗐 未知计算机		日志 □读	日志 □ 读			
			报告 □读 □写	报告 □读 □写			
			策略 □读 □写	策略 □读 □写			
	□ 📄 账户管理		客户端代理	漏洞管理	E		
			日志 🗌 读	日志 🗌 读			
			报告 □读 □写	报告 □读 □写			
			策略 □读 □写	策略 □读 □写			
			IT资产管理	防病毒			
			日志 □读	日志 □读			
			报告 □读 □写	报告 □读 □写			
			策略 □读 □写	策略 □读 □写			
			XP盾		-		

6.5.2 修改

修改和创建用户的操作一致,请参考 6.5.1 创建用户。

6.5.3 修改密码

修改用户的登录密码,需要输入当前密码和确认密码,点击【确定】即可。

提示:数字、英文字母均可且不限字符数,但是不可为空且英文字母区分大小写。

修改用户admin	竹密码	х
旧密码:		
新密码:		
确认密码:		确定

6.5.4 详情

详情和新建用户的信息一致,请参考 6.5.1 创建用户。

7. 审计控制台

瑞星企业终端安全管理系统软件——审计控制台是将管理控制台的部分审计功能重新 优化组合,使 WEB 页面更加的简洁明了,有利于审计员快速了解整个网络内的计算机的安全 状况,为科学管理提供决策依据。

审计控制台的页面布局由五大子产品组成:【平台】、【防病毒】、【漏洞扫描】、【资产管理】和【XP 盾】。

审计控制台 WEB 页面主要由切换按钮、菜单栏、辅助功能和列表区四部分内容组成。

计 瑞星企业终端安全管理	豚统软件<u>-</u>百	审计控制台 (体验版)	こ 刷新	你好 , admin <u>修改密码 帮助</u> ▼ <u>退出</u>
平台防病毒	漏洞扫描 资	资产管理 XP盾	➡> 菜单栏	₩ 切换至管控台 •
客户端 > 未知终端 管理范围				↓ 切换按钮
本组发现 90 台未知终端 发现时间: 网络 本周 上周 本月	1 月 指定	₩ 2014-06-25 📖 爭	2014-06-25	
搜索:		 ○ 计算机名称 ○ Ⅰ 	P地址 〇 MAC地址	
未知终端列表				
计算机名称	•	IP地址	MAC地址	上报时间
<u>192.168.90.1</u>		192.168.90.1	00-24-F9-AA-79-48	2014/06/25 15:33:26
<u>192.168.90.101</u>		192.168.90.101	00-20-19-D3-C8-4B	2014/06/25 15:33:27
<u>192.168.90.131</u>		192.168.90.131	列表区 00.82 8-E6-E2-83	2014/06/25 15:33:28
<u>192.168.90.14</u>		192.168.90.14	37-E6-2C-8C-79	2014/06/25 15:33:26
J92.168.90.140		192.168.90.140	1C-FA-68-EA-14-8F	2014/06/25 15:33:28
<u>192.168.90.142</u>		192.168.90.142	44-37-E6-2A-6F-2F	2014/06/25 15:33:28
192.168.90.15		192.168.90.15	14-CF-92-68-ED-F9	2014/06/25 15:33:26

菜单栏: 各功能分区的目录, 包括:【平台】、【防病毒】、【漏洞扫描】、【资产管理】和

【XP 盾】。

切换按钮:点击此按钮可以在管理控制台和审计控制台之间切换。

辅助功能:点击【修改密码】可以修改当前用户的登录密码;在【帮助】栏中可以查看 软件在线帮助、登录论坛和瑞星企业安全管理平台自助服务系统。

列表区:展示各审计的功能的详细信息。

7.1 平台

平台分为客户端和未知终端。

7.1.1 客户端

客户端列表展示客户端信息,包括计算机名称、IP 地址、MAC 地址、版本、上次登录时间及所属组。

客户端安全状态支持在线状态的条件查询方式,条件包括不限、已登录和未登陆。

还可以对查询结果进行关键字搜索,关键字包括计算机名称、IP 地址、MAC 地址和版

本。

→ 客户端 未知终端 新理范围						
① 查看客户端信息						
在线状态: <mark>不限</mark> 已登录 未登录						
搜索:	Q,	◉ 计算机名称 ○	IP地址 〇 MA	AC 🔘 版本		
计算机名称	IP地址	MAC地址	版本	上次登录	所属组	
<u>m xp 412F8C64464F4F7</u>	193.168.12.7	44-87-FC-A4-9C-52	2.0.0.7	2013/06/26 10:02:53	根管理组	
LIUYH-PC	193.168.11.74	00-24-E8-23-9A-A2	2.0.0.7	2013/06/26 10:04:20	根管理组	
每页显示 10 🔻 条 📑 🗐				共 2 条记录	艮 1/1 < > 跳转到:1	go

7.1.2 未知终端

未知终端列表展示未知终端信息,包括计算机名称、IP 地址、MAC 地址及上报时间。

未知终端安全状态支持发现时间的条件查询方式,条件包括不限、上周、本月、上月和 指定时间范围。

还可以对查询结果进行关键字搜索,关键字包括计算机名称、IP 地址、MAC 地址和版

本。

范围			
本组发现 133 台未知终端			
发现时间: <mark>不限</mark> 本周 上周 本月	上月 指定 从 2013-06-26 🛗 到	2013-06-26	
搜索:	💶 🔍 💿 计算机名称 🔘 🛛	Р地址 🔘 МАС地址	
知终端列表			
计算机名称	▲ IP地址	MAC地址	上报时间
<u>192.168.26.1</u>	192.168.26.1	5C-63-BF-D5-CC-A8	2014/06/17 10:18:10
<u>192.168.26.1</u>	192.168.26.1	00-0D-A3-26-52-02	2013/06/24 18:05:18
<u>192.168.26.101</u>	192.168.26.101	D0-22-BE-8B-4B-71	2013/06/24 15:24:17
192.168.26.102	192.168.26.102	C4-6A-B7-9B-66-CE	2013/06/24 17:04:16
<u>193.168.11.101</u>	193.168.11.101	84-38-38-43-53-96	2013/06/26 12:04:26
193.168.11.102	193.168.11.102	5C-F8-A1-03-D8-DE	2013/06/26 14:14:27
<u>193.168.11.103</u>	193.168.11.103	64-A7-69-81-3D-E4	2013/06/26 12:54:24
<u>193.168.11.108</u>	193.168.11.108	D0-22-BE-9C-55-F8	2013/06/26 14:24:27
102 169 11 120	193.168.11.130	00-17-61-01-37-14	2013/06/26 15:24:28
133.100.11.130			

7.2 防病毒

防病毒分为全网查杀、病毒分析、病毒详情、系统加固和应用加固。

	🗸 瑞星企业终端	端安全管理	里系统软件 - 审计	控制台(体验	版)		С 刷新	你好,admin <u>f</u> f	3改密码 <u>帮助</u> ▼ 退出		
	平台	防病毒	漏洞扫描 资产	管理 XP	盾			t	刃换至管控台 ●		
管理范围	 ▶ 全网查杀 	病毒分析	病毒详情 系统	加固 应用;	加固						
3 发	现 0 台客户端未开启文(件监控, 0 台湾	客户端未开启邮件监控。 1	台客户端长时间:	未进行全盘扫描						
文件监	控状态: <mark>不限</mark> 已开原	自 关闭									
邮件监	邮件监控状态: <mark>不限</mark> 已开启 关闭										
未执	未执行扫描: 不限 超过1周 超过1个月 从未扫描 扫描中										
在	线状态: <mark>不限</mark> 已登录	表 未登录									
	搜索:		Q ④ 计算机	l名称 🔘 IP地	地						
客户端	安全状态				◆ 快速	查杀▼	Q全盘查杀▼	▶ 文件监控 •	■邮件监控▼		
	计算机名	称 🔺	IP	文件监控	邮件监控	最	后扫描时间	病毒库版本	发现病毒		
	CUIC-PC		192.168.90.151	Ť	-	201	4/06/25 12:05	25.20.02.02	1		

7.2.1 全网查杀

全网查杀页面展示客户端安全状态信息,包括计算机名称、IP 地址、文件监控、邮件监

控、最后扫描时间、病毒库版本及发现病毒次数。

提示:最后扫描时间显示最近一次全盘扫描或者快速扫描的时间。

客户端安全状态支持以下多种条件查询方式及其组合:

- 文件监控状态查询,条件包括不限、已开启和关闭。
- 邮件监控状态查询,条件包括不限、已开启和关闭。
- 未执行扫描时间查询,条件包括不限、超过1周、超过1个月、从未扫描和扫描中。
- 在线状态查询,条件包括不限、已登录和未登录。

还可以对查询结果进行关键字搜索,关键字包括计算机名称和 IP 地址。

+ 全网查杀 病毒分析 管理范围	病毒详情 系统加	加固 应用)	口固							
\rm 🚯 发现 0 台客户端未开启文件监控, 0 台客	了户端未开启邮件监控。 1	台客户端长时间;	未进行全盘扫描							
文件监控状态: 死限 已开启 关闭 邮件监控状态: 死限 已开启 关闭 未执行扫描: 死限 超过1/月 从未扫描 扫描中 在线状态: 死限 已登录 未登录 搜索: ③ 计算机名称 ○ IP地址										
客户端安全状态			▶ 快速	査杀▼ Q 全盘査杀▼	▶ 文件监控 •	■邮件监控▼				
□ 计算机名称 ▲	IP	文件监控	邮件监控	最后扫描时间	病毒库版本	发现病毒				
xp 412F8C64464F4F7	193.168.12.7	Ŷ	-	2013/06/26 12:00	25.18.02.04	0				
	193.168.11.74	Ŷ	-	2014/06/23 17:03	25.20.02.01	55				
每页显示 10 🔻 条 📑 🕙	每页显示 10 💌 条 👼 🕲 共 2 条记录 1/1 < 🚿 跳转到: 1 💷 👔									

勾选一台或者多台客户端,激活命令按钮显示,包括【快速查杀】(开始/停止)、【全盘 查杀】(开始/停止)、【文件监控】(开启/关闭)和【邮件监控】(开启/关闭)。

窘	客户端安全状态						快速查		Q 全盘查杀▼	★ 文件监控 •	■邮件监控▼
		计算机名称 🔶	IP	文件监控	þ		开始		最后扫描时间	病毒库版本	发现病毒
		💻 cui	193.168.12.93	÷			停止		扫描中查看	24.38.03.02	0
		I F192C90240A3405	193.168.12.203)		Ŷ				24.38.03.02	0
		HQI-PC	193.168.12.215	Ť		Ŷ		20)12/11/29 13:27	24.38.03.02	0

点击命令按钮,即可对勾选客户端下发相应指令,屏幕右下角同步弹出命令已发送提示 框。



当客户端进行扫描时,该客户端最后扫描时间显示为"扫描中"。点击查看链接,弹出 扫描状态界面,分别展示快速查杀和全盘查杀信息,点击 ••• 或 •• 可以对执行中的扫描任 务进行暂停或停止控制。



7.2.2 病毒分析

病毒分析页面以图表方式从多维角度对病毒情况进行分析展示,包括近期病毒趋势图、 近期病毒概况与排行。



김〉INC 瑞星瑞星企业终端安全管理系统软件用户手册

1. 病毒分析——近期病毒趋势

近期病毒趋势以折线图形式展示某段时间内病毒的爆发趋势,管理员能够清晰了解全网 安全防护状况。

近期病毒趋势支持时间范围查询,条件包括不限、本周、上周、本月、上月和指定时间。

趋势图时间轴可按天、按小时、按周三种方式切换显示。



点击【本组染毒概况】,以饼状图形式展示本组染毒和未染毒客户端的数量及占客户端 总数量的比例。



点击【子组病毒排行】,以柱状图形式展示各子组染毒总次数及类型比例。



点击【本组病毒排行】,以柱状图形式展示不同类型病毒发作次数排行。



点击【本组发作最多】,以柱状图形式展示本组发作最多的病毒排行。



点击【子组染毒率排行】,以柱状图形式展示各子组平均客户端染毒次数排行。



点击【客户端染毒率排行】,以柱状图形式展示本组客户端染毒次数排行。



7.2.3 病毒详情

病毒详情页面展示客户端病毒查杀的统计信息,并以病毒为单位展示查杀信息,包括病毒名称、病毒分类、查杀数、染毒客户端和跟踪,并在右侧以折线图形式展示病毒趋势统计。 病毒查杀统计支持以下多种条件查询方式及其组合:

- 时间范围查询,条件包括不限、本周、上周、本月、上月和指定时间。
- 病毒来源查询,条件包括不限、全盘查杀、快速查杀、自定义查杀、文件监控和邮件监控。
- 病毒状态查询,条件包括不限、未处理、成功、处理失败、备份失败和处理中。

还可以对查询结果进行关键字搜索,关键字包括病毒名称和染毒文件名。

全网查杀病	● 病毒洋情 詳	系统加固 应用加固	
 累计发现 87 个病毒,其中 86 时间范围: 不限 本周 上 病毒来源: 不限 全盘查杀 病毒状态: 不限 未处理 搜索: 	个未处理(涉及1台客户端) 周 本月 上月 指定 / 快速查杀 自定义查杀 文 成功 处理失败 备份失败	 ▲ 2013-06-26 部 到 2 件监控 邮件监控 处理中 ● 病毒名称 ○ 染毒文件 	2013-06-26) 簡問
病毒 查杀统计 病毒名称 ▲	病毒分类 查杀劫	边毒客户端 跟腔	病毒趋势统计
Worm.Win32.Ms08067	·····································	1 查 <u>看</u>	
毎页显示 10 💌 条 👼 🖳	共 1 条记录 1/1	() 跳转到: 1	

瑞星企业终端安全管理系统软件 ©瑞星软件 当前贩本: 2.0.0.7

点击查杀数链接,弹出病毒详情信息,包括时间、客户端、IP、染毒文件、来源、处理 方式和状态。可以点击【恢复隔离文件】将所有客户端的隔离文件恢复到指定位置。

~	丰	-¥	44
小内	च	ŀŦ	111
	-		

						版省喧蛮立件
	1	1	1	1		恢复隔南又什
时间 🔻	客户端	IP	染毒文件	来源	处理方式	状态
2013/06/27 14:05:47	💻 xp 412F8C64464F	193.168.12.7	D:\病毒样本\ELF123\712999_13ab17fb.ELF	全盘查杀	刪除	成功
2013/06/27 14:05:46	💻 xp 412F8C64464F	193.168.12.7	D:\病毒样本\aa\ELF(1)rar>>ELF\712999_13ab17fb	全盘查杀	刪除	成功
2013/06/27 14:05:36	💻 xp 412F8C64464F	193.168.12.7	D:\\$RECYCLE.BIN\S-1-5-21-3519700922-358011405	全盘查杀	刪除	成功
每页显示 10 💌 条	a B		" 共 3	3 条记录 1/1		1 go

点击染毒客户端数量链接,弹出客户端列表信息,包括计算机名称和 IP 地址。

×

客户端列表								
计算机名称			IP地址					
— xp 412F8C64464F4F7		193.168.12.7						
每页显示 10 💌 条 🝶 📳	共 1 条记	录 1/1 < 📐	〕跳转到: 1	go				

点击病毒跟踪查看链接,显示相应病毒跟踪信息,包括病毒爆发的起始时间、传播路径 和客户端感染过程记录。



7.2.4 系统加固

系统加固是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。

系统加固支持以下多种条件查询方式及其组合:

- 时间范围查询,条件包括不限、本周、上周、本月、上月和指定时间。
- 防护类型查询,条件包括不限、文件防护、注册表防护、进程防护和系统防护。
 还可以对查询结果进行关键字搜索,关键字包括计算机名称和 IP 地址。

 全 内 査: 型 范 围 	一 病毒分析	病毒洋情 > 系统加固	应用加固						
● 您可以在此查看系统加固的防护记录 时间范围:不限 季周 上周 本月 上月 指定 从 2013-06-25 营 到 2013-06-26 营 防护类型: 不限 文件防护 注册表防护 进程防护 系统防护									
搜索: Q ④ 计算机名称 ◎ IP地址 系统加固									
计具机名称			•	IP					
每页显示 10 ▼ 条	-				│ 共 0 条记录 0/0 🔀				
		建昆金北核建立全管研究	幼生 @理里乾件 当	前版本・2007					

RISING 瑞星 瑞星企业终端安全管理系统软件用户手册

7.2.5 应用加固

应用加固是允许您添加需要加固保护的程序,通过检测应用程序的运行状态,拦截程序 的一次行为,防止恶意程序利用应用程序存在的漏洞对电脑进行破坏。

应用加固支持以下多种条件查询方式及其组合:

- 时间范围查询,条件包括不限、本周、上周、本月、上月和指定时间。
- 应用类型查询,条件包括不限、IE 浏览器和办公软件。

还可以对查询结果进行关键字搜索,关键字包括计算机名称和 IP 地址。

管理范围	全网查杀	病毒分析	病毒详情	系统加固	▶ 应用加固					
 您可以在此 时间范围: 应用类型: 搜索: 你田加肉 	 ③ 您可以在此查看应用加固的防护记录 时间范围: 不限 医圆 上周 本月 上月 指定 从 2012-06-26 ● 到 2012-06-26 ● 到 2012-06-26 ● 应用类型: 不限 IE浏览器 办公软件 搜索: ④ 计算机名称 ◎ IP地址 									
计算机名称				_		•	IP	风险数	最近发生时间	
每页显示 10	● ▼ 条 👼	2	瑞星企业	终端安全管理系	系统软件 ©I满星射	2件 当	当前版本: 2.0.0.7	共 0 条记录 0/0 📿		

김〉///《 法法室瑞星企业终端安全管理系统软件用户手册

7.3 漏洞扫描

系统漏洞是指应用软件或操作系统软件在逻辑设计上的缺陷或在编写时产生的错误,这 个缺陷或错误可以被不法者或者电脑黑客利用,通过植入木马、病毒等方式来攻击或控制整 个电脑,从而窃取您电脑中的重要资料和信息,甚至破坏您的系统。

漏洞管理可为您提供全面的漏洞管理服务,可以帮助您杜绝主机层面或网络层面的威胁, 提示您安装相关系统补丁,从而阻止非法侵入或窃取,保障您系统的安全。

	·····································						С 刷新	你好,admin	<u>修改密码 帮助</u> ▼ 退出		
Kart a	平台	防病毒	漏洞扫描	资产管理	XP盾				切换至管控台) 0	
管理范围	漏洞统计	漏洞修复	▶ 补丁管理								
未在下载 ① 未下	未在下载(6059) 正在下载(0) 已下载(68)										
严重											
	类别: <mark>不限</mark> 操作系	系统 微软产品	第三方软件								
操作系统	语言: <mark>不限</mark> 中文》	简体 中文繁体	英文								
	搜索:			へ (14) (14)	「名称						
未下载	トレティング トレット トレット シート シート シート・シート シート シート シート シート シート シート シート シート シート	载 导出下	载地址	地中所有 您已送	选中 <mark>0</mark> 个补丁				刷新)	
	补丁名称			描述		严重等级	语言	大小	操作		
	KB2909921	Microsoft安全	公告 MS14-010	- 严重 Internet E	Explorer的累积…	高危	中文简体	19.3M	<u>立即下载</u>		
	KB2797052	Microsoft Security Bulletin MS13-010 - 重大 向里標記語言中的		高危	中文繁体	776.6K	立即下载				
	KB2533623	Windows 更新	Windows 更新程序 (KB2533623)				中文简体	616.2K	立即下载		
	KB910620	Cumulative U	pdate for Intern	et Explorer 5.01	Service Pack 4 (轻微	英文	2.9M	<u>立即下载</u>		

7.3.1 漏洞统计

漏洞统计页面展示的是漏洞总体信息,按照处理结果分为三页,分别是已修复、修复失 败和已忽略。本文仅介绍已修复页面,其他页面类似。

点击【己修复】,以漏洞为单位展示漏洞总体信息,包括补丁名称、描述、严重等级、 已修复客户端、操作和详情。支持进行补丁名称的关键字搜索。

1420日 日修夏(195) 修夏失败(0) 已忽略(0)									
搜索:	Q. (e))补丁名称							
补丁名称 🔺	描述	严重等级	已修复客户端	操作	详情				
KB2115168	Microsoft安全公告 MS10-052 - 严重: Mic	高危	1		谨懂				
KB2229593	Microsoft安全公告 MS10-042 - 严重: 帮	高危	1		详情				
KB2296011	Microsoft安全公告 MS10-081 - 重要: Wi	重要	1		详情				
KB2347290	Microsoft安全公告 MS10-061 - 严重: 打	高危	1		详情				
KB2360937	此安全更新解决了 Microsoft Windows 中	重要	1		谨擅				
KB2387149	成功利用此漏洞的攻击者可以完全控制受	中等	1		谨懂				
KB2393802	此安全更新解决 Microsoft Windows 中一	重要	1		谨慎				
KB2412687	Microsoft安全公告 MS11-029 - 严重 GDI+	高危	1		详情				
KB2423089	此安全更新解决了Windows通讯簿公开披	重要	1		详情				
KB2425227	此安全更新可解决 Microsoft Windows 中	重要	1	-	<u>详情</u>				
每页显示 10 💌 条			共 195 条记	录 1/20 < 🕨 🕷	N转到: 1 go				

点击已修复客户端数量链接, 弹出客户端列表信息, 包括已修复此漏洞的客户端名称和 IP 地址。

北京瑞星信息技术有限公司

客户端列表	×
计算机名称	IP地址
I xp 412F8C64464F4F7	193.168.12.7
每页显示 10 🔻 🚔 🖳	共 1 条记录 1/1 < 📐 跳转到: 1 go

7.3.2 漏洞修复

漏洞修复页面展示的是未修复漏洞信息,并在右侧以图表形式配合展示。

未修复漏洞列表以漏洞为单位展示未修复漏洞信息,包括补丁名称、描述、严重等级、 客户端数量、大小及操作,并在右侧以柱状图形式展示各未修复漏洞所在客户端数量统计。 未修复漏洞信息支持以下多种条件查询方式及其组合:

- 严重等级查询,条件包括不限、轻微、一般、中等、重要和高危。
- 类别查询,条件包括不限、操作系统、微软产品和第三方产品。

还可以对查询结果进行补丁名称的关键字搜索。

理范围	漏洞统计 🕨 漏	洞修复	补丁管理				:
🕕 发现 5 个;	高危漏洞,未修复客户	□端涉及 2 台				立即处理	
严重等级:	不限 轻微 一	般中等	重要高危				
类别:	不限 操作系统	微软产品	第三方产品				
搜索:			Q	. 0 1	补丁名称		
卡修复漏洞列制	ξ.					未修复漏洞统计	
补丁名称▲	描述	严重等级	客户端	大小	操作	2.00	
KB2834886	此安全更新可解	高危	1	1.3M	修复 〇 忽略 〇 不处理		
<u><b2835364< u=""></b2835364<></u>	此安全更新可解	高危	1	1.1M	◉ 修复 ◯ 忽略 ◯ 不处理		
(B2855844	此安全更新可解	高危	1	697.7K	◉ 修复 ◯ 忽略 ◯ 不处理		
(B2929961	此安全更新可解	高危	1	406.3K	◉ 修复 ◯ 忽略 ◯ 不处理		
B2964358	此安全更新可解	高危	1	1.7M	◉ 修复 ◯ 忽略 ◯ 不处理		
						KB2904350	
每页显示 [10	💌 条 🔒 📓	1	共 5 条	记录 1/1	> 跳转到:1 go	КВ2834886 КВ2855844	
						KB2835364	
			瑞星企业	上终端安全管	管理系统软件 ©瑞星软件 当前版	本: 2.0.0.7	
选择	漏洞相关搏	桑作(修	复/忽	略/不	处理)后,点击	页面右上角 立即处理 , 1	訂百

引入INC F带星瑞星企业终端安全管理系统软件用户手册

点击补丁名称链接或客户端数量链接,弹出漏洞-未修复的客户端信息,包括计算机名称和 IP 地址,右面展示的是漏洞的基本信息,包括补丁名称、发布日期、补丁包大小、安全公告号、漏洞影响、漏洞描述和官方下载链接。

根据所选操作处理漏洞。

漏洞-未修复的客户端		×
共有 1 台客户端未修复此漏洞!		补丁名称 :KB2834886
计算机名称	IP地址	发布日期:
	193.168.12.7	补丁包大小: 1.3M 安全公告号: MS13-054 漏洞影响:
		Microsoft 安全公告 MS13-054 -
		严重 GDI+ 中的漏洞可能允许
		远程执行代码 (2848295)
		漏洞描述: 此安全更新可解决 Microsoft W indows、Microsoft Office、Mic rosoft Lync 和 Microsoft Visual Studio 中一个秘密报告的漏洞 。如果用户查看包含特制 TrueT ype 字体的共享內容,则该漏 洞可能允许远程执行代码。 <u>富方下载</u>
每页显示 10 💌 条 📾 🖳 共 1 条记录 1/3	- <u>く</u> 跳转到: 1 go	

7.3.3 补丁管理

补丁管理页面展示的是补丁总体信息。按照下载状态结果分为三页,分别是未在下载、 正在下载和己下载。

7.3.3.1 未在下载

点击【未在下载】,展示未下载补丁信息,包括补丁名称、描述、严重等级、语言、大 小和操作。

未下载补丁支持以下多种条件查询方式及其组合:

- 严重等级查询,条件包括不限、轻微、一般、重要和高危。
- 类别查询,条件包括不限、操作系统、微软产品和第三方软件。
- 操作系统语言,条件包括不限、中文简体、中文繁体和英文。

	漏洞统计	漏洞修复 > 补丁管理				
未在下载	(6068) 正在下载	(20) 已下载 (39)				
(1) 未下	藏高危漏洞 3149,;	其他补丁 2919 : 磁盘剩余空间 15.3G				
찌르	i等级: <mark>不限</mark> 轻微	一般 重要 高危				
	类别: <mark>不限</mark> 操作	系统 微軟产品 第三方软件				
操作	■系统语 <mark>不限</mark> 中文 言。	简体 中文繁体 英文				
	□· 按章:	0 @ 11798				
	22.R: [
未下载	补丁列表 立即	「裁 导出下裁地址」 通過中所有 您已选中 0 个补丁				刷新
	补丁名称	措达	严重等级	语言	大小	操作
	KB2909921	Microsoft 安全公告 MS14-010 - 严貧 Internet Explorer 的	高危	中文简体	19.3M	立即下载
	KB2797052	Microsoft Security Bulletin MS13-010 - 重大 向量標記語言	高危	中文繁体	776.6K	立即下载 🧮
	KB2533623	Windows 更新程序 (KB2533623)	高危	中文简体	616.2K	立即下载 🗎
	KB910620	Cumulative Update for Internet Explorer 5.01 Service Pa	轻微	英文	2.9M	立即下载 🤎
	KB2564958	Microsoft Security Bulletin MS11-075 - Important:Vulner	愛愛	英文	728.6K	立即下载 🗎
	KB2876331	Microsoft Security Bulletin MS13-089 - 冀大 Windows 圖	高危	中文繁体	631.7K	立即下载 🗎
	KB963093	這個安全性更新可解決 Windows 搜尋中一項未公開報告的弱	一般	中文繁体	956.3K	立即下载 🕮
	KB2124261	Microsoft 安全公告 MS10-065 - 貧憂: Microsoft Internet I	医医	中文简体	612.3K	立即下载 👛
	KB976749	Internet Explorer 更新 (KB976749)	轻微	中文简体	1.7M	立即下载 🥮
	KB954326	Microsoft 安全公告 MS08-052 - 严重: GDI+ 中的漏洞可能	高危	中文简体	8.7M	立即下载 👛
每页显	示 10 🔻 🏯	图]	:	共 6068 条记录 1	1/607 < 🕨 跳鞍	到: 1 go

AISING 瑞星 瑞星企业终端安全管理系统软件用户手册

点击补丁对应操作的立即下载链接,启动相关补丁下载;点击户,访问相关补丁官方 介绍链接。

勾选多个补丁或一选中所有,点击 立即下载,启动补丁的批量下载。

点击 导出下载地址,导出所有未在下载补丁的官方下载地址(TXT格式)。

7.3.3.2 正在下载

点击【正在下载】,展示正在下载补丁信息,包括补丁名称、描述、严重等级、操作系 统语言、大小和下载状态。

正在下载补丁支持下载状态查讯,条件包括不限、下载中、暂停和下载失败。还支持对 查询结果进行补丁名称的关键字搜索。

AISING 瑞星瑞星企业终端安全管理系统软件用户手册

首页 计算	፤机→ 网络→	杀毒→ 防火墙→	漏洞・	软件→ i	硬件・	涉密 -	开机 -		
未下载(3933) 正在	E下载(9) 已下载(986	i)							
 ① 下载中补丁 0 个 	,下载失败补丁 9 个 ; 碇	盘剩余空间 29.8G							
下载状态: 不限	等待下载 下载中	下载失败							
搜索:		へ ④ 补	丁名称						
正在下载补丁列表	导出下载地址						(刷新)
补丁名称 ▲		描述	严重等级	操作系统语言	大小	下载状态	操	:ſF	
Flash Player	Flash Player 更新程序		重要	中文简体	2M	下载失败	重新下载	取消	•
KB2656374	Microsoft安全公告 MS1	12-025 - 严重:.NET Framework	高危	中文简体	421.9K	下载失败	重新下载	取消	
KB2705219	Microsoft安全公告 MS1	12-054 - 严重 Windows 网络组	重要	中文简体	389.4K	下载失败	重新下载	取消	
KB2705219	Microsoft安全公告 MS1	12-054 - 严重 Windows 网络组	重要	中文简体	67 1 K	下载失败	重新下载	取消	•
KB2705219	Microsoft安全公告 MS1	12-054 - 严重 Windows 网络组	重要	中文简体	362.8K	下载失败	重新下载	取消	
KB2705219	Microsoft安全公告 MS1	12-054 - 严重 Windows 网络组	重要	中文简体	292.8K	下载失败	重新下载	取消	•
KB2753842	Microsoft安全公告 MS1	12-078 - 严重 Windows 内核模	重要	中文简体	635.6K	下载失败	重新下载	取消	
KB2753842	Microsoft安全公告 MS1	12-078 - 严重 Windows 内核模	重要	中文简体	431.2K	下载失败	重新下载	取消	-
KB2823324	Microsoft安全公告 MS1	3-036 - 重要 内核模式驱动程序	有 高危	中文简体	774.3K	下载失败	重新下载	取消	•
每页显示 10 💌	条 🚔 🗐				共 9 条	记录 1/1 <) 跳转到:	1 go	ור

点击补丁对应操作的重新下载链接,重启相关补丁下载;点击取消链接,取消相关补丁下载;点击,访问相关补丁官方介绍链接。

点击 导出下载地址,导出所有正在下载补丁的官方下载地址(TXT格式)。

7.3.3.3 已下载

点击【已下载】,展示已下载补丁信息,包括补丁名称、描述、严重等级、操作系统语 言和大小。

已下载补丁支持以下多种条件查询方式及其组合:

- 严重等级查询,条件包括不限、轻微、一般、重要和高危。
- 类别查询,条件包括不限、操作系统、微软产品和第三方软件。
- 操作系统语言,条件包括不限、中文简体、中文繁体和英文。

还可以对查询结果进行补丁名称的关键字搜索。

RISING 瑞星 瑞星企业终端安全管理系统软件用户手册

首页 计算机	- 网络 - 杀毒 -	防火墙 -	漏洞▼	软件▼	硬件,	步密 - 开机	Ŧ
未在下载(3933) 正在	下载(9) 已下载(986)						
\rm 🕑 已经下载系统类补丁	804 ,微软产品类补丁 182 ,第3	方产品类补丁 0 ; 磁		.8G			
严重等级: 不限	轻微 一般 重要 高危						
类别: 不限	操作系统 微软产品 第三方转	件					
操作系统语言: <mark>不限</mark>	中文简体 中文繁体 英文						
搜索:		へ 	高称				
已下载补丁列表							刷新
补丁名称	4	載述		严重等级	操作语言	大小	操作
KB2533623	Windows 更新程序 (KB253362:	;)		高危	中文简体	616.2K	下载到本机 🗎
KB954326	Microsoft 安全公告 MS08-052 -	^亚 重: GDI+ 中的漏洞	同可能允许远…	高危	中文简体	8.7M	下载到本机 🗎
KB910437	Windows XP 更新程序 (KB9104	37)		一般	中文简体	1.1M	<u>下载到本机</u>
KB977074	Windows 7 更新程序 (KB97707	4)		重要	中文简体	1.1M	下载到本机 🗎
KB2597120	Microsoft Office 2007 suites 更亲	(KB2597120)		高危	中文简体	14.2M	下载到本机 🗎
KB923191	Windows 资源管理器中的漏洞可	能允许远程执行		高危	中文简体	4.1M	下载到本机 🗎
KB2799494	Microsoft安全公告 MS13-017 -	重要 Windows 内核中	中的漏洞可能…	高危	中文简体	2.2M	下载到本机 🗎
KB2809289	Microsoft安全公告 MS13-021 -	亚重 Internet Explore	r的累积性安	高危	中文简体	13.3M	下载到本机 🗎
KB943295	Windows Server 2003 更新程序	(KB943295)		轻微	中文简体	538K	下载到本机 🚔
KB2656351	Microsoft安全公告 MS11-100 -	≖重:.NET Frameworl	k 中的漏洞可…	高危	中文简体	8.7M	下载到本机 🗎
每页显示 10 🔻 条					共 986 条记录	1/99 < 🕨 跳	转到: 1 go

点击补丁对应操作的下载到本机链接,保持相关补丁至本机;点击[▶],访问相关补丁 官方介绍链接。

7.4 资产管理

资产管理包括七部分内容:禁用软件、保护软件、关注软件、软件详情、软件部署、硬件异动和硬件详情。通过此功能可以有效管理企业软件的使用情况,保障企业软件资产安全, 还可以有效监控企业硬件的使用情况保障企业硬件资产安全。

RISING 瑞星 瑞星企业终端安全管理系统软件用户手册

Y	よる	星企业组	冬端安全管理	系统软件 - 审	计控制台	(体验版)		С 刷新	你好 , admin	修改密码	帮助▼ 退出
8		平台	防病毒	漏洞扫描 资	铲管理	XP盾				切换至	管控台 🖸
管理	范围	禁用软件	保护软件	关注软件	软件详情	软件部署	硬件异动	▶ 硬件详情			
•	查看客户端	的硬件信息									
	时间范围: 在线状态:	<mark>不限</mark> 本 不限已	周 上周 本月 登录 未登录	上月 指定 ,	₩ 2014-06-:	25 🗂 到	2014-06-25				
	搜索:			Q,	◎ 计算机:	名称 🔘 IPti	3址				
_											
	计算机:	名称 🔺	IP地址	上报时间		电脑型号		操作系统	充	详	情
Ę.	CUIC-PC		192.168.90.151	2014/06/25 14:23	3:51 联想 LE	ENOVO QiTianM	6900 台式机···	Microsoft Windows 7	′ 旗舰版 32-bit	硬件详情	设备详情

7.4.1 禁用软件

在客户端机器上禁止使用某些软件,以达到统一管理的目的。禁用列表展示信息包括禁 用软件名称、厂商名称和装机数量。

禁用软件支持以下多种条件查询方式及其组合:

- 时间范围查询,条件包括不限、本周、上周、本月、上月和指定时间。
- 软件分类查询,条件包括聊天工具、浏览器、音频播放、视频播放、输入法、下载工具、系统工具、图形图像、办公学习、安全防护、压缩刻录、股票网银、媒体编辑、游戏休闲、编程开发、网络应用、文字处理、其他软件、服务和自定义规则。还可以对查询结果进行关键字搜索,关键字为软件名称。

北京瑞星信息技术有限公司

管理范围	禁用软件	保护软件	关注软件	软件详情	软件部署	硬件异动	硬件详情		
🕕 发现 0 款	禁用软件被安装访	5ì可							
时间范围:	不限 本周	上周 本月	上月 指定	从 2013-06-2	26 🛗 到	2013-06-26	<u>010</u>		
软件分类:	不限 聊天工 股票网银 媒	具 浏览器 体编辑 游戏体	音频播放 视频 闲 编程开发	播放 输入法 网络应用 、	下载工具 →字外理 耳·	系统工具 医 他软件 服务	形图像 办公学习 白完义规则	安全防护 压缩刻录	
搜索:	1007101-1040 MA		Q Q	 · · · · · · · · · · · · · · · · · · · · · · · ·	~	1040(11)110/0			
*****						***	7357622231		
禁用软件列表						· []	用软件统计		
	软件名称	•	厂商名称		装机数量				
							丰优列200条(出的粉锯、天注豆子肉主。	
							TRAEN D.K.	TH MANDO / /6/2322/142120 *	
每页显示 10	▼条 🖶	8	共 0 条记录 0	/0 < _> 跳	转到: 0	go			
			瑞星企业组	冬端安全管理系统	充软件 ©瑞星软	件 当前版本:2	.0.0.7		

7.4.2 保护软件

在保护软件页面中统计了所有保护软件的信息,包括软件名称、厂商名称和装机数量, 使管理员可以实时了解管理网络内所有装机软件。

保护软件支持以下多种条件查询方式及其组合:

- 时间范围查询,条件包括不限、本周、上周、本月、上月和指定时间。
- 软件分类查询,条件包括聊天工具、浏览器、音频播放、视频播放、输入法、下载工具、系统工具、图形图像、办公学习、安全防护、压缩刻录、股票网银、媒体编辑、游戏休闲、变成开发、网络应用、文字处理、其他软件、服务和自定义。

还可以对查询结果进行关键字搜索,关键字为软件名称。

管理范围	禁用软件	▶ 保护软件	‡ 关注软件	软件详情	软件部署	硬件异动	硬件详情		
🕕 发现 0 款1	保护软件被安	装访问							
时间范围: 软件分类: 搜索:	不限 本. 不限 聊 股票网银	周 上周 天工具 浏览 媒体编辑	本月 上月 指定 包器 音频播放 视线 游戏休闲 编程开发 Q	从 2013-06 频播放 輸入法 网络应用 の 、 、 、 、 、 、 、 、 、 、 、 、 、	<u>26</u> 一 26 一 到 五 五 五 二 二 一 到 一 到 二 二 具 文 字 处理 其 二 二 二 具 文 字 处理 其 二 二 二 二 二 二 二 二 二 二 二 二 二	2013-06-26 系统工具 图 他软件 服务	聞 御	安全防护 压缩刻	₹
保护软件列表						保护	软件统计		
	软件名称	•	厂商名称		装机数量				
							未找到符合条	件的数据,无法显示图:	表。
每页显示 10	▼ 条	-	共 0 条记录	0/0 < > 5	姚转到: 0 [go			
			瑞星企业	终端安全管理系	S 经软件 @F#2早的	?件 当前版本:2	007		

点击保护软件界面默认打开的即为按软件显示的列表。在此列表中提供了装机软件的名称、厂商名称和装机数量。

点击【软件名称】、【厂商名称】或【装机数量】相应的信息会按照升序或降序的方式重 新排列。点击【装机数量】项中的数字会弹出显示已安装此软件的计算机名称、IP 地址信 息的对话框。

客户端列表			×
计算机名称		IP地址	
CSC-045		192.168.30.120	
CSC-159		192.168.30.122	
LUHANG-PC		193.168.20.236	
MOYH-PC		192.168.170.42	
ZHAOLIYAN		192.168.110.56	
毎页显示 10 🔻 条	共 5 条记录 1/	1 < > 跳转到: [][go

7.4.3 关注软件

关注软件界面由关注软件列表和关注软件装机量统计两部分内容组成。

关注软件支持时间范围的查询方式,条件包括不限、本周、上周、本月、上月和指定时间。

还可以对查询结果进行关键字搜索,关键字为软件名称。

The second secon	理范围	禁用软件	保护软件	: ▶ ≯	总注软件	软件详情	软件部署	硬件异动	硬件详情		
	发现 0 款	关注软件被安装									
	时间范围:	不限 本周	上周	本月上	二月 指定	从 2013-06-26	1 1 1	2013-06-26			
	搜索:				Q	◎ 软件名称					
Ì	注软件列表							关注	E软件装机里统计		
						1					
		软件名利	λ 		▲ 大小	已安装客户端	場 操作	_			
								3	▶ 设置关注软件(只能在根组下设	置)或关注软件未被安	
									装,无法显示图	表。	
	每页显示 [10	_▼ 条 🖶	B)	́,	ŧ 0 条记录 0,	/0 【< 】 跳棘	题: [o] [g	0			
					理見会.11.4	2.当中へ巻ままでか	わみ (の)当日わり	+ 当台版本, 2	0.0.7		
					师生止115	>>而以土昌理杀统	秋日~満生秋日	↑ ヨ別派本: 2	.0.0.7		

在关注软件列表中显示的是关注软件名称、大小、已安装客户端和操作。点击【已安装 客户端】栏中的数字会弹出所有已安装此禁用软件的客户端的计算机名称以及 IP 地址的对 话框。

客户端列表			×
计算机名称	•	IP地址	
20110621-2327		192.168.150.68	
20110704-1138		192.168.70.25	
20110704-1138		192.168.70.25	
20110704-1138		192.168.70.25	
20110727-1343		192.168.70.35	
ADMIN-PC		192.168.170.5	
CHENYUNLONG-PC		193.168.20.174	
CSC_011		192.168.30.134	
CSC_011		192.168.30.134	
CSC_249		192.168.30.150	
毎页显示 10 🔻 条	共 36 条记录 1/	4 < 🕨 跳转到:	go

关注软件装机量统计以柱状图的形式展示了装机量排名前十位的软件。



7.4.4 软件详情

在软件详情页面中统计了所有装机软件的信息,包括软件名称、大小、已安装客户端和 加关注,使管理员可以实时了解管理网络内所有装机软件。

软件详情支持时间范围的查询方式,条件包括不限、本周、上周、本月、上月和指定时间。

还可以对查询结果进行关键字搜索,关键字为软件名称。

禁用: 理范围	欠件 保护软	件 关注软件	▶ 软件详情	软件部署	硬件异动	硬件详情	Ĩ	
查看客户端的软件	信息,还可以将软	件加为关注软件或禁	用软件					
时间范围: 不限	本周 上周	本月 上月 排	锭 从 2013-06-	26 🗂 到	2013-06-26	<u>9:9</u>		
搜索:			<u> </u> 9] (④ 软件名)	称				
		软件名称		•	大小		已安装客户端	加关注
【南京银行签名控件	1				836.6K		1	
360极速浏览器					233.2M		1	
360驱动大师					27.9M		1	
7-Zip 9.32 alpha							1	✓
dobe Flash Player	13 ActiveX						1	
dobe Flash Player	13 Plugin						1	
Adobe Reader XI (11	.0.07) - Chinese S	Simplified			117.9M		1	
oure RP Pro 6.5					32.7M		1	
Canon MF4400 Seri	es						1	
CMBEdit					238.4K		1	
每页界示 10 💌	条 🚔 🖻					共 10)条记录 1/10 < 🕨	跳转到: 1 (

김〉INC 這這是瑞星企业终端安全管理系统软件用户手册

瑞星企业终端安全管理系统软件 ©瑞星软件 当前版本: 2.0.0.7

软件详情页面显示的是客户端软件信息等。点击软件详情界面默认打开的即为按软件显示的列表。在此列表中提供了装机软件的名称,装机量等信息;在此列表中管理员可以勾选 【加关注】。

【加关注】勾选后,此软件将会在【软件管理】/【关注软件】中显示。点击【软件名称】、【大小】、【已安装客户端】或【加关注】,相应的信息会按照升序或降序的方式重新排列。

客户端列表		>
	计算机名称	IP地址
💻 LIUYH-PC		193.168.11.74
每页显示 10 🔻 🖡		共 1 条记录 1/1 < > 跳转到: 1 😡 go

点击【已安装客户端】项中的数字会弹出显示已安装此软件的计算机名称、IP 地址信 息的对话框。

客户端列表		;	
计算机名称	IP地址		
CSC-045		192.168.30.120	
CSC-159		192.168.30.122	
LUHANG-PC		193.168.20.236	
MOYH-PC		192.168.170.42	
ZHAOLIYAN		192.168.110.56	
毎页显示 10 🔻 条	共 5 条记录 1/	/1 < > 跳转到:go	

7.4.5 软件部署

在软件部署页面中统计了所有第三方应用软件的信息,包括软件名称、软件分类、厂商 名称、版本、已部署客户端和未部署客户端等信息,使管理员可以实时了解管理网络内所有 第三方软件。

软件部署支持软件分类的查询方式,条件包括聊天工具、浏览器、音频播放、视频播放、 输入法、下载工具、系统工具、图形图像、办公学习、安全防护、压缩刻录、股票网银、媒 体编辑、游戏休闲、编程开发、网络应用、文字处理、其他软件、服务和自定义。

还可以对查询结果进行关键字搜索,关键字为软件名称。

管理范围	禁用软件	保护软件	关注软件	软件详情	▶ 软件部署	硬件异动	硬件详情		:
 全方位的 	④ 全方位的了解第三方应用软件的部署情况								
软件分类:	较件分类: <mark>不限</mark> 聊天工具 浏览器 音频播放 视频播放 输入法 下载工具 系统工具 图形图像 办公学习 安全防护 压缩刻录 股票网银 媒体编辑 游戏休闲 编程开发 网络应用 文字处理 其他软件 自定义								
搜索:			Q,		名称				
第三方应用软	件部署列表							•	• 添加第三方软件
	软件名称	•	软件分类		厂商名称		版本	已部署客户端	未部署客户端
_									
_									
每页显示 10 💌 条 🖷 🖳 共 0 条记录 0/0 🖉 跳转到: 0 00									

瑞星企业终端安全管理系统软件 ©瑞星软件 当前版本: 2.0.0.7

软件部署页面显示的是第三方应用软件的信息。点击软件部署界面默认打开的即为按软件显示的列表。在此列表中提供了第三方软件的软件名称,软件分类,厂商名称,版本,已 部署客户端,未部署客户端等信息。

同时,点击【软件名称】、【软件分类】、【厂商名称】、【版本】、【已部署客户端】或【未 部署客户端】,相应的信息会按照升序或降序的方式重新排列。

客户端列表	×
计算机名称	IP地址
📃 LIUYH-PC	193.168.11.74
每页显示 10 💌 条 🖷 🖳	共 1 条记录 1/1 < 📐 跳转到: 1 🛛 😡

点击【己部署客户端】项中的数字会弹出显示已安装此软件的计算机名称、IP 地址信息的对话框。

客户端列表			×	
计算机名称	IP地址			
CSC-045		192.168.30.120		
CSC-159		192.168.30.122		
LUHANG-PC		193.168.20.236		
MOYH-PC		192.168.170.42		
ZHAOLIYAN		192.168.110.56		
毎页显示 10 💌 条	共 5 条记录 1	/1 < 📐 跳转到:	go	

7.4.6 硬件异动

点击硬件管理,默认打开的即为硬件异动审计界面。

硬件异动支持以下多种条件查询方式及其组合:

- 时间范围查询,条件包括不限、本周、上周、本月、上月和指定时间。
- 异动类型查询,条件包括添加、移除和变更。
- 硬件类型查询,电脑型号、处理器、主板、内存、硬盘、显卡、光驱、声卡、网卡、
 键盘和鼠标。

还可以对查询结果进行关键字搜索,关键字为软件名称和 IP 地址。

管理范围	禁用软件	保护软件 关注	软件 软件详情	软件部署 ▶	硬件异动	硬件详情			
🕕 发现 0 台	③ 发现 0 台客户端有硬件异动。								
时间范围: 异动类型: 硬件类型: 操作结果: 搜索:	时间范围: 不照 本周 上周 本月 上月 指定 从 2013-06-26 🛗 到 2013-06-26 🛗 异动类型: 不照 添加 移除 变更 硬件类型: 不限 电脑型号 处理器 主板 内存 硬盘 显卡 显示器 光躯 声卡 网卡 键盘 鼠标 操作结果: 不限 未确认 已确认 搜索:								
й	算机名称	▲ IP地址	时间	异动类型	硬件类型	名称	确认异动		
每页显示 (10	· · ▼ 条 →	B				共 0 条记录 0/0 🔽 🚿 跳转	9: D 90		

瑞星企业终端安全管理系统软件 ©瑞星软件 当前版本: 2.0.0.7

异动信息列表里详细列出了存在硬件异动的计算机名称、IP 地址、时间、异动类型、 硬件类型、名称以及确认异动操作。在【确认异动】栏,勾选后此异动将被视为正常情况。 点击【计算机名称】、【IP 地址】、【时间】、【异动类型】、【硬件类型】、【名称】或【确认异 动】等相应的信息会按照升序或降序的方式重新排列。

7.4.7 硬件详情

硬件详情页面提供了网络内所有计算机的信息,包括:计算机名称、IP 地址、上报时间、电脑型号、操作系统和详情。

硬件异动支持以下多种条件查询方式及其组合:

- 时间范围查询,条件包括不限、本周、上周、本月、上月和指定时间。
- 在线状态查询,条件包括已登录和未登陆。

还可以对查询结果进行关键字搜索,关键字为软件名称和 IP 地址。
き理范围	使用软件	保护软件	关注软件 软件	羊情 软件部署 硬件异动	▶ 硬件详情	:
 查看客户端的 时间范围: 在线状态: 搜索: 	硬件信息 下限 本 下限 已	周 上周 本月 登录 未登录	上月 指定 从 (2013-06-26 🛗 到 2013-06-26) 计算机名称 🔘 IP地址		
计算机名称	称 🔺	IP地址	上报时间	电脑型号	操作系统	详情
LIUYH-PC		193.168.11.74	2013/06/26 14:19:25	戴尔 0P301D Vostro 220 Series 台…	Microsoft Windows 7 旗舰版 32	<u>硬件详情</u> 设备详情
每页显示 10	▼ 条	🖶 🖄			共 1 条记录 1/1 < 🚿	〕跳转到: 1 go

ጓ▷ INC I # 2 瑞星企业终端安全管理系统软件用户手册

瑞星企业终端安全管理系统软件 ©瑞星软件 当前版本: 2.0.0.7

点击【计算机名称】或【IP 地址】等,相应的信息会按照升序或降序的方式重新排列。

点击【硬件详情】或【设备详情】可以了解对应客户端详细的硬件信息或设备信息。

硬件详情 (计算机名称:	BAO-PC IP地址: 192.168.90.	150)	×
概览 ◆	概览 ————		
主板	电脑型号	联想 To be filled by O.E.M. YangTianM6600D 台式机电脑	
处理器	操作系统	Microsoft Windows 7 旗舰版 32-bit	
酒 舟	内存	8 G	
WC mi	处理器	Intel(R) Pentium(R) CPU G630 @ 2.70GHz x64架构	
内存	主板	联想 To be filled by O.E.M.	
显卡	硬盘	ST3500418AS 465 G	
显示器	显卡	Intel(R) HD Graphics Family 1 G	
光驱	显示器	LEN10B8 20 英寸	
主 上	光驱	PLDS DVDROM DH16D6SH DVD-ROM	
严下	声卡	Realtek High Definition Audio	
网卡	网卡	Realtek	
键盘	键盘	Enhanced (101- or 102-key)	
鼠标	鼠标	USB 输入设备	

×

设备详情	×
设备详情 设备异动	📃 显示隐藏的设备
 □ ● BAO-PC ● ● DVD/CD-ROM 驱动器 ● □ DE ATA/ATAPI 控制器 ● ● 处理器 ● ● 处理器 ● ● 处理器 ● ● 碰盘驱动器 ● ● 前口 (COM 和 LPT) ● ● 计算机 ● ● 並視器 ● ● 並視器 ● ● 並視器 ● ● 通用串行总线控制器 ● ● 通用串行总线控制器 ● ● 通用串行总线控制器 ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ●	

7.5 XP 盾

XP 盾页面包括两部分内容:防御概要和攻击详情。通过以上两个功能,管理员可以看 到全网 XP 客户端安全状态的监控情况。

3	瑞星企业终	端安全管理	系统软件 - 富	i 计控制	台(体验版)		С 刷新	你好,admin	<u>修改密码 帮助</u> ▼ <u>退出</u>
800	平台	防病毒	漏洞扫描 多	萨管理	XP盾				切换至管控台 ●
管理范围	▶ 防御概要	攻击详情							
1 截至日	目前, <mark>0</mark> 台终端,共	共拦截漏洞攻击 0	次						
时间流 攻击势	如果:不限 本周 本周 本型:不限 其它	】 上周 本月]攻击类型 缓冲	上月 指定 区溢出 ret2lib攻;	从 2014-0 击方式 SH	6-25 📄 到 HE被覆盖 代码	201· 在堆上	4-06-25 🛗 执行 代码在栈上执行		
括	捜索:		Q,	◉ 计算	机名称 🔘 IP	地址			
漏洞攻击	情况统计						漏洞攻击情况		
	计算机名称	· · · ·	IP		攻击次数				
	<u>C-PC</u>		192.168.90.1	51	192				
							未找到符合条件	的数据,无法显	示图表。
							攻击方式情况		
每页显示	10 ▼ 条 🦷		共 0 条记录 0/	0 < >	跳转到: 0	go			

7.5.1 防御概要

防御概要界面由漏洞攻击情况统计、漏洞攻击情况和攻击方式情况三部分内容组成。

漏洞攻击统计情况支持以下多种条件查询方式及其组合:

- 时间范围查询,条件包括不限、本周、上周、本月、上月和指定时间。
- 攻击类型查询,条件包括其它攻击类型、缓冲区溢出、ret2lib 攻击方式、SHE 被覆 盖、代码在堆上执行和代码在栈上执行。

还可以对查询结果进行关键字搜索,关键字包括计算机名称和 IP 地址。

理范围	防御概要 攻击详情				
截至目前,	1 台终端,共拦截漏洞攻击 1 2	欠			
时间范围:	不限 本周 上周 本月	上月 指定 从 2014-0	6-26 🛗 到 201	4-06-26	
攻击类型:	不限 其它攻击类型 缓冲	区溢出 ret2lib攻击方式 SH	HE被覆盖 代码在堆上	执行 代码在栈上执行	
搜索:		Q ④ 计算	机名称 🔘 IP地址		
詞攻击情况约	ŧ ڼ			漏洞攻击情况	
	计算机名称 🔶	IP	攻击次数		
<u>412F8C64</u>	464F4F7	193.168.12.7	1	1	
				I	
				0	
每页显示 10	💌 条 🖶 📑	共 1 条记录 1/1 < 🚿	跳转到: 1 go		
				0 1 2 3 4 5 6	
				攻击方式情况	
				缓冲区溢出 100%	

7.5.2 攻击详情

攻击详情界面展示客户端安全状态信息,包括计算机名称、IP 地址、攻击类型、攻击进程、漏洞名称和漏洞描述。

攻击类型支持以下多种条件查询方式及其组合:

- 时间范围查询,条件包括不限、本周、上周、本月、上月和指定时间。
- 攻击类型查询,条件包括其它攻击类型、缓冲区溢出、ret2lib 攻击方式、SHE 被覆 盖、代码在堆上执行和代码在栈上执行。

还可以对查询结果进行关键字搜索,关键字包括计算机名称和 IP 地址。

聖范围							
) 截至目前, 时间范围: 攻击类型: 搜索:	检测出 1 种攻击类型, 涉万 不限 李周 上周 2 不强 其它攻击类型 1	瑞洞 1 个, ・ ド月 上月 ・ 家中区溢出	1 台终端受到攻击 指定 从 201 ret2lib攻击方式	4-06-28 📑 到 2014-0 SHE被覆盖 代码在堆上执行 计算机名称 🔘 IP地址	5-25 6 计 代码在栈上执行		
	计算机名称		IP地址	攻击类型	攻击进程	漏洞名称	漏洞描述
412F8C64464	F4F7		193.168.12.7	缓冲区溢出	C:\Documents and S ettings\Administrator \桌面\svchost.exe	MS08-067	stack overflo

RISING 瑞星瑞星企业终端安全管理系统软件用户手册

瑞星企业终端安全管理系统软件 ©瑞星软件 当前版本: 2.0.0.98

8. 升级中心

瑞星企业终端安全管理系统软件——升级中心是提供管理员日常部署和升级的管理页 面。升级中心管理页面主要包括【客户端安装包】、【手动升级】和【第三方软件】三部分功 能组成。

8.1 客户端安装包

客户端安装包页面主要是安装包的管理页面,管理员可以查看到正在使用的安装包的制 作时间、版本、大小、下载地址以及包含的子产品。在【全部安装包】列表中能够查看到所 有安装包的相关信息,管理员可以对这些安装包进行【删除】或者【立即发布】等操作。

点击【制作安装包】可以进行安装包制作页面,管理员可对安装包的名称、包含哪些子 产品、连接的业务中心地址及端口进行设置并打包。

ጓ▷ INC J 法全 瑞星企业终端安全管理系统软件用户手册

瑞星企业终端安全管 客户端安装包 手起	理系统软件 - 升级中心 动升级		^{当前用户} :admin <u>修改密码</u> 论坛 退出 <mark>切换至管控台 €</mark>
制作安装包 基本信自边罢。 /司四国年初会目2	后先武准会中)		
主法与专办。	コ/152表「III /	新士。 20110(西如中词,2014.07.12.10.40.25)	
☆ 50 4 初・ 客户端子产品:		MK44、2.0.1.10(史初時時, 2014-07-12 10.40.23)	
☑ 防病毒(1.)	0.2.67) 🗹 必装	📝 漏洞扫描(1.0.0.99) 必装	
病毒库版本	5: 24.00.25.32	漏洞库版本: 1.0.0.99	
默认策略	无 •	默认策略 无	•
√ II资产管理	(1.0.0.92) 📝 必装		
默认策略	无		
软件部署新	8略 无 ▼		
∪盘管理第	略 无 •		
₩ XP盾 (1.0.	0.10) 🗹 必装		
默认策略	无 🔻		
✔ 监控组件()	1.0.1.6) 🗹 必装	✔ 防火墙(1.0.1.56) ✔ 必装	
		恶意网址库版本: 24.00.25.39	
√ U盘管理(1.	. 0. 0. 40) 🗹 必装	✓ 安全助手(1.0.0.4) ✓ 必装	
客户端代理(1.	.0.2.82)	软件部署组件(1.0.3.15)	
默认策略	无	默认策略 无	•
共有策略	无 🔻		
服务器子产品 :			
📃 漏洞补丁中。	论(1.0.0.67) 📃 必装	一 升级中心(1.0.2.1)	
管理中心(1)	1.0.3.51) 📃 必装	🥅 业务中心(1.0.0.43) 🦳 必装	
公共参教 (要连接的业务中心地址) =		
服务器地址 193	.168.12.116 端口 5555		
📃 虚拟机环境			
安装包是否自动更新成最新版本等	? ●是 ◎否		
安装包保留旧版本个数?	◎不保留 ◎5 ◎10 ◎15		
安装方式?	◎常规 ⑧自动安装 ◎静默安	装 (无界面)	
高级参数设置:			
是否配置更多的安装参数?	◎是 ⑧否		
	立即制作	返 回	
	儀星企业终端安	会管理系统软件 ◎瑞星软件	

8.2 手动升级

手动升级页面提供管理员手动上传升级包至服务器的入口,并显示上次手动升级的时间。 管理员可以通过【选择文件】按钮选择需要上传的升级包,并点击【上传】,系统会自动将 升级包上传到服务器指定路径下并将升级包解压至升级目录下供客户端升级。

김১INC 瑞星瑞星企业终端安全管理系统软件用户手册

瑞星企业终端安全管理系统软件 - 升级中心 客户端安装包 手动升级 第三方软件	当前用户 : admin 参达密码 论运 退出 切换至管控台 ●
上次手动升级时间: 2014/07/12 10:50:33 请选择升级包文件上传至升级服务器: 	
瑞星企业终端安全管理系统软件 ©端星软件	

8.3 第三方软件

第三方软件页面提供第三方应用软件列表供管理员对软件进行管理。管理员可以通过列 表查看到软件名称、下载地址、版本、大小、上传时间等相关信息。并可以对软件包进行上 传和删除等操作。

瑞星企业终端3	安全管理系统软件 - 升级中心 手动升级 第三方软件			当前用户:admin) <mark>f</mark> 切打	該國國 论运 退出 ● 全管控台 ●
 可上传第三方应用软件包或删 	哪涂已上传的软件,多方便了解软件的相关信息。				
第三方应用软件列表	第三方应用软件包	1	1		
软件名称	下载地址	版本	大小	上传时间	操作
	瑞星企业终端安全管理系统软件	牛◎瑞星软件			

点击【上传第三方应用软件包】,跳转到上传包页面。管理员可以定义软件名称、选择

软件安装程序(上传包大小不能大于 100M)、设置检查是否安装的条件。支持软件名称、 注册表检查、版本检查、注册表检查及 CMD 命令等多种检查方式。

😽 瑞星企业终端安全管理系统软件 - 升级中心	当前用户:admin <u>修改密码</u> <u>论</u>
客户端安装包 手动升级 第三方软件	切換至管控
说明:上传第三方软件包功能是为了方便管理员续一分发部署相关文件;部署软件的相; 理员在分发时只需选择相应的软件即可完成分发操作;	关名称、软件包路径、规则检查、命令均可绕一成一套模板上传至RUC平台上,管
软件名称:	
上传包:	选择文件
ā.	级设置
检查是否安装	- 检查版本
 通过软件名称检查是否安装 	版本号:
◎模糊 ◎精确	· 加ェ·
◎通过注册表检查是否安装	· · · · · · · · · · · · · · · · · · ·
	CMD命令:
✐ 温馨提示: 高级设置中的信息均为选填项。	
立即	□上传

瑞星企业终端安全管理系统软件 ©瑞星软件

9. 客户端

9.1 系统托盘

本软件侧重于管理功能,将管理与操作集中于管理控制台和审计控制台。

鼠标右键点击系统托盘 ☑ 图标,可进行【显示主界面】、【设置程序】、【立即升级】、 【退出】等操作。

显示	主界面
设置	程序
立即	l升级
退	出

显示主界面

点击【显示主界面】,包括以瑞星杀毒、漏洞修复、XP 盾为主的各种功能。



设置程序

点击【设置程序】,弹出【操作确认】的弹框,需要输入正确的管理员密码或插入身份 识别器。

👮 操作确认	and a later	X
请输入管理员密码: 或插入身份识别器:		
	确定	取消

验证通过后则可弹出【ESM 配置工具】对话框,在服务控制栏中可以启动/停止服务;

在服务方式中可以更改上级中心的 IP 地址和服务端口。

🧐 ESII配置工具
服务名称 esmep
服务状态 运行中 更新状态(R)
┌服务控制
启动服务(<u>S</u>) 停止服务(<u>0</u>)
_服务方式
服务类型客户端
上级IP地址 192.168.20.95
上级端口号 5555
提示:服务运行中更改信息可能会不成功,且不会立即生效,故建议停止服务 后再做修改。

提示:服务进行中更改信息不会成功或不会立即生效,所以建议停止服务后再做更改。

立即升级

点击【立即升级】后,客户端可升级到最新版本。



退出

点击【退出】后,托盘与主界面退出。若再次启动可从 windows 桌面的快捷方式,或者 在 Windows 画面中,选择【开始】/【程序】/【瑞星企业终端安全管理系统软件】,进行启 动。

9.2 客户端主界面

9.2.1 瑞星杀毒

客户端防病毒为用户提供了杀毒软件客户端主程序,是用户操作防病毒的起始入口。安 装防病毒后,杀毒软件客户端主程序随系统自动启动。用户关闭杀毒主程序后,可通过桌面 图标、开始菜单和双击系统托盘打开主程序。



提示:拖拽杀毒软件客户端主程序,标题栏会自动根据水平位置切换上下部显示;当 主程序界面移出桌面右边界时,将以图标形式隐藏。

9.2.1.1 病毒查杀

点击左上方的 , 切换至病毒查杀功能面板,包括快速查杀、全盘查杀和自定义三项 子功能,可以勾选启用自动处理检测出的病毒和杀毒后自动关机,点击右下角的 可以 选择变频查杀的模式,包括办公模式、自动模式和高速模式。

在扫描过程中,您可以随时点击 12 按钮来暂时停止查杀病毒,点击 12 按钮则继续查

杀,或点击 建按钮停止查杀病毒。

如果需要对某一文件或者某一个文件夹进行杀毒,您可以将该文件或文件夹用鼠标拖入 客户端界面内,此时本软件将自动开始查杀。



查杀结束后显示杀毒结果。

6	× 产品 病暑	品版本: 导库版本	2.0.0 : 25.	. 7 18. 02.	04
V	1 \$	^	×	D	
) 己 デ 未 发	₹成₫ 文现處	₽杀 乾肋	
- 84	余登共 サンサ	·对象:	1994	Ŷ	
	<u></u> 查余共	耗时: 	oo:00 定	:09	
自	定义查测	Ŕ			

【快速查杀】



点击, 启动快速查杀。快速查杀会会扫描您的电脑中特种未知木马、后门、蠕 虫等病毒, 这些病毒易于存在的系统位置, 如内存等关键区域, 查杀速度快, 效率高。通常 利用快速查杀就可以杀掉大多数病毒, 防止病毒发作。



【全盘查杀】

点击,启动全盘查杀。全盘查杀会会扫描您电脑的系统关键区域以及所有磁盘,

全面清除特种未知木马、后门、蠕虫等病毒。



【自定义查杀】



选择扫描位置。自定义查杀会扫描您指定的范围。您可以根据需要确定

查杀目标后进行病毒查杀,此项操作适用于有一定电脑安全知识的用户。



开始杀毒 点击

,启动自定义查杀。

产品版本: 2.0.0. 病毒库版本: 25.1	7 8. 02. 04
Ў 🗲 🗡	
快速查杀 全盘查杀	自定义
0.1%	
正在查杀,请稍候	
扫描对象: 211 个	1. 1. A.
发现威胁: 0 个	
处理威胁: 0 个	
查杀用时: 00:00:25	
查杀速度: 15 个/秒	
□ 自动处理检测出的病毒	A
🔲 杀毒后自动关机	
病毒查杀	

任意扫描完成后显示扫描结果信息。

	产品 病毒	版本: 库版本	2.0.0 3:25.	. 7 18. 02.	.04
	+	†	×		
		已 <u></u> 完 未发	名成者 定现威	£杀 乾胁	
	共查杀河	対象:	1994	个	
	查杀共制	笔时:	00:00	:09	
	ĺ	确	Ē		
自定	义查杀	E.			

点击【确定】返回病毒查杀主页面,包括上次查杀时间、累计查杀病毒数量、引擎版本 和病毒库版本。扫描结果同时上报数据中心。



9.2.1.2 电脑防护

电脑防护可以在您进行打开陌生文件、收发电子邮件、浏览网页等电脑操作时,查杀和 截获病毒,全面保护您的电脑不受病毒侵害。此外,可以阻止恶意程序在本机执行,您还可 以根据自己系统的特殊情况,制定相应的防护规则。

点击,切换至电脑防护功能面板,包括文件监控、系统加固和应用加固三项子功能。 点击监控图标切换开关状态,相应图标显示为一和一。

方子 产品 病毒	版本:2.0.0.7 库版本:25.19.02.02
Y 4	🔶 🗶 📑
文件监控	状态: 已打开 共发现 □ 个病毒 详细设置
系统加固	状态: 已打开 共拦截 ● 个威胁 详细设置
应用加固	状态: 已打开 共拦截 ■ 个威胁 详细设置
电脑防护	

【文件监控】

能实时的监控系统中的文件操作,当您打开文件时,将自动截获和查杀木马、后门、蠕 虫等病毒,全面保护您的电脑不受病毒侵害。

点击^{详细设置},进行文件监控设置,包括:

- 监控模式:所有/智能
- 监控类型:所有/程序及文档
- 查杀引擎:

仅查杀流行病毒、启发式查杀、启用压缩包查杀及查杀压缩包容量上限

1) 仅查杀流行病毒:重点查杀近年来互联网的活跃病毒(建议开启)。

2) 启发式查杀: 启发式查杀可以识别可能是病毒或木马的文件, 启用可提高杀毒效率。

3) 启用压缩包查杀: 启用后将查杀压缩包内的文件及查杀压缩包容量上限。

- 发现病毒处理方式:自动处理/通知我
- 病毒清除成功后:开启/关闭通知我
- 多引擎设置: 传统引擎/开启云引擎

设置完成后,点击^{应用}设置成功,返回电脑防护面板;点击^{取消}恢复上次设置, 返回电脑防护面板。



【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。



- 拦截到威胁处理方式:提示我/自动处理
- 拦截日志:记录/不记录
- 监控灵敏度:由用户根据系统情况自由选择,低/中/高三个等级
- 审计模式:开启/不选开启项
- 其他:开启/关闭放过带数字签名的程序

系统加固设置	系统加固设置
拦截到威胁时:	◎记录
●提示我	◎不记录
◎不提示	监控灵敏度:
拦截日志:	◎低
●记录	● 中
◎不记录	
监控灵敏度:	审计模式:
◎低	一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一
• 中	其它:
◎高	☑放过带数字签名的程序
审计模式:	
	法田田 小男 一一田 田 米
使用默认设立	使用默认设置 四田 取消

置,返回电脑防护面板。

【应用加固】

点击 详细设置 ,进行应用加固设置,包括:

- 拦截到威胁时:允许运行/拒绝运行
- 拦截到威胁时:提示我/自动处理
- 拦截日志:记录/不记录
- 被保护的软件启动时:弹出保护框/不弹保护框

▲ 已连接瑞星云安全中心! 产品版本: 2.0.0.7	
🧶 🤸 🛧 🖉 🚍	
应用加固设置	
拦截到威胁时:	
◎允许运行	
 拒绝运行 	
拦截到威胁时:	
◎ 提示我	
◎自动处理	
拦截日志:	
●记录	
被保护的软件启动时:	
使用款以收益 型用 取用	
电脑防护	
	The Asia

设置完成后,点击^{______}设置成功,返回电脑防护页面;点击^{______}恢复上次设置,返回电脑防护页面。

提示:每个设置页面都可以选择使用默认设置。

9.2.1.3 设置中心

点击 ※, 切换至设置中心面板,包括常规项和查杀病毒两个设置页面。

1. 设置中心——常规项

常规项设置,包括:

• 白名单编辑:通过文件/目录和文件后缀两种方式进行白名单管理。

文件/目录:可点击 • ,从目录+子目录、目录、子目录和文件添加白名单。

文件后缀:可点击 •,添加白名单。

提示:加入到白名单的进程、文件和目录等在扫描和实时防护时将被自动跳过。

产品版本: 2.0.0.7 病毒库版本: 25.18.02.04 ★ ↑ ※ □ 言	产品版本: 2.0.0.7 病毒库版本: 25.18.02.04 チ ケ メ
常规项 > 添加白名单	常规项 > 添加白名单
文件/目录 文件后缀 ● ● 暫无记录 ●	文件/目录 文件后缀
	注·本 圣民收纳物团的白夕的古家
注: 宣余及监控将忽略日名单内容 应用 取消	注:查示及监控将忽略日名单内容 应用 取消

设置完成后,点击 型用 设置成功,返回常规项面板;点击 ^{取消}恢复上次设置, 返回常规项面板。

● 云服务编辑:管理公有云启用状态和私有云配置信息。可点击 添加私有云记录。



设置完成后,点击^{应用}设置成功,返回常规项面板;点击^{取消}恢复上次设置, 返回常规项面板。

恢复区

- 备份文件: 启动/关闭杀毒时备份原文件
- 恢复区空间不足时的处理方式: 自动覆盖老文件/空间自动增长
- 隔离失败时的处理方式: 询问我/删除文件/不处理
- 备份文件超过 100M 时的处理方式: 询问我/删除文件/不处理

设置完成后,点击 应用 设置成功;点击 取消 恢复上次设置。

- 病毒跟踪:开启/关闭病毒跟踪
- 病毒日志:记录病毒日志

 ◇已连接瑞星云安全中心! 产品版本: 2.0.0.7 ケ 介 ※ □ 言 	 ◆ 已连接瑞星云安全中心! 产品版本: 2.0.0.7 チ テ ※ □ 言
常规项 查杀病毒 白名单:编辑 云服务:编辑 恢复区 备份文件 ④余毒时备份原文件 恢复区空间不足时的处理方式 ●自动覆盖老文件 ●空间自动增长 隔离失败时的处理方式 ●询问我	常规项 查杀病毒 PMAGACHURHUD JULIE/JILA ④ 询问我 ④ 研除文件 ④ 不处理 备份文件超过100M时的处理方式 ④ 询问我 ④ 删除文件 ④ 不处理 病毒跟踪 病毒日志 ④ 记录病毒日志
使用默认设置 应用 取消 设置中心	使用默认设置 应用 取消 设置中心

2. 设置中心——查杀病毒

查杀病毒设置,包括:

- 查杀文件类型:所有/程序及文档
- 查杀引擎: 仅查杀流行病毒、启发式查杀、启用压缩包查杀及查杀压缩包容量上限
- 发现病毒处理方式: 自动处理/手动处理
- 多引擎设置:传统引擎、开启云引擎



9.2.1.4 日志系统

杀毒日志功能可以让用户查看病毒详情、扫描事件、系统加固和应用加固的详细信息以 及处理结果等。



日志						Ŀ	- □ >
病毒详情	3描事件	系统加固	应用加固				
							刷新 (F5
按时间: 今天 、	, 按发现源:	全部 ▼	按处理方式:	全部	•		记录数: 《
时间	文件路径		病毒	名称		威胁类型	处理结果
2014-06-24 10:47:26	D:\病毒\ELF(1)\ELF\694688 M	httpd Virl		自定义查杀	病毒	删除成功
2014-06-24 10:47:26	D:\病毒\ELF(1)\ELF\695268_V	irTo Virl	00	自定义查杀	病毒	删除成功
2014-06-24 10:47:26	D:\病毒\ELF(1)\ELF\695269_V	irTo Virl	00	自定义查杀	病毒	删除成功
2014-06-24 10:47:26	D:\病毒\ELF(1)\ELF\695494_d	dos Hack	c. D	自定义查杀	病毒	删除成功
2014-06-24 10:47:26	D:\病毒\ELF(1)\ELF\696279_E	xplo Expl	.oi	自定义查杀	病毒	删除成功
2014-06-24 10:47:26	D:\病毒\ELF(1)\ELF\696280_E	xplo Expl	.oi	自定义查杀	病毒	删除成功
2014-06-24 10:47:26	D:\病毒\ELF(1)\ELF\696381_H	ack Hack	c. E	自定义查杀	病毒	删除成功
2014-06-24 10:47:26	D:\病毒\ELF(1)\ELF\696501_J	unk Juni	c. L	自定义查杀	病毒	删除成功
2014-06-24 10:47:26	D:\病毒\ELF(1)\ELF\696510_J	unk Juni	c. L	自定义查杀	病毒	删除成功
2014-06-24 10:47:26	D:\病毒\ELF(1)\ELF\696596_L	.inux Linu	1x [自定义查杀	病毒	删除成功
2014-06-24 10:47:26	D:\病毒\ELF(1)\ELF\696597_L	.inux Linu	1x [自定义查杀	病毒	删除成功
2014-06-24 10:47:26	D:\病毒\ELF(1)\ELF\696961_T	roja Troj	an	自定义查杀	木马	删除成功
2014-06-24 10:47:26	D:\病毒\ELF(1)\ELF\697305_W	orm Worm	.L	自定义查杀	蠕虫	删除成功
2014-06-24 10:47:26	D:\病毒\ELF(1)\ELF\697306_W	orm Worn	.L	自定义查杀	蠕虫	删除成功
2014-06-24 10:47:26	D:\病毒\ELF(1)\ELF\697314_W	orm Worm	.L	自定义查杀	蠕虫	删除成功
2014-06-24 10:47:26	D:\病毒\ELF(1)\ELF\697318_W	orm Worm	.L	自定义查杀	蠕虫	删除成功
2014-06-24 10:47:26	D:\病毒\ELF(1)\ELF\697319_W	orm Worm	.L	自定义查杀	蠕虫	删除成功
2014-06-24 10:47:26	D:\病毒\ELF(1)\ELF\697320_W	orm Worm	.L	自定义查杀	蠕虫	删除成功
<	* 1.÷±1***			• •	4,44,00 ,945 %	나큐 그	nndn∧ -P-+L ∮

病毒详情

在病毒详情页面,用户可以查看到杀毒软件扫描或者监控到的所有病毒信息,包括扫描 或监控到的时间、文件路径、病毒名称、发现源、威胁类型和处理结果等。

可以按时间、发现源和处理方式对扫描或监控到的病毒进行筛选。按时间筛选分为全部、 今天、最近三天、最近一周和最近一个月。按发现源筛选分为全部、快速查杀、全盘查杀、 自定义查杀、文件监控、邮件监控和 U 盘查杀。按处理方式筛选分为全部、暂未处理、忽 略、删除、清除、信任和上报。可以点击页面右上角的^{刷新 (P5)}或 F5 键对信息进行刷新操 作。

扫描事件

点击 **扫描事件**,进入扫描事件页面,本页面记录了杀毒软件的扫描、保护等事件 记录。

김〉///《 法法室瑞星企业终端安全管理系统软件用户手册

日志				5		Ŀ	- 🗆 X
病毒详情	扫描事件	系统加固	应用加	固			
记录了杀毒软件的扫	描、保护等事件。						[刷新 (F5)
按时间: 今天	▼ 按发现源:	全部	•				记录数:
时间	发现源	共扫描	扫描用时	发现威胁	已处理	状态	
2014-06-24 10:47:	28 自定义查杀	60	00:00:13	27	27	任务结束	
2014-06-24 10:41:	13 自定义查杀	21	00:00:13	13	13	任务结束	

在扫描事件页面详细的记录了包括时间、发现源、共扫描、扫描时间、发现威胁、已处 理和状态等。可以按时间和发现源对记录进行筛选。按时间筛选分为全部、今天、最近三天、 最近一周和最近一个月。按发现源筛选分为全部、快速查杀、全盘查杀、自定义查杀、文件 监控和邮件监控。可以点击页面右上角的^{刷新(P5)}或 F5 键对信息进行刷新操作。

系统加固

点击 系统加固 ,进入系统加固页面,本页面记录了系统防护的相关事件

日志				— — X
病毒详情	田海牛	系统加固应用加固		
记录了系统防护的相关到	事件。			[刷新 (F5)
按时间: 今天 ·	▼ 按防护类	型: 全部 🔻		记录数: 11
时间	处理结果	事件	来源	目标
2014-06-24 10:45:11	拒绝	RUNLUA. EXE试图修改MS-DOS应用	C:\users\1\desktop\r	Hkey classes
2014-06-24 10:45:11	拒绝	RUNLUA. EXE试图修改MS-DOS应用	C:\users\1\desktop\r	Hkey_classes
2014-06-24 10:45:11	拒绝	RUNLUA. EXE试图修改应用程序(C:\users\1\desktop\r	Hkey_classes
2014-06-24 10:45:11	拒绝	RUNLUA. EXE试图修改应用程序(C:\users\1\desktop\r	Hkey_classes
2014-06-24 10:45:10	拒绝	RUNLUA. EXE试图修改Windows批	C:\users\1\desktop\r	Hkey_classes
2014-06-24 10:45:10	拒绝	RUNLUA.EXE试图修改Windows批	C:\users\1\desktop\r	Hkey_classes
2014-06-24 10:45:10	拒绝	RUNLUA. EXE试图修改屏幕保护程	C:\users\1\desktop\r	Hkey_classes
2014-06-24 10:45:10	拒绝	RUNLUA. EXE试图修改屏幕保护程	C:\users\1\desktop\r	Hkey_classes
2014-06-24 10:45:09	拒绝	RUNLUA.EXE试图修改Windows命	C:\users\1\desktop\r	Hkey_classes
2014-06-24 10:45:08	拒绝	RUNLUA.EXE试图修改Windows命	C:\users\1\desktop\r	Hkey_classes
2014-06-24 10:43:43	拒绝	RUNLUA.EXE试图操作hosts文件	C:\users\1\desktop\r	C:\windows\s

在系统加固页面详细的记录了包括时间、处理结果、事件、来源和目标等。可以按时间 和防护类型进行筛选。按时间筛选分为全部、今天、最近三天、最近一周和最近一个月。按 防护类型筛选分为全部、文件防护、注册表防护、进程防护和系统防护。可以点击页面右上

角的^{刷新 (F5)}或 F5 键对信息进行刷新操作。

应用加固

点击 应用加固 ,进入应用加固页面,本页面记录了常用应用程序防护的相关事件

日志				-	
病毒详情	日描事件	系统加固 应用加固			
记录了常用应用程序防护	户的相关事件	•			刷新(175)
按时间: 全部	▼ 按应用类	型: 全部 ▼			记录数 : 8
时间	程序类型	来源	操作	目标	补充信息
2014-06-19 20:12:00	浏览器	C:\Program Files\Micro	以写	C:\Program Files\Mic	啊威
2014-06-19 20:12:00	浏览器	C:\Program Files\Micro	以写	C:\Program Files\Mic	啊威
2014-06-19 20:12:00	浏览器	C:\Program Files\Micro	以写	C:\Program Files\Mic	啊威
2014-06-19 17:18:00	浏览器	C:\Program Files\Micro	以写	C:\Program Files\Mic	啊威
2014-06-18 10:18:00	浏览器	C:\Program Files\Micro	改写	C:\Program Files\Mic	啊威
2014-06-18 09:18:00	浏览器	C:\Program Files\Micro	改写	C:\Program Files\Mic	啊威
2014-06-16 16:08:00	办公软件	c:\windows\ie.exe	运行	c:\windows\ie.exe	啊威
2014-06-16 16:08:00	办公软件	c:\windows\ie.exe	运行	c:\windows\ie.exe	啊威

在应用加固页面详细的记录了包括时间、程序类型、来源、操作、目标和补充信息等。 可以按时间和应用类型进行筛选。按时间筛选分为全部、今天、最近三天、最近一周和最近 一个月。按应用类型筛选分为全部、浏览器和办公软件。可以点击页面右上角的^{刷新 (P5)}或 F5 键对信息进行刷新操作。

9.2.1.5 更多功能

9.2.1.5.1 隔离区



隔离区保存了在杀毒操作中被删除文件的备份,勾选文件后可以进行恢复到原始位置、 恢复到指定位置和删除操作。在文件较多时,可以通过文件名称的关键字搜索,精确定位到 具体文件。

ጓ▷ INC I # 2 瑞星企业终端安全管理系统软件用户手册

2件搜索:	查看	刷新(F5)
目标文件	病毒名称	处理时间
D:\TOOLS\virus\Minitest2008-800619\Mem	Worm. Win32. Nimda. a	2012-11-07 03:09
□ D:\\WORK\2010虎年工作文档\卡卡7\virus\33	Trojan. Win32. Generic. 11E85758	2012-11-07 02:52
D:\TOOLS\virus\Minitest2008-800619\Vot	Script.Redlof.htm.Head	2012-11-07 03:11
C:\USERS\HUANGQI\DESKTOP\VIRTEST_CLEA	Npox. 1010	2012-11-13 11:14
D:\TOOLS\virus\Minitest2008-800619\Vot	Worm.LovGate	2012-11-07 03:11
D:\TOOLS\virus\Minitest2008-800619\Vot	Win32.Xorala	2012-11-07 03:11
D:\TOOLS\virus\Minitest2008-800619\rea	Win32.FunLove	2012-11-07 03:10
D:\TOOLS\virus\Minitest2008-800619\Mem	Win32.Mincer	2012-11-07 03:09
D:\TOOLS\virus\Minitest2008-800619\Vot	Worm.Bugbear.b	2012-11-07 03:11
D:\TOOLS\virus\Minitest2008-800619\rea	Trojan. Win32. Generic. 122BCA30	2012-11-07 03:10
□ D:\\WORK\2010虎年工作文档\卡卡7\virus\33	Trojan.Win32.Generic.11EB554C	2012-11-07 02:52
■ D:\TOOLS\tool\zolxk\显卡\NV_65.52_2KXP	Dropper.Win32.Xema.a	2012-11-07 03:06
C:\USERS\HUANGQI\DESKTOP\VIRTEST\DELVI	Dropper.Glacier60	2012-11-13 11:14
D:\TOOLS\virus\Minitest2008-800619\Vot	Win32.Klez	2012-11-07 03:10
D:\TOOLS\virus\Minitest2008-800619\Vot	Worm.Klez.co	2012-11-07 03:10
□ D:\\WORK\2010虑年干作文档\卡卡7\virus\33	Trojan.Win32.Generic.11F078CC	2012-11-07 02:52

9.2.1.5.2 使用教程



中选择【使用教程】会弹出一个简单的使用教

程,可按照教程提示操作。



9.2.1.5.3 更多功能



展功能。



9.2.2 漏洞修复

扫描当前系统存在的漏洞,包括漏洞级别和漏洞大小等,用户可以有选择性的进行漏洞 修复。产品还提供完善的漏洞补丁库,保证扫描到的每一个补丁都能够顺利的安装。



立即修复



在漏洞修复界面用户可以勾选需要修复的漏洞,点击

被勾选的漏洞就会显示正在修复或待修复的修复状态。漏洞修复完成后就会在页面上消失。

瑞星企业终端安全	全管理系统软件 및 ¹¹¹	✔ 全选	A	- ×
KB2900986 🖌 🖌 KB13-090 - 严重 Activ 大小: 505 2 XB	KB2727528 🖌 MS12-072 - 严重 Windo 侍修复 大小:519.5 KB	KE9971557	>	K
KB2723135 ✔ MS12-053 - 严重 远程 特修复 大小:560 0 KB	KB2893294 ✓ MS13-098 - 严重 Windo	KB2876331 ✔ MS13-089 - 严重 Windo 符修复 大小:632.2 KB	立即 共检测出漏 其中19个高	<mark>修复</mark> 訥42个 玩流漏洞
KB2653956 ✔ MS12-024 - 严重 Windo 待修复	KB2712808 ✔ MS12-054 - 严重 Windo 待修复	KB2847311 	Q. 重新扫描	● 忽略漏洞
大小: 633.4 KB KB960803	大小:643.3 KB KB2850869 ✔ MS13-060 - 严重 Unico	大小:644.1 KB KB2705219	漏洞情况	补丁管理

补丁管理



在补丁管理界面查看到已安装或已忽略的补丁。



重新扫描

北京瑞星信息技术有限公司



用户可以在漏洞情况页面查看到近三个月修复漏洞的总次数,以及当天修复的漏洞数。 点击右侧的【打开补丁目录】按钮,可以查看到下载到本地的补丁目录。

ጓ▷ INC 這是瑞星企业终端安全管理系统软件用户手册

🤁 nat ch							
文件(の) 編号(の) 杏吾(の)	收費(4) 工具(4) 帮助(4)						
				~			
🕞 后退 🔹 🌍 🔹 🏂 🍃	▶ 搜索 խ 文件夹 🛄 -						
地址 (D) C:\Program Files\Riging\FSM\rls\natch							
		大小 类型	修改日期				
文件和文件夹任务	If indowsXP-KB960803-x86-CHS	657 KB 应用程序	2014-6-26 17:02				
	WindowsXP-KB971557-x86-CHS	524 KB 应用程序	2014-6-26 17:02				
🧭 创建一个新文件夹	WindowsXP-KB2653956-x86	634 KB 应用程序	2014-6-26 17:02				
🔹 🔕 将这个文件夹发布到	WindowsXP-KB2705219-v2	672 KB 应用程序	2014-6-26 17:03				
→ 土支計文件本	WindowsXP-KB2712808-x86	644 KB 应用程序	2014-6-26 17:02				
	WindowsXP-KB2723135-v2	561 KB 应用程序	2014-6-26 17:02				
	WindowsXP-KB2727528-x86	520 KB 应用程序	2014-6-26 17:02				
其它位置	WindowsXP-KB2834886-x86	1,291 KB 应用程序	2014-6-26 17:03				
	WindowsXP-KB2835364-x86	1,121 KB 应用程序	2014-6-26 17:03				
🛅 rls	WindowsXP-KB2876217-x86	1,045 KB 应用程序	2014-6-26 17:03				
🗧 🔒 我的文档	WindowsXP-KB2876331-x86	633 KB 应用程序	2014-6-26 17:02				
📄 六字文档	WindowsXP-KB2893294-x86	572 KB 应用程序	2014-6-26 17:02				
😡 我的电脑	WindowsXP-KB2900986-x86	506 KB 应用程序	2014-6-26 17:02				
◎ 网上邻居	WindowsXP-KB2929961-x86	723 KB 应用程序	2014-6-26 17:03				
G LITTAND	WindowsXP-KB2964358-x86	1,792 KB 应用程序	2014-6-26 17:03				
详细信息	*						
	_						
15 个对象			11.6 MB 🛛 😏 我的电脑				

9.2.3 XP 盾

XP 盾支持热补丁实时监控、漏洞免疫、发生攻击主动提醒和记录漏洞攻击日志等功能。



北京瑞星信息技术有限公司

9.2.3.1 热补丁实时监控

热补丁实时监控功能是针对具体漏洞,软件运行时内存中动态修补。

9.2.3.2 漏洞免疫

漏洞免疫功能是根据漏洞的共性,运行通用行为拦截,阻断漏洞攻击。

9.2.3.3 发生攻击主动提醒

开启该功能,当您的系统遭受了漏洞攻击时,瑞星企业终端安全管理系统会主动发出提 醒信息。

9.2.3.4 记录漏洞攻击日志

开启该功能,在界面左侧将展示近一月漏洞攻击走势及日志。



9.2.3.5 白名单设置

在 XP 盾首页点击 一天 , 进入白名单设置界面。



如果您还没有设置白名单,可以点击 ①进行设置。



在对话框中输入要加入白名单的程序名称即可。


9.2.4 其他功能

9.2.4.1 杀毒日志

参考 <u>9.2.1.4 日志系统</u>。

9.2.4.2 隔离中心

隔离中心保存了杀毒操作中被删除的文件的备份,用户可以将这些文件恢复到指定的位置。



RISING 瑞星瑞星企业终端安全管理系统软件用户手册

🕏 瑞星隔离中心				
文件隔离区中保存了	杀毒操作中被删除的文件的备份,	您可以将这些文件恢复到指题	定位置	
文件搜索:		查看	·	刷新(F5)
文件名	目标文件	病毒名称	隔离时间	大小
📃 KEYGEN. EXE	C:\DOCUMENTS AND SE	Trojan. Win32.Generi	2014-06-18 16:14	160 KB
📃 atl.job	C:\WINDOWS\tasks\at	未知病毒	2014-06-24 12:00	288 字节
□ 全部选择		恢复到原始位置	x复到指定位置	删除所选

隔离中心详细记录了被隔离文件的文件名、目标文件、病毒名称、隔离时间和大小等信息。用户可以在文件搜索的搜索框内输入信息,对隔离文件的各个字段进行模糊查询。输入 搜索信息后,点击 查看 即可展示出符合搜索条件的信息。可以点击页面右上角的 刷新(F5) 或 F5 键对信息进行刷新操作。

可以对隔离文件进行恢复和删除操作。选择一条或多条文件,点击 恢复到原始位置, 可以将文件恢复到原始位置。恢复前可以选择替换、全部替换、不替换、全部不替换、另存 为中的一种。

	确认文件替换 🛛 🔀
	文件 C:\DOCUMENTS AND SETTINGS\ADMINISTRATOR\桌面 \VMWARE9\DOWNLOAD\VMWARE-WORKSTATION_MYHACK58\VI 注册机\KEYGEN.EXE 已经存在.
	您是否确定替换已经存在的这个文件 大小:163840 最后修改时间:2012-8-23 13:24:33 替换后的文件?
	大小:163840 最后修改时间:2012-8-23 13:24:33 诸按 取消 放弃这个路径并选择另外一个.
选择	一条或多条文件,点击 恢复到指定位置 ,可以将文件恢复到指定位置

北京瑞星信息技术有限公司

保存在①: 予約文档 ○ ② ② ○ □ □ Wy KIX Files RIXC File List 図片收藏 予約音乐 ジェの ③ 約 音乐
 Wy RIX Files RIXC File List 图片收藏 我的音乐
我的文档 我的电脑
我的电脑
文件名 (II): KEY GEN ✔ 保存 (S) 保存类型 (II): 取消
选择一条或多条文件,点击 删除所选 ,可以将文件删除。删除前,系统会弹
出确认对话框,点击 是 2 则删除文件,点击 图 则取消删除操作。
确认文件删除 🛛
您是否确认删除此项

9.2.4.3 引导区工具

引导区工具可以帮助用户备份或者恢复引导区数据的功能。



😽 引导区工具	
引导区安全工具	V
使用安全工具可以帮助你备份或者恢复引导区数据	
◉ 备份引导区	
◎ 恢复引导区	
下一步	取消

.

备份引导区

选择"行	备份引导区后",点击 <mark>——下一步</mark> ,可以选择引导区备份的路径。
8	引导区工具 📃 🗖 🔀
	引导区安全工具
	准备引导区备份
路径选择	择完成后,点击即可完成备份,备份成功后,页面会弹出备份成功
的提示信息。	。点击 即可取消当前备份操作。
	提示信息 ↓ 备份成功! 「 猫定」
恢复引导区	

当系统引导区损坏时,可以对引导区进行恢复操作。选择"恢复引导区",点击

下一步,再选择好之前备份文件的路径。

	🖁 引导区工具	
	引导区安全工具	T
	准备恢复引导区	
	选择目录 C:\Program Files\Rising\ESM\xav\bootdat	浏览
		取消
路径进	择完成后,点击 确定 即可完成恢复,恢复成功/	后,页面会弹出恢复成功
的提示信息	1.。点击 取消 即可取消当前恢复操作。	
	提示信息 23 依复成功! 确定	

9.2.4.4 电脑修复

通过对系统的扫描,检测出电脑是否有危险项,且对危险项进行修复,也可以对扫描项 进行信任设置等功能。



RISING 瑞星瑞星企业终端安全管理系统软件用户手册

电脑修复				×	
系统扫描完成!共发现 1 个危险项,	建议您 立刻修复		已信任	(0)	
■ 检测项目		安全级别	修复方法	^	
📄 修复IE被禁用功能 (扫描完成,发现 2 处异常项)	修复IE被禁	用功能			
IE主页相关注册表权限可能被恶意软件修改	详情	未知	恢复默认		
IE主页相关注册表权限可能被恶意软件修改	详情	未知	恢复默认		
📝 系统相关项 (扫描完成,发现 1 处异常项)	修复系统的	安全隐患			
📝 windows文件保护功能	详情	危险	恢复默认		
🔄 桌面图标 (扫描完成,未发现异常项)	修复与"我的	修复与"我的电脑""网上邻居"等相关的注册表数据			
🔄 修复桌面NameSpace (扫描完成,未发现异常项)	修复桌面N	ameSpace,剔除假冒的	IE图标和恶意广告链…		
🦳 修复旧图标 (扫描完成,未发现异常项)	清除修复IE	图标,确保IE的相关功能	正常	_	
📃 清除桌面恶意快捷方式 (扫描完成,未发现异常项)	清除指向网	耻的快捷方式图标			
🔄 扫描快速启动栏中的恶意网址 (扫描完成,未发现异	:常项) 清除快速启	动栏中的恶意网址			
🔄 扫描开始菜单中的恶意网址 (扫描完成,未发现异常	项) 清除开始菜	《单中的恶意网址			
🔄 修复旧扩展按钮 (扫描完成,未发现异常项)	清除IE工具	.栏中的扩展按钮,加速IE	的启动速度		
🔄 修复About页面 (扫描完成,未发现异常项)	修复对系统	在 在 了 的 about:blank等的 题	懸意修改		
	^/× /=+++>+++		014 7.71	*	

如果发现有危险项,可以点击 立刻修复 进行修复。点击 **重新扫描**,则可以对系统进行再次扫描。

勾选检测项目,点击^{设为信任},以后进行检测此项目则不会被判断为危险项。信任后, 在"电脑修复"界面的右上角,点击 已信任(1)即可以查看信任项。也可以勾选已信任项, 点击 现消信任 进行取消。

北京瑞星信息技术有限公司

引入INC 诺尼瑞星企业终端安全管理系统软件用户手册

已信任項列表		×
前有已信任的项均记录在此,您可以随时取消对它们的	的信任。	
☑ 异常项名称	所属分类	添加时间
☑ IE主页相关注册表权限可能被恶意软件修改	修复IE被禁用功能	2014-06-24 10:45
取消信任		

在"电脑修复"界面勾选一个检测项目后,点击详情,可以查看此检测项目的详情。

項目详情	×
详情	
 一描述 路径: MACHINE\SOFTWARE\Microsoft\Internet Explorer\MAIN ⅡE主页相关注册表权限可能被恶意软件修改 	
一目前异常状况 注册表键值为 键值权限被修改	
一正常时 注册表键值为 默认完全控制权限	

9.2.4.5 开机优化

系统具有专门进行开机优化的功能,让您的开机速度飞起来。开机优化分为一键加速、

启动项和服务、优化记录三部分。

在主界面点击<mark> ^{开机}优化</mark>

进入优化开机界面。

икла	ØL						×
一一键	加速	启动项和服务	优化记录				
发现:	5个可优化	比項,您可以通过一键 ;	加速立即优化,加	快电脑开机速度。		一键加速	
		Computer Browser(2 用于为其他计算机提供在	E线计算机列表服 E线计算机列表查询	务器) 开机自启动 服务,不需要开机启动,	如…		
		Mindows Firewall/Inter 用于启用家庭网络共享和	net Connection S 响防火墙功能,不需	haring (因特网联机共 国 要开机启动。	ž		
		System Restore Servic 用于支持系统的备份还易	2 8(系统还原服务 取能,不需要开机	〕 开机自启动 启动。			
		Distributed Link Tracki 用于NTFS格式文件系统	ng Client(分布 式 上文件关联的跟踪	链接跟踪客户端) 开 维护,保证在文件移动。	枕 言		
		WebClient(Web客户) 用于提供其他计算机直接	嵩服务) 开机自动问本地文件的功	启动 能,可以禁止。			

一键加速

在一键加速界面,列出系统能分析出的本机可优化项目。选中列表中的项目后,点击右 上角的 — 建加速 即可一键关闭这些开机启动项。

启动项和服务

也可以切换到"启动项和服务"标签页,手动关闭多余的启动项。点击"启动项和服务" 标签,进入启动项和服务页面,启动项和服务包括启动项、计划任务、应用软件服务和系统 关键服务。每一项分别有各自的项目列表,都可以手动进行启动与否的操作。点击每一项右

侧的 禁止启动 按钮,即可将其关闭;点击 恢复启动,即可恢复启动。

在关闭任何启动项之前,建议大家认真阅读界面给每一项标注的功能说明,明确了解这 些启动项的作用后,再选择是否将其关闭。因为如果关了不该关闭的启动项,有可能使电脑 无法正常使用。

引入INC 诺尼瑞星企业终端安全管理系统软件用户手册

优化开机	bt.					-	×
一键	加速	启动项和服务	优化记录				
启动项	[(2) i	┼划任务(3) 应用软	件服务(87) 系统	焼关键服务(0)			
🕕 છ	下启动项	不是系统必备,开启过剩	多会拖慢开机速度。				^
	Alerter 用于将 [,]	(警报服务) "硬盘即将写满"等警告	通知给网络管理员…	建议禁止	已禁用	恢复启动	
	Applica 用于启ā	tion Layer Gateway Se 协防火墙插件支持和Win	e rvice(应用层网… dows网络连接共享…	建议禁止	已禁用	恢复启动	
	Applica 用于支持	tion Management (程 持在大型企业环境下集中	序集中管理服务) 管理软件的功能,…	建议禁止	已禁用	恢复启动	
	Comput 用于为其	t er Browser(在线计 【他计算机提供在线计算	拿机列表服务器) 和列表查询服务,…	建议禁止	已开启	禁止启动	
	Indexin 用于在原	g Service(文件搜索 音合建立磁盘文件的索引	转引服务) 以提高搜索速度,…	建议禁止	已禁用	恢复启动	
<u>)</u>	ClipBoo 用于在其	k(剪贴板查看器服务 其他电脑上共享剪切板里) 的信息,不需要开…	建议禁止	已禁用	恢复启动	*

优化记录

点击"优化记录"标签,进入优化记录页面,可以查看到已禁用的开机启动项,可以通

过点击每项右侧的恢复启动将其恢复。			
优化开机		-	×
一键加速 启动项和服务 优化记录			
共禁止启动: 5 項。这里记录了已禁用的开机启动项,您可以查看或恢复它们。			
1 2014年06月24日			
WebClient (Web客户端服务) 用于提供其他计算机直接访问本地文件的功能,可以禁止。	已禁用	恢复启动	
Distributed Link Tracking Client (分布式链接跟踪客户端) 用于NTFS格式文件系统上文件关联的跟踪、维护,保证在文件移动后仍然	已禁用	恢复启动	
System Restore Service(系统还原服务) 用于支持系统的备份还原功能,不需要开机启动。	已禁用	恢复启动	
Windows Firewall/Internet Connection Sharing (因特网联机共享和防 用于启用家庭网络共享和防火墙功能,不需要开机启动。	已禁用	恢复启动	
Computer Browser (在线计算机列表服务器) 用于为其他计算机提供在线计算机列表查询服务,不需要开机启动,如果	已禁用	恢复启动	

9.2.4.6 进程管理

进程管理可以查看和管理电脑当前正在运行的进程以及联网情况,一目了然,让用户更 方便的管理进程。进程的信息包括进程名称、安全级别、内存占用、网络流量、网络连接和 操作。



在主界面点击^{进村}

,进入进程管理界面。

进程管理					- 🗆	×
目前电脑中共有 31 个进程正在运行,其中	7 个正在联网	퀵-		I	🛛 仅查看联网)	进程
进程名称 🔨	安全级别	内存占用	网络流量	网络连接	操作	^
ATI External Event Utility EXE Module	未知	3.5 MB	下載 O KB/s 上传 O KB/s	0	结束进程	
ATI External Event Utility EXE Module	未知	4.4 MB	下载 O KB/s 上传 O KB/s	0	结束进程	
ATI External Event Utility EXE Module	未知	4.4 MB	下载 O KB/s 上传 O KB/s	0	结束进程	
Client Server Runtime Process	未知	5.6 MB	下载 O KB/s 上传 O KB/s	0	结束进程	
Client Server Runtime Process	未知	3.6 MB	下载 O KB/s 上传 O KB/s	0	结束进程	
CTF Loader	未知	6.2 MB	下载 O KB/s 上传 O KB/s	0	结束进程	
epsrv.exe (2236) 服务进程	安全	15.1 MB	下載 O KB/s 上传 O KB/s	0	结束进程	
eptray.exe (1428)	安全	28.2 MB	下载 O KB/s 上传 O KB/s	0	结束进程	~
☑ 自动刷新进程信息 查看当前	†进程DLL					

系统默认设置为自动刷新进程信息,可以通过勾选页面左下角的"自动刷新进程信息" 来取消自动刷新功能。可以对进程名称、安全级别和内存占用排序,只需点击这三项的表头 文字即可。

用户可以根据实际情况,点击进程右侧的^{结束进程}来结束这一进程,系统会弹出确 认对话框,用户点击^{确定},则进程结束,用户点击^{取消},则进程继续执行。 进程结束后,则该进程在此列表消失。



如果只想查看联网进程,则勾选进程管理界面右上角的 2 仅查看联网进程即可。用户还可以通过点击进程管理下面的 查看当前进程DLL来查看当前进程 DLL。查看完毕后点击 隐藏当前进程DLL进行隐藏。

进程管理						– 🗆 X
目前电脑中共有 30	个进程正在运行,其中	7 个正在联网	9.			📄 仅查看联网进程
进利	呈名称 🔨	安全级别	内存占用	网络流量	网络连挂	き 操作 🔷
ATI External Ev	944) vent Utility EXE Module	未知	3.5 MB	下載 0 KB/s 上传	OKB/S O	结束进程
ATI External Ev	1520) vent Utility EXE Module	未知	4.4 MB	下载 0 KB/s 上传	OKB/S O	结束进程
ATI External Ev	3604) /ent Utility EXE Module	未知	4.4 MB	下载 0 KB/s 上传	OKB/S O	结束进程
csrss.exe (70	4)	+ **				
名称	路径			描述	公司	版本 🔷
Ati2evxx.exe	C:\WINDOWS\system3	2VAti2evxx.e	ATI Externa	I Event Utility EXE	ATI Technologies	s I 06.14.10.42 😑
ntdll.dll	C:\WINDOWS\system3	2\ntdll.dll	NT Layer D	LL	Microsoft Corpora	ati 05.01.2600 🗕
kernel32.dll	C:\WINDOWS\system3	2\kernel32	Windows N	IT BASE API Client	Microsoft Corpora	ati 05.01.2600
USER32.dll	C:\WINDOWS\system3	2\USER32	Windows X	P USER API Clien	Microsoft Corpora	ati 05.01.2600
GDI32.dll	C:\WINDOWS\system3	2\GDI32.dll	GDI Client I	DLL	Microsoft Corpora	ati 05.01.2600
ole32.dll	C:\WINDOWS\system3	2\ole32.dll	Microsoft O	LE for Windows	Microsoft Corpora	ati 05.01.2600
ADVAPI32.dll	C:\WINDOWS\system3	2VADVAPI3	Advanced V	Vindows 32 Base	Microsoft Corpora	ati 05.01.2600
RECETA VII	CHIMINDOM/Qlevetom?	2) RPORTA	Remote Pri	ncedure Call Runti	Microsoft Corpor	əti 05.01.2600 ≚
☑ 自动刷新进程信息	隐藏当词	前进程DLL				

9.2.4.7 右键菜单管理

右键菜单管理功能可以对右键菜单的显示项进行设置,包括文件右键菜单和 IE 右键菜单。



在主界面点击<mark>右键菜单管理</mark>,进入右键菜单管理界面,系统默认显示文件右键菜

单设置界面。

一次一次一次一次一次一次一次一次一次一次一次一次一次一次一次一次一次一次一次	– X
文件右键菜单 IE右键菜单	
选中要在文件或者文件夹中显示的右锁	建菜单项
▲ 名称	类型
☑ 》使用瑞星杀毒	应用程序添加
 ✓ ✓ Ø 使用 RTX 发送文件 	应用程序添加
✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓	应用程序添加
✓ 》作为便携媒体设备	应用程序添加
U	
	确定 取消 应用
从七建英单	
TAWA	
用户可以勾选需要在文件或文件夹显示的	り右键菜单项,点击 确定,即
,且关闭设置对话框;点击 应用,	则可以立刻看到应用后的效果,如果
还可以继续修改设置;点击 取消,民	『可取消本次设置。
十年年	

点击	IE右键菜单,	切换至 IE 右键卖	炎单设置界面 。			
	😴 右键菜单管理				- >	٢
	文件右键菜单	IE右键菜单				
	选中要在IE页面	显示的右键菜单项	ξ			
	$\mathbf{\overline{\mathbf{V}}}$	名称			类型	
	🗹 🞤 使用迅雷	'下载			应用程序添加	
	🗹 🞤 使用迅雷	冒下载全部			应用程序添加	
	🗹 🞤 使用迅雷	离线下载			应用程序添加	
	•					Þ
			确定	取消	应用	
用户	可以勾选需要在	IE 页面显示的右	键菜单项,点;	由面定	按钮,即可	可完
关闭设	置对话框; 点击	应用按钮	田,则可以立亥	可看到应用	目后的效果,如	果戶
还可以	继续修改设置;	点击 取消	按钮,即可取	Q 消本次设	と置。	

9.2.4.8 垃圾文件清理

垃圾文件清理功能可以帮助用户扫描并清理电脑中的垃圾文件,默认选择的是电脑中最 常见的垃圾文件类型,推荐用户扫描。



垃圾文件清理

在主界面点击

,进入垃圾文件清理界面。

垃圾文件清理				– 🗆 ×
□ 请选择垃圾文件 □ 默认选择 的是 ■	"的类型后点击"开始扫描"。 电脑中最常见的垃圾文件类型,推荐您扫描	开始扫描		
	文件名		占用空间	垃圾文件数
📝 系统临时文件				
📝 无效的快捷方式				
📝 缩略图缓存文件				
📝 内存转储文件和错误	吴报告			
📝 回收站垃圾文件				
☑ Windows预读文件				
📝 已下载程序文件				
📝 Windows自动更新	时留下的补丁			
☑ Office安装文件				
📝 Windows Media Pl	ayen临时同步文件			
☑ Flash的Cookie文件	ŧ			
☑ 日志文件				
📝 音视频缓存文件(包	括迅雷看看、qqlive、pptv、风行等)			
📄 所有本地磁盘上指知	E类型的垃圾文件 设置			

点击界面右上角的

,系统则对电脑进行垃圾文件的扫描工作,扫描完成后,

会显示垃圾文件整体情况和详情,详情包括用户电脑中的垃圾文件名、占用空间和垃圾文件数。用户还可以点击 **重新扫描**,重新对电脑进行扫描。

乳>INC 计学端星企业终端安全管理系统软件用户手册

፩ 扫描完成,共发现 356 个垃圾文件, 5452.3Ⅰ	AB,建议您 ^{立即清理}	<u> 重新扫描</u>
文件名	占用空间	垃圾文件数
系统临时文件	46.8 MB	226
无效的快捷方式		
缩略图缓存文件		
内存转储文件和错误报告		
Windows预读文件		
Windows自动更新的留下的补了	466.2 MD	110
- Olite安装文件 - Windows Media Player性时同生文件	400.3 MD	112
Vinidows Media Flayen曲3回少文[开 Flash的Conkie文件		
	873 KB	6
	4939 3 MB	12
■ 6 15 3 5 1 2 11 (21) 2 1 4 1 4 1 4 1 4 1 4 1 4 1 4 1 4 1 4 1	理 对中际进行法理	法细合中户
■ 的 就 就 的 文件 () () () () () () () () () (^{雪理} 对电脑进行清理	,清理完成后, − □
■ 加茲維力文件(已加茲維予格) (4)(4) 所有本地磁盘上指定类型的垃圾文件 设置 可 可 可 可 可 可 可 可 以选择全部或部分文件,点击 立即 行 理成功的提示信息及详情。 文件 清理 了 了 行 了 了 了 了 了 了 了 了 了 了 了 了 了 了 了 " " " "	理 对电脑进行清理 夏了 46.8MB 磁盘空间。	,清理完成后, — — <u>_{重新扫描}</u>
■ DESection (Clinical and Compared of (Clinical and Compared of (Clinical and Compared of (Clinical and Clinical and Cli	50000 mD 管理 対电脑进行清理 夏了 46.8MB 磁盘空间。 占用空间	,清理完成后, — — <u>重新扫描</u> ^{垃圾文件数}
■ 的 家庭 1 文件 (在) (本) (本) (本) (本) (本) (本) (本) (本) (本) (本	577 电脑进行清理 夏了 46.8MB 磁盘空间。 占用空间 已恢复 46.8 MB	 ,清理完成后, <u>重新扫描</u> ^{垃圾文件数} 已清理 226
■ DESeating (Clinical and a plan of plan plan plan plan plan plan plan plan	新田田田田田田田田田田田田田田田田田田田田田田田田田田田田田田田田田田田田	,清理完成后, _ □ <u>重新扫描</u> ^{垃圾文件数} 已 清理 226
■ Diskert 2(f(ClaceBarler of danks ppix parts of f) 所有本地磁盘上指定类型的垃圾文件 设置 可用户可以选择全部或部分文件,点击 立即 管理成功的提示信息及详情。 文件活理 了 清理完毕,共清理 226 个垃圾文件,为您恢复 文件名 系统临时文件 无效的快捷方式 缩略图緩存文件	500.0 mD 管理 対电脑进行清理 夏了 46.8MB 磁盘空间。 占用空间 己恢复 46.8 MB	,清理完成后, _ □ <u>重新扫描</u> ^{垃圾文件数} 已 清理 226
■ bboxeti 文件(已)起告書 16、 (4)(13 (4)) 所有本地磁盘上指定类型的垃圾文件 设置 可用户可以选择全部或部分文件,点击 立即 行理成功的提示信息及详情。 文件 在 文件名 系统临时文件 无效的快捷方式 缩略图缀存文件 内存转储文件和错误报告	新田市市市市市市市市市市市市市市市市市市市市市市市市市市市市市市市市市市市市	,清理完成后, _ □ <u>重新扫描</u> ^{垃圾文件数} 己清理 226
■ bboxeti 文(r(clace) = iet (quine ppix put) 所有本地磁盘上指定类型的垃圾文件 设置 可可以选择全部或部分文件,点击 立即 這理成功的提示信息及详情。 文件活理	新田田田田田田田田田田田田田田田田田田田田田田田田田田田田田田田田田田田田	,清理完成后, _ □ <u>重新扫描</u> ^{垃圾文件数} 己清理 226
■ bbsecti 文件(ElizeBarack (Anixer ppice point) 所有本地磁盘上指定类型的垃圾文件 设置 可用户可以选择全部或部分文件,点击 立即; 适理成功的提示信息及详情。 文件清理 了 清理完毕,共清理 226 个垃圾文件,为您恢复 文件名 系统临时文件 无效的快捷方式 缩略图缓存文件 内存转储文件和错误报告 回收站垃圾文件	新田田田田田田田田田田田田田田田田田田田田田田田田田田田田田田田田田田田田	,清理完成后, _ □ <u>重新扫描</u> ^{垃圾文件数} 己 清 理 226
■ bboxeti 文((Clacebar and values ppix ord) 所有本地磁盘上指定类型的垃圾文件 设置 可可以选择全部或部分文件,点击 立即 通理成功的提示信息及详情。 文件 文件	日本のは、 日本のは、	,清理完成后, _ □ <u>重新扫描</u> ^{垃圾文件数} 已清理 226
■ 500,588,19,2(1(E),12,2),2(1),2(1),2(1),2(1),2(1),2(1),2(ま理 対电脑进行清理 ます ないのかめ す ないのかめ す は 用空 向 こ 休 复 46.8 MB	,清理完成后, □ <u>重新扫描</u> ^{垃圾文件数} [└] ^{☆扱文件数}
	日本のは、日本のは、日本のは、日本のは、日本のは、日本のは、日本のは、日本のは、	, 清理完成后, _ □ <u>重新扫描</u> 垃圾文件数 己清理 226
	日本の日本の目的では、「日本の日本の目前では、「日本の日本の目前では、「日本の日本の目前では、「日本の日本の目前では、「日本の日本の目前では、「日本の日本の日本の日本の日本の日本の日本の日本の日本の日本の日本の日本の日本の日	,清理完成后, <u>重新扫描</u> 垃圾文件数 已清理 226

9.2.4.9 隐私痕迹清理

隐私痕迹清理功能为了防止不良软件扫描用户使用痕迹、窥视用户隐私信息,系统将全

方位清理 Flash Cookie、浏览器 Cookie、搜索引擎历史记录等上网痕迹。

		-	١.
	N-	-	
	4		
		63	

在主界面点击 ^{隐私痕迹清理},进入隐私痕迹清理界面。

隐私痕迹	清理	- 🗆 🗧	×
	为了防止不良软件扫描用户使用痕迹、窥视用户隐私信息,系统将全方位洁理Flash(Cookie、历史记录等上网痕迹	Cookie、浏览器 开始扫描	
	痕迹类型	痕迹数	^
🔽 Flas	h Cookie		
🔽 F	lash Cookie		
☑ 搜索	引擎历史记录		
VĚ	度历史记录		
▼ 掲	兆 狗历史记录		
🔽 S	oso历史记录		
🔽 浏览	器cookie		
🔽 Ir	nternet Explorer Cookie		
▼ 2	歌浏览器Cookie		
▼ 掲	购浏览器Cookie		
▼ 火	《狐浏览器Cookie		
▼ 俵	旅游浏览器Cookie		
V 3	60安全浏览器Cookie		
V 3	60极速浏览器Cookie		~

开始扫描 点击界面右上角的 ,系统则对痕迹进行扫描,扫描完成后,会显示隐私痕 迹总数和详情,详情包括痕迹类型和痕迹数。用户可以勾选页面右上角的 ☑ 仅显示扫描到的痕迹,则列表将隐藏未扫描到的痕迹类型。用户还可以点击^{重新扫描},重 新对痕迹进行扫描。

ጓ▷ INC I # 2 瑞星企业终端安全管理系统软件用户手册

_				x
🛛 🛃 扫描完成,发现 1	1 处痕迹 立即清理 重新	<u>相描</u>		
			🔲 仅显示扫描到的痕	貢迹
	痕迹类型		痕迹数	^
Flash Cookie				
☑ 自度历史记录			4 处痕迹	
			4 处痕迹	
▼ SOSO历史记录				
☑ 浏览器cookie				
Internet Explorer Cookie			3 处痕迹	
✓ 谷歌浏览器COOKIE				
▼ 援狗浏览器COOKIE				
▼ 欠狐浏览器COOKIE				
▼ 微研別成番COOKIE				
▼ 300受主例免费Cookie				_
▼ 300版速网風器COOKIE				
1983949928960000C				×
用尸可以选择全部的	以 即刀派赵, 点山		清埋完成后,会	う四
用戶可以选择至部5 示清理成功的提示信息/	& 邮刀派迹,点击 □ 及详情。		清埋完成后,会	学型
用戶可以选择至部5 示清理成功的提示信息2 ^{隐私痕迹清理}	Q部刀飛⊍,魚山 ∟ 及详情。		清埋完成后,会 - □ :	× 学習
用戶可以选择至部5 示清理成功的提示信息/ ^{隐私痕迹清理} 记清理3处痕迹	Q 前 刀 很 型 , 点 山 □ Q 详 情 。 <u>■新扫描</u>		/清埋完成后,会 ≥	关显 ×
用戶可以选择至部5 示清理成功的提示信息2 ^[2] 尼清理 3 处痕迹	(前 万 飛 型 , 点 山 □ 2 (其 情 。 <u>重新扫描</u> 痕迹类型		/清埋元成后,会 _ □ ご _{痕迹数}	×
用戶可以选择全部5 示清理成功的提示信息/ 隐私痕迹清理 记清理 3 处痕迹	武田□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□		/ 清理元成后,会 _ □ 2 ^{痕迹数}	×
用戶可以选择全部5 示清理成功的提示信息/ 隐私痕迹清理	(中力派型, 点山 (二) (五) (五)		/ 清理元成后,会 ^{痕迹数}	×
用戶可以选择全部5 示清理成功的提示信息/ 隐私痕迹清理	(前) 万 很 远, 点 山 □		/ 清理元 成 后 , 会	× <
用 戸 可 以 选 择 全 部 5 示清 理 成 功 的 提 示 信 息 <i>D</i> 	(前) 刀 很 远 , 点 山 □ □		/ 清理元 成 后 , 会 <u>–</u> □ 2 痕迹数 1 3 处痕迹	× <
田戸可以选择全部5 示清理成功的提示信息 隐私痕迹清理 記者理3 处痕迹	武田 □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □		/ 清理元 成 后 , 会 _ □ 3 痕迹数 2 3 处痕迹	来
田戸可以选择全部5 示清理成功的提示信息 ¹ ¹ ² ² ² ² ² ¹ ² ² ¹ ² ² ¹ ² ² ¹ ² 	武田□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□		/ 清理元 成 后 , 会 <u>–</u> □ 2 痕迹数 2 3 处痕迹	关显 ×
田戸可以选择全部5 示清理成功的提示信息2 	Q 印 刀 很 型 , 黑 山 □ Q 详 情 。 重新扫描 痕迹类型		/ 清理元成后,会 痕迹数 ■ 3 处痕迹	■
田戸可以选择全部 示清理成功的提示信息 ^園 日本語書 ロホースの ロホースの ロホースの ロホースの ロホースの ロホースの ロホースの ロホースの			/ 清理元成后, 会 痕迹数 聲 3 处痕迹	× ▼
田戸可以选择全部5 示清理成功的提示信息の 	Q 前 刀 派 边 , 黑 山 □ Q 详 情 。 重新扫描 痕迹类型		/ 清理元成后,会 3 重3处痕迹	
田戸可以选择全部 示清理成功的提示信息 	武田 二 一 及详情。 董新扫描 痕迹类型		/ 清理元成后,会 痕迹数 聲 3 处痕迹	
田戸可以选择全部 示清理成功的提示信息 	英丽力派过,点山 《 五新扫描 道迹类型 《 道迹类型 《 书 和 和 第 和 第 和 第 和 书 者 和		/ 清理元 成 后 , 会	
田戸可以选择全部 示清理成功的提示信息 	其前分派过,点山 支详情。 重新扫描 痕迹类型		/ 清理元成后, 会 <u>痛</u> 迹数 1 3 处痕迹	
田戸可以选择全部 示清理成功的提示信息 	英丽力派过,点山 《 五新扫描 痕迹类型		/ 清理元 成 后 ,	
田戸可以选择全部 示清理成功的提示信息 	其前分派过 , 点山 及详情。 <u>重新扫描</u> 痕迹类型		/ 清理元 成 后 ,	

9.2.4.10 使用痕迹清理

使用痕迹清理功能可以将用户的使用痕迹进行清理,默认选择的地方最常出现使用痕迹,

i荐用户进行扫描。		
cookii		
在主界面点击 <mark>使用痕迹清理</mark> ,进入使用痕迹清理界面。		
使用痕迹清理	-	
□ 请选择要清理使用痕迹的地方,点击"开始扫描"检查它们。 默认选择 的地方最常出现使用痕迹,推荐您扫描。		
■ 痕迹类型	痕迹数	1
■上网痕迹		
✓ Internet Explorer 历史记录		
✓ Internet Explorer 地址栏网址历史记录		
Internet Explorer Cookies		
☑ FireFox 浏览器使用历史记录		
☑ Opera 浏览器使用历史记录		
☑ Opera 浏览器地址栏历史记录		
☑ 谷歌Chrome 浏览器使用历史记录		
☑ 腾讯□□浏览器使用历史记录		
☑ 谷歌工具栏搜索历史记录		
☑ 搜搜工具栏搜索历史记录		
☑ 百度工具栏搜索历史记录		
☑ Windows Live 工具栏历史记录		
📝 Internet Explorer 浏览器自动保存的表单		

点击界面上方的 **^{开始扫描}**,系统则对痕迹进行扫描,扫描完成后,会显示使用痕迹 总数和详情,详情包括痕迹类型、痕迹数和清理状态。用户可以勾选页面右上角的 **☑** 仅显示扫描到的痕迹,则列表将隐藏未扫描到的痕迹类型。用户还可以点击 **重新扫描**,重 新对痕迹进行扫描。

ጓ▷ INC I # 2 瑞星企业终端安全管理系统软件用户手册

使用痕迹清理	– 🗆 X
🛃 扫描完成,共发现 177 处使用痕迹,建议您	立即清理 重新扫描
—	
■ 痕迹类型	痕迹数
■ 上网痕迹	
☑ Internet Explorer 历史记录	64 处痕迹
🔽 Internet Explorer 地址栏网址历史记录	2 处痕迹
🔲 Internet Explorer Cookies	
▼ FireFox 浏览器使用历史记录	
☑ Opera 浏览器使用历史记录	
☑ Opera 浏览器地址栏历史记录	
☑ 谷歌Chrome 浏览器使用历史记录	
▼ 腾讯TT浏览器使用历史记录	
☑ 谷歌工具栏搜索历史记录	
☑ 搜搜工具栏搜索历史记录	
☑ 百度工具栏搜索历史记录	
♥ Windows Live 工具栏历史记录	
📝 Internet Explorer 浏览器自动保存的表单	可以清理
使用痕迹清理	- 🗆 ×
🛃 己清理 2 处使用痕迹。建议您经常进行痕迹清	理 ,保障您的隐私 安全。 重新扫描
[■ 痕迹类型	痕迹数
■ Internet Explorer 历史记录	
☑ Internet Explorer 地址栏网址历史记录	已清理 2 处痕迹
🔲 Internet Explorer Cookies	
🥅 FireFox 浏览器使用历史记录	
🔲 Opera 浏览器使用历史记录	
🔲 Opera 浏览器地址栏历史记录	
□ 谷歌Chrome 浏览器使用历史记录	
■ 購讯TT浏览器使用历史记录	
□ 谷歌工具栏搜索历史记录	
□ 搜搜工具栏搜索历史记录	
□百度工具栏搜索历史记录	
🥅 Windows Live 工具栏历史记录	
🥅 Internet Explorer 浏览器自动保存的表单	
🥅 Internet Explorer 浏览器自动保存的密码	~

9.2.4.11 文件粉碎器

文件粉碎器通过专业级高强度文件粉碎方法(符合美国国防部 DoD 5220.22- M 标准) 北京瑞星信息技术有限公司 162

在主界面点击 <mark>文件粉碎器</mark>	,进入文件粉碎器界面。		
■文件粉碎器			- x
通过专业级文件粉碎方法(符合美国国	I防部DoD 5220.22-M标准)彻底删除您不想要	的文件,永不被	找回。
	路径	状态	ŧ.
添加文件 添加目录 清空列表			开始粉碎
用户可以点击 添加文件,	添加想要粉碎的文件;也可以点击	添加目录,	添加想要
粉碎的目录。如果想要清空粉碎	利表,则点击		

■文件粉碎器	- X
通过专业级文件粉碎方法(符合美国国防部DoD 5220.22-M标准)彻底删除:	您不想要的文件,永不被找回。
路径	状态
😵 🗋 C:\Documents and Settings\Administrator\桌面\vmware\VMw	等待粉碎
😵 🗀 C:\Documents and Settings\Administrator\My Documents	等待粉碎
添加文件 添加目录 清空列表	开始粉碎
添加完成后,选择要粉碎的文件,点击 <mark>开始粉碎</mark> ,系	统弹出粉碎确认的对话框,点
击 确定 ,完成文件粉碎;点击 取消 ,取消本;	次粉碎操作。
圖粉碎确认	×
④ 确定要粉碎目标文件吗?粉碎不可物 复!	ζ.
福金	取消
PHAE	1/10

9.2.4.12 产品信息

产品信息为用户展示了产品详情和日志详情,以及产品当前版本号、升级时间、上级地 址等信息,还可以复制本机标识。



示当前产品的版本号。



产品详情

产品详情包括子产品、平台策略和升级策略等。



包括名称、代号、版本、安装时间和授权状态等。

端星企业终端	安全管理系统软	次件		-
● 首页・产	品信息・子产品			Ω
名称	代号 rua	版本 1.0.3.15	安装时间 2014-07-14 09:18	授权状态
核心组件	common files	1.0.2.43	2014-07-14 09:18	已授权
管理中心	manager	1.0.3.50	2014-07-14 09:18	已授权
业务中心	bus	1.0.0.43	2014-07-14 09:21	已授权
客户端代理	ер	1.0.2.81	2014-07-14 09:21	已授权
IT资产管理	ram	1.0.0.92	2014-07-14 14:28	已授权
升级中心	ruc	1.0.2.1	2014-07-14 09:21	已授权
漏洞补丁中心	rdc	1.0.0.67	2014-07-14 09:23	已授权
漏洞扫描	rls	1.0.0.98	2014-07-14 09:23	已授权
反病毒引擎	rsv	1.0.0.4	2014-07-14 09:23	已授权
防病毒	xav	1.0.2.63	2014-07-14 09:23	已授权
安全助手	rsa	1.0.0.4	2014-07-14 09:23	已授权



,可以看到平台策略详情,包括产品自定义标题、客户

端托盘、网络设置和日志清理等。

ጓ▷ INC 這是瑞星企业终端安全管理系统软件用户手册





,可以看到升级策略详情,包括部署子产品、升级策略、

网络连接和升级源等。



日志详情

日志详情包括平台日志(最近100条)、升级日志(最近100条)和状态日志等。



磁贴,可以查看最近的平台日志,最多显示最近的100

条。平台日志包括时间、来源和描述。

+)问	本派	<u>##:#</u>
014-06-24 10:03:08	小小小 [Rs BaseSrv]	〕Ⅲ/型 客户端[412F8C64464F4F7]登录成功
014-06-24 09:46:05	[Rs_BaseSrv]	客户端[412F8C64464F4F7]登录成功
014-06-24 09:32:30	[Rs_BaseSrv]	客户端[412F8C64464F4F7]登录成功
014-06-24 09:18:07	[Rs_BaseSrv]	客户端[412F8C64464F4F7]登录成功
014-06-23 14:00:08	[Rs_BaseSrv]	客户端[412F8C64464F4F7]登录成功
014-06-23 10:02:24	[Rs_BaseSrv]	客户端[412F8C64464F4F7]登录成功
014-06-23 09:22:19	[Rs_BaseSrv]	客户端[412F8C64464F4F7]登录成功
014-06-20 16:36:18	[Rs_BaseSrv]	客户端[412F8C64464F4F7]登录成功
014-06-20 14:24:17	[Rs_BaseSrv]	客户端[412F8C64464F4F7]登录成功
	[Re BeeeSrul	客户进[419280644642427]登录成功



,可以查看最近的升级日志,最多显示最近的 100 条。

升级日志包括时间、来源和描述。





,可以看到状态日志详情。状态日志包括客户端代理和

防病毒。

瑞星企业终端安全管理系统软件		- ×
● 首页,产品信息,状态日志	A	$\mathbf{\Omega}$
客户端代理		
客户端在线状态:在线	COST	-
防病毒		
病毒行为分析:已关闭	the state of the	
引擎版本:24.00.93.48		
文件监控:已开启		
病毒库版本:25.20.03.02		

9.3 漏洞补丁导入导出工具

漏洞补丁导入导出工具为用户提供漏洞补丁的导入和导出功能。安装防病毒后,点击系 统开始菜单的【瑞星企业终端安全管理系统软件】程序组中的【漏洞补丁导入导出工具】快 捷方式启动工具。

₩ 漏洞补丁导入导出工具	
存放位置: C:\Program Files\Rising\ESM\rdc\download 文件大小: 76.75 M 文件数目: 50 个	
□ 导入补丁文件 号出补丁文件 触发同步消息 打开补丁目录	修改补丁目录

可以根据用户需求,进行导入补丁文件、导出补丁文件、触发同步消息、打开补丁目录 和修改补丁目录等操作。

9.4 日志打包工具

日志打包工具为用户软件的日志提供打包保存功能。

安装防病毒后,点击系统开始菜单的【瑞星企业终端安全管理系统软件】程序组中的【日 志打包工具】快捷方式启动工具。

◯ 瑞星企业终端的	安全管理系统软件日志打包	
✓ ESM系统自身(日志 📝 ESM策略文件	📝 瑞星产品注册表
📝 系统服务列表	🔽 当前进程列表	📝 操作系统基本信息
✓ LSP信息	☑ BHO信息	📝 系统驱动信息
🔲 系统dump(可	能比较大)	
		开始
		暂停
		定位文件夹
		退出
文件名称: esmlog	2014_06_20_11_21_56	.zip
保存路径: C:\Pro	gram Files\Rising\ESM\ep	

选择需要打包的日志,输入文件的名称,选择打包后的日志保存路径,根据需要进行选择与操作。

9.5 数据库管理工具

数据库管理工具为用户提供查看和修改数据库的数据信息功能。安装防病毒后,点击系 统开始菜单的【瑞星企业终端安全管理系统软件】程序组中的【数据库管理工具】快捷方式 启动工具。

归 瑞星企业终端安全管理系统软件 - 日志管理		
登录		
用户名: admin]	
密码:		
主数据库	日志数据库	
数据库地址:	数据库地址:	-
数据库名称:	数据库名称:	
用户名: sa	用户名: Sa	
密码:	密码:	
	□ 使用主教据库信息	
	登录	

勾选 🗹 使用主数据库信息 后, 日志数据库会使用主数据库的链接; 若不进行勾选, 则主

数据库和日志数据库都是可用的。数据库设置好,点击 登录 即可连接到指定数 据库。

附录一北京瑞星信息技术有限公司简介

瑞星品牌诞生于 1991 年刚刚在经济改革中蹒跚起步的中关村,是中国最早的计算机反 病毒标志。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 曾双双连续多年蝉联总分第一的殊荣。

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。几经重组,公司已形成一支中国最大的反 病毒队伍。

目前,公司已推出基于多种操作系统的瑞星杀毒软件单机版、网络版客户端软件产品; 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 家可以提供全系列信息安全产品和服务的专业厂商。

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"服务系统。

瑞星和政府机构、商业伙伴以及媒体有着广泛而深入的合作关系,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、全国反病毒服务网以及全球病毒疫情监测网。

公司总部设立在北京,拥有国内最大的信息安全研发团队、国内最大的客户服务团队, 以及销售、市场、网站等部门,并已经建成覆盖全国的庞大的销售和市场体系。

目前瑞星拥有数千万正版个人用户,数万多家企业用户,主要软件产品以中(简、繁体)、 英、俄、德、日五种语言版本推向全球市场,销售网络覆盖北美、欧洲、亚太等地区。作为 在中关村成长起来的高科技企业,瑞星正逐步走向世界,实现公司的美好愿景——成为全球 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数千万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。