瑞星企业终端安全管理系统软件
快速使用指南

北京瑞星信息技术有限公司

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快速使用指南使用手册，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快速使用指南。

快速使用指南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）可下载本快速使用指南的最新版。因快速使用指南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。

北京瑞星信息技术有限公司

目录

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。
2. 《使用手册》：即《瑞星企业终端安全管理系统软件使用手册》，通过阅读它，掌握本软件的详细使用方法和技巧。
3. 《客户服务指南》：该指南将帮助用户获取技术支持和服务方面的信息。
4. 《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(没有上述数据库时自动安装)

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 Server 2003 系列系统

Windows Server 2008 系列系统

Windows 7系统

Windows Server 2008 R2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：1.0 GHz 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 Server 2003 系列系统

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

b. **硬件和网络要求**

剩余磁盘空间：2.0GB以上

CPU：1.0 GHz 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

1.2.4 升级中心

a. **软件环境**

1）操作系统

Windows Server 2003 系列系统

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

Windows 7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：1.0 GHz 及以上32 位 (x86) 或 64 位 (x64)

内存：2.0 GB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**

1）操作系统

Windows 7系统

Windows Server 2003 系列系统

Windows Server 2008 系列系统（包含 Windows Server 2008 R2 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：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**

1）操作系统

Windows XP 系统

Windows 2003 系统

Windows Vista 系统

Windows 7 系统

b. **硬件环境**

剩余磁盘空间：500MB以上

CPU：1.0 GHz 及以上32 位 (x86)

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

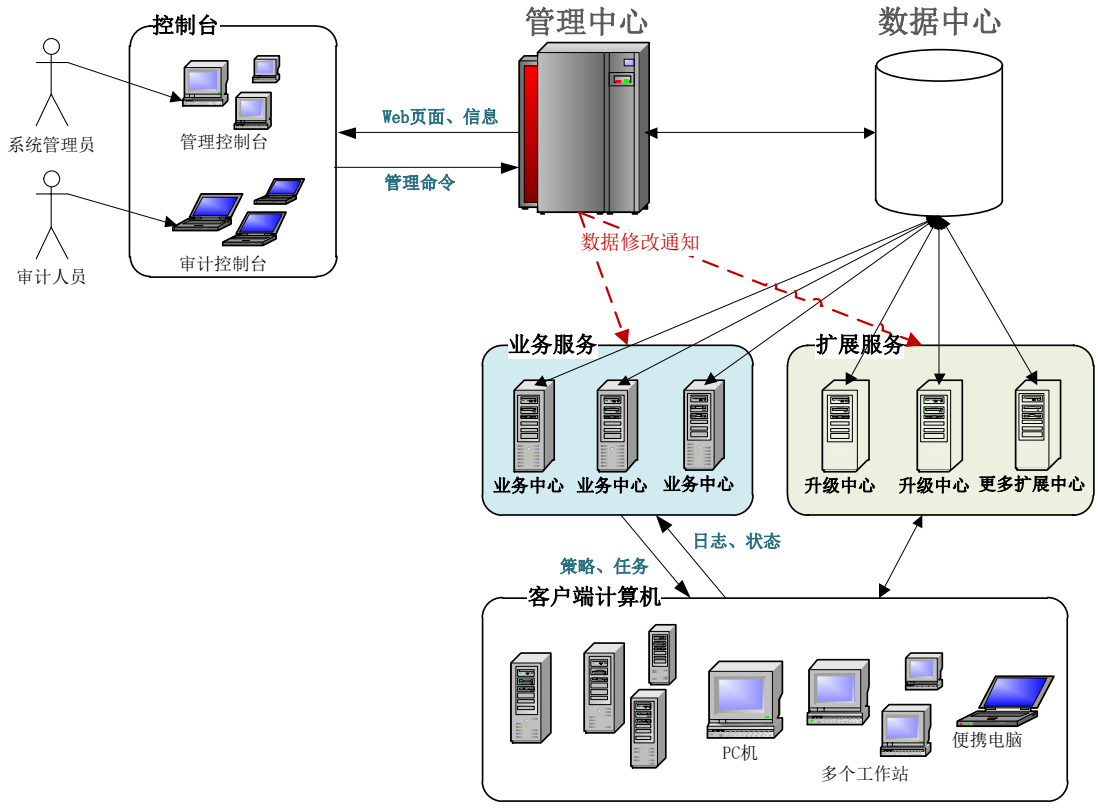
1.3 软件概述

瑞星企业终端安全管理系统软件是北京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，它对加强内网管理提供了一套统一的安全解决方案，对防止丢失或泄漏内网信息提供有力保障，并可对网络环境中各计算机的信息、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、防火墙、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，具备增强内网安全性的强大功能，提供给企业用户一个完整的企业安全解决方案，帮助企业用户更好的解决内部信息安全问题，从而达到保障企业资产安全的目的。

瑞星企业终端安全管理系统软件产品实质上只是一个管理平台，在这个平台上，企业用

户可以根据自身的需求在上面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下如下图：



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。

补丁下载中心：主要用于存储补丁文件。

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。

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 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“管理中心系统(包含数据中心)”、“业务中心系统”、“客户端基础库”、“客户端子产品——网络安全管理”、“客户端子产品——IT 资产管理”、“客户端子产品——客户端行为监控审计”和“软件部署升级中心”。

瑞星企业终端安全管理系统软件光盘提供了四种安装模式：快速服务器安装、快速客户端安装、自定义安装包安装和域脚本安装。

- 快速服务器安装

  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。

- 快速客户端安装

  单独安装客户端程序包。

- 自定义安装包安装

  高级自定义安装模式，可完成上述提到的两种快速安装的效果。

- 域脚本安装

瑞星企业终端安全管理系统软件支持在域控制器上配置软件安装的登录脚本。当计算机登录到指定的域时，实现安装程序的自动运行。

本文档以自定义安装包安装程序为例介绍瑞星企业终端安全管理系统软件的安装方法。

本文档将不对业务中心的安装与卸载、管理中心的安装与卸载、升级中心的安装与卸载、客户端的安装与卸载进行独立介绍，统一介绍服务器端和客户端的安装方法。

提示：

1. **安装本软件前请卸载第三方安全类软件。**
2. **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。**

2.1 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，启动瑞星企业终端安全管理系统软件 autorun.exe，选择【自定义安装包】按钮开始安装。

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

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

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

第四步：在【定制安装】窗口中勾选需要安装的功能组件（本文档以勾选全部为例），单击【下一步】继续安装。

第五步：在【选择目标文件夹】界面中选择安装瑞星软件的目标文件夹，单击【下一步】继续安装。

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】继续安装。

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

提示：瑞星企业终端安全管理系统软件自带有 MSDE 数据库，选择【MSDE】系统自动安装。

第七步：在【设置 esm 站点信息】窗口中，选中【站点访问模式】并对所选站点进行相应设置。有三种站点访问模式可供选择，分别为【使用默认站点（仅支持 HTTP）】、【使用自定义站点（仅支持 HTTP）】和【使用自定义站点（仅支持 HTTPS）】。选择合适站点并设置完相关信息后，单击【提交】再单击【下一步】继续安装。

第八步：在【指定管理中心对外服务端口】输入端口信息，也可以使用默认端口。单击

【提交】继续安装。

第九步：在【请填写业务中心地址窗口】输入业务中心的服务器地址和端口（可使用默认端口），单击【提交】后单击【下一步】继续安装。

第十步：在【设置 ruc 站点信息】窗口，选中【站点访问模式】并对所选站点进行相应设置。有两种站点访问模式可供选择，分别为【使用默认站点（仅支持 HTTP）】和【使用自定义站点（仅支持 HTTPS）】。选择合适站点并设置完相关信息后，单击【提交】再单击【下一步】继续安装。

第十一步：在【指定升级中心对外服务端口】输入端口信息，也可以使用默认端口。单击【提交】继续安装。

第十二步：在【结束】窗口点击【完成】结束安装。

2.2 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】/【程序】/【瑞星企业终端安全管理系统软件】/【修复】，在弹出的【瑞星软件维护模式选项】界面中选择【卸载】，按照界面提示操作即可。

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】，在弹出的【瑞星软件维护模式选项】界面中选择【卸载】，按照界面提示操作即可。

3 产品授权获取

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。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。

提示：有些特殊的安装包会带内置授权许可，如果你使用的这种安装包，则可以忽略此过程。

3.1 获取授权

购买产品后，您将获得一个格式为“X X X X X-X X X X X -X X X X X -X X X X X -X X X X X”的产品基本包序列号。使用本序列号，前往瑞星官网相应版块，进行产品注册，以获取产品授权文件。具体步骤如下：

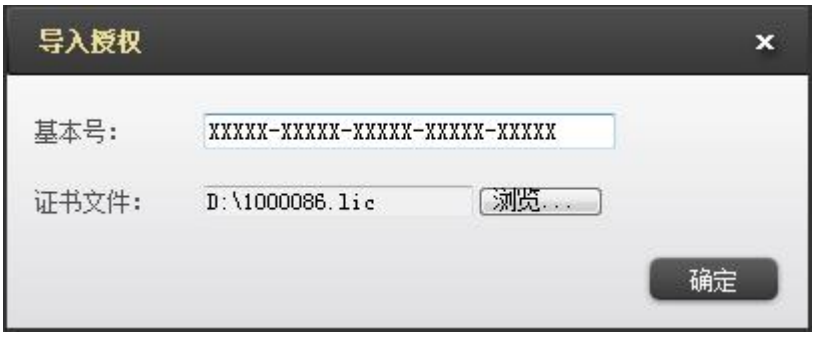
第一步：进入瑞星官网相应版块，进行用户服务号注册。

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】，下载证书文件。（如：1000086.lic），本文件用于激活中心服务器程序，请妥善保管。



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。

3.2 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。

4 系统登录

4.1 登录系统

安装完成后在桌面会自动生成瑞星内网安全管理系统 html 页面，点击此页面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。

点击瑞星企业终端安全管理系统软件——管理控制台页面上方 切换到审计控制台 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——审计控制台页面上方 

可切换到管理控制台。

4.2 未知计算机管理

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——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。

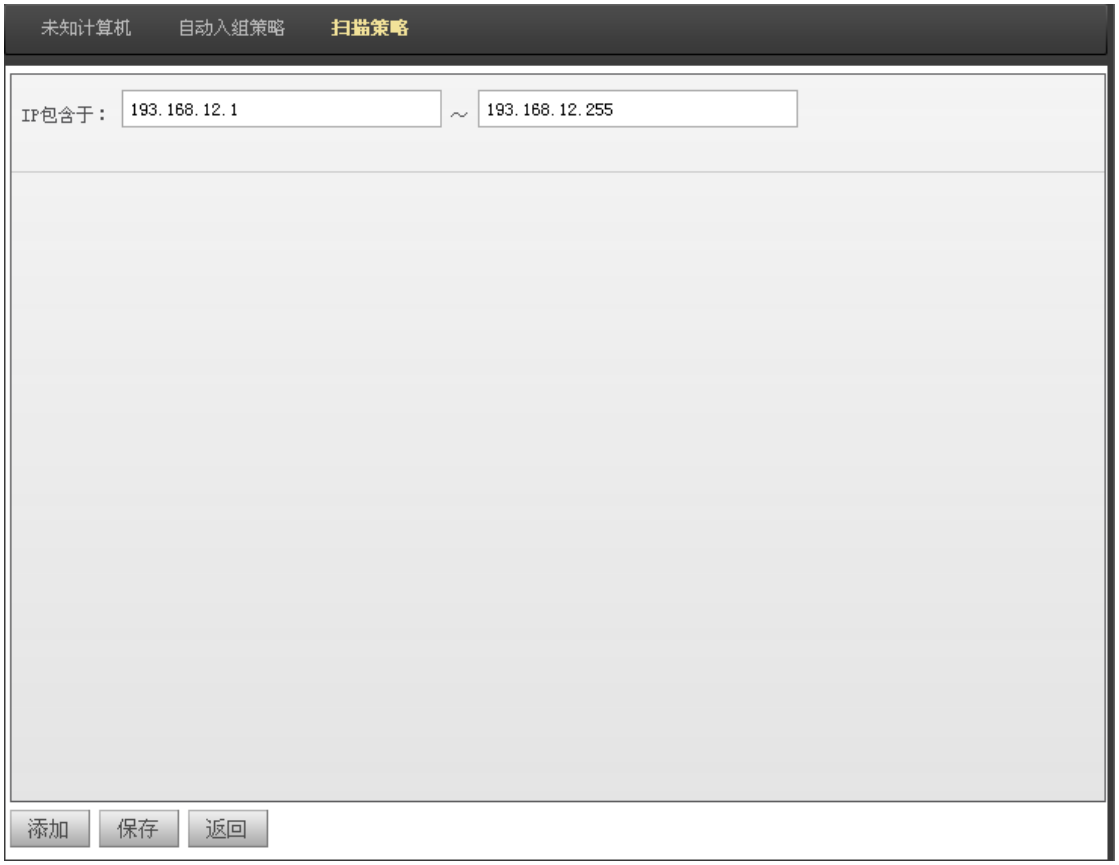
点击客户端列表中任意未知计算机组的客户端计算机名，会打开此计算机详细信息界面。此界面显示的是此客户端的详细信息包括：基本信息、产品信息、硬件信息、软件信息、网络设备信息以及系统信息等六方面的内容，可以分别打开，查看具体信息。还可以点击界面上方自动入组策略、扫描策略和未知计算机分别查看或设置未知计算机组信息。

一、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。



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。

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。

5 策略模板

【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【瑞星IT资产管理（RAM）】、【瑞星防病毒组件（XAV）】、【瑞星客户端代理（EP）】、【瑞星客户端即时通讯审计（RIM）】、【瑞星客户端漏洞扫描（RLS）】、【瑞星客户端软件部署(RUA)】、【瑞星客户端行为审计（RBA）】和【瑞星网络安全管理（RSM）】八个策略模板。

瑞星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【瑞星 IT 资产管理-默认策略】和【瑞星 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。

瑞星防病毒组件（XAV）

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

瑞星客户端代理（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。

瑞星客户端即时通讯审计（RIM）

属于日常维护性管理范畴，当客户端使用QQ、TM、RTX、MSN等主流聊天工具时，对其聊天内容、传输的文档进行监控审计。

在默认安装完后，系统会自动创建产品的一些策略到根组及策略模板，策略模板可以直接用来分配使用，也可以手动管理更多的策略模板。默认情况下不做任何修改，各子产品的基本功能是生效的。

瑞星客户端漏洞扫描（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。

瑞星客户端软件部署(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。

瑞星客户端行为审计（RBA）

属于日常维护性管理，包括了行为控制与安全审计两方面的内容,主要是满足网络管理员对客户端用户的行为进行管理。另外部分审计策略则属于收集用户行为数据后，提供给管理者决策分析使用。

该策略分为两部分内容【瑞星客户端行为审计-默认策略】和【瑞星客户端行为审计-IP规则】。用于管理员对客户端用户操作文档、邮件、设备、上网、共享资源、网络流量、非法外联等行为进行控制和审计。并且能够针对在联网过程中的程序进行有效管理、拦截外部攻击，有效的阻止黑客远程攻击。

瑞星网络安全管理（RSM）

属于日常维护性管理，主要是满足网络管理员对客户端环境的安全维护。该策略用于管理员对客户端操作系统安全设置、安全检查及防御等功能。

5.1 添加策略模板

依次点击【客户端管理】/【策略模板】/【添加策略模板】打开添加模板界面。

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。
- 已分配的组：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。

5.1.1 创建瑞星 IT 资产管理策略模板

一、 瑞星 IT 资产管理-默认策略

依次点击【客户端管理】/【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【瑞星 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【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：勾选启动记录进程启动历史。

点击【保存】模板为创建成功；点击【取消】为不保存。

二、 瑞星 IT 资产管理-软件部署策略

依次点击【客户端管理】/【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【瑞星 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、版本好、注册表等信息以达到第三方软件部署的目的。

5.1.2 创建瑞星防病毒组件策略模板

依次点击【客户端管理】/【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【瑞星防病毒组件-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】和【文件监控设置】三方面内容。

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、云连接测试间隔时间、是否启动公有云及私有云相关设置
- 隔离区：设置空间不足的处理方式、大文件的处理方式
- 启动病毒跟踪：方便管理员了解病毒爆发的起始时间、机器、数量等情况

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。
- 扫描文件类型：设置扫描的文件类型
- 普通扫描引擎：提供【启动式扫描】、【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
- 清除失败处理方式：自定义清除失败的处理方式

C. 文件监控设置

- 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【启动式扫描】、【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
- 清除失败处理方式：自定义病毒处理方式

部分项存在锁，如果设置锁后，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；如果没有加锁，下发的策略与本地冲突时，本地设置的策略优先。

点击【保存】模板创建成功；点击【取消】不保存。

5.1.3 创建瑞星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【客户端管理】/【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【瑞星客户代理-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。

5.1.4 创建瑞星客户端即时通讯策略模板

聊天审计

记录多种即时通讯聊天工具的通讯内容，管理员通过审计通讯内容即可了解员工工作状态以及是否通过聊天工具向外传送了敏感信息或机密信息等。

聊天工具：包括 QQ、MSN、RTX、TM 等主流即时聊天工具。

监控聊天内容：全面记录对话时间、对话人、对话语句数、对话内容等。

监控文档传输：监控客户端计算机通过即时通讯工具发送的文档。

气泡通知：触发规则后以弹框的形式通知管理员。

锁定计算机：将触发规则的计算机锁定，禁止使用。

离线生效：客户端上线后将离线时间内生成的文档审计日志上传管理中心。

5.1.5 创建瑞星客户端漏洞扫描策略模板

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：

- 扫描时机类型：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。
- 补丁下载顺序：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。

5.1.6 创建瑞星客户端软件部署策略模板

依次点击【客户端管理】/【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【瑞星客户端软件部署-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：可分别对瑞星 IT 资产管理（RAM）、瑞星防病毒组件（XAV）、瑞星客户端即时通讯审计（RIM）、瑞星客户端漏洞扫描（RLS）、瑞星客户端行为审计（RBA）和瑞星网络安全管理（RSM）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
- 代理服务器：
    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。

5.1.7 创建瑞星客户端行为审计策略模板

一、 瑞星客户端行为审计-默认策略

依次点击【客户端管理】/【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【瑞星客户端行为审计-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【文档审计】、【文档打印审计】、【邮件审计】、【设备审计】、【网络审计】、【联网程序管理】、【对外攻击拦截】、【共享资源管控】、【网络流量管理】和【非法外联管控】十大类审计内容，可以做到对客户端的各种使用行为进行有效监控。

点击各审计类型右侧 + 增加 - 删除 功能，增加数量无限制，删除时类型模板无法删除。

一、文档审计

对客户端机器上的各种行为进行监控并产生日志，以备查询管理。

审计类型：

a) 仅记录操作：触发规则仅记录日志并将相关日志上传管理中心。

b) 禁止并记录操作：触发规则后禁止操作并记录上传日志。

介质类型：可勾选硬盘、光盘、可移动盘和网络盘

目标文件名:输入.txt/.mpp/.docx/.exe 等文件类型或输入具体文件(如 123.txt)当发生相关行为时以预设方式反馈信息。多条记录以“|”分隔，如：*.doc|%system%*.txt。

行为类型：可勾选创建、访问、修改、重命名、复制、移动、删除。

有效时间：审计有效的时间范围，设置频率每天（xx：xx~xx：xx）/每周的某一天或某几天的 xx：xx~xx：xx 时间内/时间段。

气泡通知：触发规则后以弹框的形式通知管理员。

锁定计算机：触发规则后锁定计算机，禁止使用。

离线生效：客户端上线后将离线时间内生成的文档审计日志上传管理中心。

二、文档打印审计

该功能用于记录完整的打印日志，实现对打印资源的有效管理，降低打印成本，并保证组织的信息安全。记录信息包括：打印的时间、终端、用户、应用程序、打印机类型、打印机名称、文档标题、打印页数等信息。

可选择：

a) 记录打印审计：当打印文件时记录相关信息并将日志上传管理中心。

b) 禁用打印机：不允许计算机使用打印机。

三、邮件监控

该功能用于全面记录 POP3/SMTP、EXCHANGE 邮件收到及发送的邮件的全部内容，包括收件人、发件人、邮件标题、邮件正文和附件内容。

规则名：输入本策略的相关信息或目的。

动作：可勾选：

a) 发送：发送邮件时审计。

b) 接收：接收邮件时审计。

发送者：发送人的名称或邮箱地址。

接收者：接收人的名称或邮箱地址。

邮件主题：邮件名称。

仅监控包含附件的邮件：邮件中有附件时监控生效。

拦截：拦截触发规则的邮件。

提示：发送人/接收人/主题是并列的关系，同时满足三者条件审计才会生效。

邮件端口策略：端口号及端口协议

四、设备审计

管理员可设置策略，对以下设备派发允许或禁止使用策略：光驱、1394、蓝牙、串口、并口、PCMCIA 卡和红外设备。

五、网络审计

包括【拨号控制】和【网页浏览控制】两方面内容，可以对客户的网络行为进行有效的监控管理，保护企业资产的安全。

启用拨号控制

拨号方式：可勾选禁用 VPN、禁用 ADSL、禁用 MODEM。

有效时间：每天的某一时间段/每周的某一天或几天的时间段/直接设置时间段。

启用网页浏览控制

URL：输入要监控的网址。

有效时间：每天的某一时间段/每周的某一天或几天的时间段/直接设置时间段。

禁止访问并跳转 URL：当触发规则时跳转至该网址。

离线生效：客户端上线后将离线时间内生成的文档审计日志上传管理中心。

气泡通知：当触发规则弹出气泡提示警示用户

启用网页浏览记录

记录所有访问的网址并上传管理中心。

六、联网程序管理

该功能用于记录、控制客户端上的程序连接网络的行为，这些行为包括是否允许联网，以及联网的时间段。

离线生效：客户端离线时间内功能仍然生效

开启瑞星信任程序智能识别：内置信任程序允许联网

未知程序联网策略：不在规则内程序的联网策略设置

进程规则列表：用于设置各进程或者软件的联网策略，可设置多条规则

七、对外攻击拦截

该功能可以防范网络僵尸，傀儡僵尸等等多种僵尸网络服务端对外发送攻击数据包。

离线生效：客户端离线时间内功能仍然生效

提示用户：一旦检测到攻击，弹出气泡提示警示用户

支持勾选多种对外攻击拦截：拦截 SYN 攻击、拦截 ICMP 攻击、拦截 UDP 攻击

八、共享资源管控

该功能可以查看每个终端的共享状态，控制共享的资源，并且可以查看、限制资源的访问权限。

离线生效：客户端离线时间内功能仍然生效

记录日志：记录日志并上传到数据中心

要关闭的默认共享：用于关闭终端的默认共享

九、网络流量管理

该功能用于记录终端的某个时间段网络总流量，以及某个时刻的流速。

记录联网程序日志：勾选后能够记录日志并上传到数据中心

记录终端流量日志：勾选后记录相关日志并上传到数据中心

定时报告时间间隔：提供 10、20、30、60、120 五种间隔进行选择，默认为 10 分钟

管理规则：

启动规则：规则是否生效

离线生效：客户端离线时间内功能仍然生效

下载限速：设置最大流量限制

功能生效时间:：每天的某一时间段/每周的某一天或几天的时间段/直接设置时间段

十、非法外联管控

该支持监控内部网络中客户端的非法外联行为，实时检测内部网络（包括物理隔离和逻辑隔离网络）是否与 Internet 联通，并产生告警信息、对违规者可锁定计算机或断网。

离线生效：客户端离线时间内功能仍然生效

提示用户：勾选后触发规则后弹气泡提示用户

检查方式：提供智能检查和定时检查两种方式

检查到非法外联时：提供锁定计算机和隔离两种处理方式

点击【保存】模板创建成功；点击【取消】不保存。

二、 瑞星客户端行为审计-IP 规则

依次点击【客户端管理】/【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【瑞星客户端行为审计-IP 规则】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【阻止黑客远程攻击】、【IP 地址白名单】、【IP 地址黑名单】、【端口设置】、和【自定义 IP 规则】。

A. 阻止黑客远程攻击

- 离线生效：客户端离线时间内功能仍然生效
- 发现攻击时提示用户：勾选后触发规则后弹气泡提示用户

- 拦截后阻止此 ip 时间：提供 1、2、3、4、5 分钟 5 种选择
- 防护规则：内置 88 条防护规则，用户可以点击显示对规则对规则进行逐条启用或禁用，默认为全部启用。

B. IP 地址白名单

- 离线生效：客户端离线时间内功能仍然生效
- IP 地址白名单管理：可以对单个 IP 或者某个 IP 范围进行设置；支持多个 ip 白名单设置

C. IP 地址黑名单

- 离线生效：客户端离线时间内功能仍然生效
- 阻止访问时通知用户：匹配规则后弹出气泡提示用户
- 记录日志：勾选后记录日志并上传到数据中心
- IP 地址黑名单管理：可以对单个 IP 或者某个 IP 范围进行设置；支持多个 ip 黑名单设置

D. 端口设置

- 离线生效：客户端离线时间内功能仍然生效
- 阻止访问时通知用户：匹配规则后弹出气泡提示用户
- 端口管理：可对端口进行管理确认是否允许联网
  - ✧ 可以对单个端口号或者某个端口范围进行设置
  - ✧ 支持 tcp、udp、tcp+udp 三种协议方式
  - ✧ 可记录入站、出站及双向；

E. 自定义 IP 规则

- 离线生效：客户端离线时间内功能仍然生效
- 自定义 IP 规则列表（支持多条 IP 规则设置）
  - ✧ 启动该规则：确认是否启用此条规则
  - ✧ 阻止访问通知用户：是否触犯规则弹出气泡提示用户
  - ✧ 允许联网：匹配规则后是否允许联网
  - ✧ 规则名称：自定义规则名称
  - ✧ 可记录入站、出站及双向
  - ✧ 本地 IP 规则：支持单个 IP 或者某个 IP 范围进行设置
  - ✧ 远程 IP 规则：支持单个 IP 或者某个 IP 范围进行设置

- ✧ 支持多种协议类型
- ✧ 支持设置多组本地端口（最多 5 组）
- ✧ 支持设置多组远程端口（最多 5 组）

点击【保存】模板创建成功；点击【取消】不保存。

5.1.8 创建瑞星网络安全管理策略模板

一、 瑞星网络安全管理-安全管理策略

依次点击【客户端管理】/【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【瑞星网络安全管理-安全管理策略】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【客户端操作系统环境安全维护】、【ARP 欺骗防御】和【网络安全准入】三方面内容。

A. 客户端操作系统环境安全维护，可勾选

- 记录系统事件（包括：开机、关机、注销、锁定）
- 禁用控制面板
- 禁用计算机管理
- 禁用计算机属性
- 禁用网络连接管理
- 禁用 IE 浏览器插件管理

B. ARP 欺骗防御

- IP 冲突时防止网络断开：匹配规则后可断网已保证网内的安全环境
- 禁止本机对外发送 ARP：防止其它终端机器继续感染
- 阻止攻击时提示用户：匹配规则后弹出气泡提示用户
- 离线生效：客户端离线时间内功能仍然生效

C. 网络安全准入

- 高危漏洞过多时隔离客户端端并上报风险
  - 规则描述：可自定义规则名称
  - 检查数量：自定义检查数量

- 未安装安全防护类软件时隔离客户端并上报风险
  - 规则描述：可自定义规则名称
  - 软件名称：设置需要检查的软件名称
  - 勾选任意安全软件
- 违规时提示用户：匹配规则后弹出气泡提示用户
- 离线生效：客户端离线时间内功能仍然生效

点击【保存】模板创建成功；点击【取消】不保存。

二、 瑞星网络安全管理-开机管理策略

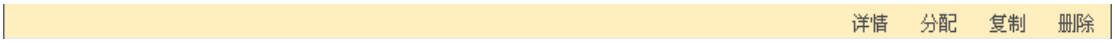
此策略为出厂内置策略，不允许设置。

5.2 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【瑞星 IT 资产管理】为例介绍模板的用法。

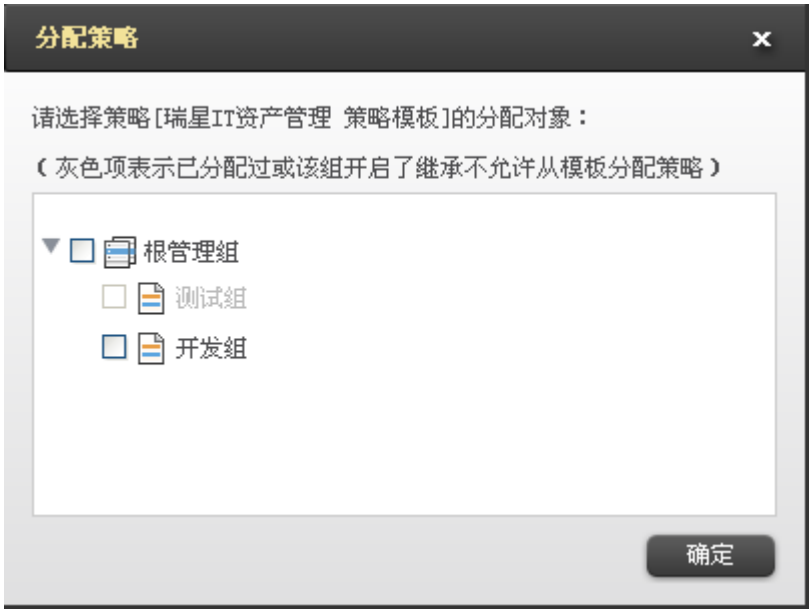
依次点击【客户端管理】/【策略模板】/【瑞星 IT 资产管理】会显示已创建模板。

将鼠标放在任意模板上会出现可用的操作项



1. 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。



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）。

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。

作用：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。

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指南，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。

瑞星原厂联系方式：

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

瑞星代理商联系方式：

客户服务：400-822-8250

网址：www.thinkcloud-time.com

邮箱：support@thinkcloud-time.com