卡巴斯基实验室

卡巴斯基® 反病毒 6.0 WINDOWS 工作站

用户指南

卡巴斯基反病毒 6.0 WINDOWS 工作站

用户指南

http://www.kaspersky.com.cn

修订时间：2007 年 7 月

目　　录

第1章. 卡巴斯基反病毒 6.0 WINDOWS 工作站

卡巴斯基反病毒 6.0 Windows 工作站是新一代的数据安全产品。

卡巴斯基防病毒 6.0 Windows 工作站提供了对几乎所有的安全威胁进行防护的功能，这使它明显区别于其它的软件，甚至是卡巴斯基实验室的其它产品。

1.1. 卡巴斯基反病毒 6.0 WINDOWS 工作站的新特性

卡巴斯基反病毒 6.0 Windows 工作站提供了对安全威胁进行防护的新功能。该程序的主要特性是在安全解决方案方面结合了本公司所有产品现有的特性并加以大幅改进。本程序提供反病毒保护、反垃圾邮件保护、反黑客保护，并且添加了可以检测未知威胁、防御网络钓鱼攻击以及 rootkits 等方面新的程序模块。

您不必为了实现计算机的整体安全而安装多款安全防护产品。事实上安装卡巴斯基反病毒 6.0 Windows 工作站是非常简单方便的。

全面防护进出您主机的数据。卡巴斯基反病毒工作站的所有组件可以灵活设置，从而使其能够适应每一用户的需要。您可以对整个程序进行配置。

让我们看一下卡巴斯基反病毒 6.0 Windows 工作站有哪些新的功能。

新增的保护功能

- 卡巴斯基反病毒 6.0 windows 工作站提供已知恶意程序以及未知恶意程序两方面的保护。主动防御 (见第 9 章在 88 页) 是本程序的主要优势。它对安装在您计算机上应用程序的行为进行分析，从而监控系统注册表的变更，跟踪宏并且瓦解隐蔽的威胁。该组件使用启发式分析来检测和记录不同类型的恶意行为，从而可以撤销恶意程序所完成的动作，同时系统也可以被恢复到恶意行为之前的状态。
- 本程序可以针对 rootkits、拨号器、横标广告、广告弹出窗口和从网络下载的恶意脚本，网络钓鱼等方面进行防护，以保护您的计算机。
- 改进了文件反病毒保护技术，从而降低了程序的对 CPU 资源占用，并且增加了文件扫描速度。iChecker™ 和 iSwift™ 有助于实现这一目标 (见 6.2.1 在 on page 63) 这样，程序就不会两次对文件进行病毒扫描。

- 当您使用计算机时，进程扫描可以在后台运行。扫描占用合理的系统资源，并且不影响用户使用计算机。如果一些进程需要系统资源，病毒扫描将暂停，直至操作完成后，才从停止的地方继续扫描。
- 如果关键区域被感染将严重影响数据质量或安全，则可以分别对这些区域执行扫描任务。您可以配置这个任务在每次计算机启动时运行。
- 有效改进了使邮件系统免受恶意程序以及垃圾邮件影响的功能。本程序会扫描使用以下这些协议发送的邮件中的病毒以及垃圾邮件:
    - IMAP, SMTP, POP3, 无论您使用哪种邮件客户端
    - NNTP (只扫描病毒)，无论您使用哪种邮件客户端
    - MAPI, HTTP (使用 MS Outlook 以及 The Bat！插件)
- 专用插件在常用客户端中广泛使用，如 Outlook 、MS Outlook Express 以及 The Bat！ 这可以直接在邮件客户端扫描病毒和垃圾邮件。
- 本程序的反垃圾邮件功能现在具有基于 iBayes 算法的学习模式，它通过监测用户处理邮件的方式进行学习。该功能也使垃圾邮件检测的配置具有最大的灵活性，例如，您可以创建黑白名单地址列表以及标记为垃圾邮件的关键字。

  反垃圾邮件使用网络钓鱼数据库，它可以过滤企图获得用户财务机密信息的邮件。
- 该程序对入站和出站数据进行过滤，追踪和阻止来自公共网络的攻击，并让您以隐身模式使用互联网。
- 使用综合网络时，您也可以定义完全信任的网络和需要尤其注意监控的网络。
- 对在程序运行期间发生的某些事件扩展了用户通知功能 (见 16.11.1 在 210 页)。您可以为这些事件选择各自事件类型通知方式：邮件，声音，弹出信息。
- 增加了对通过安全的 SSL 连接传输的数据进行扫描的功能。
- 本程序增加了自我保护功能，包括阻止远程未经授权的管理工具以及程序密码保护设置。这些功能有助于使保护功能不被恶意程序，黑客以及未经授权的用户禁用。
- 您也可以创建应急磁盘，在系统受到病毒破坏后用来重新启动操作系统并扫描计算机中的恶意代码。
- 此版本程序的保护系统增加了集中远程管理选项，使用了卡巴斯基管理工具中新增加的管理界面。

新增的程序界面功能

- 卡巴斯基反病毒 6.0 windows 工作站的新界面功能一目了然，并且易于使用。您也可以使用您自己的图片以及颜色配置来更改程序的界面。
- 使用时，程序还会经常向您提供一些使用技巧：卡巴斯基反病毒 6.0 windows 工作站会显示有关安全级别的有益信息，操作提示和技巧以及详细的“帮助”部分。

新增的程序更新功能

- 我们新推出的程序版本改进了更新程序：现在，卡巴斯基反病毒 6.0 Windows 工作站能够自动检查更新源。如果发现有新的更新库，该程序会将其下载并安装到计算机中。
- 该程序只下载增量更新的内容，而忽略已下载的文件。这将使更新时的下载流量降低 10 倍。
- 程序更新是从最有效的地址进行下载的。
- 如果更新是从本地下载，您可以选择不使用代理服务器。这会显着地减少代理服务器的流量。
- 该程序具有反病毒数据库回滚 (恢复) 功能。如果反病毒数据库受损或者拷贝时出错，则它可以将安全特征库库恢复到上次可用更新的版本。
- “更新 (Updater)”中新增的工具，可以将更新文件复制到本地文件夹中供网络中的其它计算机使用。这将减少互联网的流量。

1.2. 卡巴斯基反病毒工作站防护组件

卡巴斯基反病毒工作站在设计时考虑到了威胁源的问题。换句话说，就是利用不同的程序组件防范各种安全威胁，对其进行监控并采取必要的行动以防止其对用户数据产生不良的影响。这使卡巴斯基的“安全套装”可以灵活运用，利用其每一组件的用户友好选项来满足个人或企业用户的安全需要。

卡巴斯基反病毒工作站包括：

- “保护组件” (见 1.2.1 在 13 页) 对您计算机中所有的数据访问和交换方式进行监控。
- “病毒扫描任务” (见 1.2.2 在 15 页) 可以对计算机内存和单个文件、文件夹、磁盘或区域等文件系统进行病毒扫描。
- “支持工具” (见 1.2.3 在 15 页) 提供关于本程序的技术支持以及扩展其功能。

1.2.1. 保护组件

下列保护组件对计算机进行实时保护：

文件保护

您系统中的文件可能会存在一些病毒和其它恶意程序。恶意程序由软盘或互联网被复制到您的文件系统后可能会隐藏若干年而不会启动。但是只要您操作了受感染的文件，则病毒会随时激活。

“*文件保护*”是监控计算机文件系统的组件。它对您计算机上的所有可以进行打开、执行、保存的文件以及所有连接的磁盘驱动器进行扫描。每次访问文件时，卡巴斯基“文件保护”会对其进行拦截并扫描是否有已知病毒存在。如果文件由于任何原因无法清除，则将其删除，删除前会对染毒文件先进行备份，或者将文件移动到隔离区。

邮件保护

电子邮件已被黑客广泛地用于传播恶意程序，也是传播蠕虫病毒的主要手段之一。因此，对所有电子邮件进行监控尤为重要。

“邮件保护“组件对计算机所有收发的电子邮件进行扫描。它分析电子邮件中有无恶意程序，并且在确认邮件没有危险对象时才允许收信人接收。

Web 反病毒保护

您在浏览各类网站时，可能会使计算机感染到网页上所带病毒。因为这些网页上存储了恶意脚本。您也可能会将危险文件下载到您的计算机上。

“*Web 反病毒保护*“会对基于 HTTP 协议的通信进行监控，阻止恶意脚本对您计算机造成的危害。

主动防御

现在每天传播的恶意程序越来越多。由于它们结构日趋复杂，并采用多种方式进行传播，使恶意程序检测越发困难。

卡巴斯基实验室专门开发了“主动防御“组件来检测新的恶意程序，以防其造成任何的破坏。该组件的设计旨在对您计算机中安装的所有程序的行为进行监控和分析。卡巴斯基反病毒工作站根据程序的行为确定：是否存在潜在危险？“主动防御”可以防止您的计算机受到已知病毒以及未知新病毒的威胁。

反间谍保护

如今垃圾广告 (例如横标广告和弹出式窗口) 、未经用户授权拨叫付费网络服务的程序、远程管理和监控工具以及玩笑程序等程序日益普遍。

“反间谍保护”对您计算机中的这些行为进行跟踪和拦截。例如，该组件会拦截横标广告和弹出式窗口，拦截企图自动拨号的程序并分析含有网络钓鱼内容的网页。

反黑客

无论您的计算机是有开放端口、还是有数据传输等等动作，黑客将会利用各种漏洞对您的计算机发起攻击。

“反黑客”组件在您使用互联网以及其它网络时，可以为您的计算机提供安全保护。它对入站和出站连接进行监控，并检测端口和数据包。

反垃圾邮件

尽管垃圾邮件不会对系统造成直接的危害，但它会占有您邮件服务器的大量资源，恶意装满您的收件箱，浪费您的时间，从而造成您经济上的损失。

“*反垃圾邮件*”组件会嵌入您的计算机的电子邮件客户端程序中，并检测所有收到的邮件中有无垃圾邮件。该组件会将在所有垃圾邮件的主题上添加特殊的邮件头标记。您可以自行配置“发垃圾邮件”组件来处理垃圾邮件 (如自动删除、移到指定的文件夹等等)。

1.2.2. 病毒扫描任务

除了经常对恶意程序所有潜在的信道进行监控外，定期对您的计算机进行扫描也使极为重要的。因为有时可能安全级别设定过低，致使本程序未能发现这些恶意程序，因此有必要对这些恶意程序进行检测。

卡巴斯基反病毒工作站默认提供三个扫描任务：

关键区域

扫描计算机的所有关键区域。这包括系统内存、系统启动项、硬盘引导扇区以及 *Windows* 系统目录。扫描任务的目的在于快速检测到激活的病毒而不必对计算机进行全面扫描。

我的电脑

对您计算机中的所有磁盘驱动器、内存以及文件进行全面的病毒检测。

启动对象

扫描所有自动加载到启动项、RAM 以及硬盘引导扇区的程序。

还有创建其它病毒扫描任务及其扫描计划的选项。例如，您可以创建每周扫描电子邮件数据库一次的任务，或“**我的电脑**”文件夹的病毒扫描任务。

1.2.3. 程序工具

卡巴斯基反病毒 6.0 windows 工作站包含多种支持工具，用以提供实时的软件支持，从而提升本程序的功能并全力为您服务。

更新

为了防范黑客的攻击或删除病毒或一些其它的恶意程序，必须不断更新卡巴斯基反病毒 6.0 windows 工作站。“更新”组件正是为了实现此目的而设计的。它负责更新卡巴斯基反病毒 6.0 Windows 工作站的病毒特征库以及程序模块。

更新发布功能可以将从卡巴斯基实验室更新服务器上检索到的病毒特征库以及应用软件模块更新保存到本地文件夹中。然后允许网络中的其它计算机使用，从而节省了网络带宽。

报告、隔离和备份

每一保护组件、病毒搜索任务以及程序更新都会创建其运行报告。报告包含全部操作及其结果的信息。使用“*报告*”功能，您就可以保存卡巴斯基反病毒工作站所有组件的最新操作信息。如果出现问题，可以将报告发送给卡巴斯基实验室。这样，我们的专家就可以对问题进行深度分析，尽快地帮助您解决问题。

卡巴斯基反病毒工作站将所有被怀疑为危险的文件发送到专门的“*隔离区*”，并以加密的形式保存，以避免感染计算机。您可以对这些对象进行扫描，将其恢复到其原来的位置，删除或手动添加到“隔离”区。病毒扫描完成后，没有受感染的文件将自动恢复到其先前的位置。

“*备份*“区保留有被程序清除和删除的文件备份。创建这些备份文件以备您需要恢复文件或需要有关其感染病毒的信息时使用。这些备份文件也以加密的形式保存，以避免更大程度的感染。

您可以手动将文件由“备份”区恢复到其原来的位置并删除备份文件。

应急磁盘

卡巴斯基反病毒工作站提供了创建“应急磁盘”的功能。如果系统文件因病毒攻击而受损，并且无法启动操作系统时，“应急磁盘”可以提供备份计划。此时如果使用“应急磁盘”，您就可以启动计算机并将系统恢复到其受到恶意攻击前的状态。

支持

所有卡巴斯基反病毒软件的注册用户都可以获得我们的技术支持服务。欲了解如何获得技术支持的详细信息，请使用“*支持*”功能。

您可以使用这些链接访问卡巴斯基实验室用户论坛并可以看到一个常见问题列表，它可以帮助您解决问题。此外，您也可以填写网站上的那份表格，说明在应用卡巴斯基中所出现的问题或故障，并将其发送给“技术支持”。

您也可以使用在线“技术支持”服务，我们的员工也将随时通过电话帮助您解决问题。

1.3. 硬件和软件系统要求

要使卡巴斯基反病毒 6.0 Windows 工作站正常运行，则您的计算机必须满足以下最低要求：

常规要求：

- 50MB 可用磁盘空间
- CD-ROM (安装卡巴斯基反病毒 6.0 Windows 工作站光盘时使用)
- 微软 IE 5.5 或更高版本 (通过 Internet 更新病毒特征库以及程序模块)
- 微软 Windows Installer 2.0

Microsoft Windows 98, Microsoft Windows Me, Microsoft Windows NT Workstation 4.0 (Service Pack 6a):

- Intel Pentium 300 MHz 处理器或更高 (或兼容处理器)
- 64 MB 内存

Microsoft Windows 2000 专业版 (Service Pack 4 或更高), Microsoft Windows XP 家庭版, Microsoft Windows XP 专业版 (Service Pack 1 或更高)、 Microsoft Windows XP 专业 x64 版:

- Intel Pentium 300 MHz 处理器或兼容处理器
- 128 MB 内存

微软 Windows Vista、微软 Windows Vista x64:

- Intel Pentium 800 MHz 32 位 (x86)/ 64 位 (x64) 或更高 (或兼容)
- 512 MB 内存

1.4. 软件包

您可以从我们的代理商购买卡巴斯基反病毒 6.0 Windows 工作站盒装版，或从互联网商店，包括从 www.kaspersky.com.cn 的合作伙伴专区下载。

如果您购买的是盒装版的软件，则软件包将包括：

- 含有程序文件的密封安装盘
- 授权许可文件以及安装包或专门安装磁盘，或 CD 封套上的应用程序激活码。
- 用户指南
- 最终用户许可协议 (EULA)

打开安装盘密封套之前，请仔细阅读最终用户许可协议。

“最终用户许可协议”是您和卡巴斯基实验室之间达成的法律协议，它规定了您使用所购买的软件时应遵守的条款。

仔细阅读最终用户许可协议。

如果您不同意最终用户许可协议条款，则可以将所购盒装版产品退还给代理商，并且代理商将如数退还您购买软件所付的款项。如果这样的话，安装盘封套仍然必须是密封的。

如果打开安装盘封套，则意味着您接受最终用户许可协议的所有条款。

1.5. 注册用户支持

卡巴斯基实验室向注册用户提供一系列的服务，使卡巴斯基反病毒工作站更加高效运行。

激活本程序后，您将成为注册用户并在许可证到期前可以获得以下服务：

- 免费获得新版的卡巴斯基反病毒工作站
- 就有关软件安装、配置和运行的问题通过电话和电子邮件向卡巴斯基咨询
- 卡巴斯基实验室新产品发布和新病毒通知（本服务适用于订阅了卡巴斯基实验室新闻邮件的用户)

卡巴斯基实验室不提供操作系统使用和运行方面的技术支持或卡巴斯基以外的任何其它产品的技术支持。

第2章. 安装卡巴斯基反病毒 6.0 WINDOWS 工作站

您可以在计算机中完整或部分地安装卡巴斯基反病毒 6.0 Windows 工作站。

如果选择部分安装的话，您可以选择要安装的组件或只自动安装反病毒保护组件。您可以在以后安装程序的其它组件，不过将需要使用安装盘。建议您将安装盘上的文件复制到您的硬盘上。

您可以按照以下方式安装应用软件：

- 使用安装向导
- 从命令行窗口安装
- 使用卡巴斯基 管理工具(见卡巴斯基 管理工具使用指南)

2.1. 使用安装向导进行安装的程序

安装前，我们建议您关闭所有应有软件 (这也适用于使用卡巴斯基管理工具进行安装的情况)

要在计算机中安装卡巴斯基反病毒 6.0 Windows 工作站，请打开安装盘上的 Windows 安装程序文件。

注意：

从互联网上下载的带有安装程序包的程序的安装方法与从安装盘上安装程序的方法相同。

系统将显示程序的安装向导。每一窗口包含一组用以浏览安装规程的按钮。在此简要介绍一下其各自的功能：

- **下一步 –** 接受动作并向安装的下一步推进
- **上一步 –** 返回到到安装的上一步。
- **取消 –** 取消产品安装。
- **完成 –** 完成程序的安装步骤。

现在让我们详细说明一下安装步骤。

步骤 1. 检查系统是否符合安装卡巴斯基反病毒 6.0 Windows 工作站的要求

在计算机中安装本程序之前，安装程序会检查您的计算机的操作系统和升级包是否符合安装卡巴斯基反病毒 6.0 Windows 工作站的要求。同时还检查有无其它必要的程序并验证用户是否有权安装本软件。

如果系统不能满足这些要求，则程序会显示系统出错的消息。建议用户通过“**Windows 更新**”安装任何必要的升级包以及任何其它必要的程序，然后再安装卡巴斯基反病毒 6.0 Windows 工作站。

步骤 2. 安装欢迎窗口

如果系统完成满足所有的要求，则在您刚开始安装卡巴斯基反病毒 6.0 Windows 工作站时，在打开带有信息的安装程序文件后，系统会显示安装窗口。

要继续安装，点击“**下一步**”按钮。您可以点击“**取消**”按钮取消安装。

步骤 3. 查看最终用户许可协议

下一窗口包含您与卡巴斯基实验室之间达成的“最终用户许可协议”。仔细加以阅读，如果您同意协议的所有条款，则选择“**我接受许可协议条款**”，并点击“**下一步**”按钮。继续安装。

步骤 4. 选择安装文件夹

卡巴斯基反病毒 6.0 Windows 工作站安装的下一步将确定它安装在您计算机中的位置。**默认路径是：<Drive>\Program Files\Kaspersky Lab\Kaspersky Anti-Virus 6.0 for Windows Workstations .**

您可以点击“**浏览**”按钮，并在文件夹选择窗口选定文件夹，或在栏中输入文件夹的路径来指定不同的文件夹。

请记住，如果您手动输入安装文件夹的全称，则不能超过 200 个字符或包含特殊字符。

要继续安装，点击“**下一步**”按钮。

步骤 5. 选择安装类型

在此阶段，您可以选择程序所需安装的程度。有三种选项：

完整 如果选定此选项，则您将安装卡巴斯基反病毒 6.0 Windows 工作站的所有组件。将从错误！未找到引用源。开始安装。

自定义 如果选定此选项，则您将选定需要安装的程序组件。有关详细信息，请参见错误！未找到引用源。

反病毒组件 选定此选项后只安装病毒防护组件。不安装“反黑客”、“反垃圾邮件”、“反间谍”以及“主动防御”组件。

要选择设置类型，点击相应的按钮。

步骤 6. 选择要安装的程序组件

如果您选择“**自定义**”设置类型，则只能看到此步骤。

如果选择“自定义”安装，则您可以选择需要安装的卡巴斯基反病毒工作站的组件。默认情况下，选择所有保护组件以及使用卡巴斯基管理工具进行远程管理的网络代理插件。

欲选择需要安装的组件，双击组件名称旁边的图标并从右键菜单选择“ **将安装在本地硬盘上**”。您可以在程序安装窗口的下半部分找到更多有关所选组件的保护对象以及安装所需的磁盘空间的信息。

如果您不需要安装一个组件，则从右键菜单选择“**整个功能无效**”。请记住，如果选择不安装组件，则您将受到大量危险程序的威胁。

选择完需要安装的组件后，点击“**下一步**”。要返回到将要安装的默认程序列表，点击“上一步”。

步骤 7. 禁用 Microsoft Windows 防火墙

只有在启用了内置防火墙的计算机上安装卡巴斯基反病毒 6.0 Windows 工作站的“反黑客”组件时，才采取此步骤。

由于卡巴斯基反病毒 6.0 Windows 工作站的“反黑客”组件提供全面的防火墙保护，因此在此步骤中，卡巴斯基反病毒 6.0 Windows 工作站会询问是否需要禁用 Windows 防火墙。

如果需要将“反黑客”组件作为防火墙使用，请点击“**下一步**”。系统将自动禁用 Windows 防火墙。

如果需要使用 Windows 防火墙，则选择 “**保持启用 Windows 防火墙**”。如果选定此选项，则将安装“反黑客”组件，但不启用，以避免程序之间发生冲突。

步骤 8. 搜索其它反病毒程序

在此阶段，安装程序会搜索计算机上安装的其它反病毒产品，包括卡巴斯基实验室产品。这些产品可能会与卡巴斯基反病毒 6.0 Windows 工作站发生冲突。

安装程序将在屏幕上显示其检测到的此类程序的列表。继续安装前，本程序将会询问是否卸载此类程序。

您可以在检测到的反病毒应用程序列表中进行手动或自动卸载。

要继续安装，点击“**下一步**”按钮。

步骤 9. 完成程序的安装

在此步骤，本程序将要求您完成程序的安装。您可以决定是否需要使用基于上一版本的卡巴斯基反病毒 6.0 Windows 工作站的保护设置、病毒特征库以及反垃圾邮件组件 (例如，如果您已安装了 beta 版程序，而现在安装商业版程序)。

现在让我们详细说明一下如何使用上述选项。

如果您以前已安装了其它版本或 build 版的卡巴斯基反病毒 6.0 Windows 工作站，并且在将其卸载前保存了其病毒特征库，则您可以在当前版本的工作站中使用它。为此，复选 ☑ **病毒特征库**。带有程序安装的病毒特征库将不会复制到您的计算机中。

要使用已配置的并且由上一版本保存下来的保护设置，复选 ☑ **保护设置。**

同时如果您在卸载本程序的前一版本时已保存了“反垃圾邮件”组件，则建议您使用它。这样您就不必对“反垃圾邮件”组件进行设置。要使用已创建的反垃圾邮件组件，复选 ☑ **发垃圾邮件组件**

初次安装卡巴斯基反病毒 6.0 时，我们不建议取消选定 ☑ **安装前启用自我保护功能。**启用保护模块后，您就可以在安装本应用程序时出错的情况下退回到正确的安装。如果您试图重新安装本程序，则我们建议您取消选定该复选框。

> 如果通过“**远程桌面**”远程安装本程序，则我们建议不要复选标记 ☑ **安装前启用自我保护功能。**否则可能不能完成或正确完成安装程序。

要继续安装，点击“**下一步**”按钮。

步骤 10. 完成安装程序

“**完成安装**”窗口包含完成卡巴斯基反病毒安装程序的信息。

要启动设置向导，点击“**下一步**”。

成功完成安装后，您必须重新启动计算机，并且屏幕上会相应地予以提示。

2.2. 设置向导

完成安装后会启动卡巴斯基反病毒 6.0 Windows 工作站设置向导。它能够帮助您配置程序的初始设置，以适应您的计算机的特性并满足使用的需要。

“设置向导”界面类似标准的 Windows 向导。您可以使用“**上一步**”和“**下一步**”按钮进行各步骤的设置，或使用“**完成**”按钮完成设置。您随时可以使用“**取消**”按钮停止“设置向导”。

安装本程序时，如果关闭“向导”窗口，则可以跳过这一初始设置步骤。如果您以后恢复了卡巴斯基反病毒 6.0 Windows 工作站的默认设置，则可以从程序界面再次运行它。

2.2.1.1. 使用 **5.0** 版保存的对象

安装卡巴斯基反病毒 5.0 以上版本时系统会显示此向导窗口。系统会询问您将 5.0 版使用的哪些数据导入到 6.0 版中。这可能包括隔离、备份的文件或保护设置。

要在 6.0 版中使用这些数据，需选中必要的复选框。

2.2.2. 激活程序

激活程序前，务必确保计算机的系统日期设置与实际的日期和时间相匹配。

您可以通过安装授权许可文件激活程序。卡巴斯基反病毒 6.0 Windows 工作站检查授权许可文件并确定其有效期。

授权许可文件包含运行该程序所有功能所必须的系统信息以及其它信息。

- 支持信息 (提供程序技术支持的人员以及地点)
- 您的许可证名称、编号以及有效期

2.2.3. 选择激活程序的方法

安装授权许可文件可以激活程序。您在购买该产品时会获得授权许可文件。如果您没有获得许可文件，则您必须首先获取一个。为此，请访问卡巴斯基实验室激活服务器。 按照网页上的说明进行操作。

如果您想要安装了本程序的演示版后再决定是否购买商业版的话，可获取并安装试用的授权许可文件。它有一定的试用期限。为此，点击试用，并按照激活网站上的说明进行操作。

要激活该应用程序，请选择以下选项中的一项：

- **使用现有的授权许可文件。**使用先前获取的卡巴斯基反病毒 6.0 授权许可文件激活该应用程序。
- **稍后激活。**如果您选中该选项，则将跳过激活步骤。计算机中安装了卡巴斯基 6.0 Windows 工作站后，您就可以使用该程序除更新功能之外的所有功能。

2.2.3.1. 选择授权许可文件

如果您有卡巴斯基反病毒 6.0 Windows 工作站的授权许可文件，“向导”将会提示您是否需要安装该授权许可文件。如果需要的话，使用“**浏览**”按钮并在文件选择窗口选择带有*.key* 扩展名的授权许可文件的路径。

成功安装完授权许可文件后，在该窗口的下方您将可以看到授权许可信息。该软件注册人姓名、授权许可类型 (完全版、beta 测试版、演示版等等)，以及授权许可的有效期。

2.2.4. 完成程序激活

“设置向导”将提示您程序已成功激活。它还会显示所安装的授权许可文件的信息：该软件注册人姓名、授权许可类型 (完全版、beta 测试版、演示版等等)，以及授权许可的有效期。

2.2.5. 选择安全模式

在此窗口，“设置向导”会提示您选择程序运行时的安全模式：

基本保护 这是程序的默认设置，适用于对计算机或反病毒软件没有太多使用经验的用户。它将程序的所有组件按其推荐的安全级别进行设置，而且只在检测到恶意代码或执行危险活动等危险事件时才提示用户。

交互式保护 该模式在计算机数据的安全防御方面比“基本型模式”要更加专业化。它可以跟踪到试图修改系统设置的操作、系统中的恶意行为以及网络中的非授权活动。

恶意程序启动其中的任一行为或成为您使用的程序的标准活动。您必须逐一确定是否应该允许或阻断这些活动的发生。

如果选择该模式，则明确何种情况下应该使用：

- ☑ **启用反黑客学习模式**－计算机中安装的程序企图连接某些网络资源时会提示用户确认。您可以允许或阻断其连接并设置该程序的“反黑客”规则。如果您禁用“学习模式”，“反黑客”将在最低安全保护下运行，这意味着它允许所有的应用程序访问网络资源。

☑ **启用注册表防护** – 检测到试图修改系统注册表键的操作时提示用户作出反应

如果安装本程序的计算机运行的是 Microsoft Windows XP Professional x64 Edition、Microsoft Windows Vista、或 Microsoft Windows Vista x64，则将无法使用以下列出的交互式模式的设置。

☑ **启用应用程序完整性控制** – 模块试图载入受监控的应用程序时提示用户确认。

☑ **启用扩展的主动防御** – 分析系统的应用程序的所有可疑事件，包括使用命令行设置打开浏览器、注入应用进程以及 window hook 拦截器(默认情况下，不选择该选项)。

2.2.6. 配置更新设置

您的计算机安全直接取决于能否定期更新反病毒数据库以及程序模块。在此窗口，“设置向导”会提示您选择程序的更新模式并配置更新任务。

◉ **自动。**卡巴斯基反病毒 6.0 Windows 工作站能在指定时间自动检查更新源。病毒爆发期间，检查的频率会上升，而在病毒根除后，检查的频率会下降。如果发现有新的更新库，该程序会将其下载并安装到计算机中。这属于默认设置。

◉ **每天。**根据创建的任务自动更新。您可以点击“**编辑**”按钮设置任务。

◉ **手动。**如果您选中该选项，则将自行更新。

请注意，软件自带的反病毒数据库和程序模块在您安装程序时可能就已过期。因此我们建议您下载最新的更新程序。为此，点击 “**立即更新**”。卡巴斯基反病毒 6.0 Windows 工作站将从更新服务器下载必要的更新文件并将其安装到您的计算机中。

如果需要配置更新(设置网络属性、选择下载更新文件的来源或选择最近的更新服务器)，则点击“ **设置**”。

2.2.7. 配置病毒扫描任务

对计算机中选定区域进行恶意对象扫描时保护计算机安全的重要举措之一。

安装卡巴斯基反病毒 6.0 Windows 工作站时会创建三个默认的扫描任务：在此窗口，“设置向导”会提示您选择扫描任务设置：

启动对象

默认情况下，卡巴斯基反病毒启动后会自动扫描“启动对象”。您可以点击“**更改**”按钮，在另一窗口编辑任务属性。

关键区域

要自动扫描计算机中的关键区域 (系统内存、启动对象、引导扇形区、Windows 系统文件夹)，选中相应的复选框。您可以点击“**更改**”按钮设置任务。

禁用自动扫描默认设置。

我的电脑

要使计算机自动进行全面扫描，请选中相应的复选框。您可以点击“**更改**”按钮设置任务。

禁用定时执行该任务的默认设置。然而我们建议您在安装完本软件后立即对您的计算机进行全面的扫描。

2.2.8. 限制程序访问

由于可能有若干具有不同计算机水平的人使用同一台计算机，而且恶意程序可能会禁用安全保护，因此卡巴斯基反病毒提供了密码保护程序的选项。使用密码可使本软件免于禁用安全保护或更改设置的非法企图。

要启用密码保护，复选☑ **启用密码保护**并在**密码**和**确认新密码** 栏填写设定的密码。

选择下方需要密码保护的范围：

◉ 所有操作 (不包括警告通知)。如果用户需要操作此程序，则需要密码，但回应检测到危险对象通知时不需要密码。

◉ **选定的操作：**

- ☑ **保存程序设置 –** 用户试图保存程序设定更改时需要密码。
- ☑ **退出程序 –** 用户试图退出程序时需要密码。
- ☑ **停止/ 暂停保护组件和扫描任务 –** 用户试图暂停或完全禁用任何保护组件或扫描任务时需要密码。

2.2.9. 配置反黑客设置

反黑客是卡巴斯基反病毒 6.0 Windows 工作站组件，它可以保护本地网络以及互联网上的计算机安全。在此步骤，“设置向导”会提示您创建规则列表，以便为反黑客分析您的计算机网络活动时提供指南。

2.2.9.1. 确定安全区状态

在此步骤“设置向导”会分析您的计算机的网络环境。根据此分析将整个网络空间划分为几个区域：

互联网– 万维网 在此区域，卡巴斯基反病毒工作站起到个人防火墙的作用。这样，包过滤和应用程序的默认规则将控制所有网络活动，从而最大程度的确保安全。在此区域进行操作时您无法更改保护设置，但可以启用隐身模式以提高安全性。

安全区 – 某些区域很大程度上相当于包括您计算机在内的子网 (这可以是家中或工作单位的本地子网)。默认情况下，这些区域属于中等危险级别。您可以根据对某一子网的信任程度更改这些区域的状态，并且可以配置包过滤和应用程序的规则。

所有检测到的区域将显示在列表中。每一区域都列出了详细说明、地址、子网掩码以及反黑客允许或阻止的任何网络活动的程度。

- **互联网。**这是对互联网区域的一个默认状态设置，因为当您在线时，您的计算机会受到所有潜在威胁的影响。同时也推荐将不受反病毒程序、防火墙、过滤规则等保护的网络区域设置为此状态。当您选择此状态时，该程序会在您使用这个区域时给您最大程度的保护，特别是：
    - 阻止子网内的任何网络 NetBios 活动
    - 阻止允许在该子网内进行 NetBios 活动的应用程序和包过滤规则

  即使您已创建了共享文档夹，子网络中处于此状态的用户也不能使用该文件夹中的信息。此外，即使将该状态选定为某一子网络的设置，您也不能访问该子网络中的文件和打印机。
- **局域网。**该程序分析计算机的网络环境时，会指定以此状态访问侦测到的多数的安全区域 (除互联网外)。建议将具有中等危险程度 (例如企业局域网) 的区域设置为此状态。如果您选择此状态，该程序将允许：
    - 子网内的任何网络 NetBios 活动
    - 在子网内允许 NetBios 活动，允许应用和包过滤规则。

  如果您想要有权进入您计算机上的指定文件夹或打印机而阻止其它的网络活动，请选择此状态。
- **信任 (允许所有连接)。**将您认为绝对安全的网络设置为此状态，因此您的计算机与之连接时不会受到攻击，而且您的数据也不会被非法访问。使用此类网络时，允许所有网络的活动。即使您选择了“最大程度保护”并创建了阻止规则，它们也不会对可信任网络的远程计算机的活动起作用。

使用标注为 **Internet** 的网络时，您可以使用*隐身模式*以提高安全程度。该功能只允许您的计算机发起的网络活动，也就是说在周围的网络中看不到您的计算机。该模式不会影响用户计算机的上网活动。

当计算机作为一台服务器 (例如：邮件或 HTTP 服务器) 使用时，我们不推荐使用“隐身模式”。否则，连接到服务器的计算机不会将它作为一个连接。

要更改区域的状态或启用/禁用“隐身模式”，从列表中选择区域并使用下表**规则描述**栏中相应的链接。您可以执行类似的任务，并在**区域设置**窗口编辑地址和子网掩码。点击**编辑**可以打开区域设置窗口。

查看列表时可以添加新的区域。为此，点击**查找**。“反黑客”程序将搜索可用的网络，如果检测到，该程序将提示您选择其状态。此外，您也可以手动将新区域添加到列表中 (例如，如果您将笔记本连接到新的网络中)。为此使用**添加**按钮并在**区域设置**窗口填写必要的信息。

要删除列表中的网络，点击**删除**按钮。

2.2.9.2. 创建网络应用程序列表

“设置向导”对用户计算机上安装的软件进行分析，然后创建使用了网络连接的应用程序列表。

“反黑客”组件为每一应用程序创建控制网络活动的规则。使用通用网络应用程序模版应用规则。本软件包括这些由卡巴斯基实验室创建的模版。

您可以在反黑客设置窗口查看网络应用程序列表及其规则。点击**列表**可以打开反黑客设置窗口。

为提高网络安全，我们建议在使用 Internet 时禁用 DNS 缓存服务。DNS 缓存服务会大幅降低客户计算机与该有用 Internet 资源连接的时间，而且也极易影响客户计算机的安全。黑客利用 DNS 缓存服务可以建立数据漏洞，而使用防火墙是无法对这些数据漏洞进行跟踪的。因此要提高客户计算机的安全程度，建议禁用 DNS 缓存服务。

2.2.10. 设置向导完成

“设置向导”的最后一个窗口将提示您是否需要重新启动计算机，从而完成程序的安装。您必须重启计算机，以便注册卡巴斯基反病毒 6.0 Windows 工作站驱动。

有些程序组件只有在计算机重新启动后才能运行。

2.3. 使用命令提示安装程序

要安装卡巴斯基反病毒工作站，在命令提示中输入：

```
msiexec / i <package_name>
```

“安装向导”将开始工作。安装完程序后，您必须重新启动计算机。

安装该应用程序时，您也可以使用以下方法。

要在后台安装应用程序而不重新启动计算机 (安装后必须手动重启计算机)，输入：

```
msiexec / i <package_name> /qn
```

要在后台安装应用程序，然后重启计算机，则输入：

```
msiexec /i <package_name> ALLOWREBOOT=1 /qn
```

要在后台安装应用程序，并通过卡巴斯基管理工具安装密码保护，则输入：

```
msiexec /i <package_name> KLUNINSTPASSWD=****** /qn
```

2.4. 将 5.0 版升级到 6.0 版

如果您的计算机中已安装了卡巴斯基反病毒 5.0 Windows 工作站，则您可以将其升级到卡巴斯基反病毒 6.0 Windows 工作站。

启动卡巴斯基反病毒 6.0 Windows 工作站安装程序后，系统将让您选择首先卸载已安装的卡巴斯基 5.0 Windows 工作站。卸载完成后，您必须重启计算机，此后运行卡巴斯基 6.0 Windows 工作站安装程序。

警告！

当您从受密码保护的网络文件夹将卡巴斯基反病毒 5.0 升级到 6.0 时，卸载 5.0 后计算机将重启而不会安装 6.0。这是因为安装程序无权访问网络文件夹。要解决此问题，只要从本地文件夹运行安装程序就可以了。

第3章. 程序界面

卡巴斯基® 反病毒工作站拥有直观、用户友好的界面。本章节将讨论其基本的功能：

- 系统托盘图标
- 快捷菜单
- 程序主界面
- 程序设置窗口

除程序主界面外，还在以下程序中添加了保护插件：

- 微软 Outlook – 病毒扫描 (见 7.2.2 在 76 页) 和垃圾邮件扫描 (见 12.3.9 在 143 页)
- Outlook Express (见 12.3.10 在 146 页)
- The Bat! – 病毒扫描 (见 7.2.3 在 77 页) 和垃圾邮件扫描 (见 12.3.11 在 147 页)
- 微软 IE (见第 10 章在 100 页)
- 微软资源管理器

通过这些程序的界面对卡巴斯基反病毒工作站进行管理和设置，插件扩展了这些程序的功能。

3.1. 系统托盘图标

安装完卡巴斯基反病毒 6.0 Windows 工作站后，系统托盘中会显示该工作站图标。

该图标显示卡巴斯基反病毒工作站的功能。这个图标反映的是保护状态和显示运行任务数量。

如果图标是活动的 (颜色)，则表示您的计算机正受到保护。如果图标是不活动的 (黑白)，则表示完全停止对您的计算机的保护，或者暂停使用了一些组件 (见 1.2.1 在 13 页)。

卡巴斯基反病毒 6.0 Windows 工作站图标随着所执行的任务变化而变化。

	正在扫描电子邮件。

	正在扫描可执行脚本。
	正在扫描您或某程序正在打开、保存或运行的文件。
	正在更新卡巴斯基反病毒工作站的反病毒数据库和程序模块。
	卡巴斯基反病毒某组件出错。

也可以利用图标使用程序界面的基本功能：快捷菜单和主界面。

双击该程序图标可以打开快捷菜单。

双击该程序图标标可以直接打开程序主界面，看到默认的"**保护**"窗口。单击此图标，会打开您最后一次浏览的程序主界面。

3.2. 快捷菜单

您可以通过快捷菜单执行基本的保护任务。(见图 1)

图 1. 快捷菜单

卡巴斯基反病毒工作站菜单包含以下项目：

扫描我的电脑 – 对用户计算机进行全面的扫描。对包括可移动存储媒体在内的所有驱动器上的文件进行扫描。

病毒扫描– 选择对象并开始扫描 此默认列表包含：我的文档，启动文件夹、电子邮件数据库以及计算机上的所有驱动器等。您可以向列表中添加文件，选择要扫描的文件并开始扫描。

更新 – 下载反病毒数据库以及卡巴斯基工作站应用程序模块并安装到您的计算机上。

网络监控 – 查看已连接的网络连接，打开的端口和通信列表。

激活– 激活程序。此菜单项只有在程序是没有被激活时才会有。

设置 – 查看和修改卡巴斯基反病毒 6.0 Windows 工作站设置。

打开卡巴斯基反病毒 6.0 Windows 工作站– 打开程序主界面。

暂停保护/ 恢复保护 – 临时启用和禁用保护组件(见 1.2.1 在 13 页)。此菜单项是不影响更新以及病毒扫描任务的。

退出 – 关闭卡巴斯基反病毒 6.0 Windows 工作站。

如果运行病毒搜索任务，则快捷菜单将显示任务名称以及进度。您可以选择任务，打开报告窗口查看当前的运行结果。

3.3. 程序主界面

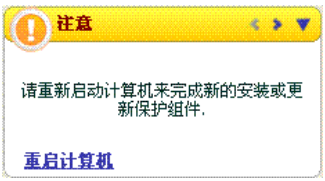
逻辑上，可以将卡巴斯基反病毒 6.0 Windows 工作站主界面 (见图 2) 划分为两部分：

- 左边窗口是导航面板，帮助您方便快速的找到并运行程序模块，执行扫描任务和获取程序的相关支持。
- 右边窗口是通知面板界面，它显示您在左边窗口选择组件的相关信息，您也可以通过这个窗口实现病毒扫描，隔离文件和备份文件，管理授权许可文件等操作。

图 2. 卡巴斯基反病毒 6.0 Windows 工作站主界面

选择左边窗口中的其中一个部分或组件后，右边窗口会出现选中界面的相关信息。

下面我们将详细介绍主界面导航面板上的这些组件。

程序主界面窗口	用途
通过该窗口主要是了解您的计算机的保护状态。“**保护**”窗口正是为了实现此目的而设计的。 	要查看卡巴斯基反病毒运行的总体信息，审核程序运行的总体统计数据并确保所有组件正常运行，请选择导航界面中的“**保护**”窗口。 在此您也可以启用或禁用保护组件。要查看具体保护组件的统计数据和设置，您只需选择想了解的“**保护**”窗口中的组件的名称。
使用主界面中专门的“**扫描**”窗口扫描您的计算机中的文件或程序。 	该窗口包含对象列表，可对该列表进行扫描。 您也可以在该窗口创建病毒扫描任务，并显示在导航面板上。该功能使扫描更加容易可行。 该窗口包含最常用而最重要的任务。其中包括对关键区域、启动程序以及整个计算机的扫描任务。
“服务”窗口包括卡巴斯基反病毒工作站的其它功能。 	在此您可以更新程序、卡巴斯基反病毒 6.0 Windows 工作站组件或任务的执行报告、使用隔离对象 和 备份件、技术支持信息、创建 应急磁盘 以及管理授权许可文件。
使用该应用程序时会出现“**提示和便签**”窗口。 	该窗口提供一些能提高计算机安全级别的技巧。也可以查找有关程序当前的运行及其设置的提示。此窗口中的链接会引导您采取推荐给特定窗口所采取的行动，或查看更多详细信息。

导航面板的每一界面都有一个专门的快捷菜单。该菜单包含保护组件和工具的指针，能帮助用户对其进行快速配置和管理以及查看报告。此外还有一个扫描和更新任务的菜单项，使用户可以通过修改现有的任务而创建自己的任务。

您可以生成和使用您自己的图片以及颜色配置来更改程序的界面。

3.4. 程序设置窗口

您可以通过主界面打开卡巴斯基反病毒 6.0 Windows 工作站设置窗口。为此，点击主界面上半部分中的设置。

设置窗口 (见图 3) 的布局与主界面的相似：

- 左边窗口帮助用户快捷地进入程序组件、病毒搜索任务以及程序工具设置。
- 右边窗口包含左边窗口所选项设置的详细列表。

选择设置窗口左侧中的任何窗口、组件或任务，在窗口右侧会显示其基本设置。您可以打开二级和三级设置窗口进行高级设置。在相应的窗口您可以查找到程序设置的详细描述。

图 3. 卡巴斯基反病毒 6.0 Windows 工作站设置窗口

第4章. 快速入门

卡巴斯基实验室研发了卡巴斯基反病毒 6.0 Windows 工作站的主要目标之一就是要为程序的每一选项提供最佳的配置。这就使对计算机具有不同熟练程度的用户在安装完本程序后能快捷地保护其计算机。

然后，您的计算机的配置信息或者根据您工作中的实际需要，可能有其具体的要求。因此我们建议进行初步的配置，这样能使您的计算机获得更加灵活和个性化的保护。

为使您能够快速入门，我们已将所有设置步骤集成在了一个“设置向导”中。该向导在完成程序安装后就会启动。按照“向导“的说明，您可以启动程序、配置更新、扫描、密码访问程序的设置，以及配置反黑客程序，从而符合您的网络属性的要求。

安装完并启动该程序后，我们建议您采取以下步骤：

- 检查当前的保护状态，确保卡巴斯基反病毒 6.0 Windows 工作站在适当的级别上运行。
- 使用反垃圾邮件的学习模式。
- 安装完该程序后如果“设置向导“没有自动启动，则更新该程序。
- 扫描电脑。

4.1. 保护的工作情况

主界面的“**保护**“窗口中提供了有关用户计算机的保护状态的全面信息。此处显示的是计算机*当前受保护的状态*以及当前程序*运行的情况统计*。

保护状态 使用专门的指示器显示计算机当前受保护的状态 (见 4.1.1 在 36 页)。统计数据 (见 4.1.2 在 39 页) 分析了程序当前进程。

4.1.1. 保护指示器

保护状态 由三个指示器来确定。每一指示器反映了某一时刻您的计算机的不同保护状态，并显示程序设置和运行方面的问题。

图 4. 反映计算机保护状态的指示器

每一指示器有三种可能的状态：

– *情况正常*；指示器显示您的计算机的保护状态符合要求，而且程序设置或运行没有问题。

– 卡巴斯基反病毒 6.0 Windows 工作站的运行与建议的运行级别相比出现一*次或多次偏差*，这可能影响到信息安全。请关注卡巴斯基实验室所建议的处理方式。

– *计算机安全处于危急状态*。请密切遵照建议改变您的计算机的安全保护。推荐的处理方式。

以下我们将详细说明这些保护指示器及其所显示的情况。

第一个指示器反映了计算机中存在恶意文件和程序的情况。该指示器的三个状态的含义如下：

	未检测到危险对象 卡巴斯基反病毒 6.0 Windows 工作站在您的计算机中未发现任何危险文件或程序。
	已处理所有危险对象 卡巴斯基反病毒 6.0 Windows 工作站已处理所有被感染文件和程序，并已删除可能无法处理的文件和程序。
	已删除危险对象 您的计算机存在受病毒感染的风险。卡巴斯基反病毒 6.0 Windows 工作站已检测到必须处理的恶意程序 (病毒、木马、蠕虫等)。为此使用全部处理链接。点击详细信息链接查看更多有关恶意对象的详细信息。

第二个指示器显示如何有效保护您的计算机。该指示器包含下列状态：

	*发布的反病毒数据库：(日期、时间)* 卡巴斯基反病毒 6.0 Windows 工作站使用的反病毒数据库以及程序模块都是最新版本的。
	*反病毒数据库已过期* 卡巴斯基反病毒工作站的反病毒数据库和程序模块已经有几天没有更新。您的计算机存在被恶意程序感染的可能性。这些恶意程序自从您上次更新程序以来就已出现。我们建议您更新卡巴斯基反病毒 6.0 Windows 工作站的反病毒数据库。为此使用更新链接。
	反病毒数据库部分受损 反病毒数据库部分受损。如果受损，建议重新运行程序更新。如果再次碰到同样出错消息，请联系“卡巴斯基实验室技术支持”。
	请重新启动计算机 为使程序正常运行，您必须重启计算机。保存和关闭所有您正在使用的文件并使用重启计算机链接。
	禁用程序更新 禁用反病毒数据库和程序模块更新服务。为保障计算机受到实时的保护，建议启用更新功能。
	*反病毒数据库过于陈旧* 卡巴斯基反病毒工作站已有段时间没有更新。您的计算机存在很大风险。请及时更新程序。为此使用更新链接。
	反病毒数据库受损 反病毒数据库文件部分受损。如果受损，建议重新运行程序更新。如果再次碰到同样出错消息，请联系“卡巴斯基实验室技术支持”。

第三个指示器显示的是程序运行的当前功能。该指示器包含下列状态：

	*所有保护组件都在运行*

	卡巴斯基反病毒 6.0 Windows 工作站在所有恶意程序可能渗透的信道保护用户计算机的安全。启用所有保护组件。
	未安装保护组件 安装卡巴斯基反病毒 6.0 Windows 工作站时，未安装监控组件。这意味着您只能扫描病毒。为了更大程度地提高计算机安全，应安装保护组件。
	*暂停所有保护* 已暂停所有保护。要恢复保护，右键点击系统托盘图标选择“**恢复保护**”。
	禁用部分保护组件 禁用一个或几个保护组件。这会导致您的计算机感染病毒并丢失数据。强烈建议您启用保护组件。为此，选择列表中未启用组件并点击  .
	禁用所有保护组件 完全禁用保护组件 未运行保护组件 要恢复保护，右键点击系统托盘图标选择“**恢复保护**”。
	*一些保护组件出错* 卡巴斯基反病毒 6.0 Windows 工作站的一个或多个保护组件内部出错。如果出现这种情况，建议您启用保护组件或重启计算机，因为组件驱动程序经更新后可能被注册。

4.1.2. 卡巴斯基反病毒 6.0 WINDOWS 工作站组件状态

要确定卡巴斯基反病毒 6.0 Windows 工作站是如何保护您的文件系统、电子邮件、HTTP 通信或危险程序可能渗透您的计算机的其它区域，或查看病毒扫描任务或反病毒数据库更新进程，只需打开程序主界面的相应窗口就可以了。

如要查看当前的“文件保护”状态，选择主界面左侧窗口上的“**文件保护**”，如要查看计算机能否防范新病毒，可选择“**主动防御**”。右侧窗口将显示个组件的完整信息。

对于保护组件，右侧窗口包含“**状态条**”，“**状态**”窗口和“**统计**”窗口。

“文件保护”组件的“*状态条*”显示如下：

- *文件保护：正在运行* – 文件保护在运行。
- *文件保护：暂停* – 文件保护在指定时间内被禁用。指定时间或重启程序后，该组件将自动恢复运行。您也可以点击状态条上的 按钮手动恢复文件保护。
- *文件保护：停用* – 用户已停用该组件。您可以点击状态条上的 按钮手动恢复文件保护。
- *文件保护：没有运行* – 由于某些原因，文件保护未运行。例如您没有程序的许可文件。
- *文件保护：禁用 (出错)* – 组件出错。您需要联系“卡巴斯基实验室技术支持”。

如果该组件包含几个模块，则“**状态**”窗口将显示各个模块的状态信息。对于没有单独的模块的组件，会显示其状态，安全级别，对于其中的一些组件，还会显示危险程序的响应情况。

病毒扫描和更新任务没有“**状态**”窗口。“**设置**”窗口中会列出安全级别、危险程序的病毒扫描活动以及更新的运行模式。

“**统计**”窗口包含保护组件运行、更新或扫描任务的信息。

4.1.3. 程序执行统计

在主界面的保护窗口的“**统计**”窗口可以找到自从安装卡巴斯基反病毒工作站后计算机保护记录的信息。

图 5. 程序统计窗口

您可以左键点击窗口任何位置来查看详细信息。标签显示：

- 已查找到的对象信息 (见 16.3.2 在 185 页) 及其状态
- 事件日志 (见 16.3.3 在 186 页)
- 全盘扫描统计(见 16.3.4 在 188 页)

- 程序执行设置(见 16.3.5 在 188 页)

4.2. 如何扫描计算机上的病毒

程序安装完成后，将会在应用程序窗口的左下方特别提示您，计算机还没有进行扫描，并建议您立即进行全盘扫描。

卡巴斯基反病毒 6.0 Windows 工作站程序主界面的“**扫描**”窗口设有计算机扫描任务。

选择扫描“我的电脑”后，右侧面板将显示如下信息：最近计算机扫描的统计数字、任务设置、选择的保护级别以及如何处理危险对象。

要扫描计算机上的恶意程序，

点击窗口左侧的“**扫描**”按钮。

随后程序开始扫描计算机，并且相关信息显示在指定的窗口中。点击“**关闭**”按钮，将隐藏进程窗口，但不会停止扫描。

4.3. 如何扫描计算机的关键区域

从安全角度看，计算机中有些区域是非常关键的。它们是恶意程序攻击的首要目标，其目的在于破坏您的操作系统、处理器、内存等计算机硬件。

保护关键区域，对维护您计算机正常运转非常重要。我们为此在程序主界面的“**扫描**”窗口建立了专门用来扫描关键区域的任务。

选择“**关键区域**”任务后，主界面的右侧面板将显示如下信息：这些区域最近扫描的统计数字、任务设置、选择的保护级别以及如何处理安全威胁。您也可以选择需要扫描的关键区域并立即对其进行扫描。

要扫描计算机关键区域上的恶意程序，

点击窗口左侧的“**扫描**”按钮。

随后程序开始对所选区域进行扫描，并且相关信息显示在指定的窗口中。点击“**关闭**”按钮，将隐藏进程窗口，但不会停止扫描。

4.4. 如何扫描文件、文件夹或磁盘

有些情况下有必要进行单个对象扫描而非全盘扫描。例如您的硬盘的某个区上有程序、游戏、带回家的电邮数据库、以及存档文件、邮件附件等。您可以利用微软 Windows 操作系统的标准工具 (例如**资源管理器窗口**或**桌面**等等) 选择扫描对象。

要扫描对象，

将光标放到所选对象的名称上， 点击鼠标右键打开快捷菜单，然后选择**扫描病毒** (见图 6)。

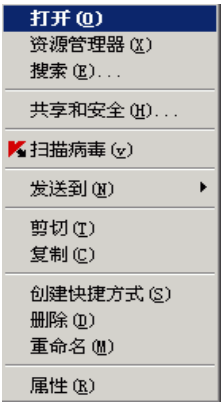


图 6. 使用标准的 Windows 快捷菜单选择扫描对象

随后程序开始对所选对象进行扫描，并且相关信息显示在指定的窗口中。点击“**关闭**”按钮，将隐藏进程窗口，但不会停止扫描。

4.5. 如何使用反垃圾邮件学习功能

快速入门的其中一项就是要使反垃圾邮件学习处理您的电子邮件并过滤掉垃圾邮件。“Spam”就是垃圾邮件，尽管用户难以说清什么是垃圾邮件。尽管有些电子邮件可以划为垃圾邮件，而且具有高度的准确性和代表性 (例如大规模投递的电邮、广告等)，但是有些用户可能需要接收这样的邮件。

因此我们会提示您来决定哪些时垃圾邮件而哪些不是。卡巴斯基反病毒 6.0 Windows 工作站在安装完后会提示您是否要使反垃圾邮件程序学习区分垃圾邮件和正常邮件。您可以使用嵌入邮件客户端 (Microsoft Outlook、Outlook Express、The Bat!)的特定按钮或专门的学习向导来使用反垃圾邮件的学习功能。

警告！

此版的卡巴斯基反病毒工作站不提供 64 位邮件客户端 (Microsoft Office Outlook, Microsoft Outlook Express 或 The Bat!) 的反垃圾邮件插件。

要使用邮件客户端上的插件按钮来进行反垃圾邮件学习，

1. 打开您的默认邮件客户端 (例如 Microsoft Office Outlook)。在工具栏上您可以看到两个按钮：**垃圾邮件**和**非垃圾邮件**。
2. 选择一封正常邮件或一组正常邮件，然后点击**非垃圾邮件**。从这时开始，您选择的发送人的邮件地址将不会被认为是垃圾邮件。
3. 选择一封或一组您认为的垃圾的邮件或邮件文件夹，点击**垃圾邮件**按钮。反垃圾邮件程序将分析这些邮件的内容，并且以后将所有含有类似内容的邮件视为垃圾邮件。

要使用“学习向导”进行发垃圾邮件学习，

1. 选择程序主界面的“**保护**”窗口上的“反垃圾邮件”，点击“**设置**”。
2. 点击设置窗口右侧上的“**学习向导**”。
3. 在步骤 1，从含有非垃圾邮件的邮件客户端选择文件夹。点击“**下一步**”按钮。
4. 在步骤 2，指定垃圾邮件文件夹。点击“**下一步**”按钮。

这个学习过程是基于您所指定的文件夹的。

当邮件到达您的邮箱时，反垃圾邮件将扫描邮件内容并在垃圾邮件的主题添加[Spam]标签。您也可以在邮件客户端为垃圾邮件指定处理规则删除或移动它们到指定的文件夹中。

4.6. 如何更新程序

卡巴斯基实验室提供专门更新服务器为卡巴斯基反病毒 6.0 windows 工作站更新反病毒数据库以及应用程序模块。

*卡巴斯基实验室更新服务器*是存储程序更新的卡巴斯基实验室互联网网站。

警告！

您需要连接互联网来更新卡巴斯基反病毒 6.0 Windows 工作站。

默认情况下，卡巴斯基反病毒 6.0 Windows 工作站自动从卡巴斯基实验室服务器检测更新。如果卡巴斯基实验室发布了新的更新文件，卡巴斯基反病毒 6.0 Windows 工作站将下载并以自动模式进行安装。

要手动更新卡巴斯基反病毒 6.0 Windows 工作站，

在程序主界面的“**服务**”窗口选择“**更新**”，并点击该窗口右侧的“**立即更新！**”按钮。

随后卡巴斯基反病毒 6.0 Windows 工作站将开始更新并在指定窗口显示更新进程的详细信息。

4.7. 如果保护出错时，应如何操作。

运行任何保护组件时如果出现问题或出错，务必要检查其状态。如果组件状态为*没有运行*或*禁用* (*操作错误*)，请尝试重启程序。

如果重启程序不能解决问题，我们建议使用程序恢复功能解决可能的出错。

如果恢复功能也不能解决的话，请联系“卡巴斯基实验室技术支持”。请将组件运行报告或整个应用程序运行报告保存到文件中并发送它到卡巴斯基技术支持，它将帮助技术支持了解问题的原因。

如何将报告保存到文件中：

1. 选择程序主界面的“**保护**”窗口上的组件，并在“**统计**”窗口任何地方点击左键。
2. 点击“**另存为**”按钮并在窗口中指定组件运行报告文件名。

如何一次性全部保存卡巴斯基反病毒 6.0 Windows 工作站组件 (保护组件、病毒扫描任务、支持功能) ：

1. 选择程序主界面的“**保护**”窗口，并在“**统计**”窗口任何地方点击左键。

   或者

   点击报告窗口中任何组件的全部报告。然后“报告”标签会列出所有程序组件的报告。
2. 点击**另存为**按钮并在打开的窗口指定该程序运行报告的文件名。

第5章. 保护管理系统

卡巴斯基反病毒工作站提供多任务的计算机安全管理：

- 启用、禁用或暂停程序
- 卡巴斯基反病毒 6.0 Windows 工作站定义危险程序类型来保护您的计算机
- 为保护组件创建排除列表
- 创建您自己的病毒扫描和更新任务
- 配置病毒扫描任务
- 为反病毒保护配置常规 (productivity) 设置

5.1. 在计算机上停止和恢复保护

默认情况下，卡巴斯基反病毒会在系统启动时启动，并为您的计算机提供全程的保护。屏幕右上角的*卡巴斯基反病毒 6.0* 字样会提示您该程序已启动。所有保护组件(见 1.2.1 在 13 页) 都在运行之中。

您可以全部或部分禁用卡巴斯基反病毒 6.0 Windows 工作站所提供的保护组件。

警告！

卡巴斯基实验室强烈建议您**不要禁用保护**，否则可能会导致您的计算机感染病毒并继而丢失数据。

请注意，这里讨论的是保护组件的保护功能。禁用或暂停保护组件不影响病毒扫描任务的执行或程序的更新。

5.1.1. 暂停保护

暂停保护是指暂时禁用所有对计算机中文件、收发的邮件、可执行脚本、应用程序的行为以及反黑客和反垃圾邮件进行监控的组件。

如何暂停运行卡巴斯基反病毒工作站：

1. 选择快捷菜单中**暂停保护**。
2. 在打开的“暂停保护”窗口 (见图 7) 选择何时恢复保护：
    - **在 <时间间隔>** – 程序将在该指定时间后恢复保护。使用下拉菜单选择时间间隔。

- **下次程序重启时**–从“开始”菜单打开程序或重启计算机后恢复保护。(只要将程序设定为在开机后自动启动 (见 5.1.5 在 48 页)。
- **仅限于用户要求** – 除非您手动启动保护，否则保护不会再启动。要启用保护，选择程序快捷菜单上的**恢复保护**。

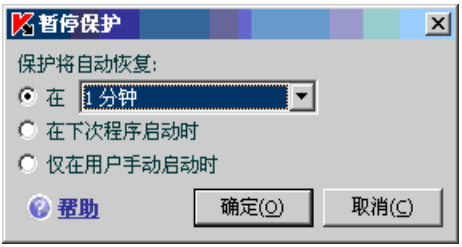


图 7. 暂停保护窗口

提示：

使用以下方法同样也可以停止保护：

- 点击**保护**窗口上的 ▮▮按钮。
- 选择快捷菜单上的**退出**。此时程序将从计算机内存中退出。

如果暂停保护，将暂停所有保护组件。其显示如下：

- 主界面**保护**窗口中禁用组件的名称显灰。
- 系统托盘图标显灰。
- 第三个保护指示器 (见 4.1.1 在 36 页) 显示为  **暂停所有保护组件。**

5.1.2. 停止保护

停止保护是指完全禁用保护组件。但病毒扫描和更新任务不受影响。

停止保护后，只有用户才能恢复保护。系统或程序重启后，保护组件也不会自动恢复。请记住， 如果卡巴斯基反病毒 6.0 Windows 工作站与安装在您计算机中的其它程序有冲突，您可以暂停部分组件或 创建排除列表。

如何停止所有保护：

1. 打开卡巴斯基反病毒 6.0 Windows 工作站主界面。
2. 选择**保护**窗口并点击“设置”链接。

3. 在程序设置窗口取消 **启用保护**。

禁用保护后将停止所有保护组件。其显示如下：

- 主界面**保护**窗口中禁用组件的名称显灰。
- 系统托盘图标显灰。
- 第三个保护指示器 (见 4.1.1 在 36 页) 显示为 **禁用所有保护组件。**

5.1.3. 暂停或停止保护组件和更新任务

这里介绍几种停止保护组件、病毒扫描或更新的方法。然而在此之前，强烈建议您确定想要停止的原因。因为可能有其它的方法可以解决问题，例如更改安全级别等。例如您的工作要使用到数据库并且您确信它们没有病毒，就可以将数据库文件添加为排除。

如何暂停保护组件、病毒扫描以及更新任务：

选择主界面左侧上的组件或任务，并点击状态栏上的 按钮。

组件或任务状态将更改为 ***暂停***。该组件或任务将暂停直至点击 按钮将其恢复。

当暂停一个组件或任务时，将保存卡巴斯基反病毒 6.0 Windows 工作站当前进程的统计信息并且更新完该组件或任务后，将继续记录。

如何停止保护组件、病毒扫描以及更新任务：

点击**状态栏**上的 按钮。您也可以取消**通用**窗口上的 **启用 <组件名>** 停止程序设置窗口上的保护组件。

组件或任务状态将更改为 *停止 (禁用)*。该组件或任务将停止直至点击 按钮将其启用。如果是病毒扫描和更新任务，您可以选择以下选项：继续被中断的任务或者重新开始。

停止一个组件或任务时，将会清除所有以前运行的统计信息，并且启用该组件后重新开始记录。

5.1.4. 恢复保护

如果有时暂停或停止保护，您可以使用以下方法恢复保护：

- 从快捷菜单恢复。

  为此，点击 **“恢复保护”**。

- 从程序主界面恢复。

为此，点击主界面“**保护**”窗口上状态栏的 ▶ 按钮。

保护状态随即更改为***运行***。程序的系统托盘图标高显 (颜色)。第三个保护指示器 (见 4.1.1 在 36 页) 也将提示您 **启用所有保护组件**。

5.1.5. 关闭程序

如需关闭卡巴斯基反病毒 6.0 Windows 工作站，从程序的快捷菜单选择**退出**。这个程序将关闭，您的计算机将处于不受保护状态。

如果关闭程序时程序监控的网络是连接的，则屏幕上会出现通知，显示将中断该连接。这对正常关闭程序来说是必要的。10 秒后或点击**是**按钮将自动中断连接。多数的连接将在短暂时间之后恢复。

请注意，中断连接时如果您没有使用下载管理器下载文件，该文件将丢失。您将需要重新下载文件。

您可以点击通知窗口上的按钮选择不中断连接。这样程序将继续运行。

关闭程序后，您可以通过打开卡巴斯基反病毒 6.0 Windows 工作站启用计算机保护 (**开始→ 程序 → 卡巴斯基反病毒 6.0 Windows 工作站 →卡巴斯基反病毒 6.0 Windows 工作站**)。

您重启操作系统后，也可以自动恢复保护。要启用该功能，在程序设置窗口选择“**保护**”窗口并复选**在系统启动时运行卡巴斯基反病毒 6.0 Windows 工作站。**

5.2. 受监控的恶意程序类型

卡巴斯基反病毒 6.0 Windows 工作站使您远离各种类型的恶意程序。无论您如何设置，该程序总是能够扫描和处理病毒、木马以及后门程序。这些程序可能会对您的计算机造成巨大破坏。为使您的计算机更加安全，您可以使该程序监控其它类型的危险程序，从而扩展威胁列表。

要选择卡巴斯基反病毒 6.0 Windows 工作站防御何种恶意程序，选择程序设置窗口上的“**保护**”窗口。

恶意软件种类复选框保护下列威胁类型：

- **病毒、蠕虫、木马、黑客工具**。该组都是最普遍、最危险的恶意程序。这是最小的安全级别。根据卡巴斯基实验室专家的建议，卡巴斯基反病毒软件要始终监控这类的恶意程序。
- **间谍软件、恶意广告软件、拨号软件**。该组程序是潜在的危险软件，可能会给用户带来不便或造成严重破坏。

☑ **潜在的危险软件**。该组包括的不是恶意或危险的程序。然而某些情况下可能会被利用来破坏您的计算机。

上一组包括程序在扫描对象时检测到的各种威胁。

如果将所有组都选上，卡巴斯基反病毒 6.0 Windows 工作站就能为您的计算机提供提供最全面的病毒保护。如果禁用第二和第三组，则该程序只能保护您的计算机远离最普通的恶意程序。它没有包含潜在的危险程序和其它可能被安装在您计算机上损害您文件的程序，窃取您的金钱或者浪费您的宝贵的时间。

卡巴斯基实验室不建议您禁用第二组监控。如果卡巴斯基反病毒 6.0 Windows 工作站认为某程序是潜在危险程序而您持反对态度的话，我们建议您将它添加到排除列表中。

5.3. 创建信任区域

信任区域是用户创建的对象列表，其对象是不受卡巴斯基反病毒 6.0 Windows 工作站监控的。换句话说，它是一组不受保护的程序。

用户基于其所使用的文件的属性及其计算机上安装的程序创建受保护区。您可能要创建一个这样的排除列表，例如卡巴斯基反病毒 6.0 Windows 工作站阻止访问目标或程序并且您确信这个文件或程序是绝对安全的。

您可以通过文件格式、文件包含的关键字、或根据扫描期间该程序赋予对象的状态排除某些区域 (例如一个文件夹或程序) 、程序进程或对象进行扫描。

警告！

不扫描排除对象，但此时要扫描其所在的磁盘或文件夹。然而如果您选择了具体的对象，则排除规则将不适应。

为创建排除列表，

1. 打开卡巴斯基反病毒 6.0 Windows 工作站设置窗口，选择“**保护**”窗口。
2. 点击“**常规**”窗口中的“ **排除码** ”按钮。
3. 配置对象排除规则，并在打开的窗口中创建可信任应用程序列表 (见图 8)。

图 8. 创建可信任区域

5.3.1. 排除规则

排除规则是一组卡巴斯基反病毒 6.0 Windows 工作站用以确定不扫描对象的条件。

您可以通过文件格式、文件包含的关键字、或根据判定中的规定排除某些区域 (例如一个文件夹或程序) 、程序进程或对象进行扫描。

*判定*是卡巴斯基反病毒 6.0 Windows 工作站在扫描期间赋予对象的状态。判定实际上利用卡巴斯基实验室病毒百科全书上定义的恶意程序或潜在的威胁行为特征来排除扫描的。

有潜在危险软件不具有恶意功能，但由于它存在漏洞和错误，因此可能会被作为恶意软件的一部分来使用。这类软件包括远程管理程序， IRC 客户端， ftp 服务，通用的停止或隐藏进程的工具，键盘记录器，密码破解程序， 自动拨号软件等。这些程序不是病毒。但可以将它们划分为几种类型，例如恶意广告软件、玩笑程序、恶意软件等 (有关卡巴斯基反病毒 6.0 Windows 工作站检测到的潜在危险程序的更多信息，可访问 www.viruslist.com 上的病毒百科全书)。扫描后，可以阻止这

些程序。由于它们中的几个十分普通，因此您可以选择将其排除扫描。为此您必须指定赋予该程序排除扫描的判定。

例如，想象您在工作中经常需要使用“远程管理”程序。这是个远程访问系统，通过它，您利用远程计算机就可以工作。卡巴斯基反病毒 6.0 Windows 工作站将此类应用程序活动视为潜在的危险，并可能加以阻止。要防止此类应用程序被阻止使用，您必须创建排除规则，将 *非病毒:RemoteAdmin.Win32.RAdmin.22* 指定为判定。

添加排除对象时，创建若干程序组件 (文件保护、邮件保护、主动防御) 以及病毒扫描任务以后可使用的排除规则。您可以在从程序设置窗口、检测到危险对象的通知窗口以及报告窗口打开的窗口中创建排除规则。

*要在**排除规则**标签页添加排除对象：*

1. 在**排除码**标签页中点击**添加**按钮。
2. 在打开窗口中 (见图 9) 的**属性**窗口点击排除类型：

对象 – 在扫描中排除包含某一类字符的某些对象、目录或文件。

判定 – 根据病毒百科全书中规定的安全威胁特征来排除对象。

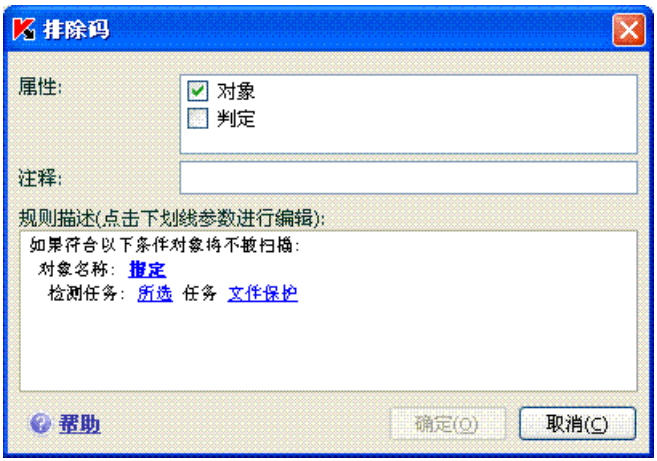


图 9. 创建排除规则

如果您同时选中这两个复选框，将要创建的规则要使用指定判定。在此情况下，要应用以下规则：

- 如果您将某文件指定为**对象**并在**判定**窗口指定了某一状态，则指定的文件只有在扫描期间归为选定的威胁才会被排除扫描。

- 如果您将一区域或文件夹选定为**对象**，并选定了**判定**的状态 (或判定类型)，则符合该状态条件的对象只有在扫描该区域或文件夹时才会排除扫描。

3. 为选定的排除类型赋值。为此左键点击**规则描述**窗口上排除类型旁的指定链接：

   - 对于**对象**类型，在打开的窗口输入其名称(这可以是文件、特定的目录或关键字。设置对象 (文件、关键字、文件夹) 时，选中 **包含子文件夹。**我们在对文件夹进行排除的同时，也可以排除它所包含的所有子文件夹。例如，如果您指定 **C:\Program Files\winword.exe** 是一个排除对象并且选中扫描子文件夹选项，在 **C:\Program Files** 的子文件夹下有任何的 **winword.exe** 都将被排除。

   - 在设置**判定**时，您可以使用“病毒库百科全书”中完整的威胁名称，也可以使用威胁包含的关键字来进行排除。

     对有些判定，您可以**高级设置**栏里应用高级排除条件。大多数情况下，在您从“主动防御通知”中添加排除规则时会自动填写该栏。

     您可以为以下判定添加高级设置：

     侵入者。对于该判定，您可以为嵌入对象 (例如一个.dll 文件) 提供一个名字，关键字或者全部的路径，以此作为附加的排除条件。

     打开互联网浏览器。对于该判定，您可以在浏览器的设置列表中添加排除设置。
     例如您可以阻止打开具有“主动防御”应用程序活动分析中某些设置的浏览器。然而，您想要允许该浏览器访问与 Microsoft Office Outlook 有链接的 *www.kasperky.com.cn*，并以此作为排除规则。为此，将 Microsoft Office Outlook 选定为排除**对象**，将打开互联网浏览器选定为**判定**，并在**高级设置**栏输入允许的区域。

4. 定义卡巴斯基反病毒 6.0 Windows 工作站的哪些组件将使用该规则。如果选择任何组件的话，则该规则将适用于所有组件。如果您要一个或若干个组件限于使用该规则，则点击任何组件，它将会更改为所选组件。在打开的窗口中，选中您想要应用排除规则的组件复选框。

如何在确定检测到威胁对象的程序通知窗口中创建排除规则：

1. 在通知窗口使用链接 (见图 10)。

2. 在打开的窗口中确保所有的排除规则设置符合您的要求。该程序将按照通知中的信息自动填入对象名和安全威胁类型。要创建规则，请点击**跳过**。

图 10. 危险对象检测通知

如何从保护窗口创建排除规则：

1. 在报告窗口，选择您想要添加到排除列表的对象。
2. 打开快捷菜单并选择**添加到信任区域** (见图 11)。
3. 然后会打开排除设置窗口。确保所有的排除规则设置符合您的要求。该程序将按照报告中的信息自动填入对象名和安全威胁类型。要创建规则，请点击**确定**。

图 11. 在报告中创建排除规则

5.3.2. 信任程序

如果您的计算机上运行的是 Microsoft Windows NT 4.0/2000/XP/Vista 操作系统，则卡巴斯基反病毒程序只能排除信任程序扫描。

卡巴斯基反病毒 6.0 Windows 工作站可以创建信任程序列表，列表中的文件或网络活动不会受到监控、怀疑。

例如，您认为 Windows 记事本使用的对象和进程是安全的，不必进行扫描。要使这些进程使用的对象不受扫描，则将**记事本**添加到信任程序列表中。然而可执行文件和信任程序进程将和以往一样将被扫描。要使该程序完全不被扫描，必须使用排除规则 (见 5.3.1 在 50 页)。

此外，对许多程序来说，一些归为危险的活动是它们的正常功能。例如键盘布局切换程序经常会干扰键盘输入的文字。要适应这样的程序并停止对其活动进行监控，建议您将其添加到信任程序列表中。

用信任程序排除可以同样解决卡巴斯基反病毒 6.0 Windows 工作站与其它应用程序的冲突问题例如，与其它计算机的网络连接已经被反病毒应用程序扫描) 以及优化计算机性能，当使用服务器软件时这是非常重要的。

在默认情况下，卡巴斯基反病毒 6.0 Windows 工作站扫描程序进程打开、运行或保存的对象，并对所有程序的活动及其生成的网络流量进行监控。

您可以在指定的**信任程序**标签页上创建信任程序列表 (见图 12)。默认情况下该列表包含程序列表，按照您安装卡巴斯基反病毒程序时卡巴斯基实验室的建议，列表中的程序将不会受到监控。如果您不信任列表中的程序，则可以取消选定相应的复选框。您可以使用右侧的**添加**、**编辑**和**删除**按钮编辑该列表。

图 12. 信任程序列表

如何向信任程序列表添加程序：

1. 点击该窗口右侧的“**添加**”按钮。
2. 使用**浏览**按钮在打开的**信任程序**窗口 (见图 13) 选择程序。快捷菜单打开，点击**浏览**后可以进入文件选择窗口，然后选择可执行文件路径，或点击**应用程序**后进入当前运行的应用程序列表，然后就需选择。

图 13. 将应用程序添加到信任列表

在您选择程序时，卡巴斯基反病毒 6.0 Windows 工作站会记录可执行文件的内部属性并在扫描期间将其用于识别信任程序。

您在选择文件名时会自动插入文件路径。

3. 指定该进程的哪些活动将不受监控：

   不扫描已打开文件 – 不扫描信任程序处理的所有文件。

   不控制程序活动 – 从主动防御中排除信任程序一些行为，可疑或其它方面的活动。

   不控制注册表访问 – 当信任的应用程序访问系统的注册表时它将不被扫描。

   不扫描网络通信量 – 排除对信任程序生成的任何网络通信量的病毒和垃圾邮件扫描。您可以排除扫描程序的所有网络通信量或加密的通信量 (SSL)。为此点击所有链接。它将更改为加密。除此之外，您还可以通过指定远程主机或端口限定排除扫描。要创建一个限制，点击任何 (远程主机或端口) 后将更改为选定的 (远程主机或端口)，然后输入确切的主机或端口。

   请注意，如果选中 **不扫描网络通信量，** 则只对该程序的通信量进行病毒和垃圾邮件扫描。然而这不会影响反黑客的扫描监控。反黑客设置控制着对该程序的网络活动的分析。

5.4. 配置有权运行任务的帐户

卡巴斯基反病毒 6.0 Windows 工作站的一个功能就是可以授权其它用户启动扫描任务。默认情况下，该功能时禁用的，导致任何登陆您系统的用户都可以运行扫描任务。

该功能十分有用，比如您在扫描期间需要有权使用某个对象时。使用该功能，您可以配置有权限运行此任务的用户。

请注意，使用 Microsoft Windows 98/ME 的计算机没有此选项。

可以从您无权访问 (例如网络更新文件夹) 的更新源或有授权用户的代理服务器进行程序更新。您可以通过另一个授权帐户使用该功能来运行“更新程序”。

如何配置不同的授权用户启动扫描任务：

1. 选择（病毒）扫描窗口上或主界面的（更新和更新发布任务）“服务”窗口上的任务名，并使用设置链接打开任务设置窗口。
2. 点击任务设置窗口上的**配置**按钮后进入打开的窗口的**附加设置**标签页 (见图 14)。

要启用该功能，选中 **运行这个任务**。在文本框中输入运行该任务的：用户名和密码。

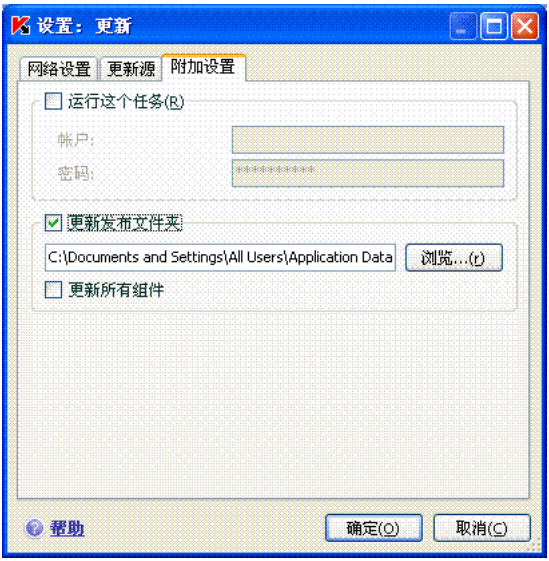


图 14. 通过其它授权帐户配置更新任务。

5.5. 配置任务计划

您可以使用手动计划或自动运行病毒扫描、更新以及更新发布任务。

应用程序预装的病毒扫描功能按照选定的任务自动启动。程序安装时生成的更新任务的默认任务设置也是关的。一旦卡巴斯基实验室服务器上发布最新的更新文件，更新程序就会自动运行。

要更改任务设置，选择主界面的 (病毒) **扫描**窗口上或 (更新和更新发布任务) **服务**窗口上的任务名，并点击设置打开任务设置窗口。

要根据计划启动任务，选中**运行模式**窗口中的自动任务启动复选框。您可以在点击**更改**后打开的**任务**窗口编辑启动扫描任务的时间 (见图 15)。

图 15. 配置任务计划

最重要的一步是要确定任务启动的频率。您可以有以下选择：

- **分钟。**扫描间隔时间按分钟计算，最大不超过 59 分钟。在任务设置中指定扫描间隔以分钟计的时间。
- **小时** 扫描间隔时间按小时计算。在任务设置中输入以小时计的时间：**每 n 小时**。输入 n 值。例如如果您想任务每小时运行一次，则输入**每 1 小时**就可以了。
- **天 –** 扫描的间隔时间按天数计算。在任务设置中指定扫描运行的频率：
  - 选择 **每 *n* 天** 选项，并输入数值 *n*。如果您想每隔一天扫描以此，则输入 *每 2 天*。
  - 如果您想从周一至周五每天都运行扫描，则选择**每个周日**。

- 选择**每个周末**，则只在星期六和星期天进行扫描。

  除了指定频率外，还要在**时间**栏指定扫描任务的具体时间。

周-扫描任务将在每周指定的时间开始运行。如果您选择该选项，在计划窗口选择您想开始运行任务的一周中的某个时间。同样在*时间*栏输入运行扫描任务的具体时间。

月-任务将在一个月中的某一天运行。

指定的时间。任务将按您指定的具体时间运行以此。

程序启动时。任务在每次卡巴斯基反病毒软件运行时启动。

每次更新后。每次更新完安全危险特征库后启动任务 (这只适用于病毒扫描任务)。

如果扫描任务因为任何原因而错过(例如计算机当时没有开机)，则您可以对错过的任务进行设置，在可能的情况下尽快使之自动启动。为此选中任务窗口中的 **是否运行错过的任务**。

5.6. 电源选项

为节省笔记本电脑电池的用电，降低中央处理器和磁盘子系统的负载，您可以推迟病毒扫描：

- 由于病毒扫描和程序更新有时需要占用相当多的资源以及费时，因此建议您禁用这些定期任务，这样会有助于延长电池使用时间。必要的话，您可以手动更新程序或启动病毒扫描。要使用电池节电功能，选中电池电源窗口上的 **当使用电池电源时禁用计划扫描** 。

- 病毒扫描会增加中央处理器和磁盘子系统的负荷，从而降低了其它程序的运行速度。默认情况下，如果发生这种情况，该程序会暂停病毒扫描，为用户应用程序释放出系统资源。

  然而在处理器资源释放出后有许多程序会启动并以后台模式运行。要使病毒扫描不受此类程序运行的影响，不选中 **强制应用于其它组件**。

  请注意，可单独为每次病毒扫描任务配置此设置。如果这样做的话，指定任务的配置具有更高的优先权。

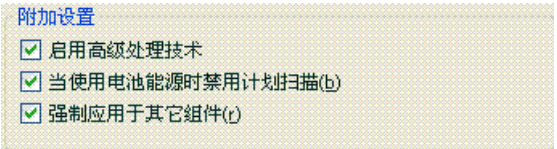


图 16. 配置电源设置

如何为病毒扫描任务配置电源设置：

选择程序主界面的“**保护**”窗口上的“反垃圾邮件”，点击“**设置**”。在高级窗口配置电能设置 (见图 16)。

5.7. 高级处理技术

现今的恶意程序能侵入最低级别要求的操作系统，而在实际操作中难以将其删除。卡巴斯基反病毒 6.0 Windows 工作站检测到系统中存在威胁时会提示您是否需要运行“高级清除技术”。这将可以处理威胁对象并将它从计算机中删除。

完成该步骤后，必须重启计算机。重启计算机后，我们建议进行全盘扫描。要使用“高级清除技术”，选中 **启用高级处理技术**。

如何启用或禁用高级清除技术：

选择程序主界面的**保护**窗口，并点击设置链接。在**高级**窗口配置配额制电源设置 (见图 16)。

第6章. 文件保护

卡巴斯基反病毒 6.0 Windows 工作站组件包含一个特殊的组件来保护在您计算机上的文件，它就是*文件保护*。当您启动系统时以及在您的 RAM 运行时它将被加载。它扫描您打开、保存以及执行的文件和程序。

卡巴斯基反病毒 6.0 Windows 工作站系统托盘图标显示其组件的活动，有文件被扫描时，该图标是这样的 。

默认情况下，“文件保护”只扫描*新建的或已修改的文件*，也就是说，只扫描那些在上次扫描后被新添加的或已更改的文件。扫描文件时采用如下算法：

1. 用户或程序每次访问时，该组件会加以阻止。
2. 文件保护扫描 iChecker™ 和 iSwift™ 数据库中被截取文件的信息。决定是否按照检索的信息扫描文件。

扫描过程包括以下步骤：

1. 分析文件有无病毒。通过比较程序的*反病毒数据库*检测到恶意对象。该反病毒数据库包含所有恶意程序的描述、安全威胁、现已知的网络攻击的描述以及处理的方法。
2. 经过分析，可采取以下三种行动：
    a. 如果文件中检测到恶意代码，“文件安全”会封锁文件，并且复制一份*备份*，同时尝试清除文件病毒。如果该文件的病毒被彻底清除，则可以再次使用。如果不能清除，则删除文件。
    b. 如果在文件中发现恶意代码但又不能确定，文件将被放到*隔离区*。
    c. 如果在文件中没有发现恶意代码，它将马上被恢复。

6.1. 选择文件保护级别

“文件保护”可采用以下几个级别保护文件 (见图 17)：

- **高** - 该级别为打开、保存以及运行的文件提供最全面的监控。
- **推荐保护** - 卡巴斯基实验室推荐您使用这个级别。它将扫描以下对象类别：
    - 按内容划分的程序和文件
    - 新对象以及自上一次扫描以来已修改的对象

- 嵌入的 OLE 对象

- **低** - 当您的程序需要大量的系统资源时您可以选择这个级别，文件扫描范围将被缩小。

图 17. 文件保护安全级别

推荐使用文件保护默认设置。

为了您的工作或者您想更改设置的保护级别，您可以调高或调低文件保护级别。

要更改安全级别：

调整滑块。您可以调整安全级别来定义扫描速度与总的扫描文件数量之比：更少的文件以更高速度进行病毒分析

如果安全级别没有您需要的，您可以自定义安全设置。为此选择最符合您需要的级别作为起点并对其设置进行编辑。这种情况下将设置为**自定义**级别。让我们看一下用户自定义文件安全级别的例子。

例子：

您在工作中要使用计算机处理各种类型的文件，有些文件可能相当地大。即使扫描任何文件多少会影响到计算机的性能，您也不会由于文件的尺寸或范围冒险跳过任何文件而不进行扫描。

选择级别提示：

基于数据源，这可能使您面临恶意程序威胁的相当高的风险。处理的文件的大小和类型会各不相同，跳过扫描这些文件会使您的计算机遭受安全风险。您需要按照内容而不是扩展名来扫描您所使用的文件。

建议您使用**推荐的**安全级别，并作以下修改：移除扫描文件大小的限制而只在扫描新文件和修改过的文件时使文件保护操作最优化。当扫描文件时加载到计算机中文件被减少，因此您可以很畅通地使用其它程序。

如何更改安全级别：

点击“文件保护”设置窗口上的**设置**按钮。在打开的窗口编辑“文件保护”设置并点击确定。

结果将创建第四安全级别-自定义级别。它包含您配置的安全设置。

6.2. 配置文件保护

设置文件保护如何保护计算机安全。该设置可以划分为以下几组：

- 设置扫描的文件类型 (见 6.2.1 在 63 页)
- 设置保护范围 (见 6.2.2 在 65 页)
- 设置检测到危险对象后的处理动作 (见 6.2.5 在 69 页)
- 文件保护高级设置

下面将详细介绍这些设置。

6.2.1. 定义扫描的文件类型

当您选择要扫描的文件类型时，依靠文件格式、大小以及驱动器的类型决定文件在打开、运行、保存时是否被扫描。

为简化配置，将所有文件划分为两类：简单和复合文件。简单文件不包含任何对象，例如.txt 文件。复合对象可能包含若干个对象，没有对象可能又包含其它对象。例如：存档文件、自解压文件、电子制表软件以及邮件附件等等。

在**文件类型**窗口定义扫描文件的类型 (见图 18)。可以选择三个选项中的一项：

扫描所有文件。选择该选项，将毫无例外地扫描所有打开、运行或保存的文件系统对象。

扫描程序和文档（根据内容）。如果选择该类文件，文件保护将只扫描病毒可能嵌入的潜在受感染文件。

> 注意：
>
> 有很多文件格式，受到恶意代码的侵入并继而被激活的可能性非常低。例如.txt 文件。
>
> 反之有些文件格式含有或可能还有可执行代码。例如.exe、.dll 或 .doc 格式。恶意代码侵入这类文件并被激活的可能性非常高。

在对文件进行病毒扫描之前，分析文件内部头的文件格式 (例如 txt、doc、exe 等)。如果分析显示该文件格式不会被感染，则不会扫描该文件并立即恢复使用。如果文件格式可能被感染，则对该文件进行病毒扫描。

扫描程序和文档（根据扩展名）。如果选择该选项，文件保护将只扫描可能受病毒感染的文件，但是文件的格式由文件扩展名来确定。使用 extension 链接，您可以查看被扫描的文件扩展名列表(见 292 页)。

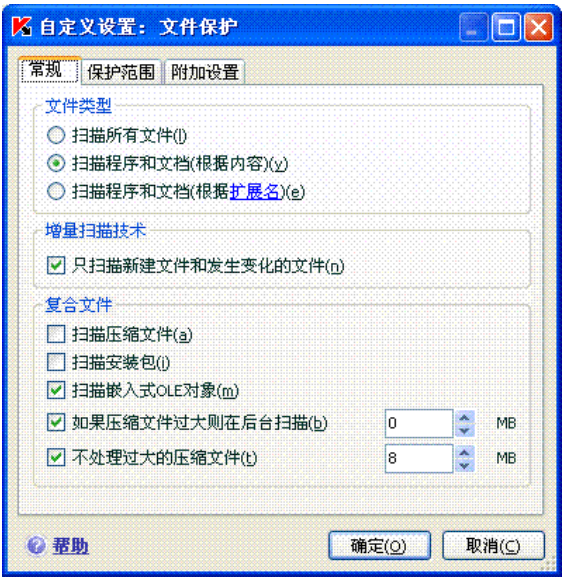


图 18. 选择扫描的文件类型

提示：

小心有人会发送病毒到您的计算机。有些时候，扩展名为 txt 的文件有可实际上是一个改名为 txt 文件的可执行文件。如果您选择 **扫描程序和文件（根据扩展名）**项， 扫描时将跳过这类文件。如果选择 **扫描程序和文件** （根据内容）项， 将忽略扩展名，而且通过文件头的分析会发现该文件时可执行文件。文件保护将对该文件进行病毒扫描。

您可以在**常规**窗口中指定只扫描新文件以及自上一次扫描以来已修改的文件。该模式明显减少了扫描时间并提高了程序的运行速度。要选择该模式，选中 **只扫描新建和发生变化的文件**项。该模式既适用于简单文件，也适用于复合文件。

在**复合文件**选项指定要扫描的复合文件：

- **扫描 压缩文件** – 扫描 .zip、.cab、.rar 和 .arj 文件。.
- **扫描 安装包** – 扫描自解压存档文件。
- **扫描 嵌入式 OLE 对象** – 扫描嵌入文件中的对象(例如嵌入 MS Office 文件、电子邮件附件等的 MS Office Excel 表格或宏文件)。

对于每一类型的复合文件，可以选择并扫描所有文件或只扫描新建文件。为此，左键点击对象名旁边的链接来切换其值。如果在**常规**窗口设置为只扫描新建和已发生变化的文件，您将无法选择要扫描的复合文件类型。

要指定不应扫描的复合文件，使用以下设置：

☑ **如果压缩文件过大就在后台扫描** 。如果复合文件对象的大小超过了该限制，程序将会把它当成单一对象进行扫描 (通过分析文件头)，并将会返回给用户。复合文件所含对象将会延迟进行扫描。如果方框没有被选中，超过指定的文件大小的文件将无法访问，直至其被扫描直完为止。

☑ **不处理过大压缩文件** 。选中该选项，则跳过超过指定大小的文件不扫描。

6.2.2. 定义保护范围

默认情况下，无论文件存储在硬盘、CD/DVD-ROM 还是闪盘中，“文件保护”都将扫描所有病毒。

您可以限制保护范围。为此：

1. 在主界面选择**文件保护，**并点击设置进入组件设置窗口。
2. 点击**设置**按钮并在打开的窗口中选择**保护范围**选项卡 (见图 19)。

该选项卡显示“文件保护”将要扫描的对象列表。默认情况下启用保护硬盘、移动介质、以及与您计算机相连的网络硬盘上的所有对象。您可以使用**添加**、**编辑**和**删除**按钮添加和编辑该列表。

如果想要保护较少的对象，可以使用以下方法：

- 只指定需要保护的文件夹、磁盘以及文件。
- 创建不需保护的对象列表。
- 结合方法 1 和方法 2-创建一个排除众多对象的保护范围。

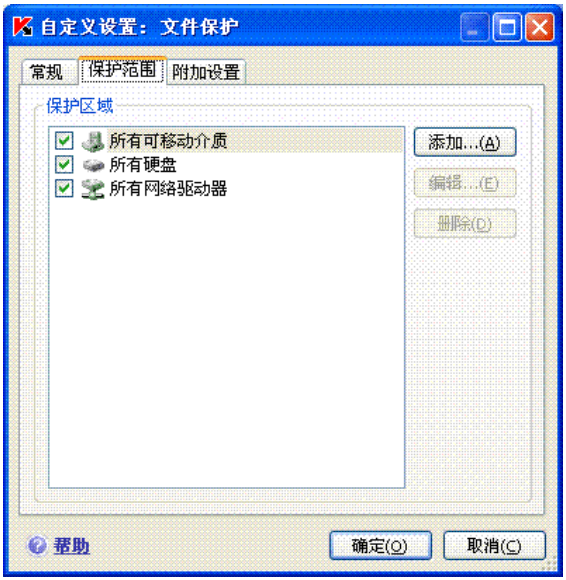


图 19. 定义保护范围

添加扫描对象时可使用关键字。请注意，您只输入直接指向对象的关键字：

- **C:\dir*.*** 或 **C:\dir*** 或 **C:\dir** - *C:\dir* 文件夹中的所有文件
- **C:\dir*.exe** - *C:\dir* 文件夹中所有扩展名为.exe 的所有文件
- **C:\dir*.ex?** – *C:\dir*文件夹中带有.ex?扩展名的所有文件，其中 ？ 可以表示任何一个字符
- **C:\dir\test** – 仅 C:\dir\test 文件

为使扫描能循环进行，选中 **包括子文件夹**

警告！

请记住，文件保护只扫描保护范围之内的文件。不在保护范围内的文件在使用时将不被扫描。这将增加您计算机感染病毒的风险。。

6.2.3. 配置高级设置

作为文件保护的高级设置，您可以指定文件系统的扫描模式并设置临时暂停组件的条件。

要配置文件保护高级设置：

1. 在主界面选择**文件保护**，并点击设置链接进入组件设置窗口。
2. 点击**自定义** 按钮并在打开的窗口选择**附加设置**标签 (见图 20)。

图 20. 配置文件保护高级设置

文件扫描模式决定了文件保护处理条件。您有三种选项：

- **智能模式**。该模式旨在加速文件处理速度并将文件返回给用户。选择该模式时，根据对文件运行的分析来确定是否扫描 。

  例如，当您使用 MS Office 文件时，卡巴斯基反病毒在文件的首次打开和最后一次关闭时会扫描文件。而期间对该文件所有操作则不扫描。

  智能模式为默认设置。

- **访问或更改时–** 文件保护在文件打开或编辑时会对其进行扫描。
- **访问时**-只在文件试图被打开时才扫描文件。
- **执行时 –** 只在文件试图被运行时才扫描文件。

在执行需要占用大量系统资源的任务时，您可能需要暂停文件保护。为了降低负载并确保用户能重新快捷地使用文件，我们建议将组件设置为在某个时间或在使用某些程序时禁用。

要在某个时间段暂停使用组件，选中 **按计划**并在打开的窗口 (见图 21) 点击**任务**，来设定禁用和恢复组件的时间框架。为此在相应的栏中按照 HH：MM 的格式输入时间。

图 21. 暂停组件

要在运行占用大量系统资源的程序时禁用该组件，选中 应用程序启动并在打开的窗口 (见图 22) 中点击应用程序来编辑程序列表。

图 22. 创建应用程序列表

使用**添加**按钮将应用程序添加到列表中。打开快捷菜单，点击**浏览**后可以进入标准的文件选择窗口，然后指定要添加的可执行文件，或从**应用程序**项进入当前运行的应用程序列表，然后就需选择。

要删除应用程序，从列表中选定并点击**删除**按钮。

在使用专门的应用程序时，您可以暂时地禁用暂停文件保护。为此取消选定应用程序名称。您不必从列表中将其删除。

6.2.4. 恢复文件保护默认设置

当配置文件保护时，您可以重置到默认设置。卡巴斯基实验室专家认为它们是最佳设置，并将它们集成在**推荐的**安全级别中。

要恢复文件保护默认设置：

1. 在主界面选择**文件保护**，并点击设置进入组件设置窗口。
2. 点击**安全级别**窗口上的**默认**按钮。

配置文件保护设置时如果修改保护区域内的对象列表，则在您恢复起始设置时，该程序会提示您是否想要保存该列表以作备用。要保存对象列表，选中打开的**恢复设置**窗口上的**保护区域**。

6.2.5. 为对象选择处理动作

如果文件保护在扫描时发现或怀疑一个文件，程序下一步将根据对象的状态来选择处理动作。

文件保护将对象划分为以下几种状态：

- 恶意程序状态 (例如 *病毒*、*木马*)。
- 潜在受感染，此时通过扫描无法确定对象是否受感染。这是指程序从未知病毒中检测到了文件中的一连串代码或是从已知病毒中检测到修改的代码。

默认情况下，所有感染病毒的文件都要清除病毒。如果它们潜在受感染，则会被放到“隔离区”。

要为对象编辑处理动作：

在主界面选择**文件保护**，并点击设置进入组件设置窗口。在适当的窗口显示所有潜在的处理动作 (见图 23)。

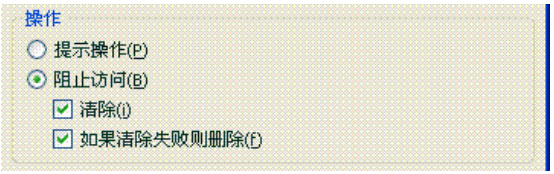


图 23. 文件保护对危险对象可能的处理动作

处理动作	发现危险对象时
提示操作	程序已感染或可能使文件感染病毒，并提供选择处理动作。

处理动作	发现危险对象时
阻止访问	文件保护阻止访问对象。报告中记录了有关信息。稍后您可以尝试清除该对象的病毒。
阻止访问 **清除**	文件保护阻止访问对象，并尝试清除对象的病毒。如果该文件的病毒被彻底清除，则可恢复正常使用。如果未能清除病毒，该文件将指定为*潜在受感染*状态，并被移到“隔离区”。报告中记录了有关信息 。稍后您可以尝试清除该对象的病毒。
阻止访问 **清除病毒** **如果清除失败则删除**	文件保护阻止访问对象，并尝试清除对象的病毒。如果该文件的病毒被彻底清除，则可恢复正常使用。如果无法清除对象，则删除。对象副本存储在“备份”中。
阻止访问 **清除**	文件保护阻止访问对象，并删除。

清除或删除对象前，卡巴斯基反病毒 6.0 Windows 工作站会创建备份，然后再尝试处理对象或将其删除，以防需要恢复对象或有可能要处理它。

6.3. 延迟清除

如果选择 **阻止访问**作为处理恶意程序的操作，将不处理对象并阻止访问对象。

如果选择的处理动作是

阻止访问
清除

同时阻止所有未处理的对象。

为了能重新访问被阻对象，必须清除其病毒。为此：

1. 选择程序主界面的“**文件保护**”窗口，并在“**统计**”窗口任何地方点击左键。
2. 选择**已检测**标签上您感兴趣的对象，并点击**处理操作 → 全部处理** 按钮。

已成功清除病毒的文件将返回给用户。对于任何无法处理的文件，您可以*删除*或*跳过*。在后一种情况时，将恢复文件访问。然而这将极大增加您的计算机感染病毒的风险。因此强烈建议您不要跳过恶意对象。

第7章. 邮件保护

“*邮件保护*”是卡巴斯基反病毒 6.0 Windows 工作站用以防范进出邮件传播危险对象的组件。它在系统启动时运行，常驻您系统的内存中，并且扫描所有基于 POP3 、SMTP 、IMAP、MAPI[1] 和 NNTP 协议以及加密的 POP3 和 IMAP (SSL) 的电子邮件。

卡巴斯基反病毒 6.0 Windows 工作站系统托盘图标显示其组件的活动，有电子邮件被扫描时，该图标是这样的  。

“邮件保护”的默认设置如下：

1. “邮件保护”拦截用户收发的每一封电子邮件。
2. 电子邮件被划分为几个部分：邮件头、邮件主体和附件。
3. 扫描电子邮件的主体和附件 (包括 OLE 附件) 以清除危险对象。使用本程序中所含的“*反病毒数据库*”以及启发式算法来检测恶意对象。安全危险特征库包含了所有现今已知的恶意程序以及对其进行处理的方法的描述。启发式算法可以检测到还没有添加到安全危险特征库中的新病毒。
4. 病毒扫描完成后，您有如下可用的处理方法：
    - 如果邮件主体或者附件包含恶意代码，“邮件保护”将阻止电子邮件，然后在“备份区”保留一份受感染对象的副本，并且试图清除感染对象。如果该电子邮件的病毒被彻底清除，则用户可以正常使用。如果不能清除，则删除电子邮件中受感染对象。病毒扫描完成后，记载着邮件被卡巴斯基反病毒 6.0 Windows 工作站处理电子邮件情况的专用文本将被附加到邮件的主题行中
    - 如果在邮件主体或者附件中被检测到的代码看似恶意的但不确切，那么邮件的可疑部分将被放到“*隔离区*”。
    - 如果在邮件中没有发现恶意代码，则用户随后就可以使用。

Microsoft Outlook 提供的专用插件 (见 7.2.2 在 76 页) 能更准确地配置扫描邮件。

使用 Microsoft Office Outlook 和 The Bat!专用插件扫描使用 MAPI 发送的电子邮件。

如果您使用 The Bat! 程序，卡巴斯基反病毒 6.0 Windows 工作站可以关联其它反病毒应用程序。The Bat! 程序直接配置了处理电子邮件通信量的规则 (见 7.2.3 在 77 页)，该规则取代了卡巴斯基反病毒 6.0 Windows 工作站的邮件保护设置。

当与其它邮件程序 (包括 OE，Mozilla Thunderbird， Eudora 和 Incredimail) 一同运作时，“邮件保护”模块扫描基于 SMTP 、POP3 、 IMAP 、 MAP 和 NNTP 协议的电子邮件。

请注意，如果您使用的过滤器将以 IMAP 方式发送的电子邮件移出您的收件箱，则 Thunderbird 不会扫描这些邮件。

7.1. 选择邮件保护级别

卡巴斯基反病毒 6.0 Windows 工作站以如下级别保护您的邮件安全 (见图 24):

高 - 该级别的大部分收发的邮件都受到监控。程序将详细地扫描包括存档文件在内的邮件附件，而不考虑扫描时间长度。

推荐 - 卡巴斯基实验室专家推荐您这个级别。它与**高级别**扫描相同的对象，但不包括扫描时间超过 3 分钟的附件或邮件。

低 - 由于设定为这个保护级别的邮件扫描范围是有限的，这将使您能够舒适地使用资源密集的程序。因此，该级别仅仅扫描接收的电子邮件，并且对扫描时间超过 3 分钟的文件夹和关联的对象 (电子邮件) 将不予以扫描。如果您的计算机中还安装了其它邮件保护程序，我们推荐您使用这个级别。

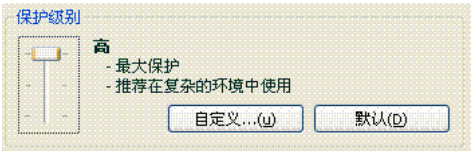


图 24. 选择邮件保护级别

默认情况下，邮件保护级别设置为**推荐**。

您可以调高或调低邮件保护级别，或编辑当前的级别设置。

要更改安全级别:

调整滑块。您可以变更安全级别来定义扫描速度与总的被扫描对象数量之比：被扫描的邮件对象越少，则扫描的速度就越快。

如果预设的级别不能满足您的要求，则您可以编辑其设置。这样，将设置为**自定义**级别。让我们看一下用户自定义邮件安全级别的例子。

例子：

您的电脑是在局域网外并使用拨号连接到互联网。您使用 OE 作为邮件收发客户端，并且您使用一个免费的电子邮箱服务。由于众多原因，您的邮件中包含存档附件。您如何最大程度地避免由于邮件而使您的计算机感染病毒呢？

选择级别提示：

通过分析您的情况，可以断定您在使用电子邮件的过程中处于高风险感染状态(没有统一的电子邮件保护并通过拨号连接)。

建议您开始使用时使用**高**保护级别，并作以下修改：建议您减少扫描附件的时间，例如，减少到 1-2 分钟。将扫描多数存档附件并且处理速度不会减慢太多。

要更改预设保护级别：

点击“邮件保护”设置窗口上的**自定义**按钮。在打开的窗口编辑邮件保护设置并点击确定。

7.2. 配置邮件保护

通过一系列的设置来让您管理如何扫描邮件。可将设置划分为以下几组：

- 设置自定义的邮件保护组(见 7.2.1 在 74 页)
- Microsoft Outlook (见 7.2.2 在 76 页) 和 The Bat!的邮件扫描设置 (见 7.2.3 在 77 页)

> 警告！
> 此版的卡巴斯基反病毒工作站不提供 64 位邮件客户端“邮件保护”插件。

- 设置对邮件中危险对象的处理动作 (见 7.2.4 在 79 页)

下面将详细介绍这些设置。

7.2.1. 选择邮件保护组

“邮件保护”允许您精确地选择哪些邮件组将被扫描。

默认情况下，“邮件保护”组件设置为**推荐**保护级别，这意味着要扫描所有进出的邮件。如果您是首次运行该程序，则我们推荐扫描发送的邮件，因为您计算机

上的蠕虫可能会利用邮件来复制其自身。这将有助于避免被您计算机感染的邮件大量地发送，而不受监控。

如果您确信您发出的电子邮件不含有危险对象，则可以禁用发送邮件扫描。为此：

1. 在主界面选择**邮件保护，**并点击设置进入组件设置窗口。点击“邮件保护”配置窗口上的**自定义**按钮。
2. 在**自定义设置**中：**邮件保护**窗口打开 (见图 25)，在**范围**区选择 **所有邮件**。

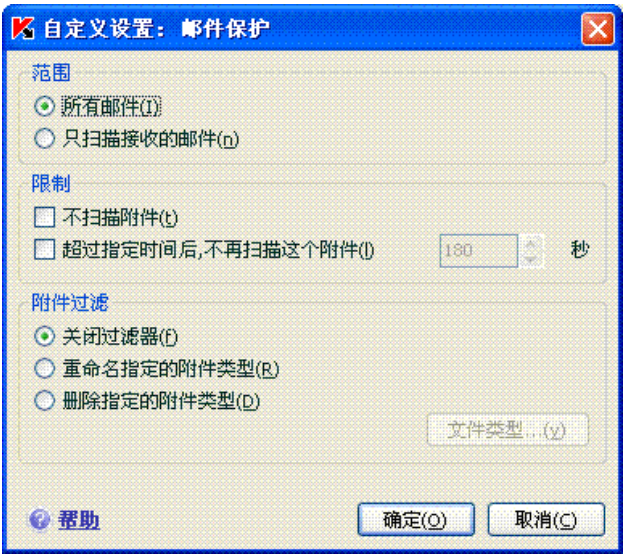


图 25. 邮件保护设置

另外，在选择邮件保护组中，您可以指定是否应扫描邮件附件，同时也可设置扫描单一邮件对象所花的最长时间。这些设置在**限制**区中配置。

如果您的电脑不受任何局域网软件保护，并且不使用代理或者防火墙来访问互联网，则推荐您**不禁用**扫描存档附件和不设置扫描时间限制。

如果您是在受保护的环境下工作，则可以更改扫描时间限制，以提高邮件扫描速度。

您可以在**附件过滤**区域设置附件过滤条件：

关闭过滤器 – 不使用其它附件扫描过滤

- **重命名指定的附件类型** – 过滤掉某种附件类型并用下划线替换文件名的最后字符。您可以点击“文件类型”按钮来选择文件类型。
- **删除指定的附件类型** – 过滤掉并删除某种附件类型。您可以点击“文件类型”按钮来选择文件类型。

您可以在 292 页 区查找到更多有关过滤附件类型的信息。

由于恶意程序频繁地通过邮件附件的形式传播，您可以通过使用过滤器来提高您的计算机的安全性。通过重命名或删除某种附件类型，保护您的计算机免受当消息收到时自动打开附件和其它潜在威胁。

7.2.2. 在 MS Outlook 中设置邮件保护

如果您将 Outlook 作为邮件客户端，则您可以为邮件扫描自定义配置。

您在安装卡巴斯基反病毒 6.0 Windows 工作站时，Outlook 中会安装一个专用插件。它可以迅速存取“邮件保护”设置，也可以设置邮件保护扫描单个邮件的最长时间。

警告！

此版的卡巴斯基反病毒工作站不提供 64 位 Microsoft Office Outlook.“邮件保护”插件。

插件位于**服务 → 选项**下的指定“邮件保护”标签页 (见图 26)。

选择邮件扫描模式：

- **接收时扫描** – 当邮件进入收件箱时对其进行分析。
- **读取时扫描**– 打开邮件读取时分析每一封邮件。
- **发送时扫描** – 当邮件发出时对其进行病毒扫描。

警告！

如果您使用 Outlook 通过 IMAP 方式连接到您的邮件服务器，建议不使用**接收时扫描**模式。启用该模式将导致邮件发送到服务器时会强行复制邮件到本地计算机，并且 IMAP 的主要优越性会丧失– 生成较小的通信量，以及处理服务上不需要的电子邮件，这样不会将邮件复制到用户的计算机上。

在“邮件保护”设置中设置处理危险邮件对象的操作。您可以在**状态**区中的点击这里链接来配置“邮件保护”设置。

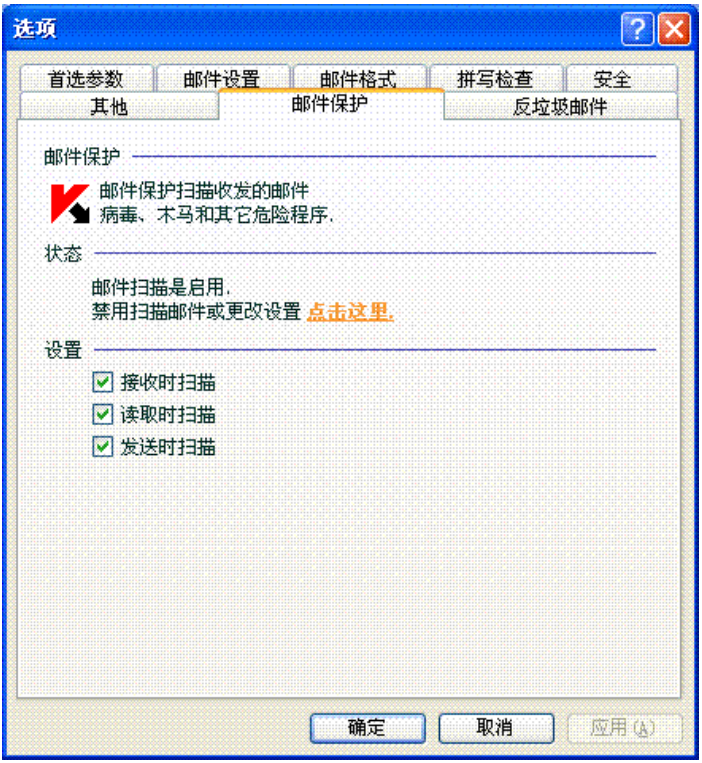


图 26. 在 MS Outlook 中配置邮件保护设置

7.2.3. 在 The Bat！中配置邮件保护

在 The Bat! 中利用其固有工具来定义处理受感染邮件对象的操作。

警告！

尽管“邮件保护”设置确定是否扫描进出的邮件，以及确定对邮件中危险邮件对象和排除对象的处理动作，但被忽略了。The Bat! 考虑到的唯一设置就是扫描存档附件和限制扫描邮件的时间 (见 7.2.1 在 74 页)。

此版的卡巴斯基反病毒工作站不提供 64 位 The Bat!“邮件保护”插件。

要在 The Bat! 中设置邮件保护规则：

1. 从邮件客户端的**属性**菜单中选择**设置**。
2. 从设置目录树中选择**病毒保护**。

显示的邮件保护设置 (见图 27) 扩展到所有安装在计算机上的支持 The Bat!的反病毒模块。

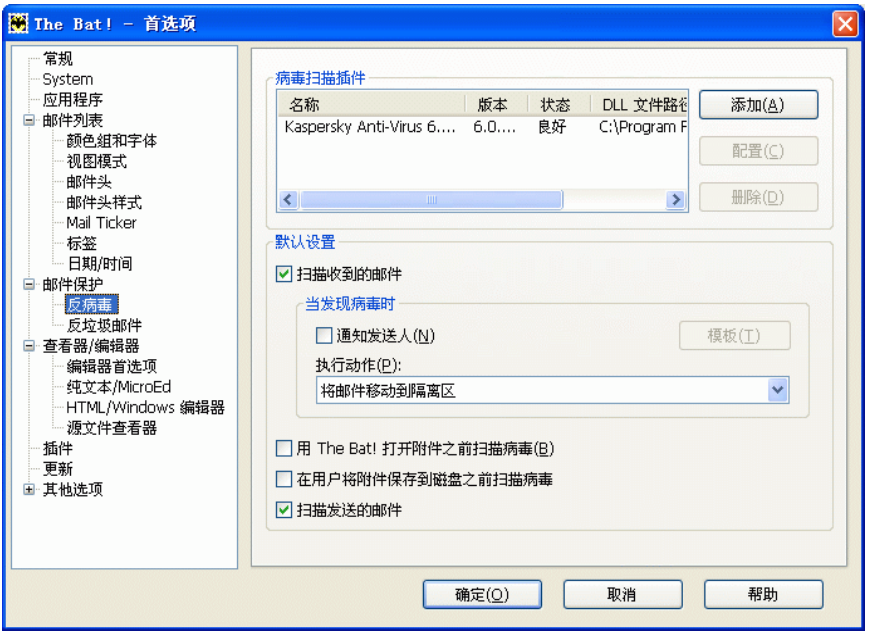


图 27. 在 The Bat！中配置邮件保护

您必须确定：

- 扫描哪种类型的邮件 (收发)
- 何时扫描邮件对象 (打开邮件时还是将邮件保存到磁盘前)
- 检测到邮件中存在危险对象时由邮件客户端采取的处理动作。例如，您可能选择：

  尝试清除被感染部分– 试图处理受感染的邮件对象，并且如果不可以清除对象的病毒，则对象仍驻留在邮件中。如果邮件被感染，卡巴斯基反病毒 6.0 Windows 工作站会始终提示您。但即使您在“邮件保护”通知窗口中选择**删除**，由于在 The Bat! 中的邮件保护处理操作中没有这样的处理案例，那么对象仍然会在邮件中不被删除。

  删除受感染部分– 在电子邮件中删除危险对象，不论该对象是被感染或者是可疑的被感染对象。

默认情况下，The Bat!程序会将所有受感染的邮件对象放到“隔离区”文件夹中而不加以处理。

警告！

The Bat!程序不标识包含特定邮件标题的含有危险对象的邮件。

7.2.4. 恢复邮件保护默认设置

当配置邮件保护时，您可以重置到默认设置。卡巴斯基实验室专家认为它们是最佳设置，并将它们集成在**推荐的**安全级别中。

要恢复文件保护默认设置：

1. 在主界面选择**邮件保护**，并点击设置进入组件设置窗口。
2. 点击**安全级别**窗口上的**默认**按钮。

7.2.5. 为危险邮件对象选择处理动作

如果扫描邮件时显示，邮件或其任意部分 (主体，附件) 受病毒感染或者可疑，则邮件保护的处理动作将取决于对象状态和选定的处理动作。

扫描完后，以下其中之一的状态可以赋予邮件对象：

- 恶意程序状态。
- 潜在受感染，此时通过扫描无法确定对象是否受感染。这是指程序从未知病毒中检测到了文件中的一连串代码或是从已知病毒中检测到修改的代码。

默认情况下，当“邮件保护”检测到危险或者潜在的受感染对象，它会在屏幕上给予警告并提示用户选择处理对象的操作。

要为对象编辑处理动作：

打开卡巴斯基反病毒 6.0 Windows 工作站设置窗口，选择“**邮件保护**”窗口。**操作**框 (见图 28) 中列出了所有可能用来处理危险对象的操作 。

图 28. 为危险邮件对象选择处理动作

邮件保护中可用以处理危险邮件对象的所有操作的详细信息如下。

处理动作	检测到危险对象时
提示操作	邮件保护发出一个包含恶意程序的文件，已经被感染的(潜在受感染的) 警告信息并且提供给您选择如下操作选择。
阻止访问	邮件保护阻止访问对象。报告中记录了有关信息。稍后您可以尝试清除该对象的病毒。
阻止访问 **清除**	邮件保护阻止访问对象，并尝试清除对象的病毒。如果该文件的病毒被彻底清除，则可恢复正常使用。如果无法处理对象，就将其移到隔离区。报告中记录了有关信息。稍后您可以尝试清除该对象的病毒。
阻止访问 **清除病毒** **如果清除失败则删除**[2]	邮件保护阻止访问对象，并尝试清除对象的病毒。如果该文件的病毒被彻底清除，则可恢复正常使用。如果无法清除对象，则删除。对象副本存储在“备份区”。 处于潜在感染状态的对象将被移到“隔离区”。
阻止访问 **清除**	“邮件保护”检测到受感染或潜在受感染的对象时，它会予以删除而不提示用户。

清除或删除对象前，卡巴斯基反病毒 6.0 Windows 工作站会创建备份副本再尝试处理对象或将其删除，以防需要恢复该对象或有必要处理它。

[2] 如果您将 The Bat！作为您的邮件客户端，当邮件反病毒采取该处理操作时 (取决于在 The Bat！中选定的处理操作)，会清除或删除危险的电子邮件对象。

第8章. WEB 反病毒保护

无论当您何时使用互联网，存储在您机器上的信息都存在受到危险程序感染的风险。当您在互联网上读文章时，它们都有可能被加载到您计算机中。

卡巴斯基反病毒 6.0 windows 工作站包括一个专用组件来保护您安全使用互联网 – 这就是 *Web 反病毒保护*。它保护通过 HTTP 方式进入您机器的信息，并且也会保护您的计算机不会加载危险的脚本。

警告！

Web 反病毒保护仅仅监控通过 HTTP 方式传输的数据，它们使用的端口被加到监控端口列表中 (见 16.3.7 在 190 页)。程序包中列出了用以邮件传输和 HTTP 传输的最普通的端口。如果您使用的端口不在这个列表中，可以将它们添加到列表中来保证传输安全通过。

如果您工作在不受保护的环境或者使用调制解调器来拨号连接互联网，当您上互联网时我们推荐您使用 Web 反病毒来保护您的安全。如果您的计算机是运行在受防火墙或者 HTTP 过滤器保护的环境中，当您浏览网页时 Web 防病毒为您提供额外的保护。

卡巴斯基反病毒 6.0 Windows 工作站系统托盘图标显示其组件的活动，有脚本被扫描时，该图标是这样的  。

下面让我们了解有关该组件运行的更详细的信息。

Web 反病毒保护由两个模块组成，它们可以：

- *通信量扫描*-扫描通过 HTTP 进入用户计算机的对象。
- *脚本扫描*-扫描所有经 MS IE 处理的脚本以及用户使用计算机时载入的 WSH 脚本 (JavaScrip、VB 脚本等等)。

  您在安装卡巴斯基反病毒 6.0 Windows 工作站时，会安装一个 MS IE 专用插件。浏览器的“标准按钮”工具条中的图标  显示它已安装完成。点击该图标，将打开一个信息面板，它会显示 Web 反病毒保护对被扫描和屏蔽的脚本数量的统计数字。

Web 反病毒保护为 HTTP 传输提供如下保护：

1. 用户或者某个程序通过 HTTP 下载的每个网页或者文件都可以被 Web 反病毒保护拦截和分析恶意代码。使用卡巴斯基反病毒 6.0 Windows 工作站中所含的反病毒数据库以及启发式算法来检测恶意对象。安全危险特

征库包含了所有现今已知的恶意程序以及对其进行处理的方法的描述。启发式算法可以检测到还没有添加到安全危险特征库中的新病毒。

2. 分析完成后，您有如下可用的处理方法：

   a. 如果用户试图允许的网页或者对象包含恶意代码，程序将会屏蔽它通过。然后在屏幕上出现一个消息框，显示对象或者网页是被感染的状态。

   b. 如果文件或者网页不包含恶意代码，程序立刻允许用户访问它。

根据以下算法扫描脚本：

1. Web 反病毒拦截运行在网页中的每个脚本并扫描有无恶意代码。
2. 如果一个脚本包含恶意代码，Web 反病毒保护会屏蔽它并且为用户弹出一个特定的通知。
3. 如果在脚本中没有发现恶意代码，就会运行该脚本。

8.1. 选择 Web 反病毒保护级别

当您在以下保护级别使用互联网时，会受到卡巴斯基反病毒 6.0 windows 工作站的保护 (见图 29)：

高 - 该级别的大部分通过 HTTP 接收的脚本和对象都受到监控。该程序使用整套的安全危险特征库对所有对象进行全面的扫描。当没有使用其它 HTTP 安全工具的敏感环境中，我们推荐使用该保护级别。

推荐 - 卡巴斯基实验室专家推荐您使用该级别。该级别扫描同**高安全级别**时相同的对象，但限制文件碎片缓存的时间，这会加速扫描并更快速地将对象返回给用户。

低 - 由于设定为该保护级别通过使用受限的反病毒数据库来减少扫描的范围，因此您可更快地使用资源密集的程序。如果您的计算机中已经使用了其它的网页保护程序，我们推荐您使用该保护级别。

图 29. 选择 Web 反病毒保护级别

默认情况下，Web 反病毒保护级别设置为**推荐**。

您可以调高或调低 Web 反病毒保护级别，或编辑当前的级别设置。

要编辑安全级别：

调整滑块。您可以变更安全级别来定义扫描速度与总的被扫描对象数量之比： 更少的对象以更高速度进行恶意代码扫描。

如果预设级别不符合您的要求，您可以创建**自定义**安全级别。让我们了解当一个安全级别生效时的例子。

例子：

您的电脑通过调制解调器连接到互联网。它不在公司局域网中，并且您没有反病毒程序来保护持续不断的 HTTP 通信量。

由于您的工作性质，您常通过互联网来下载大文件。通常像这样来扫描文件会占用您大量的时间。

您如何最大程度地保护您的计算机免受通过 HTTP 传输的文件或者脚本的病毒感染？您可以配置 Web 反病毒保护来提高组件操作速度，特别地：通过选择一个完全或者受限的反病毒数据库来设置扫描规则。

选择级别提示：

根据这些基本信息，我们认为您的计算机是运行在一个易受感染的环境中，并且您受到 HTTP 传输流高风险感染的可能（这是因为没有统一的 Web 反病毒保护，并且使用拨号连接互联网）。

建议您开始使用时使用**高**保护级别，并作以下修改： 我们建议您在扫描期间限制文件碎片整理的缓存时间。

要更改预设保护级别：

点击“Web 反病毒保护”设置窗口上的**自定义**按钮。在打开的窗口编辑 web 保护设置并点击确定。

8.2. 配置 Web 反病毒保护

Web 反病毒保护扫描所有通过 HTTP 下载到您计算机中的对象，并且会监控任何正常在运行的 WSH 脚本 (avaScript, VB 脚本等等)。

您可以配置 Web 反病毒保护来提高组件操作速度，特别是：

- 通过选择一个完全或者受限的反病毒数据库来设置扫描规则。
- 创建可信任网络地址列表

您可以选择 Web 反病毒保护将对危险的 HTTP 对象所采取的处理动作。

下面将详细介绍这些设置。

8.2.1. 设置扫描方法

您可以用如下之一的规则来扫描来自互联网的数据：

- *协议流扫描* — 网络传输恶意代码检测技术为正在流通中的数据流进行扫描。例如，您正从互联网上下载一个文件。Web 反病毒保护将对您从网上下载的那部分进行扫描。这项技术可以更快地为用户传输已扫描的对象。同时，使用有限的的反病毒数据库进行流扫描（仅是最活跃的威胁），这会极大地降低使用互联网的安全级别。
- 缓冲区扫瞄 —当扫描对象已经完全被下载到缓冲区时，网络传输恶意代码侦测技术会扫描这些对象。扫描完后，程序会将该对象返还回用户或者将其屏蔽。
  当使用这个扫描类型时，完整的反病毒数据库会被使用，这会提高检测恶意代码的水平。但是，使用这种算法会增加处理对象的时间，从而使网络浏览速度变慢。这也会造成当复制和处理大文件时引起的 HTTP 客户端超时。
  我们建议您限制从互联网下载的文件片段的缓存时间来解决这个问题。当超过限制时间时，用户将下载的文件部分将不会被扫描，并且一旦文件被完全复制，它将会被完整扫描。这可以更快地将对象传输给用户并解决使用互联网时中断连接而不降低安全级别的问题。

要选择 Web 反病毒保护将使用的扫描规则：

1. 点击“Web 反病毒保护”配置窗口上的**自定义**按钮。
2. 在打开的窗口 (见图 30) 的**扫描方法**部分选择所需选项。

默认情况下，Web 反病毒保护使用缓冲区或者完整反病毒数据库扫描来自互联网的数据。文件片段的默认缓存时间为 1 秒。

图 30. 配置 Web 反病毒保护

警告！

如果您遇到无法访问如互联网收音机、协议流录像、或互联网会议等问题，请您使用协议流扫瞄。

8.2.2. 创建信任地址列表

您可以创建一个您充分信任的地址的信任列表。Web 反病毒保护将不会对来自这些地址的数据进行分析危险对象。在 Web 反病毒保护干涉了正常浏览网页的情况下时使用该选项，例如，每次您试图下载一个文件可每次都被 Web 反病毒保护阻止。

要创建可信任网络地址列表：

1. 点击“Web 反病毒保护”配置窗口上的**自定义**按钮。
2. 在打开的窗口 (见图 30) 的**可信任 URL** 部分创建信任服务器列表。为此使用列表右边的按钮来操作。

当您输入一个可信任地址时，您可以使用如下通配符来创建关键字。

***** – 任何字符组合。

例子： 如果您创建关键字 ***abc***，则将扫描不含 **abc** 的网址。例如：www.virus.com/download_virus/page_0-9abcdef.html

? – 任何单一字符。

例子： 如果您创建关键字 **Patch_123?.com**，包含这串字符中在 3 后面任意一个字符的网址将不会被扫描。例如： **Patch_1234.com** 将不会被扫描， 然而会扫描 **patch_12345.com** 。

如果某个包含一个*或者？的网址被添加到信任列表中，当您输入它们时，您必须像如下例子使用一个斜线来忽略*或者？。

例子：您想添加如下的网址到信任地址列表中：www.virus.com/download_virus/virus.dll?virus_name=

如果在？前面加入一个斜线（\），那么卡巴斯基反病毒 6.0 Windows 工作站就不会把它当成计算机通配符来使用。然后，您正添加到排除列表中的网址将如下所示：

www.virus.com/download_virus/virus.dll\?virus_name=

8.2.3. 恢复 Web 反病毒保护默认设置

当配置 Web 反病毒保护时，您可以重置到默认设置。卡巴斯基实验室专家认为它们是最佳设置，并将它们集成在**推荐的**安全级别中。

要恢复 Web 反病毒保护默认设置：

1. 在主界面选择 **Web 反病毒保护**，并点击设置进入组件设置窗口。
2. 点击**安全级别**区域上的**默认**按钮。

8.2.4. 为危险对象选择处理动作

如果分析一个 HTTP 对象显示它包含恶意代码，那么 Web 反病毒保护对该对象的操作取决于您所选择的处理动作。

要配置 Web 反病毒保护检测危险对象的处理动作：

打开卡巴斯基反病毒 6.0 Windows 工作站设置窗口，选择“**Web 反病毒保护**”。**操作**区域 (见图 31) 中列出了所有可能用来处理危险对象的操作。

默认设置是，当检测到一个危险的 HTTP 对象，Web 反病毒保护在屏幕上会显示一个警告信息，并弹出一个包含几种处理危险对象动作的选择窗口。

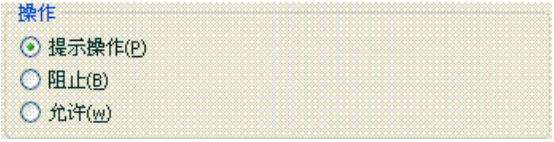


图 31. 为危险脚本选择处理动作

有关处理危险 HTTP 对象的可能操作如下;

处理动作	在 HTTP 传输中检测到危险对象
提示操作	Web 反病毒保护将弹出一个包含潜在被恶意代码感染的警告信息，并提供给您一个处理的操作。
阻止	Web 反病毒保护将会阻止对象通过，并在屏幕上显示一个关于阻止它的消息框。相似的信息将会记录到报告中。
允许	Web 反病毒保护将允许对象通过。报告中记录了有关信息 。

对于危险脚本，Web 反病毒保护总会拦截它们，并弹出包含可供用户采取处理操作的消息框。除非您禁用脚本扫描模块，否则您是不可能改变对一个危险脚本的处理操作。

第9章. 主动防御

警告！

对于运行 Microsoft Windows XP Professional x64 Edition 或 Microsoft Windows Vista 还是 Microsoft Windows Vista x64 的计算机，该版本的应用程序不提供主动防御组件。

卡巴斯基反病毒 6.0 windows 工作站能够保护您免受已知威胁和未知的新威胁的感染。这是一个专门被用来抵御越来越多新威胁的组件—*主动防御*。

由于恶意程序传播的速度比反病毒数据库升级的速度更快，这就导致对主动防御需求的不断增长。

传统的反病毒保护技术是在一个新威胁至少感染一台计算机后才能够获取病毒样本，并且分析恶意代码，最终添加到反病毒数据库然后更新到用户计算机中的反病毒数据库里。此时，新威胁可能已造成巨大的破坏。

由卡巴斯基反病毒 6.0 Windows 工作站主动防御提供的预防技术，可以避免在新威胁没有被添加到反病毒数据库期间，导致您计算机遭到破坏的情况，并且可以消除新威胁。我们如何去实现它呢？ 与快速反应技术（病毒特征码技术）相比较，分析代码，预防技术通过由某应用程序或进程执行的行为分析来识别出一个在您计算机中的新威胁。程序安装包含确定危险活动级别的一套标准。如果活动分析表明某程序的行为可疑，则卡巴斯基反病毒会对该类型的行为采取规则所指定的处理方法。

危险行为由程序总的处理活动来确定。例如，如果是程序将自身复制到网络资源中，启动文件夹或系统注册表，然后发送出大量副本这样的活动，则很可能该程序是蠕虫。危险行为也包括：

- 变更文件系统
- 模块嵌入到其它进程中
- 隐藏系统进程
- 修改微软 Windows 系统注册表键值

“主动防御”使用规则以及排除应用程序名单跟踪和阻止所有危险操作。

“主动防御”也跟踪 MS Office 应用程序中执行的所有宏命令。

“主动防御”使用一套该应用程序自带的规则以及使用该应用程序时创建的用户自定义规则。“规则”是定义可疑行为以及卡巴斯基反病毒如何对其进行处理的一套标准。

各种规则提供应用程序运行，并监控运行在计算机上的系统注册表、宏指令和进程的变化情况。您可以添加、删除或编辑规则，随意对其进行修改。规则可以阻止或允许程序的活动。

下面让我们了解一下“主动防御”的算法：

1. 计算机启动后，“主动防御”会立即使用既定规则和排除规则分析以下要素：
   - *运行在计算机上的每一程序的行为*。主动防御有规律地记录程序运行的历史记录，并把它们与危险行为特征序列 (由来自程序和反病毒数据库更新的危险行为类型数据库) 进行对比。
   - 分析*每一运行的 VBA 宏命令的活动*有无恶意活动的迹象。
   - *每个试图修改系统注册表的行为* (删除或者添加系统注册表键值，并输入可疑的键值等等)。
2. 根据“主动防御”的*允许*规则 (根据相关标准，程序行为是安全的) 以及*阻止*规则 (根据相关标准，程序行为属恶意的) 进行分析。
3. 分析完成之后，您可以执行以下的操作：
   - 如果按照相关标准 (*允许*和*阻止*规则) 程序行为不属于危险行为，则允许其运行。
   - 如果按照相关标准，程序行为属于危险行为，则组件下一步会按照规则中的指令进行操作。这种行为通常会被阻止。屏幕上将显示危险应用程序的详细说明，行为类型以及行为运行的历史记录。您必须自己决定拦截或者允许这种行为。您可以在系统中创建行为规则并取消所采取的活动。

9.1. 主动防御设置

“主动防御”组件设置 (见图 32) 类别如下：

- *是否监控计算机上运行的应用程序的行为*

  选中☑ **启用程序行为分析**复选框启用“主动防御”功能。默认情况下启用该模式，以确保在您计算机上打开的任意程序的所有行为都被严密跟踪并与危险行为配置列表相比较。您可以为该行为配置程序处理指令 (见 9.1.1 在 90 页)。您也可以创建“主动防御”排除规则来使所选应用程序活动不受监控。

图 32. 主动防御设置

- *是否监控系统注册表的变化*

  默认情况下，☑ 选中**启用注册表保护**，这意味着卡巴斯基反病毒 6.0 Windows 工作站会分析所有试图修改操作系统注册表键值的行为。

  您可以自己创建监控注册表的规则(见 9.1.3.2 在 97 页)，这取决于 MS Windows 注册表键值。

- *是否扫描宏命令*

  选中☑ **启用 Office 保护**复选框可监控所有运行在计算机上的 VB 应用程序的宏命令。选中该复选框是默认设置。

  您可以选定哪些宏命令被视为是危险的，以及如何处理 (见 9.1.2 在 94 页)。

  Microsoft Windows XP Professional x64 Edition、Microsoft Windows Vista 或 Microsoft Windows Vista x64 操作系统下不能使用该“主动防御”组件。

您可以配置“主动防御”模块排除列表 (见 5.3.1 在 50 页) 并创建可信任应用程序列表 (见 5.3.2 在 54 页)。

下面将详细予以介绍。

9.1.1. 活动控制规则

请注意，在 Microsoft Windows XP Professional x64 Edition、Microsoft Windows Vista 或 Microsoft Windows Vista x64 操作系统下配置应用过程控制不同于在其它

操作系统中的配置过程。

本部分结尾提供了有关在这些操作系统中配置活动控制的信息。

卡巴斯基反病毒监控您的计算机上的运行的应用程序。应用程序包括事件说明，可作为危险事件来跟踪。为每一个这样的事件创建监控规则。如果任何一个应用程序的活动被划为是危险事件，则“主动防御”将严格执行该事件规则的规定。

如果需要监控应用程序的活动，则选中 **启用程序行为分析**复选框。

以下让我们来了解几种应用程序将视为危险事件进行跟踪的危险的行为类型：

- *危险行为*。卡巴斯基分析计算机上安装的应用程序的活动并根据卡巴斯基实验室制定的规则列表检测程序的危险或可疑的活动。此类活动包括隐蔽的程序安装或程序自我复制等。
- *启动带参数的 IE 浏览器*。通过分析此类的活动，可以检测到企图利用设置打开浏览器的行为。此类活动的特点是，利用某命令提示设置从一应用程序打开网络浏览器。例如，您点击广告邮件中的某一网址链接。
- *侵入进程*（侵入程序）-向某程序进程添加可执行代码或其它协议流。这种行为广泛应用于特洛伊木马程序。
- *隐藏的进程（rootkit）*。Rootkits 是用于隐蔽恶意程序及其进程的程序组。卡巴斯基反病毒分析操作系统是否存在隐蔽的进程。
- *Window 钩子* 它用于企图读取操作系统对话框中显示的密码以及其它机密信息。如果有企图拦截操作系统与对话框之间传输的数据的行为，卡巴斯基反病毒会对其进行跟踪。
- *注册表中的可疑数值*。系统注册表是存储系统以及用户设置的数据库，它控制 Windows 的运行以及计算机上安装的任何实用程序。企图在系统中隐藏的恶意程序将错误值复制到注册表键值中。卡巴斯基反病毒分析系统注册表是否存在可疑键值。
- *可疑的系统活动*。该程序分析 Microsoft Windows 执行的动作并检测可以活动。破坏程序完整性就是可疑活动的一个例子，它是指自受监控的应用程序上一次运行以来，有一个或若干个模块被修改。
- 键盘记录器。这种行为通常用于试图盗取您通过键盘输入的密码和其它机密信息。
- *Microsoft Windows 任务管理保护*。当恶意模块意在阻止“任务管理器”运行时，卡巴斯基反病毒会防范恶意模块注入到“任务管理器”中。

卡巴斯基反病毒 6.0 Windows 工作站更新时可以自动扩展危险行为判断列表，但用户不可以对其进行编辑。您可以：

- 取消选中活动名称旁的 来关闭对活动的监控。
- “主动防御”检测到危险行为时，编辑它所使用的规则。
- 创建排除列表，列出您不视为能产生危险行为的应用程序。

要配置活动监控，

1. 点击程序主界面上的设置，打开卡巴斯基反病毒 6.0 Windows 工作站设置窗口。
2. 从设置目录树中选择**主动防御**。
3. 点击**启用程序行为分析** 区域上的**设置**按钮。

主动防御保护监控的活动类型列在**设置： 程序行为分析** 窗口 (见图 33)。

图 33. 配置程序活动控制

编辑危险行为监控规则，从列表中选择它，然后标签页下方进行规则的设置：

- 指定“主动防御”对危险行为的操作。

您可以指定以下任意一个行为作为处理操作：允许，提示操作和终止进程。左键点击行为链接直到变为您需要的键值。除了中止进程外，您还可以把它移到隔离区。为此，您可以使用应用程序配置的开/关链接来设置它。您可以指定扫描检测系统中的隐藏进程的频率 (时间值)。

- 选择是否您需要生成运行的报告。为此点击日志链接，直到显示所需的开或关。

要关闭危险活动监控，在列表中取消选中活动名称旁的 ☑ 。

如果使用的是 Microsoft Windows XP Professional x64 Edition、Microsoft Windows Vista 或者 Microsoft Windows Vista x64 操作系统，在卡巴斯基反病毒中配置程序活动控制时请注意：

如果您使用上述其中一种操作系统，则只控制一类系统事件－*危险行为*。卡巴斯基反病毒 6.0 Windows 工作站分析计算机中安装的程序的活动，并按照卡巴斯基实验室专家创建的规则列表检测危险或可疑活动。

如果您需要卡巴斯基反病毒监控系统进程以及用户进程，则选择 ☑ **监控系统用户账户** 复选框 (见图 34)。该项默认设置为禁用。

用户账户控制系统访问以及识别用户及其工作环境，防止其它用户破坏操作系统或数据。系统进程由系统用户账户启动系统进程。

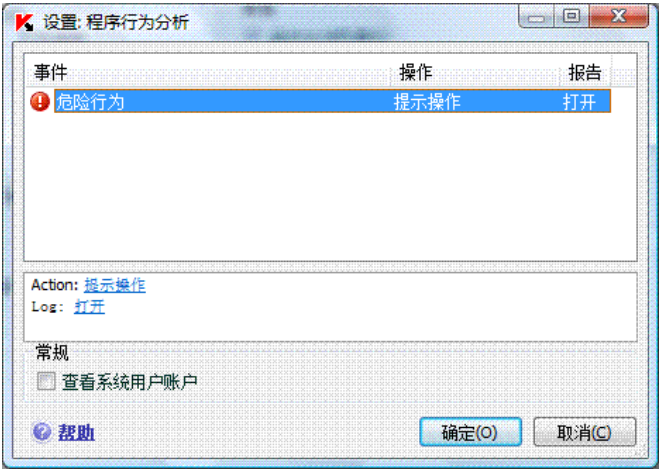


图 34. 使用 Microsoft Windows XP Professional x64 Edition、Microsoft Windows Vista、Microsoft Windows Vista x64 操作系统时的程序活动控制配置

9.1.2. Office 保护

使用 Microsoft Windows XP Professional x64 Edition、Microsoft Windows Vista 或 Microsoft Windows Vista x64 操作系统时该“主动防御”组件无法使用。

您可以选中 **启用 Office 保护** (见图 32) 来启用扫描和处理计算机上运行的危险宏命令。扫描每一个运行的宏命令。如果该宏命令包含在危险宏命令列表中，则对其进行处理。

例子：

> 宏对象 *PDFMaker* 是一个在微软公司的 word 里面的用来生成 pdf 文档的 Adobe Acrobat 工具栏的插件。主动防御模块可以识别这些隐藏在软件中的危险参数。如果启用 Office 防护，那么当一个宏对象被加载时，主动防御模块将会屏幕上给您提示一个警告信息，并提醒您检测到一个危险的宏命令。您可以选择中断该宏命令或允许它继续运行。

您可以配置宏命令有可疑行为时程序的处理操作。如果您确定该宏命令与 MS Word 文件等具体文件作用时不会造成危险，则我们建议创建排除规则。如果符合排除规则的条件，宏命令执行的可疑活动将不由“主动防御”来处理。

要配置 Office 保护：

1. 点击程序主界面上的设置，打开卡巴斯基反病毒 6.0 Windows 工作站设置窗口。
2. 从设置目录树中选择**主动防御**。
3. 点击**启用 Office 保护**窗口上的**设置**按钮。

在**设置：Office 保护** 窗口 (见图 35) 配置处理危险宏命令的规则。该窗口包含卡巴斯基实验室定义的危险宏的默认处理规则，以及“主动防御“的处理操作。处理这些危险宏命令的操作包括隐藏程序组件和删除文件。

如果您认为列表上的一项行为不危险，可以取消选中该处理操作名称旁的复选框。例如，您可能经常使用宏命令来打开文件 (非只读文件打开) 并且您确信该操作不是恶意的。

要使卡巴斯基反病毒不阻止宏命令：

> 取消选中该处理操作旁的复选框。这样程序不再认为该行为是危险的，并且“主动防御”将不会处理它。

默认情况下，无论何时程序在您的计算机上检测到一个危险宏指令，屏幕上都会弹出一个窗口询问您是否需要允许或者阻止宏执行。

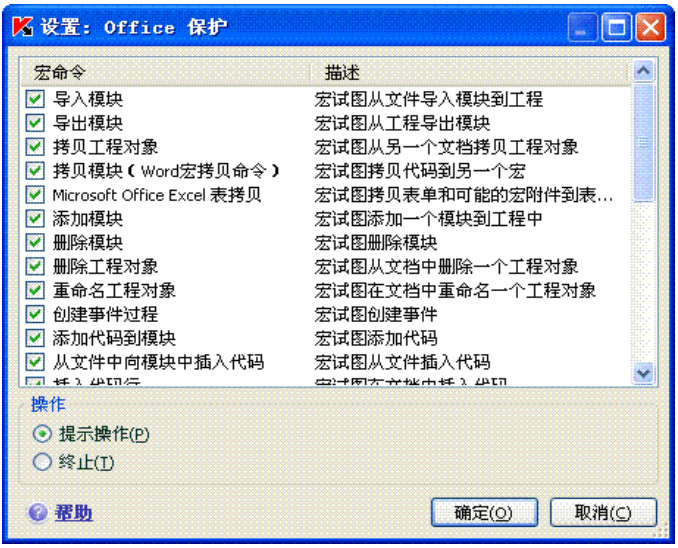


图 35. 配置 Office 防护设置

为了实现自动拦截所有危险行为而不提示用户：

在宏列表窗口选择 **终止**。

9.1.3. 注册表防护

许多恶意程序的目的之一就是修改您计算机操作系统的注册表。这包括没有破坏性的玩笑程序或者其它当前对您计算机存在威胁的恶意程序。

例如，玩笑程序可以复制自身信息到注册表的相应键中，这样在应用程序打开时会自动运行。然后当您启动操作系统时，恶意程序将会自行启动。

要设置系统注册表监控：

1. 点击程序主界面上的设置，打开卡巴斯基反病毒 6.0 Windows 工作站设置窗口。
2. 从设置目录树中选择**主动防御**。
3. 点击**启用注册表防护**窗口上的**设置**按钮。

卡巴斯基实验室已经了创建一个控制注册表键的操作列表并已将其包含在程序中。注册表文件操作被划分为*系统安全*、*Internet 安全*等逻辑组。其中的每一组都包含系统注册表文件以及操作规则。程序的其它部分更新时列表也会更新。

设置： 注册表保护窗口 (见图 36) 显示整个规则列表。

每个规则组有相应的执行优先级，但您可以使用**向上**和**向下**按钮来调高或调低优先级。规则组在列表中所处位置越高，则其优先级越高。如果在几个组中降低相同的注册表键值的优先级，第一个应用于这个键的规则将会比其它组拥有更高的优先级。

您可以采用以下方法来停止使用任意规则组：

- 取消选定组名旁的复选框 ☑ 。但规则组仍然是保留在列表但主动防御并不会使用它。
- 从列表中删除规则组。我们不推荐删除由卡巴斯基实验室创建的规则组，因为它们包含恶意程序最常用的系统注册文件。

图 36. 可控制的注册表键值组

您可以创建自己的受监控系统注册表文件组。为此，点击文件组窗口上的**添加**按钮。

在打开的窗口执行以下步骤：

1. 在**组名**框中输入用于监控系统注册表键值的新文件组组名。
2. 选择**键值**标签，并创建注册表文件列表。您需要为之创建规则的受监控组中包括此注册表文件列表。这可能是一项或多项键值。
3. 选择**规则**标签并创建文件规则。该文件规则适用于“键值”标签上所选的键值。您可以创建多个规则并设置使用它们的顺序。

9.1.3.1. 为创建规则选择注册表键值

创建的文件组应至少包括一个系统注册表文件。“键值”标签显示规则适用的文件列表。

要添加系统注册表文件：

1. 点击**编辑...**窗口 (见图 37) 中的**添加**按钮。
2. 在打开的窗口选择您需要创建监控规则的注册表文件或文件夹。
3. 为一组键值指定关键值或者关键字，这是您需要应用到**键值**区域的规则。
4. 选定**包含子键值**，使该规则适用于列出的注册表文件的所有附件。

图 37. 添加受控的注册表键值

如果通配符是被用在相同的键值中，那么您只需要同时使用含有星号和问号的关键字来作为**包含子键值**的功能。

如果您使用关键字来选择注册表文件夹并且一个文件夹指定一个组键值，那么选定组中任意键值的规则都会生效。

9.1.3.2. 创建注册表保护规则

注册表保护规则规定了：

- 监控访问系统注册表的程序
- 程序试图执行对系统注册表文件操作时“主动防御”的处理操作

要创建选定的系统注册表文件规则：

1. 点击**规则**标签上的**添加**按钮。新规则将添加到列表的顶部（见图 38）。

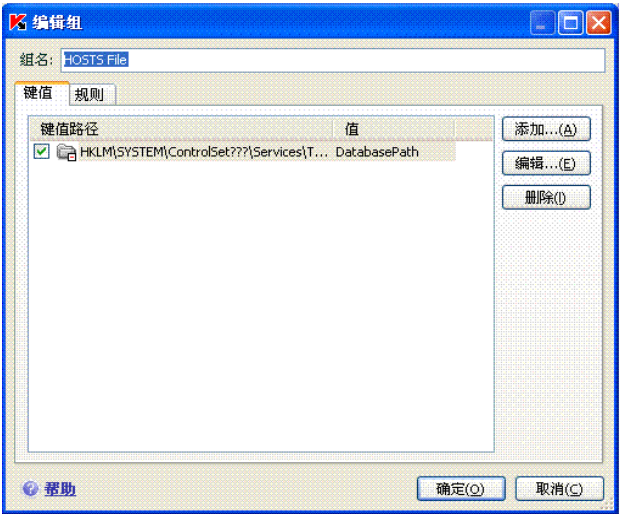


图 38. 创建注册表键值监控规则

2. 选择列表上的一个规则并标签的下方指定规则设置：

   - 指定应用。

     默认设置规则是应用于所有程序。如果您需要把规则应用到特定的程序，左键点击任意来将其更改到此值。然后点击指定应用名链接。这将会打开快捷菜单： 点击**浏览**查看标准的文件选择窗口，或点击**应用程序**查看打开的程序列表并按需要选择其一。

   - 为选定的试图读，编辑或者删除注册表键值的程序定义主动防御采取的处理操作。

     您可以使用这些处理操作中的任何一个来响应： 允许，提示操作和终止进程。左键点击行为链接直到变为您需要的键值。

   - 点击记录/不记录链接来选择是否您需要生成运行的报告。

您可以创建多项规则，并使用**向上**和**向下**按钮来调整它们的优先级。规则在列表中所处位置越高，则其优先级越高。

您也可以为系统注册表键值创建一条*允许*规则（例如允许所有处理动作），这样当一个程序试图去对键值执行操作时就会弹出通知信息。您可以这样来创建，在

通知框中点击创建允许规则然后在打开的窗口中指定系统注册表对象将应用的规则。

第10章. 反间谍功能

能够保护您的计算机免于各种类型的恶意软件的卡巴斯基反病毒 6.0 Windows 工作站组件称为*反间谍*。近来，越来越多的恶意程序将目标锁定在：

- 窃取您的机要信息 (密码、信用卡账号、重要的文件信息等)。
- 对您的计算机操作进行跟踪，并对安装在您计算机上的软件进行分析。
- 在浏览器、弹出式窗口和各种程序的横幅上面，强制显示广告内容。
- 通过您的计算机非法访问互联网的各个站点。

网络钓鱼攻击的目的就是为了窃取您的信息：自动拨号、玩笑程序和广告程序将会浪费您的时间和金钱。反间谍保护组件可以保护您防止这些程序的影响。

反间谍功能包括以下模块：

- *反钓鱼保护*组件提供反网络钓鱼攻击的保护。

  网络钓鱼攻击通常是由来自金融机构的、内容包括指向他们网站的链接的电子邮件组成。这些文本信息将会吸引读者点击这个链接，并在接下来的窗口中输入自己的机要信息。例如信用卡账号或一个他们自己网上银行站点的用户名和密码。

  网络钓鱼攻击常见的例子是用户通常收到一封包含一个链接到正式站点的电子邮件。点击该链接，您将会看到一个与网上银行站点一模一样的复制站点，您甚至还可以在浏览器的地址栏中看到一模一样的地址；但您看到的却是一个伪造的网站。因此您在这个站点上的任何操作都将会记录下来，从而可以窃取您的金钱。

  您也许会通过电子邮件或即时通信软件收到一个指向网络钓鱼网站的链接。反网络钓鱼攻击模块可以记录所有尝试打开网络钓鱼站点的行为并可以拦截这些站点。

  卡巴斯基反病毒 6.0 windows 工作站安全危险特征库包括当前所有已知的网络钓鱼攻击站点。卡巴基思实验室的专家们将从互联网组织－－“反网络钓鱼工作组”所获取的网络钓鱼攻击的地址加入到数据库中。通过更新反病毒数据库可以将站点添加到列表中。

- *弹出阻止*模块可以拦截包含与各种网站链接的广告的弹出式窗口。

  这些弹出式窗口中的信息对您基本上没有什么作用。您打开一个网站或使用一个超链接进入不同的窗口时，将会自动弹出这些窗口。这些窗口中包含一些您根本上不需要的广告信息和其它类信息。弹出阻止模块可以拦截

这些窗口，并在系统托盘图标上方显示提示信息。您就可以选择是否拦截这个窗口。

> 弹出式拦截模块可以与 windows xp SP2 操作系统上的 IE 浏览器的弹出式拦截模块结合在一起使用。您安装卡巴基思反病毒 Windows 工作站时，将会在 IE 浏览器中安装一个插件，这样您就可以设置您所允许的弹出式窗口。

有些站点使用弹出式窗口可以更容易并更迅速的向您传递信息。如果您经常访问一个站点，并且弹出式窗口中的信息会对您十分重要。这样您就可以将这个网址添加进入信任站点列表。这样，这些弹出式窗口将不会被拦截掉了。

使用 IE 浏览器时，当一个弹出式窗口被拦截掉以后，这个 图标将会显示在浏览器的状态栏中。您可以不予以拦截或双击图标将这个地址添加进入信任地址列表中。

- *广告拦截*模块可以拦截网页上面的或者安装在您计算机上的各种程序接口上的广告。

  广告里面不仅没有任何有用的信息，而且会影响您的工作，而且还会增加您计算机的通信量。反广告模块凭借卡巴斯基反病毒 6.0 Windows 工作站创建的关键字，可以拦截最普通的横标广告。您可以禁用广告的拦截功能或者创建您自己所允许的和所有拦截的广告的列表。

  > 要将反广告模块集成到 **Opera** 中，需要在 standard_menu.ini 文件的 **[Image Link Popup Menu]**:选项中添加以下字段：
  >
  > Item, "New banner" = Copy image address & Execute program, "…\Program Files\Kaspersky Lab\Kaspersky Anti-Virus 6.0 for Windows Workstations\opera_banner_deny.vbs", "//nologo %C"

- *反拨号程序*模块可以保护您使用的付费的互联网服务不被未授权的用户使用。

  > 反拨号程序模块可以运行在 Microsoft Windows 2000、Microsoft Windows XP、Microsoft Windows XP x64、Microsoft Windows Vista 和 Microsoft Windows Vista x64.操作系统上。

  拨号程序通常与色情网站建立连接。您将被强迫去为那些您根本不想或根本未使用的网站服务支付昂贵的通讯费 如果您想要从拦截列表中排除任何一个号码，则必须将其添加到可信任号码列表中。

10.1. 配置反间谍功能模块

反间谍功能模块可以保护您避免所有卡巴基思实验室已知的程序窃取您的机要信息或金钱。您可以更加个性化地配置该组件：

- 您可以为那些您不想拦截的弹出式窗口创建信任站点列表
- 创建广告黑名单和白名单 (见 10.1.2 在 103 页)
- 创建您所允许的拨号连接的可信任电话号码列表

10.1.1. 创建弹出式窗口拦截模块的可信任地址列表

默认情况下，反间谍模块可以拦截大多数的自动弹出式窗口。而那些添加到 IE 浏览器中可信任站点列表中的网站和所在内联网的弹出式窗口不会被拦截掉。

如果您运行的是 windows xp 操作系统并打了 sp2 的补丁，IE 浏览器会有自己的弹出式窗口拦截模块。您可以对它进行灵活的设置，选择您所需要拦截的窗口列表以及您不想拦截的窗口列表。反间谍程序模块与该拦截模块按照下列规则进行协调： 拦截规则优先运行。也就是说，如果 IE 或反间计模块对某一弹出式窗口有拦截规则窗口将会被拦截掉。正因为如此，所以如果您运行的是 windows xp SP2 的操作系统，我们建议您将弹出式窗口拦截模块与浏览器一起进行配置。

如果您想查看任何一个弹出式窗口，则必须将它们的地址添加到信任列表中。为此：

1. 打开卡巴斯基反病毒 6.0 Windows 工作站设置窗口，在设置目录树中选择**反间谍**。
2. 点击“**启用弹出式窗口拦截**”窗口中的“ **可信任网站**”按钮。
3. 在打开的窗口点击**添加** (见图 39)，并为您不想拦截掉的弹出式窗口的网址输入关键字。

> 提示：
>
> 当您在可信任地址栏中输入关键字时，您可以使用字符“* ”或者“ ?”。
>
> 例如，关键字 http://www.test* 排除了所有以这一系列字符串开始的网站的弹出式窗口。

4. 指定是否将 IE 可信任区域中的地址或您的本地网络中的地址排除扫描。弹出式窗口拦截模块将会默认认为这些地址是可信的，而不需要拦截这些地址的弹出式窗口。

新的被排除拦截的网址将会添加到可信任地址列表的顶部。只要取消选中地址旁的复选框，就可以停止使用已添加的排除地址。如果您想要整个移除一个排除地址，您可以选择列表上的该地址并点击“**删除**”按钮。

图 39. 创建可信任地址列表

如果您想要拦截在 IE 浏览器信任站点列表中的内联网或站点中的弹出式窗口，您可以取消选中**可信任区域**部分的相应复选框。

当可信任地址列表中没有的弹出式窗口试图打开时，将会在程序的图标上显示一条信息并表明已经拦截该窗口。通过这条信息上面的链接，您可以取消拦截这个弹出式窗口并可以将这个窗口的地址添加到可信任的地址列表中。

如果您使用 windows xp SP2 操作系统，则您也可以通过 IE 浏览器取消选中窗口。为此，您可以通过该程序图标打开快捷菜单。当有弹出式窗口被拦截时，浏览器下角的该程序图标会闪烁。

10.1.2. 广告拦截模块列表

*反广告*是卡巴斯基反病毒 6.0 Windows 工作站用以拦截广告的组件。卡巴基思实验室的专家通过专门研究而统计出的最常见的广告地址表，并已经将它们加入到了程序中。如果不禁用反广告功能，则它将会根据地址列表拦截广告。

您也可以为广告地址创建黑名单和白名单，它们允许或拦截广告。

请注意，如果拦截广告名单或黑名单包含过滤域关键字，您仍然时可以进入该根站点。

例如，如果拦截的广告列表中包括一个地址“**truehits.net**”，您将可以访问网站“**http://truehits.net**”，但是您访问网址 **http://truehits.net/a.jpg** 时，将会被阻止。

10.1.2.1. 配置标准的广告拦截列表

卡巴斯基反病毒 6.0 Windows 工作站在网站和程序接口中包含了一系列的最常见的广告的地址列表。该列表是由卡巴斯基实验室的专家们收集整理的，并将随安全威胁数据库一同更新。

当使用反广告程序模块时，您可以选择您想要使用的标准广告关键字。为此：

1. 打开卡巴斯基反病毒 6.0 Windows 工作站设置窗口，在设置目录树中选择**反间谍**。
2. 点击反广告区域上的**设置**按钮。
3. 打开**常规**标签 (见图 40)。反广告程序将会拦截标签中所列出的广告关键字。您可以在广告地址栏的任何位置，使用地址串。

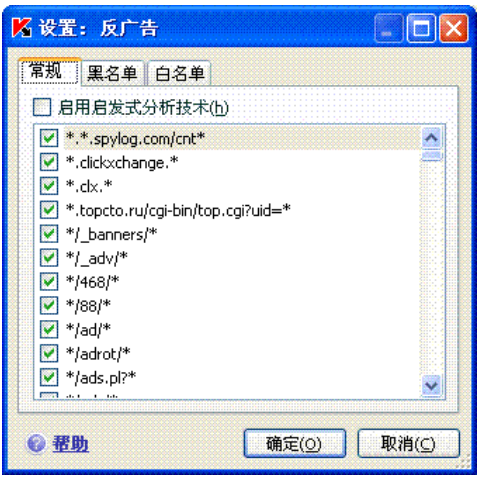


图 40. 拦截广告列表

标准拦截列表中的地址无法编辑。如果您不想按照标准关键字拦截地址栏的一个广告，您可以取消选中关键字旁的复选框☑。

如要分析与标准列表中的关键字不相匹配的广告，选中 **使用启发式分析方法**。然后程序将对具有典型广告性质的标识而载入的图像进行分析。根据这些分析，可能会将该图像标识为广告并加以拦截。

您也可以创建自己允许和拦截的广告列表。您可以在**白名单**和**黑名单**标签上创建。

10.1.2.2. 广告白名单

您可以创建广告白名单，以允许显示某些广告。该名单上包括所允许的广告关键字。

要将新的关键字添加到白名单中：

1. 打开卡巴斯基反病毒 6.0 Windows 工作站设置窗口，在设置目录树中选择**反间谍**。
2. 点击反广告区域上的**设置**按钮。
3. 打开**白名单**标签。

使用**添加**按钮，添加所允许的广告关键字。您可以为一个广告定义一个 URL 地址或一系列的字符串。在后种情况下，当广告企图加载时，程序会扫描其地址中的关键字。

创建关键字时，您可以使用通配符“* ”或者“ ?”。(此处* 代表字符串，？ – 任何单一字符) 。

要停用您创建的关键字，您可以将其从列表中删除或取消选中关键字旁的复选框 。此后属于该关键字范畴的广告将会再次被拦截。

使用**导入**和**导出**按钮，您将可以将您允许的广告列表从一台计算机复制到另一台计算机中。

10.1.2.3. 广告黑名单

除了反广告拦截的标准广告列表之外，您可以创建您自己的列表。为此：

1. 打开卡巴斯基反病毒 6.0 Windows 工作站设置窗口，在设置目录树中选择**反间谍**。
2. 点击受拦截广告区域上的**设置**按钮。
3. 打开**黑名单**标签。

使用**添加**按钮，输入想要屏蔽的横幅广告的关键字。您可以为一个广告定义一个 URL 地址或一系列的字符串。在后种情况下，当广告企图加载时，程序会扫描其地址中的关键字。

创建关键字时，您可以使用通配符“* ”或者“ ?”。(此处* 代表字符串，？ – 任何单一字符) 。

要停用您创建的关键字，您可以将其从列表中删除或取消选中关键字旁的复选框 。

使用**导入**和**导出**按钮，您将可以将受拦截广告列表从一台计算机复制到另一台计算机中。

10.1.3. 创建反自动拨号信任号码列表

反自动拨号程序模块可监测隐蔽地连接上互联网的电话号码。如果经配置，不通知用户进行该种连接或非用户自己启动的连接，则可将该连接视为是隐蔽性连接。

无论隐蔽性连接何时企图启动，该程序模块都会在屏幕上发出具体信息，提示用户允许或拦截该电话连接。如果您没有启动该连接，则很可能就是由恶意程序设置的。

如果您想要允许一个连接而不无需每次提示您确认，则您必须将它们添加到可信任的号码列表中。为此：

1. 打开卡巴斯基反病毒 6.0 Windows 工作站设置窗口，在设置目录树中选择**反间谍**。
2. 点击反自动拨号区域中的**信任号码**按钮。
3. 在打开的窗口点击**添加** (见图 41)，并输入电话号码或合法的电话号码的关键字。

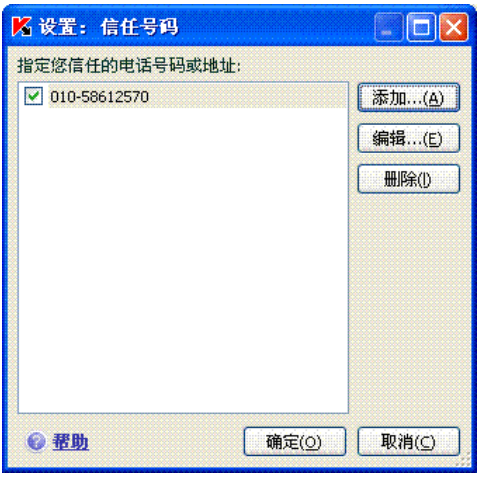


图 41. 创建信任地址列表

提示：

当您输入可信任号码关键字时，您可以使用字符“* ”或者“ ?”。

例如 0???? 79787* 将覆盖所有以 79787 开头并且所有 79787，其中区域码为 4 位。

新电话号码将添加到可信任号码列表的顶部。要停用您所添加的排除的号码，只要取消选中列表上该号码旁的复选框 ☑ 就可以了。如果需要整个地去除该排除的号码，在列表上选择并点击**删除**。

第11章. 反黑客功能

当今的计算机在上网时，越来越容易受到网络攻击。黑客们利用操作系统和软件的漏洞，主要采用病毒传播和其它类型的攻击来实现。

卡巴斯基反病毒 6.0 Windows 工作站反黑客组件确保您的本地网络和互联网冲浪时的安全，它在网络层上和应用层上保护您的计算机以及在互联网冲浪时隐藏您的计算机，从而可以防止网络攻击。

反黑客组件通过允许或拦截网络活动的行为来进行所有的包过滤的规则滤，它可以在网络层上保护您的计算机系统，其依据是以下设置：包方向、数据传输协议以及出站包端口。不管您的计算机安装了哪些应用软件以及所处的网络环境，都可以建立进入网络的数据包传输规则。

除了包过滤规则，入侵检测系统 (IDS) 也为网络层提供了安全保护。IDS 的目的就是可以对进入计算机的连接进行分析，对您计算机的端口扫描进行监控，过滤那些利用软件漏洞的数据包。当入侵检测系统运行时，它可以阻止所有对您计算机进行一定时间攻击的进站连接，而且用户也可以收到提示信息，告知其计算机正处于网络攻击之下。

入侵检测系统在进行分析时采用了一个特殊的防止网络攻击的数据库，卡巴斯基实验室会对该数据库定期扩展，并且该数据库会随着反病毒数据库一同更新。

为安装在您计算机上面的各种应用在使用网络资源时，应用网络规则，从而在应用层上保护您的计算机系统。类似于网络安全层，应用层安全是建立在数据包传输方向上，传输协议上和使用的端口上的。然而在网络应用层上，接收和发送的特定数据包以及特定的网络应用都被考虑在内。

使用应用程序规则将有助于为您的计算机系统设置更加安全的保护。例如，有些应用程序需要阻止某种类型的连接而其它程序可以允许这种连接类型。

以下是基于两个反黑客安全层的两种反黑客规则类型：

- *包过滤规则* (见 11.2.1 在 112 页)。不管您的计算机安装了哪些应用程序，它都可以用来创建网络活动通用的约束规则。**例子**：如果你要在网络端口 21 上创建一个能阻止入站连接的包过滤规则，则使用该端口的外部应用程序将无法进入您的计算机系统 (例如一台 ftp 服务器) 。
- *应用程序规则*。它为特定的网络应用程序创建网络活动限制规则。**例子**：如果 80 端口阻止任何应用程序的连接，则您在该端口上只可以为 Firefox 创建允许它连接的规则。

包过滤应用规则有两种方式：*允许*和*阻止*。程序安装包括了一系列的规则，它们管理着最普遍的网络活动，并使用使用最常见的网络协议和网络端口卡巴斯基反

病毒 6.0 Windows 工作站也为可信任应用程序创建一组允许规则。这些应用程序的网络活动不受怀疑。

卡巴斯基反病毒 6.0 Windows 工作站将整个网络空间划分为不同的区域，从而使设置和规则更加用户化：互联网和安全区域，这在很大程度上与您的计算机所属的子网有关的。您可以为每个区域 (互联网、局域网、可信任应用网络) 指定其状态，从而确定该区使用规则和监控网络活动的策略。

*隐身模式*是反黑客功能组件的一个特殊功能，它可以防止网络外部的用户侦测到您的计算机系统，从而使黑客无法侦测到要攻击的对象。该模式不会影响用户计算机的上网活动：建议您将您的计算机作为服务器使用时不要使用*隐身*模式。

11.1. 选择反黑客组件的安全保护级别

当您使用网络时，卡巴斯基反病毒 6.0 Windows 工作站可以为您的计算机提供以下级别的保护 (见图 42)：

阻止所有－拦截您计算机的任何网络活动。如果您选择这个安全级别，那么您将不能使用任何网络资源或需要网络连接的程序。我们建议您仅仅在受到网络攻击时或在不安全连接情况下使用危险网络时，才选择该级别。

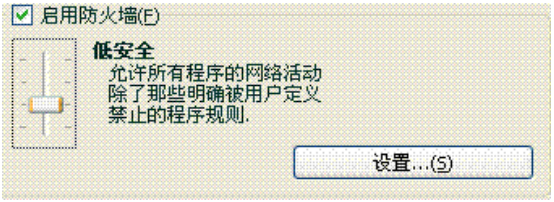


图 42. 选择反黑客组件的安全保护级别

高安全－只有使用程序中自带的允许规则或自创的规则，网络活动才被允许。卡巴斯基反病毒 6.0 Windows 工作站自带的规则组包括网络活动不可疑的应用程序允许规则以及收发绝对安全的数据包允许规则。尽管如此，如果在网络应用阻止规则列表中的一个应用规则的优先级别比这个应用程序的允许规则的优先级别更高，那么这个网络应用活动将会被阻止。

警告！

如果你选择该安全级别，则反黑客组件的允许规则列表中不存在的任何网络应用活动都将被阻止。因此，仅仅当您为所有的应用软件设置了允许规则并且不打算在您的计算机上安装新软件时，我们才建议您使用该规则。

学习模式－已创建反黑客规则的安全级别。在此保护级别，无论何时某程序企图使用网络资源，反黑客程序组件就会确认是否存在该连接的规则。如果有这样的连接规则，反黑客组件就会应用它。如果没有这样的规则，屏幕上会显示一个提示信息，其包括该网络连接的描述信息 (启动它的程序，使用哪个端口、网络协议等) 。您必须决定是否允许该连接。使用该信息窗口中的一个特殊按钮，您可以为这个连接创建规则，从而在以后再次遇到这类连接时，反黑客程序组件会应用该连接的新规则，而不会在屏幕上再次提醒您。

低安全－反黑客组件可以根据自己本身自带的阻止规则或用户已经创建的阻止规则只屏蔽屏蔽被阻止的网络活动。尽管如此，如果在网络应用允许规则列表中的一个应用程序规则的优先级别比这个应用程序的阻止规则的优先级别更高，那么该网络应用活动将会被允许。

允许所有－允许您计算机的任何网络活动。在没有发现任何的网络攻击以及您完全信任所有的网络活动时，只有在这种特殊的情况下，我们才建议您设置成该保护级别。

您可以调高或调低网络安全级别来选择您想要使用的安全级别，或者改变当前的设置级别。

要修改网络安全级别：

1. 选择卡巴斯基反病毒 6.0 Windows 工作站设置窗口中的**反黑客**组件。
2. 调节**启用防火墙**区域上的滑动条，直至显示所需的安全级别。

要配置网络安全级别：

1. 选择最适合您的网络安全保护级别。
2. 在打开的窗口中，点击**设置**按钮并编辑网络安全设置。

11.2. 应用程序规则

卡巴斯基反病毒 6.0 Windows 工作站中包括最常见的 windows 应用的规则组。这些程序的网络活动已经卡巴基思实验室的详细分析，并被严格定义为危险或可信任的网络活动。

依据所选择的防火墙的安全级别以及计算机所运行的网络类型，程序规则列表可以使用在各个不同方面。例如：在使用**最大保护模式**下，所有与允许规则不匹配的应用程序网络活动都会被阻止。

要设置应用程序规则列表：

1. 点击反黑客组件设置窗口的防火墙区域上的**设置**按钮。
2. 在打开的窗口选择**应用程序规则**标签 (见图 43)。

图 43. 安装在计算机上的应用程序的规则列表

该标签页上的规则可按以下两种方式之一进行组合：

- *应用程序规则* 如果选中 **将应用程序分组**，则已被创建规则的每一应用程序将在列表的每一行上显示出来。 每一应用程序包括以下信息：应用程序的名称和图标，命令提示，包含应用程序可执行文件的根目录，以及已创建的规则数量。

  使用**编辑**按钮，您可以进入列表中所选的应用规则列表并进行编辑：增加新规则，编辑现有规则，以及改变规则的优先级。

  使用**增加**按钮，您可以在列表中添加新的应用程序并为其创建规则。

  导出和**导入**按钮是被设计用来将已创建的规则拷贝到其它的计算机中，这有助于快速配置反黑客组件。

- *通用规则列表* 如果取消选中 **将应用程序分组**，则通用规则列表上的每一行会显示每一规则完整的信息：应用程序名和启动命令、是否允许或屏蔽网络活动、数据传输协议、数据的传输方向 (入站或出站) 以及其它信息。

您可以使用**添加**按钮来创建新的规则，并且可以在列表中选定现有规则、点击**编辑**按钮编辑对选定的现有规则进行编辑。您也可以在列表下方编辑基本设置。

您可以使用**向上**和**向下**按钮改变规则的优先级。

11.2.1. 手动创建规则

要手动创建应用程序规则：

1. 选择应用程序。为此点击**应用程序规则** 标签 (见图 43) 上的**添加**按钮。在打开的快捷菜单上点击**浏览**并选择您需要创建规则的应用程序的可执行文件。选定的应用程序的规则列表将打开。如果应用程序的规则已存在，则它们会被排列在窗口的上方。如果规则不存在，则规则列表窗口将是空的。

   当配置应用程序规则条件时，您可以稍后选择需要配置的应用程序。

2. 点击应用程序规则窗口中的**添加**按钮。

您可以使用打开的**新规则**窗口调整规则。

11.2.2. 创建规则模版

反病毒模块包含预制的规则模版，用户在创建自己的规则时可以使用它。

整个现有的网络应用程序可以划分为几种类型：邮件客户端、网络浏览器等。每一类型的应用程序都执行其特有的活动，例如收发邮件或接收和显示 html 网页。每一类型的应用程序使用某些网络协议和端口。因此使用模版有助于按照应用程序类型快捷地配置规则。

要利用模版创建应用程序规则：

1. 选中应用程序规则标签上的 **将应用程序分组**，如果没有选中，点击**添加**按钮。
2. 在打开的窗口选择您需要创建规则的应用程序的可执行文件。选定的应用程序的规则窗口将打开。如果应用程序的规则已存在，则它们会被排列在窗口的上方。如果规则不存在，则规则列表窗口将是空的。
3. 点击应用程序规则窗口上的**模版**，并从快捷菜单上选取其中一个规则模版 (见图 44)。

图 44. 为创建新规则选择模版

允许所有－该规则允许应用程序任何的网络活动。**阻止所有**－该规则阻止应用程序的所有网络活动。本应用程序任何企图启动网络连接的活动都将受到阻止并且不通知用户。

快捷菜单上列出的其它模版可以为相应的程序创建典型的规则。例如邮件客户端模板可以创建一系列规，从而允许**邮件客户端**进行发送电子邮件等标准的网络活动。

4. 必要的话，编辑已创建的应用程序规则。您可以修改网络行为：网络连接方向，远程地址，网络端口 (本地和远程)，和规则作用的时间。

5. 如果您想要将规则应用到利用某些命令行设置就可以打开的程序，选中 **命令行** 并在右侧的栏输入命令串。

已创建的规则或已设置的规则将会添加到规则列表的底部，并且优先级最低。您可以提高规则的优先级。

您可以在网络活动侦测防御窗口中创建规则。

11.3. 包过滤规则

卡巴斯基反病毒 6.0 Windows 工作站中包括对您的计算机进出数据包过滤的一系列规则。您可以启动数据包的传输或已安装在您计算机上的程序。该程序包含由卡巴斯基实验室设计的包过滤规则，它可以确定数据包是否有危险。

依据所选择的防火墙的安全级别以及计算机所运行的网络类型，规则列表可以使用在各个不同方面。例如：在使用**高**级别时，所有与允许规则不匹配的应用程序网络活动都会被阻止。

重要提示！

请注意，安全区域规则比阻止包规则有更高的优先级。例如，如果您选择**局域网**状态，则将允许包交换。所以不论阻止包规则如何，您都可以访问共享文件夹。

要设置包过滤规则列表：

1. 点击反黑客组件设置窗口的防火墙区域上的**设置**按钮。
2. 在打开的窗口选择**包过滤规则**标签 (见图 45)。

图 45. 包过滤规则列表

每一包过滤规则包括以下信息：规则名，操作 (允许或阻止包传输)，数据传输协议，包传输的方向，和包传输时需要使用的网络连接设置。

如果选中规则名旁的复选框，则将使用该规则。

您可以使用列表右侧的按钮选择所要运行的包过滤规则。

要创建新的包过滤规则：

点击**包过滤规则**标签中的**添加**按钮。

打开的**新规则**窗口中有一份表格，您可以将它用来调整规则。

11.4. 调整应用程序和包过滤规则

对于应用程序规则和数据包过滤规则来说，**新建规则**窗口中的高级规则设置实际是相同的 (见图 46)。

图 46. 创建新的应用程序规则

步骤一：

- 输入规则名。本程序使用默认名，用户应予以替换。

- 为此规则选择网络连接设置：远程网络地址、远程网络端口、本地地址、时间。选中所有您需要在规则中使用的设置。
- 配置用户通知设置。规则使用时，如果您需要屏幕上弹出简要注释信息，则选中 ☑ **显示警告**。如果您需要程序在反黑客报告中记录下规则的执行情况，则选中 ☑ **事件日志**复选框。创建规则时，默认设置是不选中该复选框。当您创建阻止规则时，我们建议您使用该设置。

请注意，当您在反黑客学习模式中使用阻止规则，则有关应用中的规则的信息将自动输入到报告中。如果您不必记录该信息，则取消选中**记入报告**复选框。

步骤二：为规则参数和选择动作创建一个指定的值。在**规则描述**区域执行这些操作。

1. 每一新规则的默认设置是*允许*规则。要将其更改为*阻止*规则，左键点击规则描述区域中的允许连接。它将更改为阻止规则。

   卡巴斯基反病毒将扫描已被创建允许规则的程序和包的网络通信量。这可能导致数据传输更加缓慢。

2. 如果您在创建规则前没有选择应用程序，则有必要点击选择应用程序选定一个应用程序。用鼠标左击链接，将会出现一个标准的文件选择窗口，然后为正创建的规则选择相应的应用程序的可执行文件。

3. 指定规则的网络连接方向。默认值为双向 (入站和出站) 网络连接的规则。在打开的窗口中，左键点击进站和出站并选择网络连接方向以更改连接方向。

   - **入站 (数据流)。**该规则仅仅应用在一个开放的网络连接中，从一台远程的计算机给您的计算机发送一系列信息。
   - **入站。**除了 TCP 协议包之外，该规则可以应用您的计算机接收到的数据包。
   - **入站和出站。**该规则可以应用到所有出站和入站的数据流。不管是什么计算机，您的或远程的计算机，都可以启动网络连接。
   - **出站 (数据流)。**该规则仅应用于您的计算机打开的网络连接。
   - **出站。**除了 TCP 协议包之外，该规则可以应用到您的计算机发送的入站数据包。

   如果对您来说，在规则中设置数据包发送的方向是特别地重要，请好择好入站和出站的数据包。如果您要为流数据创建一个规则，请选择数据流：入站、出站或两者皆选。

   *数据流的传输方向*与*数据包的传输方向*不同之处在于：当您为一个数据流创建规则时，您就必须定义网络连接的方向。而在该连接中传输数据时，您就不需要考虑数据包的传递方向。

例如：如果您要为一台运行在被动 FTP 模式下的服务器配置一个数据交换规则，您必须允许一个出站数据流。为了在主动的 FTP 模式下与 FTP 服务器交换数据，我们建议您允许出站和入站数据流。

4. 如果您选择一个远程的地址作为网络连接的地址，请在打开的窗口左键点击指定网络地址并输入 IP 地址，以及规则众多的地址或子网络地址。您可以为一个规则使用一种类型的 IP 地址或几种类型的 IP 地址。可以为一种类型指定几个地址。

5. 设定网络连接使用的协议。TCP 是默认的网络连接协议。如果您为一个应用程序创建一个规则，您可以选择 TCP 或 UDP 两种协议中的一种。为此您可以用鼠标左击这个协议名直到达到您所需要的值。如果您正在创建一个包过滤规则，并且想要改变默认协议时，在打开的窗口中点击其名称并选择您所需要的协议类型。如果您选择 ICMP，您可能需要更进一步地 指定。

6. 如果您选择网络连接设置 (地址、端口以及时间范围)，则必须准确设置其属性值。

在规则被添加到应用程序规则列表中以后，您可以进一步对规则进行设置 (见图 47)。如果您想要将规则应用到可以命令行参数打开的应用程序，选中☑ **命令行**，并在右边的区域里面输入相应的字符串。此规则将不适用于以不同命令行开启的应用程序。

在 windows98 操作系统里面，您就没有这个命令行开始设置的选项。

您可以在网络活动侦测防御窗口中创建规则。

图 47. 新规则高级设置

11.5. 规则优先级

为应用程序或数据包创建的每一规则都会有一个优先级。当其它条件相同时 (例如网络连接设置)，应用程序活动时将会应用优先级更高的规则。

一个规则的优先级根据它在规则列表中的位置来定。列表中的第一条规则具有最高的优先级。每一条手动创建的规则被添加到列表的顶部。而利用模板或提示创建的规则被添加到规则列表的底部。

要调整应用程序规则的优先级，请按照如下步骤操作：

1. 在**应用程序规则**标签页上选择应用程序名。
2. 在应用程序规则标签中，使用**向上**和**向下**按钮将规则在列表中移动，从而也改变了它们的优先级。

要调整包过滤规则的优先级，请按照如下步骤操作：

1. 在**包过滤规则**标签中选择规则。

2. 在包过滤标签中，使用**向上**和**向下**按钮将规则在列表中移动，从而也改变了它们的优先级。

11.6. 安全区域规则

在您的电脑上完成安装反黑客组件以后，它将会对您的计算机网络环境进行分析。根据此分析将整个网络空间划分为几个区域：

互联网– 万维网 在此区域，卡巴斯基反病毒工作站起到个人防火墙的作用。在这种情况下，默认的应用程序程序和包过滤规则将会管理所有的网络活动，以确保最大的安全保护。在此区域进行操作时您无法更改保护设置，但可以启用 Stealth 模式以提高安全性。

安全区 – 某些常规区域很大程度上相当于包括您计算机在内的子网 (这可以是家中或工作单位的本地子网)。这些区域通常属于中等危险级别。您可以根据对某一子网的信任程度更改这些区域的状态，并且可以配置包过滤和应用程序的规则。

如果启用“反黑客学习模式”，当您的计算机每次连接到一个新区域时都会打开一个窗口，显示基本的描述信息。您必须为该区域指定状态，基于这个状态的网络活动将会被允许。可能的状态值如下：

- **互联网。**这是对互联网区域的一个默认状态设置，因为当您在线时，您的计算机会受到所有潜在威胁的影响。同时也推荐将不受反病毒程序、防火墙、过滤规则等保护的网络区域设置为此状态。当您选择此状态时，该程序会在您使用这个区域时给您最大程度的保护，特别是：
    - 阻止子网内的任何网络 NetBios 活动
    - 阻止允许在子网内进行 NetBios 活动的应用和包过滤规则

  即使您已创建了共享文档夹，子网络中处于此状态的用户也不能使用该文件夹中的信息。此外，即使将该状态选定为某一子网络的设置，您也不能访问该子网络中的文件和打印机。
- **局域网。**该程序分析计算机的网络环境时，会指定以此状态访问侦测到的所有区域。建议将具有中等危险程度 (例如企业局域网) 的区域设置为此状态。如果您选择此状态，该程序将允许：
    - 子网内的任何网络 NetBios 活动
    - 允许在子网内进行 NetBios 活动的应用和包过滤规则

  如果您想要有权进入您计算机上的指定文件夹或打印机而阻止其它的网络活动，请选择此状态。

- **信任区域。**仅在您觉得您的计算机没有受到网络攻击或获取您计算机数据的尝试攻击的绝对安全的环境下推荐使用。如果您选择此状态，将允许所有网络活动。即使您选择了“最大程度保护”并创建了阻止规则，它们也不会对可信任网络的远程计算机的活动起作用。

请注意，对文件的任何约束或访问只限于在没有子网的情况下起作用。

使用指定为 **Internet** 的网络时，您可以使用*隐身模式*以提高安全程度。该功能只允许您的计算机发起的网络活动，也就是说在周围的网络中看不到您的计算机。该模式不会影响用户计算机的上网活动。

当计算机作为一台服务器 (例如：邮件或 HTTP 服务器) 使用时，我们不推荐使用“隐身模式”。否则，连接到服务器的计算机不会将它作为一个连接。

您计算机注册的区域列表将会在**区域**标签 (见图 48) 中显示出来。每一台都会被指定一个状态，网络的简要描述，以及是否使用“隐身模式”。

要更改区域的状态或启用/禁用“隐身模式”，从列表中选择区域并使用下表**规则描述**栏中相应的链接。您可以执行类似的任务，并在**区域设置**窗口编辑地址和子网掩码。点击**编辑**可以打开区域设置窗口。

查看列表时可以添加新的区域。为此，点击**刷新**。反黑客组件将会搜索要注册的潜在区域。如果检测到，该程序将提示您选择其状态。此外，您也可以手动将新区域添加到列表中 (例如，如果您将笔记本连接到新的网络中) 。为此使用**添加**按钮并在**区域设置**窗口填写必要的信息。

要删除列表中的网络，从列表中加以选定并点击**删除**按钮。

图 48. 区域规则列表

11.7. 防火墙模式

防火墙模式 (见图 49) 控制反黑客组件与建立多种网络连接的程序的兼容性，如网络游戏。

最大兼容性－防火墙确保反黑客组件在与其它的程序建立复杂的网络连接 (网络客户端文件共享) 时，处于最佳的工作模式。然而该模式会增加网络游戏的反应时间 如果您遇到这种问题时，建议您使用“快速响应模式”。

最快速度－在网络游戏时，防火墙会确保最可能快的反应时间。尽管如此，网络客户端文件共享或其它的网络应用可能会与这种模式产生冲突。要解决此问题，请禁用隐身模式。

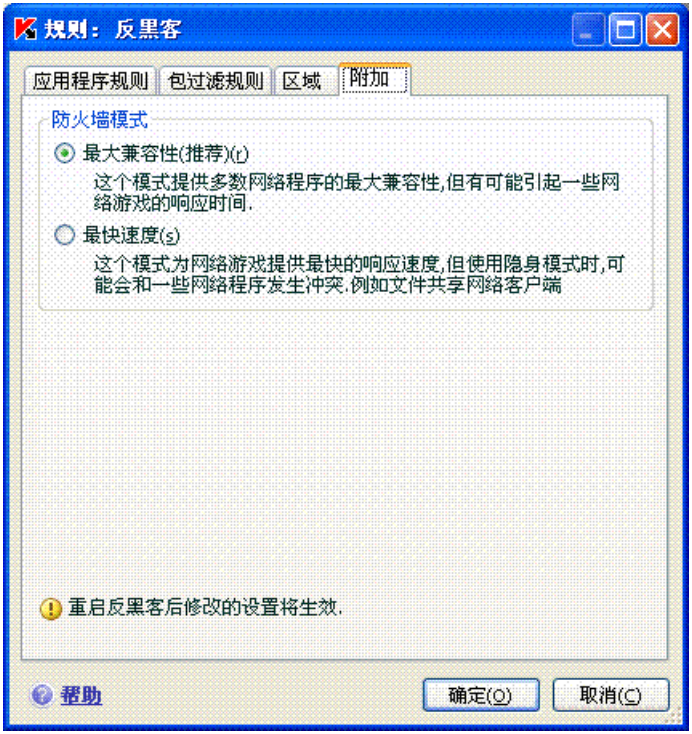


图 49. 选择反黑客模式

要选择防火墙模式：

1. 点击反黑客组件设置窗口的防火墙区域上的**设置**按钮。
2. 在打开的窗口中选择**附加**标签并选择您想要的模式，“最大兼容性”或“最快速度”。

改变防火墙设置后，反黑客必须重启才可以生效。

11.8. 配置入侵检测系统

反病毒数据库中列出了当前所知的、能危及您的计算机的所有网络攻击，并在特征库更新时获得更新。默认情况下，卡巴斯基反病毒不会更新防网络攻击特征库。

入侵监测系统能够跟踪典型的网络攻击类型，如果它检测到一个对您计算机的攻击，它会阻止您计算机上所有的网络活动，默认为一个小时。同时会在您的计算机屏幕上面显示一个受到网络攻击的提示信息，并包括攻击者计算机的具体信息。

您可以配置入侵监测系统。为此：

1. 打开反黑客设置窗口。
2. 点击**入侵监测系统**区域上的**设置**。
3. 在打开的窗口 (见图 50)，确定是否阻止网络攻击。如果选择阻止，阻止的时间为多长。默认阻止时间为 60 分钟。您可以更改**禁止计算机受攻击的时间为**旁的栏中的数值来增加或减少阻止时间。如果您想要停用阻止网络攻击这项功能，可取消选定该复选框。

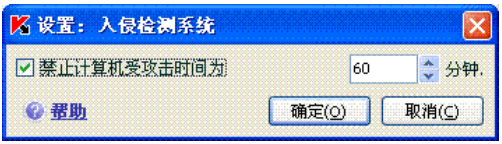


图 50. 配置网络攻击阻止时间

11.9. 侦测到的网络攻击列表

目前大多数种类的网络攻击是利用操作系统的漏洞和其它安装在您计算机上面的软件来实现的。犯罪分子经常采用网络攻击手法，学会如何去窃取机要信息，导致您系统发生故障，或者完全占有您的计算机并将其连接到陌生网络中去实施新的攻击。

为了确保您的计算机的安全，您必须了解可能会遇到的网络攻击类型。我们可以把常见的网络攻击划分为三类：

- **端口扫描**－这种网络威胁算不上真正意义的网络攻击，但是常常会被首先使用；因为这是一种获取远程计算机信息的普遍方式。使用 UDP/TCP 端口扫描的网络工具可以发现被扫描计算机的端口状态 (关闭或者打开) 。

  黑客可以通过端口扫描了解在用户计算机上面使用哪一种攻击类型起作用，哪种类型的攻击不能起作用。此外通过扫描所获得的信息还可以帮助黑客了解远程计算机用户使用的操作系统类型。这就进一步减少了潜在攻击类型的数目，相应花费在攻击上面的时间也会减少。 它也助长黑客尝试利用系统的漏洞去进行攻击。

- **Dos (拒绝服务) 攻击**－这些攻击手法可以导致被攻击的系统达到一个不稳定或者完全崩溃的状态。这些攻击的结果就是能够损坏或破坏目标计算机的信息资源，而使得用户无法使用那些资源。

  Dos 攻击的两个基本类型：

  - 向目标计算机发送经过特殊创造的、出乎目标计算机预料的数据包，从而可以导致整个系统的重新启动或死机。
  - 向目标计算机在很短的时间里面发送大量的数据包，消耗系统的资源，从而导致计算机无法运行。

  下面所列出是常见的这类攻击的例子：

  - *Ping of death* 攻击是将一个远远超过 64KB 的 ICMP 包不断地发送给目标计算机。这种攻击能够使一些操作系统崩溃。
  - *Land 攻击*是向您的计算机的一个开放端口发送一个请求并与它本身建立一个连接。发送的请求使得计算机进入一个循环之中，从而加重了进程的负担以及彻底中断操作系统的运行。
  - *ICMP Flood 攻击*就是向您的计算机发送大量的 ICMP 协议包。这种攻击将导致您的计算机不得不对每一个入站数据包进行应答，这将严重加重系统进程的负担。
  - *SYN Flood 攻击*就是向您的计算机发送大量的查询数据包并与您的计算机建立一个伪装的连接。由于系统处理那些连接的资源是一定的，这将会完全消耗掉您的系统的资源，计算机就会停止对其它尝试连接做出反应 (死机) 。

- **入侵攻击**，其目标就是控制您的计算机。这是一种最危险的攻击类型，如果攻击成功，黑客就可以完全进入您的计算机系统。

  当黑客们需要从一台远程的计算机上获取机密信息 (例如：信用卡号码或密码) 或者是他们想利用这台计算机的资源传播其它恶意程序 (在陌生的网络中使用这个控制的系统或作为实施新攻击的平台)，他们就会采用这种攻击。

  该类包含的攻击类型比其它类的要多。基于不同的操作系统，可以它们划分成三个子类：windows 攻击、Unix 攻击、对运行在操作系统上的其它服务的攻击。

  使用操作系统网络工具的常见的攻击类型是：

  - *Buffer overflow attacks (缓冲区溢出攻击)* －利用软件的漏洞，在处理大量的数据时，表面上是由于失控或无效控制。这是一种最原始的攻击类型而且更容易被黑客所利用。

- Format string attacks (格式串攻击) －利用软件的漏洞，发现程序在处理 I/O 设备的无效函数值如：来自 C 语言标准库的 printf(), fprintf(), scanf() 等其它函数。如果一个程序具有这个漏洞，一个黑客可以使用经过特别及时创造的查找程序能够获得对系统的完整控制权限。

入侵检测系统能够自动分析和拦截那些利用安装在用户计算机上的最常见网络工具 (FTP、POP3 和 IMAP) 的漏洞进行攻击的尝试。

Windows 平台的网络攻击，主要是利用安装在用户计算机上面的软件漏洞 (例如：微软的 SQL Server 、IE 浏览器、信使服务程序、和其它运行在网络中的系统组件－－DCom 、SMB 、Wins 、LSASS 、IIS5) 。

反黑客组件可以保护您的计算机，防止受到利用以下可知的软件漏洞而进行的攻击 (该列表中引用的是微软公司发布的系统漏洞信息)：

(**MS03-026**) DCOM RPC 漏洞(Lovesan 蠕虫)

(**MS03-043**) 微软信使服务缓冲区溢出

(**MS03-051**)微软 Frontpage 2000 服务器扩展缓冲区溢出

(**MS04-007**) Microsoft Windows ASN.1 漏洞

(**MS04-031**) Microsoft NetDDE Service 未授权远程缓冲区溢出

(**MS04-032**) Microsoft Windows XP 图文文件大量溢出

(**MS05-011**) Microsoft Windows SMB 客户端传输响应处理

(**MS05-017**) Microsoft Windows 信息队列缓冲区溢出漏洞

(**MS05-039**) Microsoft Windows 即插即用服务远程溢出

(**MS04-045**) Microsoft Windows Internet Naming Service (WINS) 远程大量溢出

(**MS05-051**) Microsoft Windows 分布式传输协调存储器修改

此外，也有利用各种恶意脚本而进行相关的入侵攻击事件，包括由 IE 浏览器和 Helkern-type 蠕虫执行的脚本。这种攻击类型基本上是由发送一个特殊的 UDP 数据包到远程的计算机并能执行恶意程序代码而实现的。

请注意，当您上网时，您的计算机每时每刻都处于被黑客攻击的风险之中。为了确保您的计算机安全，务必上网时启用反黑客组件并定期更新防网络攻击特征数据库。

11.10. 阻止和允许网络活动

如果防火墙的安全级别设置为**学习模式**，则在网络连接尝试没有规则可依时，屏幕上会显示特定的提示信息。

例如当您打开程序以后，该客户端就会连接到远程的服务器上。反黑客组件会始终跟踪这一类的网络活动。屏幕 (见图 51) 上将显示信息，包括如下内容：

- *活动描述*—应用程序名和连接初始化的主要特点。一般来说，已经被初始化的连接类型、本地端口以及连接地址都被显示出来。有关网络活动更详细的信息，请左键点击描述部分的任一地方。打开的窗口包含有连接的信息，初始化的进程，和应用开发商。
- *操作行为*—关于侦测到的网络活动，反黑客组件的一系列操作将会被显示出来。这就是要您自己来决定的。

图 51. 网络活动通知

仔细的查看网络活动的信息，然后只选择反黑客组件的执行操作。我们建议您做出决定后使用以下技巧：

1. 执行任何操作之前，请决定是允许还是阻止这个网络活动。在此情况下，一些已经被创建的应用程序或包过滤规则可能会对您有所帮助 (假设已创建) 。为此使用**编辑规则**链接。然后会打开窗口，显示已经创建的应用程序或数据包过滤规则的完整列表。

2. 然后决定是否去执行操作一次或当这个活动被侦测到时每次都自动执行。

如果仅此次执行该操作：

取消选中 **创建规则**复选框并点击活动名按钮，例如**允许**按钮。

为了在每次初始化时自动运行。

1. 选中 **创建规则**复选框。
2. 在**操作**区域，从下拉菜单列表中选择您所要执行操作的活动类型：
   - **所有活动**－该应用程序启动的任何网络活动。
   - **自定义** – 您必须在特殊窗口定义的特殊活动以及创建规则 (见 11.2.1 在 112 页)。
   - **<模版>** – 模板的名称，该模版包括程序典型的网络活动的规则组。如果卡巴斯基反病毒 6.0 Windows 工作站包括一个启动网络活动的应用程序的合适模板，则该网络活动类型将会显示在列表中(见 11.2.2 在 112 页)。在此情况下，您必须自定义要允许或被阻止的活动。使用模板并且将自动创建应用程序规则组。
3. 点击活动 (**允许**或**阻止**) 名按钮。

请注意，只有当所有连接参数与创建的规则相匹配，则该创建的规则才可以使用。例如，此规则不适用于从不同本地端口建立的连接。

第12章. 反垃圾邮件功能

能够检测到垃圾邮件，根据规则组进行处理并且使用邮件时能节省您的时间的卡巴斯基反病毒 6.0 Windows 工作站组件称为*反垃圾邮件*。

反垃圾邮件组件使用以下方法来确定邮件是否为垃圾邮件：

1. 扫描发信人地址是否与黑名单和白名单地址列表中的相匹配。
    - 如果发信人的地址在白名单里面，这封邮件就被标记为*接收*。
    - 如果发信人的地址在黑名单里面，这封邮件就被标记为*垃圾邮件*。根据您选择的操作作进一步处理 (见 12.3.8 在 143 页)。
2. 如果发信人的地址在黑名单和白名单中找不到，这封电子邮件就会被使用 PDB 技术进行垃圾邮件特征码的分析。(见 12.3.2 在 135 页)。分析中使用的是自学习反垃圾邮件数据库。
3. 反垃圾邮件技术能对电子邮件的文本进行详细的检查，并对黑名单或白名单进行扫描。
    - 如果电子邮件的文本包含白名单关键字行，则这封电子邮件就会标记为*接收*。
    - 如果包含黑名单短语列表中的短语，则该封电子邮件就会标记为*垃圾邮件*。根据您选择的操作作进一步处理。
4. 如果电子邮件的文本中不包含黑名单或白名单中的短语，就要对该封邮件进行网络钓鱼分析 如果电子邮件的文本中包含一个在反网络钓鱼攻击数据库中存在的网址时，则这封邮件就会被标记为*垃圾邮件*。根据您选择的操作作进一步处理。
5. 如果电子邮件中不包含网络钓鱼文本串，则要使用特殊技术对该封邮件进行扫描：
    - 使用 GSG 技术进行图像分析
    - 使用贝叶斯 (Bayes) 算法分析邮件信息文本，用来识别垃圾邮件
6. 最后根据安装反垃圾邮件组件安装时用户设置的高级垃圾邮件过滤选项进行邮件扫描。这包括对 html 超链接是否正确、字体或隐藏信息进行扫描。

对电子邮件进行垃圾邮件分析时，您可以启用或禁用扫描选项。

反垃圾邮件组件嵌入到了以下邮件客户端之中：

- Microsoft Outlook (见 12.3.9 在 143 页)
- Microsoft Outlook Express (见 12.3.10 在 146 页)
- The Bat! (见 12.3.11 在 147 页)

本选项仅支持运行 Microsoft Windows XP Professional x64 Edition 和 Microsoft Windows Vista x64 系统的计算机中的 32 位版本的 Microsoft Office Outlook 和 The Bat!

在 MS Outlook 和 Outlook Express 客户端的任务面板上面有两个按钮：**垃圾邮件**和**非垃圾邮件**，通过这两个按钮您可以设置反垃圾邮件组件，从而在您的邮件箱内能准确地侦测到垃圾邮件。然而 The Bat！中没有此按钮：但是使用**特殊**菜单上的**标记为垃圾邮件**和**标记为非垃圾邮件**的特殊项可以使该程序学习。此外，将垃圾邮件特殊处理参数 (见 12.3.1 在 135 页) 添加到电子邮件客户端的所有设置中。

反垃圾邮件组件使用了一种可修改的、自学习 Bayes 算法，这使得这个组件能够更加准确的区别垃圾邮件和可接收的邮件。算法的数据源就是电子邮件的内容。

有时，Bayes 算法不能十分准确的区分一封邮件是到底时垃圾邮件或者是可接收的邮件。这些邮件就会标记为*潜在的垃圾邮件*。

为了减少标记为潜在的垃圾邮件的数量，我们建议您为这类邮件执行附加的反垃圾邮件自学习功能。由此，您必须定义哪些邮件应该标记为*垃圾邮件*，哪些应该标记为*可接收的邮件*。

对被认为是*垃圾邮件*或*潜在垃圾邮件*的电子邮件进行修改：将标记 **[!! SPAM]** 或 **[?? Probable Spam]** 添加到相应的邮件标题中。

在 MS Outlook, Outlook Express 或 The Bat!邮件客户端的插件中，特别设定了处理垃圾邮件或潜在垃圾邮件的规则。对于其它的邮件客户端，您可以配置过滤规则，使其可以搜索到包含 **[!! SPAM]** 或 **[?? Probable Spam]** 的修改过的邮件标题，并将该邮件放到指定的文件夹中。有关过滤机制的详细的信息，请参见邮件客户端中的说明文档。

12.1. 选择反垃圾邮件组件的反应级别

卡巴斯基反病毒 6.0 Windows 工作站以如下级别保护您的计算机远离垃圾邮件(见图 52)：

阻止所有 – 最高反应级别, 除了在关键字白名单 (见 12.3.4.1 在 137 页) 中包含的以及发信人白名单包含的电子邮件之外，其它的任何电子邮件都会被阻止。其它任何邮件标记为*垃圾邮件*。在这个级别上，只根据白名单分析电子邮件。 禁用所有其它功能。

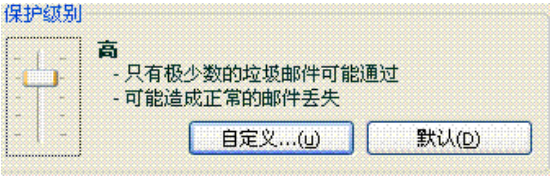


图 52. 选择反垃圾邮件组件的安全级别

高 – 当激活这个级别时，那些可能是垃圾邮件而实际上不是垃圾邮件的电子邮件将会标记为*垃圾邮件*。在此级别，使用白名单列表、PDB 和 GSG 技术和可修改的 Bayes 算法 (见 12.3.2 在 135 页) 对电子邮件进行扫描分析。

如果很有可能垃圾邮件发件人不知收件人地址，则应采用该级别。例如，收件人没有对大量邮件签名并且在非公司邮件服务器上没有邮件地址的情况。

推荐 – 划分邮件的标准设置级别。

在此级别可能会有一些垃圾邮件不被侦测到。这表明反垃圾邮件组件学习功能没有使用到位。我们建议您使用“学习向导” (见 12.2.1 在 131 页) 来执行额外的学习功能或者**“垃圾邮件/非垃圾邮件”**按钮 (或 The Bat！中相应的菜单项) 来标记不能准确判断的邮件。

低－最灵活的设置级别。如果用户接收的信件中，包含大量被认为是垃圾邮件的文本，但不被作为垃圾邮件，则推荐这样的用户使用。这可能是由于邮件收件人的专业性活动，而迫使用户在他们的信件中接收这个专业用户组，从而在同事之间广泛传播垃圾邮件。在此级别中，所有的垃圾邮件侦测技术都用来分析电子邮件。

允许所有 – 最低的反应级别。除了那些在关键字黑名单列表中的以及发信者黑名单中包含的电子邮件之外，所有其它的邮件都不会作为垃圾邮件。在此级别，只根据黑名单对电子邮件进行过滤。禁用所有其它功能。

在默认情况下，反垃圾邮件保护设置为**推荐的**反应级别。您可以提高或降低保护级别或者编辑当前级别的设置。

要修改保护级别：

在“反应”区域上下滑动滑块到所需设置。通过调节反应级别，您可以定义垃圾邮件、潜在的垃圾邮件和可接收的邮件之间的相关性要素。

要更改当前的设置级别：

在应用程序“设置”窗口，点击**反垃圾邮件**后显示组件设置。点击“反应”区域上的**自定义**按钮。 在打开的窗口中，编辑反垃圾邮件参数，完成后点击**确定**。

这样安全级别名称就更改为**自定义**。

12.2. 自学习反垃圾邮件功能

反垃圾邮件组件自带预安装的电子邮件数据库，它包含五十个垃圾邮件样本。建议您在您的电子邮件中更深入地使用反垃圾邮件模块的自学功能。

以下是使用自学习反垃圾邮件组件的几种方法：

- 使用“学习向导”(见 12.2.1 在 131 页)
- 对发出的电子邮件使用自学习反垃圾邮件功能
- 通过使用电子邮件客户端工具面板或菜单列表中的特殊按钮，直接对电子邮件进行自学习处理 (见 12.2.3 在 132 页)。
- 在反垃圾邮件报告中使用自学习处理 (见 12.2.4 在 133 页)。

使用自学习操作是使用反垃圾邮件组件的一个有力开始。可以在大量的电子邮件中，增强反垃圾邮件的自学习功能。

请注意，您不能用每个都超过 50 封电子邮件的文件夹来加强反垃圾邮件功能。如果在文件夹里面有更多的邮件，程序将使用每 50 封进行自学。

直接处理电子邮件时，如果使用邮件客户端界面上的特殊按钮进行自学习就更好 了。

12.2.1. 学习向导

“学习向导”可以使反垃圾邮件组件能够识别放置垃圾邮件和可接收邮件的文件夹。

要打开“学习向导”：

1. 选择设置窗口中的**反垃圾邮件**组件。
2. 点击设置窗口“学习”区域上的“**学习向导**”按钮。

“学习向导”采取循序渐进自学习反垃圾邮件的方式。使用**上一步**和**下一步**按钮进入进入上一步或下一步训练。

步骤一：包括选择收件箱所在的文件夹。在这一步中，您必须只选择一个文件夹存放您完全信任的内容。

步骤二：包括选择存放垃圾邮件的文件夹。

步骤三：反垃圾邮件组件在您选择的文件夹中被自动训练。那些文件夹中的电子邮件组成了反垃圾邮件数据库。可接收的电子邮件发送者的地址被自动加入到地址白名单中。

步骤四：使用下列方法来保存自学习功能的结果：添加自学的结果到当前的数据库中或将当前的数据库用自学的结果来替换。请记住：该程序必须自学至少 50 封可接收的电子邮件和侦测 50 封垃圾邮件，才能准确地工作。

为了节省时间，在每一个被选择的文件夹中，“学习向导”仅仅学习 50 封电子邮件。

12.2.2. 对发出的电子邮件进行学习

您可以在您的邮件客户端的发件箱中，自学反垃圾邮件功能。然后反垃圾邮件组件的地址白名单会加入发件箱的信息分析。仅仅只要学习开始的 50 封电子邮件，就可以完成自学习。

如何利用发件箱中的电子邮件自学反垃圾邮件功能：

1. 选择设置窗口中的**反垃圾邮件**组件。
2. 在**学习**区域选中 ☑ **利用发出的邮件来进行学习**。

警告！

在 Microsoft Outlook 的电子邮件反病毒插件 (见 12.3.9 在 143 页)中，如果您选中 ☑ **发送时扫描**选项，反垃圾邮件组件将仅仅对通过 MAPI 协议发送的电子邮件进行自学。

12.2.3. 使用邮件客户端学习

您可以使用您的电子邮件客户端的工具面板中的特殊按钮进行自学习。

当您在您的计算机上面安装反垃圾邮件组件时，它将在以下邮件客户端中安装插件：

- Microsoft Outlook
- Outlook Express
- The Bat!

例如，Outlook Outlook 的任务面板中有两个按钮，垃圾邮件和非垃圾邮件，以及在“选项”对话框(菜单项 **服务→ 选项**)的**卡巴斯基反病毒**标签 (见 12.3.9 在 143 页) 在 Outlook Express, 中，除了**垃圾邮件**和**非垃圾邮件**的这两个按钮，还在任务面板中增加了**设置**按钮。在检测到垃圾邮件时，任务面板会打开带处理操作的窗口 (见 12.3.10 在 146 页)。在 The Bat! 中，没有这些按钮，只是在程序的特殊菜单中使用了**标记为垃圾邮件**和**标记为非垃圾邮件**两个选项。

如果您确定当前打开的电子邮件是垃圾邮件，请点击**垃圾邮件**按钮。如果该邮件不是垃圾邮件，点击**非垃圾邮件**。在此以后，反垃圾邮件组件将会自学对邮件的处理。如果您选择了几封电子邮件，所有被选择的电子邮件将被会用来自学习。

警告！

万一当您需要立即处理几封电子邮件时，或者一个指定的文件夹仅仅包含一种类型的电子邮件 (垃圾邮件或不是垃圾邮件)，您就可以使用“学习向导”(见 12.2.1 在 131 页)功能进行并行处理。

12.2.4. 学习反垃圾邮件报告

通过这个报告，您可以选择自学习反垃圾邮件功能。

要查看反垃圾邮件组件的报告：

1. 选择程序主界面的**保护**窗口上的**反垃圾邮件**。
2. 左键点击**统计**窗口 (见图 53)。

反垃圾邮件组件的报告有助于您判断设置是否准确，如果有必要的话，对反垃圾邮件的设置进行一定的更正。

如何将某一邮件标记为垃圾邮件或非垃圾邮件：

1. 在**事件**标签框中的报告列表中选择一份报告，并使用**执行**按钮。
2. 从下列四个选项中选择其中一个：
   - **标记为垃圾邮件**
   - **标记为非垃圾邮件**
   - **添加到白名单**
   - **添加到黑名单**

图 53. 自学习反垃圾邮件报告

在此以后，反垃圾邮件组件将根据该邮件继续进行自学习。

12.3. 配置反垃圾邮件组件

调整反垃圾邮件组件中必要的垃圾邮件安全特征。在卡巴斯基反病毒 6.0 Windows 工作站设置窗口中可以允许您为所有的组件进行以下设置：

- 确定反垃圾邮件组件所进行的特殊操作 (见 12.3.1 在 135 页)
- 选择使用垃圾邮件过滤技术 (见 12.3.2 在 135 页)
- 控制对垃圾邮件和潜在的垃圾邮件识别的准确性
- 创建发送者和关键字的黑名单和白名单
- 配置额外的垃圾邮件过滤特性
- 尽量减少您的电子邮箱收件箱中的垃圾邮件数量

下面将详细介绍这些设置。

12.3.1. 配置扫描设置

您可以配置以下扫描设置：

- 是否扫描使用 POP3 、IMAP 协议传输的数据流。默认情况下，卡巴斯基反病毒扫描使用了这些协议。
- 是否激活 Outlook 和 The Bat!的插件功能。
- 在电子邮件从邮件服务器下载到用户的收件箱之前，应该通过 POP3 协议对电子邮件进行扫描 (见 12.3.6 在 142 页) 。

要配置这些设置：

1. 选择卡巴斯基反病毒 6.0 Windows 工作站设置窗口中的**反垃圾邮件**组件。
2. 选中或取消选中“连接”区域上与上述选项相对应的复选框 (见图 54)。
3. 必要时，编辑网络设置。

图 54. 配置扫描设置

12.3.2. 选择垃圾邮件过滤技术

垃圾邮件扫描采用了高级的过滤技术：

- **iBayes**，基于 iBayes 算法。通过分析邮件文本来检测将邮件标记为垃圾邮件的关键字。分析使用的数据来自自学习反垃圾邮件功能。
- **GSG**，使用特别的图片特征技术来侦测和分析包含图片信息的电子邮件中的垃圾邮件。
- **PDB**，基于启发式规则，根据邮件标题来分析和区分垃圾邮件。

默认情况下，启用所有这些过滤技术，并尽可能全面的检测出垃圾邮件。

要禁用这其中的过滤技术：

1. 在主界面打开反垃圾邮件设置窗口的设置链接。
2. 点击**反应**区域上的**自定义**按钮，然后在打开的窗口选择**垃圾邮件识别**标签 (见图 55)。

3. 取消选中过滤技术旁的复选框，就可以在检测垃圾邮件中停止使用这种技术。

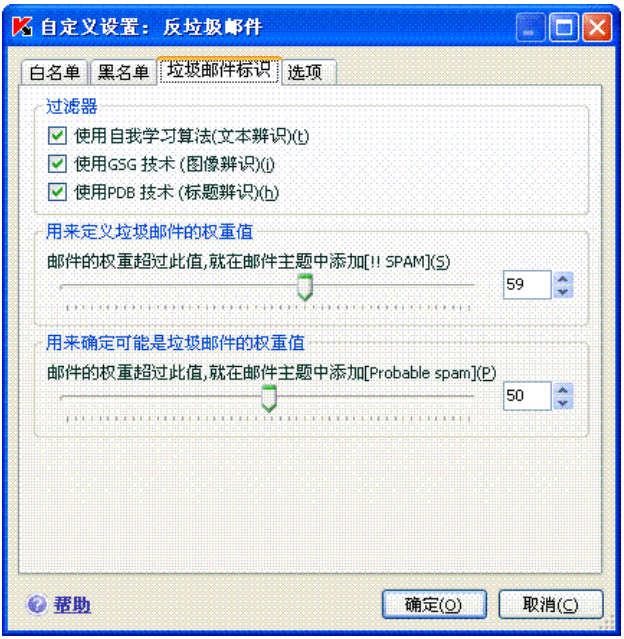


图 55. 配置垃圾邮件识别

12.3.3. 定义垃圾邮件和潜在的垃圾邮件参数

卡巴斯基实验室的专家们已经为反垃圾邮件组件去识别垃圾邮件和疑似垃圾邮件进行最佳的配置。

在最新的过滤技术下进行垃圾邮件的检测 (见 12.3.2 在 135 页)，并利用您邮箱的邮件通过自学习反垃圾邮件功能来准确地识别垃圾邮件、疑似垃圾邮件和正常的电子邮件。

使用“学习向导”并通过邮件客户端程序来进行反垃圾邮件的自学习。自学习期间，每一个可接收的电子邮件或垃圾邮件被指定为一个识别参数。当电子邮件进入您的收件箱时，反垃圾邮件组件会使用 iBayes 技术，根据这些参数来识别可接收的邮件或垃圾邮件。每一个参数都集中在一起，就形成了*垃圾邮件*和可*接收邮件的识别参数*。

疑似垃圾邮件参数可能会将一封电子邮件定义为疑似垃圾邮件。如果您使用**推荐**级别，任何处于 50% 和 59% 可能性的电子邮件将被认为是*疑似垃圾邮件*。在扫

描之后，可能性低于 50% 的电子邮件会被认为是正常的电子邮件。

垃圾邮件参数将决定反垃圾邮件组件把一封电子邮件作为垃圾邮件的可能性。任何一封可能性超出以上所列出的电子邮件将会被作为垃圾邮件。在推荐级别中，默认的垃圾邮件参数是 59% 。这意味着任何可疑性超过 59% 的电子邮件都被标记为垃圾邮件。

总之，有五个反应级别，其中三个(**高**、**推荐**和**低**)是基于不同垃圾邮件和潜在垃圾邮件的参数值。

您可以自行编辑反垃圾邮件算法。为此：

1. 选择卡巴斯基反病毒 6.0 Windows 工作站设置窗口中的**反垃圾邮件**组件。
2. 在窗口右边的**反应级别**框中，点击**自定义**。
3. 在打开的窗口中，在**垃圾邮件识别**标签 (见图 55)，调整垃圾邮件和潜在垃圾邮件的参数。

12.3.4. 手动创建白名单和黑名单

用户可以为使用反垃圾邮件组件手动创建黑名单和白名单。这些列表存储着用户地址信息，可以用它们来处理垃圾邮件以及根据关键字和短语来判断垃圾邮件。

关键字列表，尤其时白名单的主要应用在于您可以整理出可信的电子邮件地址 (例如：关于您同事的邮件信息) 以及包含特定关键字的特征库。例如您可以使用 PGP 特征库作为电子邮件特征库。您可以在特征库和地址中使用通配符：* and ?. A * 代表任何长度的任何字符串。 A ？ 代表任意一个字符。

如果特征库中有星号和问号，为防止发垃圾邮件组件在对其进行处理时出错，应在星号和问号前加反斜杠。使用 2 个字符而不是 1 个字符：* and \?。

12.3.4.1. 地址和短语的白名单

白名单包含您标记为接收邮件中的关键字以及不会发送垃圾邮件的可信任发件人的地址。白名单是手动添加的，并且发送者地址在学习反垃圾邮件组件中自动被添加。您可以编辑该名单。

要配置白色列表：

1. 选择卡巴斯基反病毒 6.0 Windows 工作站设置窗口中的**反垃圾邮件**组件。
2. 点击设置窗口右侧的“**设置**”按钮。

3. 打开**白名单**标签 (见图 56)。

该标签页分为两部分：上方包含正常邮件发送人的地址，下方包含这些邮件中的关键字。

要在反垃圾邮件过滤时启用短语和地址白名单，选中**允许发件者**和**允许短语**部分中相应的复选框。

您可以使用每一部分的按钮编辑名单。

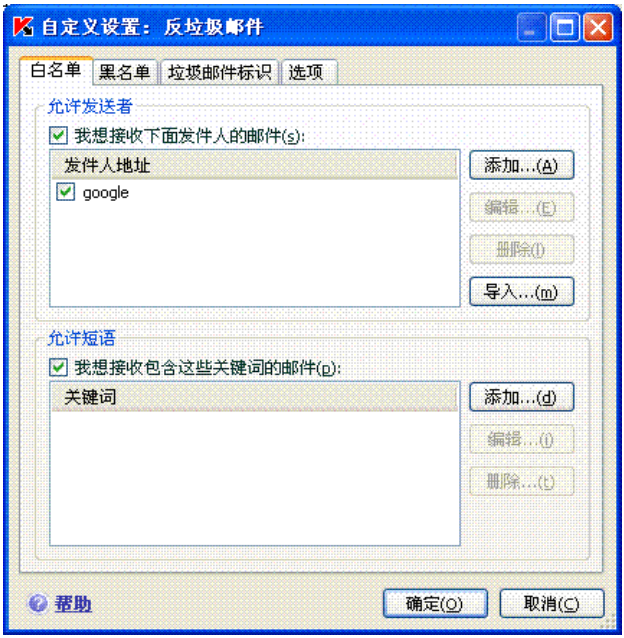


图 56. 配置地址和短语白名单

您可以在地址列表中指定地址和地址关键字。输入地址时，可以使用大写字母。让我们来看一些地址关键字的例子：

- *ivanov@test.ru* – 从该地址发送的邮件将总被认为是正常邮件。
- **@test.ru* – 域名为 test.ru 的任何发件人地址都被认为是正常邮件，例如: *petrov@test.ru*, *sidorov@test.ru*；
- *ivanov@** – 该名称的发件人,无论域名是什么都被认为是正常邮件，例如: *ivanov@test.ru*, *ivanov@mail.ru*；

- **@test** – 任何域名开始是 test 的电子邮件都被认为是正常邮件，例如: *ivanov@test.ru*, *petrov@test.com*；
- *ivan.*@test.???* 电子邮件发件人名是 ivan 开头的，域名开始是 test 结束是 3 个字符的将总被认为是正常邮件，例如：*ivan.ivanov@test.com*, *ivan.petrov@test.org*。

您可以使用短语关键字。输入短语时，可以使用大写字母。让我们来看一些地址关键字例子：

- *Hi, Ivan!* – 只包含该文本的邮件被认为是正常邮件。不推荐您使用类似短语做为白名单短语。
- *Hi, Ivan!** – 包含 Hi, Ivan! 短语开始的邮件被认为是正常邮件。
- *Hi, *! ** – 以问候 Hi 开头并且邮件中有感叹号的邮件不视为是垃圾邮件。
- ** Ivan? ** – 包含对名为 Ivan，并且名称后跟有任何字符的用户的问候的邮件不是垃圾邮件。
- ** Ivan\? ** – 包含短语 *Ivan?* 的邮件是正常邮件。

要禁用被认为是正常的地址和短语分类，可使用“删除”按钮予以删除，也可以取消选中文本旁的复选框将其禁用。

您可以选择使用可以导入 CVS 格式的白名单。

12.3.4.2. 地址和短语的黑名单

发送人黑名单包含从*垃圾邮件*中获取的关键字以及发送人的电子邮件地址。该名单需手动填写。

要填写黑名单：

1. 选择卡巴斯基反病毒 6.0 Windows 工作站设置窗口中的**反垃圾邮件**组件。
2. 点击设置窗口右侧的“**设置**”按钮。
3. 打开**黑名单**标签 (见图 57)。

该标签页分为两部分：上方包含垃圾邮件发送人的地址，下方包含这些邮件中的关键字。

要在反垃圾邮件过滤时启用短语和地址黑名单，选中**我不想接收下面发送者的邮件**和**我不想接收包含这些关键词的邮件**部分中相应的复选框。

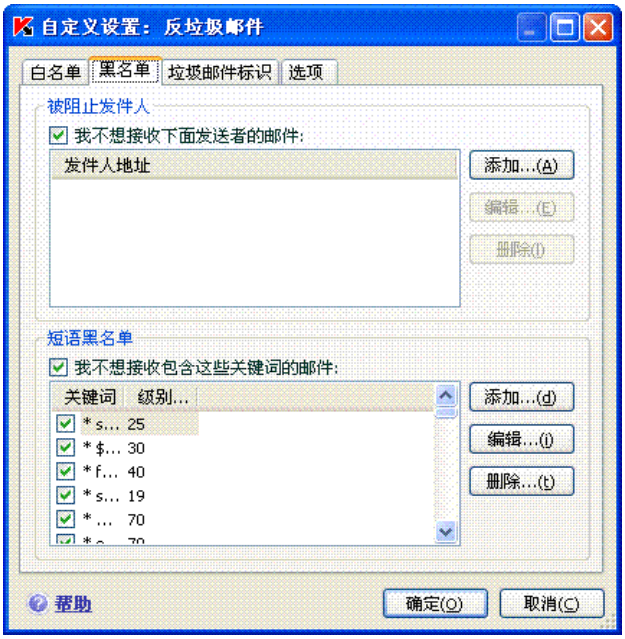


图 57. 配置地址和短语黑名单

您可以使用每一部分的按钮编辑名单。

您可以在地址列表中指定地址和地址关键字。输入地址时，可以使用大写字母。可以像前面部分的白名单一样使用地址关键字。

- 您可以使用短语关键字。输入短语时，可以使用大写字母。也可以像前面部分的白名单一样使用短语关键字。

要禁用被认为是垃圾邮件的地址和短语分类，可使用“删除”按钮予以删除，也可以取消选中文本旁的复选框将其禁用。

12.3.5. 附件的垃圾邮件过滤特点

除了被使用来过滤垃圾邮件的主要特点之外 (创建黑名单和白名单，网络钓鱼分析、过滤技术)，您还可以使用这些先进的功能。

要配置高级的垃圾邮件过滤功能：

1. 选择卡巴斯基反病毒 6.0 Windows 工作站设置窗口中的**反垃圾邮件**组件。
2. 点击设置窗口的“反应”区域上的**自定义**按钮。

3. 打开**其它**标签 (见图 58)。

该标签列表中一系列的指示器可以更好的区分垃圾邮件。

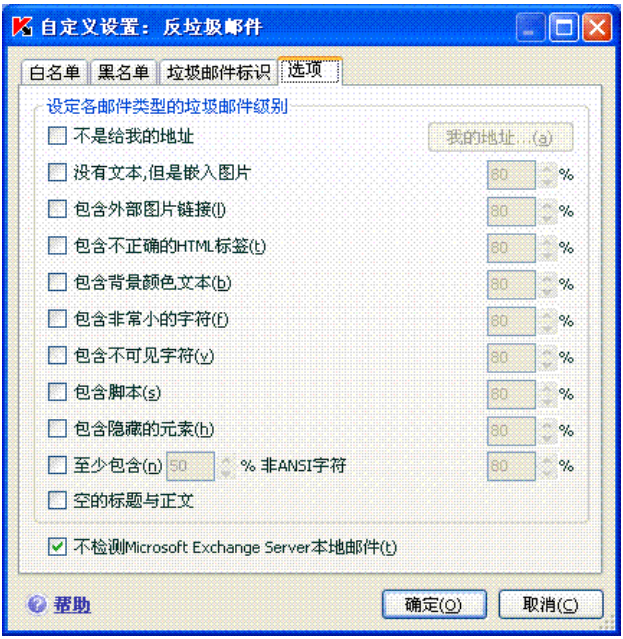


图 58. 垃圾邮件识别高级设置

要使用附加过滤指示器，选中该过滤指示器旁的复选框。每一项功能也要求您设置一个垃圾邮件参数 (百分比)，也是定义识别垃圾邮件的可疑性。垃圾邮件参数的默认值是 80%。如果所有附件的参数的可疑性总和超过 100 %，电子邮件将会标记为垃圾邮件。

垃圾邮件可能是空的电子邮件 (没有主体或正文)，包含与图像链接或嵌入图像的电子邮件，其文本与背景色相匹配或文本使用小号字体。垃圾邮件页可以是带有无形字符的电子邮件 (文本与背景色相匹配)，包含隐藏部分的电子邮件 (隐藏部分不显示)，以及含有脚本的电子邮件 (用户打开此类邮件时会执行一连串指令) 。

如果您启用“不是发给我的信息”过滤，则必须点击**我的地址**，在打开的窗口指定您的地址。

要使内联网(例如企业的电子邮件)内部转发的电子邮件免于病毒扫描，选中 **不要扫描内部的 Microsoft Exchange 服务器** 邮件。请注意，如果网络上的所有计算机都使用 Microsoft Office Outlook 作为它们的邮件客户端，并且如果用户的电子邮箱位于一个 Exchange 服务器上，或者这些服务器必须与 X00 接头连接，则

电子邮件将视为是内部邮件。如若要使反垃圾邮件组件分析这些邮件，则取消选中该复选框。

12.3.6. 创建可信任地址列表

如果您启用了“不是发给我的信息”的垃圾邮件过滤功能，您必须指定您信任的电子邮件地址。

分析电子邮件时，将扫描收件人的地址。如果这个地址与您的列表中不匹配，电子邮件将会标记为*垃圾邮件*。

在**我的电子邮件地址**窗口，您可以使用**添加**、**编辑**、和**删除**按钮创建和编辑地址列表。

12.3.7. 邮件收发器

警告！

邮件收发器只对通过 POP3 协议接收的邮件有效。

邮件收发器是设计用来在服务器上查看电子邮件的信息，而不需要将它们下载到您的计算机。您可以通过这种方式拒绝接收信息，在工作中节省时间和金钱，降低将垃圾邮件和病毒下载到您的计算机上的可能性。

如果选中反垃圾邮件设置窗口中  **接收电子邮件时打开邮件收发器**复选框，则打开“邮件收发器”。

要从服务器上直接删除子邮件而五要将其下载到您的计算机：

选中要删除的电子邮件左侧的复选框，并点击**删除**按钮。被选中的电子邮件将会从服务器删除。关闭“邮件收发器”窗口后，您其余电子邮件将会下载到您的计算机上。

有时很难根据电子邮件的主题和发送人的地址来决定是否接收该邮件。在此情况下，“邮件收发器”通过将邮件标题下载下来，从而为您提供更多的信息。

要查看电子邮件标题：

从接收的电子邮件列表中选择电子邮件。电子邮件的标题将显示在该窗口的下方。

电子邮件标题不大，一般是几十字节，而且也不可能包恶意程序代码。

这里是一个可以帮助你查看邮件标题的例子：垃圾邮件制造者将会在一台被控制的用户计算机上安装一个恶意程序，并使用该用户名向邮件客户端列表中的用户发送垃圾邮件。如果你在被控用户的联系列表中的可能性非常高，毫无疑问，您的收件箱被垃圾邮件将会塞满他发送的垃圾邮件。光凭发送人的地址很难分辨出

垃圾邮件是由你的同事或是垃圾邮件制造者发送的。然后电子邮件标题会显示这些信息，使您可以检查邮件发送人，邮件的大小并追踪邮件从发送人到您的邮件服务器的路径。电子邮件标题中应包括所有这些信息。然后您决定是否有必要将电子邮件从服务器上下载下来或还是将其删除。

注意：

您可以按照电子邮件列表上的任何栏来整理电子邮件。点击栏标题来整理邮件。各行将按照向上顺序进行整理。要更改整理的方向，重新点击栏标题。

12.3.8. 处理垃圾邮件

如果您在扫描后发现邮件是垃圾邮件或潜在的垃圾邮件，则反垃圾邮件组件将要采取的处理操作要取决于所选择的对象状态和处理操作。默认情况下，将修改垃圾邮件或潜在垃圾邮件：将标记 **[!! SPAM]** 或 **[?? Probable Spam]** 添加到相应的邮件标题中。

您可以为垃圾邮件或潜在的垃圾邮件选择其它的操作。在 Microsoft Outlook、Outlook Express 以及 The Bat! 邮件客户端中，将提供进行处理操作的专用插件。对于其它的电子邮件客户端软件，您可以配置过滤规则。

12.3.9. 在 MS Office Outlook 中设置垃圾邮件处理方式

请注意，如果该程序在 windows9x 下运行，则 MS Outlook 中就没有垃圾邮件插件。

本选项仅支持运行 Microsoft Windows XP Professional x64 Edition 和 Microsoft Windows Vista x64 系统的计算机中的 32 位的 Microsoft Office Outlook 。

默认情况下，被反垃圾邮件组件归类为垃圾邮件或潜在垃圾邮件的电子邮件在邮件主题上面会标记**[!! 垃圾邮件]** 或 **[?? 疑似垃圾邮件]**字符串。

您可以从**服务→ 选项**菜单上的特殊**反垃圾邮件**标签 (见图 59) 查找到对 Outlook 中的垃圾邮件和潜在垃圾邮件的其它操作。

安装程序之后，当您首次打开邮件客户端时，它会自动打开一个窗口并提示您是否要设置垃圾邮件处理方式。

您可以为垃圾邮件和潜在垃圾邮件指定以下的处理规则：

移动到文件夹－垃圾邮件被移动到指定的文件夹。

复制到文件夹－复制邮件并将其移动到指定的文件夹。电子邮件原件保留在您的收件箱中。

删除－从用户的邮箱中删除垃圾邮件。

忽略－您的收件箱中保留该邮件。

操作方法：在**垃圾邮件**或**疑似垃圾邮件**区域的下拉列表中选择适当的值。

图 59. 在 MS Office Outlook 中设置垃圾邮件处理方式

您也可以将 Microsoft Office Outlook 和 Anti – Spam 配置为关联。

- **接收邮件时扫描**。对所有进入用户收件箱的电子邮件都会根据 Outlook 的规则进行初步处理。处理完后，反垃圾邮件插件将会对不属于任何规则的剩余信息进行处理。换句话来说是根据规则的优先级处理邮件。有时可能会忽略优先顺序，例如，如果大量的电子邮件同时到达您的邮箱。在此情况下，有时在反垃圾邮件报告，有关 Outlook 规则处理邮件的信息中会被当成*垃圾邮件*记录下来。为了避免此情况的发生，我们建议您将反垃圾邮件插件配置为 Outlook 的规则。
- **使用 Microsoft Outlook 规则。**如果选择此选项，将按照创建的 Outlook 规则的优先级处理接收到的信息。规则之一就是必须使用反垃圾邮件组件处理电子邮件。这才是最佳配置。 这将不会造成 Outlook 和反垃圾邮件插件之间的冲突。惟一的缺点就是您必须通过 Outlook 手动创建和删除垃圾邮件处理规则。

如果您运行的是 9x/ME/NT4 操作系统，反垃圾邮件插件将不能作为 Microsoft Office XP 中 Outlook 的规则使用，否则会导致 Outlook XP 出错。

要创建垃圾邮件处理规则：

1. 打开 Microsoft Outlook ，在主菜单中选择**服务→规则和警报**。打开“向导”的命令取决于您的 Microsoft Outlook 版本。本“用户指南”说明了如何使用 Microsoft Office Outlook 2003 创建规则。

2. 在打开的**规则和警报**窗口，点击**电子邮件规则**标签上的**新规则**打开“规则向导”。**规则向导**将引导您按照以下步骤进行操作：

   步骤一

   你可以选择从头开始创建规则还是利用模版创建规则。选择**从空白规则开始**并选择**收到邮件时检查邮件信息**。点击“**下一步**”按钮。

   步骤二

   在**规则条件**窗口点击**下一步**而不选中任何复选框。在对话框中确认您想要将该规则应用到所有接收的电子邮件。

   步骤三

   在选择将操作应用到邮件信息的窗口中，选中操作列表中的☑ **执行自定义操作**复选框。点击该窗口下方的自定义操作。在打开的窗口，从下拉菜单选择**卡巴斯基反病毒**并点击**确定**。

   步骤四

   在例外规则选择窗口，点击**下一步**而不选中任何复选框。

   步骤五

   在完成规则创建的窗口，您可以对规则名进行编辑 (默认为**卡巴斯基反垃圾邮件**)。确保选中☑ **应用规则**复选框并点击 **完成。**

3. 在**电子邮件规则**窗口，新规则的默认位置在规则列表的首位。如果需要的话，可以将规则移动到列表的末尾，从而在邮件扫描时，最后才应用到该规则。

所有收取的电子邮件都会被这些规则进行处理。这些规则的应用顺序取决于规则的优先级。列表顶部的规则比其偏下的规则具有根高的优先级。您可以针对电子邮件改变规则应用的优先级。

如果应用一个规则之后，您不想反垃圾邮件保护规则对电子邮件作进一步处理，则必须选中规则设置中的☑ **停止处理更多的规则** (见创建规则中的“步骤三”)。

如果您在 Outlook 中创建电子邮件的处理规则方面很有经验，您可以根据我们所建议的设置创建您自己的反垃圾邮件规则。

12.3.10. 在 Outlook Express 中设置垃圾邮件处理方式

默认情况下，被反垃圾邮件组件归类为垃圾邮件或潜在垃圾邮件的电子邮件在邮件主题上面会标记**[!! 垃圾邮件]** 或 **[?? 疑似垃圾邮件]**字符串。

点击任务面板上**垃圾邮件**和**非垃圾邮件**按钮旁的**配置**按钮，在打开的设置窗口 (见图 60) 您可以找到 Outlook Express 中垃圾邮件和潜在垃圾邮件的其它处理操作。

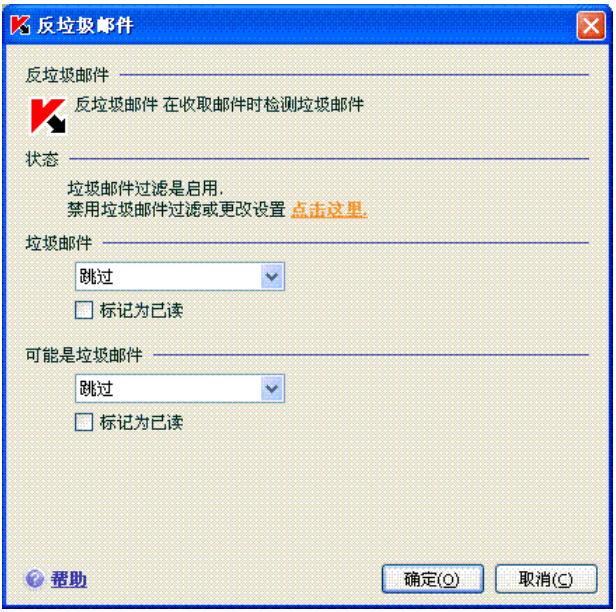


图 60. 在 Microsoft Outlook Express 中设置垃圾邮件处理方式

安装程序之后，当您首次打开邮件客户端时，它会自动打开一个窗口并提示您是否要设置垃圾邮件处理方式。

您可以为垃圾邮件和潜在垃圾邮件指定以下的处理规则：

移动到文件夹－垃圾邮件被移动到指定的文件夹。

复制到文件夹－复制邮件并将其移动到指定的文件夹。电子邮件原件保留在您的收件箱中。

删除－从用户的邮箱中删除垃圾邮件。

忽略－您的收件箱中保留该邮件。

操作方法：在**垃圾邮件**或**疑似垃圾邮件**区域的下拉列表中选择适当的值。

12.3.11. 在 The Bat！中设置垃圾邮件处理方式

本选项仅支持运行 Microsoft Windows XP Professional x64 Edition 和 Microsoft Windows Vista x64 系统的计算机中的 32 位的 The Bat！。

The Bat! 客户端自带工具定义了对其垃圾邮件和潜在垃圾邮件的处理操作。

要在 The Bat! 中设置垃圾邮件处理规则：

1. 从邮件客户端的**属性**菜单中选择**设置**。
2. 从设置目录树选择**反垃圾邮件** (见图 61)。

显示的垃圾邮件保护设置扩展到所有安装在计算机上的支持 The Bat!的反垃圾邮件模块。

您必须设置等级并指定对某等级电子邮件的处理方式 (如果是反垃圾邮件，则该邮件可能是垃圾邮件)：

- 删除等级高于给定值的电子邮件。
- 将某一范围等级的电子邮件移动到特定的垃圾邮件文件夹中。
- 将标记有特殊标题的垃圾邮件移动到垃圾邮件文件夹中。
- 将垃圾邮件保留在您的收件箱中。

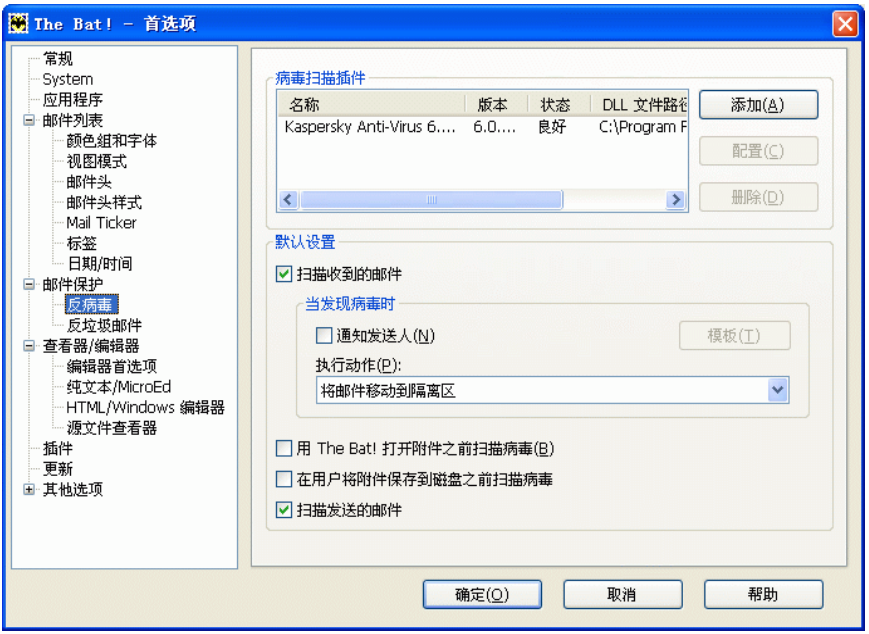


图 61. 在 The Bat!中设置垃圾邮件识别和处理方式

警告！

在处理完邮件后，卡巴斯基反病毒 6.0 Windows 工作站可以根据参数确定定该邮件是垃圾邮件或潜在垃圾邮件状态。为了确保在卡巴斯基反病毒 6.0 Windows 工作站和 The Bat! 的垃圾邮件参数之间没有差别，根据 The Bat!使用的电子邮件状态类别，指定所有被反垃圾邮件组件扫描过的电子邮件一个评级： *可接收的邮件 – 0%*, *疑似的垃圾邮件 – 50 %*, 垃圾邮件 – *100 %*。

这样，The Bat! 中的垃圾邮件的等级与反垃圾邮件组件中指定的邮件参数不一致，但是与反垃圾邮件组件中指定的相应状态参数一致。

欲了解更多垃圾邮件等级和处理规则的详细信息，请查看 The Bat! 的文档。

第13章. 扫描病毒

对用户自定义区域进行病毒扫描是保护您的计算机的重要方面之一。 卡巴斯基反病毒 6.0 Windows 工作站以为单个文件（文件夹，磁盘，即插即用设备）或者整个计算机进行病毒扫描。 扫描病毒是为了防止未被保护组件发现的恶意代码传播。

卡巴斯基反病毒工作站提供三个默认扫描任务：

关键区域

扫描计算机的所有关键区域，包括 系统内存、系统启动项、硬盘引导扇区以及 *Windows* 和 *system32* 系统目录。扫描任务的目的在于快速检测到激活的病毒而不必对计算机进行全面扫描。

我的电脑

对您计算机中的所有磁盘驱动器、内存以及文件进行全面的病毒检测。

启动对象

扫描所有系统启动时加载的程序。

推荐使用这些任务的默认设置。您可以编辑这些设置 (见 13.4.4 在 156 页) 或为运行的任务创建计划。

您同样可以选择创建您自己的任务 (见 13.4.3 在 156 页) 并为其创建计划。例如，您可以创建每周扫描电子邮件数据库一次的任务，或“**我的电脑**”文件夹的病毒扫描任务。

此外，您还可以扫描任何的对象 (例如磁盘中的程序和游戏，从公司带回家的邮件数据库以及邮件附件等等) 而不需创建特殊的扫描任务。您可以从卡巴斯基反病毒 6.0 Windows 工作站界面选择扫描目标或使用在 windows 系统的标准工具进行选择 (例如 windows **资源管理器**或您的**桌面**等等)。

通过点击程序主窗口左侧面板上的**扫描**，您就可以查看您的计算机的整个扫描任务列表。

13.1. 管理病毒扫描任务

您可以使用扫描任务手动或自动运行病毒扫描

要手动开始病毒扫描任务：

在主窗口的**扫描**区域选中任务名旁的复选框，并点击状态栏上的 ▶ 按钮。

右键点击系统托盘图标后，当前执行的任务 (包括通过卡巴斯基 Administration Kit 创建的任务) 就显示在快捷菜单上。

要暂停任务：

点击**状态栏**上的 ⏸ 按钮。任务状态将更改为*暂停*。它将暂停扫描直到您再一次手动启动或再一次按照计划启动。

要停止任务：

点击**状态栏**上的 ■ 按钮。任务状态将更改为*停止*。它将停止扫描直到您再一次手动启动或再一次按照计划启动。下次您启动这个任务时，它将提示您是否继续已停止的任务还是重新开始任务。

13.2. 创建扫描对象列表

要显示特殊扫描任务的扫描对象列表，在主窗口**扫描**区域选择任务名 (例如**我的电脑**) 状态栏下方窗口的左侧将显示对象列表 (见图 62)。

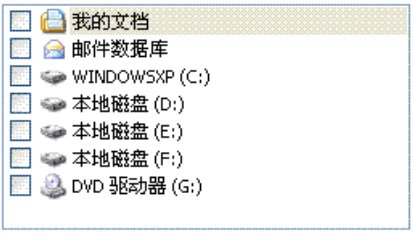


图 62. 扫描对象列表

安装程序时创建的默认任务的对象扫描列表已经创建好。当您创建自己的任务或选择一个目标进行扫描时，您可以创建一个扫描列表。

您可以使用列表右侧的按钮添加和编辑对象扫描列表。要将一个新对象添加到列表中，点击**添加**按钮并在打开的窗口中选择要扫描的对象。

为了方便用户，您可以添加类别来扫描邮件数据库、RAM、启动对象、操作系统备份件以及卡巴斯基反病毒隔离区文件夹中的文件等区域。

此外，当您将包含嵌入式对象的文件夹添加到扫描区时，您可以对该递归进行编辑。为此使用快捷菜单上相应的选项。

从列表选择对象 (选好后，对象名会显灰) 并点击**删除**按钮予以删除。您可以暂时禁用扫描单个对象而不需将其从任务列表中删除。为此取消选定不需要扫描的对象复选框。

要启动一个扫描任务，点击**扫描**按钮，或从您点击**操作**按钮时打开的菜单中选择**开始**。

此外，您还可以使用 windows 系统的标准工具 (例如 windows 资源管理器或您的桌面等) 选择扫描对象 (见图 63)。操作方法是，选择对象，右键打开快捷菜单并选择**扫描病毒**。

图 63. 从 Windows 快捷菜单扫描对象

13.3. 创建病毒扫描任务

要对计算机上的对象进行扫描，您可以使用程序自带的内置扫描任务并创建您自己的扫描任务。使用现有任务创建新的扫描任务。

要创建新的病毒扫描任务：

1. 在程序主窗口的**扫描**区域选择与您所需的设置最接近的任务。
2. 右键点击任务名，打开快捷菜单，或点击扫描对象列表右侧的**操作**按钮并选择**另存为**。
3. 在打开的窗输入新任务名并点击**确定**。在主窗口**扫描**区域的任务列表中将显示任务以及任务名。

警告！

用户能够创建的任务数量是有限制的。最多可以创建四项任务。

新任务是在原有任务的基础上创建的。您必须连续设置，做法是创建扫描对象列表 (见 13.4.2 在 154 页、设置任务属性 (见 13.4.4 在 156 页) 以及必要的话，配置自行执行任务的计划。

要重命名任务：

选择程序主界面的**扫描**区域上的任务。右键点击任务名，打开快捷菜单，或点击病毒扫描列表右侧上的**操作**按钮并点击**重命名**。

在打开的窗输入新任务名并点击**确定**。**扫描**区域上的任务名也会更改。

要删除任务：

选择程序主界面的**扫描**区域上的任务。右键点击任务名，打开快捷菜单，或点击病毒扫描列表右侧上的**操作**按钮并点击**删除**。

经提示，对您想要删除的任务予以确定。该任务将从**扫描**区域上的任务列表中删除。

警告！

您只能重命名和删除您已创建的任务。

13.4. 配置病毒扫描任务

对您计算机上的目标进行扫描的方法是由每一扫描任务的属性决定的。

要配置任务设置：

选择主界面的**扫描**区域上的任务名，并使用设置链接打开任务设置窗口。

您可以使用设置窗口为每一任务：

- 选择任务将要使用的安全级别 (见 13.4.1 在 153 页)。
- 编辑高级设置：
    - 定义要 扫描的文件类型 (见 13.4.2 在 154 页)。
    - 使用不同的授权帐户配置任务启动 (见 5.4 在 57 页)
    - 配置高级扫描设置 (见 13.4.5 在 158 页)
- 恢复扫描默认设置 (见 13.4.3 在 156 页)
- 选择一个发现被感染或可疑程序时的处理动作 (见 13.4.4 在 156 页)

- 创建自动执行任务的计划。

此外，您也可以配置执行所有任务的全局设置。

下面将详细介绍上述的任务设置。

13.4.1. 选择安全级别

每个扫描任务可以指定一个安全级别 (见图 64)：

高 – 对整个计算机，或单个磁盘，文件夹或文件执行最全面的扫描。如果您怀疑您的计算机被感染病毒，我们推荐您使用该级别。

推荐 – 卡巴斯基实验室专家推荐您使用该安全级别。除邮件数据库外，同样的文件将按照**高**安全级别设置进行扫描。

低 – 如果您使用的应用程序需要大量的系统资源时您可以选择该安全级别，因为文件扫描范围将缩小。

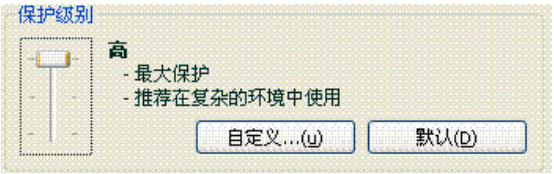


图 64. 选择病毒扫描保护级别

默认情况下，文件扫描级别设置为**推荐**。

您可以调高或调低扫描保护级别，或变更当前的安全级别设置。

要编辑安全级别：

调整滑块。您可以调整安全级别来定义扫描速度与总的扫描文件数量之比： 更少的文件以更高速度进行病毒分析，

如果所列的安全级别不能满足您的需要，您可以自定义扫描设置。为此选择最符合您需要的级别作为起点并对其设置进行编辑。这样，将安全级别重命名为**自定义**。

如何更改安全级别：

点击任务设置窗口上的**设置**按钮。在打开的窗口中编辑扫描设置数，并点击**确定**。

结果将创建第四安全级别-**自定义设置**，它包含您配置的扫描设置。

13.4.2. 定义扫描的对象类型

通过指定要扫描的文件类型，您可以确定执行该任务时将要扫描的文件格式、大小以及驱动器。

在**文件类型**窗口定义扫描文件的类型 (见图 65)。可以选择三个选项中的一项：

- **扫描所有文件**。如果选定该选项，将毫无例外地扫描所有对象。
- **扫描程序和文档（根据内容）**。如果选择该程序组，只扫描潜在受病毒感染的文件，病毒可能已嵌入该种文件。

  注意：

  有些文件，病毒是无法嵌入的，因为此类文件不含任何病毒代码。例如.txt 文件。

  反之有些文件格式含有或可能还有可执行代码。例如.exe、.dll 或 .doc 格式。恶意代码侵入这类文件并被激活的可能性非常高。

  在对对象进行病毒扫描之前，分析文件内部头的文件格式 (例如 txt、doc、exe 等)。

- **扫描程序和文档**(按扩展名)。如果选择该选项，程序只扫描可能受病毒感染的文件，但是文件的格式由文件扩展名来确定。使用链接，您可以查看被扫描的扩展名列表 (见 节 292 页)。

提示：

小心有人会发送病毒到您的计算机。有些时候，扩展名为 txt 的文件有可实际上是一个改名为 txt 文件的可执行文件。如果您选择 **(按扩展名) 扫描程序和文件**项，扫描时将跳过这类文件。如果选择 **(按内容) 扫描程序和文件** 项，程序将分析文件头，发现该文件为可执行文件并对其进行全面扫描。

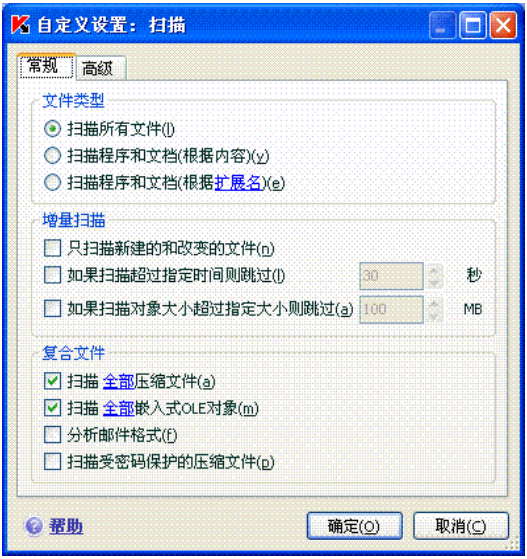


图 65. 配置扫描设置

提示：

小心有人会发送病毒到您的计算机。有些时候，扩展名为 txt 的文件有可实际上是一个改名为 txt 文件的可执行文件。如果您选择 **(按扩展名) 扫描程序和文件**， 扫描时将跳过这类文件。如果选择 **(按内容) 扫描程序和文件**，程序将分析文件头，发现该文件为可执行文件并对其进行全面扫描。

您可以在**常规**窗口中指定只扫描新文件以及自上一次扫描以来已修改的文件。该模式明显减少了扫描时间并提高了程序的运行速度。为此，您必须选中☑ **只扫描新建的和改变的文件**项。该模式既适用于简单文件，也适用于复合文件。

您也可以在**常规**区域设定扫描时间以及要扫描的文件大小。

☑ **如果扫描超过指定时间则跳过。**选中该复选框并输入扫描对象的最大时间。如果扫描时间超过该时间，则该对象将从扫描队列移出。

☑ **如果扫描对象大小超过指定大小则跳过**。选中该复选框并输入扫描对象的最大尺寸。如果超过该大小，则该对象将从扫描队列移出。

在**复合文件**选项指定要分析的复合文件：

☑ **扫描 全部/压缩文件** – 扫描 .rar, .arj, .zip, .cab, .lha, .jar, and .ice 文件。

警告！

如果无法修复对象，即使您选择自动修复或删除选项，卡巴斯基反病毒页不会自动删除它不支持的压缩文件格式 (例如 .ha, .uue, .tar)。

要删除此类压缩文件，点击危险对象检测通知中的删除压缩文件链接。程序开始处理扫描过程中检测到的对象后，屏幕上会显示该通知。您也可以手动删除感染病毒的压缩文件。

☑ **扫描 所有 嵌入式 OLE 对象** – 扫描嵌入文件中的对象(例如 MS Office Excel 表格或嵌入 MS Word 文件、电子邮件附件等的宏文件)。

对于每一类型的复合文件，可以选择并扫描所有文件或只扫描新建文件。为此使用对象名旁边的链接。左键点击该链接可以改变其值。如果在**常规**窗口设置为只扫描新建和已发生变化的文件，您将无法选择要扫描的复合文件类型。

☑ **分析邮件格式**-扫描邮件文件和邮件数据。如果选中该复选框，卡巴斯基反病毒将不扫描邮件格式文件并且分析邮件的每一部分 (正文、附件等) 如果取消选中该复选框，该格式的文件将作为单一对象被扫描。

请注意，在扫描密码保护的邮件数据库时：

- 卡巴斯基反病毒 6.0 Windows 工作站在 Microsoft Office Outlook 2000 数据库中检测到恶意代码，但不会予以清除；
- 卡巴斯基反病毒 6.0 Windows 工作站不支持扫描 Microsoft Office Outlook 2003 受保护数据库中的恶意代码。

☑ **扫描受密码保护的压缩文件** - 扫描受密码保护的压缩文件。如果选择该项，则在扫描压缩包文件之前，请求窗口会弹出，提示输入密码。如果未选中该复选框，将不扫描受密码保护的压缩文件。

13.4.3. 恢复默认扫描设置

配置扫描任务设置时，您始终可以返回到推荐的设置。卡巴斯基实验室专家认为它们是最佳设置，并将它们集成在**推荐的**安全级别中。

要恢复默认的扫描设置：

1. 选择主界面的**扫描**区域上的任务名，并使用设置链接打开任务设置窗口。
2. 点击**安全级别**区域上的**默认**按钮。

13.4.4. 为对象选择处理动作

如果扫描时发现文件被感染病毒或是疑似感染病毒，则卡巴斯基反病毒组件所要采取的处理操作要取决于所选择的对象状态和处理操作。

扫描完后，以下其中之一的状态可以赋予对象：

- 恶意程序状态 (例如 *病毒*、*木马*)。
- 潜在受感染，此时通过扫描无法确定对象是否受感染。这是指该文件部分代码与已知的恶意代码类似，或者是类似以前的病毒串结构。

默认情况下，将清除所有感染病毒的文件。如果它们潜在受到感染，则会被放到“隔离区”。

要为对象编辑处理动作：

选择主界面的**扫描**区域上的任务名，并使用设置链接打开任务设置窗口。在适当的窗口显示潜在的处理动作 (见图 66)。

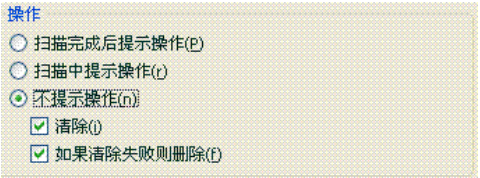


图 66. 为危险对象选择处理操作

处理动作	**发现恶意或潜在受感染的对象时**
扫描完成后提示操作	这个程序不处理对象直到扫描结束， 当扫描完成时统计窗口弹出， 显示检测到的对象的列表，并提示您是否要处理这些对象。
扫描中提示操作	程序将发出警告信息，提示哪些恶意代码已经感染或潜在感染了该文件，并且提供给您选择如下操作选择。
不提示操作	程序将检测到的对象的信息记录在报告中而没有处理或提示用户。我们建议您不要使用该功能，因为被感染以及潜在被感染的对象将驻留在您的计算机上，因此要避免病毒感染是不可能的。
不提示操作 **清除**	程序尝试去处理检测到的对象而未要求用户确认。如果未能清除病毒，该文件将指定为*潜在受感染*状态，并被放到“隔离区”。报告中记录了有关信息。稍后您可以尝试清除该对象的病毒。

◉ **不提示操作** ☑ **清除病毒** ☑ **如果清除失败则删除**	程序尝试去处理检测到的对象而未要求用户确认。如果无法清除对象，则删除。
◉ **不提示操作** ☐ **清除**	该程序自动删除对象。

处理或删除对象前，卡巴斯基反病毒 6.0 Windows 工作站会创建对象备份，并将其发送到 “备份区”，以防需要恢复该对象或可能稍后需要时对其进行处理。

13.4.5. 高级病毒扫描设置

除配置基本的病毒扫描设置外，您还可以使用高级设置 (见图 67)：

☑ **启用 iChecker 技术**-使用该项技术可以使某些对象免于扫描，从而提高了扫描速度。使用特殊的算法而使对象免于扫描。该算法考虑到了反病毒数据库的发布时间、上次扫描该对象的时间以及对扫描设置的更改。

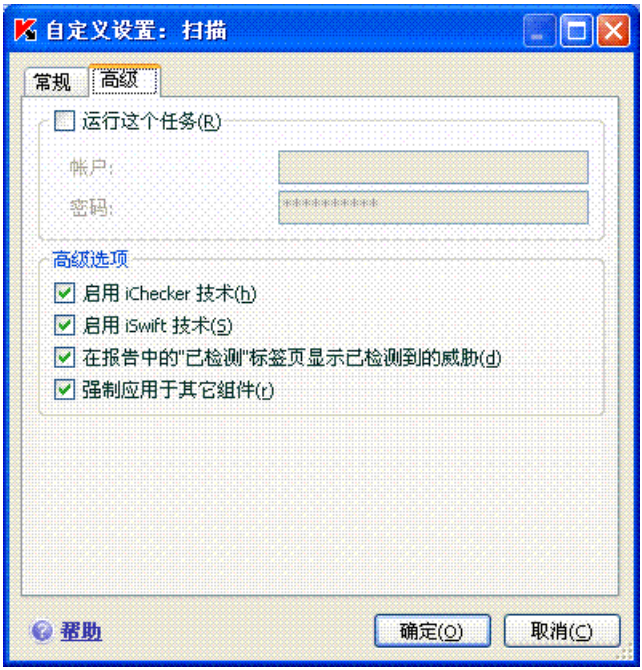


图 67. 高级扫描设置

例如，您有一个存档文件，经卡巴斯基反病毒扫描并指定为未感染状态。下次扫描时，程序将跳过该文件，除非该文件已修改或者扫描设置已更改。如果由于添加了新对象而更改了存档文件的结构，如果扫描设置已更改或者反病毒数据库已更新，则程序将再次扫描该存档文件。

iChecker™技术有其局限性： 它无法处理大型文件而只能应用到结构为卡巴斯基反病毒 6.0 Windows 工作站可以识别的对象 (例如：.exe,.dll,.lnk，.ttf,.inf,.com,.zip,.rar)。

- **启用 iSwift 技术。**该技术是对 iChecker 技术的发展，可应用于使用 NTFS 文件系统的计算机。 iSwift 技术有其局限性： 它仅限于文件系统中的特定文件区域，并且只能应用于 NTFS 文件系统中的对象。

  iSwift 技术不能应用到运行 Windows 98SE/ME/XP64 系统的计算机上。

- **在报告的“已检测”标签页显示已检测到的威胁** – 扫描报告 (见 16.3.2 在 185 页)窗口上的“已检测”标签过程中显示检测到的威胁列表。禁用该项功能，对一些特定的扫描，例如文本集的扫描来说可能时合适的，因为这可以提高扫描的速度。

- **强制应用于其它组件** – 如果处理器忙于处理其它应用程序的请求，则暂停病毒扫描任务。

13.4.6. 为所有的任务配置全局扫描设置

按照各扫描任务的设置执行其扫描任务。默认情况下，在您计算机上安装本程序时创建的任务使用卡巴斯基实验室专家推荐的设置。

您可以为所有的任务配置全局扫描设置。刚开始时，您可以使用一组用于对单个对象进行病毒扫描的属性。

为所有的任务配置全局扫描设置：

1. 选择程序主界面左侧上的**扫描**区域，并点击设置。
2. 在打开的设置窗口配置扫描设置：为对象选择安全级别 (见 13.4.1 在 153 页)、配置高级安全级别设置并选择处理操作 (见 13.4.4 在 156 页)。
3. 要将这些新的设置应用于所有的任务，点击**其它扫描任务**区域上的**应用**按钮。对弹出对话框中选定的全局设置进行确认。

第14章. 测试卡巴斯基反病毒组件特性

安装并配置完卡巴斯基反病毒组件后，我们建议您使用测试病毒及其变种来验证组件的设置是否正确，运行是否正常。

14.1. EICAR 测试病毒及其变种

该测试病毒是 eicar (欧洲计算机反病毒研究所)为测试反病毒软件的功能而专门开发的。

测试病毒“不是一种病毒”，它不含可能破坏计算机的程序代码。 然而大多数反病毒程序都将其判定为病毒。

切勿使用真正的病毒去测试反病毒软件的功能性！

您可以从 **EICAR** 官方网站下载测试病毒：http://www.eicar.org/anti_virus_test_file.htm。

由 **EICAR** 网站下载的文件包含标准的测试病毒体。卡巴斯基反病毒组件能检测到该测试病毒并将其标记为“**病毒**”，并采取与之对象类型相对应的处理操作。

在检测不同类型的对象时如果要测试卡巴斯基反病毒组件的反应能力，您可以修改标准测试病毒的内容，将下表所列的任一前缀添加到测试病毒中。

前缀	测试病毒状态	应用程序处理对象时执行的处理操作
CORR–	文件已破坏。	应用程序可以访问到该对象但无法对其进行扫描，因为该对象已被破坏 (例如文件结构被破坏或对象的文件格式无效)
SUSP– WARN–	文件感染测试病毒 (修改)。您无法清除对象。	该对象时已知病毒或未知病毒的变体。检测时，安全威胁特征数据库不含有处理该对象程序的描述。应用程序将该对象放到“隔离区”，稍后由更新过的反病毒数据库进行处理。

前缀	测试病毒状态	应用程序处理对象时执行的处理操作
ERRO–	处理出错。	处理该对象时出错： 扫描对象时，应用程序无法访问它，因为该对象的完整性被破坏 (例如多卷存档文件没有结尾) 或无法与其连接 (如果在网络驱动器上扫描该对象)。
CURE–	文件感染测试病毒。文件可以修复。 该对象会被清除，病毒体的文本将更改为修复 (CURE)。	该对象感染可以修复的病毒。应用程序将对对象进行病毒扫描，此后将全面修复该对象。
DELE–	文件感染测试病毒。您无法清除对象。	该对象感染无法清除的或木马病毒。该程序删除这些对象。

上表的首栏是前缀，需要将其添加到标准测试病毒字符串的开头。第二栏描述了测试病毒状态以及卡巴斯基反病毒对各种测试病毒的反应。第三栏包含应用程序处理过的具有同样状态的对象的信息。

反病毒扫描设置值决定了对每一对象所要采取的处理操作。

14.2. 测试文件保护

要测试文件保护的功能性：

1. 在磁盘上创建文件夹，将从该组织的官方网址下载的测试病毒复制到该文件夹中，并修改您所生成的测试病毒。
2. 允许记录所有事件，因此报告文件中存有被破坏对象以及由于出错未经扫描的对象的数据。为此选中报告设置窗口中的 **记录非重要事件**复选框。
3. 运行测试病毒或对其进行修改。

文件保护组件将阻止您企图访问该文件的行为，对其进行扫描并通知您，它已检测到危险对象：

当您选择不同的选项来处理检测到的对象时，您可以测试文件保护组件对检测到不同类型对象的反应。

您可以查看文件保护组件报告中有关它的运行的详细信息。

14.3. 测试病毒扫描任务

要测试病毒扫描任务：

1. 在磁盘上创建文件夹，将从该组织的官方网址下载的测试病毒复制到该文件夹中，并修改您所生成的测试病毒。
2. 创建新的病毒扫描任务，并选择含有作为对象供扫描的测试病毒组的文件夹。
3. 允许记录所有事件，因此报告文件中存有被破坏对象以及由于出错未经扫描的对象的数据。为此选中报告设置窗口中的 **记录非重要事件**复选框。
4. 执行病毒扫描任务。

进行扫描时，当检测到可疑或受病毒感染的对象，屏幕上将显示有关该对象的通知，并提示用户采取进一步的处理操作：

这样，通过选择不同的处理选项，您就可以测试卡巴斯基反病毒组件对检测到不同类型对象的反应。

您可以查看组件报告中有关病毒扫描任务执行的详细信息。

第15章. 反病毒数据库更新

保持反病毒软件时时更新是确保您的计算机安全的重要环节。由于每天新病毒、木马以及恶意软件层出不穷，因此定期地更新反病毒数据库来保护您的信息的完整性是非常重要的。

程序的更新包括下载以下组件并将其安装到您的计算机上：

- **反病毒数据库、网络攻击特征库以及网络驱动器**

  使用包含反病毒数据库以及网络攻击模式的数据库来保护您的计算机信息的安全。提供安全保护的保护组件使用反病毒数据库来搜索并清除您计算机上的有害对象。特征库中会时时添加新的安全危险记录并提供处理它们的方法。因此建议定期对其进行更新。

  除了反病毒数据库以及网络攻击数据库外，还要更新网络驱动器，它可以使保护组件拦截网络通信量。

  卡巴斯基实验室以前的应用程序版本支持*标准*和*扩展的数据库*组。每一组数据库处理不同类型的危险对象，从而达到保护计算机的作用。使用卡巴斯基反病毒 6.0 Windows 工作站，您无需担心能否选择了合适的反病毒数据库。现在，我们使用新的反病毒数据库来保护您计算机不受恶意和程序、潜在的危险对象以及黑客的攻击。

- **应用程序模块**

  除了反病毒数据库，您还可以更新卡巴斯基反病毒模块。定期提供新的应用程序更新。

卡巴斯基反病毒 6.0 Windows 工作站的主要更新源是卡巴斯基实验室的更新服务器。 以下是它们的地址：

http://dnl-cn1.kaspersky-labs.com
http://dnl-cn2.kaspersky-labs.com
http://dnl-cn3.kaspersky-labs.com

从更新服务器上下载可用更新，您的计算机必须连接到 Internet。

如果您不能访问卡巴斯基更新服务器 (例如，您的计算机不能连接到 Internet) ，您可以给卡巴斯基实验室打电话进行咨询 (400-611-6633) ， 询问卡巴斯基实验室合作伙伴。

可以用以下方式下载更新：

- *自动更新*。卡巴斯基反病毒能在指定时间间隔自动检查更新源。病毒爆发期间，检查的频率会上升，而在病毒根除后，检查的频率会下降。如果发现有新的更新库，该程序会将其下载并安装到计算机中。这属于默认设置。
- *按计划更新*。计划在指定时间开始更新。
- *手动更新*。选择此项，您需要手动进行更新。

更新期间，应用程序将您计算机上的反病毒数据库和程序模块与更新服务器上的版本进行比较。如果您的反病毒数据库和程序模块已是最新版本，您将会看到一个通知窗口，确认您的是最新的。如果您计算机上的反病毒数据库和程序模块与更新服务器上的不同，程序仅下载缺少的部分。更新模块不下载已经有的反病毒数据库数据和模块，这会增加下载速度，减少网络传输量。

在更新反病毒数据库之前，卡巴斯基反病毒 6.0 Windows 工作站会备份反病毒数据库，如果更新过程出现错误，可以恢复到上一次更新反病毒数据库。例如，如果您更新了反病毒数据库，但它们在使用中损坏了。您可以轻易的恢复到先前版本，并且试着以后再重新进行更新。

您在更新程序的同时，可以将检索到的更新程序分发给本地源 (见 15.4.4 在 173 页)。本功能允许您在网络计算机上更新 6.0 版程序使用的数据库和模块，从而节省网络带宽。

15.1. 开始更新

您可以随时开始更新。它将从您选择的更新源开始下载 (见 15.4.1 在 167 页)。

您可以从以下地方开始更新：

- 快捷菜单。
- 程序主界面。

要从快捷菜单开始更新：

1. 右键点击系统托盘上的该程序图标，可以打开快捷菜单。
2. 选定**更新**。

要从程序主界面开始更新：

1. 选择**服务**区域上的**更新**。
2. 点击主界面右侧面板上的**立即更新！**按钮， 或使用状态栏上的▶ 按钮。

更新进程将显示在一个专门的窗口上，点击**关闭**可以将其隐藏。窗口隐藏的情况下，更新仍继续。

请注意，更新过程中可以将更新程序传输给本地源盘，只要启用了该项服务(见 15.4.4 在 173 页)。

15.2. 恢复到上一次更新的反病毒数据库

每次启动更新程序，卡巴斯基反病毒 6.0 Windows 工作站首先会备份当前反病毒数据库，然后再开始下载更新。这样，如果更新失败，您就可以使用以前的反病毒数据库。

例如在由于连接出错导致更新失败等情况下，该恢复选项十分有用。您可以恢复到上一次更新的反病毒数据库并稍后尝试再次更新。

要恢复到上一版本的反病毒数据库：

1. 选择程序主界面的**服务**区域上的**更新**组件。
2. 点击程序主界面右侧面板上的**恢复**按钮。

15.3. 创建更新任务

卡巴斯基反病毒 6.0 Windows 工作站设有内置的更新任务，可用于更新程序模块和反病毒数据库。您也可以使用各种设置和启动计划创建您自己的更新任务。

例如，您可以在家里和办公室使用的笔记本电脑上安装卡巴斯基反病毒软件。在家时，您可以从卡巴斯基实验室更新服务器上更新程序。而在办公室则可以从保存了您所需的更新程序的本地文件夹中进行更新。使用这两种不同的任务，可以避免每次更换地点时需要更改更新设置。

要创建新高级更新任务：

1. 选择程序主界面的**服务**区域上的**更新**组件，右键点击打开快捷菜单并选择**另存为**。
2. 在打开的窗输入任务名并点击**确定**。在程序主界面的**服务**区域将显示任务以及任务名。

警告！

卡巴斯基反病毒对于用户能够创建的更新任务数量是有限制的。最多可以创建两项任务。

新任务继承了它所基于的任务的所有属性 (但不包括任务设置)。对于新任务来说，禁用自动扫描默认设置。

创建完任务后，配置高级设置：指定更新源 (见 15.4.1 在 167 页) 和网络连接设置 (见 15.4.3 在 171 页)，必要的话，启用另一授权帐户下的任务 (见 13.4.5 在 158 页) 并配置任务。

要重命名任务：

选择程序主界面的**服务**区域上的任务，右键点击打开快捷菜单并选择**重命名**。

在打开的窗输入新任务名并点击**确定**。**服务**区域上的任务名也会更改。

要删除任务：

选择程序主界面的**服务**区域上的任务，右键点击打开快捷菜单并选择**重命名**。

在确定窗口确定您想要删除该任务。该任务将从**服务**区域上的任务列表中删除。

警告！

您只能重命名和删除您已创建的任务。

15.4. 配置更新设置

更新程序设置指定了以下参数：

- 下载和安装的更新源 (见 15.4.1 在 167 页)
- 更新程序的运行模式
- 更新的对象
- 更新完成后执行的处理操作 (见 15.4.4 在 173 页)

下面将详细介绍这些设置。

15.4.1. 选择更新源

*更新源*包含反病毒数据库和卡巴斯基反病毒应用程序模块更新的资源。

您可以使用的更新源如下所示：

- *管理服务器*—位于卡巴斯基管理工具上的统一更新库 (有关详细信息，参见卡巴斯基 管理工具管理员用户指南)。
- *卡巴斯基实验室更新服务器*- 专门用于更新所有卡巴斯基实验室产品的反病毒数据库和程序模块的网站。
- *FTP 或 HTTP 服务器或本地或网络文件夹* –保存了最新更新程序的本地服务器或文件夹。

如果您无法访问卡巴斯基更新服务器 (例如，您的计算机无法连接到 Internet)，您可以给卡巴斯基实验室打电话进行咨询 (400-611-6633)，询问卡巴斯基实验室合作伙伴。

警告！

要求在移动介质上进行更新时，请指定是否也需要更新程序模块。

您可以从磁盘拷贝更新数据，将其上传到 FTP 或 HTTP 站点，或是将它们保存到本地或网络文件夹。

选择**更新源**标签页上的更新源 (见图 68)。

默认情况下，从卡巴斯基实验室更新服务器上下载更新程序。该项地址列表无法进行编辑。更新时，卡巴斯基反病毒 6.0 Windows 工作站调用该列表，并选择第一个服务器地址，并尝试从该服务器上下载文件。如果不能从第一个服务器下载，应用程序会尝试轮流连接每一服务器直至成功。能够成功下载更新程序的服务器地址将自动置于列表的顶部。从而在下次更新时，应用程序会首先连接到该服务器上。

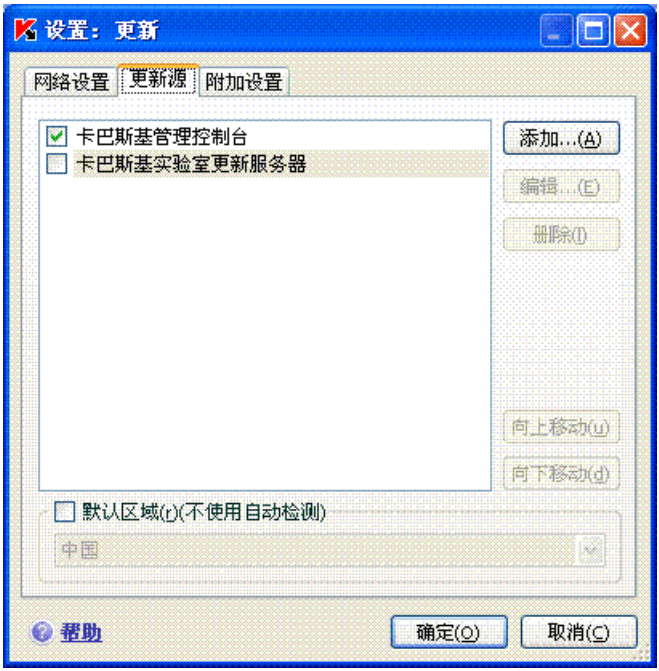


图 68. 选择更新源

要从另一 FTP 或 HTTP 网址下载更新程序：

1. 点击**添加**。
2. 在**选择更新源**对话框内选择目标 FTP 或 HTTP 或者在**更新源**栏指定该网站的 IP 地址、字符名或 URL 地址。

警告！

如果您选择网络源作为更新源，则您需要连接到 internet 来进行更新。

要从本地文件夹进行更新：

1. 点击**添加**。
2. 在**选择更新源**对话框选择文件夹或在**更新源**栏指定该文件夹的完整路径。

卡巴斯基反病毒 6.0 Windows 工作站将新的更新源添加到列表的顶部，选中更新源名称旁的复选框就可以自动启用该更新源。

如果将几个源地址选定为更新源，应用程序会试着逐一从列表的顶部开始连接，直至找到第一个可用更新源。您可以通过**向上**和**向下**按钮来改变列表中更新源的顺序。

使用**添加**、**编辑**、**删除**按钮来编辑此列表。唯一一个不能编辑的更新源是卡巴斯基实验室更新服务器。

如果使用卡巴斯基实验室更新服务器作为更新源，您可以选择最佳的服务器地点进行更新。卡巴斯基实验室在若干个国家都部署了服务器。选择离您最近的服务器进行更新可以加快更新速度，并节省时间。

要选择最近的服务器，选中 **确定地区 (不使用自动检测)** 复选框并从下拉列表中选择离您当前位置最近的国家。如果选中该复选框，更新时会考虑列表中所选的地区。默认情况下，不选中该复选框。使用操作系统注册表中当前地区的有关信息。

15.4.2. 选择更新方法和更新内容

配置更新设置时，指定更新的内容以及要使用的更新方法是十分重要的。

更新对象 (见图 69) 是将要被更新的组件：

- 反病毒数据库
- 能使保护组件拦截网络通信量的网络驱动
- 反黑客组件使用的网络攻击数据库
- 程序模块

反病毒数据库、网络驱动以及网络攻击数据库要总是更新，然应用程序模块仅在选择了相应的模式情况下才更新。

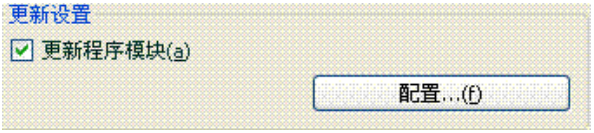


图 69. 选择更新对象

如果您需要下载和安装程序模块更新程序：

选中**更新**服务的**更新设置**对话框中的☑ **更新程序模块**。

如果更新源中有当前程序模块更新程序，则屏幕上会显示一个窗口，罗列出了程序模块所有更新的情况。您可以根据这些描述确定是否需要安装更新程序。

更新方法 (见图 70) 指定如何启动更新程序： 您可以有以下方法供选择：

- **自动更新**。卡巴斯基反病毒能在指定时间间隔自动检查更新源。如果发现有新的更新库，该程序会将其下载并安装到计算机中。该项默认设置为启用。

  如果将一个*网络资源*指定为更新源，则卡巴斯基反病毒 6.0 Windows 工作站会在前一更新包指定的时间段后尝试启动更新。如果本地文件夹被选择为更新源，则程序会尝试在上一次更新时下载的更新包规定的时间间隔内从本地文件夹下载更新程序。该选项允许卡巴斯基实验室定制在病毒爆发和其它潜在的危险情况发生时的更新频率。您的应用程序能及时接收最新的反病毒数据库，网络攻击特征码，和程序模块，从而防止恶意软件侵入您的计算机。

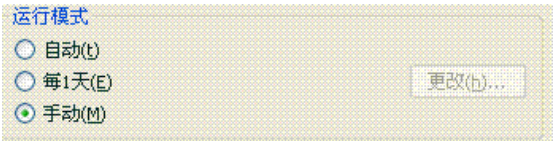


图 70. 选择更新运行模式

- **按计划更新。**计划在指定时间开始更新。默认情况下，每天进行更新。要编辑默认任务，点击模式主题旁的**更改...** 按钮并在打开的窗口作必要的更改 (有关详细信息，参见**错误！未找到引用源。**在**错误！未定义书签。**页)。

- **手动更新。**选择此项，您需要手动进行更新。卡巴斯基反病毒工作站会通知您何时需要更新。

- 系统托盘中的应用程序图标的上方会弹出信息，提示您程序需要更新(如果启用通知，请见 16.11.1 在 210 页)
- 程序主界面上的第二个指示器会提示您，您的计算机更新程序已过期(见 4.1.1 在 36 页)
- 程序主界面上的消息区域会显示建议信息，提示应用程序需要更新。

15.4.3. 配置连接设置

如果您配置了计算机从卡巴斯基实验室或其它 FTP、HTTP 站点更新，我们推荐您首先检查连接设置。

所有设置都类集在一个指定的标签页上–**局域网设置** (见图 71)。

如果您以被动方式从 FTP 服务器下载更新程序(例如通过防火墙)，则选中 ☑ **如果可能，使用被动 FTP 模式** 如果使用主动 FTP 模式则不选中该复选框。

在**连接超时 (秒)** 栏指定用于连接更新服务器的时间。如果连接失败，一旦超时，程序将尝试连接下一更新服务器。程序将持续尝试连接直至成功或直至尝试完所有可连接的更新服务器。

如果使用代理服务器访问互联网，则选中☑ **使用代理服务器**复选框，必要时选择以下设置：

- 选择更新时要使用的代理服务器设置：

  ◉ **自动检测代理服务器设置。**如果选择该项，将使用 WPAD (网络代理自动发现协议)自动检测代理服务器设置。如果该协议无法检测到地址，卡巴斯基反病毒将使用 MS IE 指定的代理服务器设置。

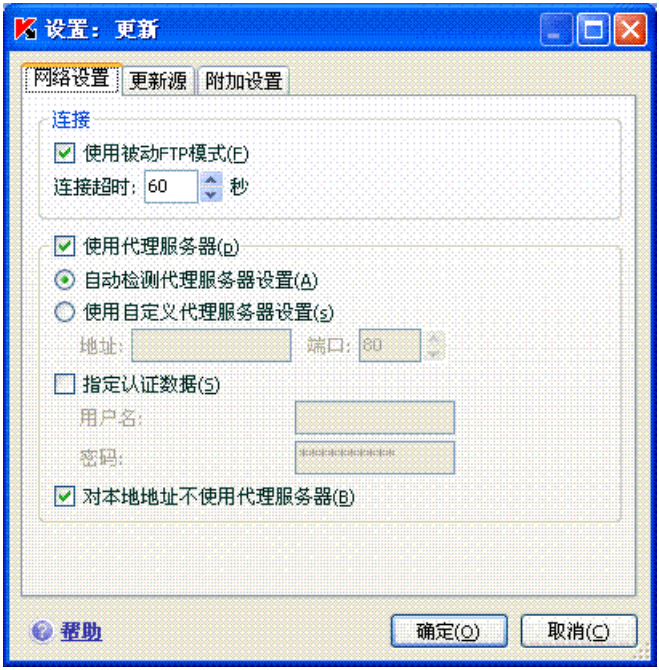


图 71. 配置网络更新设置

使用自定义代理设置-使用一个不同于浏览器连接设置指定的代理。在**地址**栏，输入代理服务器的 IP 地址或符号名，并在**端口**栏指定用于更新应用程序的代理端口的数量。

- 指定是否代理服务器需要认证。*认证*是为了控制访问而验证用户注册数据的过程。

  如果认证时需要连接到代理服务器上，则选中 **指定认证数据**并在以下栏指定 用户名和密码。 在此情况下，先尝试 NTLM 认证，然后再尝试 BASIC 认证。

  如果选中该复选框或如果不输入数据，则将使用用于启动更新的用户帐户尝试 NTLM 认证 (见 5.4 在 57 页)。

  如果代理服务器需要认证，而且您没有输入用户名和密码或者由于某原因未接受指定的数据，则开始更新时会弹出窗口，提示输入认证的用户名和密码。如果认证不成功，则下次更新程序时将使用该用户名和密码。否则，需要再次进行认证设置。

为避免在更新源为本地文件夹时使用代理服务器，选择 **对本地地址不使用代理服务器。**

该功能在 Windows9X/NT 系统的机器上不可用。然而默认情况下，本地地址不使用代理服务器。

15.4.4. 更新发布

更新复制功能可以实现对您的商业网络负载的优化。复制更新程序分为两步：

1. 网络上的一台计算机从卡巴斯基实验室网络服务器另一个载有最新更新程序的网络资源上下载程序和反病毒数据库更新包。下载的更新程序放在可以公共访问的文件夹中。
2. 网络上的其它计算机可以访问该文件夹下载更新程序。

要启用更新发布，选择**其它**标签 (见图 72) 上的 **更新发布文件夹**复选框，在下方栏指定用于保存下载的更新程序的共享文件夹。您可以在点击**浏览**时打开的窗口手动输入路径或选择路径。如果选择复选框，则下载时，更新程序将自动复制到该文件夹中。

您也可以指定更新发布的方法：

- *完整更新*，复制卡巴斯基实验室所有 6.0 应用程序的反病毒数据库和组件更新。要选择完整更新，选中 **复制所有组件的更新程序**复选框。
- *自定义更新*，只复制已安装的卡巴斯基反病毒 6.0 组件的反病毒数据库和组件更新。如果您想要选择该更新方式，则必须取消选中 **为所有组件复制更新程序**复选框。

请注意，卡巴斯基反病毒 6.0 仅从卡巴斯基实验室更新服务器下载 6.0 应用程序的更新包。我们建议您通过卡巴斯基管理工具复制其它卡巴斯基实验室应用程序的更新程序。

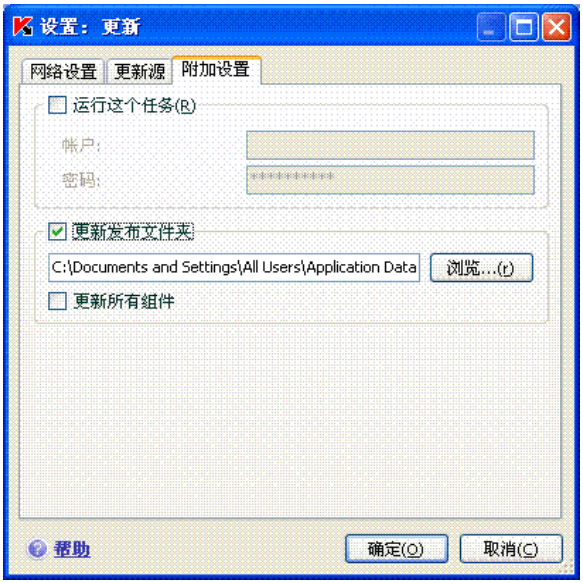


图 72. 复制更新工具设置

如果需要网络上的其它计算机从文件夹 (其中的更新程序从互联网复制而来) 进行更新，则您必须按如下操作：

1. 允许公共访问该文件夹。
2. 在更新程序设置中将网络计算机上的共享文件夹指定为更新源。

15.4.5. 更新程序后的动作

反病毒数据库每次更新后，能使您的计算机防御最新的安全威胁。

卡巴斯基实验室建议您，在每次更新完数据库后扫描*隔离区对象*和*启动对象*。

为什么要对这些对象进行扫描呢？

程序已将隔离区的对象标记为疑似或可能病毒感染。卡巴斯基反病毒 6.0 Windows 工作站使用最新版的反病毒数据库，有可能可以识别出安全威胁并将其消灭。

默认情况下，每次更新完反病毒数据库后，应用程序会扫描隔离区对象。同时建议您定期查看隔离区对象，因为经过几次扫描，它们的状态可能会发生变化。有些对象可能会恢复到原来的位置，而您可以继续使用它们。

选中**更新后动作**区域中的☑ **重新扫描隔离区**复选框，禁用扫描隔离区对象。

启动对象对于您的计算机安全来说至关重要。如果其中有对象被恶意程序感染，则可能导致操作系统无法启动。卡巴斯基反病毒 6.0 Windows 工作站有内置的扫描启动对象的任务(见第 13 章在 149 页)。建议您为该任务制定计划，从而在每次反病毒数据库更新后能自动启动该任务。

第16章. 高级选项

处理保护您的数据，卡巴斯基反病毒 6.0 Windows 工作站还具有其它的可扩展功能。

该程序将一些对象置于专用的存储区域，从而确保了最大程度地保护数据而使损失程度降至最低。

- 备份区包含由卡巴斯基反病毒 6.0 Windows 工作站已更改或者已删除的对象的副本。如果有些对象所包含的信息对您来说至关重要而在反病毒处理过程中可能不能完全恢复，则您就可以从备份副本中将其恢复。
- 隔离区包含不能使用现有反病毒数据库处理的潜在的受感染对象。

建议您定期检查存储的对象列表。 其中一些可能已经过期，而有些可能已被恢复。

高级选项包含许多不同的有用功能。 例如：

- 卡巴斯基反病毒 6.0 Windows 工作站技术支持为您提供全面的帮助 (见 16.5 在 199 页)。卡巴斯基为您提供若干的技术支持方式：在线支持，为程序使用者提供的问题和解答的论坛等等。
- 通知功能为您提供卡巴斯基反病毒 6.0 Windows 工作站使用时的关键事件的通知 (见 16.11.1 在 210 页)。这些通知可能只是一些信息服务性质的，也可能是必须立即解决的重大错误。
- 自我保护功能可以避免程序自身的文件被黑客修改或者破坏，阻止远程管理使用程序的功能，以及限制您计算机上的其它用户进行巴斯基反病毒 Windows 工作站的某些操作 (见 16.11.1.3 在 213 页)。例如，更改保护级别可能会极大地影响您计算机的信息安全。
- “授权许可文件管理程序”能够获得使用授权的详细信息，激活程序的副本以及管理授权许可文件。

该程序也提供“帮助”选项以及所有保护组件运行和病毒扫描任务执行的详细报告。

端口监控组件可以控制卡巴斯基反病毒 6.0 Windows 工作站的哪些模块控制选定的端口上的数据传输。

应急磁盘有助于恢复您受感染的计算机的功能。当恶意代码破坏系统文件后导致无法启动您的计算机操作系统时，此项功能尤其有用。

您也可以更换卡巴斯基反病毒 6.0 Windows 工作站的外观，也可以自定义该程序的界面 (见 16.8 在 204 页)。

以下将详细讨论这些功能。

16.1. 隔离潜在受感染的对象

隔离区是保存潜在受病毒感染的对象的特殊存储区。

潜在的受感染对象是被怀疑受病毒感染的对象或其变种。

为什么是潜在地受感染呢？这是因为不可能确定一个对象是否已被感染，有如下几点原因：

- *被扫描对象的代码类似于已知安全威胁但部分已修改。*

  反病毒数据库包含卡巴斯基实验室已搜集整理的安全威胁。如果黑客修改了恶意程序，但这些修改还没有被记录到反病毒数据库中，那么卡巴斯基反病毒 6.0 Windows 工作站就会把受此修改的恶意程序感染的对象定义为潜在受感染对象，并指出此次病毒感染类似何种安全威胁。

- *尽管反病毒数据库中没有类似于检测到的对象代码的记录，但这些对象代码在恶意程序结构中存在。*

  这很有可能是一种新型的安全威胁，因此卡巴斯基反病毒 6.0 Windows 工作站将该对象归为签字的受感染对象。

*启发代码*分析技术可以从潜在病毒中检测出高达 92%的新病毒。该机制相当有效，并且很少出现误报问题。

潜在的受感染对象可以被检测到，并在 文件保护, 邮件保护 , 主动防御 或病毒扫描 过程中被存储到隔离区中。

当检测到潜在受感染对象时，您可以点击弹出的消息框中的隔离来将一个对象存储到隔离区中。

对象是通过移动方式而不是通过复制方式来存储到“隔离区”。将对象从磁盘或者邮件删除掉，并保存在“隔离区”文件夹中。“隔离区”中的文件是以一种特殊的格式来存储的，因此是没有危险的。

16.1.1. 操作隔离对象

选择程序主界面的**服务**区域上的**报告、隔离和备份**选项，显示“隔离区”中对象的总量。在屏幕的右侧，“隔离区”区域显示：

- 在卡巴斯基反病毒 6.0 Windows 工作站处理过程中检测的潜在受感染对象数。
- 当前“隔离区”的大小。

您可以点击**清空**按钮来删除隔离区中的所有对象。请注意，如果这样操作，也将删除备份文件和报告文件。

要访问“隔离区“的对象：

左键点击“隔离区”区域的任何部分。

您可以在 **隔离区** 标签 (见图 图 73) 上采取以下操作：

- 把您怀疑受到感染的而程序未检测到的文件移到“隔离区”。为此，点击标准选择窗口上的**添加**按钮并选择该文件。将该文件以及*用户添加*的状态添加到列表中。

  如果手动隔离文件并且在后续扫描中确定为未受感染，则扫描后其状态不会立即更改为*正常*。隔离该文件后，如果间隔了一段时间（至少三天）后进行扫描才会出现这种情况。

- 要使用当前反病毒数据库扫描和清除“隔离区”中所有潜在的受感染对象，点击**扫描全部**。

  任何隔离的对象被扫描和清除完成后，其状态可能会变成*受感染的*，*潜在受感染的*，*无法确定的*，正常的等等状态。

  *受感染*状态意味着已确定对象已受到感染，但还没有对其进行处理。建议您删除此类对象。

  所有标识为*无法判定*的对象可以被恢复，因为它们以前的*潜在受感染*状态经程序重新扫描后并未得到确认。

图 73. 被隔离对象列表

- 隔离前 (默认) 将文件恢复到用户指定的文件夹或者它们原来的文件夹。要恢复对象，从列表中选定并点击**恢复**。当从存储在隔离区中的文件夹，邮件数据库和邮件格式文件中恢复对象时，您也必须选择它们恢复指向的目录。

> 提示：
>
> 我们推荐您只恢复状态为*不确认的*，*正常*的以及*已清除*的对象，因为恢复其它对象可能会影响您的计算机。

- 删除任何隔离对象或者指定的对象组。只删除不能被清除的对象。在列表中选定对象，然后点击**删除**就可以删除这些对象了。

16.1.2. 隔离设置

您可以配置隔离区的布局和运行设置，特别是：

- 每次更新反病毒数据库后设置“隔离区”对象自动扫描 (详细信息，见 15.4.4 在 173 页)。

> 警告！
>
> 如果您访问“隔离区”，则更新完反病毒数据库后，程序将不能立即扫描被隔离的对象。

- 设置隔离区的最大存储时间。

  默认存储时间为 30 天。过了期限，将删除对象。您可以改变隔离对象保存的时间或者完全禁用这个限制。

操作如下：

1. 点击程序主界面上的设置，打开卡巴斯基反病毒 6.0 Windows 工作站设置窗口。
2. 从设置目录树中选择**报告、隔离和备份**。
3. 在 **隔离区和备份区**区域 (见图 图 74) 输入一个时间数字，然后在这个时间过后隔离区中的对象将被自动删除。同样也可以取消选定复选框来禁用自动删除。

图 74. 配置隔离区存储时间

16.2. 备份危险对象的副本

有时清除对象时会导致对象的丢失。如果一个被清除的文件包含部分或者完全被破坏的重要信息，则您可以试图恢复备份副本到文件的初始位置。

备份副本是在对象首次被清除或删除时创建的原始危险对象的副本。 它保存在“备份区”。

备份区是一个特殊的存储区，它包含需要被清除或删除的危险对象的备份副本。“备份区”中的文件是以一种特殊的格式来存储的，因此是没有危险的。

16.2.1. 操作备份副本

备份区中的总对象数显示在程序主界面**服务**区域的**报告、隔离和备份**中。在屏幕的右侧，“备份区”区域显示：

- 在卡巴斯基反病毒 6.0 Windows 工作站创建的备份副本数量。
- 当前“备份区”的大小。

您可以点击**清空**按钮来删除备份区中的所有副本。请注意，如果这样操作，也将删除隔离对象和报告文件。

要访问危险的对象副本：

左键点击“备份区”区域的任何部分。

备份副本列表显示在“备份”标签 (见图 图 75) 中。每一副本包括以下信息： 带有文件原始路径的对象全名，扫描指定对象的状态和对象的大小。

您可以使用**恢复**按钮来恢复选定的副本。对象从“备份区”中优先于清除操作而被恢复。

如果在文件的原始位置有一个同名的文件（如果一个副本是由优先于清除而被恢复的对象组成时就有可能发生这种情况），这时就会弹出一个警告信息。您可以更改被恢复对象的位置或者将其重命名。

建议您恢复对象之后立即扫描备份区对象。您可以利用更新的特征库清除对象而不失文件的完整性，这是有可能的。

我们推荐您除非完全必要，否则不要恢复备份对象副本。这可能导致感染您的计算机。

建议您定期检查备份区，并点击**删除**按钮来清空备份区。您也可以设置程序来自动删除备份中最旧的备份副本 (见 16.2.2 在 182 页)。

图 75. 被删除或清除对象的备份副本

16.2.2. 配置备份

您可以设置备份区的最大存储时间。

默认备份区存储时间为 30 天。过了期限，将删除备份副本。您可以改变隔离对象保存的时间或者完全禁用这个限制。操作如下：

1. 点击程序主界面上的设置，打开卡巴斯基反病毒 6.0 Windows 工作站设置窗口。
2. 从设置目录树中选择**报告、隔离和备份**。
3. 在屏幕右侧的**隔离区和备份区**区域 (见图图 74) 中设定存储备份副本的期限。您也可以取消选中复选框来禁用自动删除。

16.3. 报告

报告中记录了所有卡巴斯基反病毒 6.0 windows 工作站组件的操作行为和病毒扫描任务还有升级更新的信息。

点击程序主界面**服务**区域的**报告、隔离和备份**，显示该程序创建的报告总数及其大小。该信息会显示在报告框中。

要查看报告：

左键点击*报告*框中任意位置打开“保护”窗口，该窗口总结了应用程序的所有保护执行情况。在该窗口打**报告**标签 (见图图 76)。

报告标签列出了最近有关卡巴斯基反病毒当前进程中运行的所有组件和病毒扫描任务执行情况的报告。每一组件或任务旁会列出状态，例如，*停止*或*完成*。您可以选中 **显示历史报告**查看包含程序当前进程的所有历史报告。

图 76. 组件运行报告

要查看组件或者任务的所有事件报告：

在**报告**标签中选择组件或任务的名称并点击**详细信息**按钮。

这时会打开一个包含选定的组件或者任务的详细信息的窗口。执行统计的结果会显示在窗口的上面部分，并且在标签将会提供详细信息。标签随着组件或任务的不同而不同：

- **已检测**标签包含由组件或者病毒扫描任务检测的危险对象的列表。
- **事件**标签显示组件或者任务事件。

- **统计**标签包含所有已扫描对象的详细统计。
- **设置**标签显示由组件保护，病毒扫描或者更新反病毒数据库的所有设置。
- **宏指令**和**注册表**标签只在主动防御报告中才有，它们包含了所有在您计算机上运行的宏指令和企图修改系统注册表的行为的信息。
- **网络钓鱼站点**，**弹出窗口**，**广告工具条**和**拨号企图**标签只在反间谍报告中出现。它们包含在您计算机上所有已经检测到的钓鱼攻击和所有弹出窗口，广告条以及在程序运行期间拦截的自动拨号企图的信息。
- **网络攻击**，**禁用主机**，**程序操作**和**包过滤**标签只在反黑客标签中出现。它们包含在您计算机上所有的网络攻击企图，攻击后禁用主机，匹配已创建的处理规则的网络程序的描述和所有符合反黑客过滤规则的数据包的全部信息。
- **建立连接**，**打开端口**和**传输**标签也只包含您计算机上的网络行为，它们会显示当前已建立的连接，已开的端口以及您计算机发送和接受的网络通信量。

您可以以文本文件方式导出整个报告。当一个错误已发生在一个组件或任务中，并且您自己不可能消除和您需要联系技术支持的情况下，这个特点是很有用的。如果发生这种情况，您必须以文本文件方式把报告发送给技术支持，以便我们可以了解问题的细节并尽快解决它。

要以文本文件方式导出整个报告：

点击**另存为**并指定您想要保存报告文件的位置。

当您完成导出报告操作之后，点击**关闭**。

所有标签中都有一个**操作**按钮 (除了**设置**和**统计**标签外)，您可以使用它来定义如何处理列表中的对象。 当您点击它时，就会打开一个包含如下条目的快捷菜单 (这取决于组件和不同的菜单 — 会在下面列出的所有可能的选项)：

清除—试图清除危险对象。如果没有成功清除对象，那么您可以把它放到扫描列表中，然后利用反病毒数据库进行扫描或者将其删除。您可以将该操作应用到列表上的一个对象上或若干选定的对象上。

放弃—从列表中删除检测对象的记录。

添加到信任区域—排除保护对象。打开一个窗口，显示对象排除规则。

转到文件—打开对象位于 Windows Explorer 的文件夹。

全部处理—处理列表上的所有对象。卡巴斯基反病毒 6.0 Windows 工作站试图使用反病毒数据库处理对象。

全部跳过—清除已检测对象的报告。使用该功能时，所有已检测到危险对象仍保留在您的计算机中。

访问 www.viruslist.com – 卡巴斯基实验室网站的病毒百科全书上有相应的对象的详细描述。

查找 www.google.com – 使用该搜索引擎查找有关对象的信息。

查找—根据名称或者状况在列表中输入对象搜索条件。

另外，您可以通过点击栏标题对以升序和降序显示在窗口中信息进行整理。

16.3.1. 报告设置

要配置创建和保存报告的设置：

1. 点击程序主界面上的设置，打开卡巴斯基反病毒 6.0 Windows 工作站设置窗口。
2. 从设置目录树中选择**报告、隔离和备份**。
3. 在**报告**窗口 (见图图 77) 编辑设置如下：
   - 允许或禁止记录非重要事件。这些事件通常对于安全来说不算重要。选中☑ **记录非紧急事件**复选框来记录事件;
   - 仅选择报告自上一次执行任务以来发生的事件。这通过减少报告大小来节省磁盘空间。如果选中☑ **只保留最近的事件**复选框，则每次重新启动任务时报告也从头开始。然而仅重写非紧急信息。
   - 设置报告保护的时间。默认报告存储时间为 30 天。过了期限，将删除报告。您可以改变最大保存时间或者完全禁用这个限制。

图 77. 报告设置

16.3.2. 已检测标签

该标签 (见图图 78) 包含一个由卡巴斯基反病毒 6.0 Windows 工作站已检测的危险对象列表。列表中会显示每个对象的完整名称，由程序已扫描或者已处理的指定对象的状态。

如果您想显示危险对象以及成功删除对象的列表，请您选中☑ **显示要处理的对象**。

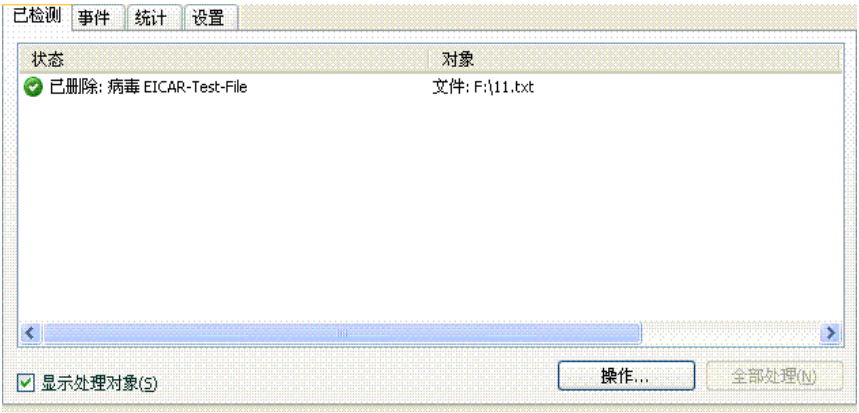


图 78. 已检测的危险对象列表

按下**处理**按钮(选定对象中的一个或一组对象) 或 **处理全部** 按钮(处理列表上的全部对象) 处理卡巴斯基反病毒检测到的危险对象。处理完每一对象后，屏幕上会显示信息。 此时您要决定如何对其进一步处理。

如果选中通知窗口中的☑ **应用于全部**复选框，则选取的操作将适用于符合在处理前选定状态的所有对象。

16.3.3. *事件*标签

该标签 (见图图 79) 这个标签给您提供了在组件操作中所有重要事件的一个完整列表，包括不能被一个活动控制规则 (见 9.1.1 在 90 页) 记录的病毒扫描、反病毒数据库更新等。

这些事件是：

危险事件是指在您计算机上面的程序操作或漏洞而产生的危险的重要事件。例如检测到病毒、操作出错。

重要事件是指必须进行调查的事件，因为它们能反应程序操作的重要情况。例如停止。

提示信息是指平时操作中所涉及到的、不重要的信息。例如，确定、未处理。如果选中☑ **显示全部事件**复选框，则这些事件只反映在事件日志中。

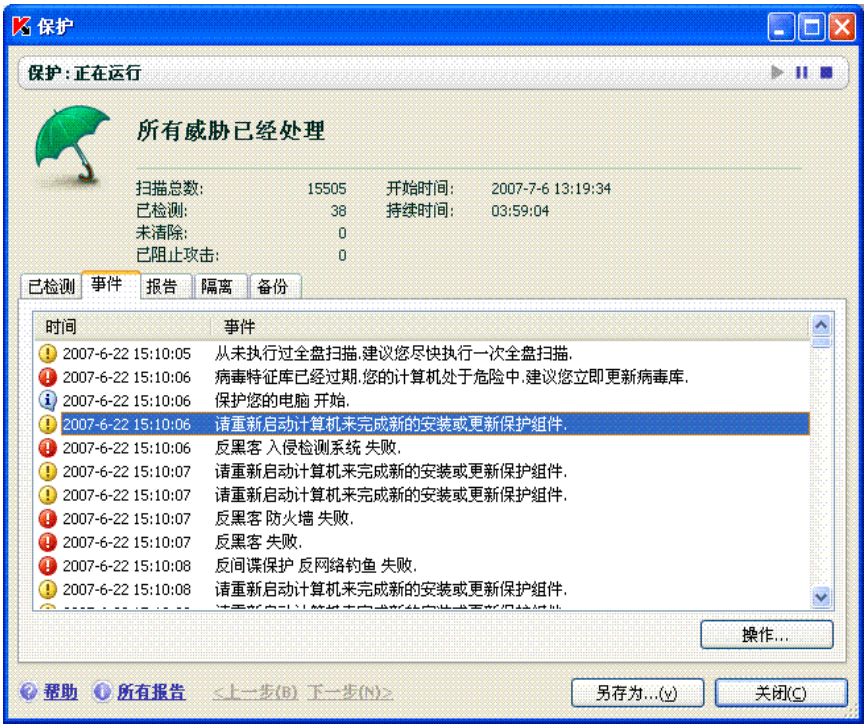


图 79. 组件运行时发生的事件

事件日志中显示事件的格式可能会随着组件或任务的不同而不同。更新任务包括以下信息：

- 事件名
- 涉及事件的对象名
- 事件发生的时间
- 加载文件的大小

在病毒扫描任务中，时间日志包括扫描的对象名和扫描/处理中所指定的状态。

当您使用特殊的快捷菜单查看报告时，您也可以使用自学习反垃圾邮件功能。操作方法是，选择电子邮件的名并点击鼠标右键打开快捷菜单，如果邮件是垃圾邮件，请选择**标记为垃圾邮件**；如果邮件是可接收的邮件，请选择**标记为可接收的邮件**。此外，根据分析邮件而获取的信息，您可以添加到反垃圾邮件组件的白名单和黑名单中。为此使用快捷菜单上相应的选项就可以了。

16.3.4. 状态标签

该标签 (见图图 80) 可以为您提供程序组件和病毒扫描任务中的详细状态。由此您可以了解：

- 在组件进程中或完成任务后，扫描了多少危险对象。显示扫描的文档、压缩文件、密码保护对象和损坏对象的数目。
- 检测到的、未清除的、删除的或移到“隔离区”中的危险对象的数量。

图 80. 组件状态

16.3.5. 设置标签

设置标签 (见图图 81) 向您显示了组件设置、病毒扫描和程序更新的完整信息。您可以找到一个组件或病毒扫描运行的级别，对危险对象采取了哪些操作，或者在程序更新中使用了哪些设置。使用更改设置链接去配置程序组件。

您可以为病毒扫描配置高级设置：

- 如果处理器负载加重，将建立病毒扫描任务优先级。默认情况下，选中**将系统资源让与其它应用程序** 复选框。由于这个功能，程序可以跟踪进程的负载和磁盘子系统的其它应用活动。如果进程负载增加时，一般情况下会阻止用户的其它应用操作，该程序就会减少扫描活动。这将会增加扫描的时间并为用户的应用释放系统资源。

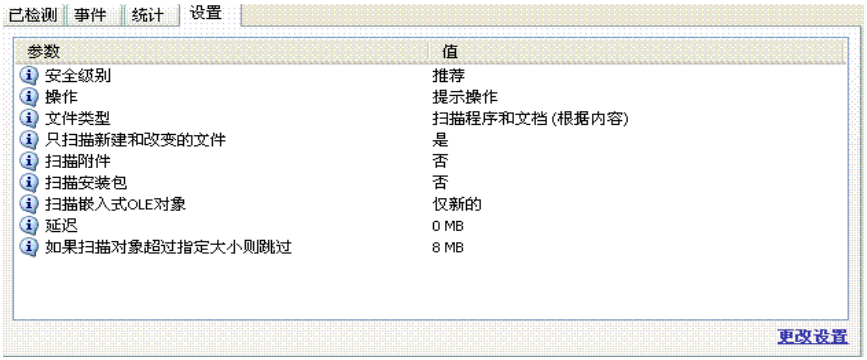


图 81. 组件设置

- 病毒扫描完成后，可以设置您计算机的操作模式。您可以设置关闭计算机，重新启动计算机，或者进入待机或休眠模式。要选择选项，左键点击超链接直到显示您需要的选项。

  您可能需要该功能，例如：如果您想在下班后开始病毒扫描而又不想等待它完成。

  但是要使用该功能，您必须按照以下步骤进行操作： 在扫描之前，如果启用了密码请求扫描对象，则您必须禁用该功能，启用自动处理危险对象而禁用程序交互功能。

16.3.6. *宏指令*标签

宏指令标签 (见 图 82) 中列出了卡巴斯基反病毒 6.0 windows 工作站的当前会话检测到试图运行的所有宏指令。这里您将会看到每个宏指令的全名，执行的时间以及处理宏之后的状态。

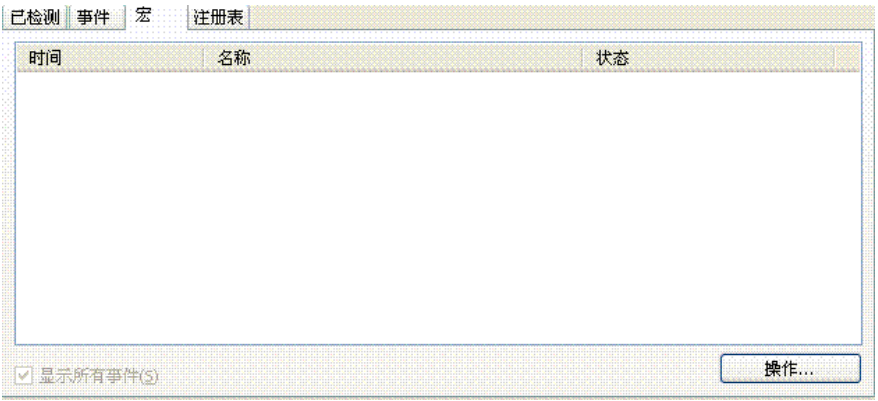


图 82. 检测到的危险宏指令

您可以选择该标签的查看模式。如果您不想查看提示性事件，取消选中 **显示全部事件**复选框

16.3.7. *注册表*标签

注册表标签 (见图图 83) 记录了程序操作注册表键值的历史，除非被规则 (见 9.1.3.2 在 97 页) 禁止。

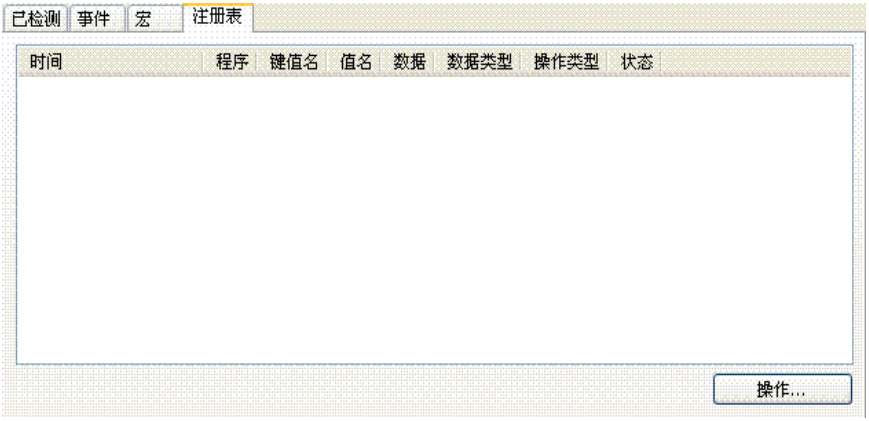


图 83. 读取和修改系统注册表事件

该标签列出了键全称、键值、数据烈性以及已发生的操作信息： 何时有哪些操作企图以及操作是否被允许。

16.3.8. 网络钓鱼标签

该报告标签 (见图图 84) 显示了卡巴斯基反病毒 6.0 Windows 工作站当前进程中发生的所有钓鱼企图。该报告列出了已检测到了邮件中的钓鱼网址的链接，检测到攻击的日期和时间以及攻击状态 (无论受阻与否) 。

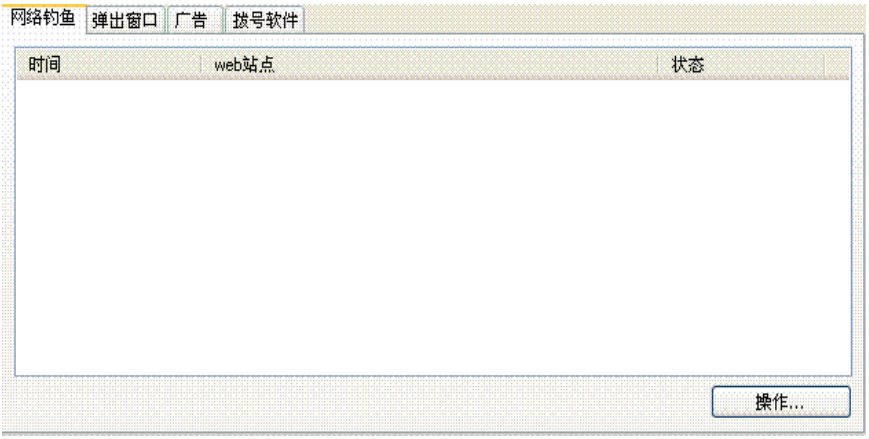


图 84. 受阻的钓鱼攻击

16.3.9. 弹出窗口标签

该报告标签 (见图图 85) 列出了由反间谍保护拦截的弹出窗口的地址。通常从网址打开这些窗口。

每一被弹出拦截器拦截的窗口的地址、日期和时间都会被记录下来。

图 85. 被拦截弹出窗口列表

16.3.10. 广告标签

该报告标签 (见图图 86) 包含由卡巴斯基反病毒 6.0 Windows 工作站当前进程检测到的广告工具条地址。每个广告工具条的网址以及处理状态被列出来 (拦截的工具条或者已显示的工具条) 。

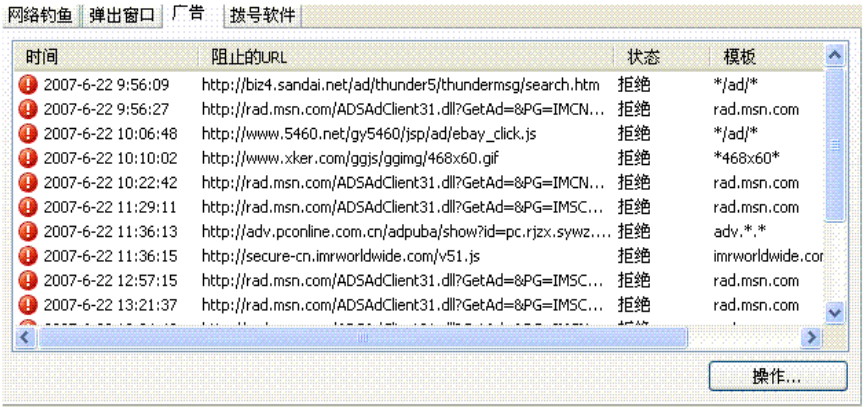


图 86. 被拦截的广告工具条列表

您可以允许显示被拦截的广告工具条。操作方法是，从列表中选择您需要的对象，然后点击 **操作 → 允许**按钮。

16.3.11. 拨号软件标签

该标签 (见图图 87) 显示所有秘密拨号软件企图连接到付费网站的行为。这类企图通常由安装到您计算机中的恶意程序来实施。

在报告中，您可以查看是什么程序试图拨号连接到互联网和请求的状态：已拦截的或者允许的。

图 87. 拨号企图列表

16.3.12. 网络攻击标签

该标签 (见图图 88) 总体显示了您计算机上受到的网络攻击。如果启用入侵检测系统，则记录这些信息。入侵检测系统能监控所有企图攻击您的计算机的行为。

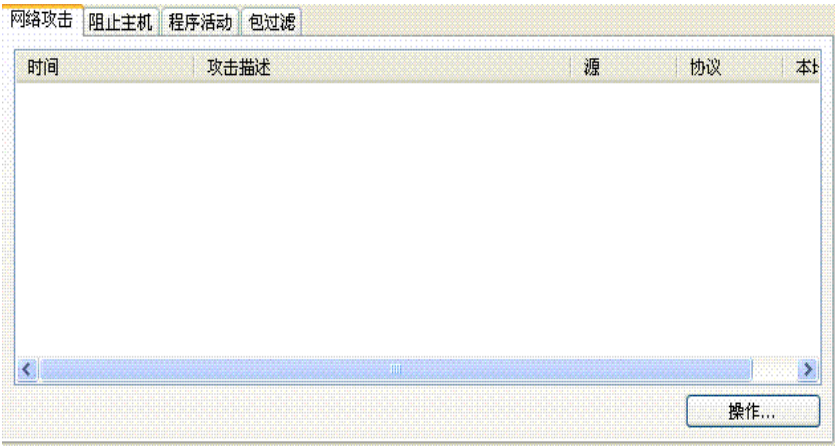


图 88. 被阻截的网络攻击列表

*网络攻击*标签列出了以下攻击信息：

- 攻击源。这可能是一个 IP 地址或主机等。
- 试图攻击您计算机的本地端口。

- 攻击的简要描述。
- 企图进行攻击的时间。

16.3.13. 阻止主机标签

该报告标签 (见图图 89) 列出了攻击被入侵检测系统检测到之后所有被拦截的主机。

每个主机的名称和禁用的时间都会显示出来。您可以在该标签上启用主机。 为此，在列表中选择主机然后点击**操作 → 启用**按钮。

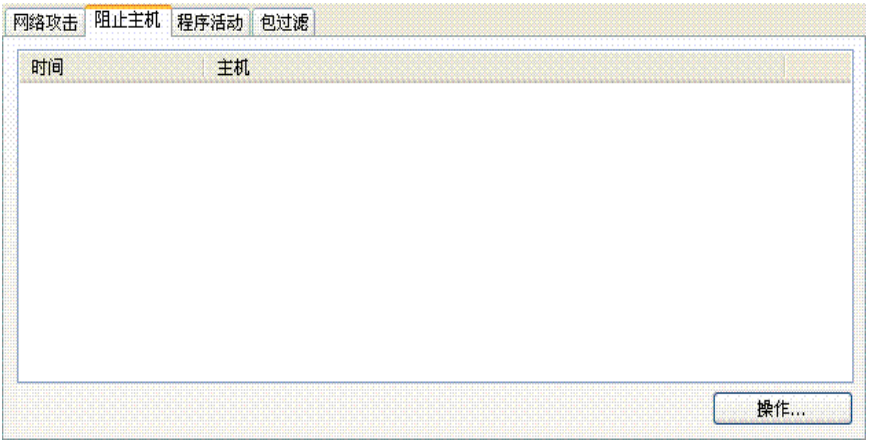


图 89. 被拦截的主机列表

16.3.14. 程序活动标签

如果卡巴斯基反病毒 6.0 Windows 工作站正使用防火墙，**程序行为**标签 (见图图 90) 中会列出所有应用程序 (其动作符合程序规则并且在本程序的当前会话期间已记录下来) 。

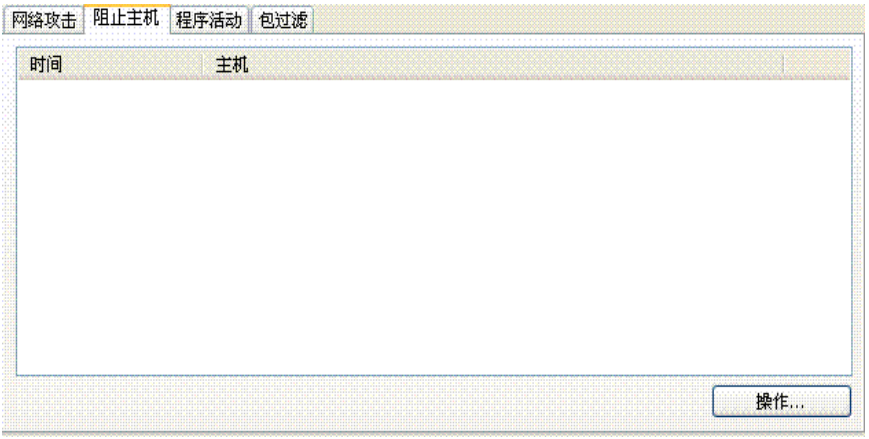


图 90. 受监控的程序行为

只有选中了规则中的 **记录事件**复选框才记录程序行为。默认情况下，在卡巴斯基反病毒 6.0 Windows 工作站自带的程序规则中，不选中该复选框。

该标签显示每个程序的基本属性 (程序名称，进程号，规则名) 及其行为的简要描述 (使用的协议，包方向等) 。也列出了程序行为是否被拦截的信息。

16.3.15. 包过滤标签

包过滤标签包含收发包的信息。这些收发包满足过滤规则并且在应用程序的当前会话期间被记录了下来 (见 图 91)。

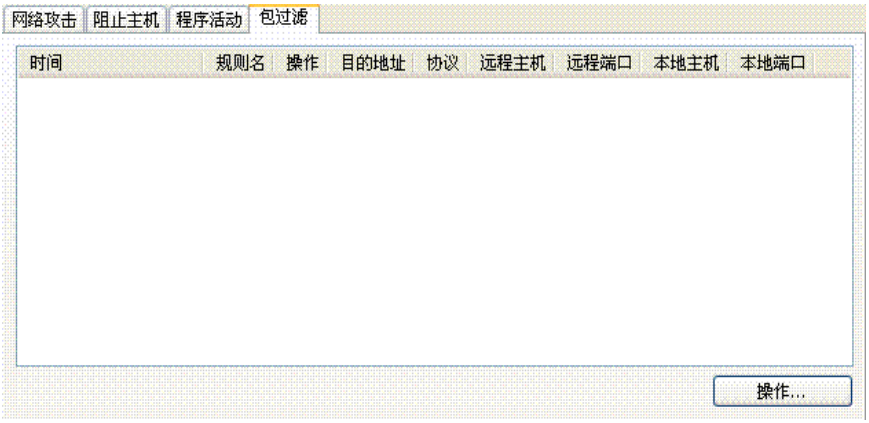


图 91. 受监控的数据包

只有选中了规则中的 **记录事件**复选框才记录程序行为。默认情况下，在卡巴斯基反病毒 6.0 Windows 工作站自带的包过滤规则中，不选中该复选框。

显示了每个包的过滤结果 (包是否被拦截)，包的去向，协议和其它收发包的网络连接。

16.3.16. 建立连接标签

已建立连接标签 (见图图 92) 中列出了目前您计算机中所有激活的已建立的网络连接。这里您可以看到启动连接的程序的名称，所使用的端口，连接指向 (进入的或者发出的) 以及连接设置 (本地和远程端口和 IP 地址)。您也可以看到一个连接已激活了多长时间以及已发送和已接收的数据量。您可以创建或删除连接规则。操作方法是，使用快捷菜单上的合适选项。您可以通过右键点击连接列表打开快捷菜单。

图 92. 已建立的连接列表

16.3.17. 打开端口标签

打开的端口 标签 (见图 图 93). 列出了您计算机上为建立网络连接而当前打开的所有端口。它列出了端口号，数据传输的端口，使用端口的程序名称和每个端口打开了多长时间等信息。

图 93. 计算机上打开的端口列表

如果您确切地知道哪些端口有漏洞，则在病毒爆发期间和网络受到攻击时，该新信息可能会有作用。您可以找出您计算机中的端口是否被打开，并采取必要的操作来保护您的计算机 (例如，启用入侵检测，关闭易受攻击端口或者为它创建规则) 。

16.3.18. *通信量*标签

该标签 (见图图 94) 包含通过您的计算机和其它计算机 (包括网页服务器，邮件服务器等等) 之间建立的连接进出的所有信息。每一连接的信息包括：主机名和主机连接使用的 IP 地址以及已发送和已接收的传输流量。

图 94. 已建立的网路连接传输

16.4. 程序的常规信息

您可以通过主窗口上的**服务**区域查看程序的常规信息 (见图图 95)。

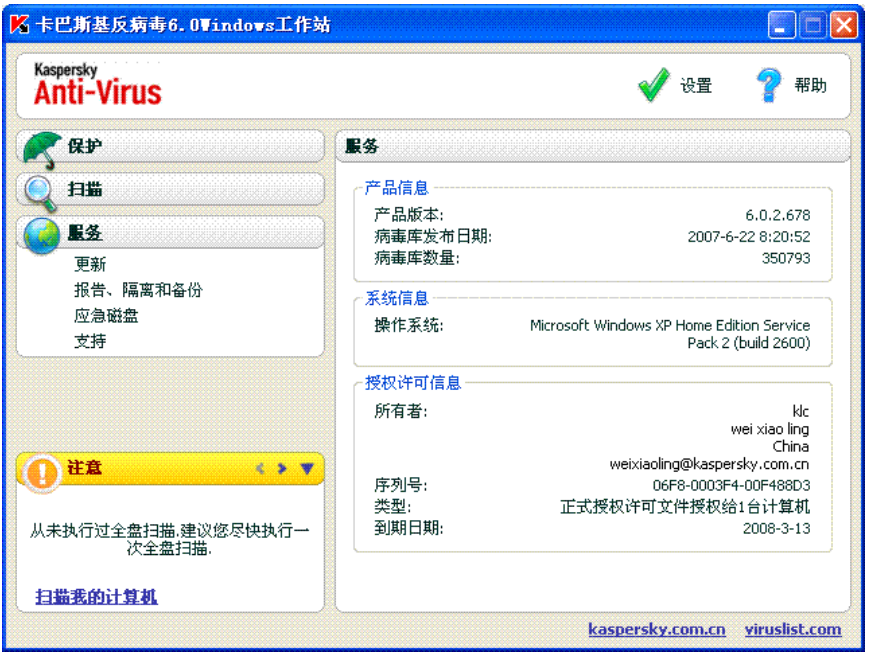


图 95. 程序、许可证以及安装的系统的信息

所有信息都分成三部分：

- 程序版本，最近更新日期，病毒记录数都显示在**产品信息**框中。

- 您计算机操作系统的基本信息都显示在**系统信息**框中。
- 您购买的卡巴斯基反病毒的基本授权信息都包含在**授权许可信息**框中。

与卡巴斯基实验室“技术支持”(见 16.5 在 199 页) 联系时，您需要提供所有这些信息。

16.5. 延长授权许可

卡巴斯基® 反病毒 Windows 工作站需要一个授权*许可文件才*能运行。购买卡巴斯基产品时会提供授权许可文件。它使您从安装完授权许可文件时起有权使用该程序。

除非使用已激活的试用版程序，否则没有授权许可文件，只能以更新模式运行卡巴斯基反病毒组件。该程序将无法下载任何更新程序。

如果本程序的试用版已激活，但在试用过期后，将无法运行卡巴斯基反病毒软件。

当授权许可过期以后，除了不能更新反病毒数据库，程序将继续工作。这时，您可以扫描病毒和使用保护组件，但反病毒数据库只是授权许可过期前的。我们不能保证您的计算机在本程序许可过期后不受病毒的侵扰。

为了避免新病毒的感染，我么建议您延长卡巴斯基反病毒 Windows 工作站的授权许可。程序会在过期前两个星期通知您。在这两个星期期间，您每次打开程序时，就会显示此信息。

要延长您的授权许可文件，您必须购买和安装一个新的卡巴斯基反病毒授权许可文件,或者输入一个程序激活码。操作如下：

与您购买产品的代理商联系再次购买程序授权许可文件

或者

点击授权许可信息窗口 (见图 **图** 96) 上的“购买”授权许可链接，直接从卡巴斯基实验室购买授权许可文件或激活码。 在我们的网址上填写表格。您付款后，我们会按照您在订单上输入的电子邮件地址将授权许可文件或激活码发送给您。

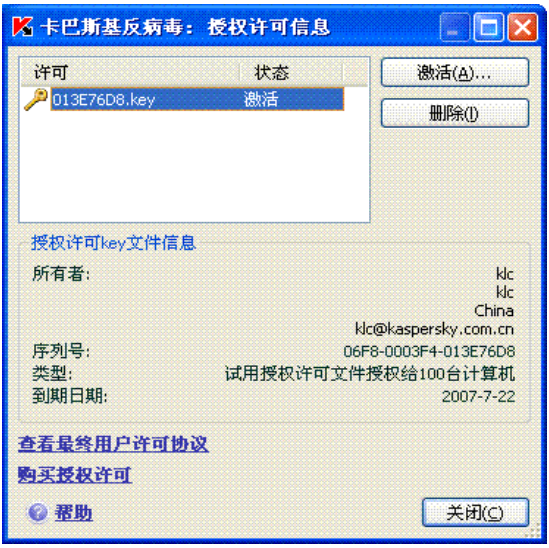


图 96. 授权许可信息

对于产品续费，卡巴斯基实验室定期有特价活动。您可以登录卡巴斯基实验室网站，在 **产品 → 销售与特价**专区查询有关特价活动的信息。

程序主界面**服务**区域上的**授权许可信息**框中提供了当前授权许可文件的信息。左键点击该框的任何部分进入授权许可管理窗口。在打开的窗口 (见图图 96)，您可以查看有关当前授权许可文件的信息，添加授权许可文件或删除。

当您从**授权许可信息**框中的列表选择授权许可文件时，将显示有关该授权许可的编号、类型以及有效期的信息。点击**添加**并通过激活向导激活应用程序来添加新的授权许可文件。要删除列表中的密钥，按下**删除**按钮。

点击查看最终用户许可协议查看许可协议的条款。点击购买授权许可，通过填写卡巴斯基实验室网址上的表格获取授权许可。

16.6. 技术支持

卡巴斯基反病毒 6.0 Windows 工作站为您提供了大量有关程序运行的问题以及解决的的方法。用户可以在**服务**区域查找到技术**支持** (见图图 97) 。

图 97. 技术支持信息

根据不同的问题，我们提供了若干的技术支持服务：

用户论坛。是程序用户对关于产品问题，内容和建议的卡巴斯基实验室网站的一部分。您可以浏览论坛的话题，也可以留下您的意见。 您还可以在这里找到您的问题的答案。

使用用户论坛链接访问该资源。

常见问题。这也是卡巴斯基实验室网站的一个专区，对使用卡巴斯基实验室软件经常出现的问题给出建议。试着找到您问题的答案或解决方案。

点击知识库链接获取在线技术支持。

提交错误报告或建议。这项服务的设立是为了就程序运行中出现的问题予以解释或加以说明。您必须填写卡巴斯基制定的关于情况细节描述的表格。为了更好地处理问题，卡巴斯基实验室需要一些您计算机的信息。您可以自己描述它，也可以使用软件进行收集。

使用提交故障报告或建议链接转入意见表格。

技术支持。如果您需要使用卡巴斯基反病毒方面的帮助，请点击**本地支持服务中心**窗口上的链接。系统会打开卡巴斯基实验室网址，并显示如何联系我们的专家。

16.7. 创建监控端口列表

当我们使用像邮件保护，web 反病毒，反间谍，反垃圾邮件这些保护组件时，使用一定协议传输的数据流都被监控，这也要求打开一定的端口。例如，邮件反病毒分析使用 SMTP 协议传输的信息，而网络反病毒分析使用 HTTP 协议传输的信息。

经常被使用的 e-mail 传输和 HTTP 传输端口列表包含在程序包中。您可以增加一个新端口或禁用监控一定端口的使用，因此这就使利用此端口的危险对象不起作用。

要编辑监控列表，请按照如下步骤操作：

1. 点击程序主界面上的设置链接，打开卡巴斯基反病毒 6.0 Windows 工作站设置窗口。
2. 选择程序设置目录树的**服务**区域上的**网络设置**。
3. 点击设置窗口右侧上的“**端口设置**”。
4. 编辑打开窗口的监控端口列表 (见图图 98) 。

该窗口提供了卡巴斯基反病毒监控的端口列表。选择 **监控所有端口**选项，扫描通过所有打开的网络端口上的数据流。选择 **仅监控所选的端口**，对受监控的端口进行手动编辑。

如果通过卡巴斯基 Administration Kit 管理卡巴斯基反病毒 6.0，而卡巴斯基 6.0 在 MS Windows98 系统下运行，则我们不建议选择**监控所有端口**选项。否则在访问网络资源和接入互联网时可能出现问题。

图 98. 受监控端口列表

要将新的端口添加到受监控的端口列表中：

1. 在**端口设置**窗口点击**添加**按钮。
2. 在**新端口**窗口的相应栏输入端口号以及端口描述。

例如，您的计算机上有一个非标准端口，它与远程计算机交换数据使用 HTTP 协议。Web 反病毒监控 HTTP 的传输。您可以将此端口添加到控制端口列表中来分析恶意代码的通信量。

任何组件启动时，卡巴斯基反病毒 6.0 windows 工作站会打开 1110 端口，以此作为所有加入的连接的监听端口。如果此端口此时是繁忙的，选择 1111，1112 等作为监听端口。

如果您同时使用卡巴斯基反病毒 6.0 Windows 工作站和其它公司的防火墙，您必须配置另外的防火墙，使它允许使用以上端口的 avp.exe 进程。

例如，您的防火墙包含一个 iexplorer.exe 的规则，它允许建立 80 端口的连接。

然而，当卡巴斯基反病毒 6.0 Windows 工作站拦截了 iexplorer.exe 对 80 端口的连接询问，它传输到 avp.exe，使其尝试建立一个独立 web 页的连接。如果有 avp.exe 不允许的规则，防火墙将会阻止该询问。因此用户将不能访问该网页。

16.8. 检查您的 SSL 连接

使用 SSL 协议进行连接可以保护互联网的数据交换。SSL 协议能够识别使用电子证书交换数据的各方，对传输的数据进行加密以及确保数据传输时的完整性。

然而黑客正是利用该协议的这些特点来传播恶意程序，因为大多数反病毒程序不扫描 SSL 传输。

卡巴斯基反病毒 6.0 可以提供对 SSL 传输的病毒扫描。如果企图安全地连接到网络资源上，则屏幕上会显示通知，提示用户进行操作。

通知包含有关该程序启动安全连接以及远程地址和端口的信息。该程序会提示您确定是否对该连接进行病毒扫描：

- **处理**-安全连接到网站时扫描通信量。

  我们建议您，如果您正在使用可疑的网址或您转入下一页时如果 SSL 数据开始传输，则应始终扫描 SSL 传输。这很可能表明，恶意程序正在通过安全协议进行传输。

- **不扫描**-与网址保持安全连接而没有对通信量进行扫描。

选中☑ **全部应用**，对所有试图建立 SSL 连接的行为采取将来选定的处理操作。

卡巴斯基反病毒使用其签署的证书替代了所要求的安全证书，以实现对加密连接的扫描。有些情况下，正在建立连接的程序不会接受这种证书，从而导致无法建立连接。我们建议遇到以下情况时禁用 SSL 传输扫描：

- 当连接到可信任网络资源时，例如您的银行网页，您通过该网页管理您个人的帐户。在此情况下，接受银行证书授权的确认是十分重要的。
- 如果程序建立了连接，则检查正在访问的网站的证书。例如，当 MSN 信使与服务器建立连接时，会检查微软公司数字签名的授权情况。

您可以在程序设置窗口的**加密连接**标签上配置 SSL 扫描设置：

检查所有加密连接-对使用 SSL 协议的全部输入的通信量进行扫描。

检测到新的加密连接时提示用户-每次建立 SSL 连接时显示信息，提示用户进行操作。

不检查加密连接-对使用 SSL 协议的全部输入的通信量不进行扫描。

16.9. 配置卡巴斯基反病毒 6.0 WINDOWS 工作站的界面

卡巴斯基反病毒 6.0 Windows 工作站给您提供了创建和使用程序界面的选择功能。您也可以配置活动接口参数，例如：系统的托盘图标和弹出式信息的设置。

您可以按照如下步骤配置程序界面：

1. 点击程序主界面上的设置链接，打开卡巴斯基反病毒 6.0 Windows 工作站设置窗口。
2. 选择程序设置目录树的**服务**区域中的**界面**选项 (见图图 99)。

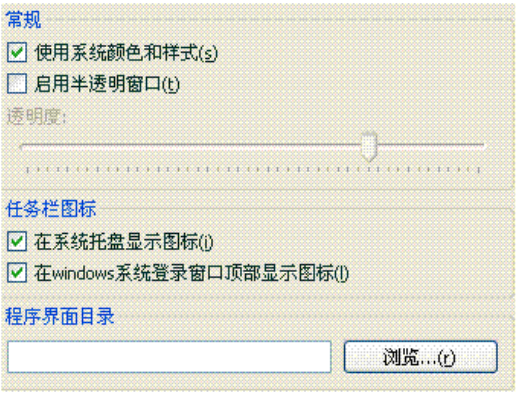


图 99. 配置程序界面设置

在设置窗口右侧，您可以确定：

- 当运行您的操作系统时，是否显示卡巴斯基反病毒 6.0 Windows 工作站的保护提示器。

  当程序加载时，提示器将默认在屏幕的右上角显示。它将通知您，您的计算机可以防御各种类型的安全威胁。如果您不想使用保护指示器，请取消选中 **在 windows 登陆窗口顶部显示图标。**

- 是否在系统的托盘图标里面使用活动的图标。

  根据程序在操作系统上面的运行状况，系统托盘的图标将会变动。例如：如果正在扫描脚本，一个小的脚本描述将会显示在托盘图标的背景上，如果正在扫描是一封邮件，则脚本描述显示在信封上。默认情况下，启用活动图标。如果您想要关闭活动图标，则取消选中 **处理时托盘图标活动**

此时图标只反映您的计算机的保护状态。如果启用安全模式，图标会变红，而如果暂停或禁用保护模式，图标将变成灰色。

- 弹出式信息的透明度。

  当弹出式信息位于系统托盘图标之上时，所有的卡巴斯基反病毒 6.0 Windows 工作站的操作必须立即到达您或要求您做出决定。为了不影响您的工作，窗口中的信息是半透明的。如果您在窗口上移动光标，透明度则会消失。您可以改变信息窗口的透明度。操作方法是时，将**透明度参数**标尺调整到合理位置。取消选中 **启用半透明窗口**去除信息透明度。

  该功能在 Windows 98/NT 4.0/ME 系统的机器上不可用。

- 使用您自己的程序界面。

  在卡巴斯基反病毒 6.0 Windows 工作站中的所有使用的颜色、字体、图标和文本都可以改变。您可以为程序创建您自己的图片或使用另外一种语言。要使用一个新界面，在**带界面描述的目录**栏可以指定目录及其设置。使用**浏览**按钮选择目录。

  默认情况下，该程序的界面采用系统的颜色和样式。您可以取消选中**使用系统的颜色和样式**将其取消。此时将使用您在屏幕主题设置中指定的样式。

请注意，如果您恢复到默认设置或卸载程序时，用户在卡巴斯基反病毒 6.0 Windows 工作站中所定义的接口设置信息将不会被保存。

16.10. 应急磁盘

卡巴斯基反病毒工作站有一个创建应急磁盘的工具。

当病毒攻击导致系统文件损坏或操作系统不能启动时，应急磁盘能够恢复系统功能。该磁盘包括：

- 微软 Windows XP SP2 系统文件
- 一套操作系统诊断工具
- 卡巴斯基反病毒 6.0 Windows 工作站程序文件
- 反病毒数据库文件

要创建应急磁盘：

1. 打开程序主窗口并选择**服务**区域上的应急磁盘。

2. 点击**开始向导**按钮开始创建应急磁盘。

“应急磁盘”只能用于创建本的计算机。将应急磁盘用于其它计算机可能会导致无法预测的后果，因为它载有某台计算机的参数信息 (例如引导区的信息)。

您只能在 Windows XP 和 Microsoft Windows Vista 操作系统下创建应急磁盘。在运行 Microsoft Windows XP Professional x64 Edition 或 Microsoft Windows Vista x64 操作系统的计算机上无法创建应急磁盘。

16.10.1. 创建应急磁盘

警告！ 创建应急磁盘需要 Windows XP SP2 安装盘。

创建“应急磁盘”需要 PE Builder 程序。

创建应急磁盘前，您先要安装 PE Builder 软件。

一个特定的向导指引您完成创建应急磁盘。 它由一系列窗口/步骤组成，您使用**上一步**和**下一步**按钮来进行导航。您可以通过点击**完成**来结束向导。您随时可以使用“**取消**”按钮停止“设置向导”。

步骤1. 准备写入磁盘

指定以下文件夹的路径来创建应急磁盘：

- PE Builder 程序文件夹
- 刻入 CD 之前，应急磁盘文件放置的文件夹

  如果您第一次没有创建应急磁盘，则本文件夹中已经包含了上次制作的一系列文件。要使用以前保存的文件，选中相应的复选框。

  请注意，以前创建的应急磁盘包含的反病毒数据库是过期的。为了更好的抵抗计算机病毒，恢复系统，我们推荐您更新反病毒数据库，然后再创建一个新的应急磁盘。

- 微软 Windows XP SP2 安装 CD

选中 ☑ **允许远程管理正在扫描的计算机**来创建可以启动远程计算机上的操作系统并且使用卡巴斯基反病毒扫描和处理恶意代码的应急磁盘。

请注意，要使用该功能，远程计算机必须支持 Intel® VPRO™ 、 Intel® Active Management Technology (iAMT)。这些技术允许管理员来控制所有与网络远程连接的计算机，包括已关闭的以及操作系统或硬盘的不能正常工作的计算机。

将路径输入到所需的文件夹后，点击**下一步**。PE Builder 将启动，并且将再次开始创建应急磁盘。等待直至完成创建。这可能会花费几分钟的时间。

步骤2. 创建.iso 文件

PE Builder 创建完应急磁盘之后，**创建.iso 文件**窗口将打开。

.iso 文件是应急磁盘的 CD 镜像，可以作为备份保存。大部分 CD 刻录程序都能正确识别.iso 文件 (例如，Nero)。

如果这不是您第一次创建应急磁盘，您可以以前的磁盘中选择.iso 文件。为此选择**现有的 .iso 文件**。

步骤3. 刻录光盘

“向导窗口”将会询问您选择现在还是以后将应急磁盘文件刻录 CD 上。

如果您选择马上刻录，则在刻录前指定您想要的 CD 格式。为此选中相应的复选框。

点击**下一步**按钮后开始刻录 CD。等待直至完成创建。这可能会花费几分钟的时间。

步骤4. 完成创建应急磁盘

该“向导”窗口会通知您已成功创建了应急磁盘。

16.10.2. 使用应急磁盘

请注意，如果打开了主窗口，则卡巴斯基反病毒只能在系统应急模式下运行。您关闭主窗口时，该程序也将关闭。

默认程序 Bart PE 不支持.chm 文件或互联网浏览器，因此在“应急模式”时，您无法在程序的界面查看到卡巴斯基反病毒“帮助”选项或链接。

如果有病毒攻击导致不能启动操作系统的情况发生，则采取以下步骤：

1. 在一台未感染的计算机上使用卡巴斯基反病毒 6.0 Windows 工作站创建一个应急启动盘。
2. 将应急磁盘插入感染的计算机并重启。微软 windows XP SP2 将会从 Bart PE 界面启动。Bart PE 内置功能支持使用局域网网络功能。当程序启动时，它会询问是否使用它。扫描您计算机之前，如果您计划通过局域网更新反病毒数据库，那应选择使用网络支持。如果不需要更新，则取消网络支持。
3. 要打开卡巴斯基反病毒，点击**开始→程序→卡巴斯基反病毒 6.0 Windows 工作站 → 启动**。

   卡巴斯基反病毒 6.0 Windows 工作站主界面将打开。在系统应急模式，您从局域网中只能选择病毒扫描和反病毒数据库更新两项 (如果您已启用了 Bart PE 的网络支持功能) 。
4. 启动病毒扫描。

请注意，默认情况下，使用创建应急磁盘当日的反病毒数据库。由此，我们建议开始扫描前要更新反病毒数据库。

应指出的是，在重启计算机前，应用程序在使用应急磁盘的当前进程期间将只使用更新的“反病毒数据库”。

警告！

扫描计算机时如果检测到受感染或潜在的受感染对象，已经处理并且移到了“隔离区”或“备份区”，则我们建议在使用应急磁盘的当前进程期间处理完成这些对象。

否则重启计算机时将丢失这些对象。

16.11. 使用高级选项

卡巴斯基反病毒工作站提供以下高级功能：

- 程序发生某些事件的通知。
- 卡巴斯基反病毒 6.0 Windows 工作站“自我保护”模块以及程序密码保护被禁用。
- 使用其它应用程序时，解决与卡巴斯基反病毒 6.0 的冲突问题。

要配置这些功能：

1. 在主界面打开程序设置窗口的设置链接。
2. 从设置目录树中选择**服务**。

在屏幕的右侧您可以定义在程序运行时是否使用高级功能。

16.11.1. 卡巴斯基反病毒 6.0 WINDOWS 工作站事件通知

卡巴斯基反病毒 6.0 Windows 工作站发生各种不同的事件。这些事件可能带有信息提示性质的或含有重要信息。例如，一个事件信息可以告诉您程序更新情况或记录一个关于组件的错误必须被立即消除。

要接收卡巴斯基反病毒工作站运行更新的通知，您可以使用通知特性。

通知有以下几种提供方式：

- 在系统托盘弹出信息
- 声音信息
- 电子邮件
- 事件日志中记录的信息

要使用该功能，您必须：

1. 选中与用户交互窗口 (见图图 100) 上的**启用通知**复选框。

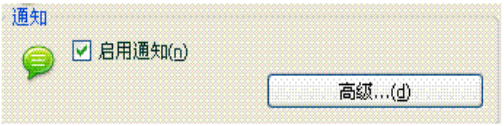


图 100. 启用通知

2. 从卡巴斯基反病毒 6.0 windows 工作站中定义事件类型中，选择 您所想要的通知类型以及提供方式 (见 16.11.1.1 在 210 页)。
3. 配置邮件通知设置，如果该通知方式存在的话 (见 16.11.1.2 在 212 页)。

16.11.1.1. 事件类型和通知方式

在卡巴斯基反病毒 6.0 windows 工作站运行期间，会出现下列几项通知类型：

严重事件：一个危险重大的事件。强烈推荐使用该通知，这表明在您计算机上程序运行出现问题或安全保护存在漏洞。例如，*反病毒数据库损坏或许可过期。*

出错事件-该类事件会导致应用程序无法正常运行。例如，*无授权许可文件或反病毒数据库。*

重要事件是指必须进行调查的事件，因为它们能反应程序操作的重要情况。例如，*保护被禁用或计算机长时间没有被扫描。*

普通信息是指平时操作中所涉及到的、不重要的信息。例如，*所有威胁对象被清除。*

要指定事件通知类型和方式：

1. 点击程序主界面上的设置链接。
2. 在程序设置窗口，选择**服务**，选中 ☑ **启用通知**复选框，并点击**设置**按钮编辑详细的设置。

在打开的**通知设置**窗口配置事件列表中事件的通知方式 (见图图 101)：

- 系统托盘上的程序图标*弹出的信息* (有关所发生事件的提示性信息) 。

  要使用该种通知类型，在**气球形**区域选中 ☑ 您想要被通知的事件。

- *声音提示*

  如果您想使用声音提示事件，从事件的声音处选中 ☑ **声音**。

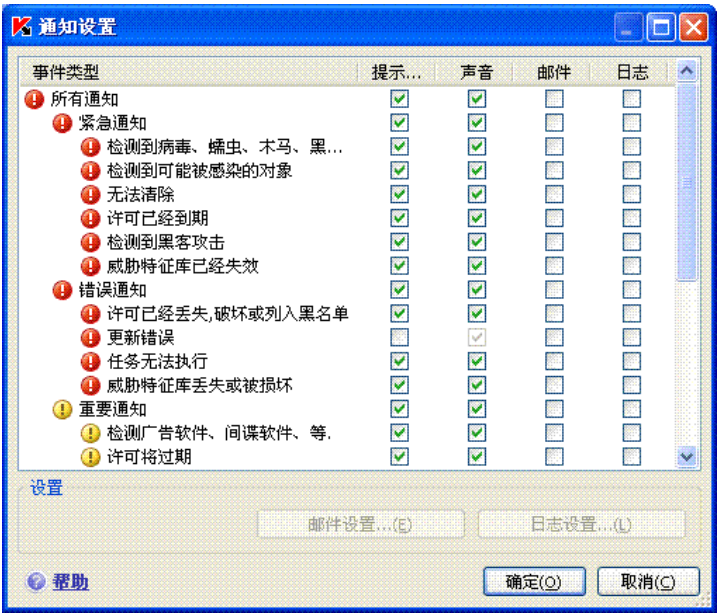


图 101. 程序事件以及事件的通知方式

- 邮件通知

  要使用该类型的通知，在想要被通知的事件栏选中 ☑ **电子邮件**并配置发送通知的设置 (见 16.11.1.2 在 212 页)。

- *在事件日志中记录信息*

  要在日志中记录事件的信息，在**日志**栏选中 ☑ 并配置事件日志设置 (见 16.11.1.3 在 213 页)。

16.11.1.2. 配置邮件通知

在您选择使用邮件来获得通知后 (见 16.11.1.1 在 210 页)，您必须设置通知发送方式。 操作如下：

1. 在主界面打开程序设置窗口的设置链接。
2. 从设置目录树中选择**服务**。
3. 点击屏幕右侧上**与用户交互**窗口 (见图图 100) 中的**高级**选项。

4. 在**通知设置**标签 (见图图 101) 上，选中 E-mail 事件图表中的 复选框。这些事件会触发一封电子邮件消息。

5. 在点击**通知设置**时打开的窗口中配置以下发送邮件通知的设置：

   - 指定**发送人**发送通知设置：**邮件地址**。
   - 在**收件人**处指定通知收件人邮件地址：**邮件地址**。
   - 在**发送模式**中指定邮件通知发送的方式。 如果想要程序在事件一发生就发送邮件，则选中 **当事件发生时立即发送**。对于某一时期内事件的通知，可以点击**编辑**，填写发送提示性信息邮件的计划。 默认设置时每天发送通知。

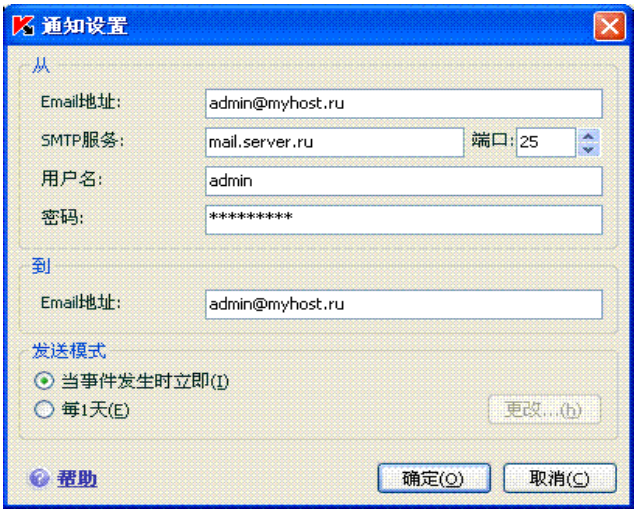


图 102. 配置邮件通知设置

16.11.1.3. 配置事件日志设置

要配置事件日志设置：

1. 在主界面打开程序设置窗口的设置链接。
2. 从设置目录树中选择**服务**。
3. 点击屏幕右侧的**与用户交互**区域中的**高级**选项。

在**通知设置**窗口选择事件日志信息选项，并点击**日志设置**按钮。

卡巴斯基反病毒在 MS Windows 通用事件日志 (**应用程序**) 或卡巴斯基反病毒专用事件日志(**卡巴斯基事件日志**)中提供了记录信息选项，用来记录有关程序运行时所发生的事件。

如果使用 Microsoft Windows 98/ME 操作系统，您将无法在事件日志中记录信息。 如果使用 Microsoft Windows NT 4.0 操作系统，您将无法在**卡巴斯基事件日志**中记录信息。

之所以存在这些局限性，是由这些操作系统的功能决定的。

可以在“MS 事件查看器”中查看日志。您可以通过**开始 → 设置 → 控制面板→ 管理 → 查看事件** 打开“MS 事件查看器”。.

16.11.2. 自我保护和访问限制

卡巴斯基反病毒 6.0 windows 工作站确保您的计算机能够防御危险程序。正因为如此，卡巴斯基反病毒本身可能成为恶意程序攻击的目标，后者会极力对卡巴斯基反病毒组件的活动进行拦截或将其从计算机中删除。

而且，计算机水平不同的人可能会共享同一台 PC。 随便可以使用计算机上的程序及其设置可能会极大降低该计算机的总体安全性。

为确保您的计算机安全系统的稳定性，卡巴斯基反病毒程序中增加了“自我保护”、远程访问防御以及密码保护机制。

如果卡巴斯基反病毒在 Microsoft Windows 98/ME 下运行，则无法使用其自我保护功能。

对于运行 64 位操作系统以及 Microsoft Windows Vista 的计算机，自我保护功能只可以用于防止本地驱动器上的程序自身文件以及系统注册表记录被修改或删除。

要启用自我保护功能：

1. 在主界面打开程序设置窗口的设置链接。
2. 从设置目录树中选择**服务**。
3. 在**自我保护** 窗口 (见图图 103) 进行如下配置：

☑ **启用自我保护**如果选中该复选框，程序将保护其自身的文件，内存中的进程以及系统注册表中的条目免于被删除或修改。

☑ **禁用外部服务控制** 如果选中该复选框，将阻截任何企图使用该程序的远程管理程序。

如果存在企图执行所列操作的行为，系统托盘上的程序图标将会显示消息(在用户没有禁用通知服务的情况下)。

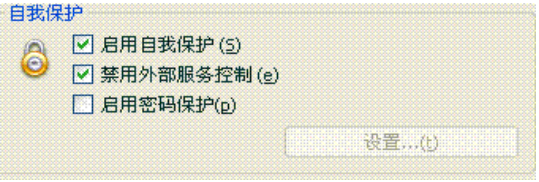


图 103. 配置程序防御功能

要密码保护程序，选中 **启用密码保护**。点击**设置**按钮打开**密码保护**窗口，并输入密码以及限制访问的区域 (见图图 104)。您可以阻止一些程序的运行，发现危险对象的通知或防止下列动作的的执行：

- 更改程序运行设置
- 关闭卡巴斯基反病毒 6.0 windows 工作站
- 禁用或暂停计算机保护

这其中的每项动作都会降低对您的计算机的保护级别，因此要尽力去确定您的计算机上的哪些用户值得信任采取这样的动作。

如果计算机上一些新的用户尝试去执行一些您选择的动作，程序将提示输入密码。

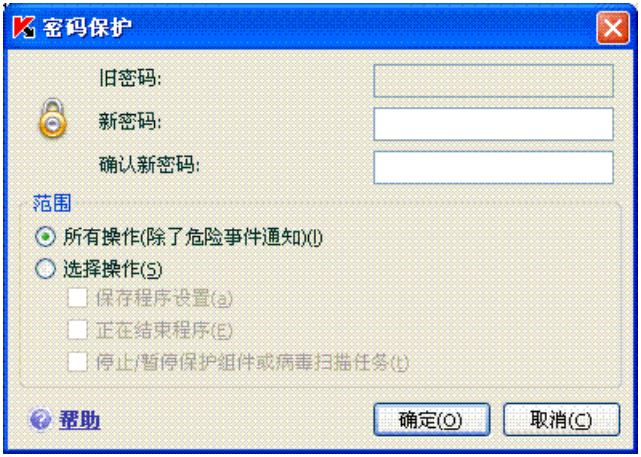


图 104. 程序密码保护设置

16.11.3. 解决与其它应用程序的冲突

有些情况下，卡巴斯基反病毒组件可能会与安装的其它应用程序发生冲突。这是因为那些程序有内置的自我保护机制，当卡巴斯基企图对其进行检测时，自我保护机制会开启。这些应用软件包括 Acrobat Reader 的 Authentica 插件 (对访问.pdf 文件的进行验证)、Oxygen Phone Manager II 以及一些配备数字版权管理工具的计算机游戏。

为解决这样的问题，选中应用程序设置窗口**服务**区域中的**与使用自我保护机制的程序兼容的模式**。为使修改生效，您必须重启计算机。

然而要注意的是，如果您选中该复选框，有些卡巴斯基反病毒功能，尤其时 Office Gard 和反拨号功能将不能使用。如果您启用这其中任何一个组件，则将自动禁用与带有自我保护的应用程序兼容功能。一旦启用这些组件，只有在您重启应用程序后它们才会开始运行。

16.12. 导入和导出卡巴斯基反病毒 6.0 WINDOWS 工作站设置

卡巴斯基反病毒 6.0 Windows 工作站设置窗口。

例如在您家里以及办公室都安装该程序时，此项功能会十分有用。 您可以像在家里一样配置程序，将那些设置保存在磁盘上，使用导入功能将其载入到您办公室的电脑上。 这些设置保存在专门的配置文件里。

要导出程序当前的设置：

1. 打开卡巴斯基反病毒 6.0 Windows 工作站主界面。
2. 选择**服务**窗口并点击设置。
3. 点击**配置管理程序**区域中的**保存**按钮。
4. 输入配置文件名并选择保存位置。

要从配置文件导入设置：

1. 打开卡巴斯基反病毒 6.0 Windows 工作站主界面。
2. 选择**服务**窗口并点击设置。
3. 点击**加载**按钮并选择您想要导入卡巴斯基反病毒 6.0 windows 工作站设置的文件。

16.13. 恢复默认设置

程序的默认设置可以认为是最理想的设置，也是卡巴斯基实验室所推荐使用的。您始终可以将程序恢复到其默认设置。 使用“设置向导”可以完成这一操作。

要重置保护设置：

1. 选择**服务**区域，并点击 设置转入程序配置窗口。
2. 点击**配置管理程序**区域中的**重置**按钮。

打开的窗口提示您指定所要恢复到默认值的设置。

该窗口列出了用户已更改的程序组件或经过自学习功能而发生了变化的程序 (反黑客或非垃圾邮件组件) 任何组件创建的特殊设置页将显示在该列表上。

特殊设置包括：反垃圾邮件组件使用的短语和地址的白名单和黑名单、网络反病毒和反间谍使用的可信任地址列表和 ISP 电话号码列表、程序组件创建的排除规则、包过滤和应用程序反黑客规则以及应用程序主动防御规则等。

基于单个任务和安全需要，这些列表通常由于该程序不断地使用而使内容逐渐膨胀，而且创建这些列表常常需要花费一定的时间。因此建议您保存这些列表后再将其恢复到程序的默认值。

默认情况下，程序在列表上保存了所有自定义设置 (这些设置都没有选中) 。 如果您不需要保存其中的设置，可以选中该复选框。

完成设置配置后，点击**下一步**按钮。初始的“设置向导”将打开。按照其说明进行操作。

完成“设置向导”的操作后，所有组件都设置为推荐的安全级别，但您要保留的设置除外。 除此以外，还将启用您通过“设置向导”配置的设置。

第17章. 命令行下执行程序

您可以在命令行下使用卡巴斯基反病毒组件。 您可以执行以下操作：

- 启动，停止，暂停和继续应用程序组件的动作
- 启动，停止，暂停和继续病毒扫描
- 获得组件、任务的当前的状态信息，及它们的统计信息
- 扫描选择的对象
- 更新反病毒数据库和程序模块
- 获得命令行语法“帮助”
- 获得命令语法“帮助”

命令行语法是：

```
avp.com <command> [settings]
```

> 您必须从程序的安装文件夹的命令行下或指定 avp.com 的完整路径来访问程序。

以下可作为 **<commands>**：

ADDKEY	使用授权许可文件激活程序（只有输入通过程序界面指定的密码才可以执行的命令）
START	启动组件或任务
PAUSE	暂停组件或任务（只有输入通过程序界面指定的密码才可以执行的命令）
RESUME	恢复组件或任务
STOP	停止组件或任务（只有输入通过程序界面指定的密码才可以执行的命令）
STATUS	在屏幕上显示组件或任务的当前状态
STATISTICS	在屏幕上显示组件或任务的统计数字

HELP	命令语法和命令列表帮助
SCAN	扫描病毒对象
UPDATE	开始更新程序
ROLLBACK	恢复到上一次更新的程序 (只有输入通过程序界面指定的密码才可以执行的命令)
EXIT	关闭程序 (您只有使用在程序界面指定的密码才可以执行该命令)
IMPORT	导入卡巴斯基反病毒 6.0 Windows 工作站设置 (只有输入通过程序界面指定的密码才可以执行的命令)
EXPORT	导出卡巴斯基反病毒 6.0 Windows 工作站设置

针对具体的卡巴斯基反病毒 6.0 windows 工作站组件，每项命令使用其自身的设置。

17.1. 激活应用程序

使用授权许可文件可以激活程序授权许可 (ADDKEY 命令) 。

命令语法：

```
ADDKEY <file_name> /password=<password>
```

参数描述：

<file_name>	扩展名为*.key* 的授权许可文件名
<password>	在应用程序界面指定的访问卡巴斯基反病毒的密码

注意： 您如果不输入密码，则无法执行该命令。

例子：

```
avp.com ADDKEY 00000000.key /password=<your_password>
```

17.2. 管理程序组件和任务

您可以在命令行下使用这些命令管理卡巴斯基反病毒 6.0 Windows 工作站组件和任务。

- START
- PAUSE (只有输入通过程序界面指定的密码可以执行的命令)
- RESUME
- STOP (只有输入通过程序界面指定的密码可以执行的命令)
- STATUS
- STATISTICS

命令适用的任务或组件由其参数所决定。

注意：**START/PAUSE/STOP** 命令对应程序界面的 ▶、⏸ 和 ■ 按钮 (见 4.1.2 在 39 页)。

命令语法：

```
avp.com <command> <profile>
avp.com STOP
        PAUSE <profile> /password=<password>
```

以下值分配给 **<profile>**：

RTP	所有保护组件 如果完全禁用 (见 5.1.2 在 46 页) 或暂停 (见 5.1.1 在 45 页) 保护，则命令 avp.com START RTP 启动所有实时保护组件。该命令也启动任何使用 ⏸ 按钮从图形用户界面或命令行下的 PAUSE 命令暂停的实时保护组件。 如果从图形用户界面使用 ■ 按钮或命令行下的 STOP 命令禁用该组件，则命令 avp.com START RTP 将无法启动它。为了启动该组件，您必须执行 avp.com START <profile> 命令，<profile> 中输入具体保护组件的值。例如，avp.com

	START FM。
FM	文件保护
EM	邮件保护
WM	Web 反病毒保护 Web 反病毒子组件值 **httpscan** – 扫描 http 通信量 **sc** – 扫描脚本
BM	主动防御 主动防御子组件值 **og** – 扫描 Microsoft Office 宏指令 **pdm** – 程序活动分析
ASPY	反间谍 反间谍子组件值 **AdBlocker** – AdBlocker **antidial** – 反拨号 **antiphishing** – 反钓鱼 **popupchk** – 弹出广告拦截器
AH	反黑客 反黑客子组件值 **fw** – 防火墙 **ids** – 侵入检测系统
AS	反垃圾邮件
UPDATER	更新
RetranslationCfg	将更新程序发布给本地源：

Rollback	恢复到上一次更新的程序
SCAN_OBJECTS	病毒扫描任务
SCAN_MY_COMPUTER	“我的电脑”任务
SCAN_CRITICAL_AREAS	“关键区域”任务
SCAN_STARTUP	“启动对象”任务
SCAN_QUARANTINE	扫描隔离的对象
<task name>	用户自定义任务
由命令行下启动的组件和任务运行时，采用在程序界面配置的设置。	

例子：

要启用文件保护组件，在命令行下键入：

```
avp.com START FM
```

要查看您计算机上的“主动防御”的当前状态，在命令行下键入：

```
avp.com STATUS BM
```

要从命令行下停止“我的电脑”扫描任务，输入：

```
avp.com STOP SCAN_MY_COMPUTER
/password=<your_password>
```

17.3. 反病毒扫描

命令行下启动扫描一定区域并处理危险对象的语法通常如下：

```
avp.com SCAN [<object scanned>] [<action>] [<file
types>] [<exclusions>] [<configuration file>]
[<report settings>] [<advanced settings>]
```

如要扫描对象，您也可以从命令行下启动卡巴斯基反病毒 6.0 windows 工作站创建的任务 (见 17.1 在 219 页)。任务将采用在程序界面指定的设置运行。

参数描述。

<object scanned> □ 该参数给出了将要被扫描检测有无恶意代码的对象。 它可以包括以下列表中的几个值，用空格分开。	
<files>	要扫描的文件和（或）文件夹的路径列表 您可以输入绝对或相对路径。 列表中的各项以空格分开。 注意： • 如果对象名包括空格，则必须有一个引号标记 • 如果您选择一个文件夹，里面的所有文件都会被扫描
/MEMORY	系统内存对象
/STARTUP	启动对象
/MAIL	电子邮件数据库
/REMDRIVES	所有可移动媒介驱动器
/FIXDRIVES	所有本地驱动器
/NETDRIVES	所有网络驱动器
/QUARANTINE	隔离区对象
/ALL	全盘扫描
/@:<filelist.lst>	文件路径，该文件保护要扫描的对象和文件夹列表。文件应是文本格式，而且每个扫描对象必须启动新的一行。 您可以输入文件的绝对或相对路径。如果路径中有空格必须用引号标出。
<action> □ 此参数设定了扫描到病毒后执行的操作。如果此参数没有指定，默认值是**/i8**。	

/i0	对目标不执行操作；只在报告中简单纪录有关信息。
/i1	处理受感染对象，如果清除失败，则跳过
/i2	处理受感染对象，如果清除失败，则删除。例外情况：不要删除复合对象中的受感染对象；删除带有可执行标题的对象，例如，.sfx 存档文件 (默认)
/i3	处理受感染对象，如果清除失败，则删除。而且如果无法删除受感染内容，则完全删除所有复合对象。
/i4	删除受感染对象，如果清除失败，则删除。而且如果无法删除受感染内容，则完全删除所有复合对象。
/i8	如果删除受感染对象，则提示用户进行操作。
/i9	扫描结束时提示用户进行操作。
<file types> □ 该参数定义了可能会被反病毒扫描的文件类型。如果此参数没有指定，默认值是/fi。	
/fe	只按扩展名扫描潜在受感染的文件。
/fi	只按内容扫描潜在受感染的文件（默认）。
/fa	扫描所有文件
<exclusions> □ 该参数定义了排除扫描的对象。 它可以包括列表中的几个值，用空格分开。	
-e:a	不扫描存档文件
-e:b	不扫描电子邮件数据库
-e:m	不扫描普通的文本邮件
-e:<filemask>	不按关键字扫描对象

-e:<seconds>	在指定时间参数**<seconds>** 内不能扫描完成，跳过此对象。
-es:<size>	跳过大于**<size>** 指定值的文件 (MB)。
<configuration file> □ 定义包含扫描的程序设置的配置文件路径。 配置文件是文本文件，它包含一组反病毒扫描的命令行设置。 您可以输入文件的绝对或相对路径。如果不定义该参数，卡巴斯基反病毒 6.0 windows 工作站中的设定值都可以使用。	
/C:<settings_file>	使用分配到配置文件**<settings_file>**中的设定值
<report settings> □ 该参数决定扫描结果报告的格式。 您可以使用文件的绝对或相对路径。 如果不定义该参数，屏幕上就会显示扫描结果以及所有事件。	
/R:<report_file>	文件中记录重要事件
/RA:<report_file>	文件中记录所有事件
<Advanced settings> – 该设定值定义了使用反病毒扫描技术。	
/iChecker=<on:off>	启用/ 禁用 iChecker
/iSwift=<on:off>	启用/ 禁用 iSwift

例子：

*启动扫描 RAM、启动程序、电子邮件数据库、**我的文档**和**程序文件**目录以及 test.exe 文件：*

```
avp.com SCAN /MEMORY /STARTUP /MAIL "C:\Documents and
Settings\All Users\My Documents" "C:\Program Files"
"C:\Downloads\test.exe"
```

暂停扫描选定的对象并且开始全盘扫描，然后继续扫描选定的对象。

```
avp.com PAUSE SCAN_OBJECTS /password=<your_password>
avp.com START SCAN_MY_COMPUTER
avp.com RESUME SCAN_OBJECTS
```

*扫描 RAM 以及文件 **object2scan.txt** 中列出的对象。 使用配置文件 **scan_setting.txt**。 扫描完后，生成一份记录所有事件的报告。*

```
avp.com SCAN /MEMORY /@:objects2scan.txt /C:scan_settings.txt
/RA:scan.log
```

17.4. 程序更新

在命令行下更新卡巴斯基反病毒 6.0 Windows 工作站程序模块和反病毒数据库的命令行语法是：

```
avp.com UPDATE [<path/URL>] [/R[A]:<report_file>]
[/C:<settings_file>] [/APP]
```

参数描述：

[<path/URL>]	从 HTTP 或 FTP 服务器或网络文件夹下载更新。 如果不选择路径，更新源将从更新程序设置中选定。
/R[A]:<report_file>	**/R:<report_file>** – 文件中仅记录重要事件。 **/R[A]:<report_file>** – 报告中记录所有事件。 您可以使用文件的绝对或相对路径。 如果不定义该参数，屏幕上就会显示扫描结果以及所有事件。
/C:<settings_file>	包含程序更新设置的配置文件的路径。 配置文件是文本文件，它包含一组更新程序的命令行设置。 您可以输入文件的绝对或相对路径。 如果不定义参数，在卡巴斯基反病毒 6.0 windows 工作站中的设定值都可以使用。
/APP	更新程序模块

例子：

更新反病毒数据库以及在报告中记录所有事件：

```
avp.com UPDATE /RA:avbases_upd.txt
```

*使用配置文件 **updateapp.ini** 中的设置更新卡巴斯基反病毒 6.0 Windows 工作站的程序模块：*

```
avp.com UPDATE /APP /C:updateapp.ini
```

17.5. 恢复设置

命令行语法：

```
ROLLBACK [/R[A]:<report_file>][/password=<password>]
```

/R[A]:<report_file>	**/R:<report_file>** – 文件中仅记录重要事件。 **/R[A]:<report_file>** – 报告中记录所有事件。 您可以使用文件的绝对或相对路径。 如果不定义该参数，屏幕上就会显示扫描结果以及所有事件。
<password>	在应用程序界面指定的访问卡巴斯基反病毒的密码

注意：您如果不输入密码，则无法执行该命令。

例子：

```
avp.com ROLLBACK /RA:rollback.txt /password=<your_password>
```

17.6. 导出设置

命令行语法：

```
avp.com EXPORT <profile> <filename>
```

参数描述：

<profile>	组件或任务的设置正在导出。 您可以使用任何**错误！未找到引用源。**列出的值作为**<profile>**（见**错误！未定义书签。**页)。
<filename>	可以将配置文件作为文本文件保存。为此在文件名中指定*.txt* 扩展名。您也可以以二进制格式保存文件。 配置文件以二进制格式 (*.dat*) 保存，除非指定其它格式或如果为指定该格式，则以后可以使用它将应用程序设置导入到其它计算机中。可以将配置文件作为文本文件保存。 为此在文件名中指定*.txt* 扩展名。注意，保护设置不能从文本文件中导入。

例子：

```
avp.com EXPORT c:\settings.dat
```

17.7. 导入设置

命令行语法：

```
avp.com IMPORT <filename> [/password=<password>]
```

<filename>	可以将配置文件作为文本文件保存。 为此在文件名中指定.*dat* 扩展名。 只可以从二进制文件导入设置。
<password>	在应用程序界面指定的访问卡巴斯基反病毒的密码。

注意：您如果不输入密码，则无法执行该命令。

例子：

```
avp.com IMPORT c:\settings.dat /password=<your_password>
```

17.8. 启动程序

命令行语法：

```
avp.com
```

17.9. 停止程序

命令行语法：

```
avp.com EXIT /password=<password>
```

<password>	在应用程序界面指定的访问卡巴斯基反病毒的密码。

注意：您如果不输入密码，则无法执行该命令。

17.10. 查看帮助

该命令是在命令行下查看帮助，其语法如下：

```
avp.com [ /? | HELP ]
```

为获得具体命令的语法，您可以使用以下命令：

```
avp.com <command> /?
avp.com HELP <command>
```

17.11. 命令行界面返回代码

本部分包含命令行返回代码列表。 使用命令行下的任何命令可以返回通用代码。返回代码包括通用代码以及特殊类型任务的专有代码。

通用返回代码	
0	成功完成操作
1	无效设定值
2	未知错误
3	任务完成出错
4	取消任务
反病毒扫描任务返回代码	
101	已处理所有危险对象
102	检测到的危险对象

第18章. 修改、修复和卸载程序

您可以按照以下方式卸载应用软件：

- 使用应用程序“设置向导”
- 从命令行窗口
- 使用卡巴斯基 管理工具(见卡巴斯基 管理工具使用指南)

18.1. 使用安装向导修改、修复和卸载程序

如果您发现在不正确的配置或文件损坏的情况下，程序执行出错，那您必须修复此程序。

修改程序可以是安装卡巴斯基反病毒工作站丢失的组件或删除不需要的组件。

要修复或修改卡巴斯基反病毒工作站丢失的组件或删除该程序。

1. 退出本程序。操作方法是，在系统托盘上左键点击程序图标，从快捷菜单上选择**退出**。
2. 如果使用光盘安装，则将安装盘插入 CD-ROM。如果卡巴斯基反病毒 6.0 Windows 工作站的安装源不同 (共享文件夹，硬盘上的文件夹等等)，确保安装包含在文件夹中并且您有访问权限。
3. 选择 **开始 → 程序 → 卡巴斯基反病毒 6.0 Windows 工作站 → 修改、修复或卸载**

安装向导将打开该程序。 现在让我们详细说明一下修复、修改或删除程序步骤。

步骤 1. 安装欢迎窗口

执行完上面所讲的操作，进行修复和修改程序，系统将显示卡巴斯基反病毒 6.0 windows 工作站安装欢迎窗口。 要继续安装，点击“**下一步**”按钮。

步骤 2. 选择操作

在此阶段，选择您要进行什么操作。您可以修改程序组件，修复已经安装的组件，卸载组件或整个程序。要选择您需要执行的操作，点击相应的按钮。程序的响应取决于您所选择的操作。

修改程序如同自定义安装，您可以指定您想要安装以及删除的组件。

修复程序取决于已经安装的程序组件。 将修复所有已安装组件的文件，并将每一文件设置为“推荐”安全级别。

如果您要卸载程序，可以选择将哪些该程序生成和使用的数据保留在您的计算机中。要删除卡巴斯基反病毒 6.0 windows 工作站的所有数据，选择 **完全卸载**。要保存数据，选择 **保存应用程序对象** 并指定该列表中的哪些对象不删除：

- *激活数据* - 运行应用程序所需的授权许可文件。
- *反病毒数据库* - 截至上一次更新的全套危险程序、病毒以及其它反病毒数据库。
- *反垃圾邮件知识库* - 用于检测垃圾电子邮件的数据库。 此数据库包含垃圾邮件和非垃圾邮件的详细信息。
- *备份文件* – 已删除或清除对象的备份。 建议您保存这些对象，以防日后可能需要恢复。
- *隔离文件* – 潜在地受到病毒或其变种感染的文件。 这些文件包含类似于已知病毒的代码，但难以断定它们是否具有恶意性。 建议您将其保存，因为它们可能实际上并未感染病毒，或者在更新完反病毒数据库后可能会被清除。
- *应用程序设置* – 所有程序组件的配置。
- *iSwift 数据流* – 记录着扫描 NTFS 文件系统后的信息数据库，这能加快扫描速度， 使用该数据库时，卡巴斯基反病毒 6.0 windows 工作站仅扫描自上次扫描以来修改动过的文件。

> 警告！
>
> 如果卸载某一版本的卡巴斯基反病毒 6.0 windows 工作站和重新安装另一版本时间间隔太厂，我们建议您不要使用先前版本保存的 iSwift 数据库。因为在这段时间，危险程序可能会侵入您的计算机，而数据库可能未检测到，从而导致病毒感染。

要启动选项，点击“**下一步**”按钮。 程序将开始把必要的文件拷贝到您的计算机或者删除组件和数据。

步骤 3. 完成程序的修改、修复或卸载

屏幕上将显示程序修改、修复或删除的进程，直至系统将提示您修改、修复或卸载完成。

通常卸载程序会要求您重启计算机，因为它要对您计算机中的信息进行修改。程序将会询问您是否重启计算机。点击**同意**则立即重启。要稍后重启，则点击**不同意**。

18.2. 命令行下卸载程序

要从命令行下卸载卡巴斯基反病毒 6.0 Windows 工作站，输入：

```
msiexec /x <package_name>
```

将打开“设置向导”。您可以使用它来卸载该应用程序 (见第 18 章在 230 页)。

您也可以使用以下命令。

要在后台卸载该应用程序而不重新启动计算机（卸载后必须手动重启计算机），输入：

```
msiexec /x <package_name> /qn
```

要在后台卸载该应用程序，然后重启计算机，则输入：

```
msiexec /x <package_name> ALLOWREBOOT=1 /qn
```

如果您在安装该程序时通过卡巴斯基管理工具选择卸载该程序时使用密码保护，则您在卸载该程序时必须输入密码。 否则无法卸载该程序。

要在后台卸载该应用程序，并通过卡巴斯基管理工具输入密码，则输入：

```
msiexec /x <package_name> KLUNINSTPASSWD=****** /qn
```

第19章. 使用卡巴斯基管理工具管理程序

卡巴斯基管理工具是基于包括卡巴斯基反病毒中小企业 在内的应用程序的系统。它用于集中管理在公司网络的安全系统运行中的关键性的行政任务。

卡巴斯基反病毒 6.0 Windows 工作站是卡巴斯基实验室推出的产品之一。可以通过该工作站的界面、命令行 (“用户指南”中对这些方法已作说明) 或使用卡巴斯基管理工具 (如果计算机是集中式远程管理系统的一部分) 管理该工作站。

有两种方式通过卡巴斯基管理工具管理该程序。

- **本地**：如果选择该选项，则在计算机中安装卡巴斯基反病毒 6.0 Windows 工作站、*网络代理*以及*管理工具*，它们都是 卡巴斯基 管理工具软件包的组件。这样可以通过管理工具实现本地管理。

  如果您计划在未来通过卡巴斯基管理工具远程管理该程序，则当您安*网络代理*时，务必要正确地输入*管理服务器*的地址 (名称和端口) 。

  通过 *管理工具* 进行本地管理时，您只需使用目录树上的**本地计算机** 选项 (图 图 105)。

  在该种模式下，您可以管理卡巴斯基反病毒任务以及计算机的设置。

- **远程**：如果选择该选项：

  - 在网路上部署*管理服务器*，在管理员的工作间安装 *管理工具* (有关详情，请见“卡巴斯基管理工具 6.0 安装管理员指南”)；
  - 在网络的计算机上安装卡巴斯基反病毒 6.0 Windows 工作站以及*网络代理* (卡巴斯基管理工具的组件) 。更多有关在网络计算机上安装卡巴斯基反病毒的信息，请见“卡巴斯基管理工具 6.0 安装管理员指南”)。

如果网络上的计算机安装了卡巴斯基反病毒 5.0，则将其通过卡巴斯基管理工具升级到 6.0 之前，您必须按照以下步骤操作：

- 首先，停止使用该程序的前一版本 (可以通过卡巴斯基管理工具远程实现)；
- 安装前，关闭所有其它应用程序；

- 安装完成后，重启远程计算机行的操作系统

管理工具(图图 105) 允许您通过卡巴斯基管理工具 管理该程序。 它提供了标准的 MMC-集成界面，并且管理员利用它可以实现以下功能：

- 在网络的计算机上远程安装卡巴斯基反病毒 6.0 Windows 工作站以及*网络代理*
- 远程配置网络计算机上安装的卡巴斯基反病毒
- 更新卡巴斯基反病毒反病毒数据库和程序模块
- 管理网络计算机上的本程序的授权许可文件
- 在客户端计算机上查看程序运行的信息

管理员通过卡巴斯基管理工具集中管理该程序时，要确定策略、任务以及应用程序的设置。这些设置都具有保护功能。

应用程序设置 程序运行的基本设置，包括通用保护设置、“备份区”设置等。

任务是应用程序执行的特别操作。可以按类型来划分卡巴斯基反病毒 6.0 的任务(许可文件安装任务、按需扫描任务、反病毒数据库更新恢复任务以及反病毒数据库和应用程序模块更新任务)。每项特殊任务执行时都要在卡巴斯基反病毒中进行设置 (*任务设置*)。

集中管理的重要特点是通过创建和配置组策略来集中远程计算机并管理其设置。

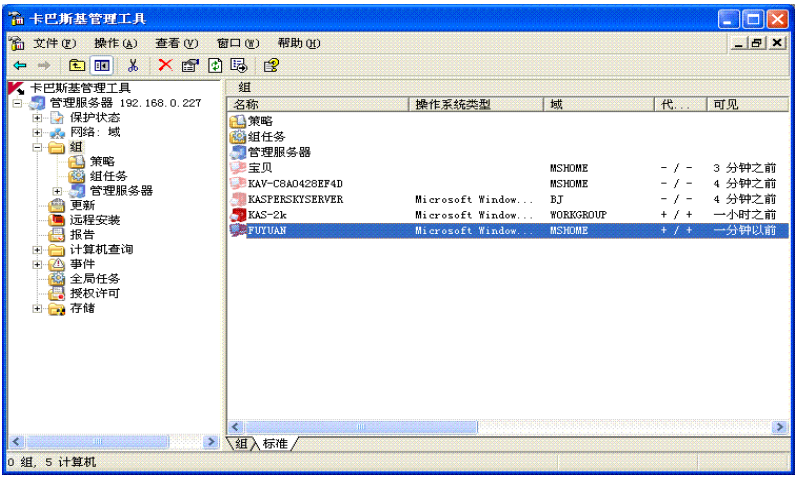


图 105. 卡巴斯基 管理工具界面

组策略是指卡巴斯基反病毒在一个网络组内运行的设置集。策略也可以包括对设置应用程序或任务时指定的配置进行修改的限制。

策略允许您管理应用程序的完整功能，因为它包含应用程序的设置以及所有任务类型的设置，但不包括启动任务时必须直接配置的设置 (例如，任务计划)。

19.1. 管理应用程序

凭借卡巴斯基管理工具， 您可以在客户端计算机上远程启动和暂停卡巴斯基反病毒，以及配置应用程序通用设置，例如启用或禁用计算机保护，配置“备份区”和“隔离区”设置以及配置创建报告的设置。

要管理应用程序设置：

1. 在**组**文件夹 (图图 105) 中选择包含客户端计算机的组文件夹。
2. 在结果面板，选择需要修改应用程序设置的计算机。从快捷菜单或**操作**菜单选择**应用程序**命令。
3. 客户端计算机属性窗口上的**应用程序**标签 (图 图 106) 显示客户端计算机上安装的卡巴斯基实验室应用程序的完整列表。 选择**卡巴斯基反病毒 6.0 Windows 工作站**。

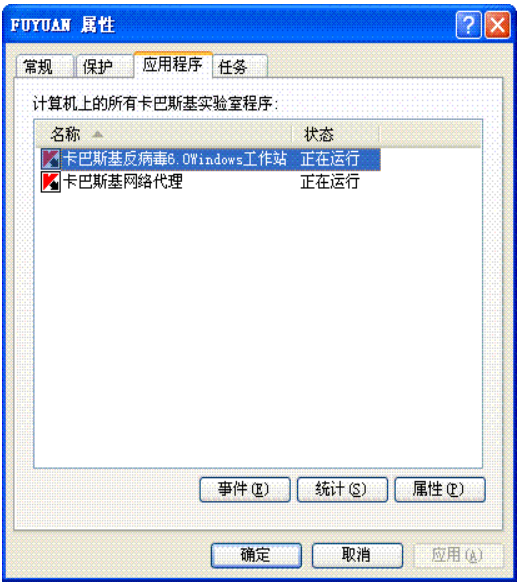


图 106. 卡巴斯基实验室应用程序列表

您可以使用列表下方的按钮：

- 查看服务器上应用程序运行以及记录在管理服务器上的事件列表
- 查看应用程序运行的统计信息
- 配置应用程序设置 (见 19.1.2 在 237 页)

19.1.1. 启动或停止应用程序

您可以在**计算机名称属性**窗口 (图 图 106) 使用快捷菜单上的命令启动或暂停远程计算机上的卡巴斯基反病毒产品。

您可以通过使用**常规**标签 (见图图 107) 上设置窗口中的**开始/停止**按钮来启动或暂停卡巴斯基反病毒组件。

图 107. 配置卡巴斯基反病毒设置，**常规**标签

在该窗口的上方您可以看到已安装的应用程序、版本信息、安装日期、状态（应用程序是否正运行在本地计算机上或暂停使用）以及反病毒数据库状态的信息。

19.1.2. 配置应用程序设置

要查看或修改应用程序设置：

1. 打开**应用程序**标签上的客户端计算机属性窗口 (图 图 106)。
2. 选择**卡巴斯基反病毒 6.0 Windows 工作站**。 点击**属性**按钮打开应用程序设置窗口 (见 图 108)。

卡巴斯基管理工具中，除了**属性**标签，其它所有标签都是标准的。 有关标准标签的详细信息，参见“管理员指南”。

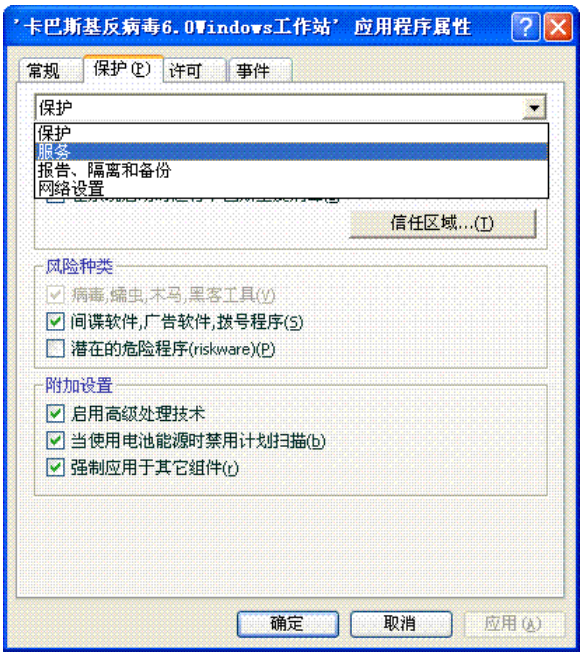


图 108. 配置卡巴斯基反病毒设置，**属性**标签

该应用程序能防止重新配置某些设置，如果已为该程序 (见 19.3.1 在 245 页) 创建了策略，则在配置该程序时，将无法对这些设置进行编辑。

在**属性**标签上，您可以配置常规保护设置、应用程序保护工具设置以及创建和保存应用程序报告统计信息的设置。操作方法是：从该窗口的上半部分中的下拉菜单选择所需的设定值。

保护
在**保护**区域中的**属性**标签上，您可以： • 启用或禁用计算机实时保护； • 配置计算机开机时应用程序的自动启动功能 (见 5.1.5 在 48 页)； • 创建信任区域或排除列表； • 选择应用程序要监控的恶意程序的类型； • 配置应用程序的常规设置以及多处理器设置。
服务
在**服务**区域中的**属性**标签上，您可以： • 配置已发生的事件通知 (见 16.11.1.2 在 212 页)； • 管理应用程序的自我保护功能以及应用程序密码保护设置 (见 16.11.1.3 在 213 页)； • 配置应用程序的界面 (见 19.3.1 在 245 页)； • 配置卡巴斯基反病毒与其它程序间的兼容性设置 (见 16.11.1.3 在 213 页)。
报告、隔离和备份
在该窗口，您可以配置记录应用程序运行的统计信息 (见 16.3.1 在 185 页) 以及指定文件在“备份区” (见 16.1.2 在 179 页) 和“隔离区”(见 16.2.2 在 182 页) 内的保存时间。
网络设置
在该窗口，您可以编辑卡巴斯基反病毒用于扫描的端口的列表以及启用或禁用 SSL 扫描。

19.1.3. 配置专项设置

通过卡巴斯基 管理工具管理卡巴斯基反病毒时，您可以启用或禁用交互性并编辑“技术支持”信息。操作如下：

1. 打开**应用程序**标签上的客户端计算机属性窗口 (图图 106) 。选择**卡巴斯基反病毒 6.0 Windows 工作站并点击属性按钮。** 随后打开应用程序设置窗口。

2. 转至**设置**标签 (图 图 108) 从该窗口的上半部分的下拉菜单选择**服务**。

在**界面**窗口中的**服务**标签上，您可以启用或禁用远程计算机上的卡巴斯基反病毒交互性：显示系统托盘上的卡巴斯基反病毒图标，发布应用程序所发生事件的通知 (例如，检测到危险对象) 。

如果选中 **启用界面交互**复选框，则远程计算机用户将可看到反病毒图标和弹出式信息，并且可以决定通知窗口在发生事件时所要采取的操作。要禁用应用程序交互性，取消选中复选框。

在点击**设置**按钮后打开的窗口中的**自定义支持信息**标签上，您可以编辑用户技术支持信息。该信息显示在卡巴斯基反病毒**支持**选项的**服务**区域上。(图 图 97)。

要变更栏上半部分的信息，输入当前所提供的支持选项上的文字。在该栏的下方，您可以编辑显示在**在线技术支持**窗口上的超链接。选择**服务**区域上的**支持**选项时会上拉“在线技术支持”窗口。

您可以使用**添加**、**编辑**和**删除**按钮编辑链接源列表。卡巴斯基反病毒将添加新链接到列表的顶部。要变更列表中链接的顺序，使用**向上/向下**按钮。

如果该窗口没有任何数据，则不能编辑默认的技术支持信息。

19.2. 管理任务

本部分列出了有关管理卡巴斯基反病毒 6.0 Windows 工作站任务的信息。 更多有关通过卡巴斯基管理工具 6.0 管理任务的概念，请见该程序的“管理员指南”。

安装该应用程序时，每台计算机中都创建了系统任务列表。 该列表 (图 图 109) 包括实时保护任务 (文件保护、网络反病毒保护、邮件保护、主动防御、反间谍、反黑客)、病毒扫描任务 (“我的电脑“、“启动对象”、“关键区域”) 以及更新任务(反病毒数据库和应用程序模块更新以及更新恢复)。

> 您可以启动系统任务，并且为之配置设置和任务，但无法将其删除。

除此之外，您还可以创建自己的任务，例如病毒扫描、应用程序更新、更新恢复以及许可文件安装任务 (见 19.2.2 在 241 页)。

要查看为客户端计算机创建的任务：

1. 在**组**文件夹 (图 图 105) 中选择包含客户端计算机的群组文件夹。

2. 在结果面板，选择您想要查看本地任务列表的计算机。从快捷菜单或**操作**菜单选择**任务**命令。在主界面将打开一窗口，显示出客户端计算机的属性。

3. **任务**标签 (图 图 109) 显示为该客户端计算机创建的任务的完整列表。

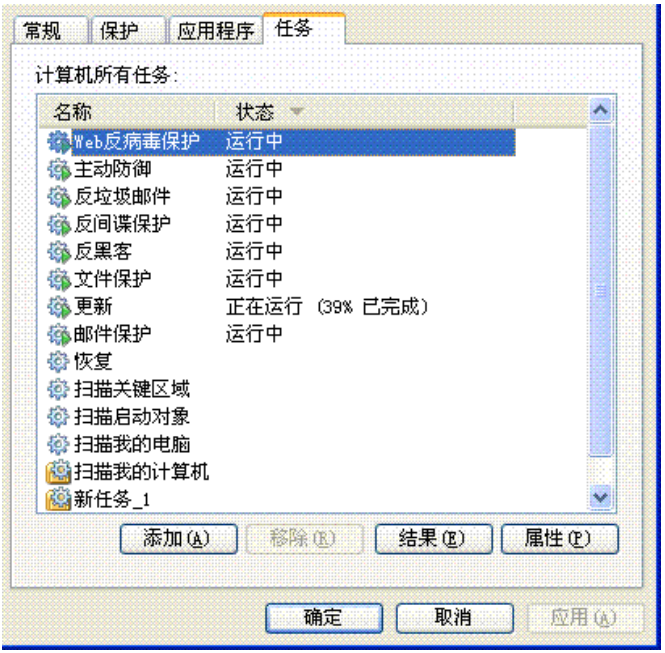


图 109. 应用程序任务列表

19.2.1. 启动和停止任务

只有相应的应用程序在运行时才可以在客户端计算机上启动任务 (见 19.1.1 在 236 页)。如果停用应用程序，所有已启动任务都将中断。

任务根据计划自动启动和暂停，或使用快捷菜单以及“查看任务设置”窗口上的命令手动启动和暂停。 您也可以暂停任务后又恢复任务。

要手动启动/停止/暂停/恢复病毒扫描任务：

从结果面板上选择需要执行的任务 (群或全局)，打开快捷菜单并选择**启动/停止/暂停/恢复**或使用**操作**菜单上同样的命令。

您可以从**常规**标签上的任务设置窗口，使用相同的命令按钮启动所有任务类型的相同操作 (图 图 110)。

19.2.2. 创建任务

通过卡巴斯基管理工具使用该程序时，您可以创建：

- 为个人计算机配置的本地任务
- 为网络组中的计算机配置的组任务
- 为任何网络组中的任何计算机组配置的全局任务

您可以修改任务设置、监控其执行情况、在组之间复制和移动任务并且还可以使用快捷菜单上标准的**复制/粘贴**、**剪切/粘贴**和**删除**命令或**操作**菜单上相同的命令将任务删除。

19.2.2.1. 创建本地任务

要创建本地任务，请按照如下步骤操作：

1. 打开**任务**标签 (图图 109) 上的本地客户端属性窗口。
2. 将启动任务创建向导。该向导包括一系列窗口和步骤，您可以利用**上一步**和**下一步**按钮来回进行操作。您可以按下**完成**按钮来结束向导。您随时可以按下“**取消**”按钮停止“向导”。

步骤 1. 输入任务通用数据

首个主窗口是介绍性的：在此您必须指定任务的名称。

步骤 2. 选择应用程序和任务类型

在此步骤中，您必须指定要创建任务的应用程序 (卡巴斯基反病毒 6.0 Windows 工作站)。您也必须选择任务类型。卡巴斯基反病毒 6.0 可执行的任务包括：

- *病毒扫描* – 对用户指定的区域进行病毒扫描
- *更新* – 下载和应用程序更新包
- *更新恢复* – 恢复到上一次的更新程序
- *许可文件安装* – 添加新的许可文件，以便使用该应用程序

步骤 3. 配置所选任务类型设置

由于上一步所选的任务类型的不同，以下窗口的内容可能会有变化：

病毒扫描

病毒扫描任务配置窗口要求您指定卡巴斯基反病毒检测到危险对象时所要采取的操作(见 13.4.4 在 156 页)。您也必须创建要扫描的对象列表。

更新

对于反病毒数据库和应用程序更新任务，您必须指定将要使用的更新下载源 (见 15.4.1 在 167) 默认的更新源是卡巴斯基管理工具更新服务器。

更新恢复

对于恢复到最近的更新，没有专门的设置。

安装许可文件

对于许可文件安装任务，使用**浏览**按钮来指定许可文件的路径。要添加备份密钥，选中 **添加备份授权许可文件。**一旦当前的许可授权许可文件到期，授权备份文件将激活。

以下栏将显示添加的密钥的有关信息（许可编号、类型以及有效期）。

步骤 4. 选择用户帐号

在此步骤中，系统要求您使用用户帐号配置启动任务，并且该帐号有权访问被扫描对象或更新源 (有关详情，请见 57 页上的 5.4)。

步骤 5. 设置计划

配置完任务设置后，系统会提示您配置自动执行任务计划。

操作方法是：从下拉菜单上选择执行任务的频率并在该窗口的下半部分调节任务设置。

步骤 6. 完成任务创建

“向导”的最后窗口会通知您已成功创建了任务。

19.2.2.2. 创建组任务

要创建组任务，请按照如下步骤操作：

1. 从控制板目录树选择您需要创建任务的组。
2. 选择它的 **任务** 文件夹，打开快捷菜单并选择 **创建 → 任务** 命令，或使用**操作**菜单上相同的命令。类似于本地任务创建向导，任务创建向导将启动 (有关详情，请见 19.2.2.1 在 241 页)。按照其说明进行操作。

向导结束后，该任务将添加到该组及其所有子组的**任务**文件夹中，这将在结果面板中可以看到。

19.2.2.3. 创建全局任务

要创建全局任务，请按照如下步骤操作：

1. 选择 控制台目录树 (见图 105) 上的**全局任务**节点，打开快捷菜单，选择 **创建 → 任务**命令或使用**操作**菜单上的相同命令。
2. 类似于本地任务创建向导，任务创建向导将启动 (有关详情，请见 19.2.2.1 在 241 页)。不同的是，需要创建网络客户端计算机列表（该网络是要创建全局任务的网络）。
3. 从该网络选择将要执行任务的计算机。 您可以从多个文件夹选择计算机，也可以从真个文件夹中选择(有关详情，请见“卡巴斯基管理工具 6.0 管理员指南”)。

只有在选定的计算机上才可以执行全局任务。如果将新的客户端计算机添加到已创建远程安装任务的计算机组中，则新添加的计算机无法执行该任务。您必须创建新的任务或对当前的任务设置做相应的变更。

向导结束后，全局任务将添加控制面板目录树的**全局任务**节点上，这将在结果面板中可以看到。

19.2.3. 配置专项任务设置

要查看或修改客户端计算机设置：

1. 打开**任务**标签 (图 图 109) 上的客户端计算机属性窗口。
2. 从列表中选择任务并点击**属性**按钮。随后任务设置窗口将打开 (见图 110)。

卡巴斯基管理工具 6.0 中，除了**设置**标签，其它所有标签都是标准的。 “管理员用户指南”中对它们进行了更深入的说明。 **设置**标签包含卡巴斯基反病毒专项设置。 该标签的内容会随所选任务类型的不同而不同。

通过卡巴斯基管理工具界面配置程序任务设置类似于通过本地的卡巴斯基反病毒界面进行的设置，不同之处在于，在前者中，要为每一用户单独配置有些设置，例如反垃圾邮件白名单和黑名单。见 第 6 章 – 第 15 章，61 – 164 在本用户指南的这几页中，对任务设置配置进行了更深入的说明。

如果已为应用程序 (能防止一些设置被重新配置) 创建了策略，则在配置该任务时，这些设置将不编辑。

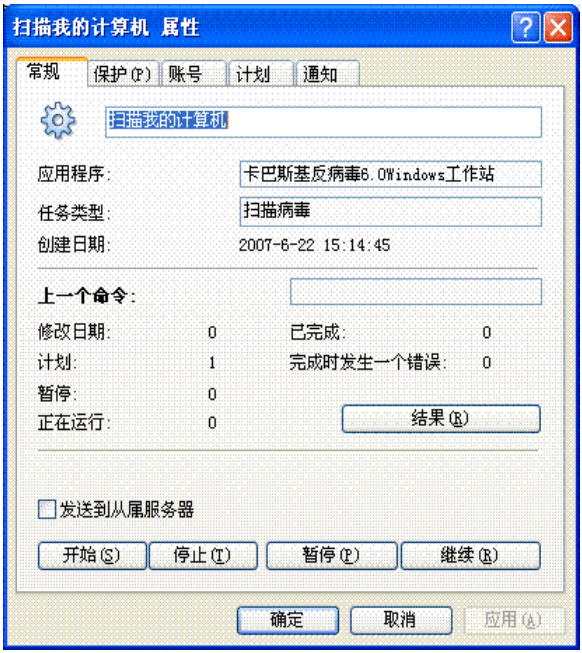


图 110. 配置任务设置

19.3. 管理策略

您可以通过设置策略将通用的应用程序和任务设置应用到单一网络组的客户端计算机上。

本部分包括有关创建和配置卡巴斯基反病毒 6.0 Windows 工作站策略的信息。更多有关通过卡巴斯基管理工具 6.0 管理任务的概念，请见该程序的“管理员指南”。

19.3.1. 创建策略

要创建卡巴斯基反病毒策略，请按照如下步骤操作：

1. 在**组**文件夹 (图图 105) 中选择您需要创建策略的计算机组。
2. 选择属于所选组的**策略**文件夹，打开快捷菜单，使用**创建→策略** 命令。系统将显示“创建新策略”窗口。

在 Windows 向导中创建策略。该向导包括一系列窗口和步骤，您可以利用**上一步**和**下一步**按钮来回进行操作。您可以按下**完成**按钮来结束向导。您随时可以按下“**取消**”按钮停止“向导”。

在创建策略的每一步中，可使用 按钮锁定输入的设定值。 如果该按钮上的锁已关闭，则当您在以后客户端计算机上使用该策略时，将会使用到由该策略指定的设定值。

步骤 1. 输入策略通用数据

向导的第一步是介绍性的。在向导的第一个窗口，您必须指定策略的名称。在第二个窗口，从**应用程序名称下**拉菜单选择**卡巴斯基反病毒 6.0 Windows 工作站**。创建完策略后，如果您想要该策略设置立即生效，则选中**激活策略**复选框。

步骤 2. 选择策略状态

该窗口将提示您指定策略状态。操作方法是，将开关移动到需要的位置：已激活策略、未激活策略或移动用户策略（在计算机与网络断开后生效）。

在一个应用程序组中可以创建若干个策略，但是其中只有一个是当前 (激活的) 策略。

步骤 3. 选择和配置保护组件

在此步骤中，您可以启用、禁用和配置策略中将要使用到的保护组件。

默认情况下，启用所有保护组件。要禁用组件，只要取消选中组件名称旁的文本框就可以了。从列表中选择保护设置并点击**设置**按钮来调整保护设置或配置文件保护。

步骤 4. 配置病毒扫描设置

在此步骤中，您可以配置病毒扫描任务将要使用到的设置。

在**安全级别**区域选择其中一个预设的安全选项 (见 13.4.1 在 153 页)。点击**设置**按钮来调整所选级别。要恢复**推荐**的设置，点击**默认**按钮。

在**操作**区域指定反病毒组件在检测到危险对象时应采执行的操作 (见 13.4.4 在 156 页)。

步骤 5. 配置更新设置

在此窗口配置卡巴斯基反病毒更新发布设置。

在**更新设置**区域指定更新的对象。在点击**设置**按钮时打开的窗口中指定本地网络设置 (见 15.4.3 在 171 页) 并指定更新源 (见 15.4.1 在 167 页)。

在**更新后动作**区域启用/禁用接收到新的更新包后扫描“隔离区” (见 15.4.4 在 173 页)。

步骤 6. 执行策略

在此步骤中，选择对组中的客户端计算机执行策略的方法 (有关详情，请见“卡巴斯基管理工具 6.0 管理员指南”)。

步骤 7. 完成策略创建

“向导”的最后窗口会通知您已成功创建了策略。

向导完成后，卡巴斯基反病毒策略会被添加到相应群组的**策略**文件夹 (见图 105) 中，并且在结果面板中将可以看到。

您可以使用 按钮为每一设置组编辑已创建的策略设置以及设定修改设置的限制。如果按此方式锁定设置，客户端计算机用户将不能更改设置。客户端与服务器首次同步时，该策略将应用到客户端计算机上。

您可以使用快捷菜单上标准的**复制**/**粘贴**、**剪切**/**粘贴**和**删除**命令或**操作**菜单上相同的命令在组之间复制和移动任务，还可以将任务删除。

19.3.2. 查看和编辑策略设置

在此编辑步骤中，您可以修改策略并阻止在嵌套组策略以及应用程序和任务设置中修改设置。

要查看和编辑策略设置：

1. 在**组**文件夹中选择必须从控制面板目录树编辑设置的计算机群组。
2. 选择属于该群组的**策略**文件夹 (见图 105)。选择完后，结果面板将会显示所有为该群组所创建的策略。
3. 从**卡巴斯基反病毒 6.0 Windows 工作站**的策略列表选择您所需的策略 (**应用程序** 栏指定了应用程序名称)。
4. 从所选策略的快捷菜单选择**属性**命令。 将打开策略设置窗口，该窗口包含几个标签 (见图 111)。

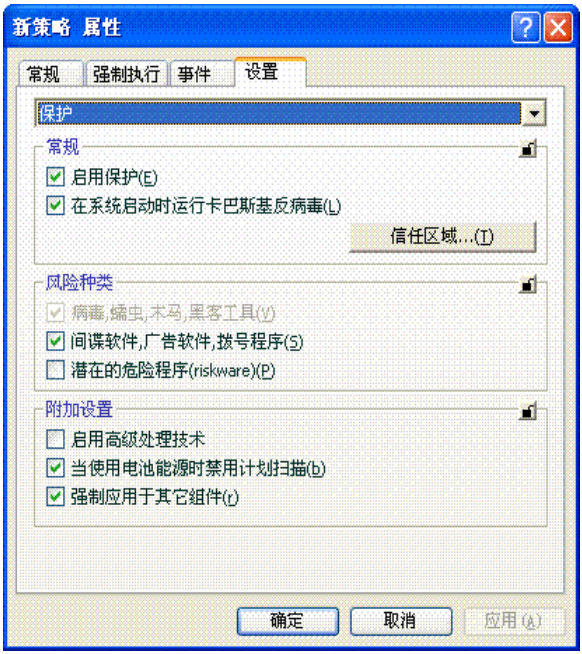


图 111. 配置策略设置

在卡巴斯基管理工具中，除**设置**标签外，所有其它的标签都是标准的。(有关详细信息，请参见该程序的“管理员指南”)。

设置标签包含卡巴斯基反病毒 6.0 策略设置。策略设置包括程序设置 (见 19.1.2 在 237 页) 和任务设置 (见 19.1.3 在 238 页)。

要配置其设置，从下拉菜单中选择所需设定值并予以配置。

第20章. 常见问题

本章主要涉及用户在安装、设置和运行卡巴斯基反病毒 6.0 Windows 工作站中最常遇到问题，在此我们将就这些问题予以详细的解答。

问题： *可以在使用卡巴斯基反病毒 6.0 Windows 工作站的同时使用其它公司的反病毒产品吗？*

不行。我们建议您在安装卡巴斯基反病毒 6.0 Windows 工作站之前，卸载其它公司的反病毒产品，以避免发生软件冲突。

问题： *卡巴斯基反病毒 6.0 Windows 工作站不会对早先已扫描的文件再次进行扫描么？ 为什么呢？*

确实如此。卡巴斯基反病毒 6.0 Windows 工作站不会对自上一次扫描以来没有变化的文件再次进行扫描。

由于采用新型的 iChecker 和 iStream 技术，从而使这成为现实。本程序在采用该技术时在 NTFS 交替数据流中使用了文件校验和与件校验和存储数据库。

问题： *为什么需要授权许可文件？ 没有授权许可文件，卡巴斯基反病毒 6.0 Windows 工作站程序可以运行吗？*

没有授权许可文件卡巴斯基反病毒 6.0 Windows 工作站也能够运行，但您将无法获得“更新程序”和“技术支持”。

如果您还没有决定是否购买卡巴斯基反病毒 6.0 Windows 工作站，我们将提供给您试用的授权许可文件，它可以使用 2 周或 1 个月的时间。时间一到期，该授权将作废。

附录. 标准产品最终用户授权许可协议

所有用户请注意：以下是卡巴斯基实验室(以下称为“卡巴斯基实验室”)编制的、关于网络版工作站端反恶意程序软件(以下简称为“软件”)的授权许可的法律协议(以下简称为“协议”)，在继续安装及开始使用本软件前，务请仔细阅读。

若您不同意本协议的所有条款，请单击表明您不接受本协议条款的按钮，且不要安装本软件。

若您是以物理介质的形式合法购得此软件，且已打开光盘的封套，则表明您(无论是个人还是一个独立的机构)已同意受此协议的约束。

此处所述“软件”包含由卡巴斯基实验室提供给您的软件激活文件(亦称“授权许可文件”或“Key 文件”)。

1. 授权许可。在已支付相应的许可费用及同意本协议条款和条件的前提下，卡巴斯基实验室在此授予您以非独占的、非转让的方式在本协议的条款下仅为自己内部事务目的而使用本软件指定版本的副本以及附随文档(以下简称“文档”)的权利。您可以在合法安装了本软件限定的操作系统的一台计算机、或一个工作站、或一个个人数字助理、或本软件针对其设计的其它一件电子设备(每个都是一个“客户端设备”)上安装本软件的一个副本。若本软件的使用许可是作为一个套装或与多个指定软件产品的捆绑包而获得的，则本授权许可在用户支付了规定的费用，且接受产品包装上规定的适用于各软件产品的所有限制或使用条款的条件下，适用于所有这些指定的软件产品。

1.1 使用。本软件允许用户保护的工作站端设备的数量由特制的授权许可文件确定，并在“服务”窗口显示。本软件不能用于保护任何工作站数超过授权许可数量的计算机网络。

1.1.1 当软件被载入工作站端设备的内存(即随机存储器或 RAM)或安装到固定存储器(如硬盘、光盘、或其它存储设备)中时，即视软件在工作站端设备上“使用”。为本软件的合法使用及备份的目的，本授权许可您制作本软件必要数量的备份，所有这些备份必须包含本软件所有权的全部公告。您负责保存本软件和文档的所有备份(包括数量和备份地点)的记录，并负责采取一切适当的预防措施，以避免本软件被未经授权地复制或使用。

1.1.2 本软件保护您的工作站免受恶意代码和网络攻击的侵扰。这些恶意代码和网络攻击的相应特征已包含在卡巴斯基实验室升级服务器上的反恶意代码数据库和反网络攻击数据库中。

1.1.3 如果您要将安装有本软件的工作站端设备出售，请确保在售出前将本软件从工作站端设备上完全删除。

1.1.4 您不能通过反编译、反向工程、反汇编等手段将本软件的任何部分破译为人类可读的形式，也不能许可任何第三方这样做。为获得使本软件与独立创建的计算机程序的协同操作所需的接口信息，在提出请求并支付了合理的费用后，由卡巴斯基实验室提供上述相关信息。如果卡巴斯基实验室通知您，由于任何原因(包括但不限于成本)不能提供这些信息，您才被许可在法律允许的反向工程或反编译的范围内获得软件的互用性信息。

1.1.5 在获得明确的书面许可之前，您不能对本软件进行错误修正，或修改、改编、翻译本软件，不能创建本软件的衍生工程，也无权为任何第三方或允许任何第三方复制本软件。

1.1.6 您不能向任何其他人租用、出租或借出本软件，也不应将您获得的授权许可转让或向任何其他人二次授权。

1.1.7 您不能使用本程序制作自动、半自动或手动的任何可以生成反病毒数据库的工具、进行病毒检测的程序和其他的用于检测恶意代码和数据的代码及数据。

1.1.8 卡巴斯基实验室可以要求用户安装本软件的最新版本(包括最新版本的程序和最新的程序修正包)。

1.1.9 清除潜在的有害的软件。您了解并同意，除检测有害和可疑的软件之外，本产品可能认定、清除和/或失活有潜在危险的软件，包括相关或分类为广告软件、风险软件、色情软件等软件。

1.2 无论您无意或有意地违反了上述条款，都将面临无法更改的本授权许可被中止的风险，并将使您的商业信誉和经济利益受到损害。

2. 支持。

2.1 卡巴斯基实验室将在合法的授权许可的有效期内，向您提供 24╳365 技术支持服务。合法的授权许可有效期从您第一次合法正式激活本程序之时算起，即

2.1.1 已支付软件及技术支持费用；而且

2.1.2 完成最终用户的卡巴斯基实验室的技术支持服务资格认定的附加注册，以建立给予服务的身份档案。

2.1.3 在本软件激活和/或获得终端用户 ID 后获得终端用户享有的技术支持服务。

2.2 完成支持服务预约表，表明您已接受卡巴斯基实验室的隐私政策条款(该条款附在本协议之后)，并明确同意根据上述条款传送相关数据。

2.3 一般情况下，用户需要按年度和当时的服务费用标准支付下一年度的产品和技术支持服务费用，并重新成功完成技术支持服务预约表，以保证软件的升级和工作正常连续，享受的技术支持服务正常连续。

2.4 在合法的授权许可的有效期内，技术支持服务包括下列部分或全部内容：

(a) 在您的计算机有效连网的条件下，按照定制的频率自动更新您本地的反恶意代码数据库。

(b) 在您的计算机有效连网的条件下，按照定制的频率自动更新您本地的反网络攻击数据库。

(c) 在您的计算机有效连网的条件下，按照定制的频率自动更新您本地的反垃圾邮件数据库。

(d) 免费更新软件，包括免费的版本升级。

(e) 由销售商和/或分销商提供的、通过电子邮件和热线电话进行的技术支持。

(f) 24 小时内病毒检测和处置升级。

2.5 卡巴斯基实验室建议您，在软件的升级版本正式发布后，尽快从卡巴斯基实验室的官方中文网站(www.kaspersky.com.cn)下载并换装最新的程序版本(包括程序修正包)，以保证获得高标准的技术支持服务。

3. 所有权。本软件受俄罗斯联邦版权法、中华人民共和国著作权法和相关法律法规保护。卡巴斯基实验室及其供应商拥有并保留本软件的所有权利、名称和利益，包括所有著作权、版权、专利权、商标专有权和其它知识产权。您在合法购买本软件并获得合法使用的授权许可后，可在一定时限内持有、安装及使用本软件，但并未获得本软件的任何知识产权。除本协议明确阐述的内容外，您未获得与本软件相关的任何其它权利。

4. 保密。您同意本软件和相关文档(包括各程序的特殊设计、结构及授权许可文件或 Key 文件)属于卡巴斯基实验室的专有机密信息。未经卡巴斯基实验室事先书面同意，您不能以任何形式向任何第三方泄露、提供这些机密信息或使这些机密信息可被获得。您应采取适当的安全措施以保护这些机密信息，对保障授权许可文件或 Key 文件的安全采用的最佳方式没有限制。

5. 有限担保。

5.1 卡巴斯基实验室担保，本软件首次下载或合法安装后 90 天内，遵循本产品文档指示进行正确操作，完全可以实现文档中描述的功能。

5.2 您自行承担选择本软件来满足您的需求的全部责任。卡巴斯基实验室不担保本软件和/或文档适合您的需求。由于影响软件正常运行的因素具有复杂和不可预测等特征，因此卡巴斯基实验室不担保任何使用都不会间断、或运行毫无差错。

5.3 卡巴斯基实验室不担保本软件可识别所有已知病毒和垃圾邮件，也不担保本软件不会偶尔出现病毒误报。

5.4 卡巴斯基实验室不担保本软件在授权许可文件过期后仍可对工作站提供保护。

5.5 在合法的授权许可的有效期内，如果将出现与 5.1 款不符的情况报告给卡巴斯基实验室或其指定的分销商，卡巴斯基实验室的全部责任及对您的赔偿由卡巴斯基实验室在修复、更换本软件或退还本软件购买款选项中做出选择。您应当向供应商提供所有合理和必要的信息，以协助解决缺陷问题。

5.6 在 5.1 中的担保不适用于下列情况：

(a) 未经卡巴斯基实验室同意，用户对本软件做了修改。

(b) 用户用不恰当的操作方式使用本软件。

(c) 用户没有遵照本授权许可协议使用本软件。

5.7 本协议中陈述的担保和条件取代所有其它有关提供、假设提供、无法提供或延迟提供本软件或文档的条件、担保或期限。除本条第 5.6 款外，被取代的信息或许已在卡巴斯基实验室与您之间的暗示或合并加入此授权许可协议或任何间接合约之间发生作用。无论是法规、习惯法或其它律法，都据此排除(包括但不限于暗示的条件、担保或其它诸如满意的品质、适用性及合理的使用技巧等条款)。

6. 有限责任。

6.1 本协议不排除或限制卡巴斯基实验室的下列责任：

(a) 欺诈性民事侵权行为。

(b) 因违背习惯法的关照责任或因任何疏忽而违背本协议的某项条款导致的死亡或者人身伤害。

(c) 违反 s.12 商品销售法案 1979 或违反 s.2 商品和服务供应法案 1982 中所暗示的义务。

(d) 法律规定不得排除的任何责任。

6.2 在 6.1 款条件下,供应商对下列任何损失或损害(无论这些损失或损害是预见的、可预见的、已知的或其它任何情况)不承担任何责任(无论在合同、民事侵权行为、复原或其它方面):

(a) 收入损失。

(b) 实际或预期利润的损失(包括合同利润损失)。

(c) 资金使用的损失。

(d) 预期储蓄的损失。

(e) 商业交易的损失。

(f) 机会丧失。

(g) 商誉损失。

(h) 名誉损失。

(i) 数据的丢失、损坏或讹误。

(j) 无论任何原因引起的任何间接或继发的损失或损害(包括为避免疑惑，从本条第 6.2 款(a)段到第 6.2 款(i)段中列明的损失或损害的种类)。

6.3 根据第 6.1 款，与提供本软件相关的卡巴斯基实验室的全部责任(无论在合同、民事侵权行为、复原或其它方面)在任何情况下不超过您为本软件所支付的费用。

7. 本协议的解释服从中华人民共和国的法律。合法用户可据此向中华人民共和国的法院提起诉讼。卡巴斯基实验室保留做为原告时在中华人民共和国法律管辖的任何法院提起诉讼的权利。

对自愿使用卡巴斯基实验室的新版试用版产品和演示版产品的用户，将无法享受本标准最终用户授权许可协议第 2 条中提供的技术支持服务，也无权向任何第三方销售自己使用的产品。

在授权许可文件的有效期内，允许用户演示本软件。