卡巴斯基

安全部队 2011

KASPERSKY pure

用户指南

程序版本：11.0

亲爱的用户！

感谢您选择我们的产品。我们衷心的希望该文档能对您有所帮助，并为 您解答产品相关的疑问。

文档版本日期：07/23/2010

http://www.kaspersky.com.cn
http://support.kaspersky.com.cn

目录

关于本指南

该指南是卡巴斯基安全部队 2011 的安装、配置及操作指南。该文档为广大用户量身打造。该软件的用户应具备计算机操作的基本水平：熟悉微软 Windows 操作系统的界面和导航，知道如何使用流行的电子邮件和互联网，例如，微软的 Office Outlook 和微软的 IE 浏览器。

本指南的目标：

- 帮助用户安装、激活该程序，并配置任务；
- 提供与产品相关问题的快速搜索信息；
- 提供获取产品相关的技术支持的方法。

用户指南内容

该指南包含以下几个部分：

附加信息

这一部分包括附加信息的数据描述，互联网上程序相关信息的讨论，分享见解，问题以及收到的答复。

卡巴斯基安全部队 2011

这部分包含程序新功能的描述，以及组件和功能的简要信息。不仅囊括各部分功能而且还向已注册用户提供了一系列的服务。这一部分还包含安装卡巴斯基安全部队 2011 必须满足的软件和硬件的最低要求。

程序安装

这一部分包含的指示将帮助您在计算机上安装该程序并顺利的对其执行初始配置。本节还描述了改程序的卸载过程。

管理授权许可

这一部分包含程序授权许可的基本信息。从这一部分您可以了解到如何延长授权的使用时间，以及从哪里可以查看当前的授权许可信息。

程序界面

这一部分包含程序基本的 GUI 组成部分的描述： 图标和快捷菜单、程序主界面、设置窗口和通知窗口。

启用和禁用程序

这一部分包含程序启用和禁用的相关信息。

计算机保护状态

这一部分将告诉您如何获知您的计算机是否处于受保护的状态，或者一旦您的计算机安全受到威胁，如何消除威胁。在这一部分中，您也可以了解到当卡巴斯基安全部队被启用，禁用，或暂停保护时的相关信息。

常见问题解答

这一部分中包含大多数用户在使用该程序时所遇到的常见问题解决方案。

联系技术支持服务

这一部分包含通过我的卡巴斯基账号与卡巴斯基实验室取得联系的技术支持服务的网站和电话。

专业术语

这一部分包括本文中用到的专业术语目录。

指南规定

该指南中的所有规定详见下表中的描述。

表1. 指南规定

样本	文件中相关描述
请注意...	警告以红色突出显示并括在图文框中。警告包含重要信息，例如，对计算机安全至关重要的计算机操作的相关信息。
推荐使用...	注意括在图文框中的附加信息和参考信息。
例如: ...	示例以独立小节提供，采用黄色背景并具有标题“示例”字样。
更新...	新术语以斜体标记。
Alt+F4	键盘键的名称以半加粗字体标记，并采用首字母大写形式。 键的名称加上“+”号表示使用组合键。
启用	界面组件（例如输入字段、菜单命令、按钮等）的名称以半加粗字体标记。
配置任务计划：	操作说明以箭头符号标记。 操作说明的介绍性短语采用斜体。
`help`	命令行中的文本或在屏幕上显示的消息文本具有特殊的字体。
<您的计算机的 IP 地址>	变量放置在尖括号中。在所有情况下，均放置变量的对应值而不是变量本身，并省略尖括号。

附加信息

若您在选择、购买、安装或者使用卡巴斯基安全部队的时候遇到问题，您可以选择各种信息源寻求答案。您可以根据问题的严重性的紧急程度选择最为合适的信息源。

独立搜索的信息源

卡巴斯基实验室提供以下信息源：

- 卡巴斯基实验室网站上程序相关网页；
- 技术支持网站上程序相关网页；
- 快速技术支持的服务页面；
- 帮助系统。

卡巴斯基实验室网站上程序相关的网页

页面(http://www.kaspersky.com.cn) 将向您提供程序的相关信息，功能和操作菜单。

技术支持网站上程序相关的网页

在(http://support.kaspersky.com.cn) 页面中，您将找到由技术专家创建的技术支持服务条款。

快速技术支持的服务页面

在这一服务页面中，您可以查到基本的程序相关操作的问题和解答。但，若要使用这项服务，首先必须保证互联网的网络连接。

帮助系统

程序的安装包中包含所有的帮助文件。帮助文件中的信息包括如何管理计算机的保护（查看保护状态、扫描病毒以及执行其他操作）。

若要开启帮助文档，您可以点击相关界面上的**帮助**按钮，或按 **F1** 快捷键。

卡巴斯基实验室的官方论坛

如果您的问题不需要马上得到答案，您也可以在卡巴斯基的官方论坛——卡巴一族上进行讨论网址是：http://bbs.kaspersky.com.cn。

联系销售部门

如果您有问题需要与销售部门进行沟通，您可以点击 http://www.kaspersky.com.cn/KL-AboutUs/ConnectionUs.htm 联系我们的销售部门。

您也可以将您的问题通过邮件发送到 sales@kaspersky.com.cn。

联系文档开发组

如果您有任何问题想与文档开发组沟通，或在文档中发现了什么错误您需要反馈，您可以发送邮件至：product@kaspersky.com.cn。请使用“卡巴斯基用户手册反馈：卡巴斯基安全部队”作为邮件的标题。

卡巴斯基安全部队 2011

这部分包含新功能的描述，以及组件和功能的概述；给注册用户提供的服务范围；还有安装卡巴斯基安全部队 2011 的硬件和软件的要求。

新增功能

以下是卡巴斯基安全部队 2011 的新增部分：

- 新增的**系统监控**保护组件可监控系统中的应用程序活动，并为其他保护组件提供详细信息。由于可恢复应用程序的历史活动，因此当检测到恶意程序操作时，该组件可以回滚该程序在系统中所执行的所有操作。
- **安全堡垒**中的高级功能**安全桌面**是一个隔离的桌面，可以在其中启动可疑应用程序，而不会对主操作系统造成任何危害。
- 添加了新模块以改进 Internet 保护：
  - **安全浏览** – 包括上一版本程序中闻名遐迩的链接扫描模块，并且还可以阻止访问不安全的网站，使您能够停留在安全的 Internet 区域。
  - **地域过滤** – 使您能够基于网站所属的特定区域授予或拒绝对网站的访问。例如，可以阻止访问属于高感染风险的地域的网站。
- **应用程序控制**可以使用卡巴斯基安全网络数据更有效地定义应用程序状态以及配置应用程序规则，卡巴斯基安全网络数据是基于对大量用户计算机上的应用程序控制操作的统计信息得出的。
- 通过**空闲扫描**，程序可以在计算机空闲时自动运行病毒扫描，并在您恢复工作时停止扫描。这样即可以定期执行扫描，又可避免在您使用计算机时运行扫描导致计算机运行速度下降。
- 扩展了**上网管理**功能：现在您可以控制用户对计算机和 Internet 的访问及计算机应用程序的启动，限制对包含不当内容的网站的访问和从 Internet 下载文件，控制用户在社交网络中和通过 Internet 寻呼工具的通信，以及查看受控制用户的操作报告。为优化上网管理配置，该模块还包含导入和导出选项，并可按账户分别进行设置。

确保计算机受到保护

卡巴斯基安全部队全面保护您的计算机抵御已知和未知的威胁，来自网络和入侵者的攻击，垃圾邮件以及其他的恶意信息。

威胁的每一种类型都受控于对应的一个独立的*安全组件*（参见这部分中对组件功能的详述）。每一个组件均可以独立于其他组件的启用和禁用，可根据需要进行相应的配置。

此外为了持续的保证您的计算机安全，我们建议您定期扫描计算机。.

若要保证卡巴斯基安全部队完成更新，您不但需要更新数据库，还要更新程序的模块。默认的情况下，程序自动更新。一旦需要，您也可以通过手动设置完成数据库和程序模块的更新。

您可以通过*应用程序控制*来监控已经安装在您的计算机上的所有应用程序。这样的话应用程序在访问*个人数据*时将要受到特定的限制。这些数据包括文件、文件夹、注册表项、用户文件（我的文档文件夹，cookies，以及用户操作相关的信息）。当任何一个应用程序可疑时，可以在*安全桌面*中运行该程序。

偶尔需要执行某些具体的任务，您可以借助附加工具和向导来辅助完成，例如，配置微软 IE 或者清除用户在操作系统上的使用痕迹。

保护组件

下列保护组件对计算机进行实时监控和保护：

- **文件反病毒**

文件反病毒监控计算机的文件系统。它扫描计算机上的所有打开，运行和保存的文件，以及所有连接至计算机的磁盘驱动器。卡巴斯基安全部队能够拦截每个访问文件的尝试，并对这些文件进行已知病毒扫描。只有在文件没有被感染或是被程序成功处理后，文件才能继续运行。如果由于任何原因无法清除病毒，程序将把文件删除，并在备份去保存一份它的拷贝，或是将它移动到隔离区。

- **邮件反病毒**

邮件反病毒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时才允许收信人接收。该组件也会对邮件进行分析以检测钓鱼攻击。

- **网页反病毒**

网页反病毒拦截并阻止网站上的具有威胁的脚本，还会对所有的 HTTP 通信进行深入的监控。该组件还会分析网页以检测钓鱼攻击。

- **即时通讯反病毒**

即时通讯反病毒保证您能够安全地使用互联网即时通讯软件。该组件保护通过 IM 协议来到您计算机的信息。IM 反病毒保证各种即时通讯程序的安全使用。

- **主动防御**

主动防御能够在一个新的恶意程序运行恶意活动之前就对其进行检测。该组件能够监控和分析所有安装在计算机上的应用程序的行为。基于这些行为，卡巴斯基安全部队能够决定应用程序是否具有潜在危险。因此，您的计算机不仅会受到针对已知病毒的保护，还会受到针对那些尚未被发现的新病毒的保护。

- **反钓鱼**

反钓鱼与网页反病毒，反垃圾邮件和即时通讯反病毒相结合，能够对网址进行检测，已确定其是否包含在钓鱼网址和可疑网址列表中。

- **应用程序控制**

应用程序控制会基于它对系统中应用程序的分组来记录它们所执行的动作，并管理它们的活动。该模块会为每个程序组定义一系列的规则，这些规则可以管理应用程序对各种资源的访问。

■ **防火墙**

防火墙组件在您使用互联网以及本地网络时，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，并使用应用程序规则和包过滤规则来过滤所有的互联网活动。

■ **反网络攻击**

反网络攻击在操作系统启动时就会启动，并对入站的网络流量进行跟踪，以检测其是否具有网络攻击的特征。一旦检测到针对计算的攻击尝试，卡巴斯基安全部队就会阻止从攻击计算机发起的所有针对您的计算机的攻击。

■ **反垃圾邮件**

反垃圾邮件嵌入到安装在您计算机上的邮件客户端中，能够监控所有的入站邮件以检测垃圾邮件。它会为所有包含垃圾信息的邮件头部都添加一个特殊标记。同时，该模块也为垃圾邮件处理提供了相应的反垃圾邮件配置选项（自动删除，移动到特殊文件夹等）。该组件还会分析邮件信息以检测钓鱼攻击。

■ **网络监控器**

网络监控器组件用于在实时模式下查看网络活动相关信息。

■ **反广告**

反广告组件能够阻止您计算机上安装的各种应用程序内置的广告条信息，或是在线显示的广告。

■ **上网管理**

上网管理组件监控用户对网页资源的访问。其主要目的就是限制对成人网站的访问，隔离色情、武器、毒品滥用、暴力等信息。同时，它也可以限制用户不在互联网上浪费时间（聊天室、游戏网站等）和金钱（电子银行、网上拍卖等）。

购买方式

您可以从我们的销售人员那购买卡巴斯基安全部队的盒装产品，或者在直接在线购买，如**网上商店** http://www.kaspersky.com.cn/buy/1.php。

如果您购买的是盒装产品，则包装中应包括：

- CD 光盘，其中包括程序的安装文件以及 PDF 格式的文档。
- 快速安装指南（包含激活码）。
- 用户手册及授权许可协议（视地区而定）。

请仔细阅读最终用户授权许可协议（参见 20 页的“关于最终用户授权许可协议”）！

如果您不同意最终用户授权许可协议上面的条款，您可以在安装盘打开之前联系您购买盒装产品的经销商进行退货。

一旦打开安装光盘，就代表您已接受最终用户授权许可协议上的所有条款。

在打开光盘之前，请仔细阅读最终用户授权许可协议。

若您在线购买卡巴斯基安全部队 ,您可以从卡巴斯基实验室的官方网站上下载产品。在确认收到您的付款后，我们会通过邮件向您发送激活码。

注册用户可以享受到的服务

卡巴斯基实验室为授权用户提供一系列的服务，以便于能够更高效的使用该程序。

一旦您购买了授权许可，您就成为了我们的注册用户，我们将竭诚为您提供以下服务：

- 每小时一次的程序数据库更新，并提供产品的最新版本；
- 如果您需要，我们将通过电话或私人账号指导您如何安装、配置及使用我们的产品；
- 卡巴斯基实验室会通知您产品新版本的发布信息，并实时发布世界各地新威胁的信息。该服务仅提供给那些在技术支持网站（http://support.kaspersky.com/subscribe）订阅卡巴斯基实验室新闻的那些用户。

不提供对第三方软件的技术支持服务。

硬件和软件需求

要使卡巴斯基安全部队 2011 正常运行，则您的计算机必须满足以下最低要求：.

常规需求：

- 480 MB 剩余磁盘空间。
- CD / DVD-ROM （用于从 CD 安装卡巴斯基安全部队）。
- 互联网连接（用于产品激活）。
- Microsoft Internet Explorer 6 或更高。
- Microsoft Windows Installer 2.0.

Microsoft Windows XP Home 版（Service Pack 2 或更高）， Microsoft Windows XP Professional 版（Service Pack 2 或更高）， Microsoft Windows XP Professional x64 版 （Service Pack 2 或更高）需求：

- Intel Pentium 800 MHz 32-位 (x86) / 64-位 (x64) 处理器或更高 （或一个更为适合的值）；
- 512 MB 剩余内存。

Microsoft Windows Vista Home Basic， Microsoft Windows Vista Home Premium， Microsoft Windows Vista Business，Microsoft Windows Vista Enterprise， Microsoft Windows Vista Ultimate， Microsoft Windows 7 Starter，Microsoft Windows 7 Home Basic，Microsoft Windows 7 Home Premium，Microsoft Windows 7 Professional, Microsoft Windows 7 Ultimate：

- Intel Pentium 1 GHz 32-位 (x86) / 64-位 (x64) 处理器或更高（或一个更为适合的值）；

- 1GB 剩余内存 （32-位）； 2 GB 剩余内存 （64-位）。

在Microsoft Windows XP （64-位）操作系统中安全堡垒不能工作。在Microsoft Windows Vista （64-位）和 Microsoft Windows 7（64-位）操作系统中工作也会受限。

上网本需求：

- Intel Atom 1.33 MHz (Z520) 处理器或一个更为适合的值。
- Intel GMA950 video card with video RAM 超过 64 MB （或一个更为适合的值）。
- 屏幕规格不小于 10.1"。

安装卡巴斯基安全部队

这一部分包含的信息将协助您安装该程序并完成初始配置。这部分同样包括卸载该程序的描述。

安装程序

在安装向导的协助下，卡巴斯基安全部队将以交互模式安装到您的计算机上。

向导中包含一系列的**上一步**和**下一步**按钮来完成屏幕导航。一旦向导完成导航，您可以点击**完成**按钮关闭向导。若想在某一步骤停止该向导，请使用**取消**按钮。

若在您的计算机上安装卡巴斯基安全部队，

运行包含在产品 CD 光盘上的安装文件（一个扩展名为*.exe 的文件）。

在线下载的卡巴斯基安全部队的安装文件同盒装CD中的安装文件相等同。

步骤 1. 搜索该程序的更新版本

在安装卡巴斯基安全部队之前，先确认卡巴斯基的服务器上是否存在更新的版本。

若在卡巴斯基实验室的服务器上没有搜索到更新的版本，安装向导将被启动。

若更新服务器上提供了卡巴斯基安全部队的新版本程序，您将会看到相应的下载并安装的提示。若您取消下载新版本的程序，安装向导将被启动。若您决定安装更新版本的程序，产品描述文件将下载到您的计算机，并且新版本程序将自动运行安装向导。对于更新版本的程序描述，请参照其对应的文档。

步骤 2. 核查系统是否满足安装需求

在安装卡巴斯基安全部队之前，请核查您的计算机的系统是否符合该软件的安装需求（参见 12 页 “硬件和软件需求”）。

若任何条件不满足，程序会进行相应的提示。这样的情况下，在安装卡巴斯基实验室的产品之前，请按照提示利用 Windows 的更新服务下载或更新所需要的软件环境，以满足要求。

在这一步骤中，卡巴斯基实验室的程序会自动搜索与之不兼容的程序，若您的计算机中的确存在这样的程序，请您将其卸载。

若您的计算机中存在卡巴斯基反病毒软件或卡巴斯基安全部队的早期版本，其相应的数据可以在卸载的时候被保存下来并应用于卡巴斯基安全部队 2011（激活信息、程序设置等。）

步骤 3. 选择安装类型

在这一步骤中，您可以选择卡巴斯基安全部队的安装类型：

- *典型安装*。 若您选择此种类型（没有选中**更改安装设置**复选框），程序将以卡巴斯基实验室的专家们推荐的设置进行完全安装。

- *自定义安装*。若您选择此种类型（选中**更改安装设置**复选框），您将可以选择指定的文件夹作为该程序的安装地址（参见 15 页“步骤 7.选择目标文件夹” ），若需要，您也可以禁用安装过程保护（参见 16 页“步骤 8. 准备安装” ）。

若继续安装，请点击**下一步**。

步骤 4. 查看授权许可协议

眼下，您应该仔细的阅读您和卡巴斯基实验室之间的授权许可协议。

仔细阅读之后，若您同意所有条款，请点击**我同意**按钮。安装将继续进行。

若想取消安装，请点击**取消**按钮。

步骤 5. 卡巴斯基安全网络数据收集声明

这一阶段，您将会被邀请加入卡巴斯基安全网络。加入卡巴斯基安全网络可以加快对新威胁的反应速度，增强保护组件的性能，您加入卡巴斯基安全网络后，将自动向卡巴斯基实验室发送病毒感染的相关信息，包括加载程序和可执行程序的扩展信息统计。但卡巴斯基安全网络不会收集和处理任何个人信息。

详见卡巴斯基安全网络数据收集声明。若您同意加入，请选中**我同意加入卡巴斯基安全网络**复选框。

若您希望自定义安装，请点击**下一步**按钮。（参见 14 页“步骤 3.选择安装类型” ）。当加载标准安装时，请点击**安装**按钮。安装继续进行。

步骤 6. 搜索不兼容的程序

这一步骤中，程序会在您的计算机上自行搜索与卡巴斯基安全部队不兼容的程序。

若没有不兼容的程序，向导会自动执行下一步骤。

若检测出任何不兼容的程序，这些程序会以列表的形式显示出来，您可以根据提示自动或手动将其卸载。移除不兼容的程序之后，需要重启计算机，然后再继续安装卡巴斯基安全部队。

若要继续安装，请点击**下一步**。

步骤 7. 选择目标文件夹

仅使用自定义安装模式，才会出现此步骤。（参见14 页“步骤3.选择安装类型 ” ）。 默认安装时，这一步骤将会被省略，程序将安装到默认的文件夹中。

以下是默认安装路径：

- **<disk> \ Program Files \ Kaspersky Lab \ Kaspersky Internet Security 2011** – 针对 32-位的系统；
- **<disk> \ Program Files (x86) \ Kaspersky Lab \ Kaspersky Internet Security 2011** –针对 64-位的系统。

若将卡巴斯基安装到其他文件夹，请点击**浏览**并在开启的窗口中指定文件夹。

安装文件的路径不能超过200个字符，也不能包含特殊字符****，**/**，**?**，**:**，*****，**"**，**>**，**<** 和 **|**。

若想了解是否有足够的空间安装该程序，您可以点击**磁盘使用**按钮进行查看。在开启的窗口中，您可以查看磁盘信息，若关闭窗口，请点击**确定**。

若继续安装，请在安装向导中点击**下一步**。

步骤 8. 准备安装

仅使用自定义安装模式，才会出现此步骤。（参见14 页“步骤3.选择安装类型 ”）。默认安装时，这一步骤将会被跳过。

一旦您的计算机感染了恶意程序，势必会影响到卡巴斯基安全部队的安装，所以安装过程也应受到保护。

默认情况下，安装过程中是受保护的状态—在安装向导中**保护安装程序**选框默认被勾选。

若程序不能顺利安装，建议您先取消选中该选框（例如，在使用 Window 的远程桌面进行远程安装时）。选中该复选框有可能影响安装。

这种状况下，请中断安装，重启，在选择安装类型这一步骤中选中**更改安装设置**复选框。（参见 14 页“步骤 3.选择安装类型 ”），并且在到达准备安装这一步骤时，取消选中**保护安装程序**。

若继续安装，请点击**安装**。

在Microsoft Windows XP 的系统中安装该程序，安装过程中网络连接可能被中断。稍后连接会自动恢复。

步骤 9. 安装

程序安装的过程大概会花费一些时间。请您耐心等待，直至安装完成。

一旦程序安装完成，向导会自动跳转到下一步骤。

一旦安装的过程中出现错误，若是由于之前计算机上的病毒程序没有被完全清除所引起的，安装向导会向您提供名为 *卡巴斯基病毒移除工具*来协助完成安装。

在您完成移除工作之后，您可以将其删除，并重新安装卡巴斯基安全部队。

步骤 10. 激活程序

激活 是启用授权许可文件以确保您在授权期内完整的应用程序功能的一个必要步骤。

在激活程序时，您需要连接网络。

卡巴斯基安全部队有以下几种激活方式：

- **激活商用版本。**若您选择激活商用版，请选择该选项并输入激活码（参见 21 页“关于激活码”）。

若您输入的是卡巴斯基反病毒软件的激活码，在激活完成之后，程序将转换至卡巴斯基反病毒软件。

- **激活试用版本。** 若您在决定购买商用的授权之前，试用该产品，您可以安装试用版本。您可以使用该程序的全部功能。试用到期后，不能进行第二次试用。
- **稍后激活。** 若您选择该操作，卡巴斯基安全部队的激活步骤将被跳过。您可以使用程序的大部分功能，但不能更新。您仅能在安装卡巴斯基安全部队之后进行一次反病毒数据库和程序模块的更新。**稍后更新**项仅在安装程序后激活向导第一次启动时出现。

若卡巴斯基安全部队安装后被卸载，但激活信息被保留的话，激活步骤将被跳过。激活向导将自动检索激活码并直接继续下一步骤（参见 17 页“步骤 12.完成激活”）。

步骤 11. 注册用户

该步骤仅针对激活商用授权的用户有效。激活试用版时，该步骤被跳过。

注册之后您可以从卡巴斯基实验室获得相应的技术支持。非注册用户仅能得到小部分的技术支持服务。

若您同意注册，填写好对应的注册信息后点击**下一步**按钮。

步骤 12. 完成激活

该向导会向您显示卡巴斯基安全部队成功激活的相关信息。此外，还会提供授权许可的相关信息：授权许可类型（商用或试用），到期日期，以及可用于几台计算机激活。

点击**下一步**按钮继续进行。

步骤 13. 分析系统

在这一步骤中会自动收集 Microsoft Windows 程序的相关信息。这些 程序会被收录到信任列表中，他们对系统的操作将不受限制。

一旦完成分析，该向导会自动跳转到下一步骤。

步骤 14. 关闭向导

向导的最后一个窗口将向您展示安装成功的信息。若要运行卡巴斯基安全部队，请选中**启动卡巴斯基安全部队**复选框，并点击**完成**按钮。

某些时候，您需要重启系统。若选中**启动卡巴斯基安全部队**复选框，系统重启之后会自动运行该程序。

若在关闭向导前，没有选中该复选框，则系统启动后您需要手动运行该程序（参见 28 页“手动启动和禁用卡巴斯基安全部队”）。

启用程序

程序安装完成之后，为了确保更好的保护您的计算机安全，建议您进行以下操作：

- 更新程序数据库（参见 34 页“如何更新程序数据库”）。

- 扫描计算机（参见 36 页“如何执行全盘扫描”）及漏洞扫描（参见 37 页“扫描计算机漏洞”）。
- 核查计算机的保护状态（参见 29 页），必要的话解决安全问题（参见 29 页“诊断和排除计算机保护问题”）。

卸载程序

卡巴斯基安全部队下载之后，您的个人数据将不再受其保护。

您可以使用卸载向导卸载卡巴斯基安全部队。

若要启动向导，则：

1. 在**开始**菜单中，选择**所有程序>卡巴斯基安全部队 2011>修复或卸载**。
2. 在开启的窗口中，点击**卸载**按钮。

步骤 1. 保存数据以备再次使用

在这一部分中您可以指定需要保存的数据，以备下次使用。

默认情况下，程序将从您的计算机上完全卸载。

若要保存数据，请执行以下操作：

1. 选择**保存程序对象**。
2. 核查希望保存的数据：
   - **激活数据** – 卸载程序但并没清除激活数据，只要激活数据不过期，下次再安装程序时，该数据可以继续使用。
   - **反垃圾邮件数据库** – 基于程序下载并保存的垃圾邮件中的特征码。
   - **备份和隔离文件** – 被程序备份或存储至隔离区中的文件。
   - **程序的操作设置** – 在配置程序时所用到的设置值。
   - **iSwift 和 iChecker 数据** – 已经从文件中扫描出来的病毒包含的相关对象信息。
   - **安全桌面共享文件夹数据** –文件保存在一个安全的共享文件夹中，这些文件在主桌面环境和虚拟的安全桌面中均可用。

步骤 2. 确认卸载

若要卸载该程序，可以点击**卸载**按钮。

若想取消卸载，您可以在任何时候点击**取消**按钮。

步骤 3. 完成卸载

这一步骤中，向导会指导您卸载该程序，直至卸载完成。

卸载程序时，您的计算机会提示需要重启。若您取消重启，直至程序重启或下一次开机在启动，卸载过程才算完成。

管理授权许可

这部分包含了程序授权许可的相关信息。从这一部分您还能了解到如何延长授权许可时间以及如何查看当前的授权许可信息。

关于最终用户授权许可协议

最终用户授权许可协议 – 一份自然人和法人之间共同达成的合法协议。最终授权许可协议包含于卡巴斯基实验室的任何一个产品中。其中包含卡巴斯基安全部队使用规则的详细说明。

遵循最终授权许可协议，当您购买和安装卡巴斯基实验室的产品的时候， 您可以拥有拷贝的权限。

关于授权许可

授权许可 是一个使用卡巴斯基安全部队及由卡巴斯基实验室和其合作伙伴提供的额外的服务的授权。

每个授权都有截止日期和相应的类型。

授权许可条款 – 一段时间内提供的额外的服务：

- 技术支持；
- 更新数据库和程序模块。

基于授权类型提供的服务。

以下是被提供的授权类型：

- *试用* – 有一定限期的免费的授权许可，例如，30 天，用于熟悉卡巴斯基安全部队所提供的授权许可。

  试用授权许可只能使用一次，且不能在商用授权许可之后使用！

  一个试用的授权许可仅支持一个试用的程序。一旦试用的授权许可被激活，您就可以连接到程序激活或购买商用授权许可文件对应的技术支持服务。一旦试用期满，卡巴斯基安全部队的所有功能均会失效。如想继续使用该程序，您可以将其激活（参见 33 页“如何激活程序”）。

- *商业授权许可* – 一个商业的授权许可也是有有效期的（例如，一年）。

  一旦激活商用的授权许可，程序所有功能及附加服务均可用。

  在商用授权许可到期后，卡巴斯基反病毒软件仍然具有全部功能，仍然可以扫描计算机以查找病毒和使用保护组件，但是无法更新反病毒数据库，只能使用授权许可到期时所拥有的数据库。在到期之前两周，程序会通知您授权许可即将到期，以便您提前续订授权许可（参见 33 页面“如何购买和续费授权许可”）

关于激活码

*激活码*是随卡巴斯基安全部队商业授权许提供用以激活程序的序列号。

程序的激活码需要一系列的拉丁字母和数字以每五个为一组，一共四组组成。例如，11111-11111-11111-11111。

如果通过在线商店购买该程序，则通过电子邮件发送激活码。如果购买程序的盒装版（零售版），则激活码打印在光盘封套的内表面上，或者打印在包含安装光盘的包装盒的内表面上（位于标签保护层的下方）。

查看授权许可信息

如要查看授权许可文件的相关信息，则：

1. 打开程序的主窗口。
2. 点击窗口底部的**授权许可**按钮，打开**授权许可管理**窗口。

   在该窗口中，您可以启动程序激活。（参见 33 页“如何激活程序”），或购买一个新的授权许可或更新授权许可（参见 33 页“如何购买和续费授权许可”）。

图 1. 授权许可管理窗口

程序界面

卡巴斯基安全部队的程序界面非常的简单易用。这一部分中将详细的讨论这款产品的基本功能。

通知区域图标

安装卡巴斯基安全部队之后，在 Microsoft Windows 的任务栏中将显示程序的图标。

在Microsoft Windows 7的操作系统中，默认的情况下程序图标是被隐藏的，但是您可以设置为显示，以便于访问程序（参见操作系统的文档）。

该图标具有以下基本目的：

- 它是程序运行的指示器。
- 通过它可以直接访问快捷菜单，主程序窗口，以及新闻窗口。

指示程序的活动

该图标是程序活动的指示器。它可以展示程序保护状态和执行一些基本功能时的状态：

 – 扫描邮件；

 – 扫描网页流量；

 – 升级数据库和程序模块；

 – 需要重启计算机以应用更新；

 – 程序的某些组件运行中失败。

默认的情况下，图标是动画形式：例如，扫描邮件的过程中，一个小的邮件图标就在该图标的右下角闪动；更新的时候，一个小的旋转图标就一直在闪动。

访问快捷菜单和程序窗口

您可以使用该图标打开快捷菜单（详见 22 页）和主程序窗口（参见 23 页 “卡巴斯基安全部队主窗口”）。

若要打开快捷菜单：

将鼠标指到该图标上，并右键单击即可。

若要打开程序的主窗口：

将鼠标指到该图标上，左键单击即可。

如果卡巴斯基实验室有新闻发布，则  图标将在 Microsoft Windows 任务栏中显示出来。双击该图标即可查看新闻。

快捷菜单

从快捷菜单，您可以运行基本的保护。

卡巴斯基的快捷菜单中包含以下项目：

- **工具** – 点击该项可以看到以下子菜单：
  - **应用程序控制** – 打开**应用程序活动**窗口；
  - **网络监控** – 打开**网络监控**窗口；
  - **安全键盘** – 显示安全键盘。
- **安全桌面** – 运行可疑程序的一个安全的环境。
- **打开卡巴斯基安全部队** – 打开程序主窗口。
- **暂停保护 / 恢复保护** – 临时禁用实时运行的保护组件。这个菜单项不影响程序的更新，也不影响扫描病毒。
- **启用上网管理 / 禁用上网管理** – 启用 / 禁用当前账号的上网管理。
- **设置** – 打开程序设置窗口。
- **关于**– 打开包含程序信息的窗口。
- **新闻** –打开新闻代理。如果有未读新闻，则会显示此菜单项。
- **退出** – 禁用卡巴斯基安全部队（一旦选择该菜单项，程序将退出计算机 RAM 的加载）。

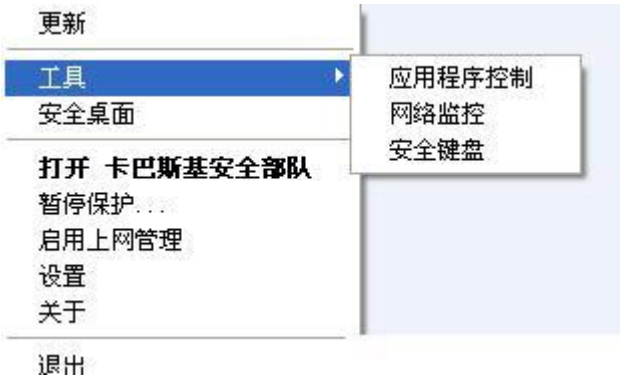

图 2. 快捷菜单

卡巴斯基安全部队主界面

您可以通过程序的主界面访问到程序的所有功能。

程序的主界面可以分成三个部分：

- 窗口顶部包含保护状态指示标志，可以通知您当前的计算机保护状况。

图 3. 当下计算机的保护状态

有三个可能的保护状态值：每个都以特定颜色指示。绿色指示计算机保护处于合适级别，而黄色和红色指示存在各种安全威胁。除了恶意程序之外，威胁还包括应用程序数据库已过时，已禁用保护组件以及选择了最低级别的保护设置等。

安全威胁必须在出现的第一时间进行清除（参见 29 页）。

- 您可以从窗口左侧快速切换到主要程序功能：启用和禁用保护组件、运行病毒扫描任务、更新数据库和程序模块等。

图 4. 主界面的左侧部分

- 窗口右侧包含在窗口左侧选择的程序功能的信息，并且可以让您配置程序功能设置，同时还提供了用于执行病毒扫描任务及检索更新等操作的工具。

图 5. 程序主窗口的右侧部分

还可以使用以下按钮和链接：

- **设置** – 用于打开程序设置窗口。
- **隔离区** – 用于处理隔离对象。
- **报告** – 用于切换到图表格式的程序操作报告。
- **新闻** – 用于切换到新闻代理窗口以查看新闻。程序收到第一条新闻之后，便会显示该链接。
- **帮助** – 用于查看卡巴斯基安全部队帮助系统。
- **我的卡巴斯基账号** – 用于进入技术支持服务网站的用户个人账户。（参见 49 页“我的卡巴斯基账号”）。
- **技术支持** – 用于打开包含系统信息以及卡巴斯基实验室信息资源（技术支持服务网站、论坛）链接的窗口。
- **授权许可** – 用于激活卡巴斯基安全部队以及授权许可续订。

可以使用可选皮肤更改卡巴斯基安全部队的外观。

若要打开程序主窗口，请执行以下操作之一：

- 将鼠标指针滚动到任务栏通知区域中的程序图标上方，并在图标上点击鼠标左键。

在 Microsoft Windows 7 操作系统中，默认情况下程序图标处于隐藏状态，但可以显示该图标以轻松访问程序功能（请参阅操作系统文档）。

- 从快捷菜单中选择**卡巴斯基安全部队**。（参见 22 页“快捷菜单”）；
- 点击位于卡巴斯基工具中心的卡巴斯基安全部队图标（仅适用于 Microsoft Windows Vista 和 Microsoft Windows 7）。

通知窗口

如果在卡巴斯基安全部队操作期间发生事件，屏幕上会显示专门的通知，具体以弹出消息的形式在 Microsoft Windows 任务栏通知区域中的应用程序图标上方显示。

根据事件对计算机安全性的重要程度，您可能会收到以下类型的通知：

- 紧急通知 - 通知您对于计算机安全性而言至关重要的事件：例如，在系统中检测到恶意对象或危险活动。如果显示此类通知，应立即确定进一步的操作。此类型的通知窗口显示为红色。
- 重要通知 - 通知您对于计算机安全性而言可能重要的事件：例如，在系统中检测到可能受感染的对象或可疑活动。如果显示此类通知，应确定检测到的对象或进程的危险程度，并选择进一步的操作。此类型的通知窗口显示为黄色。
- 信息通知 - 通知您非关键事件。此类型的通知窗口显示为绿色。

程序设置窗口

卡巴斯基安全部队设置窗口主要用于配置程序保护组件、扫描和更新任务以及运行其它高级配置。

程序设置窗口由两部分组成：

- 在窗口的左侧，可以选择程序组件、任务或其他需要配置的项目；
- 在窗口的右侧，包含用于配置在窗口左侧选择的项目的控制项。

图 6. 程序设置窗口

窗口左侧的组件、任务和其他内容包含在以下部分中：

– **实时保护**；

– **智能扫描**；

– **免疫更新**；

– **高级设置。**

若要打开设置窗口，请执行以下操作之一：

- 点击程序主窗口顶部的**设置**链接；
- 从程序快捷菜单中选择**设置**；

- 点击卡巴斯基工具界面中带有 **设置**图标的按钮（仅适用于 Microsoft Windows Vista 和 Microsoft Windows 7）。应为按钮指定打开设置窗口的选项。

若要在配置窗口中选择所需的部分，

请点击窗口左上方该部分所对应的图标（请参阅上文）。

卡巴斯基工具

当在微软 Vista 操作系统或 Win7 操作系统中运行卡巴斯基安全部队时，您可以使用卡巴斯基工具。

卡巴斯基工具的设计目的是快速访问程序的主要功能：计算机保护状态、对象扫描、程序操作报告等。

在微软 Win7 操作系统下安装卡巴斯基安全部队后，卡巴斯基工具会自动显示在桌面上。在微软 Vista 操作系统下安装卡巴斯基安全部队后，需要将其手动添加至微软 Windows 边栏（详见操作系统文档）。

图 7. 卡巴斯基工具

运行和停止程序

安装卡巴斯基安全部队后，该程序将自动启动。每次启动操作系统时，都会自动启动该程序。

启用和禁用自动运行

自动运行程序意味着将在启动操作系统启之后启动卡巴斯基安全部队。这是默认启动模式。

禁用或启用自动运行：

1. 打开程序设置窗口。
2. 在窗口左侧的实时**保护部分**中，选择**常规设置**子部分。
3. 若要禁用自动运行，请在窗口右侧的**自动运行**部分中取消选中**计算机启动时运行卡巴斯基安全部队**复选框。若要启用程序自动运行，请选中此框。

手动运行和停止程序

卡巴斯基实验室专家建议您不要停止运行卡巴斯基安全部队 ,因为对您的计算机和个人数据的保护将会面临风险。如果确实需要禁用保护，建议您按所需的时间段暂停计算机保护，而不必关闭该应用程序。

如果已禁用程序自动运行，则应手动启动卡巴斯基安全部队。

手动运行程序，

在开始菜单中，选择**所有程序** ——**卡巴斯基安全部队 2011** ——**卡巴斯基安全部队 2011。**

退出程序，

右键点击任务栏通知区域中的程序图标打开快捷菜单，然后选择**退出。**

在 Microsoft Windows 7 操作系统中，默认情况下程序图标处于隐藏状态，但可以显示该图标以便轻松访问程序功能（请参阅操作系统文档）。

计算机保护状态

本节包含有关如何了解您的计算机当前是否受到保护、其安全是否受到威胁以及如何消除新出现的威胁的信息。在本节中，还可以找到有关在使用卡巴斯基安全部队时启用、禁用和暂停保护的信息。

诊断和排除计算机保护问题

计算机保护出现的问题由位于程序主窗口顶部的计算机保护状态指示器来指示。指示器的颜色根据主机保护状态而改变 绿色表示计算机受到保护 ,黄色指示出现保护相关的问题 ,红色警报计算机安全面临严重威胁。建议您立即修复问题和安全警报。

图 8.当前的计算机保护状态

单击程序主窗口中的指示器图标可打开**保护状态**窗口（请参见下图），其中包含有关计算机保护状态的详细信息，以及检测到的问题和威胁的故障排除建议。

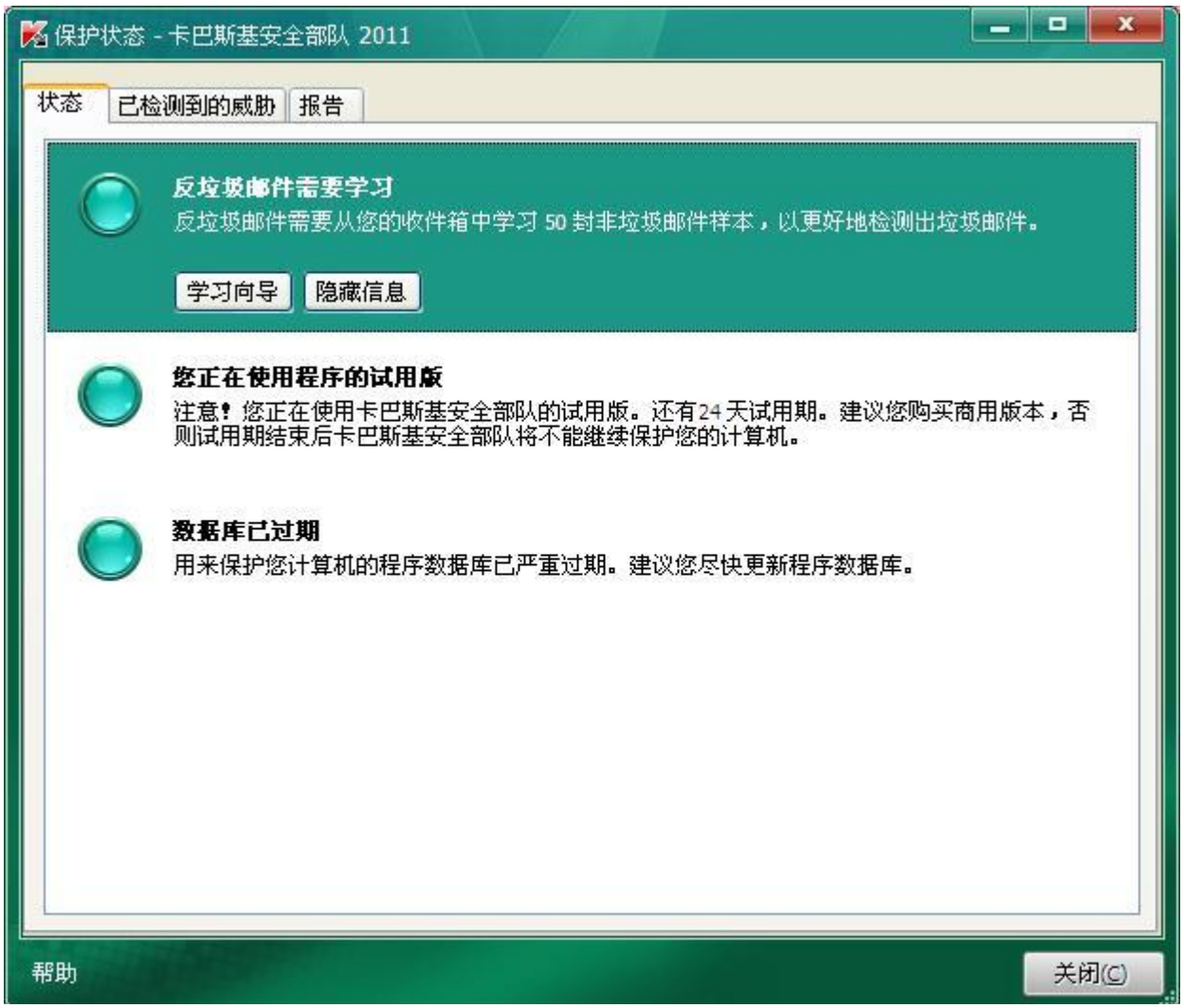

图 9. 解决安全问题

保护状态窗口的**状态**选项卡列出了保护相关的问题，包括由偏离产品正常操作模式（例如，数据库过期）所导致的问题。要处理问题，产品提供以下选项作为额外的步骤：

- 立即消除。单击相应按钮将为您显示适当的问题解决方案。这是建议的操作。
- 推迟消除。如果无论出于何种原因，都不可能立即消除问题，则您可以推迟此操作并稍后返回。为此，请单击**隐藏消息**按钮。

请注意，推迟消除不可用于严重问题。例如，此类问题包括未杀毒的恶意对象，一个或多个组件故障或程序文件损坏。

要在公用列表中显示先前隐藏的通知，请选中**显示隐藏的消息**框（当存在隐藏的消息时，选项卡底部会显示此框）。

您可以使用**检测到的威胁**选项卡查看所揭露的恶意软件和风险程序的列表，并选择将对相关对象执行的操作（例如，移至隔离区）。要选择一项操作，请使用列表上方的控件以及所列记录的快捷菜单。

使用**报告**选项卡，您可以查看程序操作报告（参见 45 页的“如何查看程序操作报告”）。

启用和禁用保护

默认情况下，卡巴斯基安全部队在操作系统加载时启动，并在关闭前保护您的计算机。所有保护组件都会处于运行状态。

您可以全部或部分禁用卡巴斯基安全部队提供的保护。

卡巴斯基实验室专家强烈建议您不要禁用保护，因为这可能导致计算机感染和数据丢失。如果确实需要禁用保护，建议您在指定时间内暂停计算机保护（参见31页的“暂停和恢复保护”）。

禁用保护后，所有组件都将处于未激活状态。

通过下列符号指示：

- 未激活（灰色）在任务栏的通知区域显示应用程序图标（参见 22 页的“通知区域图标”）；
- 主应用程序窗口上方的安全指示标志为红色。

这种情况下，我们讨论的保护都是以保护组件处于运行状态为前提。禁用或暂停保护组件不会影响病毒扫描任务和卡巴斯基安全部队更新的性能。

您可以在程序设置窗口中完全启用或禁用保护（参见 26 页的“程序设置窗口”）。如果想启用或禁用单独的程序组件，可以在设置窗口或程序主窗口中进行（参见 23 页的“卡巴斯基安全部队主窗口”）。

完全启用或禁用保护：

1. 打开程序设置窗口。
2. 在窗口的左侧，选择**实时保护**部分的**常规设置**。
3. 如果需要禁用保护，则取消选中**启用保护**框。如果需要启用保护，选中此框即可。

在设置窗口中启用或禁用保护组件：

1. 打开程序设置窗口。
2. 在窗口左侧的**实时保护**部分中，选择应启用或禁用的组件。
3. 如果需要禁用组件，则在窗口右侧取消选中**启用 <组件名>**框。如果需要启用组件，选中此框即可。

在程序主窗口中启用或禁用保护组件：

1. 打开程序主窗口，并选择**实时保护**部分。
2. 在窗口的左侧，左键点击包含要启用或禁用的组件的部分。
3. 点击带有组件名称的按钮打开操作选择菜单。如果需要启用组件，则选择**启用 <组件名>**，如果需要禁用，则选择**禁用 <组件名>**。

   启用组件后，组件左侧的图标会变绿；禁用组件后，图标则变灰。

暂停和恢复保护

暂停保护表示在某段时间内暂时禁用所有保护组件。

由于暂时禁用保护，因此需要暂停所有保护组件。

下面显示的是程序暂停保护后的状态：

- 不活动（灰色）任务栏通知区域中显示的程序图标（参见 22 页的“通知区域图标”）；
- 程序主窗口上半部分中的安全指示器显示红色。

在本例中，在保护组件的上下文中讨论保护。禁用或暂停保护组件不会影响病毒扫描任务和卡巴斯基安全部队更新的性能。

如果暂停保护的同时建立了网络连接，则会显示一个关于终止此类连接的通知。

当在于 Microsoft Windows Vista 或 Microsoft Windows 7 下运行的计算机上工作时，您可以使用**卡巴斯基工具暂**停保护。为此，应先对**卡巴斯基工具**进行配置以便将打开报告窗口选项分配给其按钮之一（参见 47 页的“如何使用卡巴斯基工具”）。

要暂停对您的计算机的保护，请：

1. 从程序快捷菜单选择**暂停保护**（参见 22 页的“快捷菜单”）；
2. 在暂停保护窗口中，选择其后应恢复保护的时间间隔：
   - **暂停指定时间** – 将在下面的字段中指定的时间间隔后启用保护。
   - **暂停到重新启动** – 将在程序或操作系统重新启动后启用保护（假定配置了程序自动运行（参见 28 页的“启用和禁用自动运行”））。
   - **暂停** – 仅当您决定恢复保护时才启用它（请参阅下文）。

要恢复计算机保护，请

从程序图标**快捷菜单**选择恢复保护（参见 22 页的“快捷菜单”）。

当选择了**暂停**选项或您已选择**暂停指定时间**或暂**停到重新启动**时，您可以采用此方法来恢复计算机保护。

常见问题解答

本节包含大多数用户在使用应用程序时遇到的基本任务的说明。

如何激活程序

*激活*是指激活授权许可的过程，这样在授权许可到期之前，您可以使用应用程序的完整功能版本。

如果在安装过程中未激活应用程序，则可以稍后进行激活。在系统托盘中显示的卡巴斯基安全部队消息将提醒您需要激活应用程序。

若要运行卡巴斯基安全部队激活向导，请执行以下操作之一：

- 在显示于系统托盘处的卡巴斯基安全部队通知窗口上点击**激活**链接。
- 点击程序主窗口底部的**授权许可**链接。在打开的**授权许可管理**窗口中，点击**激活新授权许可**按钮。

让我们更详细地查看一下向导的各个步骤。

步骤 1. 选择授权许可类型并输入激活码

确保在激活向导窗口中已选择**激活商用版本**（参见 21 页的“关于激活码”），在对应字段中输入激活码，然后点击**下一步**按钮。

步骤 2. 请求激活

在步骤 1 中，向导向激活服务器发送请求以获得程序商业版本的激活许可。如果请求发送成功，向导会自动进入**下一步**。

步骤 3. 输入注册数据

户必须进行注册才能与支持服务联系。未注册的用户只能获得最低限度的支持。

指定注册数据，然后点击**下一步**按钮。

步骤 4. 激活

在此步骤中，向导将与激活服务器连接，以便完成应用程序激活和用户注册，之后向导将自动转到下一个窗口。

步骤 5. 关闭向导

此窗口显示有关激活结果的信息：使用的授权许可类型和授权许可到期日期。

点击**完成**按钮关闭向导。

如何购买或续费授权许可

如果在没有授权许可的情况下安装卡巴斯基安全部队，则可以在安装后购买授权许可。当授权许可到期时，可以续订授权许可。购买或续订授权许可时，您将收到用来激活程序的激活码（参见 33 页的“如何激活程序”）。

购买授权许可：

1. 打开程序主窗口。
2. 点击窗口底部的**购买授权许可**按钮。将打开**在线购买**页面，可以通过该网页购买授权许可。

续订授权许可：

1. 打开程序主窗口，并点击窗口底部的**授权许可**链接。

   将打开**授权许可管理**窗口。
2. 点击**续费授权许可**按钮。

   将打开授权许可**续费中心**页面，可以通过该网页续订授权许可。

如何处理程序通知

在任务栏通知区域中出现的程序通知用于通知您在程序操作中发生的事件以引起您的注意。根据事件的重要程度，您可能会收到以下类型的通知：

- 紧急通知 - 通知您对于计算机安全性而言至关重要的事件：例如，在系统中检测到恶意对象或危险活动。如果显示此类通知，应立即确定进一步的操作。此类型的通知窗口显示为红色。
- 重要通知 - 通知您对于计算机安全性而言可能重要的事件：例如，在系统中检测到可能受感染的对象或可疑活动。如果显示此类通知，应确定检测到的对象或进程的危险程度，并选择进一步的操作。此类型的通知窗口显示为黄色。
- 信息通知 - 通知您非关键事件。此类型的通知窗口显示为绿色。

  当屏幕上弹出通知信息时，您应该从建议操作选项中选择一个操作。卡巴斯基专家推荐的操作是默认的最优选项。

如何更新程序数据库

默认情况下，卡巴斯基安全部队会自动检查卡巴斯基实验室更新服务器上的更新。如果服务器包含新的更新，程序便会以后台模式下载并安装这些更新。您可以随时启动卡巴斯基安全部队更新。

若要从卡巴斯基实验室服务器下载更新，应先建立 Internet 连接。

从程序主窗口启动卡巴斯基安全部队更新：

1. 打开程序主窗口，并在窗口左侧选择**免疫更新**部分。
2. 点击窗口右侧的**开始更新**按钮。

   更新信息将显示在程序主窗口的**免疫更新**部分，以及程序快捷菜单中。

如何进行关键区域扫描

关键区域扫描包括扫描操作系统启动时加载的对象、系统内存、磁盘驱动器的引导扇区以及用户添加的对象。

可以使用以下方法之一启动关键区域扫描：

- 使用之前创建的快捷方式；
- 通过程序主窗口（参见 23 页的“卡巴斯基安全部队主窗口”）。

使用快捷方式启动扫描：

1. 打开 Microsoft Windows 资源管理器窗口，转到创建的快捷方式所在的文件夹。
2. 双击快捷方式启动扫描。

   扫描过程中，单击程序主窗口**智能查杀**中的**正在进行关键区域扫描**按钮，在打开的**关键区域扫描**对话框中会显示任务执行进度。此外，在程序快捷菜单中也会显示任务执行进度。

通过应用程序主窗口启动扫描：

1. 打开应用程序主窗口，并在窗口左侧选择**智能查杀**部分。
2. 在应用程序主窗口的右侧，点击**开始关键区域扫描**按钮。

   扫描过程中，单击程序主窗口**智能查杀**中的**正在进行关键区域扫描**按钮，在打开的**关键区域扫描**对话框中会显示任务执行进度。此外，在程序快捷菜单中也会显示任务执行进度。

如何进行对象（文件、文件夹、磁盘驱动器）扫描

可以使用以下方法扫描对象以查找病毒：

- 使用对象的快捷菜单；
- 通过程序主窗口；
- 使用卡巴斯基工具（仅适用于 Microsoft Windows Vista 和 Microsoft Windows 7）。

从对象快捷菜单启动病毒扫描任务：

1. 打开 Microsoft Windows 资源管理器，并转到包含要扫描的对象的文件夹。
2. 点击右键打开对象的快捷菜单（见下图）并选择**智能查杀**。

将在打开的扫描病毒窗口中显示任务的进度和结果。

图 10. Microsoft Windows 中对象的快捷菜单

通过程序主窗口启动对象扫描：

1. 打开程序主窗口，并在窗口左侧选择**智能查杀**部分。
2. 使用以下方法之一指定要扫描的对象：
   - 点击窗口右侧的**选择**链接打开**对象扫描**窗口，并选中需要扫描的文件夹和驱动器旁边的复选框。如果该窗口中未显示要扫描的对象，请点击**添加**链接打开**选择扫描对象**窗口，然后选择要扫描的对象。
   - 将要扫描的对象拖动到主窗口的专用区域（见下图）。

     将在打开的**扫描病毒**窗口中显示任务运行进度。

图 11.应将要扫描的对象拖动到其中的窗口区域

使用卡巴斯基工具扫描对象以查找病毒：

将要扫描的对象拖动到卡巴斯基工具上。

将在打开的**扫描病毒**窗口中显示任务运行进度。

如何进行全盘扫描

可以使用以下方法之一启动全盘扫描以查找病毒：

- 使用之前创建的快捷方式；
- 通过程序主窗口。

使用快捷方式启动全盘扫描：

1. 打开 Microsoft Windows 资源管理器窗口，转到创建的快捷方式所在的文件夹。
2. 双击快捷方式启动扫描。

   扫描过程中，单击程序主窗口**智能查杀**中的**正在进行关键区域扫描**按钮，在打开的**关键区域扫描**对话框中会显示任务执行进度。此外，在程序快捷菜单中也会显示任务执行进度。

通过程序主窗口启动全盘扫描：

1. 打开程序主窗口，并在窗口左侧选择**智能查杀**部分。
2. 点击窗口右侧的**开始全盘扫描**按钮。

   扫描过程中，单击程序主窗口**智能查杀**中的**正在进行关键区域扫描**按钮，在打开的**关键区域扫描**对话框中会显示任务执行进度。此外，在程序快捷菜单中也会显示任务执行进度。

扫描计算机漏洞

*漏洞*是指在不受保护的应用程序中，可能被入侵者为达到其目的（例如，复制数据）而蓄意利用的不受保护的软件代码部分。扫描计算机以查找漏洞可帮助您发现计算机中的任何此类弱点。建议您消除检测到的漏洞。

可以使用以下方法扫描系统以查找漏洞：

- 通过程序主窗口；
- 使用之前创建的快捷方式。

使用快捷方式启动任务：

1. 打开 Microsoft Windows 资源管理器窗口，转到创建的快捷方式所在的文件夹。
2. 双击快捷方式以启动扫描系统以查找漏洞的任务。

   在程序主窗口中将显示任务进度。

从应用程序窗口启动任务：

1. 打开程序主窗口，并在窗口左侧选择**系统优化**部分。
2. 点击窗口右侧的**漏洞扫描**按钮。
3. 在显示的**漏洞扫描**窗口中，点击窗口顶部的**开始漏洞扫描**按钮。

   在**完成时间字段**中将显示任务进度。若要停止任务，请点击窗口顶部的**正在进行漏洞扫描**按钮。

如何防止个人数据被盗

使用卡巴斯基安全部队，可以防止个人数据被盗；个人数据包括以下各项：

- 密码、用户名和其他注册数据；
- 账号和银行卡号。

卡巴斯基安全部队包含可用于防止黑客使用钓鱼和拦截键盘输入数据等方法试图盗窃个人数据的组件和工具。

在网页反病毒、反垃圾邮件和即时通讯反病毒组件中实现的反钓鱼功能可确保防御钓鱼。

使用*安全键盘*可确保防止在键盘上输入的数据遭到拦截。

防御钓鱼

*钓鱼*是一种在线欺骗行为，它通过欺骗的方式诱使用户暴露信用卡号、PIN 码和其他个人详细信息以达到盗窃钱财的目的。

钓鱼通常以网上银行用户为目标。不法分子创建所选银行网站的精确副本，并以此银行的名义向客户发送电子邮件。他们声称因网上银行系统软件故障或更换导致用户详细信息丢失，需要用户在银行网站上确认或修改此类详细信息。用户点击可将他们转到假冒网站的链接，输入其详细信息，这些信息最终会落入不法分子手中。

在网页反病毒、反垃圾邮件和即时通讯反病毒组件中实现的反钓鱼功能可确保防御钓鱼。启用这些组件可确保全面防御钓鱼。

安全键盘

当在您的计算机上工作时，在输入您的个人数据时经常会出现一些情况，或者需要用户名和密码。例如，在网站上进行账户注册、网上购物或使用网上银行期间会发生这种情况。

系统存在使用硬件键盘侦听器或按键记录器（记录击键的程序）拦截个人信息的风险。

安全键盘工具防止了拦截通过键盘输入的数据。

如果需要输入此类数据的网站受到黑客攻击，则安全键盘无法保护您的个人数据，因为在这种情况下，入侵者会直接获得信息。

许多被分类为间谍软件的应用程序具有屏幕截图的功能，然后将屏幕截图传送给入侵者进行进一步分析以及窃取用户的个人数据。安全键盘防止了通过使用屏幕截图拦截输入的个人数据。

安全键盘只能在使用 Microsoft Internet Explorer 和 Mozilla Firefox 浏览器时防止拦截隐私数据

在您开始使用安全键盘之前，请了解其特性：

- 在从安全键盘输入数据之前，请确保使用鼠标指针选择了相应输入字段。
- 您可以使用鼠标按安全键盘按钮。
- 与实际键盘不同的是，在安全键盘上无法同时按两个键。因此，要使用键组合（例如，**ALT+F4**），您必须先按第一个键（例如，**ALT**），再按下一个键（例如，**F4**），然后再按第一个键。第二次按键的行为类似于实际键盘上的键释放。
- 安全键盘的输入语言根据指定设置使用 **CTRL+SHIFT** 键组合（**SHIFT** 键应使用鼠标右键来按）或 **CTRL+LEFT ALT**（**LEFT ALT** 键应使用鼠标右键来按）来切换。

您可以通过以下方式打开安全键盘：

- 从程序快捷菜单；
- 从程序主窗口；
- 从 Microsoft Internet Explorer 或 Mozilla Firefox 的窗口；
- 使用键盘快捷方式。

要从程序图标的快捷菜单打开安全键盘，请

从程序图标的快捷菜单选择**工具→安全键盘**。

要从程序主窗口打开安全键盘，请：

1. 打开程序主窗口，并在窗口左半部分中选择**安全运行**部分。
2. 在窗口右半部分中选择**安全键盘**部分。

要从浏览器窗口打开安全键盘，请

单击 Microsoft Internet Explorer 或 Mozilla Firefox 工具栏中的  **安全键盘**按钮。

要使用计算机键盘打开安全键盘，请

按 **CTRL+ALT+SHIFT+P** 快捷键。

如果怀疑某个对象感染病毒该怎么做

如果怀疑某个对象感染了病毒，首先应使用卡巴斯基安全部队扫描该对象（参见 35 页的“如何进行对象（文件、文件夹、磁盘驱动器）”扫描）。

如果在扫描之后应用程序报告该对象未受感染，但您认为该对象受到了感染，则可以执行以下操作：

- 将该对象移至*隔离区*。隔离的对象存储在压缩文件中，因此它们不会对计算机造成威胁。在更新数据库之后，卡巴斯基安全部队可能能够清晰地识别威胁并将其消除。
- 将该对象发送到*病毒实验室*。病毒实验室专家将扫描该对象。如果发现它感染了病毒，则他们会立即将新病毒的描述添加到数据库中，应用程序将通过更新来下载数据库（参见 34 页的“如何更新程序数据库”）。

可以使用以下两种方法之一将对象移至隔离区：

- 使用**保护状态**窗口中的**移至隔离区**链接；
- 使用对象的快捷菜单。

通过保护状态窗口将对象移至隔离区：

1. 打开程序主窗口。
2. 点击窗口顶部的**隔离区**链接，打开**保护状态**窗口中的**已检测到的威胁**选项卡
3. 点击威胁列表上方的**移至隔离区**链接。
4. 在打开的窗口中，选择要移至隔离区的对象。

使用快捷菜单将对象移至隔离区：

1. 使用快捷菜单将对象移至隔离区：
2. 点击右键打开对象的快捷菜单，然后选择**移至隔离区**。

将对象发送到反病毒实验室：

请将病毒样本压缩,并用“infected”作压缩口令发送到 Kaspersky Labs 病毒上报邮箱：viruslab@kaspersky.com.cn

如何处理大量垃圾邮件

如果收到大量未经请求的邮件（垃圾邮件），请启用反垃圾邮件组件并设置推荐的安全级别。然后使用学习向导进行组件学习。正确的垃圾邮件识别要求至少使用 50 封正常邮件示例和 50 封垃圾邮件示例来进行学习。

启用反垃圾邮件并设置推荐的安全级别：

1. 打开程序设置界面。
2. 在窗口左侧的**实时保护**部分中，选择**反垃圾邮件**组件。
3. 选中窗口右侧的**启用反垃圾邮件**复选框。
4. 在**安全级别**部分中，默认情况下，安全级别应设置为**推荐**。

如果安全级别设置为**低**或**自定义**，请点击**默认级别**按钮。安全级别将设置为**推荐**。

使用学习向导进行反垃圾邮件学习：

1. 打开程序设置窗口。
2. 在窗口左侧的**实时保护**部分中，选择**反垃圾邮件组件**。
3. 点击窗口右侧**反垃圾邮件学习**部分中的**学习**按钮。

   将打开学习向导窗口。

向导步骤的详细描述。

步骤 1. 启动向导

点击**下一步**按钮开始学习。

步骤 2. 选择包含正常邮件的文件夹

在此阶段，可以指定包含正常邮件的文件夹。应仅选择您绝对确信包含正常电子邮件的文件夹。

仅可访问 Microsoft Office Outlook 和 Microsoft Outlook Express (Windows Mail) 账户。

步骤 3. 选择包含垃圾邮件的文件夹

在此阶段，可以指定包含未经请求的邮件（垃圾邮件）的文件夹。如果在电子邮件客户端应用程序中没有此类文件夹，请跳过此步骤。

仅可访问 Microsoft Office Outlook 和 Microsoft Outlook Express (Windows Mail) 账户。

步骤 4. 反垃圾邮件学习

在此阶段，使用在前面的步骤中选择的文件夹对反垃圾邮件组件进行学习。这些文件夹中的电子邮件将填充反垃圾邮件数据库。正常邮件的发件人将自动添加到允许发件人列表中。

步骤 5. 保存学习结果

在向导的此阶段，必须使用以下方法之一保存学习结果：

- 将学习结果添加到现有的反垃圾邮件数据库（选择**添加此次学习结果到已有的反垃圾邮件数据库**）；
- 将当前数据库替换为仅包含学习结果的数据库（选择**创建新的反垃圾邮件数据库**）。

点击**完成**按钮关闭向导。

如果怀疑计算机感染病毒该怎么做

如果您怀疑计算机感染病毒，则使用“系统恢复向导”消除系统中恶意活动的后果。卡巴斯基实验室建议您在对计算机进行了杀毒后运行该向导，以确保修复病毒感染导致的所有威胁和损害。

该向导会检查是否对系统进行了任何更改，如：对网络的访问受阻，已知格式文件扩展名被更改，工具栏受阻等。此类损害可能有各种原因。后者可能包括恶意程序的活动、系统配置错误、系统故障，或者甚至是系统优化应用程序的操作错误。

在查看完之后，向导会分析信息以评估系统损害是否需要立即注意。基于查看，系统会生成消除问题所需的操作列表。向导会基于检测到的问题的严重性按类别对这些操作进行分组。

此向导由一系列屏幕（步骤）组成，可使用**上一步**和**下一步**按钮进行导航。要在向导完成工作后关闭向导，请使用**完成**按钮。要在任意阶段停止向导，请使用**取消**按钮。

要启动系统恢复向导，请：

1. 打开程序主窗口，并在窗口左半部分中选择**系统优化**部分。
2. 在窗口的右半部分中，单击**恢复系统**按钮。

向导步骤的详细说明。

步骤 1. 启动系统还原

确保选择了**搜索恶意软件活动导致的问题**按钮，然后单击**下一步**按钮。

步骤 2. 问题搜索

向导将搜索应修复的问题和损害。完成搜索后，向导将自动执行下一步。

步骤 3. 选择故障排除操作

上一步期间发现的所有损害均基于其造成的危险类型进行分组。对于每组损害，卡巴斯基实验室推荐了一系列修复损害的操作。存在三组操作：

- *强烈建议的操作*会避免造成严重安全威胁的问题。建议您执行本组中的所有操作。

- *建议的操作*会避免带来潜在威胁的问题。建议您也执行本组中的所有操作。
- *其他操作*会修复目前不会造成威胁但将来可能会对计算机安全造成危险的系统损坏。

若要查看组中的操作，请单击组名称左侧的 + 图标。

若要使向导执行某项操作，请选中相应操作名称左侧的框。默认情况下，向导会执行所有建议的操作和所有强烈建议的操作。如果您不希望执行某项操作，请取消选中它旁边的框。

强烈建议您不要取消选中默认选中的框，因为这样容易使计算机遭受攻击。

在定义向导将执行的一组操作后，单击**下一步**按钮。

步骤 4. 消除问题

向导将会执行在上一步中选择的操作。消除问题可能需要一些时间。完成故障排除后，向导将自动执行下一步。

步骤 5. 关闭向导

单击**完成**按钮关闭向导。

如何恢复被应用程序删除或清除的对象

卡巴斯基实验室建议您避免恢复被删除和清除的对象，因为它们可能会对计算机造成威胁。

如果要恢复被删除或清除的对象，可以使用程序在扫描该对象时创建的备份副本。

恢复已被应用程序删除或清除的对象：

1. 打开程序主窗口。
2. 点击窗口顶部的**隔离区**链接，打开**保护状态**窗口中的**已检测到的威胁**选项卡。
3. 点击威胁列表上方的**已清除威胁的对象**链接，选择要显示的已清除威胁的对象。将在**已检测到的威胁**选项卡上显示已清除和删除的对象列表。对象按其状态进行分组。若要显示某个组中对象的列表，请点击组标题左侧的 + 图标。
4. 点击右键打开要恢复的对象的快捷菜单，然后选择**恢复**。

如何创建和使用应急磁盘

建议您在安装和配置卡巴斯基安全部队，扫描计算机并确保计算机未被感染后创建应急磁盘。之后，将能够使用应急磁盘执行扫描，并对使用其他方法（例如，使用反病毒应用程序）无法杀毒的受感染计算机进行杀毒。

创建应急磁盘

创建应急磁盘意味着创建具有最新的反病毒数据库和配置文件的磁盘镜像（ISO 文件）。

可以从卡巴斯基实验室服务器下载充当新文件创建基础的源磁盘镜像，也可以从本地源进行复制。

可以使用应急磁盘创建向导创建应急磁盘。该向导创建的 rescuecd.iso 文件将保存在计算机的硬盘驱动器上：

- 在 Microsoft Windows XP 中 – 保存在以下文件夹中：Documents and Settings\All Users\Application Data\Kaspersky Lab\AVP11\Data\Rdisk\；
- 在 Microsoft Windows Vista 和 Microsoft Windows 7 中 – 保存在以下文件夹中：ProgramData\Kaspersky Lab\AVP11\Data\Rdisk\。

此向导由一系列屏幕（步骤）组成，可使用**上一步**和**下一步**按钮进行导航。要在向导完成工作后关闭向导，请使用**完成**按钮。要在任意阶段停止向导，请使用**取消**按钮。

启动应急磁盘创建向导：

1. 打开程序主窗口，并在窗口左侧选择**系统优化**部分。
2. 点击窗口右侧的**创建应急磁盘**按钮。

向导步骤的详细说明。

步骤 1. 搜索现有的磁盘镜像

如果向导已找到以前在专用文件夹（见上文）中创建的应急磁盘镜像文件，则可以选中**使用现有的 ISO 镜像**复选框将此文件用作原始磁盘镜像，并继续执行**更新镜像文件**步骤（见下文）。如果不希望使用已找到的磁盘镜像，请取消选中此复选框。向导将转到**选择 ISO 镜像源**窗口。

如果向导找不到任何 ISO 文件，则将跳过此步骤，向导将转到**选择 ISO 镜像源**窗口。

步骤 2. 选择 ISO 镜像源

如果在向导的第一个窗口中选中**使用现有的 ISO 镜像**复选框，则将跳过此步骤。

在此步骤中，应从选项列表中选择镜像文件源：

- 如果已具有应急磁盘或为其准备的镜像并存储在您的计算机上或本地网络资源上，请选择**从本地网络或光盘拷贝 ISO 镜像**。
- 如果没有镜像文件，且希望从卡巴斯基实验室服务器下载镜像文件（文件大小约为 100 MB），请选择**从卡巴斯基实验室服务器下载 ISO 镜像**。

步骤 3. 复制（下载）磁盘镜像

如果在向导的第一个窗口中选中**使用现有的 ISO 镜像复选框**，则将跳过此步骤。

如果在上一步（**从本地网络或光盘拷贝 ISO 镜像**）中选择了从本地源复制镜像的选项，则应在此当前步骤中指定 ISO 文件的路径。为此，请点击**浏览**按钮。在指定文件的路径后，点击**下一步**按钮。在向导窗口中将显示磁盘镜像复制的进度。

如果选择了**从卡巴斯基实验室服务器下载 ISO 镜像**，则会立即显示磁盘镜像下载的进度。

完成 ISO 镜像的复制或下载后，向导将自动继续执行下一步骤。

步骤 4. 更新镜像文件

文件更新过程包括：

- 更新反病毒数据库；
- 更新配置文件。

配置文件确定从使用向导提供的应急磁盘镜像刻录的可移动磁盘或 CD/DVD 启动计算机的可能性。

更新反病毒数据库时，使用在最后一次更新卡巴斯基安全部队时分发的数据库。如果数据库已过期，建议进行更新并重新启动应急磁盘创建向导。

若要开始更新 ISO 文件，请点击**下一步**按钮。在向导窗口中将显示更新的进度。

步骤 5. 在数据媒体上刻录镜像

在此窗口中，向导通知您已成功创建应急磁盘，并提示您在数据媒体上刻录镜像。

指定用于刻录 ISO 镜像的数据媒体：

- 选择**刻录到 CD/DVD** 可在 CD/DVD 上刻录镜像。

  系统将提示您指定要在其上刻录镜像的 CD/DVD。之后，将在此 CD/DVD 上刻录 ISO 镜像。刻录过程可能需要花费一些时间，请耐心等待刻录完成。

- 选择**刻录到 USB 设备**选项可在可移动驱动器上刻录镜像。

卡巴斯基实验室建议您不要在不是专门设计用于数据存储的设备(如智能电话、移动电话、PDA 和 MP3 播放器) 上刻录 ISO 镜像。在这些设备上刻录 ISO 镜像可能会导致设备将来无法正常工作。

  系统将提示您指定要在其上刻录镜像的可移动驱动器。之后，将在此可移动驱动器上刻录镜像。刻录过程可能需要花费一些时间，请耐心等待刻录完成。

- 选择不刻录选项可取消刻录在数据媒体上创建的镜像。在这种情况下，将打开包含已创建的磁盘镜像文件的文件夹。

步骤 6. 关闭向导

若要完成向导，请点击完成按钮。可以使用所创建的磁盘在将来加载计算机 (参见 44 页)。

从应急磁盘启动计算机

如果操作系统因病毒攻击而无法启动，请使用应急磁盘。

若要引导操作系统，应使用在其上刻录了应急磁盘镜像 (.iso) 文件的 CD/DVD 或可移动驱动器。

并非在所有情况下都可执行从可移动驱动器加载计算机的操作。特别是，某些过时的计算机型号不支持此模式。在关闭计算机以便进一步从可移动驱动器引导之前，请确保可以执行此操作。

从应急磁盘引导计算机：

1. 在 BIOS 设置中，启用从 CD/DVD 或可移动驱动器启动 (有关详细信息，请参阅计算机主板的文档)。

2. 将包含应急磁盘镜像的 CD/DVD 插入到受感染计算机的 CD/DVD 驱动器中，或者将可移动驱动器与计算机相连。
3. 重新启动计算机。

   有关使用应急磁盘的详细信息，请参阅卡巴斯基应急磁盘用户指南。

如何查看程序操作报告

卡巴斯基安全部队会为每个组件创建操作报告。例如，使用报告可以查看在指定的时间段内应用程序已检测并消除多少恶意对象（如病毒和木马程序）、在同一时间段内更新应用程序多少次、检测到多少垃圾邮件以及许多其他特征。

在运行 Microsoft Windows Vista 或 Microsoft Windows 7 的计算机上工作时，可以使用卡巴斯基工具来打开报告。为此，应对卡巴斯基工具进行配置，以便将打开报告窗口的选项分配给其按钮之一（参见 47 页的“如何使用卡巴斯基工具”）。

查看应用程序操作报告：

1. 使用以下方法之一，打开**保护状**态窗口的**报告**选项卡：
   - 点击程序主窗口顶部的**报告**链接；
   - 点击**卡巴斯基工具**界面中带有 **报告**图标的按钮（仅适用于 Microsoft Windows Vista 和 Microsoft Windows 7）。

     报告选项卡将以图表格式显示应用程序操作报告。
2. 如果要查看详细的程序操作报告（例如，显示每个组件的操作的报告），请点击**报告**选项卡底部的**详细报告**按钮。
3. 将打开**详细报告**窗口，在该窗口中，数据以表格的形式显示。为了便于查看报告，可以选择不同的条目排序选项。

如何恢复程序默认设置

您始终可以恢复卡巴斯基实验室推荐并视为最优的卡巴斯基安全部队设置。这些设置可以使用*卡巴斯基安全部队配置向导*进行恢复。

向导完成操作后，将为所有保护组件设置**推荐**的安全级别。恢复设置时，您还可以在恢复推荐的安全级别的同时定义为组件保留（或不保留）的设置。

恢复保护设置：

1. 打开程序设置窗口。
2. 使用下列方法之一运行应用程序配置向导：
   - 点击窗口底部的**恢复**链接
   - 在窗口的左侧，选择**高级设置**部分和**设置管理**子部分，然后点击**恢复默认设置**中的**恢复**按钮。

向导步骤的详细描述。

步骤 1. 启动向导

点击**下一步**按钮继续向导操作。

步骤 2. 选择要保存的设置

向导的这一窗口可以显示哪些卡巴斯基安全部队组件的设置与默认值不同，原因可能是用户更改了这些值，也可能是卡巴斯基安全部队的累计学习（防火墙或反垃圾邮件）更改了这些值。如果为任何组件创建了特殊设置，那么这些设置也会显示在此窗口中。

特殊设置包括反垃圾邮件使用的允许和阻止的词组和地址列表、可信网址和 ISP 电话号码列表、为应用程序组件创建的排除规则、防火墙的数据包和应用程序过滤规则。

在使用卡巴斯基安全部队执行个别任务以及满足安全需求时，会创建这些列表。创建这些列表可能需要很长时间，因此建议您在恢复应用程序默认设置之前保存它们。

选中希望保存的设置对应的复选框，然后点击**下一步**按钮。

步骤 3. 分析系统

此阶段将收集有关 Microsoft Windows 应用程序的信息。这些应用程序将会添加到信任程序列表，并且不会对这类应用程序在系统中执行的操作进行限制。

完成分析后，向导将自动执行下一步。

步骤 4. 完成恢复

请点击**完成**按钮结束向导。

将卡巴斯基安全部队设置应用到其他计算机

完成产品配置后，您可以在安装于其他计算机上的卡巴斯基安全部队中应用相关设置。这样，两台计算机中的应用程序配置将完全一样。例如，在家庭计算机和办公室计算机中均安装了卡巴斯基安全部队时，这项功能会非常有用。

程序设置会存储在一个特殊的配置文件中，您可以将该文件转移到其他计算机。为此，您需要：

1. 执行*导出*过程 – 将程序设置保存到配置文件。
2. 将保存的文件移至另一台计算机（例如，通过电子邮件发送或者使用可移动数据媒体）。
3. 执行*导入*过程 — 将设置从配置文件应用到安装在其他计算机上的卡巴斯基安全部队。

导出卡巴斯基安全部队的当前设置：

1. 打开程序设置窗口。
2. 选择窗口左侧的**设置管理**部分。
3. 在恢复默认设置部分中，点击**保存**按钮。
4. 在打开的窗口中，输入配置文件名和文件的保存路径。

从保存的配置文件中导入程序设置：

1. 打开程序设置窗口。
2. 选择窗口左侧的**设置管理**部分。
3. 在**加载设置**部分中，点击**加载**按钮。
4. 在打开的窗口中，选择要从中导入卡巴斯基安全部队设置的文件。

如何使用卡巴斯基工具

当在微软 Vista 操作系统或 Win7 操作系统中运行卡巴斯基反病毒软件时，您可以使用卡巴斯基工具。

在微软 Win7 操作系统中，安装卡巴斯基反病毒软件后，会自动在桌面上显示卡巴斯基工具。在微软 Vista 操作系统中，安装卡巴斯基反病毒软件后，你需要手动将该工具添加至 Windows 边栏（详见操作系统文档）。

该小工具的颜色指示着电脑的保护状态，原理和主窗口的保护状态指示一样（参见 23 页的“卡巴斯基安全部队主窗口”）。绿色代表电脑已被保护，黄色代表有一些保护问题，而红色则表示处于高风险状况。灰色说明程序已停止保护。

小工具的外观可以监控更新下载：当正在更新数据库和程序模块时，一个旋转的球形图标会显示在小工具的中间位置。

您可以利用小工具来执行以下任务：

- 重新运行已暂停的程序；
- 打开程序主窗口；
- 为特定对象扫描病毒；
- 打开新闻窗口。

重新运行已暂停的程序，请

点击小工具中间的启用图标。

打开程序主窗口，请

点击小工具中间的卡巴斯基标志。

为特定对象扫描病毒，请

将所需对象拖至小工具上。

在随之打开的病毒扫描窗口会显示任务运行进程。

在有新闻发布时打开新闻窗口，请

点击小工具中间的 图标。

配置小工具

您可以配置小工具，就可以利用它的按钮来完成以下操作：

- 编辑程序设置；
- 查看程序报告；
- 使程序运行在安全模式下；
- 切换至安全桌面（仅适用于 32 位操作系统）；
- 查看上网管理报告；
- 查看网络活动信息（网络监控）；
- 暂停保护。

另外，您可以为小工具挑选其它皮肤来更改其外观。

配置小工具：

1. 如果用鼠标划过小工具，就会在该区域右上角显示图标，点击图标打开小工具设置窗口。
2. 从**左侧图标**和**右侧图标**的下拉菜单中选择所需操作。
3. 点击 按键来选择一个皮肤。
4. 点击**确定**来保存更改。

联系技术支持服务

如果在卡巴斯基安全部队操作期间出现问题，请首先检查在文档、帮助、卡巴斯基实验室技术支持网站上的知识库或用户论坛中是否介绍了这些问题的解决方法。

如果找不到问题的解决方法，请通过以下方式之一与卡巴斯基实验室技术支持服务联系：

- 发送电子邮件：support@kaspersky.com.cn；
- 拨打电话：400-611-6633

技术支持服务专家将解答您提出的有关安装、激活和使用应用程序的任何问题。如果计算机已被感染，他们将帮助您消除恶意软件活动产生的影响。

在与技术支持服务联系之前，请阅读技术支持规则 (http://www.kaspersky.com.cn/KL-Services/techsupport.htm)。

在与技术支持服务联系时，服务专家可能会要求您编制系统状态报告和追踪文件，并将它们发送到技术支持服务。技术支持服务专家分析您发送的数据后，他们可以创建 AVZ 脚本以帮助您解决问题。

我的卡巴斯基账号

我的卡巴斯基账号 – 您在技术支持服务网站上的个人空间。使用我的卡巴斯基账号，可以执行以下操作：

- 与技术支持服务和病毒实验室联系；
- 在不使用电子邮件的情况下与技术支持服务联系；
- 实时跟踪请求状态；
- 查看您向技术支持服务发出的请求的详细历史记录。

若要登录我的卡巴斯基账号，请使用以下选项之一：

- 点击卡巴斯基安全部队主窗口中的**我的卡巴斯基账号**链接；
- 在浏览器的地址栏中，键入 https://my.kaspersky.com/cn/。

如果还没有账号，可以在我的卡巴斯基账号注册页上进行注册。输入电子邮件地址和密码登录我的卡巴斯基账号。若要发送有关卡巴斯基安全部队使用情况的请求，系统将要求您输入激活码。

请注意，一些请求不应发往技术支持服务，而应发往卡巴斯基病毒实验室。它们是以下类型的请求：

- 未知恶意程序 – 您怀疑某个对象是恶意程序，但卡巴斯基安全部队尚未将其归类为恶意程序；
- 未知恶意程序 – 您怀疑某个对象是恶意程序，但卡巴斯基安全部队尚未将其归类为恶意程序；
- 恶意程序描述 – 您希望获取对指定病毒的描述。

向病毒实验室发送请求无需输入激活码。

您无需是我的卡巴斯基账号的注册用户，即可从包含请求表单的页面向卡巴斯基病毒实验室发送请求。

通过电话寻求技术支持

如果遇到问题，需要提供紧急帮助，可以致电最近的技术支持办事处。

创建系统状态报告

在为您解决问题的过程中，卡巴斯基实验室技术支持服务专家可能需要您提供有关系统状态的报告。该报告需要包含运行中的进程、已加载模块和驱动程序、Microsoft Internet Explorer 和 Microsoft Windows Explorer 插件、开放端口以及检测到的可疑对象等详细信息。

创建系统状态报告时，不会收集任何个人用户信息。

创建系统状态报告：

1. 打开程序主窗口。
2. 点击窗口底部的**技术支持**链接打开**支持**窗口，然后点击**支持工具**链接。
3. 在打开的**技术支持服务信息**窗口中，点击**创建系统状态报告**按钮。

系统状态报告以 HTML 和 XML 格式创建，并保存在 sysinfo.zip 压缩文件中。信息收集过程完成后，您可以查看报告。

查看报告：

1. 打开程序主窗口。
2. 点击窗口底部的**技术支持**链接打开**支持**窗口，然后点击**支持工具**链接。
3. 在打开的**技术支持服务信息**窗口中，点击**查看**按钮。
4. 这时会打开包含报告文件的 sysinfo.zip 压缩文件。

创建追踪文件

安装卡巴斯基安全部队之后，操作系统或个别应用程序的操作可能会出现某些故障。最可能的原因是卡巴斯基安全部队与计算机上安装的软件或计算机组件的驱动程序之间存在冲突。这种情况下，系统会提示您创建追踪文件，以便卡巴斯基实验室技术支持服务专家成功解决问题。

创建追踪文件：

1. 打开程序主窗口。
2. 点击窗口底部的**技术支持**链接打开**支持**窗口，然后点击**支持工具**链接。
3. 在打开的**技术支持服务信息**窗口中，从**追踪**部分的下拉列表中选择追踪等级。

建议使用技术支持服务专家告知的所需追踪等级。如果技术支持服务未提供任何指示，建议您将追踪等级设置为 **500**。

1. 要启动追踪进程，请点击**启用**按钮。
2. 重现出现问题时的情形。

3. 要停止追踪进程，请点击**禁用**按钮。

您可以切换到上传追踪结果（参见 51 页的“发送数据文件”）到卡巴斯基实验室的服务器。

发送数据文件

创建追踪文件和系统状态报告之后，您必须将其发送给卡巴斯基实验室的技术支持服务专家。

需要一个需求编号才能将数据文件上传到技术支持服务服务器。如果您的需求有效，便会在技术支持服务网站上的个人账号中提供该编号

将数据文件上传到技术支持服务服务器：

1. 打开程序主窗口。
2. 点击窗口底部的**技术支持**链接打开**支持**窗口，然后点击**支持工具**链接。
3. 在打开的**技术支持服务信息**窗口中，找到操作部分，然后点击**将技术支持服务信息上传到服务器**按钮。

   这时会打开将技术支持服务信息上传到服务器窗口。
4. 选中要发送到技术支持服务的追踪文件旁边的框，并点击**发送**按钮。这时会打开**需求编号**窗口。
5. 指定联系技术支持服务之后通过个人账号分配给您的需求编号，并点击**确定**按钮。

所选数据文件会进行打包并送到技术支持服务服务器。

如果因任何原因无法联系技术支持服务，可以将数据文件存储到您的计算机上，稍后以个人账号发送。

将数据文件保存到磁盘：

1. 打开程序主窗口。
2. 点击窗口底部的**技术支持**链接打开**支持**窗口，然后点击**支持工具**链接。
3. 在打开的**技术支持服务信息**窗口中，找到操作部分，然后点击**将技术支持服务信息上传到服务器**按钮。

   这时会打开将技术支持服务信息上传到服务器窗口。
4. 选中要发送到技术支持服务的追踪文件旁边的框，并点击**发送**按钮。

   这时会打开需求编号输入窗口。
5. 点击**取消**按钮，并在打开的窗口中点击**是**按钮，确认将文件保存到磁盘。

   将打开压缩文件保存窗口。
6. 指定压缩文件名并确认保存。

   这时创建的压缩文件会从个人账号发送到技术支持服务。

执行 AVZ 脚本

卡巴斯基实验室专家会使用追踪文件和系统状态报告分析计算机安全问题。通过分析，将给出一系列旨在消除检测到的问题的操作。此类操作列表可能很长。

为了简化这一过程，将使用 AVZ 脚本。AVZ 脚本是一个指令集，可用于编辑注册表项、文件隔离、搜索文件类以及与这些文件类相关的潜在隔离文件，阻止 UserMode 和 KernelMode 拦截机等。

要运行脚本，应用程序中应包含 *AVZ 脚本执行向导*。

此向导由一系列屏幕（步骤）组成，可使用**上一步**和**下一步**按钮进行导航。要在向导完成工作后关闭向导，请使用**完成**按钮。要在任意阶段停止向导，请使用**取消**按钮。

建议您不要更改卡巴斯基实验室专家提供的 AVZ 脚本的文本。如果在脚本执行期间出现问题，请联系技术支持服务。

启动向导：

1. 打开程序主窗口。
2. 点击窗口底部的**技术支持**链接打开**支持**窗口，然后点击**支持工具**链接。
3. 在打开的**技术支持服务信息**窗口中，点击**执行 AVZ 脚本**按钮。

   如果脚本成功执行，向导便会关闭。如果在脚本执行过程中出错，向导会显示相应的错误消息。

卡巴斯基实验室

有的公司擅于宣传，而有的公司擅长创造一流的产品。无论在哪个行业，只有那些全面专注并始终致力于一件事情的公司才能获得成功。对于卡巴斯基实验室 而言，我们关注的事情就是与一切恶意软件和程序的长期抗争。12 年以来，我们一直致力于发现、分析和清除 IT 威胁。多年来，我们已积累了关于恶意软件和如何处理这一问题的大量经验和知识。

今日的卡巴斯基实验室

卡巴斯基实验室是一家拥有 1700 多名高级专家的国际集团，总部位于莫斯科，在全球五大洲都设立了代表机构，包括西欧、东欧、中东和非洲、美洲、亚太和日本。这些机构与当地的合作伙伴开展着重要的交流。目前，公司的业务遍布全球 100 多个国家，为超过 3 亿的用户提供安全保护。

集团的主要决策机构是董事会，负责制定总体发展战略和任命高级管理人员。董事会由 9 名股东和来自集团总部及全球各地区的高级管理人员代表组成。

独特的经验和知识

2009 年，卡巴斯基实验室迎来 12 周岁的生日，而以尤金·卡巴斯基为首的专家团在研发反病毒软件的领域中耕耘的时间却是公司成立时间的两倍。毫无疑问，公司最宝贵的财富是丰富的经验和知识，多年以来，卡巴斯基实验室一直走在对抗病毒和其它的 IT 威胁的最前沿，这不仅使我们能够预测恶意软件的发展态势，也帮助我们在市场竞争中，一直保持领先一步的优势。我们的使命就是为用户提供最可靠的保护，阻挡新类型的攻击。

卡巴斯基反病毒技术

由于高度的专业精神和奉献精神，卡巴斯基实验室已经成为市场领先的信息安全解决方案提供商。公司的主要产品——卡巴斯基反病毒软件，多次在国际知名研究中心和 IT 出版物主导的测试中脱颖而出，获得最高奖项。卡巴斯基实验室是第一个开发出诸多反病毒行业技术标准的公司，这些标准包括针对 Linux、Unix 和 NetWare 的全面解决方案、用于检测新出现病毒的新一代启发式分析程序、防止多态性病毒和宏病毒的有效保护技术、持续更新反病毒数据库技术，以及检测档案文件病毒技术。

完善的信息安全解决方案

卡巴斯基实验室为每一位用户提供有效对抗病毒、垃圾邮件以及黑客攻击的安全解决方案。随着恶意软件程序变得日益复杂，功能也日趋增多，公司提供全方位的系列产品，保护个人计算机用户和企业网络免受这些问题的困扰。

1999 年，卡巴斯基实验室就首次运行 Linux/FreeBSD 操作系统的工作站、文件服务器及应用程序服务器推出集成式反病毒软件。如今，针对最受欢迎的 Linux/FreeBSD 系统， 公司提供一整套有效的 IT 安全解决方案，同时为服务器和客户端应用程序提供保护。

卡巴斯基实验室还为各种规模的企业提供全新的 IT 安全 外包服务。卡巴斯基主机邮件安全解决方案（Kaspersky Hosted Email Security）确保各种可能携带病毒、垃圾信息、黑客攻击以及网络钓鱼的邮件在到达公司服务器之前就被清除。卡巴斯基主机网络安全解决方案 （Kaspersky Hosted Web Security）保护公司网络免受通过互联网网关渗入的各种 IT 威胁。卡巴斯基主机 IM 安全解决方案（Kaspersky Hosted IM Security）主要为即时信息（IM）系统提供保护，还可以对员工使用 IM 的情况进行控制。

卡巴斯基实验室的全线产品具有前所未有的保护能力 ，保护用户免受恶意软件和其它外部威胁的困扰。

卡巴斯基实验室的用户可以获得广泛的附加服务，以确保 最有效地使用我们的产品。公司发布的反病毒数据库每小时更新一次，反垃圾邮件数据库每天更新 12 至 24 次。同时，我们提供全天候的多语言技术支持（通过电 话和电子邮件），每天实时更新反病毒数据库和反垃圾邮件数据库。我们还可以根据企业客户的需求设计、部署、支持自定义的反病毒解决方案和信息安全系统。

我们的客户

我们的企业用户中除了中小型企业以外，还包括诸多俄罗斯及国际政府机构和商业组织。

如果您有任何疑问 ,见解和建议 ,都可以通过我们的销售商或者直接联系我们。我们将很高兴通过电话、电子邮件帮助您解决所有产品问题。

卡巴斯基（中国）官方网站： http://www.kaspersky.com.cn

病毒百科： http://www.securelist.com

反病毒实验室: viruslab@kaspersky.com.cn

卡巴一族论坛： http://bbs.kaspersky.com.cn