

卡斯基®  
**反病毒软件**  
**2010**  
用户手册



卡斯基(天津)科技有限公司

[HTTP://WWW.KASPERSKY.COM.CN/](http://www.kaspersky.com.cn/)

修订时间：2009年6月

亲爱的卡巴斯基反病毒软件 2010 的用户：

感谢您选择卡巴斯基实验室的产品。我们希望本文档能够在您的使用过程中提供帮助，并为您解答产品相关的疑问。

**警告！**

本文档的所有权属于卡巴斯基实验室，其所有版权受俄罗斯联邦版权法和国际条约保护。根据俄罗斯联邦法律，非法复制和发布本文档或其中某些部分的违反者将承担民事、行政或者刑事责任。只有经过卡巴斯基实验室的书面授权，才能复制和发布其中内容，包括翻译文档。本文档和相关图形可以被用于非商业或个人目的的资料中。

本文档包括已注册的和尚未注册的商标。所有提及的商标均属于相关所有者。

版权所有©卡巴斯基实验室， 1997-2009

电话(Tel)：(010)84186111

传真(Fax)：(010)84186222

24 小时技术支持电话：400-611-6633

<http://www.kaspersky.com.cn/>

<http://www.kaspersky.com.cn/KL-Services/techsupport.htm>

## 目 录

引言.....	6
产品描述.....	6
注册用户服务.....	8
硬件和软件需求.....	9
卡巴斯基反病毒软件 2010.....	10
获得程序的信息.....	10
帮助资源.....	11
联系销售部门.....	12
联系技术支持服务.....	13
卡巴斯基官方论坛.....	13
卡巴斯基反病毒软件 2010 的新功能.....	14
计算机保护概念.....	15
病毒扫描任务.....	16
更新.....	17
数据和在线安全保护.....	17
向导和工具.....	18
程序支持功能.....	19
安装卡巴斯基反病毒软件.....	21
步骤 1. 搜索应用程序新版本.....	22
步骤 2. 验证系统满足安装需求.....	22
步骤 3. 选择安装类型.....	22
步骤 4. 查看授权许可协议.....	23
步骤 5. 卡巴斯基安全网络数据收集声明.....	23
步骤 6. 选择目标文件夹.....	24
步骤 7. 选择所要安装的程序组件.....	25
步骤 8. 使用程序设置保存之前的安装.....	25
步骤 9. 查找其他反病毒程序.....	26
步骤 10. 安装的最后准备.....	27
步骤 11. 完成安装.....	27

使用入门.....	28
程序配置向导.....	29
步骤 1. 激活程序.....	29
步骤 2. 选择保护模式.....	32
步骤 3. 配置程序更新.....	32
步骤 4. 限制应用程序的访问权限.....	33
步骤 5. 选择所检测的威胁.....	34
步骤 6. 关闭向导.....	34
更新程序.....	35
扫描病毒.....	35
扫描计算机漏洞.....	36
管理授权许可文件.....	37
加入卡巴斯基安全网络.....	38
安全管理.....	39
保护状态.....	40
暂停保护.....	42
保护组件.....	43
文件反病毒.....	43
邮件反病毒.....	45
网页反病毒.....	47
即时通讯反病毒.....	50
主动防御.....	51
扫描计算机.....	52
工具中心.....	56
报告.....	57
通知.....	58
确认卡巴斯基反病毒设置.....	60
测试病毒和变种：EICAR 和它的变种.....	60
测试 HTTP 流量保护.....	61
测试 SMTP 流量保护.....	62
确认文件反病毒设置.....	62

解决问题.....	63
创建系统状态报告.....	64
创建跟踪文件.....	65
发送数据文件.....	66
执行 AVZ 脚本.....	68
卡巴斯基安全网络数据收集声明.....	69
关于卡巴斯基实验室.....	75
最终用户授权许可协议.....	77




## 引言

## 产品描述

您可以从我们的销售商处购买盒装产品，或在网上购买产品，例如：在官方网站 <http://www.kaspersky.com.cn> 上在线购买。

如果您购买了盒装产品，将获得以下内容：

- 一个装有安装 CD（包含安装程序文件和 PDF 文档）的信封
- 用户手册文档和快速安装指南文档
- 授权许可协议（根据区域不同）
- 产品密码卡卡，包含激活码和应用程序激活手册（根据区域不同）
- 卡巴斯基手机安全软件 8.0 半年卡（根据区域不同）



最终用户授权许可协议是您与卡巴斯基实验室的有效法定协议，表明了您使用所购产品时需要遵守的条款。

请仔细阅读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的条款，可以将盒装产品退回销售商，前提是，您没有打开过安装 CD 的信封。

如果您打开了安装磁盘的信封，我们将视为您同意了最终用户授权许可协议的所有条款。

在打开安装磁盘的信封之前，请仔细阅读最终用户授权许可协议。

如果您是在线购买的卡巴斯基反病毒软件，您需要从卡巴斯基实验室的官方网站下载产品程序；用户手册页包含在安装包中。收到您的付款之后，我们将通过邮件给你发送激活码。



## 注册用户服务

卡斯基实验室为所有合法的注册用户提供的服务，提高应用程序性能。

在购买授权许可之后，您就成为一个注册用户，在授权许可有效期内，您将享受以下服务：

- 每小时都在更新的应用程序数据库和软件包更新；
- 您可以通过电话或邮件获得关于安装，配置和使用产品的技术支持；
- 新产品发布和新病毒出现的通知。该服务提供给那些订阅了卡斯基实验室新闻的用户(<http://www.kaspersky.com.cn/KL-Services/techsupport.htm>)。

我们不提供关于操作系统的性能和使用，以及或其它非卡斯基的技术支持。

## 硬件和软件需求

想要确保程序具备正常的功能，计算机必须具备如下最小的系统需求：

常规需求：

- 300 MB 剩余磁盘空间；
- CD-ROM(从 CD 安装卡巴斯基反病毒软件 2010)；
- Microsoft Internet Explorer 6.0 或更高(更新应用程序数据库和软件模块)；
- Microsoft Windows Installer 2.0。
  - ▶ *Microsoft Windows XP Home Edition (Service Pack 2)*, Microsoft Windows XP Professional (Service Pack 2), Microsoft Windows XP Professional x64 Edition.
- Intel Pentium 300 MHz 处理器或更高；
- 256 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.*

- Intel Pentium 800 MHz 32 位(x86) / 64 位(x64)处理器或更高;
- 512 MB 剩余内存。

## 卡巴斯基反病毒软件 2010

卡巴斯基反病毒软件 2010 是新一代的信息保护方案。

卡巴斯基反病毒软件 2010 真正区别与其它软件并和以往的同类型卡巴斯基实验室的产品的是，它能为用户计算机上的数据安全提供多面性的保护。

### 获得程序的信息

如果您有任何关于购买，安装或使用卡巴斯基反病毒软件的问题，我们很乐意为您解答。

卡巴斯基实验室提供各种应用程序的信息资源。您可以根据问题的重要性和紧急状况，选择最合适的。

## 帮助资源

您可以参考应用程序的以下信息来源：

- 卡巴斯基实验室网站上的应用程序页面；
- 技术支持网站的应用程序页面(在知识库)；
- 快速支持服务；
- 帮助系统；
- 文档。

### 卡巴斯基实验室网站上的应用程序页面

[.http://www.kaspersky.com.cn/KL-Products/HomeUsers.htm](http://www.kaspersky.com.cn/KL-Products/HomeUsers.htm)

该页面提供了程序的常规信息，以及它的功能和选项的常规信息。

### 技术支持网站的应用程序页面(知识库)

[.http://www.kaspersky.com.cn/KL-Services/techsupport.htm](http://www.kaspersky.com.cn/KL-Services/techsupport.htm)

在该页面，您会找到技术支持专家创建的文章。

这些文章包含购买、安装和应用程序使用方面的有用信息建议和常见问题问答。例如，在个人用户中，管理授权许可文件，设置数据库更新，或激活程序失败。这些文章都提供了问题的解决方法，不仅仅是本产品的，还有其它产品。

## 快速支持服务

在该标签，您可以找到定期更新的一些常见问题答案。如要使用该服务，您需要连接互联网。

在主应用程序窗口，点击**技术支持**的链接，在打开的窗口中点击快速支持按钮。

## 帮助系统

应用程序安装包含有全部帮助文件，关于如何管理计算机保护（查看保护状态，扫描计算机，执行其它任务），还有程序的设置方法，执行任务列表，等等。

若要打开帮助文档，点击程序窗口的**帮助**按钮，或按<F1>键。

## 文档

卡斯基反病毒软件的安装包里有用户手册(PDF 格式)。该文档含有应用程序功能和主要运算法则的描述。

## 联系销售部门

如果您在选择、购买产品或需要延长产品的使用方面有疑问，请致电我们的销售部门：

(010) 8418 6111 - 7198/7186

或是通过电子邮件发送您的问题至：  
[sales@kaspersky.com.cn](mailto:sales@kaspersky.com.cn)。

## 联系技术支持服务

如果您已经购买了该产品，那么您就可以通过电话或网络的方式从技术支持服务获取您想知道的信息。

卡巴斯基实验室的技术支持服务专家将会就您提出的关于程序的安装、使用，以及如果您的计算机被病毒感染等问题，给出有用的建议以解决这些问题。

在联系技术支持之前，请阅读卡巴斯基实验室产品的技术支持规则。

### 通过电话支持

如果您有紧急事件，请拨打本地的技术支持服务电话。在您给技术支持专家打电话之前，请收集您计算机和反病毒程序的信息。这将有助于我们的专家更快速的帮助您。

## 卡巴斯基官方论坛

如果您不需要立即得到问题的答案，可以在我们的官方论坛上 <http://bbs.kaspersky.com.cn> 提出问题，跟我们的工作人员或其它用户一起讨论。

在这个论坛上，您可以查看已有的帖子，留下您的评论和看法，发表新的帖子，或搜索帖子。

## 卡巴斯基反病毒软件 2010 的新功能

卡巴斯基反病毒软件 2010 是全面的数据保护工具。对所有通道的数据传输和交换提供多方位的保护。为每个组件提供了灵活的配置，能满足不同用户对卡巴斯基反病毒的不同要求。

让我们仔细讨论下卡巴斯基反病毒软件 2010 的新功能：

*新功能：*

- 新的组件：即时通讯反病毒，为主流的即时通讯程序提供保护。该组件扫描来往信息发现恶意对象。
- 卡巴斯基反病毒软件包括网页反病毒的 URL 扫描模块。该模块检查网页链接是否属于可疑网站和钓鱼网站列表。该模块将内嵌在 Microsoft Internet Explorer 和 Mozilla Firefox 浏览器中作为插件。
- 监控访问钓鱼网站，当检测到访问网站的企图时，通过使用钓鱼网址的数据库扫描邮件信息和网页中的链接防御钓鱼攻击。您可以检查网站地址是否包含在钓鱼网站地址列表中；该项仅适用于网页反病毒，即时通讯反病毒和反垃圾邮件。
- 一个新工具漏洞扫描；它使检测和消除安全威胁以及操作系统和计算机上安装的应用程序漏洞变得容易。



## 新界面:

- 新的保护管理保护中心。计算机保护分为三种：用户文件和个人数据，操作系统对象和计算机上安装的应用程序，和网络活动。每个保护方面都有专门的卡巴斯基组件。使用保护中心，用户可以知道哪个组件为特定资源类型提供保护，然后快速转换到该组件编辑设置。
- 工具中心的向导和工具，帮助执行特殊的安全任务。

## 计算机保护概念

卡巴斯基反病毒软件使您的计算机得到安全保护，使它免受已知威胁，新的威胁，黑客和入侵攻击，垃圾邮件和其它垃圾信息的侵扰。每一类型的威胁都有单独的应用程序模块来处理。这使设置更加灵活，为所有的组件设计简单的配置选项来满足特殊用户或商业团体的需要。

卡巴斯基反病毒软件包括:

- 保护组件，提供保护：
  - 文件和个人数据；
  - 系统；
  - 网络活动。

- 病毒扫描任务，扫描单独的文件，文件夹，驱动器，区域范围或整个计算机。
- 更新，确保使用最新的内部应用程序模块和数据库来扫描恶意程序，检测黑客攻击和垃圾信息。
- 向导和工具在卡巴斯基反病毒软件运行期间，向导和工具使任务的执行更为便利。


技术支持功能为程序和扩展信息提供技术支持。

## 病毒扫描任务

除了持续保护恶意程序可以破坏的各种方法，特别重要的是定期扫描计算机。这对排除安全组件没有发现的恶意程序传播的可能性是必要的，例如，由于安全级别设置过低的原因。

卡巴斯基反病毒软件有以下扫描任务：

- **对象扫描。** 扫描用户选择的对象。您可以扫描计算机文件系统中的任何对象。
- **完全扫描。** 彻底扫描整个系统。以下对象默认被扫描：系统内存，启动加载程序，系统备份，邮件数据库，硬盘驱动器，移动存储设备和网络驱动器。
- **快速扫描。** 操作系统启动对象的病毒扫描。



## 更新

若要阻止任何网络攻击，删除病毒或其它恶意程序，卡巴斯基反病毒软件应该及时更新。更新组件正是为了这个目的。它处理应用程序数据库和模块的更新。

更新发布从卡巴斯基实验室服务器上下载数据库和程序模块更新到本地文件夹，然后赋予其它计算机访问的权限，从而减少了网络流量。

## 数据和在线安全保护

卡巴斯基反病毒软件保护您的计算机防止遭受恶意程序和未经授权的访问，尽力确保您在本地网络和互联网上操作的安全。

受保护的對象分为以下三种：

- 文件，个人数据，不同资源的准入参数（用户名和密码），关于银行卡的信息等。这些对象均由文件反病毒和主动防御来保护。

- 安装在您计算机上的应用程序及操作系统。这些对象由邮件反病毒，网页反病毒，即时通讯反病毒和主动防御来保护。
- 在线安全：使用在线支付系统，邮件保护来预防垃圾邮件和病毒等。这些对象由邮件反病毒，网页反病毒，反钓鱼来保护。

## 向导和工具

确保计算机的安全不是一项简单的任务，这需要了解操作系统特点和利用其漏洞的方式。除此以外，大量且多样的关于系统安全的信息使分析和处理变得困难。

为了帮助解决各项保证计算机安全的任务，卡巴斯基反病毒软件中包含了以下这组向导和工具：

- 浏览器配置向导，对 Microsoft Internet Explorer 浏览器的设置进行分析，首要的一点是该向导是从安全角度出发来分析。
- 系统恢复向导，用于消除系统中恶意对象的踪迹。
- 个人隐私清理向导，查找并清除系统中用户活动的踪迹和操作系统设置，这些设置可以收集用户活动信息。

- 应急磁盘，用来扫描和清除感染的 x86-兼容机。当使用反病毒程序或恶意程序清除工具无法清除计算机中的病毒时，使用该程序。
- 漏洞扫描，执行计算机诊断，扫描操作系统中和计算机上安装的应用程序中的漏洞。
- 虚拟键盘，防止对键盘上输入数据的拦截。

## 程序支持功能

应用程序包含一组支持功能。设计这些功能是为了使计算机的保护处于最新状态，扩展应用程序的性能，以及在使用过程中为您提供帮助。

### 数据文件和报告

在应用程序运行期间，每个保护组件，扫描任务，或应用程序更新任务都会创建报告。它包括执行动作和运行结果的信息；使用这些信息，您可以详细了解本程序任何组件是如何工作的。如果有问题，您可以发送报告给卡巴斯基实验室，我们的工作人员可以根据情况帮助您尽快解决问题。

卡巴斯基反病毒软件将所有可疑的文件移动到专门的存储区-隔离区。它们被加密存储在隔离区，以避免感染计算机。您可以扫描这些对象，恢复它们，删除它们，或者添加新的文件到隔离区。病毒扫描结束后，所有被证明未感染的文件将自动恢复到原始位置。

被清除或删除的对象副本存储在备份区。为了恢复文件或图

片，需要给它们创建副本。这些备份副本也被加密存储，以避免感染。

您可以从备份区还原一个文件到原始位置，或删除一个副本。

## 授权许可文件

只有激活程序后，您才可以获得完整保护功能和技术支持，授权许可文件详细说明了使用的有效期以及可以安装的计算机数目。点击左下角的授权许可文件，您可以查看该授权许可文件的详细信息，您也可以购买或续费授权许可文件。

## 技术支持

所有已注册用户可以享有我们的技术支持服务。为了获悉具体在哪些方面您能得到技术支持，请使用**技术支持**功能。

点击相应的链接您可以访问卡巴斯基用户的论坛，给技术支持发送一个错误报告，或者通过填写一个指定的在线表格来给予反馈意见。

您也可以访问在线技术支持服务，个人用户专区服务；我们的工作人员将很乐意为您提供关于应用程序的电话技术支持。

## 安装卡巴斯基反病毒软件

使用安装向导以互动模式安装卡巴斯基反病毒软件。

在安装之前，建议您关闭所有当前运行的应用程序。

若要安装卡巴斯基反病毒软件，运行产品 CD 中的安装文件(带有.exe 扩展名)。

从互联网下载的安装文件安装卡巴斯基反病毒软件，与从 CD 安装应用程序是一样的。

之后，将搜索卡巴斯基反病毒软件的安装包(带有.msi 扩展名的文件)，如果发现安装包，将在卡巴斯基实验室的服务器上搜索有无更新的版本。如果没有发现安装包文件，您需要下载它。下载完成后，卡巴斯基反病毒软件开始安装。如果取消下载，应用程序安装将以标准模式进行。

安装程序使用一系列标准的窗口向导执行，每个窗口包含一些按钮控制安装过程。以下为按钮的简单描述：

- **下一步** – 接受动作，进行下一步安装。
- **后退** – 返回安装的前一步骤。
- **取消** – 取消安装。
- **完成** – 完成应用程序安装。

下面我们详细讨论每一步安装。

## 步骤 1. 搜索应用程序新版本

安装之前，应用程序在卡巴斯基实验室的更新服务器上搜索有无卡巴斯基反病毒软件的新版本。

如果没有新版本，当前版本的安装向导开始运行。

如果发现新版本，您可以下载并安装新版本。如果新版本的安装被取消，当前版本的安装向导开始运行。如果您决定安装新版本，安装文件下载到本地计算机后，安装向导将自动运行。

## 步骤 2. 验证系统满足安装需求

安装卡巴斯基反病毒软件之前，向导会检查操作系统和补丁是否满足安装需求。此外，还检查所需的软件和软件安装权限。

如果有任一不满足条件，屏幕上会显示相应的通知。因此，安装卡巴斯基实验室的产品之前，建议您使用 Windows 更新服务安装所需的系统补丁和所有需要的程序。

## 步骤 3. 选择安装类型

如果您的系统完成符合要求，而且没有发现新版本或者您取消安装新版本，安装向导将安装当前版本。

该步骤，您需要选择最适合您的安装类型：

- **快速安装。**如果您选择该项，整个程序根据卡巴斯基实验室专家的建议都会安装在您的计算机上，安装完成之后，程序安装向导将会启动。
- **自定义安装。**您可以选择希望安装的程序组件，指定程序要安装的文件夹，使用特殊向导激活程序，并配置程序。

如果您选择了第一项，应用程序安装向导可以让您查看授权许可协议和卡巴斯基安全网络数据收集声明。之后，应用程序将被安装在您的计算机上。

如果您选择了第二项，需要输入或确认安装每一步的信息。

继续安装，点击**下一步**按钮。取消安装，点击**取消**按钮。

## 步骤 4. 查看授权许可协议

在这一步骤中，您可以查看您和卡巴斯基实验室之间的授权许可文件。

请仔细阅读该协议，如果您接受该协议中的每一项，请点击**我同意**按钮。将继续安装该程序。

若要取消安装，请点击**取消**按钮。

## 步骤 5. 卡巴斯基安全网络数据收集声明

在这一步骤中，您将可以加入到卡巴斯基安全网络中。加入到这一计划包括发送卡巴斯基实验室在您的计算机上检测出的

新威胁的相关信息，发送卡巴斯基反病毒软件为您的计算机分配的唯一ID号码和系统信息。而且，公司承诺不泄露任何隐私数据。

查看卡巴斯基安全网络数据收集声明。如果您接受其中所有的项目，选中**我接受加入卡巴斯基安全网络条款**复选框。

点击**下一步**按钮，将继续进行安装。

## 步骤 6. 选择目标文件夹

此安装向导的步骤仅适用于自定义安装类型（详见步骤 3. 选择安装类型）。

在这一安装步骤中，您可以指定安装卡巴斯基反病毒软件的目标文件夹。以下是默认设置的路径：

- <drive> \ Program Files \ Kaspersky Lab \ Kaspersky Internet Security 2010 – 针对32位系统。
- <drive> \ Program Files (x86) \ Kaspersky Lab \ Kaspersky Internet Security 2010 – 针对64位系统。

您可以另外指定其他的文件夹作为目标路径，点击**浏览**按钮，并在标准的文件夹选择窗口中选择文件夹，或者在相应的输入区域中输入对应的路径。

如果您是手动的输入安装程序的目标文件夹的完整路径，请记住这个路径。该路径中可能包括200多个字符或者一些任意的特殊字符。

如继续安装，请点击**下一步**按钮。

## 步骤 7. 选择所要安装的程序组件

此安装向导的步骤仅适用于自定义安装类型（详见步骤 3. 选择安装类型）。

若选择自定义安装，您需要指定需要安装到你计算机上的卡斯基反病毒软件的相应组件。默认的情况下，所有的卡斯基反病毒软件的组件均会被选择安装，包括保护组件，扫描任务和更新任务。

若想要决定安装哪个组件，请首先查看与这个组件相关的信息。这样的话，从列表中选择组件并阅读其下面对应的信息。信息中包含简要的说明，以及安装这一组件所需的磁盘空间。

若要取消安装一个组件，打开组件名字旁边图标对应的上下文菜单，并选择**所有功能将无法使用**项。注意，一旦您取消安装一些组件，您就有可能受到大量的危险程序的侵袭。

若要选择安装一个组件，打开组件名字旁边图标对应的上下文菜单，并选择**将在本地硬盘安装该功能**项。

当您完成选择所需要安装的组件时，点击**下一步**按钮。若要所安装的默认组件列表，点击**重置**按钮。

## 步骤 8. 使用程序设置保存之前的安装

在这一步骤中，您可以决定是否需要在将来的工作中使用保护设置和程序的数据库——前提是在移除上一个版本的卡斯基反病毒软件之后，在您的计算机上保存有原来的设置和数据库。

让我们详细了解下如何使用上述功能。

若您的计算机上安装了卡斯基反病毒软件的之前的版本，并且在移除程序时保存了程序的数据库，之后您可以将该数据库关联到您即将安装的新版本中。若要完成该操作，则勾选**程序数据库**这一栏。程序的数据库包含在程序的安装包内而不会直接复制到您的计算机上。

若想使用您计算机中保存下来的前一个版本的保护设置，请选中**程序的运行设置**复选框。

## 步骤 9. 查找其他反病毒程序

在这一步骤中，向导会查找其他的可能与卡斯基反病毒软件相冲突的反病毒程序，包括其他的卡斯基实验室的程序。

一旦在您的计算机中发现其他的反病毒程序，会将其罗列在计算机屏幕上。由您决定是否将其卸载继续完成卡斯基反病毒软件的安装。

您可以在被检测出来的反病毒程序下面选择删除的模式（自动或手动）。

一旦检测出卡斯基实验室的程序的2009版本也包含在反病毒程序的列表中，建议您将其手动移除时使用该程序保存关键的文件。您可以使用该程序的升级版本。也同样建议您保存隔离区中的数据 and 备份的文件；这些对象将被自动的归置到升级版本的隔离区中，您同样可以继续使用。

如果在安装2010版本时自动移除2009版本的程序，原来版本中的激活信息会继续沿用至即将安装的2010版本中。

若继续安装，请点击**下一步**按钮。

## 步骤 10. 安装的最后准备

该步骤是为完整的安装卡巴斯基反病毒软件作准备。

在最初的和自定义安装（详见“步骤 3. 选择安装类型”）程序时，建议您不要勾选**保护安装程序**这一栏。一旦在安装程序的过程中出现任何错误，程序开启的保护能够允许您执行正确的安装步骤的回滚。当您再次进行安装时，推荐您不勾选这一栏。

若使用 *Windows* 远程桌面 进行远程安装时，建议您不要勾选**保护安装程序**这一栏。一旦勾选了这一栏，安装程序就有可能出现安装不完整或者执行错误等情况。

若继续安装，请点击**安装按钮**。

当安装卡巴斯基反病毒软件的组件时，它会拦截网络流量，当前的网络连接将被终止。短时间的一个暂停之后将恢复大量被终止的连接。

## 步骤 11. 完成安装

**安装完成**窗口中包括完整安装卡巴斯基反病毒软件相关信息。

下一个步骤是配置程序的设置以便于最大限度的保护您计算机上存储的信息。配置向导（详见“程序配置向导”）将有助于您快速正确的配置卡巴斯基反病毒软件。

点击**下一步**按钮跳转至程序的配置窗口。

## 使用入门

卡巴斯基实验室创建卡巴斯基反病毒软件的一项主要目的就是为应用程序提供最优的配置。这就可以使那些掌握不同的计算机知识的用户在安装程序之后不用浪费更多的时间而直接能更好的保护他/她的计算机。

为了用户的方便，我们竭尽全力整合程序配置向导（详见“程序配置向导”）的界面接口承接在完成安装的下一步。遵循该向导的操作指南，您可以激活卡巴斯基反病毒软件，修改更新设置，使用密码实现程序的访问限制，以及修改其他设置。

在安装卡巴斯基反病毒软件之前您的计算机可能会感染到一些恶意程序。若要删除这些恶意程序，请运行全盘扫描任务。

由于恶意软件的操作和系统故障等因素，您的计算机的设置就有可能被损坏。运行漏洞扫描任务（详见“漏洞扫描”）查找已安装软件的漏洞以及不规则的系统设置。

在程序刚刚安装完成时，包含在安装包中的应用程序就可能已经过期。开始更新程序（除非在程序安装完成之后或在使用设置向导之后已经完成更新）。

反垃圾邮件组件包括了卡巴斯基反病毒软件所使用的自我学习法来检测垃圾邮件。利用您的邮件运行反垃圾邮件的学习向导的配置。

在完成如上操作之后，卡巴斯基反病毒软件就将准备开始运作。若要对您的计算机的安全级别作出评估，则使用安全管理向导（详见“安全管理”）。

## 程序配置向导

在安装完成之后开始运行程序配置向导。基于您的计算机的特征以及任务，这是旨在帮助您在原来程序设置的基础上进一步的编辑完善。

程序设置向导的接口是一系列的Windows的步骤，您可以使用上一步按钮和下一步链接进行转换，或在关闭的时候使用取消按钮。

### 步骤 1. 激活程序

激活该程序的过程中包括在登记许可的地方安装key文件。程序将根据该授权许可来确定现有的权限以及就算出使用的时间范围。

key文件包括了允许卡巴斯基反病毒软件能够提供全面服务的必要信息：

- 技术支持信息（有谁提供支持，以及从哪获得支持）；
- key文件的名字和序号，以及产品的有效期。

您需要联网去激活该应用程序。

若要在激活的过程中获得key文件，首先您需要有一个激活码。激活码是作为您购买该程序的凭证。卡巴斯基反病毒软件将提供给您如下的操作方式：

- **激活商用授权**。如果您已经购买了商用的授权许可文件，您可以选择这种激活方式，而且前提是您需要有一个激活码。用这个激活码，您可以获得一个对于整个授权期限可以使用程序所有功能的key文件。

- **激活试用授权。**如果在决定购买一个商用的授权许可文件之前，您可以使用激活试用的许可文件这种方式。您将获得一个指定使用时间期限的免费的key文件。
- **稍后激活。**如果您选择该操作，卡斯基反病毒软件将会跳过激活这一步骤。接下来程序将安装在您的计算机上，所有的组件均可用，除了更新（在安装完成之后，您仅可以更新一次）**稍后激活**这一操作仅在程序完成安装后第一次打开激活向导时可见。

如果已经安装过卡斯基反病毒软件，之后又卸载了，且保存了激活信息，则将跳过该步骤。在这种情况下，配置向导将自动的收到与现有授权许可文件的相关信息，并显示在向导的窗口中。

## 激活商用版本

如果您选择该操作，由于要通过卡斯基实验室进行激活，所以需要网络的连接。

激活是需要输入激活码的，这个激活码可以是您在网上购买通过邮件获取的。如果您购买的是盒装产品（零售版），那么激活码将打印在激活卡上。

激活码是一串被分隔成四个小组，每小组由之间没有空格的五个符号，这样的形式构成。例如，11111-11111-11111-11111。注意，请使用拉丁文输入这段字符。

激活向导通过互联网连接到卡斯基实验室的激活服务器上，并向其发送您所提供的激活码，然后验证激活码。如果激活码成功的通过验证，该向导就会收到一个key文件并将其自动安装。窗口中会显示完成激活后的关于购买授权许可详细信息。

如果您激活订购，除了以上提及的部分有关订购方便的信息也会相应的显示出来（详见 订购自动更新授权许可 ）。

一旦激活码没有通过验证，您会在屏幕中看到相应的信息。这种情况下，您可以同您购买软件的经销商取得联系并获得相应的信息。

一旦超过了激活码激活次数的最大限度，相应的信息也会在屏幕上显示出来。激活过程就将被阻断，程序会向您提供连接到卡巴斯基实验室技术支持这项服务。

如果在连接激活服务器的过程中出现任何错误，从而导致您不能顺利的获得key文件，请您联系技术支持。

### 激活试用版本

如果在决定购买一个商用的授权许可文件之前，您可以使用激活试用版本进行激活。您将获得一个指定使用时间期限的免费的key文件。当试用期限已满，就将不可以再激活第二次。

如果在连接激活服务器的过程中出现任何错误，从而导致您不能顺利的获得key文件，请您联系技术支持。

### 完成激活

在成功激活卡巴斯基反病毒软件之后，激活向导将会向您发出通知。此外，还会提供授权许可的相关信息：授权许可的类型（商用，试用，等），产品的有效期，以及能够同时使用该授权许可的机器数量。

如果您激活订购，订购信息的状态会相应的显示出来，而不是key文件的到期日期。

## 步骤 2. 选择保护模式

选择卡巴斯基反病毒软件所提供的保护模式。

以下为两种可用的保护模式：

- *自动模式*。一旦发生了什么重大的事件，卡巴斯基反病毒软件会根据卡巴斯基实验室的推荐自动执行操作。一旦发现威胁，程序将试图为被感染对象清除病毒；如果清除病毒失败，程序将删除被感染对象。受怀疑的对象将被跳过而不会被执行操作。弹出窗口信息向用户通知新事件。
- *交互模式*。在这一模式中，程序会按照您指定的方式对事件做出反应。一旦某一事件需要引起您的关注，程序会弹出通知并提出解决方案供您选择操作。

无论选择哪种保护模式，检测到积极感染事件都会显示出相应的通知。

## 步骤 3. 配置程序更新

如果您选择了快速安装模式，程序配置向导这一步骤将被跳过。在这一步骤中程序设置编辑将为默认值。

对您的计算机的保护的质量取决于数据库和程序模块的更新。在该窗口中，配置向导会要求您设置卡巴斯基反病毒软件的更新模式以及编辑计划设置。

- **自动更新。** 卡斯基反病毒软件会在指定的时间间隔内从更新源核对更新包。在没有更新包时，反病毒爆发或减少的过程中扫描的频率会提高。一发现新的更新资源，程序会自动下载并安装到计算机上。这是默认的模式。
- **按计划更新**（时间间隔可能会根据计划的设定而改变）根据创建的计划自动运行更新。点击**设置**按钮，您可以在打开的窗口中更改计划设置。
- **手动更新。** 如果您选择该操作，您将根据您的需要来运行程序更新。

注意，截止到安装卡斯基反病毒软件的时候集合在安装包中的数据库和程序模块可能均已过期。所以，程序会建议您获取卡斯基反病毒软件最新的更新版本。若要获取最新版本，请您点击**立即更新**按钮。届时，程序会在更新服务器上下载所需的更新的版本，并安装到您的计算机上。

如果安装包中的数据库已经过期了，而且更新包可能会很大，那么就有可能导致额外的网络流量（可能会高达几十兆）。

若您想切换到编辑更新设置（例如，选择更新源，使用用户的帐户运行更新程序，以及将更新服务指向本地更新源），点击**设置**按钮。

## 步骤 4. 限制应用程序的访问权限

如果您选择了快速安装模式，程序配置向导这一步骤将被跳过。在这一步骤中程序设置编辑将为默认值。

由于一台个人的计算机可能由计算机水平不一的几个人共用，并且一些恶意程序可以暂停保护，所以您需要选择密码保护来

控制卡巴斯基反病毒软件的使用权限。使用密码，可以防止未经授权的对卡巴斯基反病毒软件进行禁用保护或修改设置等操作。

若要使用密码保护，则勾选**启用密码保护**这一栏并在**密码**和**确认新密码**栏中输入您要设定的密码。

以下，您可以指定使用密码保护的范围：

- **配置应用程序设置** – 当用户希望保存对卡巴斯基反病毒软件的设置更改时，需要输入密码。
- **退出应用程序** – 当用户希望退出程序时，需要输入密码。

## 步骤 5. 选择所检测的威胁

如果您选择了快速安装模式，程序配置向导这一步骤将被跳过。在这一步骤中程序设置编辑将为默认值。

在这一步骤中，您能够选择卡巴斯基反病毒软件检查威胁的类型。卡巴斯基反病毒软件监察能够对您的计算机造成危害的程序，包括病毒，蠕虫和木马。

## 步骤 6. 关闭向导

向导的最后一个窗口将通知您完成程序的安装。若要立即运行卡巴斯基反病毒软件，请确保启动**卡巴斯基反病毒软件**栏被勾选，并点击**完成**按钮。

## 更新程序

您需要一个用于更新卡巴斯基反病毒软件的网络连接。

卡巴斯基反病毒软件所依赖的数据库中包含威胁的数字签名，典型的垃圾邮件词组，以及网络攻击的相关描述。在卡巴斯基反病毒软件完成安装的时候这些数据就可能已经过期了，因此卡巴斯基实验室要对数据库和程序模块都定期的更新。

在程序配置向导中，您可以选择更新的启动模式（详见步骤 3 “配置程序更新”）默认的情况下，卡巴斯基反病毒软件会自动到卡巴斯基实验室的更新服务器上自动搜索更新源。若服务器上有新的更新资源，程序会以静默模式完成下载并安装。

如果安装包中的数据库已经过期了，而且更新包可能会很大，那么就有可能导致额外的网络流量（可能会高达几十兆）。

若要确保您的计算机的保护不是过期的保护，建议您在完成安装卡巴斯基反病毒软件之后立即运行更新。

*若要手动更新卡巴斯基反病毒软件，则：*

1. 打开程序的主窗口。
2. 在窗口的左侧选择**更新中心**部分。
3. 点击**开始更新**。

## 扫描病毒

恶意软件的开发者会竭尽全力来掩饰他们的程序的操作行为，所以您就可能注意不到您计算机中的恶意软件。

一旦安装了卡巴斯基反病毒软件，它会对您的计算机自动的执行**快速扫描**。该任务意在在操作系统启动过程中，查杀被加载对象中的恶意程序。

卡巴斯基实验室的专家还建议您执行**全盘扫描**任务。

▶ 若要开启病毒扫描任务，请执行如下操作：

1. 打开程序的主窗口。
2. 在窗口的左侧选择**扫描中心**部分。
3. 点击**开始全盘扫描**按钮开始扫描。

## 扫描计算机漏洞

系统故障或者恶意程序活动造成的有害行为导致操作系统被破坏。另外，您计算机上安装的程序的漏洞可能被入侵者利用并破坏您的计算机。

为了检测并清除这些安全问题，卡巴斯基实验室专家建议您在安装完程序后启用安全分析向导。安全分析向导查找本地安装程序的漏洞以及操作系统和浏览器设置的异常和损害。

▶ 启动漏洞扫描认为：

1. 打开程序主窗口。
2. 在打开的窗口左边选择**扫描中心**组件。
3. 点击**打开漏洞扫描窗口**按钮。
4. 打开的窗口，点击**开始 漏洞扫描**按钮。

## 管理授权许可文件

卡斯基反病毒软件需要一个有效的授权许可来激活。当您购买程序时会提供一个授权许可文件。有了授权许可文件，您从购买并安装好它的那天起才具有程序的使用权。授权许可文件包含信息:类型，到期日期，可安装的主机数量。

如果没有授权许可文件，除非激活了试用序列号，那么程序将运行在只能进行一次升级的模式下，也不能下载任何新的更新文件。

如果激活了程序的试用序列号，当试用期限过期时，将不能运行该程序。

当授权许可文件过期时，该程序可以继续运行，只是您不能继续更新数据库。和以前一样，您还是可以进行病毒扫描并使用保护组件，但是只能使用过期的数据库。当您的授权许可过期后，我们不能确保您的电脑免受在此之后出现的新病毒的侵害。

为了保护您的电脑不被新病毒所感染，我们建议您更新授权许可文件。应用程序会提前两周通知您授权许可文件即将到期。在此期间启动应用程序时，屏幕上会也显示一条消息来提醒您。

当前使用的授权许可信息被显示在**许可管理**窗口：类型(商用、商用订购、试用、测试)，主机数量，到期日期，和剩余天。如果安装了商用订阅的授权许可文件或被保护的商用授权许可，到期日期将不会显示。

查看应用程序授权许可协议的方法是，点击**查看最终用户授权许可协议**键。若要删除许可文件，点击 **×** 按钮。若要激活新的许可文件，点击**激活新授权**按钮。

使用**购买授权(更新授权)**按钮，您可以在卡巴斯基实验室网站上进行购买。

## 加入卡巴斯基安全网络

大量的新威胁在时间范围内每日出现。为了方便搜集新威胁的状态，这些资源可以帮助用来清除这些他们，卡巴斯基实验室邀请您使用卡巴斯基安全玩了服务。

使用卡巴斯基安全网络需要发送下面的数据到卡巴斯基实验室：

- 卡巴斯基网络安全分配给您的计算机特有的标识符，用来描述您计算机的硬件设置，并不包含其它信息。
- 被程序组件检测到威胁的信息。信息结构和内容依靠检测到的威胁类型。
- 关于系统信息：操作系统的版本，安装的服务包，下载服务和驱动，查看版本和邮件客户端，浏览扩展部分，安装的卡巴斯基实验室程序版本。

卡巴斯基网络安全也包含下面信息的扩展数据：

- 您电脑上的执行文件和签名的程序；
- 您计算机上运行的程序。

统计信息在更新完成后发送。

卡巴斯基实验室保证不搜集和发布用户的个人数据来执行卡巴斯基安全网络。

▶ 若要配置统计发送设置：

1. 打开程序设置窗口。

2. 在窗口左边选择用户反馈。
3. 选中我同意加入卡巴斯基安全网络复选框来确认您加入卡巴斯基安全网络。

## 安全管理

计算机保护中出现的问题将会通过计算机保护状态来显示。保护状态图标及其所处面板的颜色变化将指示出当前的保护状态。一旦保护系统中出现问题，我们建议您立即修复。



图 1: 计算机保护的当前状态

您可以在**状态**标签查看问题发生的列表，它们的描述和可能解决的方法。(详见下图)；您可以点击状态图标或本地面板上显示(详见上图)。



图 2: 解决安全问题

标签显示当前问题列表，问题关于他们的危险程度，首先，严重的威胁(例如，红色的状态图标)，不严重的威胁 – 黄色的状态图标；最后是一些提示信息。每个问题都有详细的描述，同时还可以对其采取以下的操作：

- **立即清除**。使用相应的按钮，您可以立即对问题进行修复，这也是建议的操作。
- **延迟处理**。如果有于某些原因，不可能立即修复该问题，那么您可以点击**隐藏信息**按钮，稍后解决。

请注意，对于严重问题，不提供该选项。这一类问题包括，无法清除恶意对象，一个或多个组件出错，或是程序文件出错。

如要再次显示隐藏的信息，选中 **恢复隐藏信息**复选框。

## 保护状态

执行卡巴斯基反病毒软件组件或执行病毒扫描任务都将记录在计算机保护状态摘要信息中。您可以知道多少危险和可疑对象被程序检测到，并找到他们进行清除或隔离。

计算机保护状态警告用户关于恶意对象检测，并更改保护状态颜色。如果恶意对象被检测到，图标颜色和面板上的颜色将变成红色。这种情况下，所有出现的威胁将立刻处理。

- ▶ **若要查看计算机保护状态：**
  1. 打开程序主界面。
  2. 点击**报告**连接。
- ▶ **在计算机保护中清除发生的问题：**
  1. 打开程序主窗口。



2. 点击**报告**链接。
  3. 在打开窗口的状态标签执行需要的操作。如要显示隐藏在常规列表中的信息，选中**恢复隐藏信息**复选框。
- ▶ 对检测到的对象执行操作。
1. 打开程序主窗口。
  2. 点击**报告**的链接。
  3. 在打开窗口的**已检测到的威胁**标签中，在列表中选择需要的对象或右击它。
  4. 在打开的目录菜单中选择需要的操作。

## 暂停保护

暂停保护意味着在一个特定的时期内临时禁用所有保护组件。

暂停保护，所有的保护组件都将被暂停。下面将显示程序暂停后的状态：

- 在任务栏程序图标变为灰色；
- 程序主窗口的图标显示为红色。

如果计算机正与网络连接，当保护被暂停时，将会显示一条关于终止当前连接的通知。

▶ *若要暂停计算机保护：*

1. 在应用程序的快捷菜单中选择**暂停保护**。
2. 在打开的**暂停保护**窗口，选择暂停的时间，经过这段时间后，保护会自动启用：

- **下一次暂停 <时间间隔>** – 保护将会在这段时间后被启用。使用下拉菜单来选择时间间隔的值。
- **重新启动后继续运行** – 保护将在系统重启后启用。
- **手动** – 保护只有由您手动来启动。想要启用保护，在应用程序快捷菜单选择**继续保护**。

## 保护组件

### 文件反病毒

文件反病毒防止计算机文件系统被感染。在您启动操作系统时加载文件反病毒并开始在内存中运行，该功能扫描所有打开的，保存的和执行的文件。

默认时，文件反病毒仅扫描新建和更改过的文件。安全级别决定了扫描文件的方法。如果文件反病毒检测到威胁，它将执行指定的操作。

您计算机的文件和内存保护等级由以下固定设置决定：

- 创建保护区域；
- 扫描方式；
- 扫描复合文件 (包括扫描大的复合文件)；
- 扫描方式；
- 允许根据计划暂停组件或选择程序操作。

卡巴斯基实验室专家建议您不要自己配制文件反病毒设置。大部分情况下，更改安全级别就已经足够了。若要恢复文件反病毒的默认设置，选择一个安全级别就可以了。

若要修改文件反病毒设置：

1. 打开程序界面，点击窗口顶部的**设置**链接。
2. 在打开的窗口的**保护**部分选择**文件反病毒**组件。

3. 为您选择的组件点击**设置**按钮。
4. 在相应的设置中做必要的更改。

## 组件运行规则

当您打开计算机将在内存中运行文件反病毒，它将扫描所有被打开，被保存和被运行的文件。

默认的情况下，文件反病毒只扫描最新的或是已修改的文件；换句话说，就是在最近的一次扫描结束后，只扫描新添加的和已经修改的文件。文件将通过以下方式扫描：

1. 组件拦截用户或任意程序试图访问文件的行为。
2. 文件反病毒扫描 iChecker 和 iSwift 数据库中被拦截文件的信息，然后基于被检索的信息来决定是否扫描该文件。

扫描包含如下步骤：

1. 扫描文件中的病毒，程序通过对比应用程序数据库来检测恶意程序。该数据库中包含所有的恶意程序和目前已知威胁的描述和处理它们的方法。
2. 经分析，程序可能采取如下的操作：
  - a. 如果在文件中检测到恶意代码，文件反病毒将阻止这个文件，创建备份，同时试图去清除病毒。如果恶意程序被成功地清除，则该文件可以重新被访问，而如果清除恶意程序的操作失败，这个受感染的文件将被删除。
  - b. 如果在文件中检测到一段疑似恶意程序的代码时，该文件有可能被清除病毒，并将其发送到隔离区。
  - c. 如果在文件中没有发现恶意代码，那么该文件将直接恢复。

一旦检测到已感染对象或潜在的感染对象文件，程序将通知您选择如何操作：

- 隔离新威胁，稍后使用更新的数据库来处理；
- 删除对象；
- 跳过（如果您确定该文件不包含恶意程序）。

## 邮件反病毒

邮件反病毒扫描用来检测进站和出站邮件是否存在恶意对象。它在操作系统启动期间加载到计算机内存并且一直运行，扫描所有通过 POP3, SMTP, IMAP, MAPI 和 NNTP 协议接收的邮件信息。

通过使用已经设置的安全级别来对邮件进行扫描。如果邮件反病毒检测到一个威胁，它将执行指定的操作。邮件扫描时使用的规则通过一组设置来定义。该设置可以分为下列四类：

受保护的邮件；

使用启发式分析；

扫描复合文件；

过滤附件。


卡巴斯基实验室专家不推荐您亲自配置邮件反病毒的设置。大多数情况下，根据需要选择不同的安全级别已经足够保证安全。想要恢复默认的邮件反病毒设置，选择安全级别的其中一个。

若要修改邮件反病毒设置：

1. 打开主程序窗口，点击窗口上部的**设置**链接。
2. 在打开的窗口**保护**部分选择**邮件反病毒**组件。
3. 为您选择的组件点击设置按钮。
4. 在组件设置中做必要的更改。

## 组件运行规则

程序有一个专门的组件用来防御入站和出站邮件中的危险对象：邮件反病毒。邮件反病毒在操作系统启动时加载并一直运行，扫描所有通过 POP3, SMTP, IMAP, MAPI 和 NNTP 协议接收的邮件，以及扫描 POP3 和 IMAP 安全连接(SSL)。

在任务栏通知区域的程序图标就是组件操作的指示器，当扫描邮件时，图标显示为.

默认情况下，邮件保护是这样实现的：

1. 每封用户收到的或发出的邮件被该组件拦截。
2. 邮件被分成三部分：邮件头，正文和附件。
3. 扫描正文和附件（包括 OLE 对象）中的危险对象，利用程序中的数据库进行启发式扫描检测恶意对象，数据库包含所有已知恶意程序的描述和处理它们的方法。启发式扫描可以检测到没有加入数据库中的新病毒。
4. 病毒扫描完成后，进行以下操作：

如果邮件正文或附件包含恶意代码，文件反病毒会阻止该邮件，创建它的备份并尝试清除病毒。如果病毒被成功清除，它将重新变为可用的。如果病毒清除失败，感染的对象会被删

除。在反病毒扫描之后，邮件主题行会插入一个特定的文本，表明该邮件被处理过。

如果在正文或附件里检测到的代码看起来是恶意的但是不能确定，邮件的可疑部分会被送到隔离区。

如果邮件里没有发现恶意代码，将立即发送给用户。

一个专门提供给 **Microsoft Office Outlook** 的插件可以调整邮件规则。

如果您使用 **The Bat!**，该程序可以与其它反病毒程序一起使用。在 **TheBat!** 里直接配置邮件流量处理规则，并且代替程序的保护设置。

当与别的邮件程序（包括 **Microsoft Outlook Express**，**Windows Mail**，**Mozilla Thunderbird**，**Eudora**，**Incredimail**）一起使用时。邮件反病毒根据 **SMTP**，**POP3**，**IMAP** 和 **NNTP** 协议传递的扫描邮件。

注意，在 **Thunderbird** 中，如果您使用过滤器将那些通过 **IMAP** 传递的邮件移出信箱，这些邮件将不被扫描。

## 网页反病毒

当您使用网络时，计算机上的存储信息就会存在被危险程序感染的风险，当您下载免费软件或浏览您认为安全的网站（在您访问之前已经受到黑客攻击）时，这些恶意程序就能渗入您的计算机。此外，只要您的计算机与网络连接，在您打开网页和下载文件之前，网络蠕虫也可能侵入您的计算机。

网页反病毒组件确保您安全地使用网络。它能保护由 **HTTP** 协议传入您计算机的信息，阻止危险脚本在您的计算机中执行。

网页反病毒仅监控那些通过监控端口列表上的端口传输的 HTTP 流量。这些经常用来传递邮件和 HTTP 流量的端口列表包含在程序包里。如果您使用的端口不在这个列表中，可以把它们添加到列表以保护通过它们的流量。

如果您在未保护区工作，建议您在连接互联网时使用网页反病毒来保护您的计算机。如果您的计算机运行在一个有 HTTP 流量过滤的防火墙保护的网路里。网页反病毒会为您使用互联网提供充分的保护。

流量扫描仅使用安全级别的设置。如果网页反病毒检测到威胁，就会按照预定的操作执行。

您的网页保护级别由设置组决定，这些设置可以分为以下几组：


保护范围设置：

决定流量保护效率的设置（使用启发式分析，扫描最优化）。

卡巴斯基实验室专家建议您不要自己配置网页反病毒设置。多数情况下，需要选择不同的安全级别。

若要修改网页反病毒设置：

1. 打开主程序窗口，点击窗口上部的**设置**链接。
2. 在打开的窗口**保护**部分选择**网页反病毒**组件。
3. 为您选择的组件点击**设置**按钮。
4. 在组件设置中做必要的修改。



## 组件运行规则

网页反病毒保护通过 HTTP 进入计算机的信息，并预防在计算机上执行危险脚本。

让我们来详细了解组件操作的设计。使用下面这个算法来保护 HTTP 通信信息：

1. 每个能被用户或通过 HTTP 特定程序访问的网页或文件都会被 Web 反病毒拦截，并对其进行恶意代码分析。使用包含在卡巴斯基反病毒软件中的数据库和启发式扫描来检测恶意对象。数据库包含了对所有目前已知的恶意程序和处理他们的方法的描述。启发式算法可以检测出数据库中有无新病毒。

2. 通过分析，会出现下列处理方式：

如果用户访问的网页或对象包含恶意代码，那么停止访问此对象。并且会显示一个通知，告知您此对象或网页已经被感染。

如果文件或网页不包含恶意代码，那么用户可以立即访问它。

脚本文件根据下面算法进行扫描：

1. 每个运行网页的脚本将被网页反病毒截断并分析其恶意代码。
2. 如果脚本中包含恶意代码，网页反病毒将阻止它并弹出一个消息通知用户。
3. 如果在脚本中没有发现恶意代码，它将继续运行。

脚本仅在用 Microsoft Internet Explorer 打开的网页中被拦截。

## 即时通讯反病毒

除了网上冲浪的功能外，当前流行的即时通讯客户端已经给计算机安全带来了潜在威胁。那些含有可疑站点 URLs 的信息和那些被入侵者利用进行钓鱼攻击的信息可能利用 IM 客户端传输。恶意程序使用 IM 客户端发送垃圾邮件信息和 URLs，盗取用户的 ID 号和密码。

*即时通讯反病毒*组件用来确保 IM 客户端的安全性，它保护通过 IM 协议进入您计算机的信息。

本程序确保各种即时通讯程序安全运行，包括 ICQ, MSN, AIM, Yahoo!, Messenge, Jabber, Google Talk, 等等。

应用程序使用 SSL 协议。为了即时通讯反病毒扫描这些应用程序的流量，必需使用扫描加密连接。在**网络**选项中选中  **扫描加密的连接**。

本程序设置扫描即时通讯的流量。如果检测到威胁，即时通讯反病毒使用警告信息替换含有威胁的信息。

您的即时通讯流量保护等级由一系列设置决定。这些设置可以被分为以下几组：

创建保护范围的设置；

决定扫描方法的设置；

若要修改即时通讯反病毒设置：

1. 打开主程序窗口，点击窗口上部的**设置**的链接。
2. 在打开窗口的**保护**部分，选择**即时通讯反病毒**组件。
3. 在选择组件的设置中作必要的更改。

## 组件运行规则

卡斯基反病毒包含一个组件，扫描通过即时通讯工具传输的信息，叫即时通讯反病毒。它在操作系统启动时加载，运行在计算机内存中。扫描所有入站和出站的信息。

默认情况下，使用如下算法来进行即时通讯流量保护：

1. 每个接收和发送的信息都被该组件拦截。
2. 即时通讯反病毒扫描信息中是否含有危险对象或可疑网站或者钓鱼网站的地址。如果检测到威胁，信息文本将被警告信息替换。
3. 如果在信息中没有检测到安全威胁，信息对用户是可用的。

通过即时通讯客户端传输的文件在保存时会被文件反病毒组件扫描。

## 主动防御

卡斯基反病毒软件不仅可以防御已知威胁，还可以防御数据库中还没有的最新出现的威胁，该功能就是**主动防御**。

主动防御提供的预防技术可以 避免浪费时间并且在新威胁

危害您的计算机之前就将其控制。与基于数据库记录的分析代码的反应技术相比，预防技术通过一系列特定程序执行的操作来识别新威胁。如果活动分析发现这些操作可疑，卡巴斯基反病毒软件将阻止这个程序的活动。

所有应用程序都会进行活动分析，包括那些应用程序控制组件的**信任组**中的程序。为这些程序您可以禁用主动防御的通知。

与应用程序控制组件完全不同的是，主动防御对定义的应用程序活动立刻做出反应。

若要编辑主动防御设置，请执行如下操作：

1. 打开主程序窗口并点击窗口顶部**设置**的链接。
2. 在打开窗口的**保护**部分选择**主动防御**组件。
3. 在设置中为您选择的组件做必要的修改。

## 扫描计算机

扫描计算机中的病毒和漏洞是确保计算机安全的最重要的任务之一。病毒扫描检测恶意代码的传播，因为某些原因反恶意程序无法检测到这些恶意代码。漏洞扫描检测软件漏洞，入侵者可能利用这些漏洞来传播恶意对象和访问私人信息。

卡巴斯基专家辨别病毒扫描任务的几种类型：

- **对象扫描**。用户选择的对象会被扫描。计算机文件系统的任意对象可能会被扫描。在该任务中您可以为扫描可移动磁盘配置设置。
- **完全扫描**。整个系统的完全扫描。默认情况下扫描如下的对象：系统内存，在启动时加载的程序，系统备份，邮件数据库，硬盘，可移动存储介质和网络驱动。

- **快速扫描。**扫描操作系统启动对象。

完全扫描任务和快速扫描任务是指定的任务。推荐您更改这些任务扫描的对象列表。

在指定的区域执行每一个扫描任务并可以根据创建的任务来运行。定义在安全级别中的一组病毒扫描任务参数。默认情况下，提供了三个级别。

病毒扫描任务开始后，在卡巴斯基反病毒软件的主窗口的**扫描中心**部分显示它的过程。在检测到威胁后，程序会执行指定的操作。

当扫搜到威胁时，关于结果的信息将会记录到卡巴斯基反病毒软件的报告中。

## 更新

保持反病毒数据库的更新是确保计算机得到可靠保护的前提条件。因为每天都会出现新的病毒，木马，和恶意软件，有规律的更新应用程序对持续保护您的信息是很重要的。关于威胁的信息和处理它们的方法包含在应用程序数据库中，因此更新数据库是关键组成之一。

应用程序更新时下载和安装的组件有：

- 卡巴斯基反病毒软件数据库。

储存在您计算机的保护信息是根据包含威胁，网络攻击的特征描述和常用的处理它们的方法的数据库，使您的计算机得到安全保护。本程序的组件提供保护并使用它们来搜索和清除计算机上的有害的对象。每小时都向数据库中添加新威胁的记录和处理它们的方法。因此，推荐您定期更新数据库。

除了卡巴斯基反病毒软件数据库，网络驱动也会得到更新，使用它来拦截网络流量。

- 程序模块。

除了更新数据库，您还可以更新应用程序模块。更新包用来修复应用程序的漏洞。添加新的功能或改进现有的功能。

卡巴斯基反病毒软件的主更新源是卡巴斯基实验室专门用来更新的更新服务器。

想要成功地从服务器下载更新，您的计算机需要连接到因特网。默认情况下，因特网连接设置是自动的。如果代理服务器设置不是自动的，手动为它配置连接设置。

在更新过程中，您计算机上的应用程序模块及数据库和更新源上的做比较。如果已经是最新版本的数据库和应用程序模块，您将看到一个提示窗口，来确认计算机上的保护已经是最新了。如果计算机和更新源上的数据库和模块不一样，应用程序仅下载更新增加的部分。不是下载全部的数据库和程序模块，这样显著地增加了复制文件的速度和节省了网络流量。

如果数据库已经过期，更新包可能会很大，从而增加网络流量。

在更新数据库之前，应用程序为它们创建备份文件。这份备份文件可以在您不想要使用最新版本的数据库时，用来还原数据库。

您可能需要恢复到上一次更新，例如，如果您更新了数据库，但是在运行期间它们损坏了。您可以轻松还原到之前的版本并稍后再尝试数据更新。

在程序更新的同时可以执行复制下载的更新到本地更新源。该服务允许在网络计算机上更新数据库和程序模块，从而节省互联网流量。

您也可以配置自动更新启动。

主程序窗口的**更新中心**显示了应用程序当前数据库状态的信息：

- 数据库记录数相关信息；
- 数据库状态（最新的，过期的，或损坏的）；
- 数据库状态（最新的，过期的，或损坏的）。

您可以查看更新报告，报告里有更新任务发生时发生的事件信息（**报告**链接在窗口顶部），您也可以通过点击**病毒活动查看**链接。

## 工具中心

确保计算机的安全是一项艰巨的任务，这需要在操作系统的功能及发掘其弱点方面具有专业的知识技能。此外，与系统安全相关信息的大量及多样性也增加了在分析和处理方面的难度。

为了在提供计算机安全方面能够更为方便的解决具体的问题，将这一系列的向导和工具纳入卡巴斯基反病毒软件中。

- 虚拟键盘，防止对键盘上输入数据的拦截。
- 创建应急磁盘，在遭受病毒攻击后，如病毒攻击破坏了操作系统的系统文件，并使其无法运行，用于恢复系统的可操作性。
- 浏览器配置向导，该向导从安全角度出发，对 Microsoft Internet Explorer 浏览器的设置进行分析。
- Windows 设置修复，恢复被恶意软件损坏的设置。
- 活动痕迹清理，搜索和清除系统中用户活动的跟踪。



# 报告

报告中记录了应用程序每个组件的操作、每次病毒扫描的执行和应用程序的更新。

在报告中您可以选择以下操作：

- 选择您需要查看相关报告的组件和任务；
- 管理数据分组并在屏幕上显示数据；
- 根据卡巴斯基反病毒安全软件创建一个计划将提醒您报告就绪；
- 选择您想要创建报告的事件类型；
- 选择统计信息在屏幕上显示的方式；
- 以文件来保存报告；
- 指定复合过滤条件；
- 配置搜索发生在系统中的事件并根据程序来处理。

## 通知

当事件发生在应用程序运行时，屏幕上会弹出相关的信息。根据事件关于计算机安全的危急程度，您可能会收到以下的通知类型：

- **警报**。发生一件严重的事件，例如，在系统中检测到一个恶意软件对象或危险行为。您应该立即决定程序如何响应。这种类型的通知窗口显示为红色。
- **警告**。发生一件潜在的危險事件。例如，在系统中检测到潜在地被感染对象或可疑行为。根据您判断的事件危险程度，来指示程序执行操作。这种类型的通知窗口显示为黄色。
- **信息**。该通知告诉您非紧要事件的信息。这种类型的通知窗口显示为绿色。

通知窗口由四个部分组成：

1. 窗口标题。通知窗口标题包含一个事件的概述，例如：权限请求，可疑行为，新的网络连接，警报，病毒。
2. 事件描述。事件描述区域显示了关于出现通知原因的详细信息：引起事件发生的程序名，检测到的威胁名，检测到的网络连接的设置等。
3. 操作选择区域。这一部分您可以为该事件选择一个可用的操作。建议的操作选项取决于事件的类型，例如：**清除**，**删除**，**跳过** - 如果检测到一个病毒，**允许**，**阻止** - 如果一个程序请求执行潜在有害的操作的权限。卡巴斯基实验室专家推荐的操作将以粗体字的形式显示。

如果您选择了**允许**或者**阻止**，您可以在接下来打开的窗口中选择操作应用模式。对于**允许**操作您可以选择一个如下的模式：

- **总是允许**。需要允许程序更改访问系统资源的规则，请选择该选项。
- **现在允许**。在程序当前对话期间应用选择的操作到检测到的所有类似的事件，请选择该项。应用的时间为从对话开始直到对话被关闭或者重启。
- **添加到受信任**。选择该项来移动程序到**受信任**组。

对**阻止**的操作您可以选择一个如下的方式：

- **总是阻止**。需要阻止程序更改访问系统资源的规则，请选择该选项。
- **现在阻止**。在程序当前对话期间应用选择的操作到检测到的所有类似的事件，请选择该项。应用的时间为从对话开始直到对话被关闭或者重启。
- **终止**。选择该项来终止程序的运行。

4. 附加操作选择区域。使用该部分您可以选择一个附加操作：

- **添加到排除**。如果您确定检测到的对象是无害的，我们推荐当您在使用该对象时添加它到信任区域，这样在你使用对象时，将不需要进行反复的人工确定
- **应用到所有对象**。选中该复选框，强行将指定的操作应用到在类似情况下有相同状态的所有对象。

## 确认卡巴斯基反病毒设置

安装和配置完程序后，您可以使用一个测试“病毒”和其变种来检查应用程序的配置是否正确。您还可以针对每一个保护组件和协议进行独立的测试。

### 测试病毒和变种：**EICAR** 和它的变种

该测试病毒是由eicar(欧洲计算机反病毒研究中心)专门设计用来测试反病毒产品。

该测试病毒不是一个真正的病毒。因为它不包含会损害计算机的代码。然而，大部分的反病毒产品制造厂商鉴定该文件是一个病毒。

不要使用真正的病毒来测试反病毒产品的运行！

您可以从 **EICAR** 的官方网站下载这个测试“病毒”：

[http://www.eicar.org/anti\\_virus\\_test\\_file.htm](http://www.eicar.org/anti_virus_test_file.htm).

在下载该文件之前，您需要禁用反病毒保护，因为应用程序会鉴别和处理文件anti\_virus\_test\_file.htm为一个通过HTTP协议传送的被感染对象。在下载完该测试“病毒”后，不要忘记立即启用反病毒保护。

应用程序鉴定从 **EICAR** 站点下载的文件是一个包含病毒的被感染对象。如果病毒**不能被清除**，并对这个对象执行指定的操作。

您也可以使用标准测试病毒的变种来检验应用程序的运行。方法是通过添加以下前缀之一（见下表）到标准病毒来更改其内

容。想要创建测试病毒的变种，您可以使用任意的文本或超文本编辑器。例如 **Microsoft Notepad, UltraEdit32**，等。

只有反病毒数据库最后更新时间在2003年10月24日或这个日期之后（2003年10月累计的更新）。您才可以使用EICAR病毒变种来检测反病毒应用程序运行的正确性。

在下表中，第一列包含前缀，用来添加到标准测试“病毒”字符串的开头。第二列列出了反病毒基于扫描结果给对象赋予的所有可能的状态值。第三列包含关于在指定状态下处理对象的信息。请注意对对象执行的操作由程序中设置的值来确定。

在您对测试病毒添加完前缀后,用不同名字保存新文件,例如:  
eicar\_dele.com.给所有变种“病毒”指定类似的名字。

## 测试 HTTP 流量保护

- ▶ 若要验证对通过 *HTTP* 协议传输的数据流中的病毒的检测功能,请执行如下操作:

从官方网站下载一个测试“病毒”，网址为：  
[http://www.eicar.org/anti\\_virus\\_test\\_file.htm](http://www.eicar.org/anti_virus_test_file.htm).

当您尝试下载测试“病毒”时，卡斯基反病毒安全软件将会检测到该对象，将其识别为无法被清除的被感染对象，并且将执行在 HTTP 流量保护设置中针对该类对象相应的操作.默认情况下，当您从该网站下载测试“病毒”时,网络连接将被终止，浏览器将显示一条信息来通知用户，该对象被测试“病毒”EICAR-Test-File 感染。

## 测试 SMTP 流量保护

为了检测使用 SMTP 协议传输的数据中是否有病毒，您必须使用一个利用该协议传输数据的电子邮件系统。

我们建议您测试反病毒如何处理出站的电子邮件，包括正文和附件。若要测试检测正文中的病毒，将标准的测试“病毒”或者修改过的“病毒”复制到邮件中。

### ▶ 测试步骤：

1. 使用安装在计算机上的邮件客户端创建一封**普通文本格式**的邮件。

如果以RTF或HTML格式创建的话，含有测试病毒的邮件不会被扫描！

2. 将标准的或修改过的测试“病毒”复制到邮件的开头，或者附加一个含有测试“病毒”的文件。
3. 发送邮件给管理员。

应用程序将检测对象，判定为受感染的，并阻止该邮件。

## 确认文件反病毒设置

### ▶ 若要验证文件反病毒的配置是否正确,请执行如下操作:

1. 在磁盘上创建一个文件夹，将从 EICAR 组织官方网站 ([http://www.eicar.org/anti\\_virus\\_test\\_file.htm](http://www.eicar.org/anti_virus_test_file.htm)) 下载的测试“病毒”及您创建的所有病毒的变种复制至该文件夹。

2. 允许记录所有事件，所以报告文件保留了关于被破坏对象的数据和因为错误无法扫描的对象。
3. 运行测试“病毒”或其变种。

文件反病毒将截断对文件的调用扫描文件。并且执行设置中指定的操作。通过选择在检测到对象时的不同操作。您将可以对组件的操作进行全盘检查。

您可以在关于组件的操作的报告中查看关于文件反病毒组件运行结果的信息。

## 解决问题

如果应用程序使用时出现任何问题，首先确认问题的解决方法是否在帮助系统或者在卡巴斯基实验室知识库中。*知识库*是技术支持网站的单独部分，有卡巴斯基实验室产品推荐和常见问题解答。尽量使用这个资源来找到您问题的答案或者解决办法。

若要使用知识库：

1. 打开主程序窗口。
2. 在窗口底部点击[技术支持](#)的链接。
3. 在打开的[支持](#)窗口点击[知识库](#)的链接。

另外一个程序应用信息源是卡巴一族论坛。这也是技术支持网站的一个单独区域，且包含用户疑问、反馈和请求。您能查看主题，留下反馈意见或者找到问题的答案。

打开用户论坛的步骤：

1. 打开主程序窗口。
2. 在窗口底部点击**技术支持**链接。
3. 在打开的**技术支持**窗口点击**用户论坛**的连接。

如果您在帮助或论坛中未找到解决方法，我们建议您联系技术支持。

## 创建系统状态报告

当卡斯基实验室的专家在帮您解决电脑问题时,可能要求一个系统状态报告.这个报告包含了关于运行的进程、下载的模块和驱动、Microsoft Internet Explorer 和 Microsoft Windows Explorer 插件、打开的端口、检测到的可疑对象等详细信息。

当创建系统状态报告时，不会收集用户私人信息。

▶ 若要创建一份系统状态报告：

1. 打开主程序窗口。
2. 在窗口底部点击**技术支持**的连接。
3. 在打开的**技术支持**窗口点击**支持工具**的连接。
4. 在打开的**技术支持服务信息**窗口，点击**创建系统状态报告**按钮。

创建的系统状态链接是以 *html* 和 *xml* 格式保存在压缩包 *sysinfo.zip* 中的。一旦收集信息过程结束，您可以查看报告。

▶ 若要查看报告：

1. 打开主程序窗口。
2. 在打开的**技术支持**窗口点击**支持工具**的链接。
3. 在打开的**技术支持服务信息**窗口点击**查看**按钮。
4. 打开包含报告文件 *sysinfo.zip* 压缩包。

## 创建跟踪文件

在卡斯基反病毒安全软件安装后。在操作系统或个别的程序运行时可能会发生一些故障。很可能是卡斯基反病毒安全软件和您计算机上安装的软件或计算机组件的驱动发生了冲突。您需要创建一份跟踪文件。以方便卡斯基实验室的专家来顺利地解决您的问题。

▶ 若要创建一份跟踪文件：

1. 打开主程序窗口。
2. 在窗口的底部点击的**支持**链接。
3. 在打开的**技术支持**窗口点击**支持工具**的链接。
4. 在打开的**技术支持服务信息**窗口的**跟踪**部分使用下拉菜单来选择跟踪等级。跟踪等级由技术支持专家来定

义。如果从技术支持处没有可用的提示，那么推荐使用  
等级标准（500）。

5. 点击**启用**按钮来启动跟踪程序。
6. 重现情形来使问题发生。
7. 选择**禁用**按钮，停止跟踪。

您可以切换到上传跟踪结果到卡巴斯基实验室服务器。

## 发送数据文件

在您创建完跟踪文件和系统状态报告后，您将需要发送它们到卡巴斯基实验室技术支持服务专家。

您将需要输入要求的编号来上传数据文件到技术支持。如果申请是激活的。在技术支持站点上您的个人专区中的这个号码是有用的。

### ▶ 想要上传数据文件到技术支持服务服务器：

1. 打开主程序窗口。
2. 在窗口底部点击**支持**的链接。
3. 在打开的**支持**窗口点击**支持工具**的链接。
4. 在打开的**技术支持服务信息**窗口的**操作**部分，点击**上传技术支持服务信息到服务器**按钮。

5. 选中您想要发送到技术支持服务的跟踪文件的复选框，然后选择**发送**按钮。
6. **输入请求编号**窗口输入号码。

选择了的跟踪文件会被压缩并发送到技术支持服务服务器。

如果不能联系技术支持，您可以在您的电脑上保存数据文件。

▶ **想要保存数据文件到硬盘中：**

1. 打开主程序窗口。
2. 在窗口底部点击**支持**的连接。
3. 在打开的**支持**窗口点击**支持工具**的连接。
4. 在打开的**技术支持服务信息**窗口的**操作**部分点击**将技术支持服务信息上传到服务器**按钮。
5. 选中您想要发送到技术支持服务的跟踪文件的复选框，然后选择**发送**按钮。
6. 在打开的**输入要求编号**窗口点击**取消**按钮，并确认保存文件到磁盘。
7. 在打开的窗口置顶压缩包名称。

稍后您可以在个人专区的帮助下发送保存的文件到技术支持。

## 执行 AVZ 脚本

卡斯基实验室专家将基于追踪文件和系统状态报告来分析您的电脑。分析结果通常是一串很长的操作序列，目的是消除检测到的问题。

使用 AVZ 脚本来简化过程。AVZ 脚本是一系列允许进行以下操作的指令：修改注册表、隔离文件、查找能隔离相关文件的类别，禁止用户模式和内核模式的阻止者等。

应用程序包含一个 AVZ 脚本执行向导来运行脚本。这个向导包含一系列窗口，使用上一步和下一步来操作。一旦完成，使用**完成**键来关闭向导。用**取消**键来取消向导。

卡斯基实验室专家不建议您更改脚本内容。如果在脚本执行过程中出现问题，请联系技术支持。

▶ 若要启动向导：

1. 打开主窗口程序。
2. 在窗口底部点击**支持**的链接。
3. 在打开的**支持**窗口点击**支持工具**的链接。
4. 在打开的**技术支持服务信息**窗口点击**执行 AVZ 脚本**按钮。

成功执行脚本后，向导会关闭。如果在脚本执行过程中发生了一个错误，向导将显示相应的错误信息。

## 卡巴斯基安全网络数据收集声明

### A. 简介

在您继续使用我们的服务或软件之前请仔细阅读该文档，其中包含您需要了解的重要信息。如果继续使用卡巴斯基实验室软件和服务，您将被视为已经接受了卡巴斯基实验室数据收集声明。我们保留随时修改该声明的权利，并将更改公布在网页中。在您决定接受条款之前，请检查最后的修改日期，因为在您最后一次审阅后这些条款有可能被修改。在数据收集声明更新后，您对卡巴斯基实验室服务的任何一部分的使用，都等同于您已经接受已更改的声明。

卡巴斯基实验室和他的分支机构（通称为卡巴斯基实验室）创建了这份数据收集声明，目的是告知和公开卡巴斯基反病毒软件和卡巴斯基反病毒软件数据收集和分发方法。

卡巴斯基实验室承诺 卡巴斯基实验室郑重承诺将对我们用户提供最优质的服务，尤其尊重您对数据收集的关注。我们理解您可能对卡巴斯基安全网络如何收集和使用数据有疑问，因此我们准备了这份声明以告知您运行卡巴斯基安全网络（“数据收集声明”或者“声明”）的数据收集原理。

这份数据收集声明中包含很多常规和技术的详细信息，目的是告诉用户我们是如何收集和使用数据的。我们针对主要的方法和范围编制了这份数据收集声明。目的是您可以快速查阅自己感兴趣的内容。我们的主旨是满足您的需要和期望—包括保护您的数据收集。

如果您在查阅完数据收集声明后有任何疑问，请送电子邮件到 [help@kaspersky.com.cn](mailto:help@kaspersky.com.cn)。

什么是卡巴斯基安全网络？

卡巴斯基安全网络服务将帮助全球的卡巴斯基实验室安全产品用户，更加方便地识别威胁并减少抵御针对您计算机的最新安全风险所需要的时间。为了识别新威胁和它们的来源，并帮助提高用户的安全性和产品功能，卡巴斯基安全网络收集选定的安全和应用程序数据（有关针对计算机的潜在威胁）并把它们提交到卡巴斯基实验室进行分析。这些信息不包含用户个人身份信息，卡巴斯基实验室只会利用这些数据来加强其安全产品的保护能力，并且提供更先进的解决方案以防御恶意威胁和病毒，不会作其它用途。如果用户个人信息意外传送，卡巴斯基实验室将根据本数据收集声明来妥善保护这些数据。

通过加入卡巴斯基安全网络，您和其他来自全球的卡巴斯基实验室安全产品的用户就构成了一个安全的互联网环境。

### 法律相关

卡巴斯基安全网络需要遵从于一些管辖区的法律，因为它的服务会用于不同的管辖区，包括中华人民共和国和香港特别行政区。当法律要求或者我们相信是为了协助调查或保护卡巴斯基实验室的客人，访客，合作伙伴，或者财产及其他人免受危害时，卡巴斯基实验室会在不经过个人允许的情况下透露这些信息。如上所述，卡巴斯基安全网络收集数据和信息的相关法律会因国家不同而有所改变。

当开始收集上述信息，分享这些资料，特别是用于商业开发用途时，卡巴斯基安全网络会及时通知用户，并允许这些网络用户在线选择加入（中华人民共和国，香港特别行政区，和其他需要选择加入程序的国家）或者选择退出（所有其他国家）将这些数据用于商业用途或传递这些数据给第三方。

卡巴斯基实验室会根据执法或司法机关要求，提供一些个人信息给相关的政府部门。若执法或司法机关要求，我们会在

收到适当的文件后提供这些信息。为了保护个人的财产，健康和安  
全，当法律许可时，卡巴斯基实验室也可以提供这些信息。

个人信息保护成员国当局的声明将依照中华人民共和国和香港特别行政  
区的法律生效。关声明的信息内容，可以从卡巴斯基安全网络服务上获  
得。

## B. 收集信息

我们收集的数据卡巴斯基安全网络服务将收集并提交针对您计算机的潜在  
安全威胁数据，这些数据分为核心数据和扩展数据，这些收集到的数据包  
括：

### 核心数据

关于计算机的硬件和软件信息，包括操作系统和服务升级包，内核对象，  
驱动程序，服务，WEB 浏览器，打印机，Windows 浏览器，下载的程序文  
件，活动安装元素，控制面板，主机和注册表，IP 地址，浏览器类型，  
e-mail 客户端和卡巴斯基实验室产品的版本号，这些都不涉及个人身份  
信息；

卡巴斯基实验室产品生成的唯一 ID，该 ID 不包含任何个人信息，用  
来识别个人计算机而不是用户；

有关您计算机反病毒保护的状态信息，一些文件和可疑对象数据（例如，  
病毒名称，检测时间/日期，受感染文件的名称/路径和大小，IP 地址和  
网络攻击的端口，可疑恶意程序的名称）。这些收集的数据不包括个人身  
份信息。

### 扩展数据

用户下载的具有数字签名的程序信息（URL，文件大小，签名者名称）；

可执行程序的信息（大小，属性，创建日期，PE 头信息，区域，名称，  
位置和使用的压缩工具）。

## 传输和存储数据的安全

卡巴斯基实验室致力于保证信息安全，收集到的信息将被存储在受到限制和控制访问的服务器上。卡巴斯基实验室运行着由达到行业标准的防火墙和密码保护系统保护的安全数据网络。卡巴斯基实验室采用了多种安全技术和程序来防护收集到的资料免受未经授权的访问，使用或泄露的威胁。我们的安全策略是定期检查和加强的，仅获得授权的个人能访问收集的数据。卡巴斯基实验室采取措施保证您的信息如本声明所述的一样安全。遗憾的是，我们不能保证所有的数据安全。因此，尽管我们将努力保护您的数据，但我们仍不能保证您传送给我们的任何数据或者从我们的产品或服务传送的任何数据是安全的，这些服务包括但不限于卡巴斯基安全网络，您使用这些服务可能产生的风险需要自己承担。

收集来的数据将被传送到卡巴斯基实验室服务器，卡巴斯基实验室已经采取措施保护这些数据安全，在传送时，我们把收集的信息视为机密信息并提供相应的保护级别；它会遵守我们机密数据使用的安全程序和企业策略。按照行业惯例，收集到的信息传送到卡巴斯基实验室后，将被存储在具有物理和电子保密措施保护的服务器上，这些措施包括密码/登录程序和专为阻止那些来自卡巴斯基实验室之外的未经授权的访问而设计的防火墙。本声明涉及的卡巴斯基安全网络收集的数据，将会在中华人民共和国和香港特别行政区，或者在其他有卡巴斯基实验室商业行为的管辖区或国家进行处理和储存。所有卡巴斯基实验室的员工都知道我们的安全策略。您的数据仅会被那些需要用它来完成工作的员工使用。任何存储的数据都不包含个人身份信息。卡巴斯基实验室不会将卡巴斯基安全网络存储的数据与任何其他数据，联系人列表，或者由卡巴斯基实验室收集来为宣传或做其他用途的订阅信息相结合。

C. 使用收集到的数据如何使用您的信息？

卡巴斯基实验室收集这些数据是为了分析和识别潜在的安全威胁，提高卡巴斯基实验室产品的检测恶意行为、欺诈站点、流氓软件和其它类型的互联网威胁的能力，以便为用户提供更高水准的保护。

向第三方透露信息 若执法人员要求或法律允许，作为对法律程序或者法院传票的回应，或者如果我们相信这样做是为了遵守法律，法规或其他法律程序或政府要求，卡巴斯基实验室可以透露任何收集的信息。当我们有理由相信透露这些信息是为了查明，联系或针对您提出诉讼所必需的，当您可能违反了本声明、您与本公司的协议条款时，或者保护我们用户和公众的安全，或是针对签定了保密协议与授权许可协议的某些特定的第三方（帮助我们开发，运作和维护卡巴斯基安全网络），卡巴斯基实验室也可以透露这些信息。为了宣传，检测及预防互联网安全风险，卡巴斯基实验室可与研究组织和其他安全软件厂商共享某些信息，还可以利用收集来的统计数据，跟踪或发表关于安全风险趋势的报告。

您的选择加入卡巴斯基安全网络是可以选择的。您可以通过卡巴斯基实验室产品选项的反馈设置，随时启动或者禁止卡巴斯基安全网络服务。然而，如果您拒绝提供要求的资料或数据，我们可能无法向您提供基于这些数据资料的服务。一旦卡巴斯基实验室产品服务周期结束，卡巴斯基实验室软件的某些功能还能继续工作，但是信息将不再能自动发送到卡巴斯基实验室。

我们也保留发送少量的警告信息给用户的权利，这些信息用于通知他们先前签署服务的某些变更可能对他们使用我们的服务产生影响。我们也保留与您联系的权利，在不得不作为法律程序的一部分，或者有任何违反许可，授权和购买协议的行为发生时，我们将会与您联系。

卡巴斯基实验室保留与您联系 的权利，因为在一些情况下，

我们需要联系您（如果法律需要或是由于对您十分重要的事件）。我们不会使用这些权利来向您推广新的或现存的服务，如果您要求我们不这样做，我们不会给您发送这种类型的信息。

#### D. 数据收集相关的查询和投诉

卡巴斯基实验室以最大的尊重与关注，来处理用户的数据收集。如果您认为本声明中关于您的信息资料有不符之处，或者您有其它相关的咨询或关注，您可以通过电子邮件联系卡巴斯基实验室，邮件地址：[help@kaspersky.com.cn](mailto:help@kaspersky.com.cn)。

在您的邮件当中，请尽可能详细描述您的问题。我们将及时调查您的问题或投诉。

个人信息的提供是自愿的。用户可以随时通过卡巴斯基产品“反馈”中禁用数据收集这一功能。

版权所有 © 2009 卡巴斯基实验室 保留所有权利。

## 关于卡巴斯基实验室

卡巴斯基实验室成立于 1997 年。今天，它已经成为一家领先的国际信息安全软件提供商。卡巴斯基实验室研发、生产和销售广泛的信息安全解决方案，包括：反病毒、反垃圾邮件和反黑客系统。

卡巴斯基实验室的总部设在俄罗斯莫斯科，并在英国、法国、德国、荷兰、波兰、日本、中国、韩国、罗马尼亚以及美国设有分支机构。最近我们的欧洲反病毒研究中心也在法国成立了。卡巴斯基实验室的全球合作伙伴超过 500 家，网络覆盖全球各地。

目前，卡巴斯基实验室由超过千名的高素质员工组成，其中 10 位具有 MBA 学位，还有 16 位具有博士学位。卡巴斯基实验室的众多反病毒领域专家同时也是计算机病毒研究组织(CARO)的成员。

卡巴斯基实验室的专家在过去 14 年与计算机病毒的不懈斗争中，积累了大量的业内领先经验和知识，这也是我们公司最大的财富。对计算机病毒的透彻分析，使得我们公司的专家能够准确地预见恶意软件的发展趋势，并给我们用户提供针对最新威胁的最及时保护。该优势为卡巴斯基实验室的产品和服务铸就了稳固的根基。同时，这也使我们能够随时为我们的用户提供领先一步的反病毒保护。

公司员工年复一年的辛勤工作，使卡巴斯基实验室成为了顶尖的反病毒软件研发提供商之一，我们在行业内率先开发出了大量的反病毒软件标准。我们公司的旗帜产品，卡巴斯基反病毒，能够为几乎所有的计算机提供可靠的反病毒保护，这些计算机包括：工作站、文件服务器、邮件系统、防火墙、网关和掌上电脑。我们方便易用的集中管理工具能够为企业网络和各类计算机提供最大化地自动反病毒保护。许多知名的业内厂商都在他们的产品中内嵌了卡巴斯基反病毒的内核程序。他们包括：

Nokia ICG (美国), F-Secure (芬兰), Aladdin (以色列 I), Sybari (美国), G Data (德国), Deerfield (美国), Alt-N (美国), Microworld (印度) 和 BorderWare (加拿大)。

卡巴斯基实验室的客户将享受周到的服务，我们每小时更新数据库。公司给客户提供了 24 小时的免费技术支持服务，并用多种语言为全世界客户服务。

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。

卡巴斯基实验室官方网站: <http://www.kaspersky.com.cn>

病毒百科全书: <http://www.viruslist.com>

反病毒实验室: [viruslab@kaspersky.com.cn](mailto:viruslab@kaspersky.com.cn)

(您可以发送可疑对象的压缩文件)

<http://www.kaspersky.com.cn/KL-Services/techsupport.htm>

(技术支持网站)

卡巴斯基实验室官方论坛: <http://bbs.kaspersky.com.cn/>

## 最终用户授权许可协议

标准最终用户授权许可协议 所有用户（含自然人、法人或其它组织）请注意：以下是卡巴斯基实验室(以下称为“卡巴斯基实验室”)编制的卡巴斯基反病毒软件 2010(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。

若您是通过国际互联网, 选择点击“接受”按钮购得本软件, 则表明您已同意受此协议约束, 并成为此协议中的一方。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购得本软件, 且已打开光盘的封套, 则表明您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(包括“激活码”及“授权许可文件”)。

1. 授权许可。在您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。

1.1 使用。本协议仅授权您将本软件用于保护您所购买的激活码或授权许可文件 (key 文件) 中所指定的数量的计算机操作系统(以下简称为“设备”), 即在激活码或授权许可文件指定的数量的计算机、工作站、终端机、手持式计算机或其它数字电子仪器 (每个虚拟机, 虚拟系统也算作一个独立的计算机系统) 上安装、使用、显示、运行 (“运行”) 本“软件”的指定的数量的副本, 一份“软件”激活码或授权许可文件不得在超出其所指定的数量的设备上共同或同时使用。

1.1.1 当软件被载入上述设备的内存(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,即视软件在您的设备上“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 1 份备份,该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。但如果您已经将软件装入硬盘,您应该将原盘作为备份而不能复制。在您丧失该备份的所有权时,您应该负责将备份复制品销毁。

1.1.2 本软件致力于保护您的设备免受病毒的侵扰。这些病毒的相应特征信息已包含在卡巴斯基实验室升级服务器上的反病毒数据库中。

1.1.3 如果您要将安装有本软件的设备出售,请确保在售出前将本软件从设备上完全删除。

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(含自然人、法人或其它组织)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(含自然人、法人或其它组织)或允许任何第三方(含自然人、法人或其它组织)复制本软件。

1.1.6 您不能向任何第三方（含自然人、法人或其它组织）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第三方（含自然人、法人或其它组织）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。本软件作为一个整体，您不得将本软件分解在不同的计算机上使用或嵌入其他软件系统。

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(包括最新的版本和最新的程序修正包)。

1.1.9 终端用户必须保存好合法购得的卡巴斯基产品的资格证明，包括产品光盘、用户手册、激活码或授权许可文件、及购买凭证等。这些在您享受服务、重新安装、及产品升级时是不可复得且不可或缺的。在您无法提供合法购得卡巴斯基产品的资格证明时，卡巴斯基实验室有权拒绝为您提供服务。

1.1.10 您有权为卡巴斯基实验室提供关于您计算机的潜在威胁和漏洞的信息（详细信息，请查阅数据收集声明）。这些信息用来提高卡巴斯基实验室的产品性能。

1.1.11 为了达到 1.1.10 条款中规定的目标，软件将自动收集在计算机上执行的文件信息，并发送到卡巴斯基实验室。

## 2. 支持。

2.1 卡巴斯基实验室将在合法的授权许可(授权许可文件或激活码)的有效期内，向您提供 **24 小时\*365 天**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，但您必须同时具备下列条件：

2.1.1 已支付软件及支持费用。

**2.1.2** 完成终端用户享受卡巴斯基实验室的技术支持服务所需的资格认定附加注册，以建立给予您技术服务的身份档案。在激活本软件和/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** 卡巴斯基实验室具有绝对的独立判断权，以决定您是否满足享受上述技术支持服务的条件。卡巴斯基实验室有权在必要时向终端用户要求附加的注册以便检验与技术支持服务相关的信息。一般情况下，您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。

**2.3** 在合法的授权许可的有效期内，向卡巴斯基反病毒软件 2010 用户提供的技术支持服务包括：

- (a) 反病毒数据库的常规升级；
- (b) 网络攻击数据库更新；
- (c) 反垃圾邮件数据库更新；
- (d) 免费的同类型软件之间升级，包括同类型软件版本升级；
- (e) 由销售商和/或分销商提供的、通过互联网和热线电话给予的技术支持；
- (f) 24 小时循环的病毒检测与杀毒更新；

**2.4** 在您的计算机设备中安装了最新版本软件（包括程序修正包）的情况下，技术支持服务才可生效，最新的软件及程序修正包可在卡巴斯基官方中文网站（[www.kaspersky.com.cn](http://www.kaspersky.com.cn)）或卡巴斯基指定的官方下载网站下载。

**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 及激活码或授权许可文件)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，对保障激活码或授权许可文件的安全采用的最佳方式没有限制。

**5. 有限担保。**

**5.1** 卡巴斯基实验室承诺，本软件首次下载或合法安装后半年内，遵循本产品文档 指示进行正确操作，实现文档中描述的功能。

**5.2** 您同意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/或文档适合您的全部需求。由于影响软件正常运行的因素具有复杂性、进行性和不可预测等特征，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、或数据毫无损失。

**5.3** 卡巴斯基实验室不担保本软件可识别所有已知或未知的病毒，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设备提供保护。

**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。您应当向软件供应商提供所有合理和必要的信息，以协助解决其它问题。

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，用户直接或间接地对本软件作了修改。
- (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 5.4 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) 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。当事人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作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。

**8.** 对本协议的理解。

**8.1** 本协议包含了双方就所述软件的完整谅解, 并代替您与卡巴斯基实验室之间所有和任何先前的、无论口头的还是书面的谅解、担保和承诺。这些谅解、担保和承诺或许先于本协议, 由我们或我们的代表在商谈中以任何书面或口头的形式给出或隐含, 均将在本协议生效日期终止。除第 6.2~6.3 款列出的内容, 基于您期望接受此授权许可协议所做出的不实陈述(“误解”), 您无须做出任何赔偿; 卡巴斯基实验室除依照此协议宣示的条款, 也无须承担任何责任。

**8.2** 本协议不能排除或限制卡巴斯基实验室对任何已知不实的内容导致误解的责任。

**8.3** 若对基本事项(包括供应商在本协议下履行其义务的能力)发生误解,卡巴斯基实验室的责任按照第 6.3 款限定。对自愿使用卡巴斯基实验室的新版试用版产品的用户,将无法享受本协议第 2 条中提供的技术支持服务。

**8.4** 如果您未遵守本《标准最终用户授权许可协议》的条款,卡巴斯基实验室有权 在不做任何通知的情况下终止授权。一旦发生此情况,您必须立即终止使用本软件 并销毁所有副本。