bitdefender

INTERNET SECURITY 2008

使用指南

BitDefender 互联网安全版2008
使用指南

出版方 2008.04.07

法律须知

目录

授权与保证

如果您不赞同这些条款和条件，请不要安装此软件。无论在何种情况下，如果您点击"我接受"，"确定"，"继续"，"是" 或者安装、使用此软件，就表示您完全理解并接受本协议的所有条款。

这些条款覆盖了BitDefender为家庭用户设计的解决方案和服务,包括相关的文档及购买许可证后进行的更新和升级,或在文档和这些条款的副本中规定的相关服务协议.

此使用许可协议是建立在您（个体或单个实体最终用户）和BitDefender之间的关于使用BitDefender软件产品的一份法律协议，以上所说的产品包括计算机软件以及相关多媒体产品，印刷资料，在线查阅的文档或者电子文档（“BitDefender”），所有这些都受到美国以及国际版权法、国际版权条约的保护。只要您安装、拷贝或者使用BitDefender，就表示您愿意受到此协议条款的制约。如果您不同意此协议上的条款，请不要安装或使用BitDefender；您还可以在购买之后30天内将其退还到您购买的地方，您可获得全额退款。当然您需要出示您的购买证明。

如果您不同意本协议的条款,就不能安装或使用BitDefender.

BitDefender 使用许可. BitDefender 受到版权法、国际版权条约以及其它知识产权法律、条约的保护。用户只是被授予BitDefender的使用权，其所有权并未被出售。

使用权授予。BitDefender 在此授予您并且仅授予您一人使用BitDefender的非专有权限。

应用软件。您可以在唯一的一台计算机终端上安装并使用BitDefender，您也可以选择用于同一操作系统的任何其它以前版本的BitDefender。装有BitDefender的计算机的所有者也可以在他或她专用的手提电脑上安装一份BitDefender拷贝

桌面用户许可.该许可证用于能安装在某一不提供网络服务的电脑上的BitDefender软件.每一位初始用户都可以将这个软件安装在一台电脑上,并在另一台电脑上安装其副本.初始用户的数量等于许可证用户的数量.

使用许可期限。 授权使用期限将从您安装、拷贝或者第一次使用BitDefender那天开始计算，并且只能在最初安装的那台计算机上继续生效。

到期。该产品的授权许可到期将停止其功能。

更新。如果BitDefender被标记被可更新的，那么您必需被正确地授予BitDefender的使用权，以使用能被BitDefender识别出的可更新的产品。被标记为升级版的BitDefender 将替换并且/或者补充您产品升级的资格依据。您只能根据本使用许可协议的条款使用升级后的产品。如果BitDefender 是作为单一产品被授权的软件包

中的一个部件的升级产品， 那么BitDefender 只能作为那个软件产品包的一个部件被使用和转移，并且不能被拆开在多台计算机上使用。

版权。BitDefender的所有权益、标题，利益， 以及BitDefender的所有版权(包括（但不仅仅限于这些）任何图象、照片、标记、动画、视频、音频、音乐、文本 以及 BitDefender的"Applet")，任何相关的印刷资料，以及所有的BitDefender的复制品都归BitDefender所有。BitDefender 受到版权法和国际条约的保护。因此您必须像对待其他受产权保护的物品一样对待BitDefender。您只可以在一台计算机上安装BitDefender， 并只能将原版用于备用或存档之用。您不能复印与BitDefender相关的印刷资料 。无论以何种形式拷贝BitDefender，您都必须保留其原始形式的版权告示。您不可以自行再度授权、出租、出售，或租赁BitDefender 。您不可以进行反向工程，重新编译，分解，创造衍生产品，修改，翻译，或作任何找出BitDefender源代码的尝试 。

一定范围内的保证。BitDefender保证从发货之日起的三十天之内，含有BitDefender的媒介不会出现质量问题。万一出现问题，BitDefender提供以下解决方案，您可以凭购买收据更换产品或者退款。BitDefender 不保证BitDefender 将不被中断或者不发生错误或者错误将被改正。BitDefender 不保证BitDefender 将符合您的要求。BitDefender 特此拒绝其它所有保证，无论是明确表达的或是暗示的。上述保证是唯一的并且代替其它所有表述或暗示的保证， 包括暗示的关于商品的、适用于特殊目的的，或非侵犯性的保证。此保证给予您特定的法律权利。根据所在的不同国家，您可能拥有其它特定的权利。

无论明文规定或默认. 为了表示对公司产品的尊重,除非在协议中清楚表明,BitDefender公司有权拒绝提供其他任何担保升级、维护或相关技术支持，或其他材料（有形的或无形的）及服务。无论用于法律法规、交易习惯、贸易惯例或业务习惯，BitDefender公司在此明确表示将无限制地放弃任何暗含保证和条件，包括拒绝提供任何可销售性或者符合某特定目的的暗含保证，如无干预、资料的准确性、信息内容的准确性、系统集成、通过过滤对第三方网站造成侵权或残缺、移除第三方网站的软件、间谍程序、广告软件、Cookie信息、电子邮件、文档、广告等。

不承诺损害赔偿。任何使用， 测试， 或评估BitDefender的人将自行承担所有对BitDefender 质量和表现造成的风险。BitDefender 在任何情况下都不对任何损害承担责任，包括任何情况下使用、表现或者交付BitDefender时带来的任何直接或间接的损害，即使BitDefender 被提醒过存在或者可能存在这样的损伤。有些国家不允许对偶然或者必然的损害限制或者拒绝承担责任，因此上述的局限或者不承诺可能不适用于您。但无论何种情况下，BitDefender 所承担的责任将不超出您购买BitDefender时所支付的价格。无论您是否接受、使用、评估或是测试BitDefender，以上的不承诺声明以及限制声明都将被执行。

对用户的重要告知。. 本软件并不具有容错性能，也不是为了在要求有自动防故障措施的危险环境中应用而专门设计的。本软件不适合应用于航空航天领域、核设施、或是通讯系统、武器系统、直接或间接的生命救护系统、空中交通管制系统、或是任何的由于系统失误可能导致死亡、严重身体伤害或者财产损害的任何应用领域或者设施。

常规。此协议受到罗马尼亚法律和国际版权规则和条约的管理。只能由您和BitDefender 作书面文件签字才能对此协议作修改。此协议只能以英语书写，不能用其他语言翻译或解释

使用BitDefender的价格、花费和收费将随时变化，这将不会预先通知您。

如果出现此协议有不合法的部分，那么不合法的部分将不会影响此协议的其他部份的合法性。

BitDefender 和BitDefender 标记是BitDefender的商标。Microsoft, Windows, Excel, Word, Windows标记, Windows NT, Windows 2000是微软公司的注册商标。所有其它商标都是其各自所有者的财产。

如果您违反了该许可证的条款和条件,它可能不事先通知就突然中止服务.您不能因为服务中止而向BitDefender或其他BitDefender销售商要求退款.与软件使用机密性和限制性有关的条款和条件在中止后仍然有效.

BitDefender公司可以在任何时候修订这些条款,修订后的条款将自动应用于相应的修订软件.如果在这些条款中有一部分是无效的和不可执行的,不会影响其他条款的有效性,它们仍然是有效的,可执行的.

由于将这些条款翻译成其他语言可能产生的争议或矛盾,BitDefender公司发行的英文版本是最权威的.

Contact BITDEFENDER, at 5, Fabrica de Glucoza street, 72322-Sector 2, Bucharest, Romania, or at Tel No: 40-21-2330780 or Fax:40-21-2330763, e-mail address: office@bitdefender.com.

前言

本指南是专为引导选择BitDefender 互联网安全版2008保安解决方案的用户而写的。本指南中的资料不仅适用于拥有电脑知识的人， 它同时适合任何能在视窗系统下工作的人。

这本书将给你介绍BitDefender 互联网安全版2008安全系统的研发公司和团队,指导大家安装过程以及教导你如何设定系统。 你会学习到如何利用BitDefender 互联网安全版2008如何更新、测试和设定。你也会学会如何从BitDefender取得最好的成效。

我们祝你有个愉快和有益一课。

1. 本书中所使用

1.1. 字型

本书中使用了几种不同字型,以提高本书的可读性。以下的表格分列出它们的意义。

字型例子	说明
sample syntax	语法样本打印 monospaced 字符。
http://www.bitdefender.com	URL 连接一些外部的http或ftp司服机。
support@bitdefender.com	电子邮件讯息插入文本内以提供联系信息
“前言” （第 xii 页）	这是一个连接到本书内部某些篇章的联系。
filename	文件和目录都印有使用 monospaced 字体。
option	所有选择性产品会以粗体字书写strong 。
sample code listing	篇码表是以空间字型书写monospaced。

1.2. 额外说明

这是在附加在文内的说明,生动地标记,以引导你对请注意相关的补充相关资料。

注意
笔记是短的观察。虽然您能省去它，笔记可能提供可贵的信息，譬如具体特点或链接对某一相关题目。

重要
这就需要注意,建议不要省略. 通常,它提供非关键但重要信息。

警告
这是要更加谨慎处理的关键信息。 你应该阅读和理解其内容,是非常危险的。

2. 本书的结构

这本书包括几个部分，含有的主要议题。 此外，词汇是为澄清一些技术性的术语。

安装步骤. BitDefender一步步的安装指示. 这是一个安装BitDefender 互联网安全版2008的综合性的讲解。从安装成功的先决条件开始，引导你经过整个安装进程。最后,这里也为你描述如何删除BitDefender。

集中管理. 描述bitDefender基本管理功能

高级安全管理. BitDefender安全功能的详细介绍。 该章节，详细解释各选项的高级设置控制台。 你学会了如何配置和使用所有的bitdefender模块等，以有效地保护您的计算机免受各种威胁（恶意软件，垃圾邮件，黑客， innapropriate内容等）。

BitDefender救援光盘. BitDefender救援光盘的说明。 它有助于理解和运用这一可起动光盘的特点。

获得援助. 如果出现意外状况时到哪里求救。 它也包括常问问题(FAQ)

词汇. 解释一些你会在此文件中发现罕见的和技术性的词汇。

3. 寻求意见

我们请你帮助我们改进本书. 我们尽我们所能验证所有的资料。如果你觉得这本书里有什么缺点,或认为可以改善之处，请写信给我们以帮助我们提供给你最好的文件。

电子邮件可发送到 documentation@bitdefender.com.

重要
请用英语书写所有与您的文档相关的电子邮件,以便我们有效地处理.

安装步骤

1. BitDefender 互联网安全 2008 安装

BitDefender 互联网安全版2008人版的装置使用指南本节包含以下主题:

- System Requirements
- Installation Steps
- Initial Setup Wizard
- Upgrade
- Repairing or Removing BitDefender

1.1. 系统要求

为确保产品的正常运作,在安装前,请核实以下系统所需

- 操作系统: Windows 2000 SP4 / XP SP2 32b & 64b / Vista 32b & 64b; Internet Explorer 6.0 (或者更高)
- 支持的电子邮件客户端: 微软公司的Outlook 2000 / 2003 / 2007 ; Microsoft Outlook Express移动; Microsoft Windows的邮件;雷鸟1.5和2.0

Windows 2000

- 奔腾200MHZ处理器或以上
- 内存至少为256MB(推荐值512MB).
- 硬盘空间至少60MB

Windows XP

- 奔腾200MHZ处理器或以上
- 内存至少为256MB(推荐值1GB).
- 硬盘空间至少60MB

Windows Vista

- 奔腾200MHZ处理器或以上
- 内存至少为512MB(推荐值1GB).
- 硬盘空间至少60MB

BitDefender 互联网安全版2008能在 BitDefender公司的专业资料安全网站上下载.http://www.bitdefender.com.

1.2. 安装步骤

找到设置档案后双点。这将发起一个将引导你通过设置过程的助手:

然后启动安装向导， bitdefender将检查更新版本的安装包。如果不是最新版本，系统会提示您下载它。点击 是 下载新的版本或不继续安装版本，然后可以在设置文件中。

安装步骤

遵循这些步骤，以安装BitDefender互联网安全2008:

1. 点击 下一步 以继续或点击 取消 如果您想要放弃安装.
2. 点击 下一步.

BitDefender 互联网安全版2008 能提示您的电脑上是否安装了其他杀毒软件. 点击 删除 以卸载产品. 如果你想卸载此软件, 请点击 下一步。

警告

安装BitDefender前,强烈建议卸载其他杀毒软件.在一台电脑上同时运行两个或两个以上杀毒软件可能使系统瘫痪.

3. 请阅读许可协议,选择 我接受许可证协议的条款 然后点击 下一步. 如果你不同意这些条件只要点击 取消. 安装过程将会被取消并会退出体系.
4. 你可以选择你想要安装本产品的文件夹。预设的文件夹视C:\Program Files\BitDefender\BitDefender 2008. 如果你想选择另一个文件夹,只需点击 浏览窗口 选择你要安装BitDefender的文件夹然后点击 下一步

   点击 下一步.
5. 选择安装过程的选项 默认选择
   ■打开readme文档 – 在安装完成后打开readme档案。
   ■在桌面安装捷径 – 在安装完成后在桌面装置BitDefender捷径
   ■BitDefender2008 — 在安装完成后更新BitDefender。 你的系统必须与互联网联接系统更新。
   ■关闭windows防火墙

重要

我们建议你关掉Windows防火墙自bitdefender互联网安全的, 2008年已包括一个先进的防火墙。运行两个防火墙, 在同一部电脑上可能造成问题。

   ■关掉 Defender窗口 –关掉窗口;Windows V ista。

   点击 安装 以开始安装产品.

重要

安装过程中将出现一个 向导 界面,它将帮助您进行 BitDefender 互联网安全版2008, 的注册,建立一个BitDefender帐户并设定BitDefender运行重要的安全任务. 完成向导进程后才能进入下一步.

6. 点击 Finish. 你可能会被要求重新启动你的系统,以便安装助手能尽快完成安装过程。 我们建议你维持这个选择。

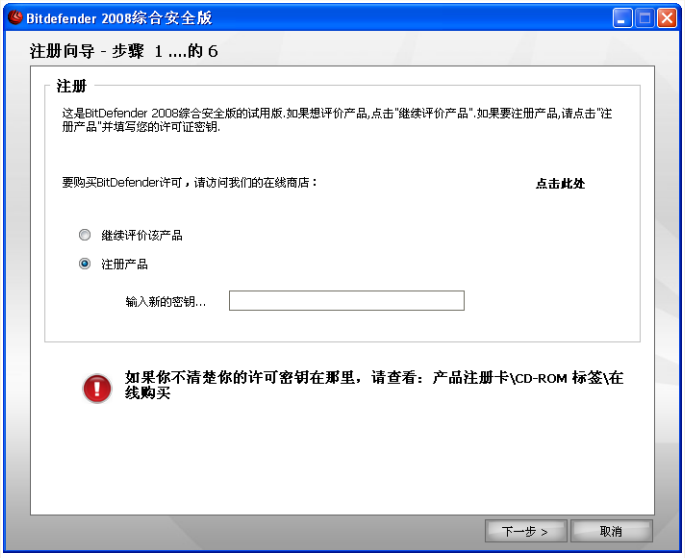
   完成 只要完成产品安装. 如果你选择同意设置的Program Files, 一个新的文件夹名称BitDefender将会在程式档案出现,BitDefender, 它将包含次文件夹 BitDefender,

1.3. 初始安装向导

安装过程中将出现一个向导界面,它将帮助您进行BitDefender 互联网安全版2008的注册,建立一个BitDefender帐户并设定BitDefender运行重要的安全任务.

完成向导进程并不是强制性的:但为了节约时间并保证系统在安装BitDefender 互联网安全版2008 之前的安全性,我们推荐您完成该程序.

1.3.1. 步骤1 - 注册 Bitdefender 网络安全 2008



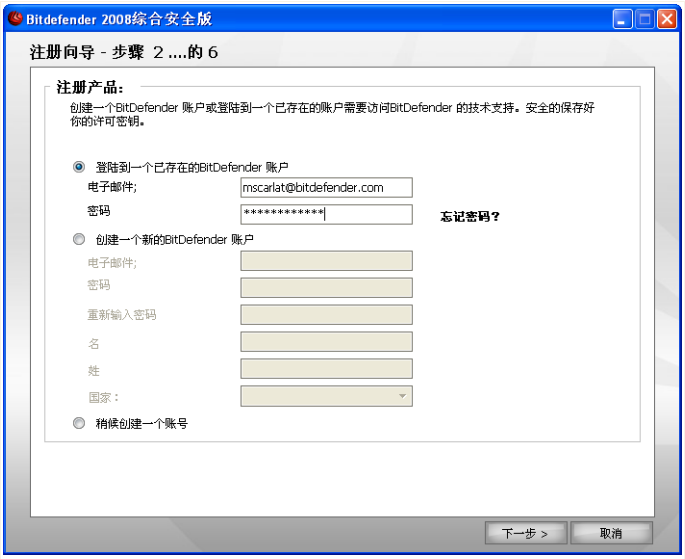
注册

选择产品注册来进行BitDefender 互联网安全版2008的注册.在输入新密钥处输入新的许可证密钥.

要继续评价产品,请选择继续评价产品。

点击 下一步.

1.3.2. 步骤2/6:建立一个BitDefender帐户



建立帐户

我没有BitDefender帐户

为获得BitDefender的免费技术支持和其他免费服务,您需要建立一个帐户.

注意
如果要选择其中一项, 请在相应的格子打勾。

创建BitDefender 账户, 选择 创建Bitdefender新账户和提供必要的信息。 您在这里提供的信息都将保密.

- E-mail – 你的E-mail地址。
- 密码 – 你bitdefender账户的密码。

注意
密码不得少于四个字符

■再次输入密码 – 请输入先前输入的密码。

■名字 – 你姓名中的名

■姓– 你的姓。

■国家–选择你居住的国家。

注意
使用提供的email地址和密码注册你的账户在http://myaccount.bitdefender.com.

成功建立帐户必须先激活您的邮件地址.检查您的邮件地址,按照BitDefender注册服务系统发给您的邮件里的说明进行.

点击 下一步 继续。

我已经有一个BitDefender帐户

bitdefender会自动检测你这台计算机以前有没有注册国bitdefender账户。 在这种情况下，你所需要做的是点击 下一步 .

如果您已经有一个活跃帐户，但是bitdefender没有检测到，选择登录已存在的bitdefender账户 并提供email地址和密码。

注意

如果你点击 下一步. 所有端口将被选择。如果要削除端口选择它和点击 点击 好的可回到上一个步骤。同样的，点击 取消 可继续到向导的下一个步骤。

如果忘记密码,点击"忘记您的密码?",并按照说明进行.

点击 下一步 继续。

1.3.3. 步骤3/6:学习实时病毒报告

RTVR信息

点击 下一步 以继续或点击 取消 以回到第一步.

1.3.4. 步骤4/6 选择任务开始运行

选择任务

对BitDefender 互联网安全版2008 进行设置,使其执行重要的任务以维护系统安全.

你可做以下选择:

- 更新BitDefender Antivirus 2008引擎(可能需要重启 在下一步中),BitDefender反病毒2008引擎将运行以保护您的电脑免受最新威胁的攻击
- 运行快速系统扫描(可能需要重启 在下一步中) ,BitDefender反病毒2008将运行快速系统扫描,以确保您电脑中的 Windows and Program Files文件夹免受感染.
- 每天凌晨2点需运行一次全面系统扫描-每天凌晨2点运行一次全面系统扫描

重要

为了保证您的系统的安全,我们建议您在进入下一步之前确认这些选项.

如果只选择上一个选项或不选,您将跳过下一步.

点击 下一步 以继续或点击 取消 以回到第一步.

1.3.5. 步骤5/6-等待任务完成

任务状态

等待任务完成.您可以看到之前选择的步骤的任务完成状态.

点击 下一步 以继续或点击 取消 以回到第一步.

1.3.6. 步骤6/6 – 总结

完成

Antispam配置对话框

点击 完成 以完成产品的安装.

1.4. 升级

更新程序可以在下列方式之一:

■不删除以前的版本下安装，只有v8 和v9 可以

双击安装对话框 “安装步骤” （第 3 页）部分。

重要

在安装过程期间 Filespy service，服务造成错误信息出现。 点击 赞成 继续安装。

■删除你的前一版本，并安装新的版本 – 所有BitDefender版本

首先要删除你先前的版本,重新启动电脑，并按照 “安装步骤” （第 3 页)一节所描述的安装一个新的.

重要

如果你从v8提升到v9我们推荐您储存BitDefender、 朋友名单，电邮名单及防火墙规则、朋友名单,名单上的电邮. 升级过程结束后,你可以装载他们

1.5. 删除，修复BitDefender

如果你想改变、维修或拆除 BitDefender 互联网安全版2008 按照Windows的开始菜单: 开始 ；→ 程式; → BitDefender 2008 → 修改、修复或删除.

你们将被要求确认你选择点击 下一步. 一个新窗口就会出现让你可以选择:

■修复 重新安装以前安装的所有程式内容

重要

修复产品之前我们建议您保存BitDefender设置修复过程完成后可以重新下载.

如果你选择这设置， 新的视窗会出现。 点击 修复 重新安装以前安装的所有程式内容

重新启动计算机提示时，事后，点击 安装 重新BitDefender 互联网安全版2008。

一旦安装过程完成后，一个新的窗口就会出现。 点击 Finish.

■删除 – 删除所有已安装组件。

注意

删除 删除所有已安装组件。

如果你选择这设置， 新的视窗会出现。

重要

通过消除bitdefender ，你将不再受到保护，免遭病毒，间谍软件和黑客的攻击。If you want Windows Firewall and Windows Defender (only on Windows Vista) to be enabled after uninstalling BitDefender, select the corresponding check boxes.

点击 移除 开始拆除BitDefender 互联网安全版2008从你的电脑。

在删除过程中，你将被提示给我们您的反馈。 点击 好的 来保存新的质料. 若没有任何更改，请点击 取消.

如果删除完成， 新的视窗会出现。 点击 Finish.

注意

删除结束后,我们建议删除你的BitDefender在Program Files的文件夹。

在删除过程中出现一个错误

如果一个错误出现，同时去bitdefender ，清除过程将被退出了新的窗口就会出现。 点击卸载工具以确保bitdefender已被完全删除。 在删除过程中卸载工具将删除所有文件和注册表

集中管理

2. 开始

一旦你已经安装了bitdefender您的计算机受到保护。您可以打开bitdefender安全中心，以检查系统的安全状况，采取预防措施，或完全配置的产品在任何时候。

要进入管理介面， 使用视窗的开始菜单， 步骤是 开始 → 程式 → BitDefender 2008 → BitDefender 2008 互联网保安 更快的方法是直接双点BitDefender icon 系统托盘里的

BitDefender 安全中心

bitdefender安全中心包含两个方面:

■状态区域: 包含帮助您解决安全漏洞的电脑。Fix All Issues 你可以很容易看到多少的问题，可能会影响您的计算机。通过点击相应的红色 解决所有问题，Fix 按钮您电脑的漏洞就会迎刃而解， 。在同一时间内，四名地位按钮对应的四个安全类别可供选择。绿色地位按钮显示，不存在风险。黄色或红色按钮，显示中或高的安全风险。为了解决这些问题，点击黄色/红色按钮，然后 修理 Fix all now 按钮，一个又一个或 修理所有现在 按钮。灰度显示非配置的组成部分。

■快速任务 区域：帮助您的系统安全，并保护您的数据。

此外， bitdefender安全中心包含几个有用的捷径。

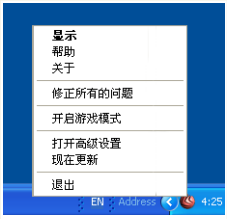
链接	说明
购买	打开一个页面，您可以购买该产品。
我的账户	打开您的 BitDefender 文档页面
注册	打开注册对话框
帮助	打开帮助文档
支持	打开Bitdefender支持网页
设置	打开高级设置台
历史	打开Bitdefender历史事件

2.1. Bitdefender系统图标

更快的管理这个软件，可以使用bitdefender图标在系统托盘。

双击此图标将打开管理控制界面.点右键则出现内容目录.这将为BitDefender用户提供快捷管理.

显示 Bitdefender安全中心



Bitdefender图标

■

■帮助 – 打开帮助文件.
■关于 打开Bitdefender页面
■匹配所有项目 帮助你修复安全漏洞
■开关游戏模式，开关游戏模式。
■打开高级设置 打开高级设置台
■现在更新 立即更新 一个新的窗口将出现在你可以看到更新的状态。
■退出– 关闭这个应用程序

只要游戏模式开启，你可以看到G bitdefender图标。

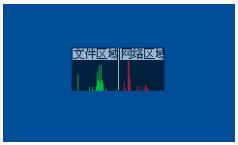
如果有重要问题，影响系统的安全，一个大大的惊叹号标志，展现在bitdefender图标。 你可以悬停鼠标在图标上看到的一些问题，影响了系统的安全性。

2.2. 扫描活动工具条

扫描活动工具条 以图像显示吧你的系统的扫描活动。

绿色指标（档案区）显示每秒扫描的档案数量，规模从0到50.

在 网域 里的红色指标显示每秒转移的Kbytes数(从互联网上收发),规模从0到100.



工具条

注意

扫描活动标 将在相应的地区（档案区或网络区)打上红色的叉以通知你病毒屏障 或防火墙被停止了。这样,不打开管理介面你也可以知道你是否被保护。

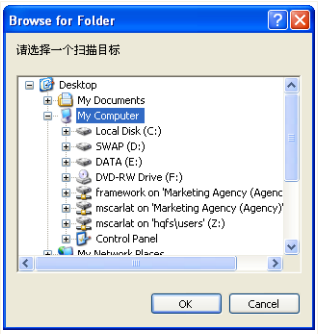
扫描活动工具条 以图像显示吧你的系统的扫描活动。 更多信息请翻阅 “拖放扫描”（第 64 页）.

当你不再想观看图像显示，只要右点击然后选择 隐藏. 彻底隐藏这个窗口，点击高级，在设置控制台和明确的复选框对应使扫描活动酒吧（屏幕上的图形产品活动）

2.3. Bitdefender 手动扫描

如果你想快速扫描某一个文件夹，你可以用bitdefender手动扫描。

进入bitdefender手动扫描，利用Windows开始菜单，按以下路径 Start → Programs → BitDefender 2008 → BitDefender Manual Scan 就会出现下面的窗口：



Bitdefender 手动扫描

你所要做的是浏览文件夹，选择该文件夹，你想将扫描和点击 好的。 BitDefender扫描 将出现并引导您完成整个扫描过程。

2.4. 游戏模式

新的游戏模式，暂时改变保护设置等，以减低它们对系统的性能。 当您打开游戏模式，以下的设置是否适用于：

- 所有bitdefender警报和弹出窗口都被禁用。
- 该bitdefender实时保护级别设置为许可.
- Bitdefender防火前设置成 游戏模式.

只要游戏模式开启，你可以看到G bitdefender图标。

2.4.1. 使用游戏模式

如果你希望选择游戏模式，使用下列方法：

- 在系统任务栏中，右击 BitDefender的图标，再选择 打开游戏模式.
- 按 Alt+G

重要
不要忘了把游戏模式关闭。使用相同的方法你可以打开。

2.4.2. 改变游戏模式热键

如果您想改变热键，请按照下列步骤：

1. 点击设置 在安全中心里设置

注意
在系统任务栏中，右击 BitDefender的图标，再选择 打开高级设置.

2. 点击 高级.
3. 热键游戏模式命令，创建你希望的热键：

■选择修改键如下：按Ctrl ， Shift键 ， Alt。

■在编辑方面，你可以定义规则。

例如：你可以使用Ctrl+Alt+D热键 Ctrl and Alt and type D.

注意
清除记号 使热键为游戏模式 将禁用热键。

3. 安全状态

安全状况明显表现出有系统有组织的和容易管理的名单上的安全漏洞，在您的计算机上。 bitdefender互联网安全的， 2008年将让你知道，每当一个问题，可以影响到你的计算机的安全性。

有四个安全状态按钮:

■电脑安全
■网络安全
■身份识别
■家长控制

在同一时间内，你可以在左边看到的一些问题，影响了系统的安全 按 解决所有问题 按钮。

四个地位按钮，可以显示在绿色，黄色，红色或灰色，而目前的保护水平。

■绿色 显示您的电脑低安全风险
■黄色 显示您的电脑中等安全风险
■红色 显示您的电脑高安全风险
■灰色 显示您的电脑没有配置安全风险

解决安全问题，只需要点击就 解决所有问题 按钮。 会有一个新的窗口出现

安全级别

你可以看到一个名单上的安全问题，并简短介绍了他们的状态。

修理只是一个特定问题上点击相应 修理 按钮。它就会迎刃而解，无论是对现货或之后，你的后续步骤的一个精灵。如果你决定要解决这些问题，点击 修理所有现在"按钮"，并遵守相应的向导。

如果您需要更多的帮助，请点击 更多帮助 按钮，位于窗口底部。 上下文帮助页面会显示您提供详细资料，对这些问题，以及如何去解决这些问题。

重要

对于每一个问题，有一个复选框，默认启用。如果你不希望有一个具体的问题，必须考虑到在计算安全风险，明确了相应的复选框。请使用此选项与谨慎，因为它是很容易的，以增加安全风险，你的电脑是暴露。

待会修理 按 关闭.

3.1. 家长控制状态按钮

如果家长控制的状态按钮是绿色，家长控制功能。如果是灰色的，它是残疾人。

应用父母控制，有下面这些步骤:

1. 点击父母控制状态按钮。
2. 做下列情形之一:
   ■应用父母控制到所有用户，点击 修正所有问题.
   ■应用父母控制对特殊用户，点击 修正 按钮

3.2. 电脑安全状态按钮

安全状况明显表现出有系统有组织的和容易管理的名单上的安全漏洞，在您的计算机上。 bitdefender互联网安全的， 2008年将让你知道，每当一个问题，可以影响到你的计算机的安全性。

颜色地位按钮，可以改变并非只有当你配置设置可能影响到你的计算机的安全性，但是当你忘了做的重要任务。例如，如果你的最后一个系统扫描是旧，安全状态按钮将黄色。如果是很老的，将是红色。

桌子下面将向您提供的资料，哪些内容时，考虑到计算的安全风险。

出版	颜色
最后系统扫描	黄色
最后系统扫描	红色
实时保护被禁用	红色
防毒保护级别设置为许可	黄色
自动更新禁用	红色
最后一次更新是一天前	红色
反垃圾邮件禁用	灰色

请跟随以下一步骤为你的电脑扫描病毒:

1. 点击安全状态按钮
2. 点击要么 修理 按钮，以解决这些问题一个接一个，或 修理所有现在 按钮，以解决这些问题。
3. 如果一个问题是不是固定在现场，跟随向导，以解决它。

3.3. 网络安全状态按钮

如果网络的安全状态按钮是绿色没有什么要担心的问题。否则，如果按钮是红色的，有一个高安全性的风险你的电脑是暴露。

桌子下面将向您提供的资料，哪些内容时，考虑到计算的安全风险。

出版	颜色
防火墙禁用	红色
隐私模式禁用	红色
无线网络不安全	红色

请跟随以下一步骤为你的电脑扫描病毒:

1. 点击网络安全状态按钮
2. 点击要么 修理 按钮，以解决这些问题一个接一个，或 修理所有现在 按钮，以解决这些问题。
3. 如果一个问题是不是固定在现场，跟随向导，以解决它。

3.4. 主监控状态

如果身份地位的控制按钮是绿色，没有什么要担心的问题。否则，如果按钮是红色或灰色，有一个高安全性的风险你的电脑是暴露。

桌子下面将向您提供的资料，哪些内容时，考虑到计算的安全风险。

出版	颜色
隐私保护	绿色
隐私保护关闭	红色
没有建立隐私保护	灰色

请跟随以下一步骤为你的电脑扫描病毒:

1. 点击隐私状态按钮
2. 点击要么 修理 按钮，以解决这些问题一个接一个，或 修理所有现在 按钮，以解决这些问题。

3. 如果一个问题是不是固定在现场，跟随向导，以解决它。

4. 快捷任务

在四个状态按钮下面是 快捷任务 区域。

4.1. 安全

BitDefender可以对必要的安全任务进行快捷扫描。运行这些任务时您可以更新BitDefender、扫描系统或阻止流量。

进入安全模式，再点击 安全 条目。

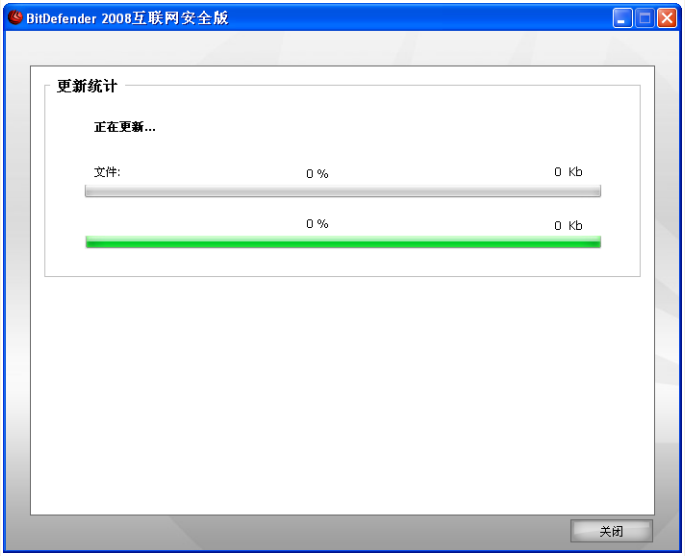
下列按钮可用：

- 现在更新 立即更新
- 扫描我的文档
- 深度扫描
- 完全扫描

4.1.1. 更新Bitdefender

每天都有发现新病毒， 所以随时更新BitDefender最新病毒签名是很重要的。 因此BitDefender已经与设每小时自动更新检查。

默认，Bitdefender每小时做更新 如果你想更新Bitdefender 按 立即更新. 更新过程中，将发起并就会出现下面的窗口立即：



更新Bitdefender

在这个窗口中你可以看到地位的更新过程。

更新过程越快，意味影响软件的操作越短，同时防止攻击。

如果你想关闭窗口，单击 关闭. 这会停止更新

注意

如果您是用拨号方式连接到网络，请经常进行用户要求更新来更新BitDefender 。

如果需要重启计算机. 在一个重要更新，你将被要求重启你的计算机： 如果你不想被提示更新，需要重新开机，等待重新开机来代替提示. 这样，在下一次更新时，需要重新开机后，产品会继续工作旧的病毒库直到你重启系统。

点击 重新启动 会立即重启你的机器。

如果你想重新启动那个 点击好的. 我们建议您尽快重新启动您的系统。

4.1.2. 扫描

为您的计算机扫描恶意软件，运行某一特定扫描任务，通过点击相应按钮。 下表介绍了可扫描任务，并附上自己的描述：

任务	说明
扫描我的文档	使用这项任务，以扫描重要的当前用户文件夹：我的文档 桌面 和 启动项. 这将保证他们的安全将您的文件，一个安全的工作和廉洁运行的应用程序在启动时。
深度扫描	扫描全部系统 在默认配置，它可以扫描所有类型的恶意软件威胁到你的系统的安全，如病毒，间谍软件，广告软件， rootkit和他人。
完全扫描	扫描整个系统，除了卷。 在默认配置，它可以扫描所有类型的恶意软件威胁到你的系统的安全，如病毒，间谍软件，广告软件， rootkit和他人。

注意

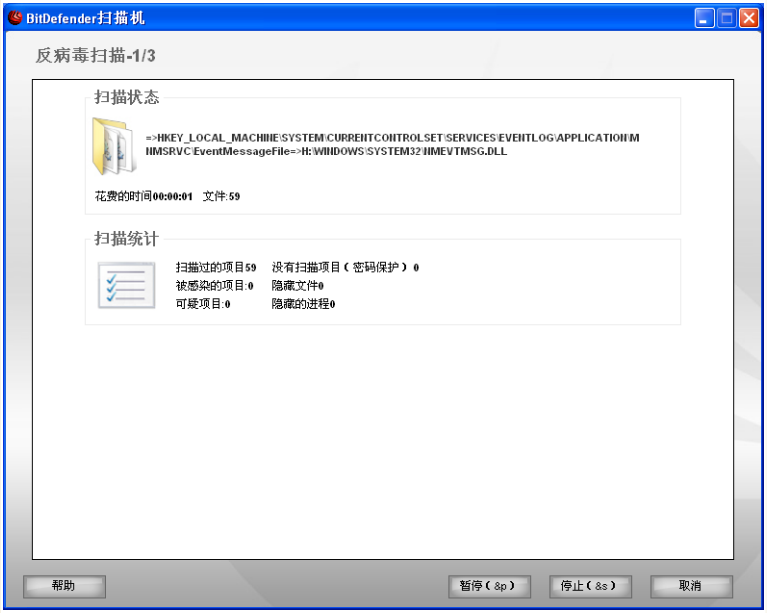
自从深度扫描和完整系统扫描任务分析整个系统，扫描可能需要一段时间。因此，我们建议您在运行这些任务对低优先级或更好的，当你的系统处于闲置状态。

当你开始一种按需扫描过程中，无论是快速或完整扫描， bitdefender扫描器就会出现。

遵循三个步骤的引导程序来完成扫描过程。

步骤1/3 — 正在扫描

Bitdefender正在开始扫描选定项目。



正在扫描

你可以看到扫描的地位和统计（扫描速度，经过时间，有多少扫描/感染/可疑/隐藏物体及其他） 。

注意
这可能需要一段时间,取决于你硬盘的大小。

暂停扫描 点击 暂停 你可以点击 继续 继续扫描

你可以在任何时候停止扫描 点击 停止 是的 . 直接点击对话框。

等待Bitdefender扫描完成

步骤2/3 — 选择动作

当扫描完成后，一个新的窗口将出现，在那里你可以看到扫描的结果。

行动

你可以看到，在一些问题，影响你的系统。

受感染的物体都张贴在集团的基础上，他们的恶意软件感染。 点击链接所对应的一个威胁，以了解更多有关受感染物体。

您可以选择一个整体将要采取的行动，为每个小组的问题，或者你可以选择单独行动，为每一个问题。

你可做以下选择:

行动	说明
没有行动	没有察觉受感染的文件
杀毒	清理受感染的文件。
删除	删除受感染的文件

行动	说明
未隐藏	隐藏条目

点击 继续 应用特殊的行动

步骤三 — 查看结果

当bitdefender饰面操纵问题，扫描的结果将出现一个新窗口。

总结

您能看结果总结。 Logs section from the Properties报告会自动保存

重要
如有需要，请重新启动系统以完成清除过程。

点击 退出 来关闭窗口。

bitdefender未能解决的一些问题

在大多数情况下， bitdefender成功消除受感染的文档或者隔离受感染的文档。 是，有些问题不能得到解决。

在这些情况下，我们建议您联络bitdefender支持团队www.bitdefender.com. 我们的技术支持人员将帮助您解决问题。

Bitdefender侦查密码保护项目

密码保护的类别包括两种类型的项目：文档和安装。 他们没有提出一个真正的威胁系统的安全性，除非它们含有受感染的文件仅仅执行。

确保这些项目都是要清除的：

- 如果密码保护项目保护密码，分开扫描。 最简单的方法来扫描是按右键，并选择 BitDefender反病毒2008 菜单。
- 如果密码保护的项目被安装，确保 实时保护 在你启用安装之前。 如果安装被感染， bitdefender将检测和隔离感染源。

如果你不想让这些文件再次被bitdefender发现你必须将它们添加到扫描例外。 添加扫描例外，点击 设置 打开设置控制台Antivirus > Exceptions 反病毒例外。 更多信息，请提及文件例外扫描。.

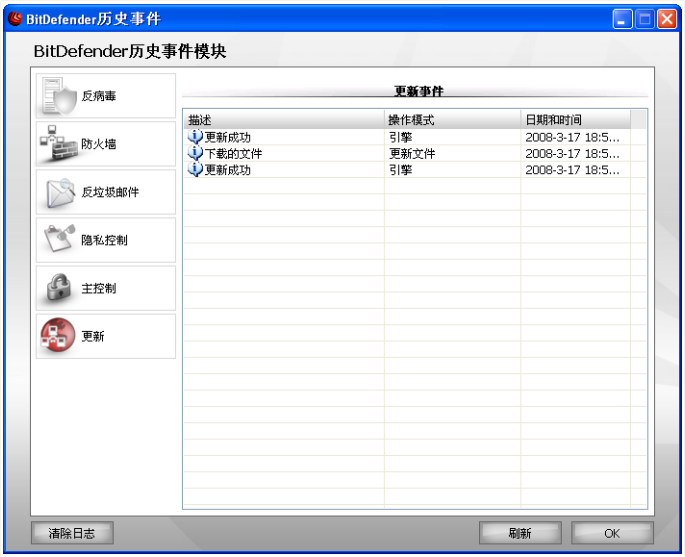
Bitdefender检测怀疑文件。

嫌疑人文档被启发式分析发现，潜在的感染了恶意代码但并没有被释放。

如果嫌疑人档案被发现在扫描期间，你会被要求提交给bitdefender实验室。 点击好的 发送这些文件到bitdefender实验室做分析。

5. 历史

该历史连接在底部的bitdefender安全中心窗口打开另一个窗口，与bitdefender历史及活动。这个窗口为您提供的概况与安全有关的事件。例如，你可以很容易查到，如果升级成功，如果恶意软件被发现在您的计算机上，如果你的备份任务来说，如果没有错误，等等。



事件

为了帮助您过滤bitdefender历史及活动，为以下几类提供在左侧：

- 反病毒
- 防火墙
- 反垃圾邮件
- 隐私控制
- 家长控制
- 更新

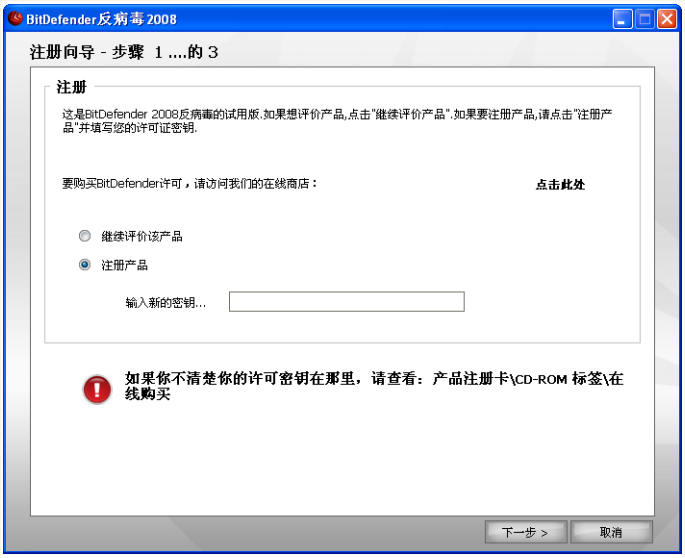
事件表是可用于不同的类别。每次活动具有下列资料：有简短的描述，行动bitdefender了它的时候所发生的事情，日期和时间，当它发生。如果您想了解更多信息，对某一事件，在该份名单中，双击这个活动。

点击 清楚日志，如果你希望删除日志或者刷新最后的日志。

6. 注册

BitDefender 互联网安全 2008 有30天的试用期。 如果你想要注册的bitdefender互联网安全2008，改变许可证或创建一个bitdefender帐户，点击 注册，位于bitdefender安全中心窗口的顶部。 注册对话框会出现。

6.1. 步骤1/3 - 注册 BitDefender 互联网安全版2008



注册

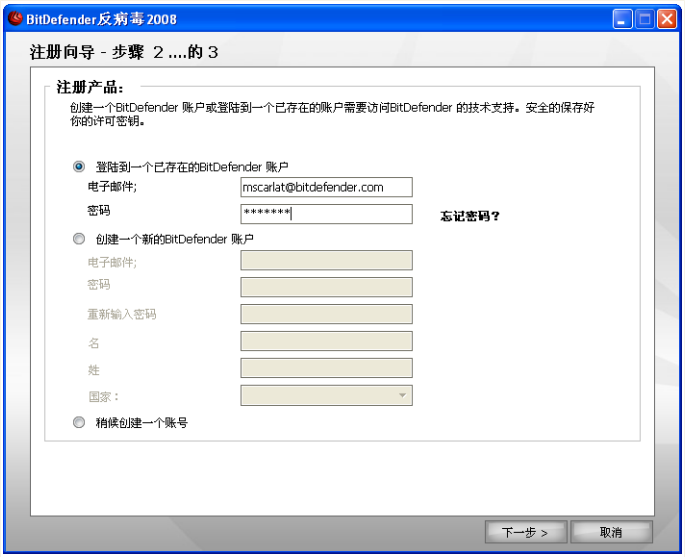
如果您不具备bitdefender许可证，按提供的连接去了bitdefender网上商店和购买软件许可密钥。

注册bitdefender2008 选择 注册产品 在输入新密钥 栏输入新的许可证密钥。

如果测试版本没有到期你要继续评价产品，请选择 继续评价产品.

点击 下一步 继续。

6.2. 步骤2/3: 创建BitDefender帐户



建立帐户

我没有BitDefender帐户

为获得BitDefender的免费技术支持和其他免费服务,您需要建立一个帐户.

注意
如果要选择其中一项, 请在相应的格子打勾。

创建BitDefender 账户, 选择 创建Bitdefender新账户和提供必要的信息。 您在这里提供的信息都将保密.

■E-mail – 你的E-mail地址。

■密码 – 你bitdefender账户的密码。

注意
密码不得少于四个字符

■再次输入密码 – 请输入先前输入的密码。

■名字 – 你姓名中的名

■姓– 你的姓。

■国家–选择你居住的国家。

注意
使用提供的email地址和密码注册你的账户在http://myaccount.bitdefender.com.

成功建立帐户必须先激活您的邮件地址.检查您的邮件地址,按照BitDefender注册服务系统发给您的邮件里的说明进行.

点击 下一步 继续。

我已经有一个BitDefender帐户

bitdefender会自动检测你这台计算机以前有没有注册国bitdefender账户。 在这种情况下，你所需要做的是点击 下一步 .

如果您已经有一个活跃帐户，但是bitdefender没有检测到，选择登录已存在的bitdefender账户 并提供email地址和密码。

注意
如果你点击 下一步. 所有端口将被选择。如果要削除端口选择它和点击 点击 好的可回到上一个步骤。同样的，点击 取消 可继续到向导的下一个步骤。

如果忘记密码,点击"忘记您的密码?",并按照说明进行.

点击 下一步 继续。

6.3. 步骤3/3 - 注册 BitDefender 互联网安全版2008

总结

选择打开我的bitdefender账户 进入你的bitdefender账户。网络连接是必须的。

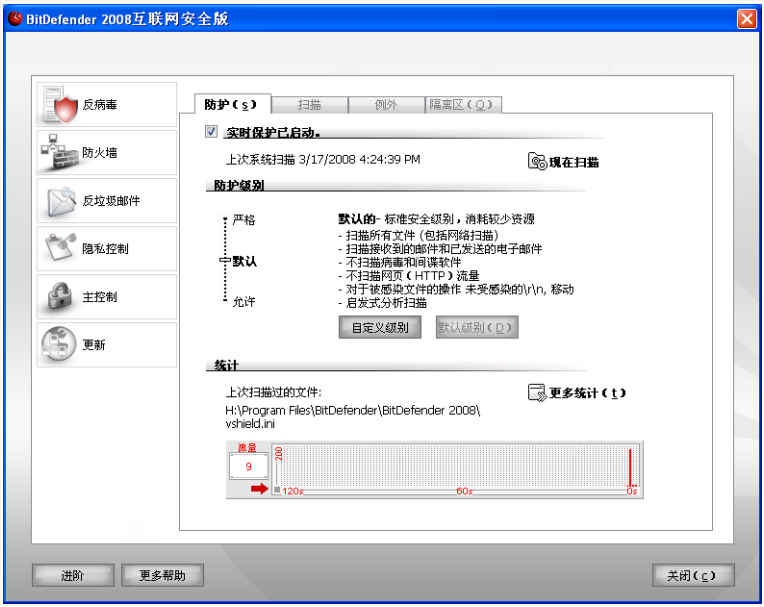
点击 完成 来关上视窗。

高级安全管理

7. 设置台

BitDefender 互联网安全版2008 包括一张可启动的光碟（以LinuxDefender 为基础的BitDefender 拯救光碟）。此光碟能扫描以及在操作系统启动前洁净您所有的硬盘。

进入设置控制台，点击 设置 环线，位于底部的安全中心。



设置台

BitDefender 2008 互联网保安模块包括：普通防毒，防火墙，防垃圾邮件， 防间谍软件，家长控制和更新。 这可以让你轻松管理bitdefender的基础上，各种类型的安全问题的解决。

你可以在管理介面的左边看到以下的单元选择：

■防毒 – 你可以在这一节里设置防毒单元。
■防火墙 – 你可以在这一节里设置防火墙模块。

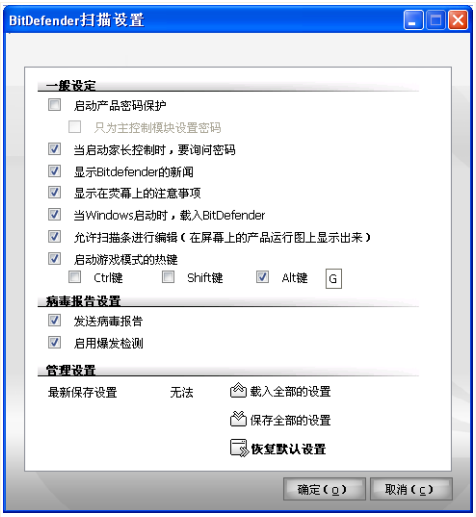
■防垃圾邮件 – 你可以在这一节里设置防垃圾邮件单元。
■隐私控制 你可以配置隐私控制
■父母监控 – 你可以在这一节里设置父母监控模块。
■更新 – 你可以在这一节里设置更新模块。

在设置控制台底部，这里是 更多帮助，打开帮助页面的按钮。 点击此按钮了解更多信息，随时你都可以得到更多帮助

如果您需要更多的帮助，请点击 更多帮助 按钮，位于窗口底部。 上下文帮助页面会显示您提供详细资料。

7.1. 配置一般设置

配置一般设定为bitdefender互联网安全的， 管理其设置，请点击 高级. 会有一个新的窗口出现



一般设置

在这里你可以设定BitDefender行为。 BitDefender已经预设是在视窗的启动和缩小工作巴黎。

7.1.1. 一般设置

■启动密码保护 – 可设定密码,以保护管理BitDefender

注意
如果你不只是个人使用这台电脑,建议你有密码保护你BitDefender设定

如果你选择这设置， 新的视窗会出现。

输入密码

在密码栏输入密码，在重新输入密码栏再次输入相同的密码，按确定

如果你忘了你的密码， 你必须修复BitDefender 以调整产品的设定 其他的系统管理员（如果有的话）也将提供这方面的密码，以改变bitdefender设置。

如果你想被提示输入密码，只有当配置父母控制，你还必须检查 要求/申请密码，只有父母控制模块. 在另一方面，如果一个密码才订定为父母控制和你选了这个选项，各自的密码将被要求配置的时候，任何bitdefender选择。

重要
如果你忘了你的密码，你必须修复BitDefender 以调整产品的设定

■要求有密码的时候，让家长控制 –如果你选择了这项功能，没有密码设置，系统会提示您设置密码时，使家长控制。
■获得保安通知 – 不定时收到由BitDefender服务器发出的病毒爆发通知。
■在荧幕显示注释 – 弹起的视窗显示产品的状况
■BitDefender 和视窗同时开启 – 系统在启动时自动打开BitDefender 我们建议你维持这个选择。
■启用扫描工具栏）展示扫描活动工具栏。 清除复选框如果你不想扫描工具栏被显示。

注意
这个选项可以配置当前windows用户账户

■使热键为游戏模式 –允许运用多种键盘键（热键），以开启/关闭游戏模式 默认热键 Alt+G.

修改热键在下面：

1. 检查修改关键字Ctrl), Shift key (Shift) or Alternate key (Alt

2. 在编辑方面，你可以定义规则。

7.1.2. 病毒报告设置

■发送病毒报告 – 把在你的电脑发现的病毒报告给BitDefender病毒实验室。 这将帮助我们了解和追踪病毒的爆发

该报告将不会含有机密数据，例如你的名字、IP地址或他人资料。 也不会用于商业目的。 资料将只包括病毒名称，且仅用作篇制统计报告。

■发送病毒报告 – 把在你的电脑发现的病毒报告给BitDefender病毒实验室。 这将帮助我们了解和追踪病毒的爆发

该报告将不会含有机密数据，例如你的名字、IP地址或他人资料。 也不会用于商业目的。 资料将只包括病毒名称，且仅用作篇制统计报告。

7.1.3. 管理设置

使用 保存所有设置 / 启动所有设定 来储存/启动你为指定地点安排的BitDefender设定。这样你可以在重新装置或修复BitDefender后使用同样的设定。

重要

只有具备管理权限的用户才能保存和加载设置。

载入默认设置 点击 恢复默认设置.

8. 防毒

bitdefender可以保护电脑免受一切形式的恶意软件（病毒，木马，间谍软件，rootkit和等）。

以智慧型扫描档案。目的是,在发现病毒的定义前根据一些算法和模式找出新的病毒。有时会出现虚惊。 这样的例子是当做疑似案例。在这种情况下,我们建议你送档案给BitDefender实验室分析。

病毒保护分为两类:

- 按访问扫描 –防止新的恶意威胁进入你的系统。这也是所谓的实时保护–档案进行扫描，因为您使用它们–按访问。 bitdefender会，举例来说，扫描Word文件已知的威胁，当你打开它，电子邮件时，您会收到一张。
- 对按需扫描 –允许检测和删除的恶意软件已经居住在您的系统。 命令扫描 – 发掘已经驻留在你系统里的病毒。 这是由用户命令病毒扫描的典型例子， 然后BitDefender按需求扫描. 扫描任务，让你能够创建定制的扫描例程，并能如期运行，定期通报。

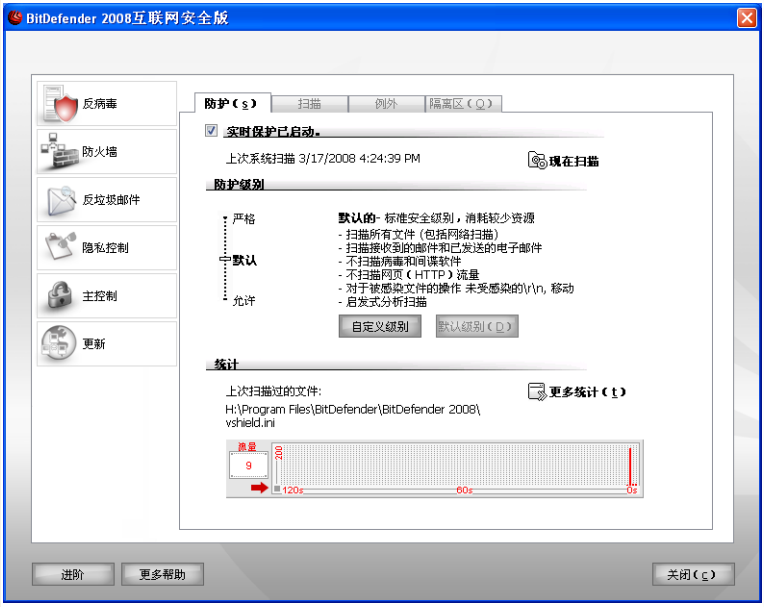
在这个防毒模块的用户指南中包括下列内容:

- 按访问扫描
- 按需扫描
- 在需要时扫描
- 隔离

8.1. 按访问扫描

按访问扫描，也称为实时保护，让您的计算机免受各种恶意软件威胁扫描所有存取档案，电子邮件和通信是通过即时通讯软件应用（ ICQ的， NetMeeting的，雅虎的IM ， MSN信使）。

配置和监控实时保护，点击 防毒 ，在设置控制台。 就会出现下面的窗口:



实时保护.

重要
请保持实时防毒开启以防止病毒入侵你的电脑.

在这个单元的底部可以看到实时病毒保护罩扫描资料档案或电子邮件的统计讯息。如果你想要看到更多有关统计数字的解释， 请点击 更多统计资料

想启动快速扫描，请点击 立即扫描.

8.1.1. 配置防护级别

您可以选择最符合您的防护需要的安全级别.上下拖动滚动条以设定最合适的防护级别。

共有3个安全级别:

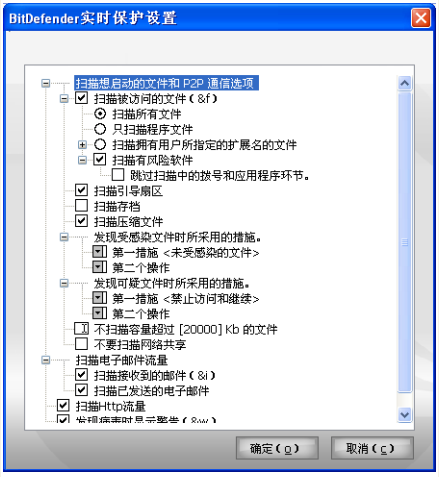
防护级别	说明
许可	包含基本的安全需求。资源消耗级别非常低。 只扫描程序和邮件信息中的病毒。除了经典特征病毒扫描，还使用了启发式分析。对感染文件采取的措施有：清除文件/禁止访问。
默认	提供标准安全级别。资源消耗级别较低。 扫描所有文件和邮件信息中的病毒和间谍软件。除了经典特征病毒扫描，还使用了启发式分析。对感染文件采取的措施有：清除文件/禁止访问。
侵略	提供高级安全级别。资源消耗级别中等。 扫描所有文件、邮件信息和网页流量中的病毒和间谍软件。除了经典特征病毒扫描，还使用了启发式分析。对感染文件采取的措施有：清除文件/禁止访问。

要启动实时保护，请选中 默认级别.。

8.1.2. 定制防护级别

先进用户可以利用BitDefender提供的扫描– 设定。这个扫描设定可以跳过那些你知道是无害的的档案延伸、目录或档案。这可大大减少扫描时间,提高你的电脑在扫描时的反应。

修改公司经营进入实时保护. 以下窗口照常按 输入新码. 以更改预设的执照。 以下的视窗会打开:



病毒保护罩设定

扫描选择的以扩大的菜单方式呈现，非常类似视窗。 按"+"的格子以打开选择或“–”的格子以关闭打开的选择。

注意
你会看到一些扫描选择虽然有“+”格子但却无法打开，因为这些格子尚未选定。 当你选择它们后就可以打开了。

■扫描被接触过的档案和P2P转移的选择 – 扫描被接触过的档案及通过即时信息应用软件(ICQ、NetMeeting、Yahoo Messenger，MSN Messenger) 的通讯。下一步，选择一种你想扫描的档案。

选择		说明
扫描访问文件	扫描所有档案	无论类别扫描全部被接触过的档案。
	只扫描程式档案	只有程式档案将被扫描。这意味着只有带下列延伸的: .exe; .bat; .com; .dll; .ocx; .scr; .bin; .dat; .386; .vxd; .sys; .wdm; .cla; .class; .ovl; .ole; .exe; .hlp; .doc; .dot; .xls; .ppt; .wbk; .wiz; .pot; .ppa; .xla; .xlt; .vbs; .vbe; .mdb;

选择		说明
		.rtf; .htm; .hta; .html; .xml; .xtp; .php; .asp; .js; .shs; .chm; .lnk; .pif; .prc; .url; .smm; .pdf; .msi; .ini; .csc; .cmd; .bas; .eml and .nws.
	只扫描用户指定的档案	只扫描带有用户指定的延伸的档案。 这些档案延伸必须用 “; ” 间隔。
	扫描riskware	扫描riskware 找寻恶意软件 – 找寻病毒以外有恶意的软件。比如：拨号软件，间谍软件，广告程序。找到的恶意软件将被系统当成受病毒感染的文件。选择这选项有可能使运用广告程序的软件无法再正常操作。 选择跳过拨号软件和应用软件扫描如果你想排除这些类型的文件扫描。
扫描启动单元		扫描系统的启动单元
在档案内扫描		被接触过的档案将会被扫描。这一选择会使电脑放慢。
扫描包装档案		所有的包装档案将会被扫描。
第一行动		请从以下措施当中选择一项:
	拒绝通行并继续	如果发现有感染的档案，这会被拒绝通行。
	清理档案	清理受感染的文件。
	删除档案	没有任何警告下立即删除受感染的档案。
	把档案移到检疫处	受感染的档案移入检疫措施。
第二行动		当第一项行动失败后采取的第二项行动 – 当第一项行动失败后，从垂下的菜单选择要对受感染的档案采取的第二项行动。
	拒绝通行并继续	如果发现有感染的档案，这会被拒绝通行。
	删除档案	没有任何警告下立即删除受感染的档案。
	把档案移到检疫处	受感染的档案移入检疫措施。
扫描所有文件。不管什么种类，[x] Kb一律扫描。		不扫描大于xx的档案 – 输入将扫描档案的最大体积。 如果是0KB，所有档案将会被扫描。

选择	说明
不要扫描共享文件夹	如果你选择了这项功能， bitdefender不会扫描网络股，允许更快的网络接入。 我们建议您，让这个选项只有当你的网络的一部分，是受保护的防毒解决方案。

■扫描进入的电邮 – 扫描所有进来的电子邮件。

你可做以下选择:

选择	说明
扫描收到的邮件	扫描所有接收邮件信息。
扫描发出的邮件	扫描所有发出邮件信息。

■扫描网络浏览

■当发现病毒时发出警报 – 当在档案或电子邮件发现病毒时会开启一个警报视窗。

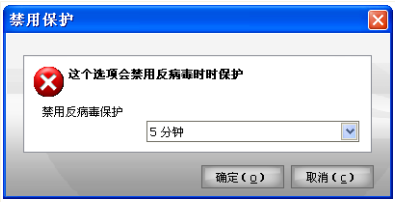
如果是档案感染，警报视窗将包含病毒的名称,它的通道，BitDefender所采取的行动和联接你到可以找到更多的资料的BitDefender网页。 如果是电子邮件感染，警报视窗也将同时包含发送和接收资料.

如果您发现可疑的档案， 你可以从警报视窗启动一个助手帮助你把该档案传给BitDefender实验室作进一步分析。 你可以提供你的电邮地址以索取一份有个关报告。

点击 好的 来保存修改和关闭窗口.

8.1.3. 禁用实时保护

如果你禁用实时保护， 会有警告窗口出现。



禁用实时保护

你必须确认你的选择，选择从菜单多久，你想实时保护被禁用。您可以禁用实时保护为5年， 15年或30分钟，一小时，永久或直到系统重新启动。

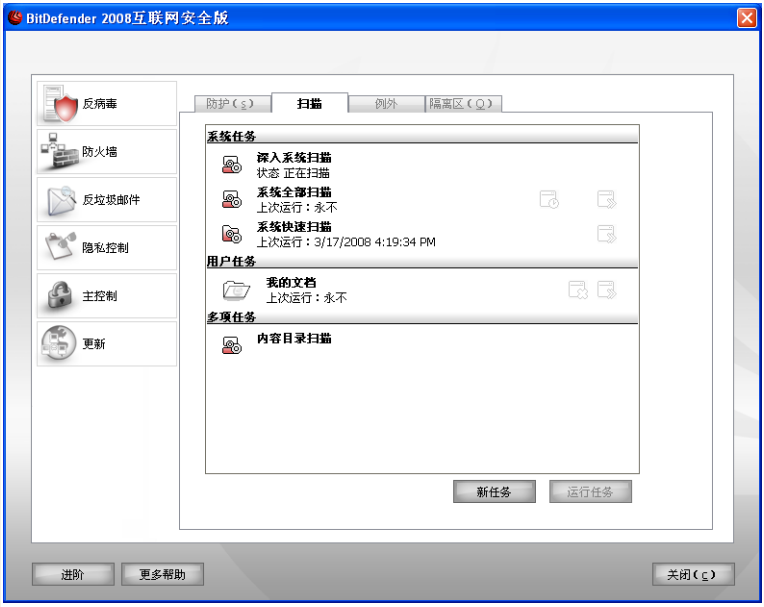
警告
这是一个关键的安全问题。我们建议您禁用实时保护，因为没有时间进行。如果实时保护，是残疾人，你会不会受到保护，免遭恶意威胁。

8.2. 在需要时扫描

BitDefender的主要目标是使你的电脑不受病毒侵害。这首先是通过排除新病毒入侵你的电脑和扫描你的电子邮件信息，并任何下载或复制到你系统的新文件.

在你装置BitDefender前病毒有可能已经在你的系统里了。 因此最好在你装置BitDefender后立即扫描你的电脑。同时最好经常扫描你的电脑检查病毒。

配置并启动对按需扫描，点击 防毒 扫描，在设置控制台。 就会出现下面的窗口：



扫描任务

对按需扫描是基于扫描任务。扫描任务，指明扫描选项和对象都被扫描。 您可以扫描电脑，每当你想通过运行默认的任务还是自己的扫描任务（用户自定义任务） 。您也可以安排他们来说就定期或当系统处于闲置状态，以便不干扰你的工作

8.2.1. 扫描任务

bitdefender还带有一些任务，默认建立的，其中包括共同的安全问题。您也可以创建你自己定制的扫描任务。

欲知更多有关防毒单元的资料， 请查阅“设置扫描任务”（第 53 页）.

扫描任务可分为三种:

■系统任务– 包含默认系统任务。以下是那些任务可用:

默认任务	说明
深度扫描	扫描全部系统 在默认配置，它可以扫描所有类型的恶意软件威胁到你的系统的安全，如病毒，间谍软件，广告软件， rootkit和他人。
完全扫描	扫描整个系统，除了卷。 在默认配置，它可以扫描所有类型的恶意软件威胁到你的系统的安全，如病毒，间谍软件，广告软件， rootkit和他人。
快速系统扫描	扫描 windows，Program Files and All Users文件夹 在默认配置，它可以扫描所有类型的恶意软件，除了rootkit攻击，但不扫描内存，注册表中或cookies

注意

自从深度扫描和完整系统扫描任务分析整个系统，扫描可能需要一段时间。因此，我们建议您在运行这些任务对低优先级或更好的，当你的系统处于闲置状态。

■用户任务 包含用户定义的任务

任务被命名 我的文档 使用这项任务，以扫描重要的当前用户文件夹： 我的文档，桌面 和 启动 。这将保证他们的安全将您的文件，一个安全的工作和廉洁运行的应用程序在启动时。

■多重任务 －包括一系列类型的扫描。这些扫描任务指的是不能在这个窗口上运行的交互扫描类型。用户只可以更改设置，或者查看扫描报告。

有三个任务按钮

■ 附表 －显示选定的任务是如期供后人。点击此按钮打开 性能 窗口， 调度 标签，在那里你可以看到任务调度，并修改它。

■ 删除 删除所有任务

注意

对系统任务无效。用户无法移动系统任务。

■ 立即扫描 运行立即扫描 immediate scan.

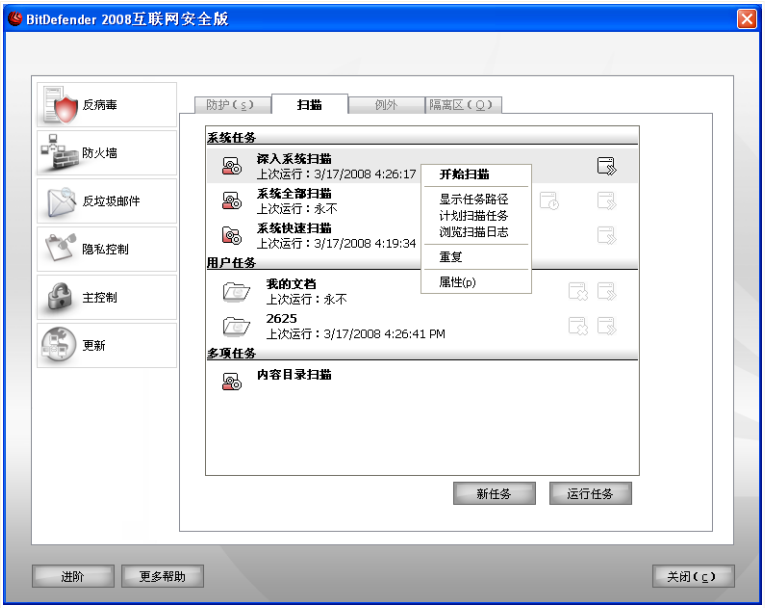
向左边的每项任务，你可以看到 性能 按钮，可让您设定的任务，并查看扫描日志。

8.2.2. 快捷菜单

快捷目录对任何任务都有效. 右击选中目标，并打开文件:

以下命令是可用的快捷菜单

立即扫描 运行这个任务立即开始



快捷目录

■

■改变扫描对象 –打开 性能 窗口， 扫描路径 标签，在那里你可以改变扫描对象的选定工作。

注意
在案件的系统工作，这个选择是取代 查看任务路径 ，因为你只能看到自己的扫描目标

■计划任务 –打开 性能 窗口， 调度 标签，在那里你可以如期选定任务。
■浏览扫描日志 –打开性能 窗口， 扫描日志 标签，在那里你可以看到生成报告后，选定的任务是运行。
■复制 – 复制指定的扫描工作。

注意
建立新任务时这是有效的,因为用户能修改任务副本的设置.

■删除 – 删除指定的扫描工作。

注意
对系统任务无效。用户无法移动系统任务。

■道具–打开 性能 窗口， 浏览Overview 标签，在那里你可以改变设置的选定的任务。

注意
由于特殊的性质以及 杂项任务 类别中，只有 性能 和 查看扫描日志 选项，可在这起案件。

8.2.3. 增加扫描任务

你可以选择以下方法来增加扫描任务：

■复制 现有任务,可进行重命名,在 属性 窗口可进行必要的修改.
■点击 新任务 创建一个新任务并配置。

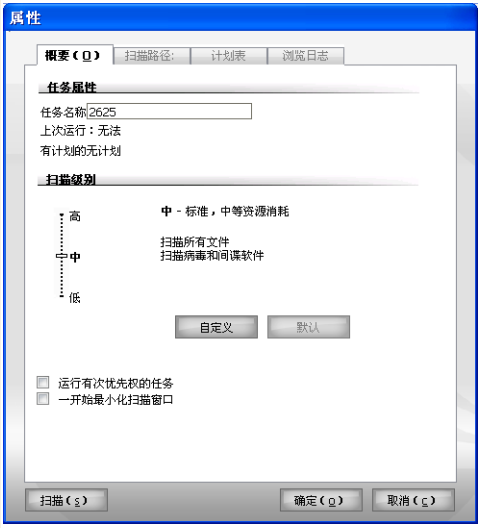
8.2.4. 设置扫描任务

每个扫描任务都有 属性 界面，用户可以设置扫描选项、扫描目标、安排任务或查看扫描报告等。双击任务后即可出现下面的窗口： 如果你想选择另一个文件夹,只需点击 Open打开窗口 选择你要安装BitDefender的文件夹然后点击 打开

注意
欲知更多有关防毒单元的资料， 请查阅“浏览扫描日志” （第 70 页）.

扫描设置

配置更多的扫描任务 选择 道具. 就会出现下面的窗口：



概要

现在您能查看任务信息（名称、最后运行时间和运行状态），并对扫描任务进行设置。

扫描级别

首先，选定扫描级别。通过拖动滚动条以设定合适的扫描级别。

共有3个扫描水平:

防护级别	说明
低	提供基本检测。资源消耗级别较低。 只扫描程序中的病毒。除了经典特征病毒扫描，还使用了启发式分析。对感染文件采取的措施有：清除文件/移至隔离区。
中等	提供较好检测。资源消耗级别中等。

防护级别	说明
	扫描所有文件中的病毒和间谍软件。除了经典特征病毒扫描，还使用了启发式分析。对感染文件采取的措施有：清除文件/移至隔离区。
高	提供高级检测。资源消耗级别较高。 扫描所有文件和文档中的病毒和间谍软件。除了经典特征病毒扫描，还使用了启发式分析。对感染文件采取的措施有：清除文件/移至隔离区。

下列扫描程序常用选项也很有用：

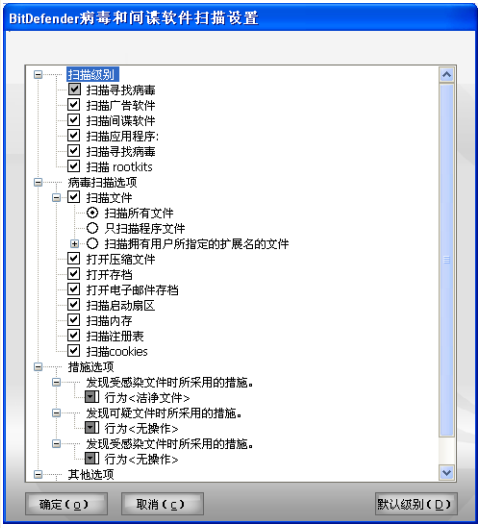
选择	说明
指派低优先任务	调低扫描过程的优先性。 你可让其他程式高速度
缩小扫描窗口	把扫描视窗缩小到系统托盘上。 双点BitDefender的图标打开。

按 好的 以储存改变，或按 预设 以打开预设的设定.

定制扫描级别

先进用户可以利用BitDefender提供的扫描– 设定。这个扫描设定可以跳过那些你知道是无害的的档案延伸、目录或档案。这可大大减少扫描时间,提高你的电脑在扫描时的反应。

点击 设置 – 打开在隔离区的高级选项。以下的视窗将会出现：



扫描设定

扫描选择的以扩大的菜单方式呈现，非常类似视窗。 按"+"的格子以打开选择或 “–” 的格子以关闭打开的选择。

扫描分为四类选择:

- 扫描级别
- 病毒扫描选项
- 行动
- 其他

- 选定将扫描对象的类别 (档案、电子邮件信息等)和其他的选择。 这是通过选择一些 扫描选择 类别。

  你可做以下选择:

选择	说明
扫描病毒	扫描内存以检测已知间谍软件的威胁。

选择	说明
	bitdefender侦测到不完整的病毒机构，也因此消除了任何可能的威胁，可能影响您的系统的安全性。
扫描广告	找寻恶意软件 – 找寻病毒以外有恶意的软件。比如: 拨号软件，间谍软件，广告程序。找到的恶意软件将被系统当成受病毒感染的文件。选择这选项有可能使运用广告程序的软件无法再正常操作。
扫描间谍软件	扫描已知间谍软件的威胁。检测档案，将被视为感染。
扫描应用程序	扫描应用程序 .exe and .dll files
扫描拨号器	找寻恶意软件 – 找寻病毒以外有恶意的软件。比如: 拨号软件，间谍软件，广告程序。找到的恶意软件将被系统当成受病毒感染的文件。选择这选项有可能使运用广告程序的软件无法再正常操作。
扫描的rootkit	扫描隐藏对象（档案及工序），一般称为rootkit攻击。

■选定将扫描对象的类别 (档案、电子邮件信息等)和其他的选择。 这是通过选择一些 扫描选择 类别。

你可做以下选择:

选择		说明
扫描	扫描所有档案	无论类别扫描全部被访问的文件。
	只扫描程式档案	Only the program files will be scanned. This means only the files with the following extensions: exe; bat; com; dll; ocx; scr; bin; dat; 386; vxd; sys; wdm; cla; class; ovl; ole; exe; hlp; doc; dot; xls; ppt; wbk; wiz; pot; ppa; xla; xlt; vbs; vbe; mdb; rtf; htm; hta; html; xml; xtp; php; asp; js; shs; chm; lnk; pif; prc; url; smm; pdf; msi; ini; csc; cmd; bas; eml and nws.

选择	说明
只扫描用户指定的档案	只扫描带有用户指定的延伸的档案。 这些档案延伸必须用 “; ” 间隔。
打开后台项目	扫描后台文件
打开档案	扫描内部的档案。
打开电子邮件	扫描邮件内的档案。
扫描启动单元	扫描系统的启动单元
扫描内存	扫描内存以发现病毒和其他恶意软件。
扫描注册表	扫描注册表
扫描cookies	扫描cookies包。

■具体说明将采取的行动就被感染，可疑的或隐藏文件，发现在 行动选项 类别。你可以指定一个不同的行动，为每个类别。

・选择所要采取的行动对受感染的文件。 你可做以下选择:

行动	说明
没有日志	不对受感染的档案采取任何行动。 这些文件将提交的报告中出现。
杀毒文件	清理受感染的文件。
删除档案	没有任何警告下立即删除受感染的档案。
移动文件到隔离区	受感染的档案移入检疫措施。

・选择所要采取的行动对可疑文件 你可做以下选择:

行动	说明
没有日志	不对受感染的档案采取任何行动。 这些文件将提交的报告中出现。
删除档案	直接删除可疑的文件不需要警告。
移动文件到隔离区	移动可疑的文件到隔离区。

注意
档案，如发现有可疑的，由启发式分析。我们建议您将这些文件到bitdefender实验室。

- 选择所要采取的行动就隐藏对象（的rootkit ）侦破。 你可做以下选择:

行动	说明
没有日志	不对受感染的档案采取任何行动。 这些文件将提交的报告中出现。
移动文件到隔离区	移动隐藏文件到隔离区。
有形的	显示隐藏文件，让你可以看到它们。

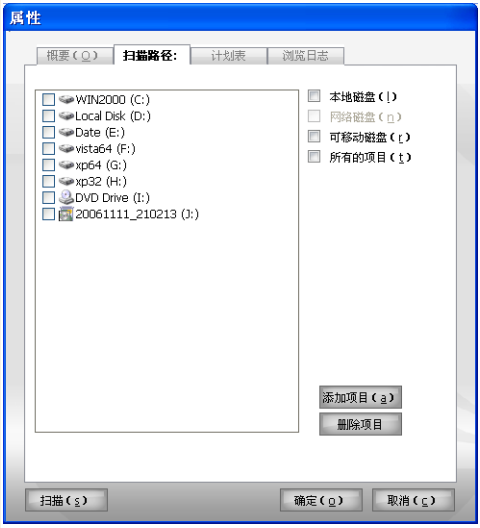
注意
如果你选择忽略了检测档案，或者如果选择的行动失败，你都必须选择自己的一个行动，并在扫描向导。

■为了促使递交所有可疑文件到bitdefender实验室后，扫描过程完毕后，检查提交嫌疑人档案，以bitdefender实验室 在其他选项类别。

如果您单击 默认 默认值将会载入。 点击 好的 来保存修改和关闭窗口.

设置扫描目标

当你不再想观看图像显示，只要右点击然后选择 隐藏 就会出现下面的窗口：



扫描目标

你可以看到，名单上的地方，网络和可移动驱动器以及文件或文件夹补充说：以前，如果有的话。所有检查项目，将被扫描时，运行任务。

这个环节包含以下按钮:

■增加档案 – 打开一个可以浏览和选择你想扫描的档案的视窗。

注意
您也可以使用拖放添加文件/文件夹，在该份名单。

■删除 – 删除先前已选定将扫描的档案/文件。

注意
只有随后又增加的档案/文件，可以删除，但不是那些自动出现在BitDefender的.

除了按钮以上所解释的，也有一些选项，能快速选择扫描的位置。

■随机驱动器 – 扫描随机驱动器。
■网络驱动器 – 扫描所有的网络驱动器。
■可拆除驱动器 – 扫描可拆除驱动器(光碟，软碟等)。
■所有 – 扫描所有驱动器，无论是本机、网络或拆除可拆除驱动器

注意
如果你想你扫描整个电脑，选择相应全部的格子.

按 好的 以储存改变，或按 预设 以打开预设的设定.

看扫描的目标系统任务

你不能改变扫描对象的扫描任务，从 系统任务category 类别。 您能看到扫描目标。

要查看扫描目标的一个具体的系统扫描任务中，右击任务，并选择 查看任务路径. 深系统扫描 – 例如，所有的窗口：

深扫描目标

全面的系统扫描 和 深系统扫描 ，将扫描所有的本地驱动器，而 快速系统扫描 ，将只扫描 窗口 和 程序文件 文件夹

点击 OK 来关上视窗。 要运行任务 点击 扫描.

扫描任务安排

与复杂的任务，扫描过程将需要一些时间，而且会工作，你最好关闭所有其他程序。这就是为什么它是最适合你如期进行此类任务的时候，你是不是用你的电脑和资讯科技已进入空闲模式。

见附表的特定任务或修改它，右击任务，并选择 计划任务. 就会出现下面的窗口：

调度程式

你可以看到任务调度，如果有的话。

任务运行时间确定后,用户必须选择下列选项之一:

■不能如期 –发射任务，只有当用户请求。
■一次 –发射扫描只计算一次，在某一个时刻。指定起始日期和时间，在 开始日期/时间 领域的合作。

■定时性 – 从指定的时日开始，在您订下的时日定时性（每小时，每天，每周，每月，每年）地扫描系统。

如果你想要扫描加以重复的，在一定的时间间隔，选择 定期 和类型在 在每一个编辑框中的分钟数/小时/天/周/月/年，显示频率这一进程。您还必须指定起始日期和时间，在 开始日期/时间 领域的合作。

按 好的 以储存改变，或按 预设 以打开预设的设定.

8.2.5. 扫描对象

然后你开始一项扫描过程中，你必须确保bitdefender ，是截至目前为止，与它的恶意代码签名。扫描你的电脑上用一个过时的签名数据库，可以防止bitdefender从检测新的恶意攻击，发现自从上一次更新。核实当最后一次更新是在演出中，单击 更新，在设置控制台。

注意

为了能让BitDefender完全的扫描,你必须关闭所有的程式，尤其是你的电子邮件客户(如Outlook，Outlook Express 或 Eudora)必须关闭。

扫描方式

BitDefender允许四种需求扫描

■立刻扫描 – 扫描系统和用户任务;
■上下文扫描 –右键点击一个文件或文件夹，并选择BitDefender反病毒2008。
■拖放下拉扫描 –拖放文件或文件夹在 扫描工具条
■手动扫描 –使用bitdefender手动扫描，以直接选取文件或文件夹被扫描。

立刻扫描

使用默认扫描人或创建自定义扫描任务可进行全面或局部扫描.建立扫描任务的方法有两种: 立刻扫描

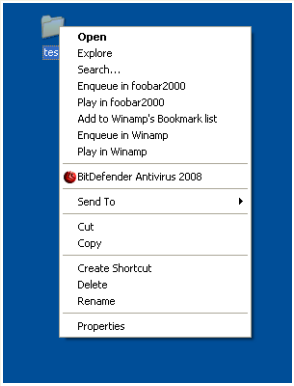
你可以选择下列任何一个行动:

■双击期望的扫描任务，在名单上。
■点击 现在扫描 按钮对应执行这项任务。
■双击选定一个任务，再点击扫描。

bitdefender扫描器将出现并扫描将着手。 更多信息 请翻阅 “BitDefender 扫描”（第 66 页）.

指定扫描

扫描一个文件或文件夹，如果没有设定一个新的扫描任务时，您可以使用上下文菜单。 这是指定扫描



指定扫描

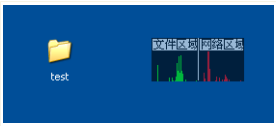
右键单击文件或文件夹，你不想被扫描，并选择 BitDefender反病毒2008

bitdefender扫描器将出现并扫描将着手。 更多信息 请翻阅 “BitDefender 扫描”（第 66 页）.

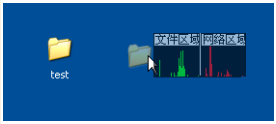
您可以修改扫描选项，看看该报告档案进入 性能 窗口的 上下文菜单扫描 的任务。

拖放扫描

拖动文件或文件夹，你想将扫描和下降，它比 扫描活动 ，如下图所示。



拖放文件



删除文件

bitdefender扫描器将出现并扫描将着手。 更多信息 请翻阅 “BitDefender 扫描”(第 66 页).

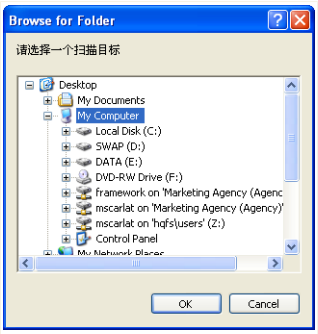
手动扫描

手动扫描构成直接选拔对象将扫描使用bitdefender手动扫描选项，从bitdefender程序组，在开始菜单。

注意
手动扫描是非常有用的，因为它可以演出时，窗口工程，在安全模式下也是如此。

选拔对象当作扫描bitdefender ，在Windows开始菜单，走开始 → 节目 → bitdefender 2008 → bitdefender手动扫描.

就会出现下面的窗口：



手动扫描

选择对象，你想将扫描和点击好的.

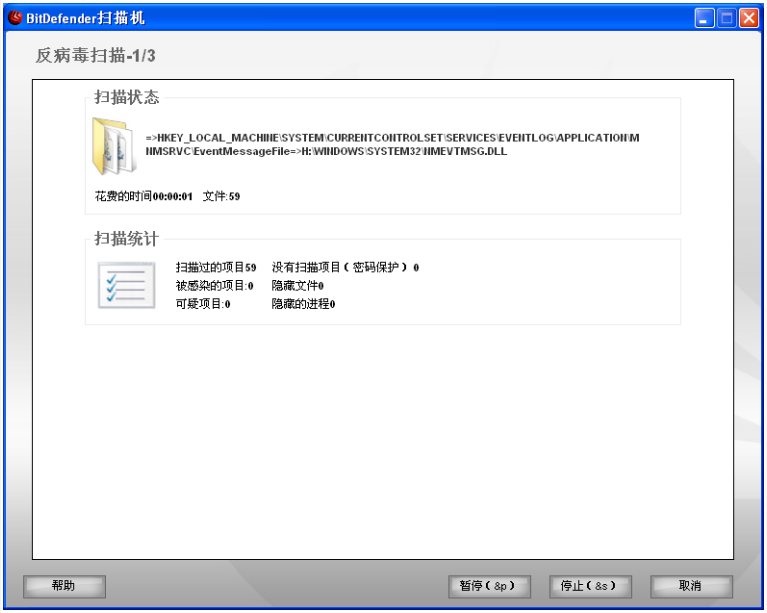
bitdefender扫描器将出现并扫描将着手。 更多信息请翻阅 “BitDefender 扫描” （第 66 页）.

BitDefender 扫描

当你开始一种按需扫描过程中， bitdefender扫描器就会出现。 遵循三个步骤的引导程序来完成扫描过程。

步骤1/3 — 正在扫描

Bitdefender正在开始扫描选定项目。



正在扫描

你可以看到扫描的地位和统计（扫描速度，经过时间，有多少扫描/感染/可疑/隐藏物体及其他） 。

注意
这可能需要一段时间,取决于你硬盘的大小。

暂停扫描 点击 暂停 你可以点击 继续 继续扫描

你可以在任何时候停止扫描 点击 停止 是的 . 直接点击对话框。

等待Bitdefender扫描完成

步骤2/3 — 选择动作

当扫描完成后，一个新的窗口将出现，在那里你可以看到扫描的结果。

行动

你可以看到，在一些问题，影响你的系统。

受感染的物体都张贴在集团的基础上，他们的恶意软件感染。 点击链接所对应的一个威胁，以了解更多有关受感染物体。

您可以选择一个整体将要采取的行动，为每个小组的问题，或者你可以选择单独行动，为每一个问题。

你可做以下选择:

行动	说明
没有行动	没有察觉受感染的文件
杀毒	清理受感染的文件。
删除	删除受感染的文件

行动	说明
未隐藏	隐藏条目

点击 继续 应用特殊的行动

步骤三 — 查看结果

当bitdefender饰面操纵问题，扫描的结果将出现一个新窗口。

总结

您能看结果总结。 Logs section from the Properties报告会自动保存

重要
如有需要，请重新启动系统以完成清除过程。

点击 退出 来关闭窗口。

bitdefender未能解决的一些问题

在大多数情况下， bitdefender成功消除受感染的文档或者隔离受感染的文档。 是，有些问题不能得到解决。

在这些情况下，我们建议您联络bitdefender支持团队www.bitdefender.com. 我们的技术支持人员将帮助您解决问题。

Bitdefender侦查密码保护项目

密码保护的类别包括两种类型的项目：文档和安装。 他们没有提出一个真正的威胁系统的安全性，除非它们含有受感染的文件仅仅执行。

确保这些项目都是要清除的：

- 如果密码保护项目保护密码，分开扫描。 最简单的方法来扫描是按右键，并选择BitDefender反病毒2008 菜单。
- 如果密码保护的项目被安装，确保 实时保护 在你启用安装之前。 如果安装被感染， bitdefender将检测和隔离感染源。

如果你不想让这些文件再次被bitdefender发现你必须将它们添加到扫描例外。 添加扫描例外，点击 设置 打开设置控制台Antivirus > Exceptions 反病毒例外。 更多信息，请提及文件例外扫描。.

Bitdefender检测怀疑文件。

嫌疑人文档被启发式分析发现，潜在的感染了恶意代码但并没有被释放。

如果嫌疑人档案被发现在扫描期间，你会被要求提交给bitdefender实验室。 点击好的 发送这些文件到bitdefender实验室做分析。

8.2.6. 浏览扫描日志

当你想看结果，只要右点击然后选择 浏览扫描日志. 就会出现下面的窗口：

扫描日志

在这里你可以看到报表文件生成的每一次任务执行过期。

现在您可以查看每次任务运行时产生的报告文件.每个文件上都附有其状态信息(清除/感染),日期,扫描运行的时间及小结(扫描完成).

二个按钮可用

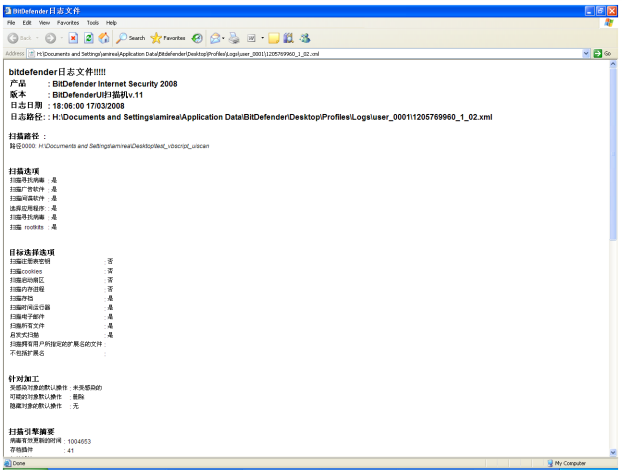
■删除日志 – 删除选中的扫描日志;
■显示日志 – 打开选中的扫描日志; 扫描日志, 会打开你的默认浏览器。

注意
此外,要查看或删除一个文件,右击文件,在快捷目录中选定相应的选项.

按 好的 以储存改变, 或按 预设 以打开预设的设定.

扫描日志例子

以下数字代表了一种典型的扫描日志:



扫描日志例子

扫描日志包含的详细资料登录扫描过程中，如扫描选项，扫描目标，我们发现威胁，并采取行动，对这些威胁。

8.3. 部分不扫描

有些案件的时候，你可能需要排除某些文件的扫描。例如，你可能想排除一个eicar测试文件，从按访问扫描或。.AVI 档案从对按需扫描。

bitdefender允许扣除的对象，从按访问或按需扫描，或从两者。这项功能是为了减少扫描时间，以及避免干扰你的工作。

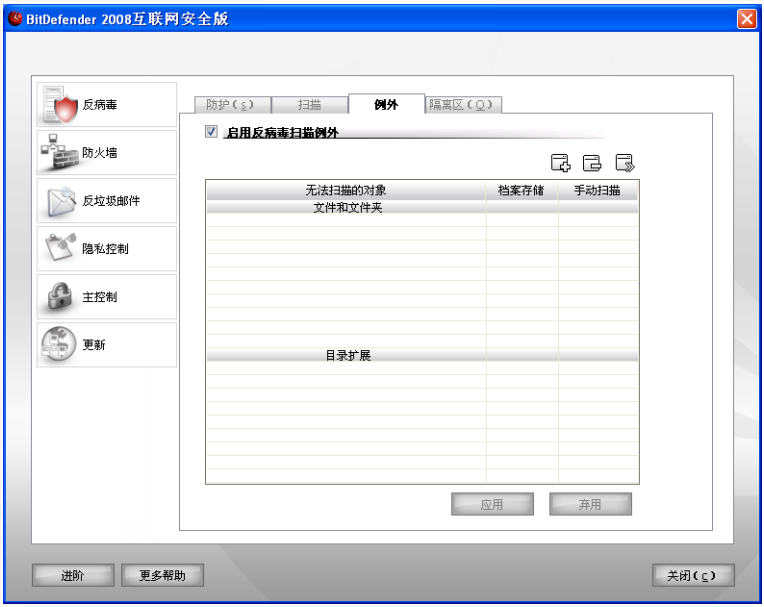
两种类型的对象可以被排除扫描:

- 路径 –文件或文件夹（包括所有的物体，它包含）表示，由指定的路径将被排除扫描。
- 延长–所有的档案有一个具体的延长将被排除扫描。

注意

该物体被排除在按访问扫描，将不会扫描，不管他们是进入你，或由一个应用。

看到和管理对象排除扫描，点击 防毒 例外 ，在设置控制台。 就会出现下面的窗口：



除外

你可以看到对象（文件，文件夹，扩展）是不受扫描。对于每个物体，你可以看到，如果它被排除在按访问，按需扫描或两者兼而有之。

注意
例外指定这里，将不适用于对来龙去脉扫描。

从名单削除项目，选择它和点击 删除 按钮。

要编辑条目从表中，选择它，并点击 编辑 按钮。 一个新的窗口将出现在你可以改变或延长道路被排除和类型的扫描你希望他们被排除，按需要发放。作必要的修改，然后点击 好的.

注意
您也可以右键点击一个对象，并使用该方案对快捷菜单进行编辑或删除。

您可以点击 抛弃 回复所作的修改，以法治表，只要你没有救他们通过点击 应用.

8.3.1. 拒绝扫描路经

排除路径扫描，请点击 添加 按钮 您将被引导的过程中，不包括路径扫描所配置向导就会出现。

步骤1/3 — 选择类型

类型

选择扫描路经

点击 下一步.

步骤2/3 — 指明排除路经

排除路经

指明了路子，被排除在扫描使用以下任一方法：

- 单击 浏览，然后选择要被阻止的应用程序，最后单击 添加.
- 键入路径，你不想被排除在扫描在编辑领域和点击 添加.

注意
如果提供的路径并不存在，一个错误讯息将出现。点击 好 ，并检查路径的有效性。

路径将出现在桌上，作为你加入他们。您可以添加很多的路径，因为你想要的。

从名单削除项目，选择它和点击 删除 按钮。

点击 下一步.

步骤3/3 — 选择扫描类型

扫描类型

你可以看到一个表，包含了路经，被排除在扫描以及采用何种扫描他们被排除。

默认情况下，选定的路径被排除在双方对访问和对按需扫描。改变时，以申请例外，点击右边一栏，并选择理想的选择，从名单上。

点击 Finish.

单击 应用 来保存修改。

8.3.2. 不包括扩展扫描

排除扩展扫描，请点击 添加 按钮。 您将被引导的过程中，不包括扩展扫描所配置向导就会出现。

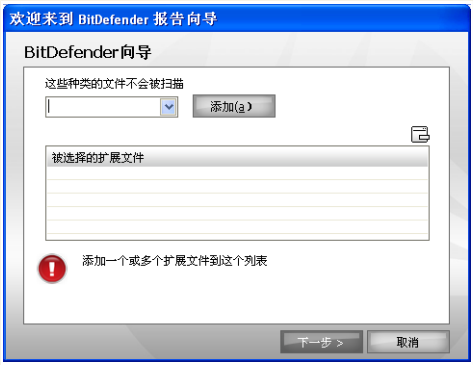
步骤1/3 — 选择类型

类型

选择不含有效期由扫描。

点击 下一步.

步骤2/3 — 排除扩展



排除扩展

明延被排除在扫描使用以下任一方法：

■选择从菜单中的扩展，你不想被排除在扫描，然后再点击 添加.

注意
该菜单包含列出了所有的扩展注册您的系统。当您选择延期，你可以看到它的描述，如果有的话。

■类延说，你不想被排除在扫描在编辑领域和点击 添加.

扩展功能将出现在桌上，作为你加入他们。你可以添加了许多扩展，因为你想要的。

从名单削除项目，选择它和点击 删除 按钮。

点击 下一步.

步骤3/3 — 选择扫描类型

扫描类型

你可以看到一个表，其中载有扩建工程被排除在扫描以及采用何种扫描他们被排除。

默认情况下，选定的扩展是被排除在双方对访问和对按需扫描。改变时，以申请例外，点击右边一栏，并选择理想的选择，从名单上。

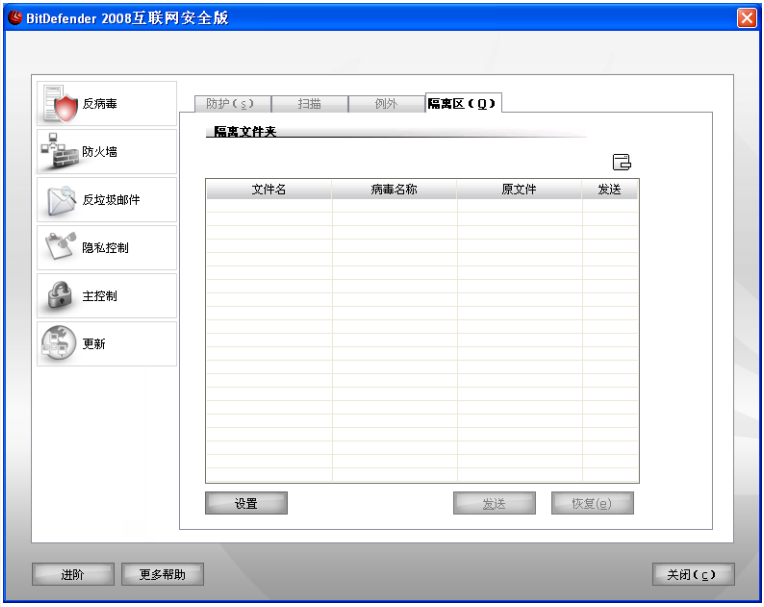
点击 Finish.

单击 应用 来保存修改。

8.4. 隔离区

BitDefender允许隔离被感染的或是可疑的文件到一个安全的区域。通过隔离这些文件到隔离区，被感染的危险将会消失，同时您有责任把这些文件发送给BitDefender实验室作进一步的研究。

看到和管理被隔离的文件和配置检疫设置，请点击 防毒 ，在设置控制台。



隔离区

8.4.1. 管理隔离文件

可能您已经注意到了，在 隔离区 界面中有一个含有所有被隔离的文件的列表。每一个列表栏中，有被隔离的文件的名字，大小，隔离时间和提交时间。 如果您想要查看有关的被隔离的文件的更多信息，请单击 更多信息.

注意
当一个病毒被隔离在隔离区内，他就不可以再危害系统。因为它不可以运行或被阅读。

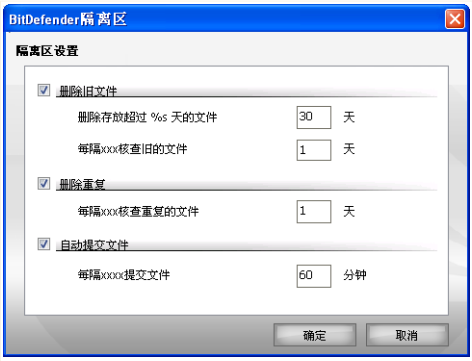
删除选定的文件从检疫，点击 除去 按钮。如果您想恢复选定的文件到原来的位置，按一下 恢复.

点击发送可以将隔离区内任何选定的文件发送到BitDefender实验室.

指定菜单. 上下文菜单，可让你管理被隔离的文件很容易。相同的选项，因为这些前面提到的数据。您也可以选择 刷新 刷新检疫科。

8.4.2. 隔离区设置

配置隔离区域 点击 设置. 会有一个新的窗口出现



隔离区设置

利用检疫设置，你可以设置bitdefender自动履行下列行动:

删除旧文件. 自动删除旧被隔离的文件，选中相应的选项。 你必须要指定的天数后，其中被隔离的文件应予以删除和频率与bitdefender应检查的旧文件。

注意
默认情况下， bitdefender将检查旧档案，每天和删除文件老年人超过10天。

删除复制. 自动删除重复隔离的文件，选中相应的选项。 你必须明确的间隔天数连续两次检查重复的。

注意
默认情况下， bitdefender将检查重复隔离的档案每一天。

自动提交文件. 动提交被隔离的文件，选中相应的选项。 你必须要指定频率与提交的文件。

注意
默认情况下， bitdefender将自动提交被隔离的文件，每60分钟。

点击 好的 来保存修改和关闭窗口.

9. 防火墙

电脑防火墙保护避免擅自进出的联接尝试。 这是一个类似在你门口守卫--它将密切注视和确保谁可以连接互联网

注意
如果你有宽频或数字用户线路，防火墙是必不可少的。

在秘密模式中,将对恶意软件和黑客隐藏用户电脑.防火墙模块能自动发现和防护端口扫描(通常黑客准备攻击电脑前,会对电脑发送许多程序包以发现"进入点").

这个用户向导里的防火墙 部分包含以下论题:

■防火墙识别
■防火墙状态
■流量保护
■高级设置
■防火墙活动
■网络区

9.1. 防火墙的见解

bitdefender防火墙设计，以提供最佳的保护您的网络/互联网连接，如果没有，你不必配置它。不管你是直接连接到互联网上，以一个单一的网络或几个网络（以太网，无线， VPN或其他网络型） ，要么亲信或来路不明的，防火墙将自我配置，以适应相应的情况。

默认情况下， bitdefender自动检测网络配置您的计算机上，它创造了一个适当的基本防火墙简介。这也增加了检测网络，以知名度作为可信任或来路不明的网区，这取决于它们的配置。

9.1.1. 什么是防火墙的好处?

防火墙剖面是一套规则，控制应用网/互联网接入。

依靠网络配置您的计算机上， bitdefender自动创建一个特定类型的档案。基本概况创建包含网路存取规则或初等上网规则，所需要的系统应用和bitdefender组件。

注意
一个单一的防火墙档案建立后，不管有多少，你的网络连接了。

有3 类型好处:

好处	说明
直接地连接到互联网	包含初等上网规则推荐一个网络配置，使直接接入互联网。 规则不容许任何网络用户访问您的计算机，或者您浏览网络。
没被信任的地区网络	包含网路存取规则，建议为网络配置与一个不可信的网络。 规则允许你浏览网络，但防止其他网络成员访问您的计算机。
被信任的地区网络	包含网路存取规则，建议为网络配置相关的一个值得信赖的网络。 没有限制，是强加给网络接入。这意味着你必须进入网络共享，网络打印机和其他网络资源。在同一时间内，网络成员可以连接到您的计算机，并接入您的股票。

作为应用程序试图连接到网际网路，适当的规则被添加到档案。 您可以选择允许或拒绝默认接入因特网的申请，其中的规则没有得到配置，或者仅允许whitelisted申请，由违约，并要求准许进行有关的其他应用领域。

注意
具体准入政策，为应用程序尝试连接到互联网，为第一时间，去到 状态 节并设置保护级别。 要编辑现有的简介，去到 流量 ，并点击 编辑简介

9.1.2. 什么是网络区

网络区代表了计算机内部网络或整个网络是完全孤立的，从你的计算机或者相反的，可以侦测到你的电脑，并连接到它。实际上，一个区是一个IP地址或一系列的IP地址是允许还是拒绝进入你的电脑。

默认情况下， bitdefender自动添加区为特定的网络配置。一个区，是补充，通过建立一个适当的网络访问规则，适用于整个网络，在目前的概况。

有2 类型区域:

区域类型	说明
被信任的地区网络	电脑从一个可信任的区可以连接到您的计算机，并可以连接到他们。 所有连接尝试从这样一个区域，以及所有的连接尝试从您的电脑这样一个区，是不允许的。 如果一个网络，增加一条，作为可信任区，你可以不受限制地查阅网络共享，网络打印机和其他网络资源。同时，网络成员可以连接到您的计算机，并接入您的股票。
没被信任的地区网络	电脑从一个不可信区不能连接到电脑，你不能连接到这些政策和制度。 所有连接尝试从这样一个区域，以及所有的连接尝试从您的电脑这样一个区都堵住了。 由于ICMP的交通是否认和隐形模式被激活，你的电脑几乎是看不见的，为计算机在这一带。

注意

要编辑区域，去区域部分 编辑法治相应的一个区，然后向 交通，并点击 编辑简介

9.1.3. 防火墙操作

当重新启动系统安装完毕后， bitdefender会自动侦测你的网络配置，创造一个适当的基本概况，并加入带视检测网络。

注意

如果你直接连接到互联网，没有网络，是开发区创造了相应的网络配置。 如果您连接到一个以上的网，带，加上取决于各自的网络。

每一次网络配置的变化，无论您连接到另一个网络，或者您禁用网络连接，一个新的防火墙剖面产生了。在同一时间内，该网络区相应的改动。

当一个新的防火墙档案建立后，旧的档案保存起来，以便有需要时可重装上阵时，你回去给其相应的网络配置。

依赖于网络配置， bitdefender将配置本身。 这是bitdefender防火墙默认配置:

- 如果你直接连接到互联网上，无论你也是连接到其他网络，直接连接剖面产生了。否则， bitdefender创建一个不可信的防火墙简介。

注意

作为一种安全，可信赖的档案是不是默认建立的。 创造一个可信任的档案，你必须复位现行档案。如需更多资讯，请参阅 “修改文档” （第 97 页）.

■区是补充依赖于网络配置。

区域类型	网络配置
被信任的地区网络	私有IP ，没有门户 –电脑的一个组成部分，局域网（ LAN）和不连接到互联网。 例子，这种情况是一个家庭网络创造了让家庭成员共享文件，打印机或其他资源。
	私有IP与域控制器侦破 –电脑的一个组成部分，局域网，并连接到域。 例子，这种情况是指一个办事处网络，允许用户共享文件或其他资源的内域。 网域意味着存在一套政策与哪一位电脑遵守。
没被信任的地区网络	打开（不担保）无线 –电脑的一个组成部分，无线区域网路（ W LAN） 。 例子，这种情况是当你接入互联网使用免费接入点，从公共场所。

注意

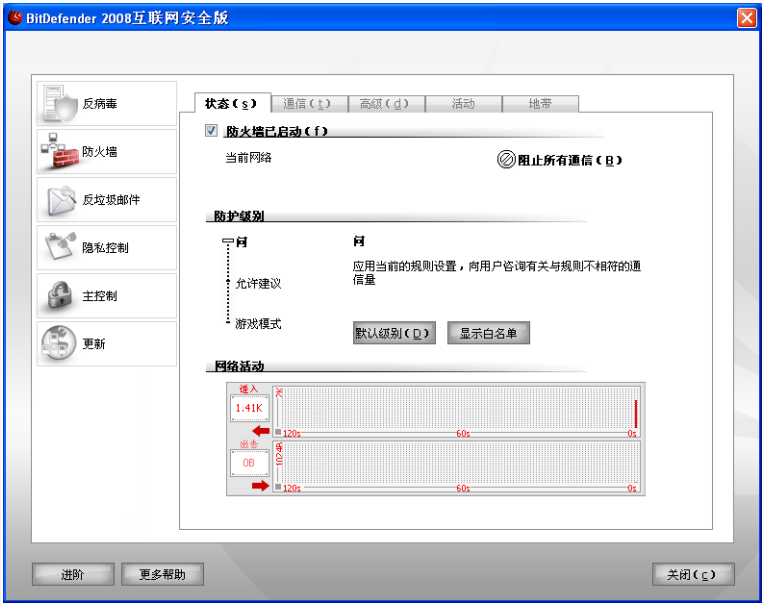
区本身并不是造成一些网络配置，例如：

- 公网的IP –电脑是直接连接到互联网。
- 私有IP网关，但没有域控制器侦破 –电脑的一个组成部分，蓝鸿震，没有一个组成部分域太大，它可以连接到互联网上通过一个网关。 例子，这种情况，是一所学校的校园网，允许用户共享文件或其他资源。

■隐形模式被激活。
■VPN和路由连接被允许
■Internet连接共享是不允许用于来路不明区。
■whitelisted申请自动获准进入，而对于其他应用程序，你将被要求批准他们第一次尝试连接。

9.2. 防火墙状态

配置防火墙保护，点击 防火墙 状态，在设置控制台。 就会出现下面的窗口：



防火墙状态

在这个部分您能使用/使无能力防火墙，阻拦所有network/internet 交通和设置缺省行为在新事件。

重要
请保持防火墙 启以防止网路攻击

Block Traffic and then 好的 to confirm your choice. 得到保护，对互联网攻击，保持 防火墙 启用了。

从名单削除项目，选择它和点击 移除 . 按钮。

在底下部分您能看BitDefender 统计关于接踵而来和外出的交通。图表显示互联网话务量在前二分钟期间。

注意
图表出现既使 防火墙 是解除的。

9.2.1. 配置防护级别

您可以选择最符合您的防护需要的安全级别.上下拖动滚动条以设定最合适的防护级别。

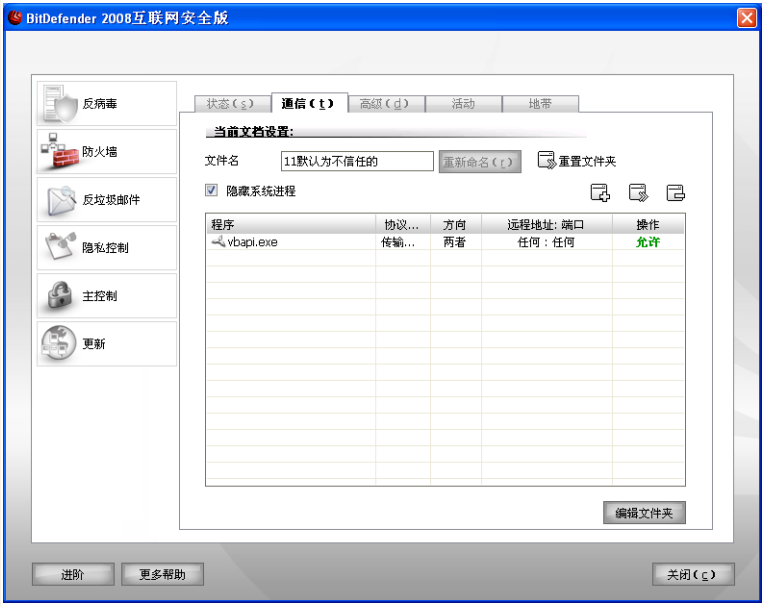
共有3个安全级别:

防护级别	说明
游戏模式	适用于目前的规则，并允许所有车辆的企图不符合任何现行规则没有提示。 这项政策是极力劝阻，但也可能是有用的，为网络管理员和玩家
允许	允许所有通过程序尝试拨出的连接，这些连接必须是BitDefender杀毒软件认定为合法的。您能看到在 流量 环节中形成的流量规则。 白名单程序是全世界最常用的应用程序.它们包括最常见的网页浏览器、视听程序、图像播放器、聊天软件和文件共享程序，以及服务器客户和操作系统程序。 如果你想看看哪个节目是whitelisted ，点击 显示白名单.
问	适用于目前的规则，并征询大家对所有车辆的企图不符合任何现行规则。

点击 默认级别 设置缺省政策（允许推荐).

9.3. 流量控制

管理防火墙规则的现行档案中，点击 防火墙 交通，在设置控制台。 就会出现下面的窗口：



流量控制

可以允许或否认哪些进出的连接。 定立有关门户、应用程式和/或远程地址的规定。

规则可能自动地(通过警惕的视窗) 或手工输入点击 添加 按钮和选择参量为规则。

9.3.1. 自动添加规则

与 防火墙 使用，每当与互联网的联系被建立，BitDefender将请求您的允许:

防火墙警告

您能看以下：设法访问互联网、协议 地址和应用软件设法连接的 端口。

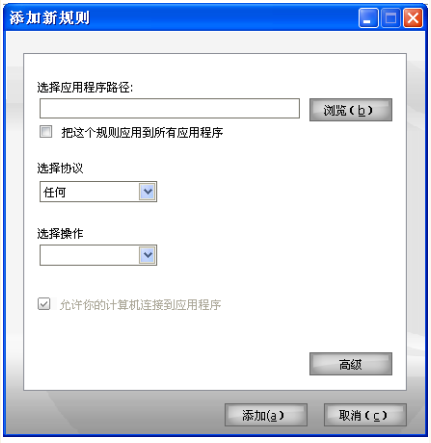
点击 允许 ，让所有交通（呼入和呼出）上产生的这种应用，从本地主机向任何目的地，在各自的IP协议，并在所有港口。如果你点击 阻止，申请将被拒绝进入互联网超过各自的IP协议完全。

根据你的回答，一项规则，将可创造，应用和列于附表。未来时间的应用会试图连接，这条规则将适用于默认。

重要
允许入站连接企图只从您明确地信任的IP’s或您明确地信任的域名。

9.3.2. 人工添加规则

点击 添加规则 按钮和选择参量为规则。 就会出现下面的窗口：



添加规则

请跟随以下一步骤为你的电脑扫描病毒:

1. 选择应用程序，为把新的防火墙规则，将可创造。

   要选择一个应用程序，点击 浏览 中，找到它并点击好的.

   如果你想创造一个规则，所有申请，只是检查适用本规则的所有申请.
2. 选择议定书，其中规定将适用。

   一张名单以最共同的协议有时间帮助您选择唯一具体协议。选择指定的协议(在哪些规则运用）从对应的下Menu单或选择 任何 选择所有协议。

   下表列出了协议，你可以选择随简短描述每个:

协议	说明
ICMP	网际控制信息规约– 是引伸对互联网协议(IP) 。ICMP 支持数据包包含错误、控制，和新闻消息。PING 命令，例如，使用ICMP 测试互联网连接。
TCP	TCP（传输控制协议）使二个主机建立连接并且交换数据. TCP保证数据交付并且保证那数据包将被交付在他们被送的同样次序。

协议	说明
UDP	UDP（用户数据协议）是基于IP 的运输被设计为高性能。游戏和其他录影根据 也使用UDP.

3. 如果要选择其中一项，请在相应的格子打勾。

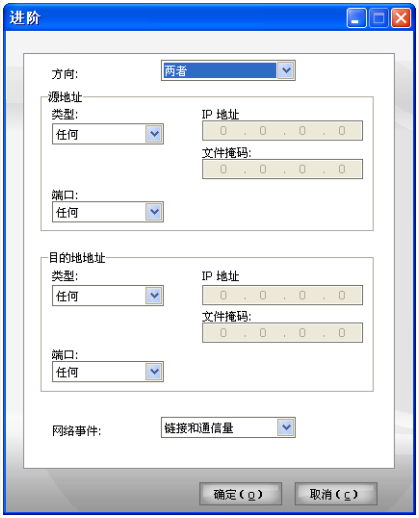
行动	说明
准许	指定的申请将被允许网络/互联网接入，根据指定的情况下。
拒绝	指定的申请将被拒绝网/互联网接入，根据指定的情况下。

4. 如果先前选定的协议是TCP或UDP时，你可以指定规则是否将适用于申请时，它可以作为一台服务器或不是。

   检查 让其他电脑连接到这个应用 适用于行动，所有的网络事件。含蓄，你会允许或拒绝这项申请的权利，以开放口岸。

   如果你想申请的行动只以交通为UDP数据及交通&连接的TCP ，分别明确了相应的复选框。

你们将被要求确认你选择点击 高级. 一个新窗口就会出现让你可以选择:



高级规则设置

你可以配置下列任何一个行动:

■方向–选择交通方向发展。

类型	说明
外出	规则申请只外出的交通。
进入	规则申请只入局通信量。
都是	规则申请在同方向。

■源地址 特殊的源地址

明源地址，选择地址类型，从菜单，并指定了所需的数据。 你可做以下选择:

类型	说明
任何	规则应用任何源地址。
主机	规则允许这个主机地址。 你必须键入IP地址的主机。

类型	说明
网络	规则允许特殊源网络。 你必须键入IP地址和子网掩码的网络。
本地主机	规则允许本地主机。 如果你使用一个以上的网络界面，选择从菜单中的网络界面，这条规则同样适用。如果你想要使用规则适用于所有本地主机中，选择 任何.
本地网络	规则允许本地网络。 如果您连接到一个以上的网络中，选择从菜单中的网络，这条规则同样适用。如果你想要使用规则适用于所有本地网络中，选择 任何.

如果你已经选择了TCP或UDP作为议定书您可以设置一个特定的港口或射程介于0和65535 。如果你想要使用规则适用于所有港口中，选择 任何.

■目的地址 特殊的目的地址

具体目标地址，选择地址类型，从菜单，并指定了所需的数据。 你可做以下选择:

类型	说明
任何	规则允许目的地址。
主机	规则允许目的主机。 你必须键入IP地址的主机。
网络	规则允许目的网络。 你必须键入IP地址和子网掩码的网络。
本地主机	规则允许目的本地主机。 如果你使用一个以上的网络界面，选择从菜单中的网络界面，这条规则同样适用。如果你想要使用规则适用于所有本地主机中，选择 任何.
本地网络	规则允许目的本地网络。 如果您连接到一个以上的网络中，选择从菜单中的网络，这条规则同样适用。如果你想要使用规则适用于所有本地网络中，选择 任何.

如果你已经选择了TCP或UDP作为议定书您可以设置一个特定的港口或射程介于0和65535 。如果你想要使用规则适用于所有港口中，选择 任何.

■网络活动 –如果你已经选择了T CP或U DP作为议定书中，选择网络的活动，这条规则同样适用。

点击 好的 来关上视窗。

点击 添加 添加防火墙规则

9.3.3. 添加规则

你可以看到规则创造了目前为止，已为当前的简介于下表

选择此复选框对应 隐藏系统流程 隐藏规则有关制度或bitdefender进程。

规则被列出按他们的优先权的顺序从上面开始，意味第一规则有最高居先权。进入详细浏览 的显示菜单能改变他们的优先权由上上下下移动他们。

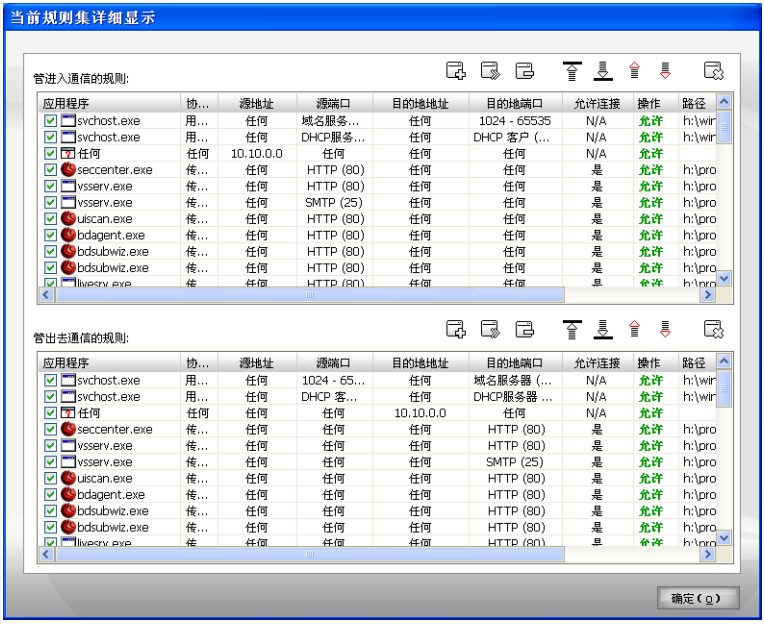
从名单削除项目，选择它和点击 删除规则 按钮。

从修改项目，选择它和点击 编辑规则 按钮。

注意
上下文菜单中还有和它包含下列选项： 加入规则，删除 和 编辑规则.

9.3.4. 修改文档

修改公司经营进入新的重要关键点. 以下窗口照常按 输入新码. 以更改预设的执照。 以下的视窗会打开:



浏览详情

规则分为两个方面:上载规则和下载规则.您可以查看应用程序和每条规则的参数(源地址、目的地址、源端口、目的端口、措施等)

要削除规则，选择它并且点击 删除规则按钮。暂时地 解除一个 编辑规则并没有削除它，清除对应的复选框。

你可以增加或减少的优先处理的规则。点击 上移进名单 按钮，增加一个层次优先选择，或点击 下移进名单 按钮，以减少一个层次优先选择。 转让规则的最高优先事项，请点击 先搬到按钮。转让规则最低优先，点击 最后移动 按钮。

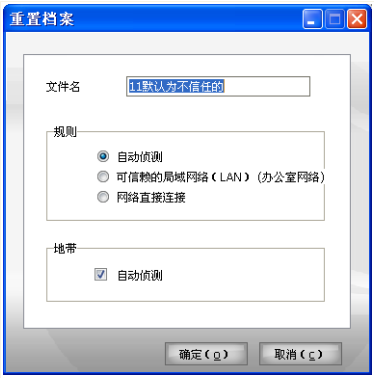
注意

进入状态 环节 设定防火墙权限 禁止所有 允许所有 允许所有白名单 询问.添加规则，编辑规则，删除规则，上移，下移，转到第一步，转到最后一步 and 清除所有.

点击 OK 来关上视窗。

9.3.5. 修改文档

进阶使用者可以选择重新配置防火墙简介，以优化的防火墙保护，或进行定制，根据他们的需要。 重置防火墙档案中，点击 复位简介. 就会出现下面的窗口：



复位简介

你可以配置下列任何一个行动：

■档案名称 –键入一个新名称，在编辑领域。
■规则 – 如果任何当前联系的规则不符合政策要求，它将会请求准许。这是缺省政策。

你可做以下选择：

选择	说明
自动检测	bitdefender检测网络配置并创造一套合适的基本规则。
被信任的地区网络	建立一套基本规则适合可信任的网络。
直接地连接到互联网	建立一套基本规则适合直接连接到互联网。

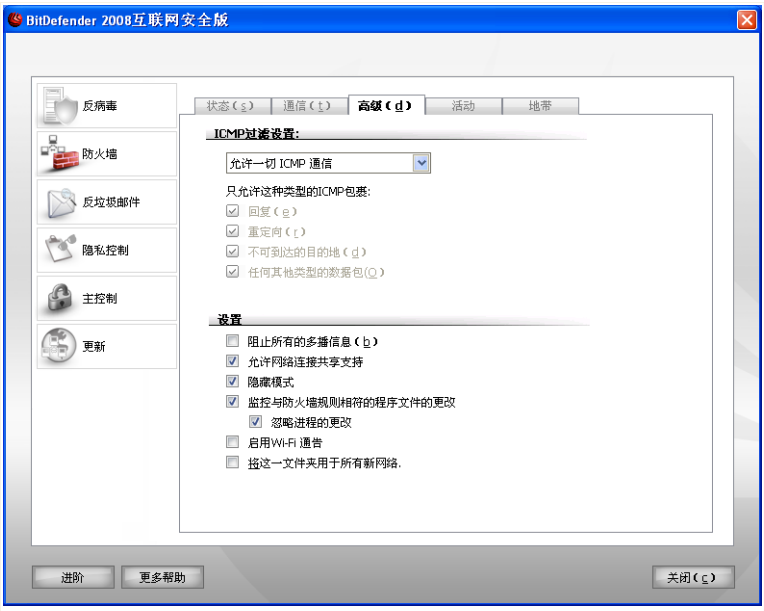
■区 –检查 自动检测 ，让b itdefender创造适宜区为检测网络。

点击 好的 来关上视窗并重设。

重要
如果您选择重新设置网络文档,在此添加的所有规则将丢失.

9.4. 高级设置

配置高级设置的bitdefender防火墙，点击 防火墙 高级 ，设置控制台。 就会出现下面的窗口:



高级设置

在这一节,你可以设置BitDefender来扫描你的电脑。 在这里您能设置BitDefender防火墙的高级设置.高级设置能使用户设定ICMP设置 访问的过滤规则(在 ICMP过滤设置中设定)、阻止多址流量、共享网络连接或在恶意软件和黑客前隐藏电脑在 设置 中设定

9.4.1. 配置ICMP过滤设置

在菜单中,用户可以选定下面的规则之一对ICMP过滤进行设置:

■点击 允许所有ICMP流量 允许所有ICMP流量
■阻止所有ICMP流量 – 阻止所有ICMP流量
■制定ICMP过滤 和您能配置ICMP过滤: 您将可以选择何种类型的ICMP的包。

你可做以下选择:

选择	说明
Echo	这个选择使用Echo 回复和Echo 请求消息。Echo 请求是寄发数据小包到主人的ICMP 消息并且期待数据被送在回归在Echo 回复。主人必须反应所有Echo 请求以Echo 回复包含确切的数据被接受在请求消息。Echo 回复是ICMP 消息引起以回应ICMP Echo 请求消息, 和是必须的为所有主人和路由器。
改方向	这是通知一个主人改它的路由选择信息方向的ICMP消息(送小包在一条供选择路线) 。如果主人设法送数据通过路由器(R1) 并且其它路由器(R2) 然后到达主人, 并且一个直接方式从主人对R2 是可利用的, 改方向将通知主人这样路线。路由器更将送原始的数据图到意欲的目的地。但是, 如果数据图包含路由选择信息, 这信不会被送既使一条更好的路线是可利用的。
目的地不能得到	这是由路由器引起通知客户的ICMP 消息目的地主人是不能得到的, 除非数据图有一个multicast 地址。这则消息的原因也许包括与主人的物理连接不存在(距离是无限的), 被表明的协议或端口不是活跃的, 或数据必须被分割但' 不要分割' 旗子是。
其他型包	与这个选择使用其他包裹比 Echo, 目的地不能得到或 改方向 将通过。

9.4.2. 配置高级防火墙设置

以下的高级防火墙设置可供选择:

■阻拦所有网络流量 – 丢弃所有的包。

多址流量是一种把信息同时传递给网络中一组特定的目的地址的方式.只要多址用户允许,程序包将被发送到用户可以接收到的某个特定地址

例如,一个拥有TVT-tuner数字电视卡的成员可以播放(发送到每个网络成员)或多址播放(发送到指定地址)该视频流.听到多播地址的电脑用户可以接收或拒接这个安装包.如果选择接收,多播用户就能收看该视频了.

过多的多址流量将占用带宽和资源.如果开启了这个功能,任何多址安装包都不能运行.但我们不建议选择该项.

■允许网络连接共享支持 – 支持因特网链接。

注意

允许网络连接共享.该选项不会自动开启用户系统上的网络连接共享功能,只会在用户从操作系统中开启后才允许这类连接.

网络连接共享使本地网络成员能通过您的电脑连接到网络.当您受益于某种特定/特殊的网络连接方式(如无线网络),想让其他成员也共享您的网络时,网络共享是十分实用的.

与本地网络中的成员共享您的网络连接将导致消耗更多的资源并带来一定的风险.这还将打开您电脑的一些端口(被使用您电脑连接的成员打开)

■隐形模式 –让您的计算机隐形恶意软件和黑客的攻击。

一种简单的发现您的电脑是否易受攻击的方法.它尝试连接端口,然后检查是否有回应,这叫做端口扫描.BitDefender能自动发现和阻止端口扫描.

恶意个体或软件程式不需要发现您的电脑机是否存在, 更不用说对网络提供服务。秘密行动方式 的选择将停止任何想查出您的机器的端口是否开放, 或它确切地是的地方的企图。

■监察变化程序文件相匹配的防火墙规则 –检查每一个应用试图连接到网际网路, 看看是否已经改变, 因为规则控制其准入补充。如果该申请已变了, 一个警示, 将提示您是否允许或阻止访问的应用到互联网。

一般情况下, 申请改变更新。但是, 有一种风险是, 他们可能会有所变化, 由恶意软件应用, 其目的是感染您的计算机和其它计算机网络。

注意

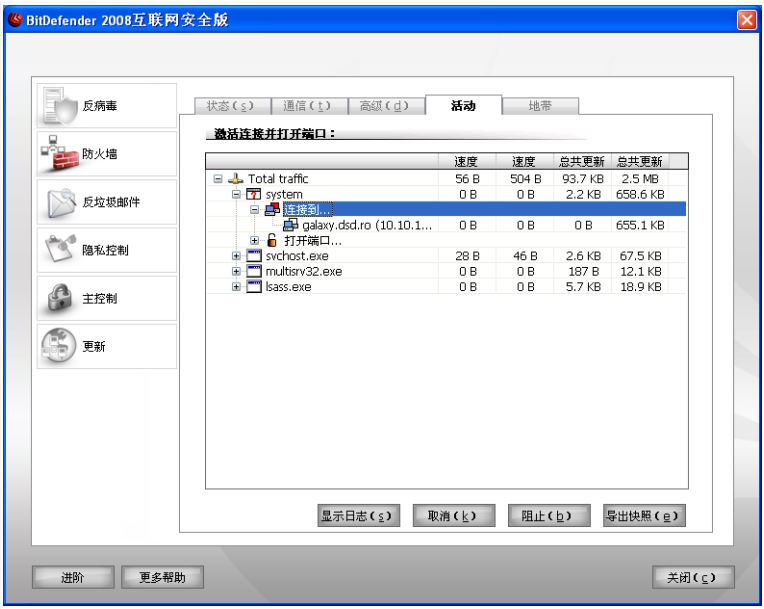
我们建议你把这个选项选中, 并允许进入的只是那些申请你期待已改变后的规则控制他们获得创造。

签署的申请是为了可以信赖的，具有更高程度的安全性。 你可以查阅 忽视的变化，签署过程 ，以使改变签署应用连接到互联网，没有你的手中接到了警报关于此事件。

- 启用Wi – Fi通知 –使W i– F i的通知。
- 应用相同的新网络 – 创建默认防火墙，命名一般网络，配置新网络检测。 如果你回去老网络配置已存在的防火墙，但各自的防火墙替代一般配置。

9.5. 连接控制

监测网络现有/网际网路活动（ TCP和UDP ）排序方法的应用，并打开了bitdefender防火墙日志，点击 防火墙 活动 ，在设置控制台。 就会出现下面的窗口：



连接控制

你可以看到全部的交通分类应用。每项申请的，你可以看到连接，以及开放口岸，以及统计方面卸任&来袭交通速度和总金额的数据发送/接收。

窗口介绍了当前网络/网际网路活动，在实时性要求。作为连接或港口关闭，你可以看到相应的统计是暗淡的，并说，最终，他们消失。 同样的事情发生在所有数据相应的应用所产生的交通，或有个开放口岸，与你密切。

点击 阻止 创造制约交通由选择的应用、端口或连接的规则。

注意
阻止一个应用，端口或网络连接，你也可以右键单击它并选择 阻止.

点击 杀死 ，以结束所有的选定过程。 您将被要求以确认您的选择。

注意
杀死一过程中，您也可以右键单击它并选择 杀死.

点击 对外映射 .txt文件出口名单。

制订一个全面的活动清单就防火墙模块的使用（开始/停止防火墙，交通阻断，使隐形模式，修改设置，申请档案） ，或所产生的活动检测（扫描端口，阻断连接尝试或交通按照规则）检查bitdefender防火墙日志文件，可以浏览点击 查看日志. 该文件的位置，在共同文件夹的当前Windows用户，根据路径： ... bitdefender \ bitdefender防火墙\ bdfirewall.txt.

9.6. 网络区

一个区是一个IP地址或一系列的IP地址，其中一个特殊的规则是创造了一个轮廓。法治可以允许网络成员不受限制地进入你的电脑（可信任区） ，或与此相反，完全孤立您的计算机免受网络计算机（非信任区） 。

默认情况下， bitdefender自动侦测你的网络连接，并增加了一个带视网络配置。

注意
如果您连接到几个网络，这取决于它们的配置，不止一个区可能会增加。

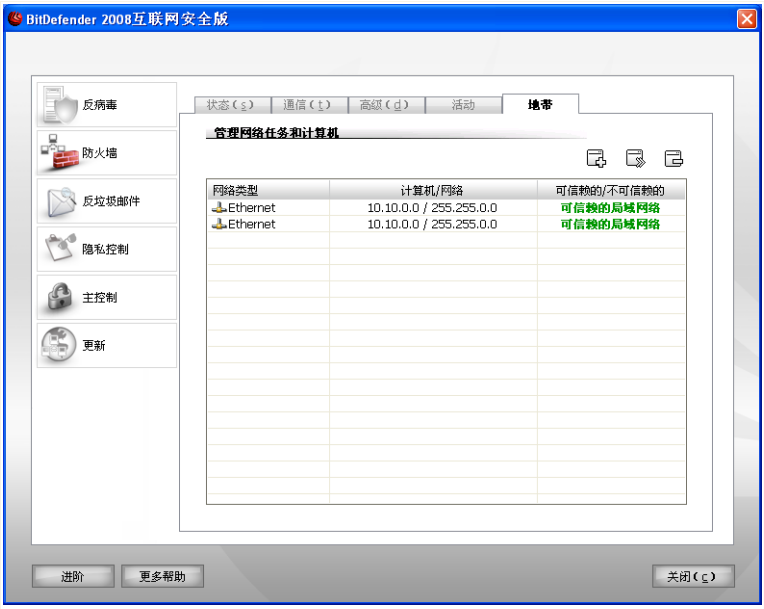
值得信赖的地带，加上默认为以下网络配置：

- 私有IP ，没有门户 –电脑的一个组成部分，局域网（ L AN）上，并没有连接到互联网。
- 私有IP与域控制器侦破 –电脑的一个组成部分，局域网，并连接到域。

来路不明区是补充，默认为以下网络配置:

■打开（不担保）无线 –电脑的一个组成部分，无线区域网路（ W LAN） 。

管理网络区，点击 防火墙 ，在设置控制台。 就会出现下面的窗口:



网络区

你可以看到网络区相对应的电流分布列于下表。每个区，您可以看到网络类型（以太网，无线，购买力平价等） ，计算机或网络相关的，以该地区是否带亲信或来路不明的。

修改一个区，选择它并点击 编辑 按钮或双击它。

注意

默认情况下， bitdefender增加开放式无线网络作为不可信区。 如果您是连接到一个特设开放无线网络与可信赖的电脑（在家里或一对夫妇的朋友） ，你可能要编辑的

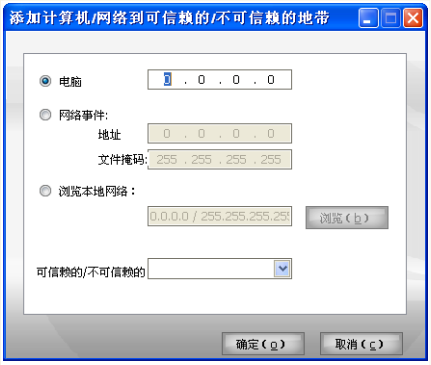
相关区。为了能够实现资源共享，与其他网络成员，就必须设定网络作为一个可信赖的地带。

删除一个区，选择它并点击 删除 按钮。

9.6.1. 添加区域

你可以手动区域 这让你，举例来说，共享文件，只有给你的朋友里面一个开放的无线网络（加入自己的电脑作为可信任区），或阻止计算机从一个可信任的网络（加入它作为一个不可信带）。

加入一个新的开发区，点击 添加 按钮。 就会出现下面的窗口：



添加区域

添加区域有下面的步骤:

1. 指定计算机从一个本地网络或整个本地网，你想成为补充说，作为一个区。 你可以选择下列任何一个方法:
   ■加入一个特定的计算机中，选择 电脑，并提供其IP地址。
   ■加入一个具体的网络中，选择 网络 ，并提供其IP地址和子网掩码。
   ■浏览本地网络，以查找并添加电脑或网络。

   浏览本地网络中，选择 浏览本地网络，然后按一下 浏览。一个新的窗口将出现在你可以看到所有你的网络连接，以作为以及所有成员的每一个网络。

   选择从列表中的电脑或网路，你想增加一款，作为一个区，并点击 好的
2. 选择从菜单中是什么样的区，你想创造（可信任或不可信）。

3. 点击 好的 添加到区域。

10. 反垃圾邮件

bitdefender反垃圾邮件雇用了显着的技术创新和行业标准的反垃圾邮件过滤器，以彻底清除垃圾邮件才达到用户的收件箱。

这个用户向导里的 反垃圾邮件 部分包含以下论题:

■反垃圾邮件见解
■反垃圾邮件状态
■反垃圾邮件设置
■登录到邮件客户端

10.1. 反垃圾邮件见解

垃圾邮件问题对个人与团体来说日趋严重。垃圾邮件不漂亮,你不希望孩子看到它,你可以应此被开除(浪费太多时间或在你的办公室邮箱接受色情邮件),你却不能阻止这些垃圾邮件的发送。 退而求其次,显然要停止接受。不幸的是,垃圾邮件没有一定的形状和大小而且数目繁多。

10.1.1. 防垃圾邮件过滤器

BitDefender 反垃圾邮件引擎一共用七种不同的过滤器来为您去除垃圾邮件: 白名单, 黑名单, 字节过滤, 图像过滤, URL 过滤r, NeuNet (Heuristic) filter and 贝叶斯过滤.

注意
在 反垃圾邮件 模块 设置 ，您可以启用/不启用各个过滤器。

白名单/ 黑名单

通常人们都会与一群一定的人有来往或与某些公司或集团有时常联络。利用 朋友或垃圾邮件发信者单，您可以指定某些您不管内容一律接受邮件的邮址，和指定您向拒绝来信的邮址。

注意
白单/黑单 也另称为 朋友单/垃圾邮件发信者单.

在 反垃圾邮件工具条 或 管理界面内，您可以设置 朋友/垃圾邮件 发信者单。

注意
我们建议您将朋友的名字和电子邮件邮址加入 朋友单. BitDefender不会拒绝这单内的邮址的来信。所以，把朋友加入朋友单能确保收到合法的邮件。

字符集过滤器

多数的垃圾邮件都是用斯拉夫文和/或亚洲语文编成的。若您想拒绝用这些语文编成的邮件，请利用此过滤器。

图像过滤器

既然如今逃脱启发性过滤器对电脑病毒是很难得，现有的垃圾邮件都多半只拥有非法内容的图影。为了解决这现象，BitDefender采用了 图影过滤器 。此过滤器将邮件内的图影签名和BitDefender档案内的对比。如有类似的，BitDefender将在邮件上打上垃圾邮件的标签。

URL过滤器

多数的垃圾邮件都有连往其他网址的连线（多数都是广告和购物网）。BitDefender有这类型网址的档案。BitDefender会把电子来信内的连线与档案内的对比，如有类似，来信的垃圾分数将。

bitdefender保持一个数据库的这种联系。 URL过滤器检查每一个URL连结在贺电中对自己的数据库。如果匹配的话，这个信息就是，标帜为垃圾邮件。

neunet （启发式）滤波器

启发性过滤器 会在邮件的各个部分进行测试，（除了标题以外，还有ＨＴＭＬ形式或本文形式的主文），寻找有垃圾邮件性态的文字，词句，等。 根据分析的结果，它增加了一个垃圾邮件评分，以讯息。

过滤器还可以检测邮件标记为SEXUALLY-EXPLICIT：明确： 在主题栏和标签，他们为垃圾邮件。

注意
从２００４年，５月１９号起，含有色情内容的垃圾邮件都必须在标题内加入SEXUALLY-EXPLICIT：的词句否则将面对联邦法律的制裁。

贝叶斯过滤器

贝叶斯过滤器 会按照指定文字出现的次数的统计资料分类邮件。若指定的文字在邮件内的次数符合垃圾邮件内的，邮件将列入垃圾邮件的类型，否则将列入非垃圾邮件类型（按照您或贝叶斯过滤器的指示）。

比如说，要是一个四个字母的字在垃圾邮件里经常出现，那接下来内容含有这字的邮件是垃圾邮件的可能性将提高。所有邮件内的相关字都会经过过滤器的计算。邮件是垃圾邮件的可能性将以统计资料决定。

此模块还有另一项特别功能：它是能够接受训练的。它能快速的配合用户所收到的邮件类型，存入所有的相关资料。若要有效的运行此过滤器，您必须给予它垃圾邮件和合法邮件的例子，训练它。在适当的时候，您可能必须更改过滤器的设置，以免它错误认定垃圾邮件。

重要

您可以用在 Is Spam and Not Spam buttons from the Antispam toolbar. 件按钮更改贝叶斯模块的设置。

注意

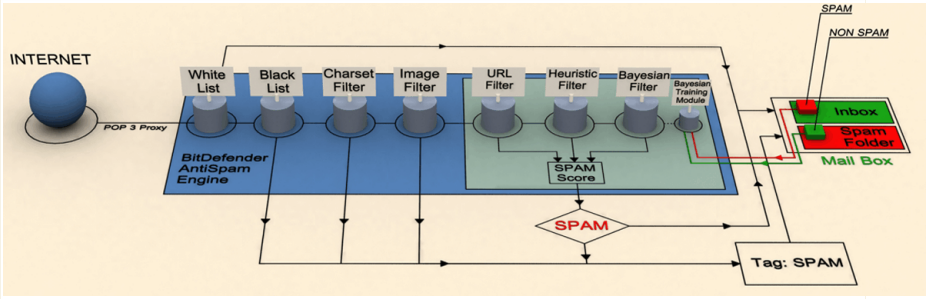
每当您进行更新:

- 新的图影签名会加入 图像过滤器.
- 新的链接会加入 URL过滤器.
- 新的规矩将列入 启发式过滤器.

这些都会帮助提高反垃圾邮件引擎的效率。
为了保护您的系统，BitDefender可以自动更新。请您保持您的 自动更新选项.

10.1.2. 反垃圾邮件设置

以下的图示说明BitDefender如何操作。



反垃圾邮件设置

该防垃圾邮件过滤器以上示意图(白名单，黑名单，字节过滤，图像过滤，URL 过滤，NeuNet (Heuristic) filter and 贝耶斯 filter) 使用bitdefender没有垃圾邮件到到你的 收件箱 与否。

每个来自网路的电子邮件首先是经查询白名单/黑名单过滤。如果寄件人的地址是白名单中发现的电子邮件是直接进入你的收件箱.

否则黑名单过滤接收电子邮件核实如果发送者的地址在名单上。 黑名单的电子邮件将被标示为垃圾邮件和移到垃圾邮件箱(位于微软outlook) 。

否则，charset过滤器将查证电子邮件是否是由西里尔文或亚洲字书写的。如果是，电子邮件将会被移到垃圾邮件箱。

如果电子邮件不是由西里尔文或亚洲字书写的， 就会交给图像过滤. 图像过滤器会检查所有的电子邮件与接收图象信息附载的内容.

URL过滤器会寻找联接,并将发现的联接和BitDefender数据库比较。 如果符合，BitDefende将增加一项垃圾电子邮件。

NeuNet (Heuristic) filter会接收电子邮件,并进行一系列测试,寻找字句或其他垃圾邮件特点。结果是,它会增加垃圾电子邮件标签。

注意
如果电子邮件是色情的问题,BitDefender会认为是垃圾邮件。

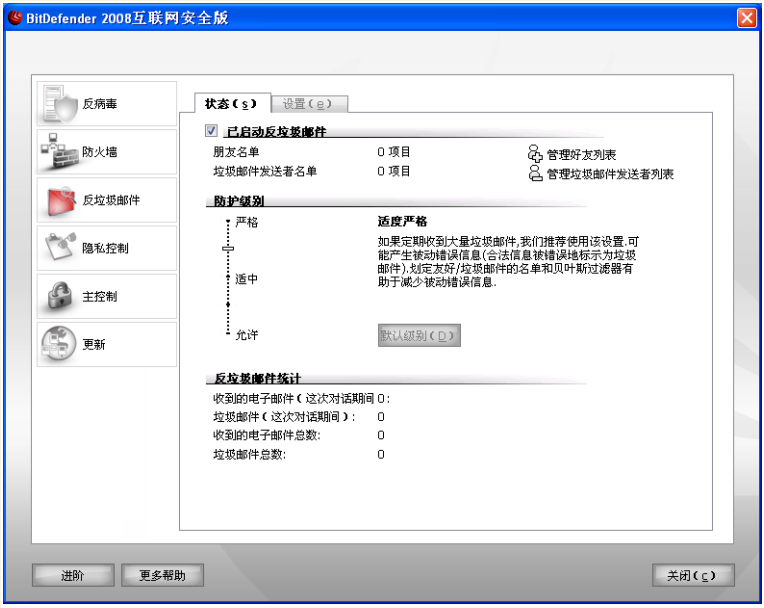
Bayesian的过滤 单元,将进一步分析信息,根据统计资料的速度出现在特定文字信息垃圾分类为垃圾或非垃圾。它会增加垃圾电子邮件分数。

如果总得分(URL评分分数+智慧+Bayesian得分)超过了垃圾信息状态(用户设定的防垃圾邮件为可允许承受能力),被认为是垃圾信息.

重要
如果你不是用微软或微软展电子邮件客户， 你应该有建立一个规则将电子邮件接收的讯息标示加到BitDefender检疫文件。[SPAM] BitDefender附在头的问题[电子邮件]的信息视为垃圾.

10.2. 反垃圾邮件状态

配置反垃圾邮件保护，点击 反垃圾邮件状态，在设置控制台。 就会出现下面的窗口:



反垃圾邮件状态

在这个部分您能配置 反垃圾邮件 模块并且您能观看信息关于它的活动。

重要
防止Spam进入您的 收件箱 ， 保持 反垃圾邮件过滤 使用。

在 统计部分您能观看antispam 活动的结果出席每会议(从您发动了您的电脑) 或总结(从BitDefender 的设施) 。

为了配置 反垃圾邮件 模块它是必要如下进行:

10.2.1. 步骤1 – 建立安全等级

您可以选择最符合您的防护需要的安全级别.上下拖动滚动条以设定最合适的防护级别。

共有5个安全级别:

安全级别	说明
容忍	为收到大量合法商业邮件的帐户提供保护. 过滤器将允许大部分邮件通行,但可能产生被动错误信息(合法信息被错误地标示为垃圾邮件).
允许调整	为收到合法商业邮件的帐户提供保护. 过滤器将允许大部分邮件通行,但可能产生被动错误信息(合法信息被错误地标示为垃圾邮件).
中等	为常规帐户提供保护. 为定期收到大量垃圾邮件的帐户提供保护.
中度至侵略性	过滤器允许少量垃圾邮件通行,但可能产生被动错误信息(合法信息被错误地标示为垃圾邮件). 过滤器允许少量垃圾邮件通行,但可能产生被动错误信息(合法信息被错误地标示为垃圾邮件). 对好友/垃圾邮件名单 进行设置,通过了解引擎（贝叶斯过滤器） 都能减少被动错误信息的数量.
侵略	为定期收到大量垃圾邮件的帐户提供保护. 过滤器允许少量垃圾邮件通行,但可能产生被动错误信息(合法信息被错误地标示为垃圾邮件). 加强与好友名单的来往以减少被动错误信息的数量.

设置缺省保护级别（ 中度至侵略性 ）按 默认级别。

10.2.2. 步骤2 – 填入地址名单

地址名单包含关于寄发您合法的电子邮件或Spam的电子邮件的信息。

朋友名单

好友名单 是您总想要收到消息所有电子邮件的名单，不管他们的内容。消息从您的朋友不被标记作为spam，既使内容类似Spam。

注意
任一邮件来自地址包含在 好友名单，自动地将被交付对您的Inbox 没有进一步处理。

处理 好友列表 click (corresponding to the 好友列表) 或者点击 好友 按钮位于反垃圾邮件工具条.

朋友名单

您能补充说或从 好友名单 去除词条。

如果您想要增加 电子邮件.检查 选择，. 键入地址和点击地址将出现在 好友名单.

重要
句法: name@domain.com.

如果您想要加域名检 域名 选择, 键入域名和点击 域名将出现在 好友名单

重要
句法:

- @domain.com, *domain.com and domain.com – –所有收到的电子邮件从 domain.com 将到达您的 Inbox 不管他们的内容
- *domain* – –所有收到的电子邮件从 domain (没有问题域名词尾) 将到达您的 Inbox 不管他们的内容
- *com – 所有收到的电子邮件有域名词尾 com 将到达您的 Inbox 不管他们的内容

删除一个项目, 从清单中, 选择它并点击 删除 按钮。如果你点击 清除列表 按钮你会删除所有参赛作品从名单, 但公告: 这是不可能收回。

使用 保存/ 载入按钮 保存文件好友列表 . 文件包含.bwl 例外.

选择加载时清空现有名单能在装载以前保存的名单时,重设现有名单的内容.

注意
我们建议您将朋友的名字和电子邮件邮址加入 朋友单. BitDefender不会拒绝这单内的邮址的来信。所以, 把朋友加入朋友单能确保收到合法的邮件。

点击 应用 和 好的保存和关闭 好友列表

垃圾邮件清单

垃圾邮件清单 是您不想要收到消息所有电子邮件的名单, 不管他们的内容。

注意
任何一个电子邮件收到从地址包含在 垃圾邮件清单 自动地将被标记作为SPAM , 没有进一步处理。

管理 垃圾邮件发送清单 点击 垃圾邮件发送清单, 或点击 垃圾邮件发送 按钮 从 反垃圾邮件工具.

垃圾邮件清单

您能补充说或从 垃圾邮件清单 去除词条。

如果您想要增加电子邮件 电子邮件地址 选择，键入地址和点击 地址将出现在垃圾邮件列表。

重要
句法: name@domain.com.

如果您想要加域名 选择，键入域名和点击 域名将出现在 垃圾邮件列表。

重要
句法:

- @domain.com, *domain.com and domain.com – 所有收到的电子邮件从 domain.com 将被标记作为SPAM
- *domain* – –所有收到的电子邮件从 domain（没有问题域名词尾）将被标记作为SPAM
- *com – 所有收到的电子邮件有域名词尾 com 将被标记作为SPAM

删除一个项目，从清单中，选择它并点击 删除 按钮。如果你点击 清除列表 按钮你会删除所有参赛作品从名单，但公告：这是不可能收回。

使用 保存/ 载入 按钮保存/ 载入垃圾邮件列表 文件可以.bwl 引伸。

选择加载时清空现有名单能在装载以前保存的名单时,重设现有名单的内容.

点击 应用 和 好的 保存和关闭 垃圾邮件清单。

重要

如果您想要重新再安装BitDefender 这是一个好想法保存 好友 / 垃圾邮件 名单前面，并且在重新安装过程是结束之后您可以装载他们。

10.3. 反垃圾邮件设置

配置反垃圾邮件设置，请点击 反垃圾邮件 设置，在设置控制台。 就会出现下面的窗口：

反垃圾邮件设置

您能使用/使无能每一个反垃圾邮件 过滤器并且您能指定其它设置关于 反垃圾邮件模块。

选择三个类别是可使用的 反垃圾邮件设置 和 基本反垃圾邮件过滤 和 高级反垃圾邮件过滤被组织象一份可伸缩的菜单，相似与那些从视窗。

注意
点击箱子被标记"+" 打开类别或点击那个被标记"-" 结束它。

10.3.1. 反垃圾邮件设置

■标记垃圾邮件标题 – 所有电子邮件认为是Spam组用SPAM 将被标记在附属的线。
■Mark phishing messages in subject – 所有电子邮件认为phishing 消息用SPAM 将被标记在附属的线。

10.3.2. 基本反垃圾邮件过滤

■友好或者非友好列表 – 激活或撤销友好或者非友好列表.
- 自动添加受助人的好友名单 –自动添加接受者发送电子邮件给朋友的名单。
- 自动添加友好列表 – 当下次您点击 非友好 按钮从 反垃圾邮件工具条发件人将自动添加到 好友名单
- 自动添加到垃圾邮件发送者名单 –未来的时候，你点击 是垃圾邮件 按钮从 反垃圾邮件工具条 发件人将自动添加到 垃圾邮件发送者名单

注意
Not Spam 和是 Is Spam 按钮被使用训练 Bayesian filter.

■阻止邮件写在亚洲字符 –座讯息写在 亚洲字符集.
■阻止邮件写在西里尔字符 –座讯息写在 西里尔字符集.

10.3.3. 高级防垃圾邮件过滤器

■使学习引擎（贝叶斯） –激活/关闭该 学习引擎（贝叶斯).
- 限制字典大小，以200000字 – 设置Bayesian dictionary – 更小是更加快速的，更大是更加准确的。

注意
被推荐的大小是: 200.000 词。

・培训学习引擎（贝叶斯）对进出的电子邮件 –火车学习引擎（贝叶斯）对进出的电子邮件。

■URL 过滤 – 激活或撤销 URL 过滤.

■neunet （启发式）滤波器 –激活/关闭该 Neunet（启发式）滤波器.

・阻止明确内容 –激活/失活的检测信息，并露骨性，在主题行。

■Image filter – 激活或撤销 Image filter.

注意
激活或撤销过滤器选择或清除复选框对应于它。

点击 应用 保存变动或点击 默认级别 装载缺省设置。

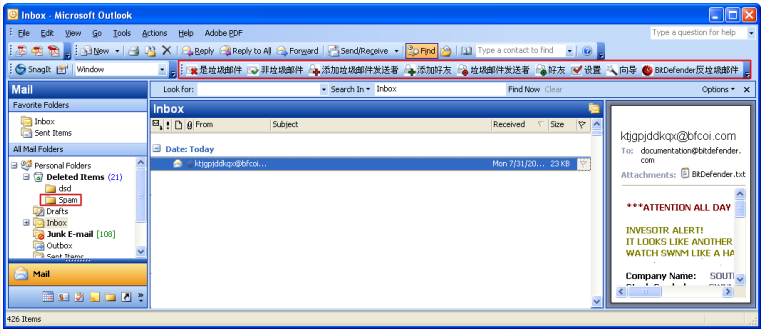
10.4. 登录到邮件客户端

BitDefender 集成直接地与Microsoft Outlook/Outlook Express 通过一个直觉和易使用的工具栏。

■Microsoft Outlook
■Outlook Express
■Windows Mail
■Mozilla Thunderbird

10.4.1. 反病毒工具栏

在Microsoft Outlook/Outlook Express 的顶边您能看Antispam 工具栏。



反病毒工具栏

重要

BitDefender Antispam 在Microsoft Outlook 或Outlook Express 的区别是，SPAM 消息被移动到 Spam 文件夹为Microsoft Outlook 当为Outlook Express 他们被移动被 Deleted Items 文件夹。在两个案件消息被标记作为SPAM 在附属的线。

Spam 文件夹由BitDefender 自动地创造在Microsoft Outlook 和是列出的在同样水平以项目从 Folder list(日历，联络等等）。

各个按钮从BitDefender 工具栏将被解释如下:

■ Is Spam – 寄发一则消息到Bayesian模块表明，选择的电子邮件是Spam。电子邮件将被标记作为SPAM 和将被移动向 Spam 文件夹。

以后同样的电子邮件样式将被标记象SPAM 。

注意

您能选择一电子邮件或许多个电子邮件当您要。

■ Not Spam – 寄发一则消息到Bayesian模块表明，选择的电子邮件不是Spam，BitDefender 不应该标记了它。电子邮件从 Spam 文件夹将被移动向 Inbox 目录。

以后同样的电子邮件样式不再将被标记象SPAM 。

注意

您能选择一电子邮件或许多个电子邮件当您要。

重要

Not Spam 按钮变得勤勉当您选择一则消息被标记作为SPAM 由BitDefender (这些消息通常位于 Spam 文件夹)。

Add spammer – 加选择的电子邮件的发令者到 Spammers list.

添加垃圾邮件名单

精选 Don't show this message again 如果您不想要提示对于确认当您加犯规推销者的地址到名单。

点击 OK 来关上视窗。

以后电子邮件从那个地址将被标记作为SPAM 。

注意

您能选择一个寄件人或许多个寄件人。

Add friend – 加上选择的电子邮件的发令者到 Friends list.

加上朋友

精选 Don't show this message again 如果您不想要提示对于确认当您加朋友的地址到名单。

点击 OK 来关上视窗。

您将收到电子邮件从这个地址不管他们包含。

注意

您能选择一个寄件人或许多个寄件人。

Spammers – 打开 Spammers list 可以列出您不想要收到消息与他们的内容的所有电子邮件地址。

注意
任何一个电子邮件收到从地址包含在 垃圾邮件清单 自动地将被标记作为SPAM ，没有进一步处理。

垃圾邮件清单

您能补充说或从 垃圾邮件清单 去除词条。

如果您想要加上电子邮件检查 Email address 选择，键入地址和点击按钮 。地址将出现在 Spammers list.

重要
句法: name@domain.com.

如果您想要增加域名检查 Domain name 选择，键入域名和点击按钮 。域名将出现在Spammers list.

重要
句法:

- @domain.com, *domain.com and domain.com – 所有收到的电子邮件从 domain.com 将被标记作为SPAM

- *domain* – –所有收到的电子邮件从 domain（没有问题域名词尾）将被标记作为SPAM
- *com – 所有收到的电子邮件有域名词尾 com 将被标记作为SPAM

输入电子邮件地址， Windows通讯录 / Outlook Express文件夹到 微软Outlook Outlook Express的 / 窗户邮件 /选择合适的方案，从 进口电子邮件地址从 下拉式选单。

Microsoft Outlook Express / Windows 微软Outlook Express /窗口邮件 一个新的窗口将出现在那里你可以选择该文件夹包含电子邮件地址，你要添加到 Microsoft Outlook Express / Windows 垃圾邮件 发送清单。选择它们，然后点击 Microsoft Outlook Express / Windows 选择

在两个案件电子邮件将出现在海关进口货物分类表。选择指定的部分和点击增加他们到 to add them to the Spammers list. 如果您点击 所有电子邮件将加上到名单。

删除一个项目，从清单中，选择它并点击 删除 按钮。如果你点击 清除列表 按钮你会删除所有参赛作品从名单，但公告：这是不可能收回。

使用 保存/ 载入 按钮保存/ 载入垃圾邮件列表 文件可以.bwl 引伸。

选择加载时清空现有名单能在装载以前保存的名单时,重设现有名单的内容.

点击 应用 和 好的 保存和关闭 垃圾邮件清单。

- Friends – 打开 Friends list 包含所有电子邮件您总想要收到电子邮件，不管他们的内容

注意

任一邮件来自地址包含在 好友名单，自动地将被交付对您的Inbox 没有进一步处理。

朋友名单

您能补充说或从 好友名单 去除词条。

如果您想要加上电子邮件检查 Email address 选择，键入地址和点击按钮 地址将出现在 友好列表

重要
句法: name@domain.com.

如果您想要增加域名检查 Domain name 选择，键入域名和点击 按钮。域名将出现在 Friends list.

重要
句法:

- @domain.com, *domain.com and domain.com – –所有收到的电子邮件从 domain.com 将到达您的 Inbox 不管他们的内容
- *domain* – –所有收到的电子邮件从 domain（没有问题域名词尾）将到达您的 Inbox 不管他们的内容
- *com – 所有收到的电子邮件有域名词尾 com 将到达您的 Inbox 不管他们的内容

输入电子邮件地址， Windows通讯录 / Outlook Express文件夹到 微软Outlook Outlook Express的 / 窗户邮件 /选择合适的方案，从 进口电子邮件地址从 下拉式选单。

Microsoft Outlook Express 一个新视窗将出现从您能选择包含电子邮件您想要加到 友好列表 的文件夹的地方。选择他们和点击 选择

在两个案件电子邮件将出现在海关进口货物分类表。选择指定的部分和点击 加上他们到 Friends list。如果您点击 所有电子邮件将增加到名单。

删除一个项目，从清单中，选择它并点击 删除 按钮。如果你点击 清除列表 按钮你会删除所有参赛作品从名单，但公告：这是不可能收回。

使用 保存/ 载入按钮 保存文件好友列表 . 文件包含.bwl 例外.

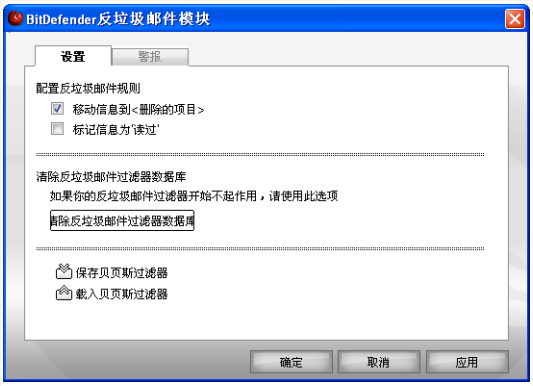
选择加载时清空现有名单能在装载以前保存的名单时,重设现有名单的内容.

注意

我们建议您将朋友的名字和电子邮件邮址加入 朋友单. BitDefender不会拒绝这单内的邮址的来信。所以，把朋友加入朋友单能确保收到合法的邮件。

点击 应用 和 好的保存和关闭 好友列表

- Settings – 打开您能指定一些选择为 Antispam 模块的 Settings 视窗。



设置

你可做以下选择:

- 移动信息删除的项目 –动作，垃圾邮件讯息给 删除的项目 （只适用于微软的OutlookE xpress/窗口邮件）；
- Mark message as 'read' – 标记象读标记消息所有Spam消息至于不干扰新Spam消息到达。

如果您的antispam 过滤器是非常不精确的，您可能需要清楚滤器数据库和再培训 Bayesian filter. 点击 Wipe antispam database 重新设置贝 Bayesian database.

使用 节省贝叶斯/ Load Bayes按钮以节省/负载该 贝叶斯数据库 名单，以理想的位置。该文件将有。.dat 延期。

点击 Alerts 符如果您想要访问您能使确认视窗幻象失去能力为增加 Add spammer 和 Add friend 按钮的部分。

注意
在这个提醒此窗口您能开启/关闭请选择一封电子邮件信息的提醒.如果您选择了一组邮件信息,而不是一封的话,就会出现这个提醒窗口.

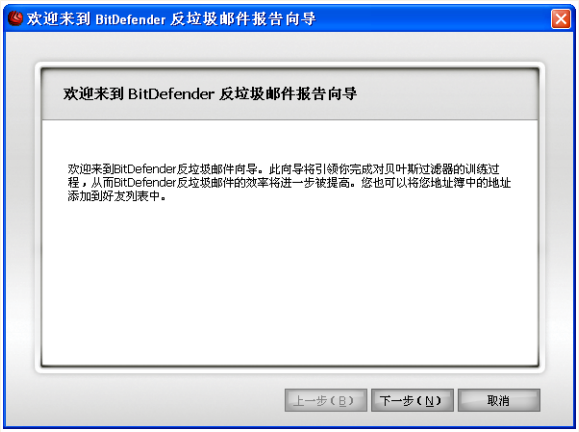
- 向导–向导表示，将加强你的整个过程，培养 贝叶斯过滤， 这样的效率 bitdefender反垃圾邮件将得到进一步提高。你也可以添加地址，从你的 通讯录 好友名单/ 垃圾邮件发送者名单
- BitDefender Antispam – 打开 Management Console.

10.4.2. 反病毒配置对话框

当您第一次运行你的邮件客户端后，你已经安装了bitdefender ，一个精灵会出现帮助你配置 好友名单 和 垃圾邮件发送者名单 以及训练 贝叶斯过滤，以提高工作效率的反垃圾邮件过滤器。

注意
对话框也可以发射任何时候你想通过点击 对话框 按钮从 反垃圾邮件工具.

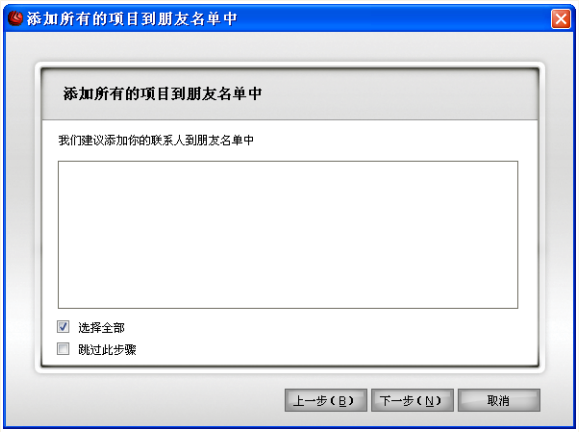
步骤一 — 欢迎窗口



欢迎窗口

点击 下一步.

步骤2/6 - 填录好友名单



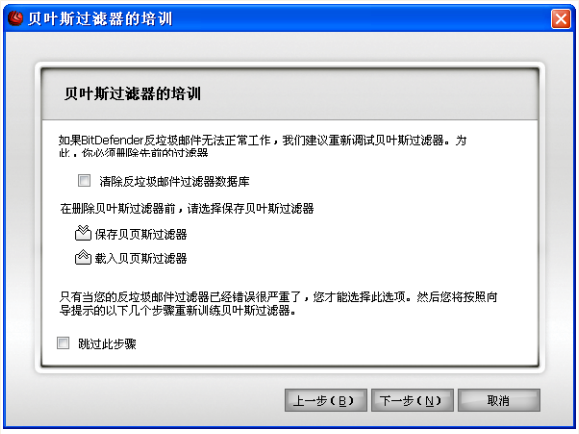
填录好友名单

您能看所有地址从您的 Address Book。请选择那些您想要增加到您的 Friends list (我们推荐选择他们全部)。您将收到所有电子邮件从这些地址，不管任何的内容。

加上所有你接触到好友名单中，选中 全部选择.

选择 Skip this step 如果您想要通过在这步。点击 Back 到早先步骤或点击 Next 继续巫术师。

步骤3/6 - 删除 Bayesian 数据库



删除 Bayesian 数据库

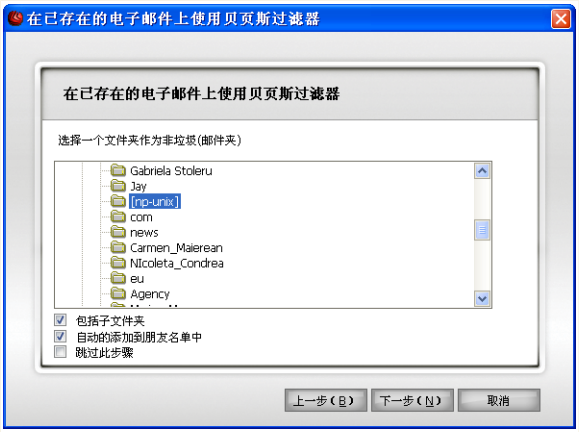
您可以发现您的antispam 过滤器开始丢失效率。这也许归结于不正当的训练(即您错误地标记了一定数量合法的消息作为Spam，或反之亦然）。如果您的过滤器是非常不精确的，您可能需要清楚滤器数据库和再培训过滤器由从事下步这位巫术师。

选择 Wipe antispam filter database 如果您想要重新设置贝Bayesian database。

使用 Save Bayes 或 Load Bayes 按钮保存/装载 Bayesian database 名单对一个指定的地点。文件将有 .dat 引伸。

选择 Skip this step 如果您想要通过在这步。点击 Back 到早先步骤或点击 Next 继续巫术师。

步骤4/6 - 训练Bayesian 过滤以合法的电子邮件



训练Bayesian filter以合法的电子邮件

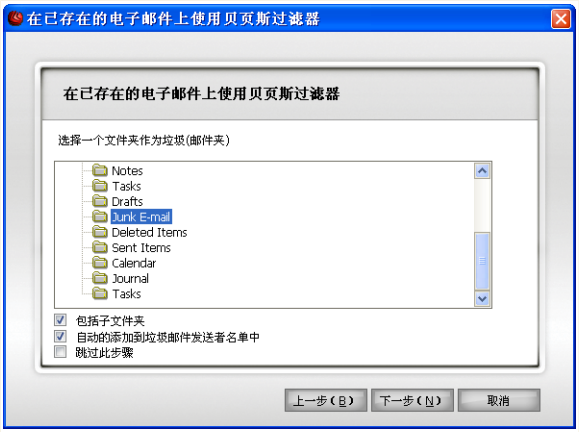
请选择包含Spam电子邮件的一个文件夹。这些消息将使用训练antispam filter。

有两个高级选项下的目录清单:

- 包括子文件夹 –包括子文件夹, 以您的选择。
- 自动添加到好友列表 – 加发令者到 好友列表

选择 Skip this step 如果您想要通过在这步。点击 Back 到早先步骤或点击 Next 继续巫术师。

步骤5/6 - 训练Bayesian filter以Spam电子邮件



训练Bayesian 过滤反垃圾邮件

请选择包含Spam电子邮件的一个文件夹。这些消息将使用训练antispam filter。

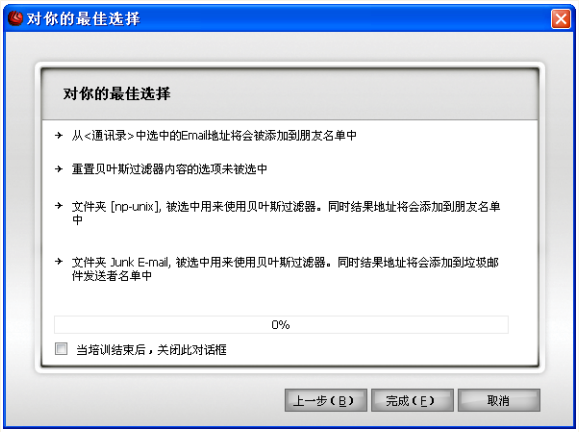
重要
请确信，您选择的文件夹根本不包含合法的电子邮件，否则antispam 可观表现将被减少。

有两个高级选项下的目录清单：

■包括子文件夹 –包括子文件夹，以您的选择。
■自动添加到垃圾邮件列表 – 加发令者到 垃圾邮件列表

选择 Skip this step 如果您想要通过在这步。点击 Back 到早先步骤或点击 Next 继续巫术师。

步骤6/6 – 总结



总结

您能观看所有设置为配置巫术师。您能做所有艮改，由返回到早先步(点击 Back). 如果您不想要做任何改动，点击 Finish 结束巫术师。

11. 隐私控制.

BitDefender监视着您的系统内容易被间谍软件侵犯地方和任何系统内的更改。想危害系统的间谍软件也能够即时阻挡。BitDefender能阻挡木马以及其他骇客所用的工具，避免它们把您的私人资料，比如信用卡号码传送给它们。

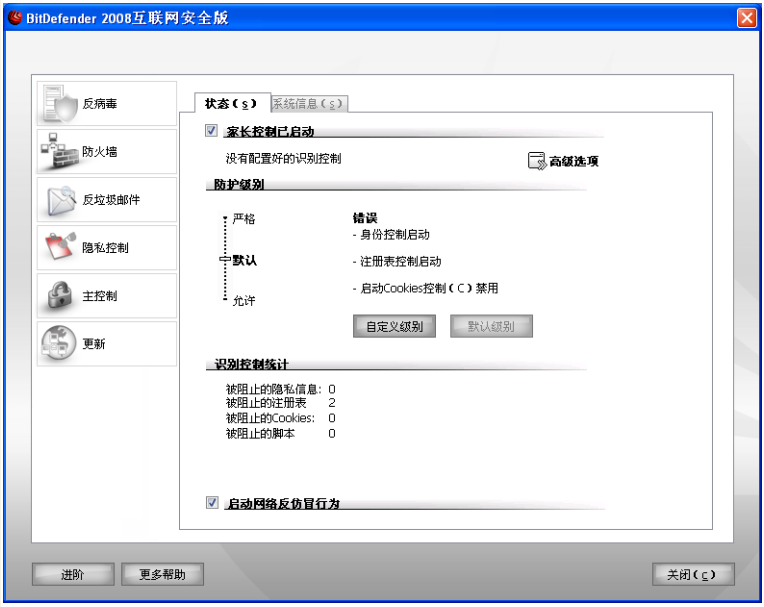
bitdefender也扫描网站，你的访问，并提醒您如果有钓鱼式检测到威胁。

隐私控制 章节包括以下内容:

■隐私状态
■高级设置 识别控制
■高级设置 注册表控制
■高级设置 cookie控制
■高级设置 脚本控制
■系统信息
■反钓鱼工具栏

11.1. 隐私状态

配置个性化的控制和查看资料，就其活动的，按 隐私控制 地位 ，在设置控制台。就会出现下面的窗口:



隐私状态

11.1.1. 隐私控制.

重要
为防止资料被窃取，并保护您的隐私保持 隐私控制 启用了。

隐私保护控制你的电脑用5重要的保护管制:

■身份控制 –保护您的机密资料进行过滤，所有离任的H TTP和S MTP交通按照议事规则，你创造了 识别

注意
在底层的章节里，你可以看到身份管制的统计数字。

■拨号控制–如果要通过拨号访问电脑调制解调器,需经过用户的允许.

■拨号控制–如果要通过拨号访问电脑调制解调器,需经过用户的允许.

■拨号控制–如果要通过拨号访问电脑调制解调器,需经过用户的允许.

配置设置为这些管制点击 高级设置.

配置防护级别

您可以选择最符合您的防护需要的安全级别.上下拖动滚动条以设定最合适的防护级别。

共有3个安全级别:

防护级别	说明
许可	仅注册表控制可用
默认	注册表控制和身份识别可用。
侵略	注册表控制 身份识别 脚本控制 可用

您也可以自订防护水平点击 自定义级别. 在窗口中会出现，专责保护控制功能，您不想让并点击 好的.

单击 默认 默认值将会载入。

11.1.2. 反钓鱼保护.

钓鱼是一种犯罪活动，在因特网上使用社会工程学技术，以诱骗人们赠送的私人信息。

大部分的时候，网络钓鱼企图归结为群众送电子邮件，其中附有虚假产地来源标签自称来自一个既定的，合法的企业。这种欺骗邮件发送，希望至少有一小部分的接收器相匹配的概况，将诈骗目标，将说服泄露私人信息。

网路讯息通常是一个问题涉及到你的网上帐户。它试图说服你点击一个链接提供的信息，进入一个假定的合法网址（事实上，一本伪造一）凡私人资料的要求。你可能会问，例如，为了确认帐户信息，如用户名和密码，并提供您的银行账户或社会安全号码。 有时，为了增强说服力，信息，可假装你的账户已经或正在威胁要暂停使用，如果你不使用提供的链接。

钓鱼还利用间谍软件，如木马键盘记录程序，窃取帐户信息直接从您的电脑上。

主网页仿冒的目标是顾客的在线支付服务，例如eBay和PayPal ，以及银行，推出网上服务。 最近，用户的社交网络网站也已针对钓鱼，以取得个人识别资料用于身份盗用。

防止spyware 传染您的电脑保持Spyware Shield使用。 这样， bitdefender将扫描每一个网站之前，你访问它，它会提醒你的存在任何网络钓鱼威胁。 白名单的网站，将不会扫描bitdefender可以配置。

为了更容易管理反钓鱼保护和白名单，使用bitdefender反钓鱼工具栏集成到Internet Explorer的。 更多信息 请翻阅 “反钓鱼工具栏” （第 150 页）.

11.2. 高级设置 身份识别控制

保证机密文件的安全是一个困扰我们的大问题.资料盗窃总是与网络的发展同时发生,它总是利用新技术骗取人们的个人隐私资料.

不管是不是您的电子邮件地址或信用卡号码,当它们落入不法分子手中,这些信息总会给您带来天大的麻烦:您可能会收到源源不断的垃圾邮件,也可能获得一个空头帐户.

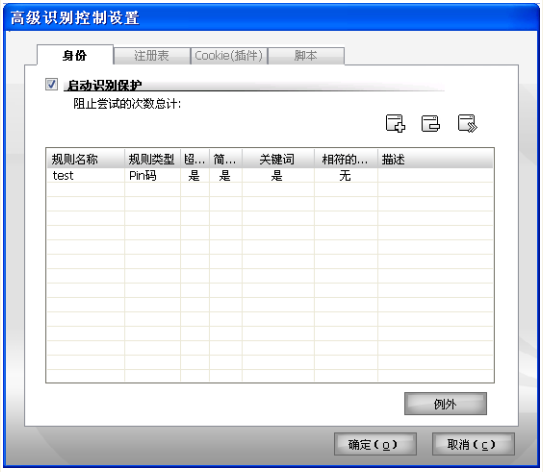
隐私控制 能保证机密文件的安全.它能扫描网页或邮件,或二者中用户定义的字符串.如果发现可匹配字符,网页或邮件将被关闭.

多用户提供支持，使任何其他用户，该系统可以看到规则您配置了。

隐私规则，可以配置在 身份 section. 在 普通单元 里点击 活动 进入窗口身份标签

注意

打开 先进隐私控制设置 窗口中，点击 隐私控制 地位 ，在设置控制台，然后点击 高级设置.



身份识别控制

11.2.1. 创建身份识别规则

规则可能自动地 或手工输入 点击 添加 按钮和选择参量为规则。

此设置向导共有3个步骤。

步骤一 建立规则类型和数据

设置规则类型和资料

在编辑一栏输入对规则的简要描述.

你必须设置的参数

■规则类型 选择规则类型（地址，名字，信用卡等）
■规则数据 – 数据规则类型

注意
如果你进入少于三个字符，系统会提示您验证数据。我们推荐您进入至少有三个特征，以避免造成误堵的讯息以及网页。

您输入的所有资料都已加密。如需更加安全，请不要输入您想保护的所有资料。

点击 下一步.

步骤2 – 选择流量

选择流量设置

选择型的交通你想bitdefender扫描。 你可做以下选择:

■扫描网页– 选择交通方向和协议为规则。
■扫描电子邮件 – 扫描所有出去的电子邮件。

您可以选择适用规则，只有当法治数据匹配整词或如果该规则的数据和侦破案件串匹配。

点击 下一步.

步骤 3 规则描述

规则描述

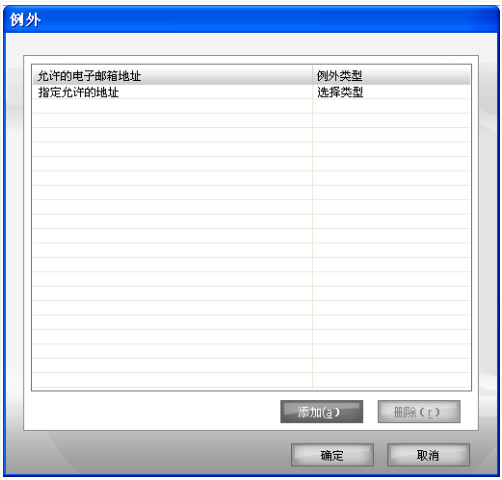
在编辑一栏输入对规则的简要描述.

点击 Finish.

11.2.2. 定义例外

在有些情况下，当你需要确定例外的具体身份的规则。 让我们考虑案件的时候，你建立规则，防止你的信用卡号码不被发送的HTTP （网络） 。每当你的信用卡号码，提交一个网站上，从你的用户帐户，分别一页，是堵住了。如果你想要做的，例如，购买鞋类从一个网上商店（你知道是安全的） ，您将需要指定一个例外，以各自的规则。

打开窗口，您可以在管理例外，点击 例外.



除外

添加一种例外，按照下列步骤进行：

1. 点击添加，以增加新的条目在表中。
2. 双击注明获准地址，并提供网址或电子邮件地址，你要添加的，作为例外。
3. 双击选择类型，并选择从菜单中可以选择相应的类型，地址先前提供的。
   ■如果您有指定的网站地址，选择的HTTP.
   ■如果您有指定一个电子邮件地址中，选择邮件.

清除一个例外，从清单中，选择它并点击删除.

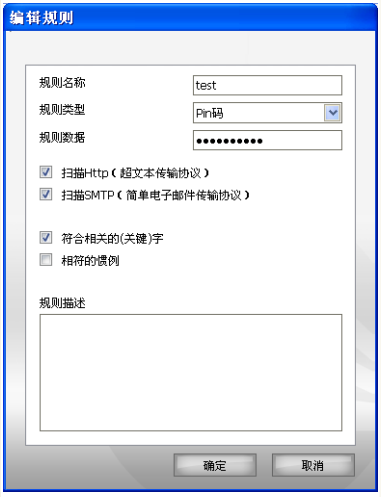
点击好的，以保存更改。

11.2.3. 添加规则

您能看资源的名字。

删除一条规则，只要选择它并点击 "删除"按钮。暂时中止一项规则，没有它删去，明确了相应的复选框。

要编辑规则选择它，并点击 "编辑"按钮或双击它。一个新的窗口就会出现。



编辑规则

在这里您可以更改名称，说明和参数的法治（类型，数据和交通）。点击好的，以保存更改。

点击 好的 来保存修改和关闭窗口.

11.3. 高级设置–注册控制

一个非常重要的组成部分的Windows作业系统称为注册。这就是Windows保存其设置，安装的程式，用户信息等

该注册，也被用来确定哪些程式应该展开时自动Windows是开始。病毒常常利用这一点是为了自动发射，当用户重新启动计算机。

注册控制一直着眼于Windows注册表–这又是有用的检测特洛伊木马。它会提醒你每当一个节目将设法修改注册入学，以被处决，在Windows开始行动。

注册处戒备

你可以否认这一点，修改通过点击没有或者你可以允许它通过点击是.

如果你想bitdefender要记住你的回答，检查总是运用这一行动这一计划. 通过这种方式，规则将创造和同样的行动，将适用时，对于这个计划试图修改注册入学，以被处决，在Windows开始行动。

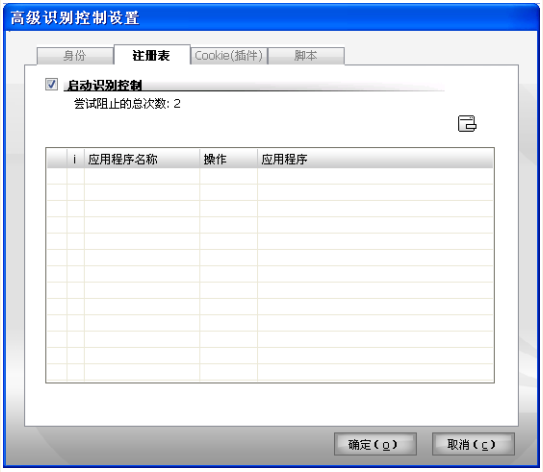
注意

bitdefender通常会提醒您，当您安装新的程序需要运行后，下次启动你的电脑。在大多数情况下，这些程序都是合法的和可以信任

每个规则已经记住可接在注册节作进一步微调。 要进入此节，打开先进隐私控制设置 窗口，并点击注册标签。

注意

打开 先进隐私控制设置 窗口中，点击 隐私控制 地位 ，在设置控制台，然后点击 高级设置.



登记控制

你可以看到规则至今已创造列于附表。

删除一条规则，只要选择它并点击 "删除" 按钮。 暂时停用规则，没有它删去，明确了相应的复选框。

要改变行动的一项规则，双击行动领域，并选择合适的方案，从菜单中。

点击 OK 来关上视窗。

11.4. 高级设置-曲奇控制

Cookies 在互联网是非常普篇。他们是小文件被存放在您的电脑。网站创造这些Cookies为了记录关于您的具体信息。

Cookies一般被制作使您的生活。例如他们能帮助网站记住您的名字和特选，以便您不必须输入他们在每次参观。

但Cookies可能由跟踪并且使用减弱您的保密性，您上网的样式。

这是cookie控制有帮助。启用后，cookie控制 ，将要求你允许每当一个新的网站试图设置一个cookie:

Cookies控制警戒

您能看到设法送Cookies文件应用的名字。

检查记住这个答案"选项并点击是或没有，并规定会创造，应用，并列举了在规则表。你将不再另行通知，下一次当您连接到同一地点。

这将有助于你选择哪一个网站，您信任的，哪些是你没有这样的规定。

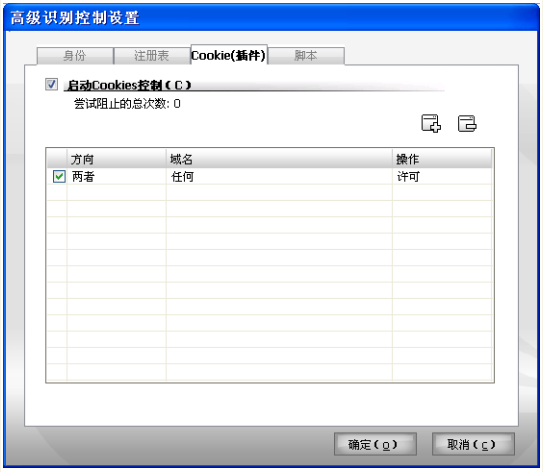
注意

由于大量的饼干在互联网上使用的今天， cookies控制 可以相当麻烦首先。首先，它会问了很多问题，关于用地试图把您电脑上的cookies 。一旦你添加你的网站，定期向法治名单，冲浪将成为一样容易。

每个规则已经记住可接在曲奇节作进一步微调。 要进入此节，打开先进隐私控制设置窗口，并点击曲奇标签。

注意

打开 先进隐私控制设置 窗口中，点击 隐私控制 地位 ，在设置控制台，然后点击 高级设置.



Cookie控制

你可以看到规则至今已创造列于附表。

重要
该规则的上市，为了自己的优先出发，从最高层的意思，第一条规则有最高优先级。拖放下降规则，以改变他们的优先考虑。

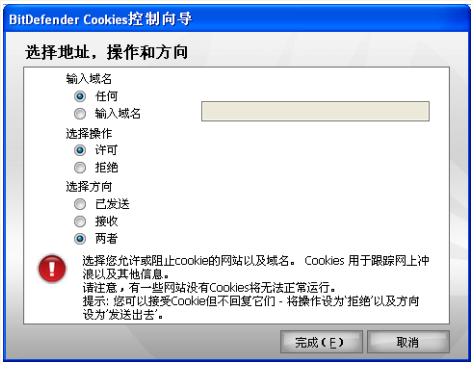
删除一条规则，只要选择它并点击 "删除"按钮。修改参数的规则，只是双击其领域做出理想的修改。暂时中止一项规则，没有它删去，明确了相应的复选框。

这些规则可以自动输入（通过警报窗口）或手动（点击 "添加" 按钮，并选择参数为规则） 。配置向导就会出现。

11.4.1. 配置向导

配置向导是一个1步骤程序。

步骤1/1 – 选择地址、行动和方向



选择地址、行动和方向

您可以设定参数:

■域名地址–类型，在域上的法治应当适用。
■行动–选择行动的规则。

行动	说明
允许	Cookie文件对这一领域将会执行。
拒绝	Cookie文件对这一域将不会执行。

■方向–选择交通方向发展。

类型	说明
外出	规则申请只被派出回到被连接的站点的Cookies。
进入	规则申请只被接受从被连接的站点的Cookies。
都是	规则申请在同方向。

点击 Finish.

注意
您可以选择接受Cookies ，但回不来了，他们通过设置行动否认卸任

点击 好的 来保存修改和关闭窗口.

11.5. 高级设置–脚本控制

剧本及其他规定，如ActiveX控件和Java applets，这是用于创建交互式网页，可以通过编程产生有害影响。 ActiveX的元素，例如，可以得到总访问您的数据，他们可以读取数据，从您的电脑中，删除信息，捕捉密码和拦截讯息，而你在线上。你应该只接受积极从网站下载你充分了解和信任。

bitdefender让您选择运行这些分子或阻止他们执行。

与脚本控制，你将负责哪些网站，你的信任和你没有这样的规定。 bitdefender会问你的许可，每当一个网站，试图激活一个脚本或其他活动内容:

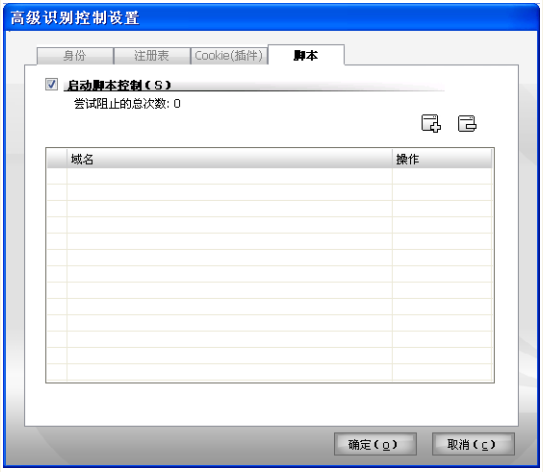
脚本警告

您能看资源的名字。

记号 Remember this answer 选择和点击 Yes 或 No 设立规则，应用和列出在规则桌中. 这样您不再将被通报何时过程重覆。

那被记得了的每条规则都能够被使用在 Script 部分为进一步优化。 要进入此节，打开 先进隐私控制设置 窗口，并点击 脚本 标签。

注意
打开 先进隐私控制设置 窗口中，点击 隐私控制 地位 ，在设置控制台，然后点击 高级设置.



语言控制

你可以看到规则至今已创造列于附表。

重要
该规则的上市，为了自己的优先出发，从最高层的意思，第一条规则有最高优先级。拖放下降规则，以改变他们的优先考虑。

删除一条规则，只要选择它并点击 "删除"按钮。修改参数的规则，只是双击其领域做出理想的修改。暂时中止一项规则，没有它删去，明确了相应的复选框。

这些规则可以自动输入（通过警报窗口）或手动（点击 "添加" 按钮，并选择参数为规则） 。配置向导就会出现。

11.5.1. 配置向导

配置向导是一个1步骤程序。

步骤 1/1 – 选择地址和行动

选择地址和行动

您可以设定参数:

■域名地址–类型，在域上的法治应当适用。
■行动–选择行动的规则。

行动	说明
允许	行动将被允许。
拒绝	行动将被否认.

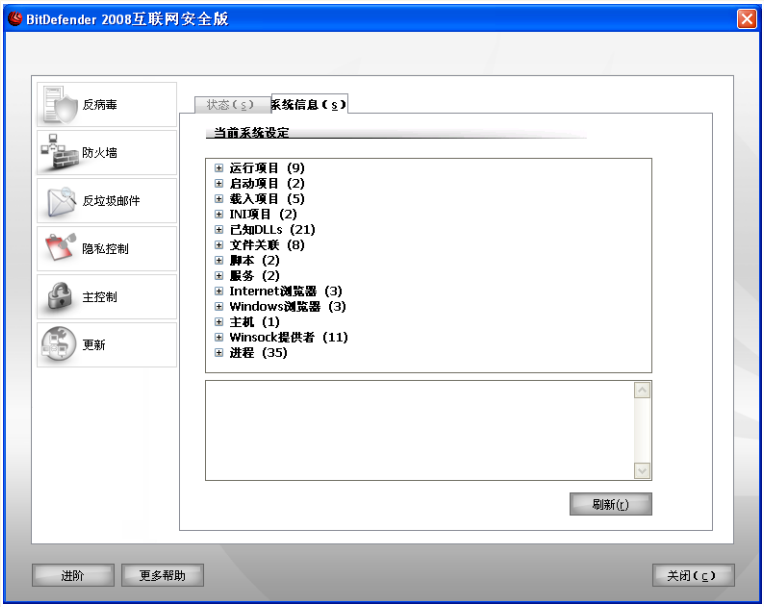
点击 Finish.

点击 好的 来保存修改和关闭窗口.

11.6. 系统信息

bitdefender可以让你看，从一个单一地点，所有的系统设置和应用程序注册运行时启动。这样，你可以对该活动进行监督的体系，并申请安装了它，以及找出可能的系统感染。

为了获取系统信息，请点击 隐私控制系统信息 ，在设置控制台。 就会出现下面的窗口：



系统信息

名单包含所有项目被装载每当系统开始和那些不同的应用的项目也同时被装载。有三个按钮

■Remove – 削除选择的项目. 你必须点击 是 ，以确认您的选择。

注意
如果你不想被提示再次确认您的选择当前的信息，点击 不要再次询问我.

■Go to – 打开选择的项目被安置的视窗(例如 Registry)。

■Refresh – 重开 System Info 部分。

注意
取决于选定项目时， 移除 或 到 按钮可能不会出现

11.7. 反钓鱼工具栏

bitdefender保护您免受网页仿冒企图的时候，你是在因特网上浏览。 它扫描浏览网站，并提醒您如果有任何网络钓鱼威胁。 白名单的网站，将不会扫描bitdefender可以配置。

你可以很容易和有效地管理反钓鱼保护和白名单的使用bitdefender反钓鱼工具栏集成到Internet Explorer的。

反钓鱼工具栏，在 bitdefender图标，浏览器的顶部。 点击打开工具菜单

注意
如果你没有看到工具条，打开菜单 工具栏 点击 Bitdefender工具栏.。

反钓鱼工具栏

你可以在工具栏做以下选择:

■启用或者禁用 Bitdefender反钓鱼工具条。

注意
如果你选择禁用反钓鱼工具栏，你将不再受到保护，免遭钓鱼式攻击企图。

■设置 – 打开你选择的反钓鱼工具栏视窗。

你可做以下选择:
・扫描– 反钓鱼扫描
・添加白名单之前询问 – 当你添加网页站点到白名单时。

■添加到白名单 – 添加当前页到白名单。

注意
增加安全名单意味着bitdefender不会扫描网站网页仿冒企图了。我们建议您添加到安全名单中。

■查看安全名单 – 打开安全名单.

你可以看到，名单上的所有网站都没有检查bitdefender反钓鱼引擎

如果你要删除站点从安全名单，以便通知您，您的任何现有网络钓鱼的威胁，在该网页中，点击移除按钮旁边。

您可以添加网站，你完全相信到安全单，使他们不会被扫描，由反钓鱼引擎了。必须要用户亲自通过选中措施和增加站点（单击添加)来添加规则。

■帮助 – 打开帮助文件.

■设定 – 打开了一个视窗，可以指定要扫描的档案，感染档案的行动,产生警报信息、储存扫描结果到报告里。

12. 家长监控

父母控制，可阻止访问：

- 不适当的网页。
- 在互联网上，对某些长一段时间（如当它的时间为教训） 。
- 网页和电子邮件，如果他们含有某些关键字。
- 应用，如游戏，聊天， filesharing程式或其他人。

重要

只有具备管理权限的用户(系统管理员)才能保存和加载该设置。如果该设置有密码保护,只有提供密码才能对其进行修改.管理员不能对使用其他管理员以前作出规定的用户设置新的规则.

本说明书的 主监控 章节包括以下内容:

- 保护父母控制设置
- 主监控状态
- 网络监控
- 应用程序监控
- 键盘过滤
- 网络限时器

12.1. 保护父母控制设置

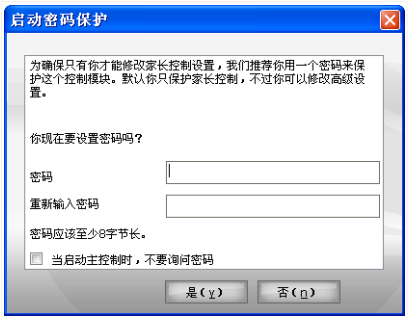
如果你是不是唯一的人与行政权的使用这台电脑，我们建议你，保护你的父母控制设置同一个密码。 通过设置一个密码，你将阻止其他用户对行政权力运作，从改变父母控制设置你的配置，为特定的用户。

bitdefender会问你默认设定一个密码时，使家长控制。

设置密码保护有以下内容:

1. 键入密码，在 密码区。
2. 再次输入密码，在 再次输入密码 实地证实。
3. 点击 好的 来保存密码和关上视窗。

一旦你设定密码，如果您想改变父母控制设置，你将会被要求提供密码。 其他的系统管理员（如果有的话）也将提供这方面的密码，以改变家长控制设置。



设置密码保护

注意
此密码将不会保护其他bitdefender设置。

如果您不要设定一个密码，你不希望这个窗口再出现，检查 不要问一个密码时，使家长控制

12.2. 家长监控状态

配置父母监控 – 你可以在这一节里设置父母监控模块。 就会出现下面的窗口:

家长监控状态

重要
开启 家长控制,防止你的孩子通过使用你的个人用户电脑获取不正当内容.

12.2.1. 选择保护控制

要设定安全级别,首先要选定要运用这些设置的用户.然后使用下面的管理权设定安全级别:

- 网络控制 –让 网络控制 ，以过滤网站导航根据该规则所定的，你在 网站。
- 应用程序控制－开启 应用程序控制可以根据您在应用程序环节设定的规则阻止运行您电脑上的应用程序.
- 网页时间限制 － 开启 网页时间限制 可以根据您在 时间限制 环节设定的规则允许网页访问.
- 网络接入–使这个选项，以阻止我们获得所有网站（不只是那些在网站栏目） 。

■关键词过滤 －开启 关键词过滤可以根据您在关键词环节设定的规则过滤网页和邮件.
■启发式网页过滤 －使这个选项，以过滤网络接入按照事先确定的规则，根据年龄分类。

注意

为了充分受益的特点，所提供的各项父母的控制，你必须配置选定管制。 要了解如何配置，请参阅下列主题在这一章中。

12.2.2. 配置启发式Web过滤

启发式网页过滤分析网页并阻挡那些匹配模式的潜在不适当的内容。

为了过滤网络接入按照预先确定基于年龄的规则集，你必须确定一个具体容忍的水平。 拖曳滚动条为指定用户设定防护级别.

共有3个安全级别:

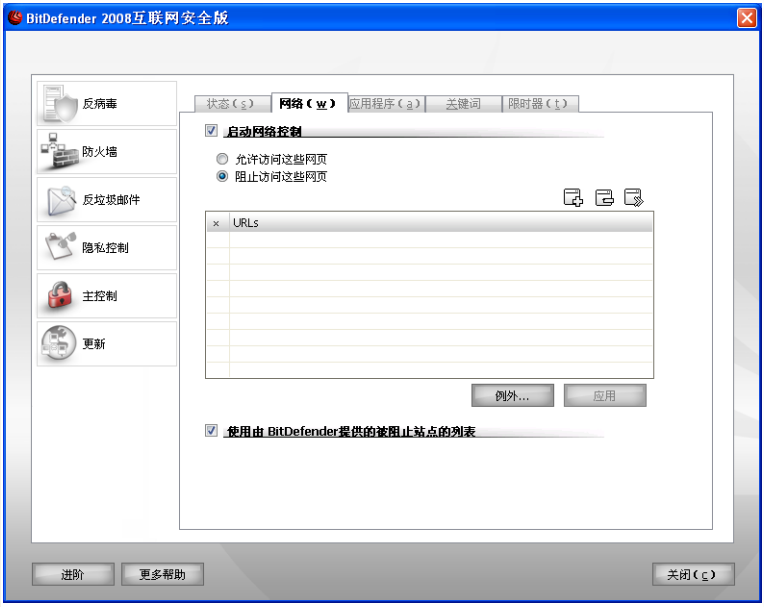
安全级别	说明
儿童	根据对14周岁以下用户的推荐设置,限制网页访问. 阻止含有对儿童可能有害内容的网页(色情、性、毒品、打杀等）.
少年	根据对14-18周岁用户的推荐设置,限制网页访问. 阻止所有关于性、色情作品或成人内容的网页.
成人	无论网页内容是什么,不限制访问所有网页.

点击 默认级别 定滑块在默认级别。

12.3. 网络监控

网络监控 帮助您阻止访问有不适当内容的站点。BitDefender会提供一份要阻止的网站站点和网页的名单，同时BitDefender也会不时更新此名单。您可以选择是否阻止那些含有在黑名单上站点链接的网页。

配置网络控制，点击 “父母控制” 网站 ，在设置控制台。 就会出现下面的窗口：



网络监控

要启动这保护，请选中相应 启动网络监控的检验盒。

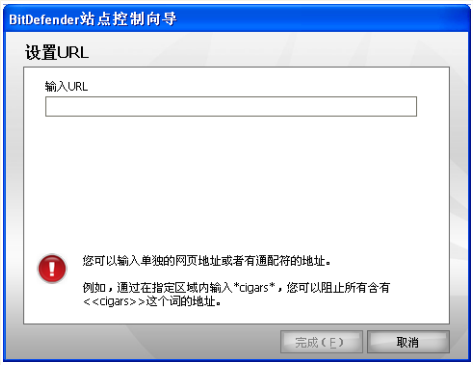
通过选择跟 指定被允许的网站 指定被阻止的网站 相应检验盒来允许/ 阻止访问在步骤二指明的网站。

规则必须手动输入。首先，选择 允许访问这些网页的 / 阻止访问这些网页 ，以许可证/块进入该网站你会在向导。然后，点击 放入 按钮启动配置向导。

12.3.1. 配置向导

配置向导是一个1步骤程序。

步骤1— 特殊网站



特殊网站

键入网址，其中的规则，将适用并点击 完成.

重要
句法:

- *.xxx.com – 此规矩的措施将会应用在所有以 .xxx.com:作为结尾的网站;
- *porn* – 此规矩的措施将会应用在所有含有 porn在其网址的网站;
- www.*.com – 此规矩的措施将会应用在所有以 com:
- www.xxx.* – 此规矩的措施将会应用在所有以www.xxx. 作为开头无论任何领域结尾的网站;

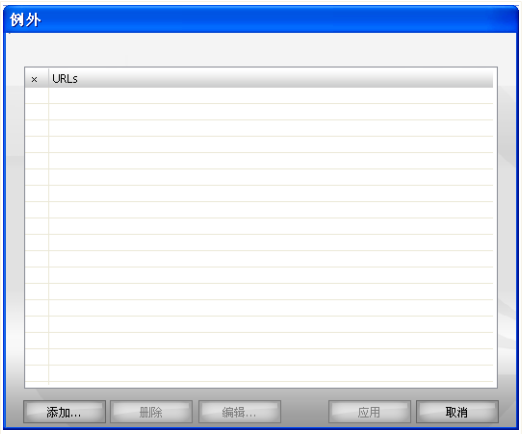
单击 应用 来保存修改。

要削除规则，选择它并且点击 删除按钮。要削除所有规则，进入 显示并且点击 清楚 的按钮。修改规则精选它和点击 编辑 按钮。暂时地解除一个规则并没有削除它，清除对应的复选框。

12.3.2. 具体例外

有时您可能需要对某一特定的规则指定排除项.例如,您设置阻止所有含有关键词"Killer"(syntax: *killer*)的网址.您必须注意有一个叫killer-music的在线音乐网页是不用阻止的.进入排除界面能指定以前建立的规则的排除项.

点击例外。 以下的视窗会打开:



具体例外

点击 添加... 将出现一个 设置向导 界面,可以指定要排除的网址.完成该向导就能设定要排除的网址.

单击 应用 来保存修改。

要删除一个规矩，只要选中它并单击 删除。要修改一个规矩，选中它并单击 编辑 或双击它就可。要在不删除一个规矩时暂时不启动它，只要不要选中它相应的检验盒就可。

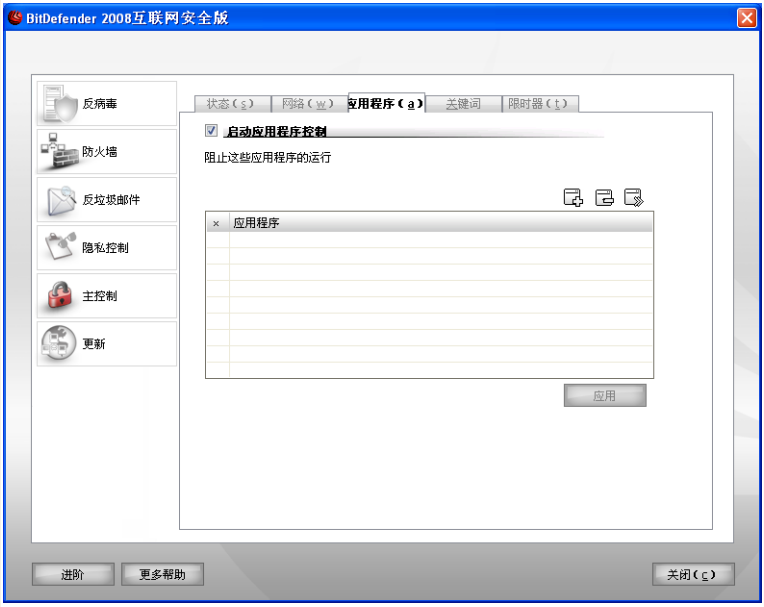
12.3.3. BitDefender 网页黑名单

为了帮助您保护孩子,BitDefeder提供了一个含有不当或潜在风险内容网页的黑名单.选定使用BitDefender提供的网页阻止名单可以阻止这个名单中出现的网址.

12.4. 应用程序监控

应用程序监控 帮助您阻止任何的应用程序运行。这样，游戏，多媒体和信息软件，还有其他种类的软件和恶意软件都会被阻止。用这样的方式阻止应用程序也同样的保护了应用程序不会被修改，不可以被复制或移动。

配置应用程序的控制，点击 父母控制 申请，在设置控制台。 就会出现下面的窗口：



应用程序监控

选中与 启动应用程序监控 相应的复选框（checkbox）以启动此保护。

规则必须手动输入。点击 放入... 按钮启动配置向导。

12.4.1. 配置向导

配置向导是一个1步骤程序。

步骤一 — 选择要被阻止的应用程序

选择要被阻止的应用程序

单击 浏览，然后选择要被阻止的应用程序，最后单击 完成。

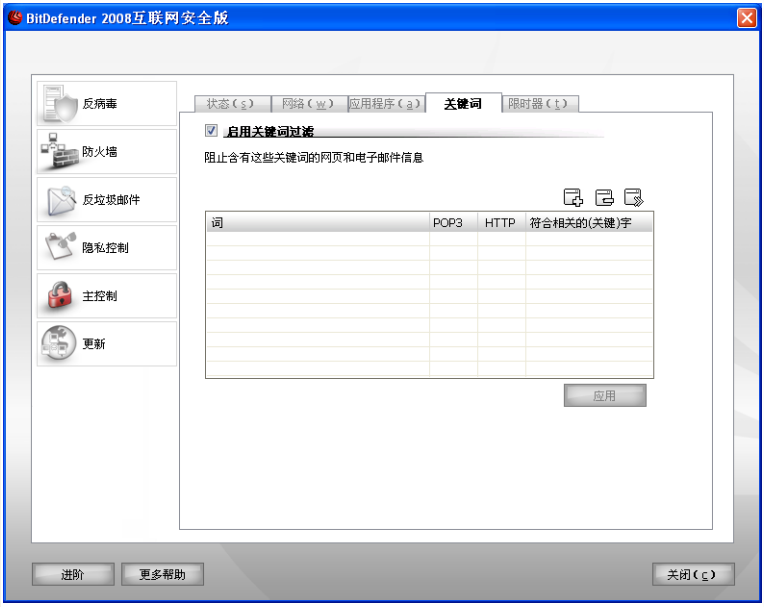
单击 应用 来保存修改。

要削除规则，选择它并且点击 删除按钮。要削除所有规则，进入 显示并且点击 清楚 的按钮。修改规则精选它和点击 编辑 按钮。暂时地解除一个规则并没有削除它，清除对应的复选框。

12.5. 关键词过滤

关键词过滤能阻止含有指定词语的邮件和网页,这样就能防止用户查看不当字段.

配置关键字过滤，点击 父母控制 关键词 ，在设置控制台。 就会出现下面的窗口：



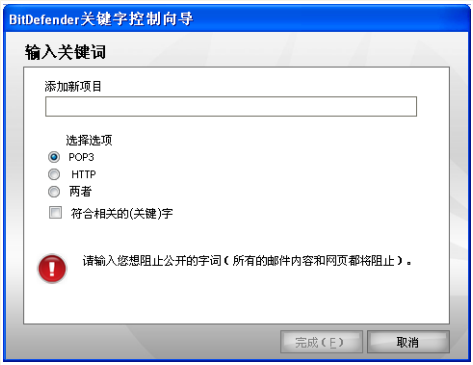
关键词过滤

为了使这项保护选择钮对应 关键字过滤
规则必须手动输入。点击 放入... 按钮启动配置向导。

12.5.1. 配置向导

配置向导包括一个1步骤程序。

步骤1/1:输入关键词



输入关键字

你必须设置的参数

■关键字 –类型，在编辑领域中的单词或短语，你想封锁。
■协议 –选择议定书bitdefender要扫描特定单词。

你可做以下选择:

选择	说明
POP3	含有这个关键词的邮件将被阻止.
HTTP	含有这个关键词的网页将被阻止.
都是	含有这个关键词的网页和邮件都将被阻止.

单击 应用 来保存修改。

要削除规则，选择它并且点击 删除按钮。要削除所有规则，进入 显示并且点击 清楚 的按钮。修改规则精选它和点击 编辑 按钮。暂时地解除一个规则并没有削除它，清除对应的复选框。

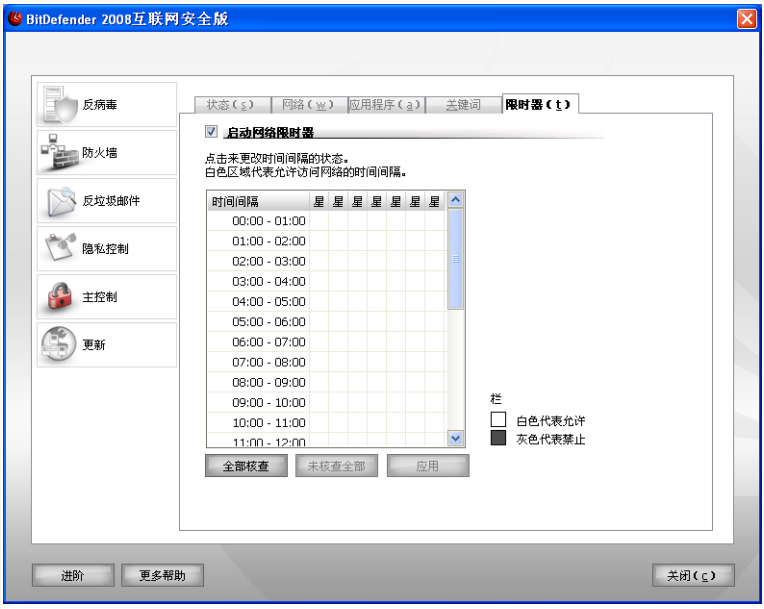
12.6. 网络限时器

指定地时间段里，网络限时器 允许或禁止在用户或应用程序访问网络.

注意

BitDefender 将会不时更新，无论什么样的 网络限时器 设置。

配置网络时间限制器，点击 父母控制 时间限制器 ，在设置控制台。 就会出现下面的窗口：



网络限时器

选中与 启动网络限时器相应的复选框（checkbox）以启动此保护。

当所有的网络连接将全被阻止时，检查所有请选择一个时间间隔。不检查所有您可以单击单元格或以单击及拖动的方式来更长的时间。

重要
灰色的方框代表着所有网络连接被禁止的时间。

单击 应用 来保存修改。

13. 更新

每天都有发现新病毒， 所以随时更新BitDefender最新病毒签名是很重要的。 因此BitDefender已经与设每小时自动更新检查。

如果您的网络是通过宽带或DSL(数字用户线)，BitDefender将会自动进行更新。它会自动检查有没有新病毒资料，当您启动您的计算机时。随后的每一个小时，它都会进行自动检查。

如果有要更新的，根据在 自动更新选项 里的选择，系统将会要求您确认更新或更新将会自动完成。

更新过程中的表现，意思是说文件，以更新正在逐步取代。这样一来，更新过程中，不会影响产品运作，并在同一时间内，任何漏洞将被排除在外。

以下是几种更新的方法:

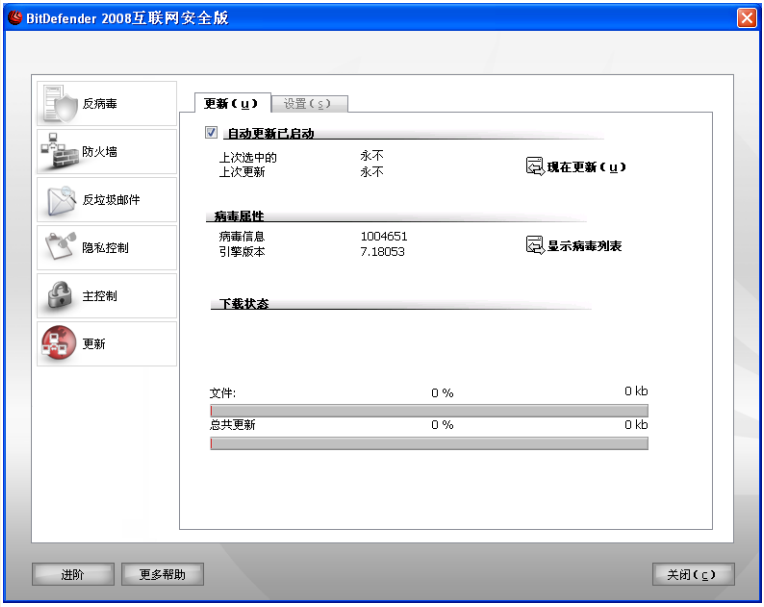
- 防毒引擎更新 – 含有病毒签名的档案必须随着新病毒的出现而更新，以确保获得持久的保护 这也称为病毒定义更新.
- 防垃圾邮件引擎更新 – 智能和网站过滤器将添加新的规则，图像过滤器将会添加图象。这有利于提高你的防垃圾邮件引擎的效率。 这也称为防垃圾邮件更新.
- 防间谍程式引擎更新 – 新的间谍程式签名会被加到数据库里。这也称为防间谍程式更新.
- 产品升级 – 当产品新版本发布时，会增加新功能及扫描技术来增强产品的性能。这是产品更新.

本说明书的 更新 章节包括以下内容:

- 自动更新
- 更新设置

13.1. 自动更新

看到即时更新相关信息，并自动更新，请点击 更新 ，在设置控制台。 就会出现下面的窗口:



自动更新

在这里你可以看到，当最后检查更新和最近更新表演，以及资料上一次更新后的表现（如果成功的话，或错误发生） 。此外，信息对当前引擎版本和签名的数目显示出来。

您可以获得恶意软件的签名，你的bitdefender点击 显示病毒名单。一个HTML文件它包含了所有可用的签名将被创造，开辟了在一个网络浏览器。你可以搜索通过数据库，为一个具体的恶意代码签名或者点击bitdefender病毒名单去线上bitdefender签名数据库。

如果你打开本节更新途中，你可以看到下载的地位。

重要
要受到保护，免遭最新的威胁保持自动更新 使用

13.1.1. 要求更新

自动更新可以在任何时候进行，只要您单击 现在更新 . 这样的更新也叫做 用户要求更新.

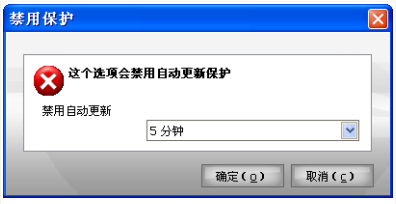
更新 模块将会连接到BitDefender的更新服务器并查证有没有任何新的更新。如果有新的更新，根据在 自动更新选项里的选择，系统将会要求您确认更新或更新将会自动完成。

重要
当更新完成，可能有必要会要重新启动计算机。建议立刻重新启动。

注意
如果您是用拨号方式连接到网络，请经常进行用户要求更新来更新BitDefender 。

13.1.2. 禁用自动更新

如果你想禁用自动更新 会有警告窗口。



禁用自动更新

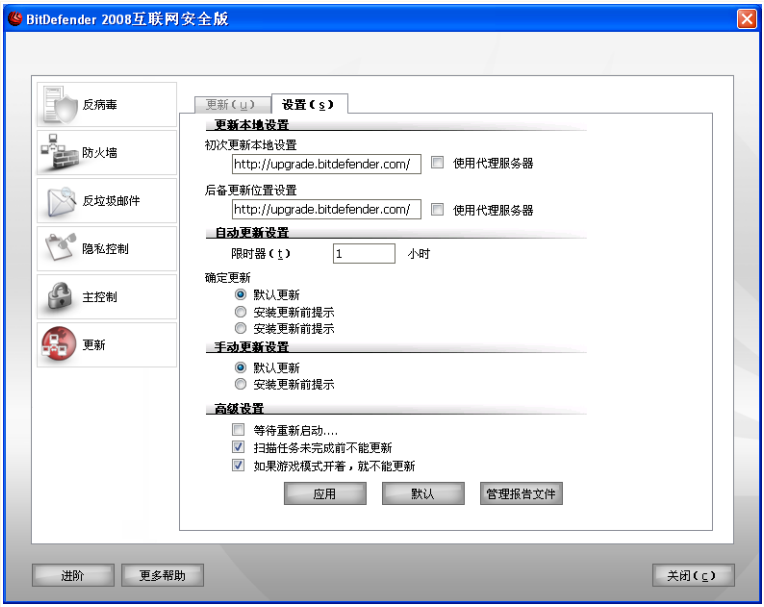
你必须确认你的选择，选择从菜单多久，你想自动更新禁用。您可以禁用自动升级为5， 15或30分钟，一小时，永久或直到系统重新启动。

警告
这是一个关键的安全问题。我们建议你要禁用自动更新，因为没有时间进行。如果bitdefender ，是不是定期更新，这将不能够保护您免受最新的威胁。

13.2. 更新设置

更新可在本地互连网上进行或通过或无通过代理服务器在网际网络上进行。 默认情况下， bitdefender将检查更新每时，透过网际网路，并安装可用的更新，没有提醒您。

配置更新设置和管理委托书，请点击更新 ，在设置控制台。 就会出现下面的窗口：



更新设置

更新设置的对话框共有四个选项 更新本地设置 自动更新选项 ， 指定更新选项 和界面选项 列在可打开的菜单内，就如视窗的。

13.2.1. 设置更新源

使用选项定更新地点，从更新位置设置 类别。

注意
配置这些设置只有当您连接到一个本地网络商店bitdefender恶意代码签名，在当地或如果你连接到互联网上，通过代理服务器

要拥有更快以及更可信赖的更新，您可以指定两个更新位置：一个主要更新位置和一个后备更新位置. 两个更新位置您都必须指定以下选项：

http://upgrade.bitdefender.com.

要修改其中一个更新的地方，提供的URL当地镜子在网址领域相对应的位置，你想改变的。

注意
我们建议您设置为小学更新所在地地方一面镜子，离开候补更新位置不变，因为故障安全计画，以防当地镜子变得无法使用。

一旦该公司使用代理服务器连接到网际网路，检查使用代理 ，然后按一下管理委托书 配置代理设置。

注意
更多信息请翻阅 “修改文档委托书管理” （第 170 页）

13.2.2. 配置自动更新

配置更新过程中自动进行bitdefender ，使用选择，在 自动更新设置 类别。

你可以指定小时数之间连续两次检查更新，在时间间隔外地。默认情况下，更新时间间隔设置为1个小时。

明文规定如何自动更新过程中应履行的，选择下列选项之一：

■沉默更新 – BitDefender 自动下载和安装更新。
■下载更新前提问 – 服务器有更新时会通过您的允许后再下载。

注意
系统会提示您之前更新下载的，即使你退出安全中心。

■安装更新前提问 – 更新下载后，系统会在安装前先得到您的允许。

注意
系统会提示您更新前安装，即使你退出安全中心。

13.2.3. 配置手动更新

明文规定如何升级手册（增订本由用户请求）应履行的，选择下列选项之一，在手动更新设置种类：

■后台更新 – 指定更新会在后台进行更新。
■下载更新前提问 – 服务器有更新时会通过您的允许后再下载。

注意
系统会提示您之前更新下载的，即使你退出安全中心。

13.2.4. 配置高级设置

为防止bitdefender更新过程中，从干扰你的工作，配置选择，在高级设置种类：

■等待从新启动，不提议从新启动 – 若更新需要从新启动，程序将继续运行旧文档直到系统从新启动。系统不会向用户者提议从新启动，所以BitDefender更新过程也不会影响用户者的工作。
■不更新，如果扫描正在取得进展 –bitdefender将没有更新，如果扫描进程正在运行。这样一来， bitdefender更新过程中，不会干预扫描任务。

注意
如果BitDefender在扫描时进行更新,扫描程序将被中止.

■在游戏模式不要自动更新 – Bitdefender不会在游戏模式自动更新。 这样，你可以尽量减少产品对系统性能，在游戏的影响，

13.2.5. 修改文档委托书管理

如果你的公司使用代理服务器连接到网际网路，你必须要指定代理服务器设置，以便bitdefender以更新自己。否则，将使用代理设置的管理员表示，安装了该产品，或当前用户的默认浏览器，如果有的话。

注意
该代理服务器设置可以配置只有通过用户与行政权对电脑或由电力用户（用户知道密码，以该产品设定） 。

修改代理设置，点击 代理设置. 会出现代理设置窗口。

代理管理

代理设置可分为三种:

■管理员代理设置（检测安装时间） –代理设置检测对管理员的帐户安装过程中，哪些可以配置只有如果你是登录到该帐户。如果代理服务器需要用户名和密码，你必须详细说明他们在相应的领域。

■当前用户代理设置（从默认浏览器）） –代理设置的当前用户，摘录自默认浏览器。如果代理服务器需要用户名和密码，你必须详细说明他们在相应的领域。

注意
该支持的Web浏览器的Internet Explorer ， Mozilla Firefox和歌剧。如果您使用另一种浏览器默认情况下， bitdefender将无法获得代理设置的当前用户

■你有自己的一套代理设置 –代理服务器设置，你可以配置如果你是管理员身份登录。

以下设置必须指明:
・地址 – 选择代理服务器。

- 端口 – 请在此输入代理服务器的域名或互联网协议地址和联系使用的端口号。
- 代理服务器用户名 – 请输入代理服务器所认同的用户名。
- 代理服务器用户密码 – 请输入以上用户名的密码。

你有自己的一套代理设置–代理服务器设置，你可以配置如果你是管理员身份登录。

首先，载你自己的代理服务器设置将用于连接到互联网。如果它不工作，代理设置检测装置的时间将在明年受审。最后，如果这些工作不要么，代理设置的当前用户将采取从默认浏览器，并用于连接到互联网。

点击 好的 来保存修改和关闭窗口.

点击 Apply 保存变动或点击 Default 装载缺省设置。

BitDefender救援光盘

14. 概要

BitDefender 互联网安全版2008带有一个可引导光碟（ bitdefender救援光盘版），能够扫描并消毒所有现存的硬盘驱动器之前，你的作业系统启动。

若您的操作系统因为电脑病毒无法正常操作，请用BitDefender 拯救光碟(Rescue CD)。若您不采用任何反病毒软件，这情况是很常见的。

为了不让用户者费心，BitDefender 拯救光碟（Rescue CD）在启动时会自动进行更新。

LinuxDefender 是按照Knoppix 改装后的BitDefender。 它将最新的为Linux 所造的BitDefender保安措施融入GNU/Linux Knoppix Live 光碟，给予瞬间的简单邮件传送协议（SMTP） 反病毒/范垃圾邮件防范措施以及桌面上的反病毒功能。它能扫描和洁净现有的硬盘（包括视窗NTFS 分解），远程的桑巴/视窗（Samba/Windows）共享件或网络文件系统（NFS）装入点 。LinuxDefender 内还含有基于网络的管理界面，可用于操控BitDefender 的防范措施。

注意

bitdefender救援CD可以在以下地址下载：http://download.bitdefender.com/rescue_cd/

14.1. 系统要求

启动LinuxDefender之前， 您必须确保您的系统符合以下的需求。

处理器种类

x86符合，频率最少166 MHz，但若真如此系统的效率并不高。提议i686 处理器，频率 800MHz。

随机存取记忆体

内存至少为512MB(推荐值1GB).

光碟驱动器

LinuxDefender 是利用光碟驱动器 CD-ROM 运行的。计算机必须装有光碟驱动器 CD-ROM，基本输入/输出系统也必须有利用光碟驱动器启动的功能。

网络联系

虽然LinuxDefender 不需网络联系运行，但更新过程就算需要通过代理服务器也要通过超文本传输协议HTTP联系进行。所以，若要最新的防范措施，网络联系是必要的。

图形分辨率
标准包括SVGA兼容图形卡。

14.2. 含有的软件

BitDefender 拯救光碟（Rescue CD）含有以下软件：

Xedit
这是一个文本文件编辑器。

Vim
是一个功能强大的文本文件编辑器，其中载有语法突出，甚至还有更多。如需更多资讯，请参阅该Vim homepage.

Xcalc
这是一个计算器。

RoxFiler
roxfiler是一个快速和强大的图形文件管理器等。

如需更多资讯，请参阅该RoxFiler homepage.

MidnightCommander
文件管理器。

如需更多资讯，请参阅该MC homepage.

Pstree
显示正在运行的进程。

Top
热门显示器Linux的任务。

Xkill
杀毒杀掉了在一个位置上

Partition Image
分割图像，有助于节省分割区中的ext2， reiserfs， NTFS的，住房公积金，将FAT16， FAT32文件系统格式，以一个图像文件。这一计划可用于备份用途。

如需更多资讯，请参阅该Partimage homepage.

GtkRecover
收回是一个基于GTK版的控制台程序收回。它可以帮助你恢复一个文件。

如需更多资讯，请参阅该GtkRecover homepage.

ChkRootKit

chkrootkit是一个工具，可以帮助您为您的计算机扫描的rootkit 。

如需更多资讯，请参阅该ChkRootKit homepage.

Nessus Network Scanner

nessus是一个远程安全扫描器为Linux ， Solaris操作系统， FreeBSD的，和Mac OS X

如需更多资讯，请参阅该Nessus homepage.

Iptraf

iptraf是一个IP网络监控软件。

如需更多资讯，请参阅该Iptraf homepage.

Iftop

iftop显示器带宽利用率上一个界面。

如需更多资讯，请参阅该Iftop homepage.

MTR

MTR是一个网络诊断工具。

如需更多资讯，请参阅该MTR homepage.

PPPStatus

pppstatus显示器统计有关，抵港及离港的TCP / IP流量。

更多信息 请查阅PPPStatus homepage.

Wavemon

wavemon是一项监测应用的无线网络设备。

更多信息请查阅 Wavemon homepage.

USBView

usbview显示器信息设备连接到USB总线。

更多信息请查阅 USBView homepage.

Pppconfig

pppconfig能自动建立一个拨号了PPP连接。

DSL/PPPoe

DSL / PPPoE协议配置一个PPPoE协议（ ADSL的）连接。

I810rotate

i810rotate切换视频输出i810硬件使用i810switch （ 1 ） 。

更多信息请查阅I810rotate homepage.

Mutt

Mutt是一个功能强大的基于文本的默剧的电子邮件客户端。

更多信息请查阅 Mutt homepage.

Mozilla Firefox

Mozilla Firefox 非常好的网络游览器

更多信息请查阅 Mozilla Firefox homepage.

Elinks

elinks是一个文字模式的网页浏览器。

更多信息请查阅 Elinks homepage.

15. BitDefender救援光盘

这一章载有关于如何启动和停止bitdefender救援光盘，为您的计算机扫描恶意软件以及保存数据，从你的毫不妥协的Windows电脑，以一个移动式装置。然而，当使用该软件的应用程序，也就有了光盘，你可以做很多任务的描述，这远远超出了范围，这个用户的指南。

15.1. 启动BitDefender救援光盘

要运行其光碟，首先要设置您的计算机的基本输入输出系统（BIOS） 是从光碟导入的，然后再把光碟放入驱动器中，最后重新启动计算机。确认您的计算机可以从光碟导入。

等待下一个屏幕出现，再根据屏幕上的指示来启动LinuxDefender.。

启动时的荧屏

为了不让用户者费心，BitDefender 拯救光碟（Rescue CD）在启动时会自动进行更新。

当启动进程完成，您将会看到刷新的桌面。现在，您可以使用LinuxDefender。

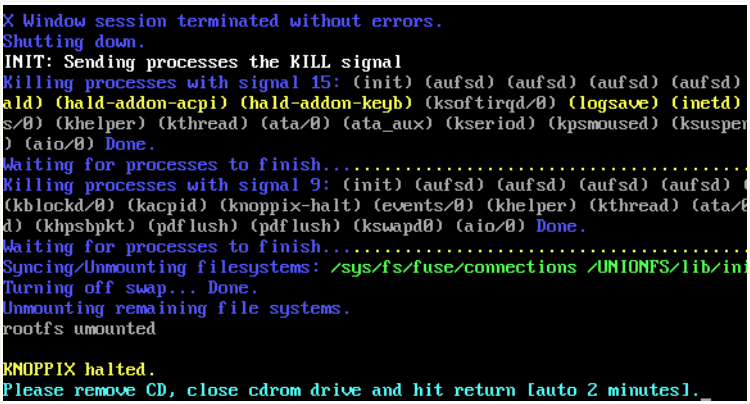
桌面

15.2. 停止BitDefender救援光盘

您可以安全地关闭你的电脑，选择 退出 ，从bitdefender救援光盘上下文菜单（右键打开它） ，或发出 停止 指挥，在一个终端。

选择 “退出”

您可以取出光碟，系统就可以从您的硬盘导入启动。现在，关闭或重新启动您的计算机都没有问题了。



当关闭时，请等待这一信息

15.3. 如何我才能进行反病毒扫描?

一个精灵时即会出现开机过程已经结束，并让您全面扫描您的计算机。所有您需要做的只是按一下 开始 按钮。

注意
如果你的屏幕分辨率是高度不够，您将被要求开始在扫描文本模式。

遵循三个步骤的引导程序来完成扫描过程。

1. 你可以看到扫描的地位和统计（扫描速度，经过时间，有多少扫描/感染/可疑/隐藏物体及其他） 。

   注意
   这可能需要一段时间,取决于你硬盘的大小。

2. 你可以看到，在一些问题，影响你的系统。

   这些问题表现在组。 点击"+"的格子以打开选择或 “–” 的格子以关闭打开的选择。

您可以选择一个整体将要采取的行动，为每个小组的问题，或者你可以选择单独行动，为每一个问题。

3. 您能看结果总结。

如果你要扫描某个目录只，做如下：

浏览您的文件夹，右击一个文件或目录并选中 发送到（Send to）。然后选择BitDefender扫描器（BitDefender Scanner）。

或您可以在一个命令提示框（terminal）内输入以下的命令。 BitDefender反病毒扫描器（BitDefender Antivirus Scanner） 将把选中的文件或文件夹当作默认的进行扫描。

```
# bdscan /path/to/scan/
```

15.4. 我怎么更新bitdefender代理?

如果有一个代理服务器，将您的电脑与因特网，一些配置都是必须做的，以更新病毒码。

更新bitdefender代理步骤如下：

1. 右键单击桌面上。该bitdefender救援光盘上下文菜单就会出现。
2. 选择终端).
3. 命令类型：cd /ramdisk/BitDefender-scanner/etc.
4. 命令类型：mcedit bdscan.conf to edit this file by using GNU Midnight Commander (mc).
5. 注释以下行：（刚刚删除 # 标志），并指定该域名，用户名，密码和服务器端口该代理服务器。举例来说，各自的路线要这个样子：

   HttpProxy = myuser:mypassword@proxy.company.com:8080
6. 按 F2 可以 可以储存当前文件，确认保存，按F10关闭.
7. 命令类型：bdscan更新.

15.5. 我如何保存我的数据?

让我们假设你不能启动你的Windows PC由于一些未知的问题。在同一时间内，你迫切需要获得一些重要数据，从您的电脑上。这是bitdefender救援光盘来得心应手。

为了节省您的数据，从计算机到一个可移动的装置，例如一个USB记忆棒，步骤如下：

1. 把bitdefender救援光盘，在光盘驱动器，记忆棒USB驱动器，然后重新启动电脑。
2. BitDefender 拯救光碟（Rescue CD）启动会有以下窗口：

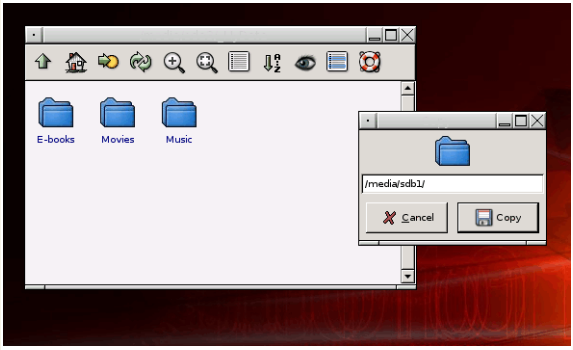
桌面

3. 双击分区数据，你想保存的是位于(e.g. [sda3]).

注意

当工作与bitdefender救援光盘，你会处理的Linux型划分的名字。所以[sda1] 可能会对应到视窗型划分为(C:) Windows-type partition, [sda3] to (F:), and [sdb1] 并到记忆棒。

4. 浏览你的文件夹，并打开想要的目录。举例来说，我的数据 包含 电影， 音乐 和 电子图书 分目录。
5. 右键单击想要的目录，并选择 拷贝.就会出现下面的窗口。



保存数据

6. 类型/media/sdb1/ 到相应的文本框，然后点击 复制.

获得援助

16. 支持

本服务公司，BitDefender尽可给客户特别快速与准确性的服务。以下列出的服务中心都确保拥有最新的电脑病毒档案。它们能迅速地解答您的问题。

BitDefender专注地为客户提供价廉物美以及最高科技的软件。例外，我们也相信与客户建立良好与诚恳的沟通和关系能帮助本公司增增日上。

我们任何时刻都欢迎您的需求。请将您的问题传送到 support@bitdefender.com 。为了帮助我们能够快速地解决您的问题，请提供您的问题详情，您的系统结构以及问题的详细状况。

16.1. BitDefender 基础知识

BitDefender 资料档案是本公司在网上列出产品的存放区。您也可以在此轻易地找寻您提出的问题的检验报告。报告是由BitDefender 的服务和创建组所提供的。它们也同时提供了一些有关反病毒防范措施的文章，BitDefender 管理组的方案和解说以及更多的有趣的文章。

BitDefender资料档案是公开的，客户可以通过它进一步地了解病毒，增进对电脑病毒的知识。客户所乘上的有效病毒报告以及咨询都即将列入BitDefender 资料档案为消灭病毒报告，解决普通病毒的向导或补充软件帮助文件的文章。

您可以任何时刻在此网址阅读BitDefender 资料档案 http://kb.bitdefender.com.

16.2. 请求帮助

16.2.1. 网上自助服务

一个问题？我们的安全专家都能帮助你时时通过电话，电子邮件或聊天，不收取额外费用。

请你，请点击以下链接：

英国

http://www.bitdefender.com/site/KnowledgeBase/browseProducts/2195/

德国

http://www.bitdefender.com/de/KnowledgeBase/browseProducts/2195/

法国

http://www.bitdefender.com/fr/KnowledgeBase/browseProducts/2195/

罗马尼亚

http://www.bitdefender.com/ro/KnowledgeBase/browseProducts/2195/

西班牙

http://www.bitdefender.com/es/KnowledgeBase/browseProducts/2195/

16.2.2. 打开支持票

如果你想要打开一个支持票，并得到帮助，通过电子邮件进行交流，只是跟随其中的链接：

英语：http://www.bitdefender.com/site/Main/contact/1/
德语：http://www.bitdefender.de/site/Main/contact/1/
法国：http://www.bitdefender.fr/site/Main/contact/1/
罗马尼亚：http://www.bitdefender.ro/site/Main/contact/1/
西班牙：http://www.bitdefender.es/site/Main/contact/1/

16.3. 联系信息

我们相信有效的通讯能增强本公司的业务。十年以来，本公司不断地为客户提供非凡和有效的通讯，为此保持着响亮的名誉。我们非常欢迎您向我们提出任何要求，问题或提议。

16.3.1. 有效网址

销售部：sales@bitdefender.com
技术部：support@bitdefender.com
文书部：documentation@bitdefender.com

联合项目: partners@bitdefender.com
行销部: marketing@bitdefender.com
媒体部: pr@bitdefender.com
人事部: jobs@bitdefender.com
提交病毒: virus_submission@bitdefender.com
提交垃圾邮件: spam_submission@bitdefender.com
报告: abuse@bitdefender.com
产品网址: http://www.bitdefender.com
产品存档: ftp://ftp.bitdefender.com/pub
本地发行公司: http://www.bitdefender.com/partner_list
BitDefender资料档案: http://kb.bitdefender.com

16.3.2. 分公司

BitDefender的分公司都非常乐意在它们的业务区内给您提供商业或主要事务的服务。以下是它们的地址以及联络电话号码。

美国U.S.A

BitDefender, LLC
6301 NW 5th Way, Suite 3500
Fort Lauderdale, Florida 33309
Web: http://www.bitdefender.com
技术支持:

■E-mail: support@bitdefender.com
■电话:
- 400-8800-361 (中国)
- 400-8800-361 (中国)

客户服务:

■E-mail: customerservice@bitdefender.com
■电话:
- 400-8800-361 (中国)
- 400-8800-361 (中国)

德国Germany

BitDefender GmbH
西欧总部
Karlsdorferstrasse 56
88069 Tettnang
德国Germany
电话号码: +49 7542 9444 60
传真号码:+49 7542 9444 99
电子邮件: info@bitdefender.com
销售: sales@bitdefender.com
Web: http://www.bitdefender.com
技术部: support@bitdefender.com

英国和爱尔兰

维多利亚广场
伯明翰
B1 1BD
电话号码:+44 207 153 9959
传真号码: +44 845 130 5069
电子邮件: info@bitdefender.com
销售: sales@bitdefender.com
网页: http://www.bitdefender.co.uk
技术部: support@bitdefender.com

西班牙

Constelación Negocial, S.L
C/ Balmes 195, 2a planta, 08006
Barcelona
技术服务Soporte técnico: soporte@bitdefender-es.com
销售服务Ventas: comercial@bitdefender-es.com
电话号码Phone:+34 932189615
传真号码Fax:+34 932179128
产品网址Sitio web del producto: http://www.bitdefender-es.com

罗马尼亚Romania

BITDEFENDER
5th Fabrica de Glucoza St.
Bucharest
技术部: support@bitdefender.com
销售: sales@bitdefender.com
电话号码: +40 21 4085600
传真号码Fax: +40 21 2330763
产品网址: http://www.bitdefender.com

词汇

ActiveX

ActiveX 是一种写程序的模型，因此其他的程序和操作系统可以调用它。ActiveX 技术和微软（Microsoft）Internet浏览器一起使用来制造交互型的并看起来和运转起来跟计算机程序的网络网页，而不单单只是静止的网页。有了ActiveX，用户可以提问或回答问题，使用按钮和用其它的方式和网页互动。ActiveX控制多数是用Visual Basic写的。

值得注意的是Active X 完全的缺少安全控制；计算机安全专家不建议在网络中使用它。

Adware（广告软件）

Adware（广告软件）一般是跟免费的主机应用程序一起的，只要用户同意并接受Adware（广告软件）。因为Adware（广告软件）应用程序一般是在用户同意了一个注明其应用程序的用途的许可协议才安装的，所以它是没有犯罪的。

但是跳出的广告可以变成一件烦人的事，同时在某些情况下降低了系统性能。同时，有一些这样的应用程序收集的资讯可能关系到没有完全的意识到在许可协议里的条款的用户的隐私权。

Archive（存档文件）

含有已经被备份的文件的磁盘，磁带或是目录。

它是一个含有一个或很多个文件的压缩文件。

Backdoor （后门）

它是一个设计者或维修者故意留下的系统安全的漏洞。这样的漏洞的动机是不一定总是恶意的，比如有些操作系统本来就存在特意给的区域服务技术员或是卖主的修复程序员的特权户口。

Boot sector（引导扇区）

它是一个在每一个磁盘的开始的扇区来确定磁盘的体系结构（扇区大小，群集器（cluster）大小等等）。为了起动磁盘，引导扇区同样包含有载入操作系统的程序。

Boot virus（引导扇区病毒）

它是一个可以感染到固定磁盘或软盘引导扇区的病毒。如果尝试从被引导扇区病毒感染的磁盘启动，那么将会导致此病毒在内存里活动。从这时起，当每次您启动您的系统时，病毒将会在内存里活动。

Browser （浏览器）
它是网络浏览器的简称。它是一个用作查找和显示网络网页的软件应用程序。两个最受欢迎的浏览器是：Netscape Navigator和微软Internet 浏览器（Microsoft Internet Explorer）。这两个浏览器都是图形的，也就是说它们可以显示图像和文字。另外，现代多数的浏览器可以呈现多媒体资讯，包括声音和视频，虽然它们需要一些格式的插入件。

Command line （文字模式）
文字模式（command line）是一种指令下达的方式。用户者将指令输入银幕上所提供的空间。

Cookie
Cookies被描绘成含有有关个人计算机信息的小文件。这些信息可以被登广告者分析和利用您的在线兴趣和口味。在网际网络的领域，cookie技术还在发展并且其目的是直接瞄准您已经说过的您的兴趣的广告。Cookie对很多人来说是一把双刃剑。因为一方面它是有用的又适当，因为您只看到您感兴趣的广告。另一方面，它事实上涉及到“跟踪”和“跟随”您的网上行为。可以理解有一个隐私权和有些人不高兴他们被网站看作"SKU 数字" （就好像在包装纸上的条形码）的辩论。当然这样的观点是极端，但是在有些情况下是准确的。

Disk drive （磁盘驱动器）
可以从磁盘存载的仪器。

硬盘驱动器可在硬盘上存载资料。

软盘驱动器可在软盘上存载资料。

硬盘驱动器可以是内在或外在的。

Download （下载）
从主机往你的计算机的复制的过程。时常用于指从网上服务器往自己的计算机复制的过程。

E-mail （电子邮件）
Electronic mail的缩写。Internet上的每一个用户都可拥有一个电子邮件信箱地址。在发送电子邮件是，用户必须输入接收方的电子邮件地址。在Internet上电子邮件地址通常的格式为person@computer。

事件
它是一个被程序发现并具有特定意思的事件。这样的事件可以是用户的任何举动,比如点击鼠标或按键，或者是系统事件，比如用尽内存。

False positive （错误检验结果）
系统错误认定受感染文件的情况。

Filename extension（文件扩展名）
它是文件名句号后的部分，表示文件类型。

许多操作系统（比如Unix，VMS，和MS-DOS）都用文件扩展名，它同常长于一到三个字母。例如C源程序的“c”，PostScript语言的"ps"，文本文件的"txt"。

Heuristic（启发式）
它是一个用来确认新病毒的基于规则的方法。这方式的扫描不需要依靠病毒签名。启发式扫描的好处不会查出变种病毒的原病毒。但是，它有可能报告一个普通程序中可疑编码，从而导致“错误检验”（"false positive"）。

IP（网际协议）
网际协议（Internet Protocol） – 在TCP/IP 协议组里的一个IP定址，路由和分裂和从新组和IP包裹为负责的协议。

Java applet（Java 小程序）
它是一个为只在网页上运行的Java程序。为了要在网页上用Java 小程序，您需要指明这个Java 小程序的名字和Java 小程序可以利用的大小（长和宽，以像素为单位）。当一个含有Java 小程序的网页被访问时，浏览器会从服务器下载其Java 小程序并在客户端上运行。Java 小程序和应用程序不同，它是被一严格的安全协议所管理。

例如，尽管Java 小程序是在客户端上运行，但是它不可以读或写在客户端的计算机。另外，小程序被进一步的约束着，所以它只可以读和写从在它服务的同一域里数据。

Macro virus （宏病毒）
一种伪装为宏潜入在文件内的电脑病毒。许多应用程序都支持宏，比如视窗Word和视窗Excel。这些应用程序让您在文件内含宏。每当文件被打开时宏也会被启动。

这些程序在文档中嵌入了宏,每次打开文档就将执行宏.

Mail client （电子邮件应用程序）
电子邮件应用程序能使用户可以编写、接收和发送邮件。

Memory （内存）
系统的内存。指的是芯片式的存量。计算机通常都有随机存取存储器（或内存）(RAM 或 physical memory 或main memory)在内。

Non-heuristic(非启发式)
这扫描方法在于特定的病毒标签上。非启发式扫描最大的好处是不会错把类似病毒的文件当成病毒， 也因此不会产生错误的警报。

Packed programs （压缩文件）

压缩后的文件。许多操作系统和应用程序都有可以压缩文件的指令让用户减少存量。比如说，原本需十字节的文件在压缩后只需两字节。这是因为系统将空格以及接下来的字用一种新字母取代。这只是压缩的其中一种方式。

减少字符串中由于字符的重复出现而占据的数据媒体空间并且等于压缩后的文件。

Path （路径）

指往系统内一个文件或文档的路径。通常，文档是从最高等级的开始分等级地分类的。或指两个终点之间的路径，比如两台计算机之间的路径。

网络中任意两个网点之间的一段路由。在数据库中,从根段到个别段之间的段(具体)值序列。在IBM的通信系统ACF/VTAM中,连接终端和主处理机中应用程序的中间网点和数据链路。在IBM系统网络体系结构(SNA)中,两个网络的可寻址单元(NAU)之间 交换的信息所经过的一系列通路控制网络成分(路径控制程序和数据链路控制程序)。通路由 虚拟路由及其扩充路由(如果有的话)所组成。

Phishing

网上欺骗的一种方式。骗子伪装成合法公司的职员发送电子邮件给目标，意图要目标公开自己的个人资料，在用此资料进行偷窃。电子邮件会将目标连往一个网站，便要求目标输入合法公司已经拥有的各人资料（比如密码，信用卡，身份证号码和银行户口号码），可网站是欺骗的工具。

Polymorphic virus （多形病毒）

可以侵略系统也同时可以变形的电脑病毒。这些病毒没有一定的二元图，也因此非常难查到。

Port （端口）

可以连接器材的端口。私人计算机共有几种端口。系统内部已有可连接硬盘，银幕和键盘的端口。系统外部又有可连接调制解调器，打印机，鼠标以及其他器材的端口。在TCP/IP和UDP网络内的终点，端口号数能指定用什么端口。

比如说，端口80是HTTP（WWW服务程序所用的协议）所用。在计算技术和通信技术中,网点上的一种功能部件,通过它数据可进入或离开一个数据网络或计算机。数据进出某功能部件的一种接口。

Report file （报告文件）

此文件列出已运用过的措施。BitDefender 保存着一个含有扫描过的路径，文件夹，存档和文件资料，以及受感染和可以文件的报告文件。

Rootkit程序

Rootkit是一系列提供系统管理的软件工具,这个名词首先是在UNIX操作系统中出现的,指提供入侵管理权的编译工具,他们能隐藏自己不被系统管理员发现.

Rootkits 的主要作用是隐藏进程、文件、登录信息或日志，同时，如果正当的软件用于不正当的目的，它们也可从终端、网络连接或外设拦截数据。

Rootkits 本质上不具有恶意目的。例如，系统甚至某些应用程序会隐藏所使用的关键文件。然而，它经常用于隐藏恶意软件或系统闯入者的出现。当与恶意软件结合在一起时，Rootkits构成了对系统完整性和安全的最大威胁。它们可以监控流量、创建系统的后门，更改文件以及日志以避免被发现。

Script （脚本）

是宏或批处理文件的另外一种名称。运用脚本不需用户者指令。

Spam （垃圾邮件）

电子垃圾邮件或新闻组的垃圾新闻。一般它是指任何的未经过用户者同意就发送的邮件。

Spyware（间谍软件）

任何擅自通过网络联系累积用户者资料的软件。通常用于传送广告。它们通常潜入可从网上下载的免费或共享软件；不过大多数的免费或共享软件都不藏间谍软件。安装后，间谍软件会通过用户的网络联系把资料暗中传送出去。

这些软件有取得电子邮址，密码和信用卡号码的能力。间谍软件与木马相似的是用户都是在不知道的情况下安装它们的。

下载和安装对等的(peer-to-peer/p2p)软件是非常容易受间谍软件侵入的方式。除了采用不道德的方式偷取个人资料以外，间谍软件也会使用户的系统缓慢，使用系统的内存和网络联系带宽。长期内会使用户系统运行不顺畅，甚至是系统崩溃。

Startup items （起动物）

在这文件夹内的任何文件都会在系统起动时起动。起动时的银幕，音响效果，日志或任何应用程序都能成为起动物。通常在此文件夹内的文件都是别名文件。

系统托盘

和视窗95同时推出，在视窗任务栏内的系统任务栏（通常在系统时钟旁）。它含有小型图形让用户轻易运用系统功能（比如传真，打印机，调制解调器，声量等）。双击任何图形可打开功能选项和详情。

TCP/IP

传输控制/互联网协议。用于不同操作系统，体系结构的网络基本协议。它定下了计算机之间的联络协议和规则，是互联网以及许多网络的通讯基础之一。

Trojan （木马）

伪装为良性程序的危险应用程序。此病毒种类并不会繁殖，但一样有危害性。最普遍的木马常伪装为反病毒软件，但其实是木马病毒。

一般此种病毒分成服务器端和客户端两部分，如计算机网络中服务器端被此程序感染，别人可通过网络其它计算机任意控制此计算机，并获得重要文件。国内流行的此类病毒有BO、NETSPY等。

更新

取代旧版本的新版本软件。另外，安装更新时，系统通常会确定旧版本已安装在系统内否则无法继续更新。

BitDefender拥有自己的更新模块让您指定或自动更新软件。

Virus （电脑病毒）

在您不知道的情况下存入系统并且启动的程序。多数的电脑病毒都能繁殖。所有的电脑病毒都是人造的。要创建一个会自己繁殖的电脑病毒并非一件难事。就连这样的简单病毒都有一定的危害性。它能够有尽系统的内存，使系统进入暂停的状态。更恶劣的病毒有通过网络联系以及保安措施的能力。计算机病毒实质上是指编制或在计算机程序中插入破坏计算机功能或数据，影响计算机使用并能自我复制的一组计算机指令或程序代码。一般病毒具有以下特性：可执行性——与其他合法程序一样，是一段可执行程序，但不是一个完整的程序，而是寄生在其他可执行程序上，当病毒运行时，便于合法程序争夺系统的控制权，往往会造成系统崩溃，导致计算机瘫痪。传染性——他通过各种渠道（磁盘、共享目录、邮件等）从已被感染的计算机扩散到其他机器上，在某种情况下导致计算机工作失常。潜伏性——一些编制精巧的病毒程序，进入系统之后不马上发作，隐藏在合法文件中，对其他系统进行秘密感染，一旦时机成熟，就四处繁殖、扩散。有的则执行格式化磁盘、删除磁盘文件、对数据文件进行加密等使系统死锁的操作。可触发性——病毒具有预定的触发条件，可能是时间、日期、文件类型或某些特定数据等。一旦满足触发染或破坏工作，使病毒进行感染或攻击；如不满足，继续潜伏。针对性——有些病毒针对特定的操作系统或特定的计算机。隐蔽性——大部分病毒代码非常短小，也是为了隐蔽。一般都夹在正常程序之中，难以发现，一旦发作，则已经给计算机带来了不同程度的破坏 。

Virus definition （病毒）

电脑病毒的二元图。反病毒软件用此找寻和消灭病毒。

Worm （蠕虫）

可以在网络上繁殖的程序。蠕虫不能潜入其他应用程序。