bitdefender
BUSINESS SOLUTIONS

BUSINESS CLIENT

用户使用指南

bitdefender

BitDefender Business Client
用户使用指南

出版方 2010.06.15

法律须知

目录

前言

本指南的目的是提供最终用户 BitDefender Business Client 概述了产品的安全功能，并确保其顺利同 BitDefender 互动。 本书的资料介绍不仅只适合计算机专业人员，任何人都可以在Windows能够轻松理解和操作。

预祝您阅读愉快，开卷有益！

1. 本书中所使用的惯例

1.1. 排印约定

本书中使用了几种不同的文本类型，提高本书的可读性。下表分别列出它们的内容和涵义。

字型举例	描述
sample syntax	格式示例采用 monospaced 字体显示。
http://www.bitdefender.com	链接到外部服务器的 URL 链接，包括 HTTP 或 FTP 服务器。
sales@bitdefender.com	电子邮件地址被插入文本内以提供联系信息
“前言” （第 ix 页）	这是一个内部链接，指向本书内部的章节。
filename	文件和目录都使用 monospaced 字体。
option	所有产品选项都以粗体字显示。
sample code listing	代码采用monospaced字体显示。

1.2. 备注说明

这些警告内容都在文本内，附有生动的图形标记，提醒您注意当前文件的更多重要信息。

注意

注意事项的篇幅不长。虽然您可以忽视它，但它可能提供有用的信息，比如具体功能或指向其他相关主题的链接。

重要
这里需引起您的注意，建议不要跳过。它提供的信息虽然不是主要问题，但却非常重要。

警告
该信息非常重要，请谨慎处理。根据提示进行操作对您有益无害。由于它涉及到非常危险的内容，您应该仔细阅读和理解它。

2. 本书结构

本书由 3 个部分组成，包括下列主要议题：基础管理、高级管理和联系信息。 此外，词汇表可以帮助您了解技术术语。

基础管理. 包含 BitDefender 的基本工作。

高级管理. 包含 BitDefender 安全功能的详细介绍。 了解如何配置和使用所有的 BitDefender 模块，以便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、不良内容等等）的侵袭。

注意
这部分只提供给超级用户，充分配置 BitDefender。

联系方式. 为您提供 BitDefender 的联系信息。

词汇表. 词汇表解释一些您会在此文件中发现罕见的和技术性的词汇。

3. 欢迎您的意见和建议

我们欢迎您对本书提出意见，尽我们的所能验证所有的资料。如果您觉得这本书里有什么缺点,或认为有可以改善的地方，请写信给我们，以帮助我们为用户提供最好的文件。

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

重要
请用英语书写与文档相关的电子邮件，以便我们有效地处理。

基础管理

1. 开始使用

BitDefender Business Client 是复杂的企业安全和管理解决方案的一个组成部分，它能集中管理和保护公司的工作站。

网络安全管理员将在您的计算机上远程安装和配置 BitDefender Business Client。一旦安装 BitDefender Business Client，您的计算机可以免受各种威胁（如恶意软件、垃圾邮件、黑客攻击、不良内容等）的侵袭。

一般来说，您无需配置 BitDefender Business Client，因为这是由网络安全管理员远程进行的。然而，您可能需打开 BitDefender 界面执行一些基本操作，如备份数据等。 您的系统管理员也可以要求您更新 BitDefender 和扫描计算机。

1.1. 操作模式

你与产品的交互和使用方式，很大程度上取决于它的操作模式。 BitDefender Business Client 可以在下列模式下操作：

- 受限用户模式
- 超级用户模式

默认的操作模式是受限用户模式，只有您的网络安全管理员可以改变它。

1.1.1. 受限用户模式

在受限用户模式下，BitDefender Business Client 的配置和管理完全取决于网络安全管理员。 您只能查看 BitDefender 的状态和配置，还能执行基本的手动任务，如更新 BitDefender、扫描计算机和备份数据。

根据网络安全管理员设置的不同，您的显示器上可能显示各种不同的 BitDefender 弹出式窗口和警报。

反垃圾邮件工具条，会集成到一些公用的电子邮件客户端，并允许你控制和改善反垃圾邮件保护。 同样，你可以管理 BitDefender 提供给 Internet Explorer 使用的反网络钓鱼工具条 进行反网络钓鱼保护。

注意

受限用户模式下，您可以在用户指南 “基础管理” （第 1 页） 部分中找到使用 BitDefender Business Client 所需要的信息。

1.1.2. 超级用户模式

超级用户模式下，您可以完全控制 BitDefender Business Client。 不同于受限用户模式的是，超级用户模式允许您全面配置和定制 BitDefender 所提供的保护功能。 超级用户的一个重要好处是只有他们才能够使用 整套备份选项。

注意
除了这部分的基本信息，你也可以参考“高级管理”（第 52 页）部分的用户指南，了解如何充分配置 BitDefender Business Client。

1.1.3. 更改操作模式

如前所述，只有网络管理员可以更改 BitDefender Business Client 的操作模式。通常情况下，更改会立即生效，而不对使用者有任何提示。如果在模式改变的时候，产品界面被打开了，您将会被通知用户权限被改变了，并需要重新启动产品界面。单击 是 重新启动产品界面，立即更改用户权限。

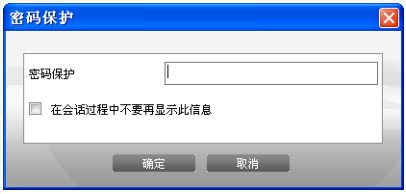
网络管理员可以配置 BitDefender Business Client，允许授权用户暂时更改操作模式(用户权限)。 这种情况下，您应该提供密码执行该操作。

要更改操作模式，请按照下列操作进行：

1. 右键单击系统托盘上的 BitDefender 图标并选择切换到超级用户模式。

注意
如果菜单上没有找到该选项，说明 BitDefender 没有配置为允许本地更改操作模式。

2. 提示您提供密码



超级用户密码

在相关的编辑栏输入网络管理员给您的密码。

3. 点击 确定。

此更改是暂时的。如果您注销、重启或关闭计算机，下次登录 Windows 时，BitDefender 将自动在受限用户模式下工作。

要手动转换用户权限，右键单击 系统托盘上的 BitDefender 图标，然后选择 切换到受限用户模式。

1.2. 主界面

您可以在主界面检查 BitDefender 的状态和配置，并采取预防措施来保护您的数据安全。 此外，如果您是超级用户，您可以根据需要配置 BitDefender 并创建复杂的备份任务。

打开主界面：

- 使用 Windows 开始菜单，按照以下路径：开始 → 程序 → BitDefender Business Client → BitDefender Business Client。
- 双击系统托盘上的 BitDefender 图标 。
- 双击桌面上的 BitDefender 图标。

BitDefender 默认打开基本视图，这是适合大多数用户的简单界面。

基本视图主界面

基本视图界面包含两个部分：

- 总体状况 部分：为您提供 BitDefender 主要模块(反病毒、防火墙及更新)的状态信息。
- 手动任务部分：协助您保护系统和您的数据的安全。 在这里，您可以更新 BitDefender、扫描计算机或文件，以及备份或恢复数据。 欲了解更多信息，请参阅 “手动任务” （第 9 页）.

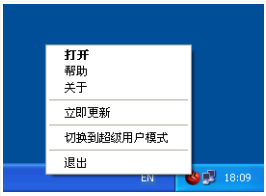
基本视图不论 BitDefender 操作模式，看上去是一样的。除了某些手动任务、备份设置只在超级用户模式下可用。

您可以切换到高级界面(高级视图)，在这里您可以访问产品设置和统计数据。 在受限用户模式，您只能看到配置的设置和统计相关产品操作，而在超级用户模式可以配置所有设置。 从 总体状况区域上 BitDefender 主要模块所对应的查看更多设置链接，快速访问 每个模块的高级视图。

如果你需要更多的帮助，请点击窗口底部的 帮助 链接。

1.3. 系统托盘图标

要想更快捷地管理整个产品，您可以使用 BitDefender 系统托盘图标。 如果双击此图标，主界面将会打开。 另外，通过右键点击图标，会出现一个弹出式菜单，您就可以迅速管理 BitDefender 产品。



系统托盘图标

- 打开 – 打开 Bitdefender 主界面。
- 帮助 – 打开帮助文件。
- 关于 – 打开一个包含 Bitdefender 及支持信息的窗口。
- 立即升级 – 立即开始升级产品。
- 切换到超级用户模式 – 使授权用户暂时更改产品操作模式。 该选项只适用于在您的网络管理员做好了相应配置的情况下。 欲了解更多信息，请参阅 “操作模式” （第 2 页）。
- 退出 – 关闭 BitDefender 应用程序。

1.4. 扫描活动工具条

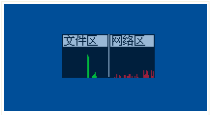
扫描活动工具条 以图形化方式显示您系统上的扫描活动。

重要

在受限用户模式下，根据网络安全管理员所设定的设置，扫描活动工具条可能不可见。 如果您想启用或禁用图形可视化，请与网络安全管理员联系。

在（文件区）显示绿色条表示每秒扫描的文件数，范围从 0 到 50。

在 网络区 显示红色条表示每秒传输的 KB 数(从 Internet 上收发)，范围从 0 到 100。



活动工具条

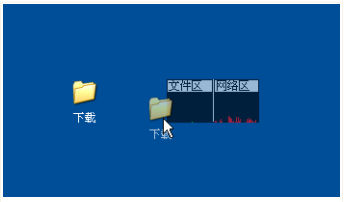
注意

扫描活动工具条将通过在相应的区域（文件区域 或 网络区域）显示红叉，表明实时保护或防火墙被禁用。

1.4.1. 扫描文件及文件夹

您可以用扫描活动工具条快速扫描文件或文件夹。 拖动您想扫描的文件或文件夹，将其放到 扫描活动工具条上，如下图所示。

拖放扫描



放下文件

BitDefender 扫描程序 将会出现并引导您完成整个扫描过程。

1.4.2. 显示/隐藏扫描活动工具条

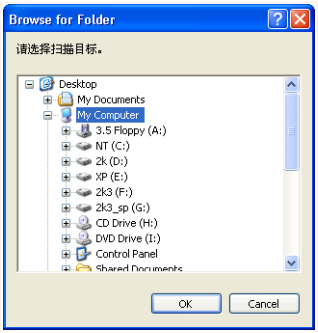
如果您是一个超级用户，您可以根据下列方式配置 BitDefender 显示/隐藏扫描活动工具条：

1. 点击 切换到高级视图（如果你在基本视图）。
2. 点击 高级设置。 显示一个新窗口。
3. 选择/取消选择启用扫描活动工具条(屏幕产品活动图形）复选框。
4. 点击 确定 保存修改并关闭窗口。

1.5. Bitdefender 手动扫描

如果您想快速扫描某一个文件夹，您可以使用 BitDefender 手动扫描。

要运行 BitDefender 手动扫描，请从 Windows 开始菜单按以下顺序点击： 开始 → 程序 → BitDefender Business Client → BitDefender 手动扫描。 就会出现下面的窗口：



Bitdefender 手动扫描

您所要做的是浏览文件夹，选择您想扫描文件夹并点击 确定。 BitDefender 扫描程序 将会出现并引导您完成整个扫描过程。

2. 手动任务

基本视图的 手动任务 部分，可以帮助您采取预防措施保护您的数据。 以下任务在受限用户和超级用户模式下都是可用的。

- 立即升级 – 立即开始升级产品。
- 扫描 “我的文档” – 扫描 “我的文档” 目录。
- 深度系统扫描 – 开始对您的电脑进行一次全面扫描(包括存档)。
- 全面系统扫描 – 开始对您的电脑进行一次全面的扫描(不包括存档)。
- 启动备份向导 – 启动一个简易的 5 步向导程序备份你的数据。
- 启动恢复向导 – 启动一个简易的4步向导程序恢复你的数据。

超级用户模式下有一个额外的任务，即备份设置，它可以让您建立和执行详细的备份操作。

重要
如果网络安全管理员选择从项目中移除备份和恢复选项，这些选项可能会丢失。

这些任务相当于附加的安全层，为您的数据提供额外的安全保护。 在本章，您可以找到关于给受限用户可用任务的详细资料。

注意
您可以在 高级视图 左边的菜单中点击 快速任务 访问相同的任务。

2.1. 更新 Bitdefender

每天都会发现新病毒，所以需要及时更新 BitDefender 病毒库。

如果您想更新 BitDefender，只要点击 立即更新。 升级进程会被启动，并显示下面的窗口：

更新 Bitdefender

在这个窗口中，您可以看到更新过程的状态。

升级过程即时执行，更新的文件会被逐步进行替换。这样，升级过程不会影响产品的正常运行，同时又可减少系统漏洞。

如果您想关闭窗口，只要单击 关闭。 不过，窗口关闭后并不会停止升级进程。

重要

如果您通过拨号方式连接到网络，建议您定期手动升级产品。

如果您通过宽带或 DSL 连接到互联网，您可以配置 BitDefender 自动更新。 要配置自动更新，需要切换到高级视图，转到更新>更新 并选择更新被禁用 复选框。 要做好这个配置，您必须是一个超级用户。

如果需要，请重启计算机。. 在一个重要的项目更新后，您将被要求重启您的计算机： 如果更新需要重新启动而不想被提示，选中 无需提示，等待重新启动。 这样，在下一次更新需要重启时，产品会继续使用旧的文件保持工作，直到您重启系统。

点击 重新启动 会立即重启您的计算机。

如果您想稍后重启系统，只要点击确定。 我们建议您尽快重启您的计算机。

2.2. 用 BitDefender 扫描计算机

要在您的计算机上扫描恶意软件，请点击对应的按钮运行一个扫描任务。 下表介绍各个扫描任务：

任务	描述
扫描“我的文档”	使用此任务扫描当前用户的重要文件夹：我的文档，桌面和启动项。 这将会确保您的文档的安全性，给您一个安全的工作空间并清理在启动项运行的应用程序。
深度系统扫描	扫描整个系统，包括压缩文档。 在默认配置下，它扫描威胁到您系统安全的所有类型的恶意软件，如病毒，间谍软件，广告软件， rootkit 和其他。
全面系统扫描	扫描整个计算机，不扫描压缩文档。 在默认配置下，它扫描威胁到您系统安全的所有类型的恶意软件，如病毒，间谍软件，广告软件， rootkit 和其他。

注意

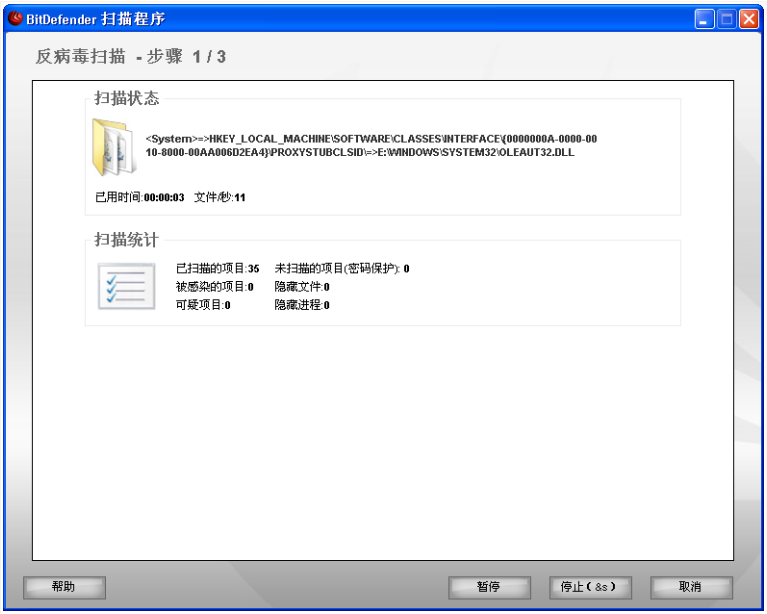
因为 深度系统扫描和全面系统扫描 任务将分析整个系统，扫描可能需要持续一段时间。因此，我们建议您以低优先级方式，最好是在系统空闲的时候运行这些任务。

当您开始一个请求式扫描过程，无论是快速或完整扫描， bitdefender 扫描程序就会出现。

请遵循向导程序的三个步骤来完成扫描过程。

2.2.1. 步骤 1/3 — 正在扫描

Bitdefender 将开始扫描选定的对象。



正在扫描

您可以看到扫描的状态和统计(扫描速度，消耗时间，扫描/感染/可疑/隐藏对象的数量及其他)。

注意
扫描过程可能需要较长时间，取决于扫描的复杂程度。

要暂停扫描，只要点击 暂停 ，您需要点击 继续 恢复扫描。

可以在任何时候停止扫描，点击 停止&是. 您将直接跳到向导的最后一步。

请等待 Bitdefender 完成扫描。

2.2.2. 步骤 2/3 — 选择操作

当扫描完成后，一个新的窗口将出现，就您可以看到扫描的结果。

操作

您可以看到有多少问题影响到您的系统。

被感染的对象根据它们所感染的病毒分组显示。 点击对应某个病毒的链接，可以看到感染对象的更多信息。

您可为每个问题组选择一个整体的操作，或者为每个问题选择单独的操作。

您可以通过菜单选择:

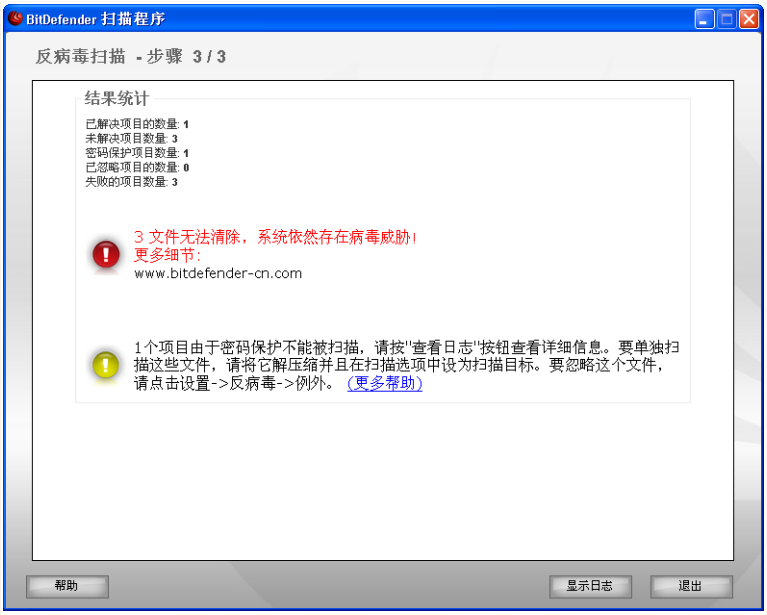
操作	描述
已处理	已处理检测出的文件。
清除病毒	从感染文件中移除恶意代码。
删除文件	删除检测出的文件。
移动到隔离区	移动受感染文件到隔离区。

操作	描述
重命名名称	通过追加 .bd.ren 在他们的名称后面更改隐藏文件的名称。 因此，您将能够在您的计算机上搜索和找到这些文件。

点击 继续 执行所选的操作。

2.2.3. 步骤 3/3 — 查看结果

当 BitDefender 完成处理检测出的问题后，将会在一个新窗口显示扫描结果。



总结

您可看到扫描结果的总结。 点击查看日志 查看扫描日志。

重要
如有需要，请重新启动系统以完成清除过程。

点击 退出 关闭结果窗口。

Bitdefender 未能解决部分问题

在大多数情况下，Bitdefender 能成功清除受感染的文件或隔离受感染的文件。 但是，有些问题当时不能得到解决。

警告
如果有未解决的问题，建议您联系网络安全管理员。

Bitdefender 检测密码保护项目

密码保护的类别有两种类型：存档和安装程序。 除非它们含有受感染的文件并执行，否则他们将不会威胁系统安全性。

确保这些项目都是要清除的：

- 如果密码保护项目是一个有保护密码的存档，解压这个文件并单独对他们进行扫描。 最简单的扫描方法是右键点击，并从菜单中选择 BitDefender Business Client。
- 如果密码保护的项目是安装程序，在执行这个安装程序之前，确保 实时防护 被启用。 如果安装程序被感染，BitDefender 将检测和隔离感染源。

如果您不想让这些文件再次被 BitDefender 检测，您必须将它们添加到扫描例外。要添加扫描例外，切换到高级视图，然后转到 反病毒> 例外。 欲了解更多信息，请参阅 扫描排除的对象。

重要
如果 BitDefender 操作在受限模式下，请要求您的网络安全管理员配置扫描例外。

Bitdefender 检测到可疑文件

可疑文件是被启发式分析程序检测为可能感染了未知的病毒特征码。

如果在扫描期间发现可疑文件，您会被要求提交给 BitDefender 实验室。 点击 确认 发送这些文件给 Bitdefender 实验室进行分析。

2.3. 备份数据

数据备份是一个数据安全性的重要部分. 备份数据有助于防止数据丢失。

有很多情况导致数据丢失，如:

●意外删除的文件和文档
●硬盘驱动器故障
●病毒损坏或删除的文件

如果您定期备份您的数据，在必要的时候您可以恢复它们。 这样，您就可以恢复丢失的文件或返回到以前版本的文件。

BitDefender 包含的备份模块，它可以帮助您对有价值的数据进行备份。 您可以备份下列位置的数据:

●您的计算机。
●可移动磁盘(CD/DVD)。
●USB 盘。
●网络位置。
●FTP 服务器。

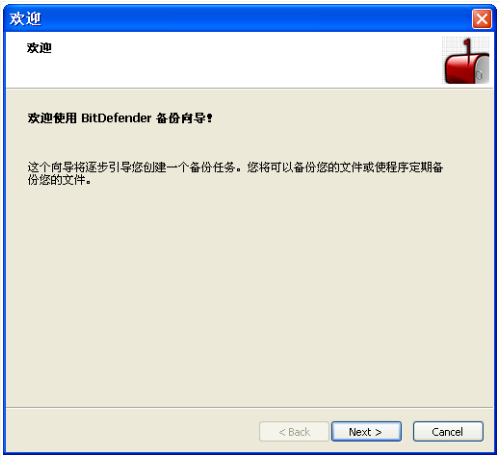
通过点击 启动备份向导 ，向导将引导您创建一个备份任务。 在结束这个过程之前，您将能够立即备份您的文件或建立计划表以后再将他们备份。

注意

高级用户可以使用 BitDefender 备份配置复杂的备份工作。 欲了解更多信息，请参阅“备份设置”（第 173 页）.

2.3.1. 步骤 1/5 – 欢迎窗口

这是欢迎页面。

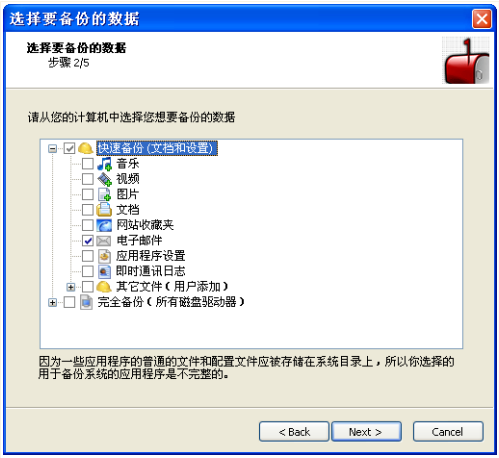


欢迎窗口

点击 下一步。

2.3.2. 步骤 2/5 - 选择备份内容

在这里，您可以选择备份您计算机上的哪些数据。



选择要备份的数据

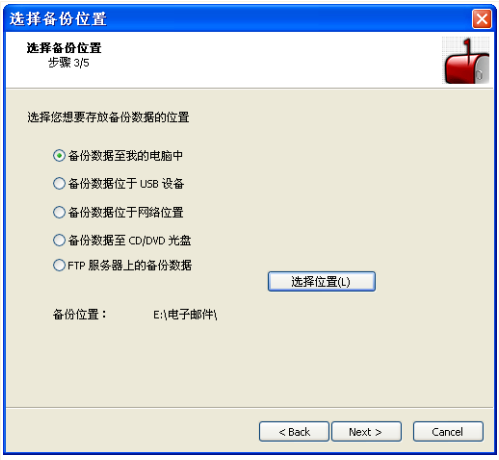
您既可以选择 快速备份(您的音乐，影片，图片，电子邮件，应用程序设置等等)，也可以选择 完整备份（所有分区)。

点击 其它文件 ，从桌面添加其他文件到快速备份 。完整备份 也可以被很容易的定制，从某个分区通过选择一些目录来备份。

点击 下一步。

2.3.3. 步骤 3/5 - 选择备份位置

在这里，您可以选择备份数据所保存的地点。



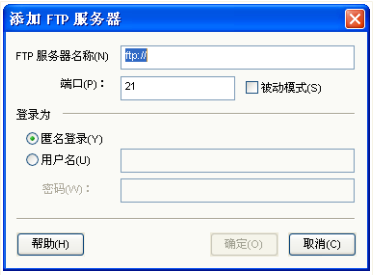
选择备份位置

您可以选择下列选项之一：

- 备份数据到我的计算机上
- 备份到我的 USB 盘上
- 备份数据在网络位置
- 备份数据到 CD 或 DVD
- 备份数据到 FTP 服务器

如果您决定备份数据到您的计算机上，您的 USB 盘上，或者网络的某一位置，点击选择位置，来选择在哪里保存数据。

如果您想在 FTP 服务器上做备份，点击选择位置 并添加 FTP 服务器。 显示一个新窗口。



添加 FTP 服务器

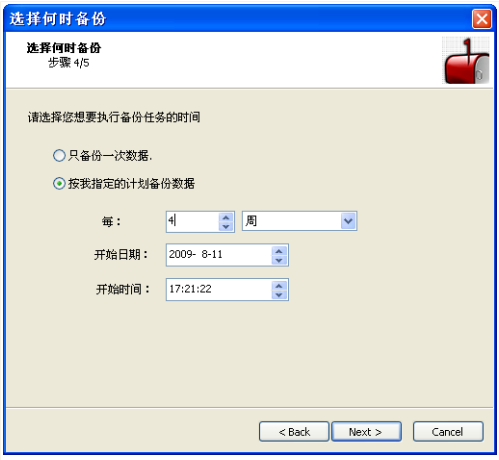
您必须配置 FTP 服务器连接设置如下：

1. 在相应的编辑栏输入 FTP 服务器名称。
2. 如果 FTP 务器使用不同的端口而不是默认端口 21 ，在相应的编辑栏中输入端口号。
3. 要使用被动模式(FTP 服务器启动连接)，选择 被动模式 复选框。
4. 如果 FTP 服务器允许匿名访问，您可以选择匿名 选项。 否则，选择 用户名 – 在FTP服务器输入用户名和密码的账户。
5. 点击 确定。

点击 下一步。

2.3.4. 步骤 4/5 – 选择备份时间

在这里，您可以选择何时备份您的数据。



选择何时备份

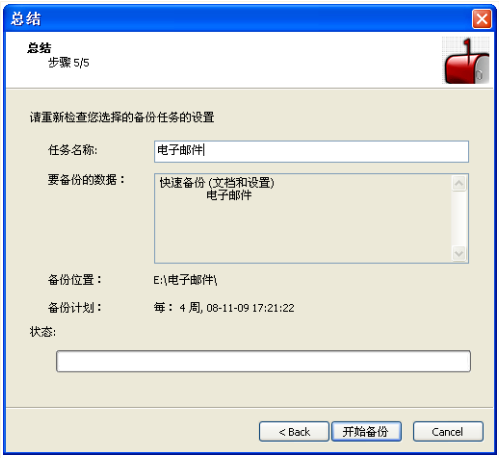
要这个时间点上备份数据，点击 只这次备份数据，要在稍后时刻，以时间表形式备份您的文件，点击 按我指定的时间表备份数据。

如果您选择 按我指定的时间表备份数据，您可以指定多久预定任务运行：每天或每周。您还可以指定开始日期和时间。

点击 下一步。

2.3.5. 步骤 5/5 - 总结

在这里，您可以重新查看备份作业的设置并开始进行备份。



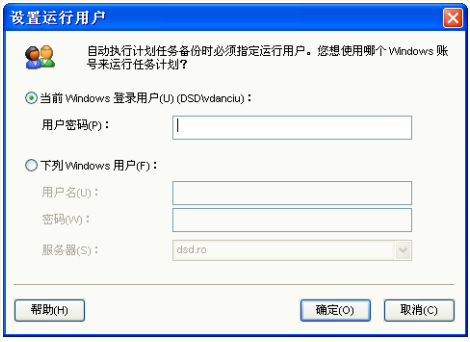
总结

您必须在相应的编辑栏键入一个任务名称。 您可以返回到前面的步骤，做任何更改(点击返回)。

如果您满意您的设置，点击开始备份。 等待 BitDefender 完成备份并点击 完成。

注意

第一次，您需要建立一个备份时间表，将提示您指定 Windows 账户用于运行工作。



设置运行用户

要使用当前用户账号，只需在相应的编辑栏输入密码。 如果您想使用不同的账号运行备份，选择 下列 Windows 用户 并填写相应的编辑栏。

- 用户名 – 键入一个 Windows 账户名。
- 密码 – 请输入指定用户账号的密码。
- 服务器 – 输入域服务器的名称。

点击 确定 继续。

2.4. 还原备份数据

使用先前的 BitDefender 备份数据，您可以轻松恢复丢失的数据。 通过点击 启动恢复向导，向导将引导您完成恢复本地备份数据过程。

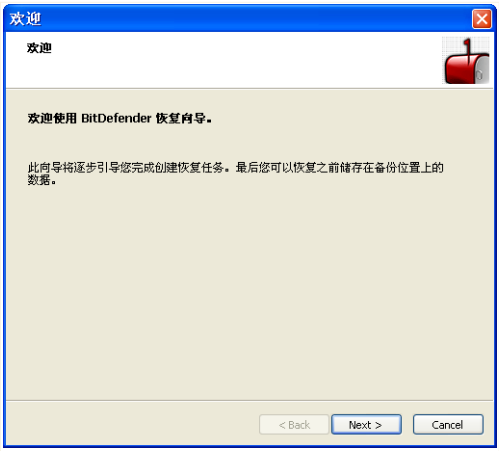
注意

在恢复任何数据之前，确认被恢复的设备是可用的。 根据您所使用的设备，您可能需要采取以下行动:

- 将备份的 U 盘插入到 USB 端口。
- 把备份的 CD/DVD 放入光驱。
- 检查是否可以连接到备份储存的网络位置或 FTP 服务器。

2.4.1. 步骤 1/4 - 欢迎窗口

这是欢迎页面。

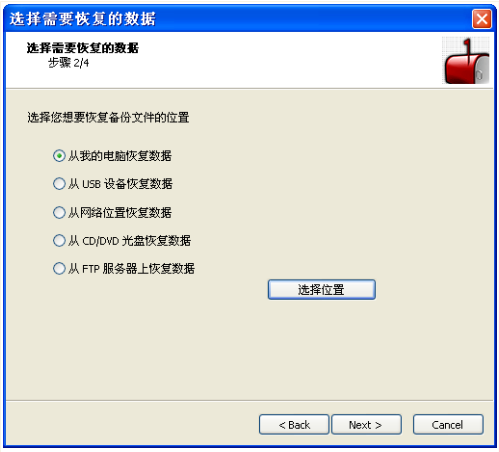


欢迎窗口

点击 下一步。

2.4.2. 步骤 2/4 - 选择从哪个备份进行恢复

在这里，您可以选择一个位置，您可以从这个位置恢复文件。



选择备份位置

您可以选择下列选项之一：

- 从我的计算机恢复数据
- 从 USB 盘恢复数据
- 从一个网络位置恢复备份
- 从 CD/DVD 恢复备份
- 从 FTP 服务器恢复数据

选择选项之后，点击 选择位置，并选择从保存的位置恢复数据。

点击 下一步。

2.4.3. 步骤 3/4 – 选择恢复位置和文件

在这里，您可以选择指定的文件，以恢复数据。

选择恢复位置和文件

您可做以下选择:

- 恢复备份到原来的位置
- 恢复备份到一个不同的位置
- 恢复所有数据从选定备份位置
- 恢复指定的文件
- 恢复时重写现有的文件

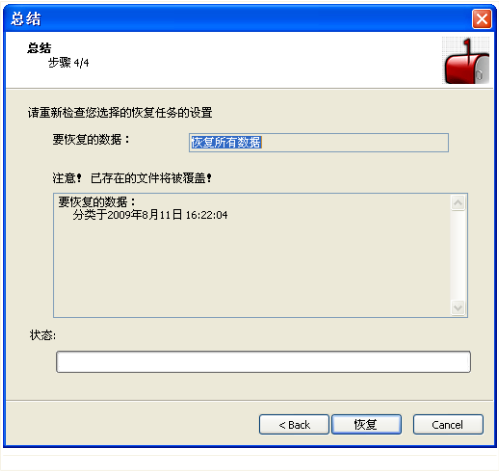
如果您想恢复数据到另一个位置或只是指定的文件，通过点击相应按钮选择位置和数据。

恢复时为了避免覆盖现有的文件，清除 恢复时，覆盖现有文件 复选框。

点击 下一步。

2.4.4. 步骤 4/4 – 总结

在这里,您可以复查恢复项目的设置并启动恢复过程。



单击 恢复，如果您满意您的设置。 等待 BitDefender 恢复选定的数据，然后点击完成。

3. 警报和弹出式窗口

BitDefender 使用弹出窗口和警报通知您有关其操作或可能令您感兴趣的特殊事件，并提示您在必要时采取行动。 本章介绍了可能会出现在您屏幕上的 BitDefender 弹出式窗口和警报。

注意
在受限用户模式下，弹出式窗口和警报可能会也可能不会显示，经由网络安全管理员不同的设置。

3.1. 弹出式窗口

弹出式窗口是指临时出现在屏幕上的小窗口，通知 BitDefender 各种活动，如电子邮件扫描，一个新的计算机登录到您的无线网络，防火墙规则增加等。 出现弹出式窗口时，您最多只需要点击 确定 按钮或链接。

如果您不希望显示弹出式窗口，请按照下列步骤操作:

1. 点击 切换到高级视图（如果你在基本视图）。
2. 点击 高级设置。 显示一个新窗口。
3. 取消选择 显示弹出式窗口（屏幕上的显示） 复选框。
4. 点击 确定 保存修改并关闭窗口。

如果您是一个受限用户，请要求您的网络安全管理员，阻止 BitDefender 弹出式窗口。

3.2. 警报

警报是一个对于您操作的提示对话框。 BitDefender 警报包括:

- 病毒警报
- 设备检测警报
- 防火墙警报
- 反网络钓鱼警报
- 注册表警报
- 脚本警报
- Cookie 警报

●用户控制警报

3.2.1. 病毒警报

BitDefender 保护您的计算机免受各种恶意软件的威胁，如病毒，间谍软件或 rootkit 。

当您尝试访问文件时， 实时保护 首先会对各个文件进行扫描。 如果该文件被感染，BitDefender 将采取具体的操作并通知您：

病毒警报

您可以看到病毒的名称，路径和受感染的文件，和 BitDefender 所采取的操作。

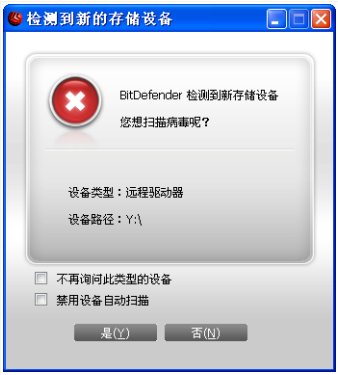
点击 确定 来关闭窗口。

重要

强烈建议您立即将受感染的文件通知网络安全管理员。

3.2.2. 设备检测警报

BitDefender Business Client 设置为自动检测存储设备（CD/DVD，USB 存储设备或映射网络驱动器），并提示您是否需要扫描。



设备检测警报

您可以查看被检测设备的信息。

要想扫描设备，请单击 是。 如果您确信设备为干净的，您可以选择不去扫描它。

在超级用户模式下，您可以选择以下选项:

- 不再询问此类型的设备. 当此类存储设备连接到计算机上时，BitDefender 将不再提供扫描。
- 禁用设备自动扫描. 当新的存储设备连接到计算机时，您将不会收到扫描新设备的提示。

3.2.3. 防火墙警报

防火墙 启用后，当需要连接到 Internet 时，BitDefender 将询问您是否许可：

防火墙警报

您能看到的信息如下：试图访问互联网的应用程序，应用程序文件路径，访问目标，访问协议和应用程序试图连接的端口。

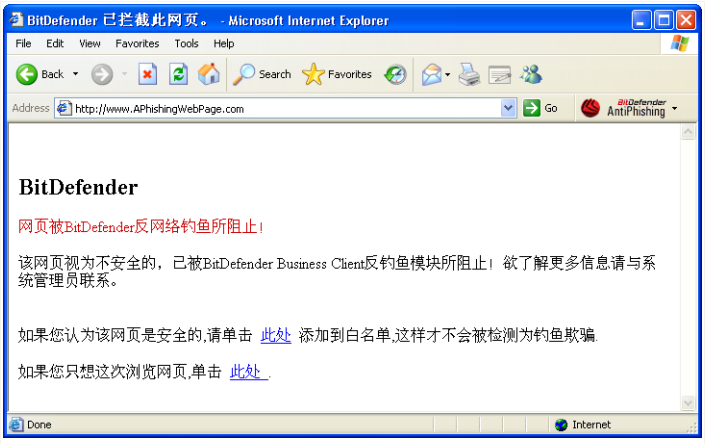
点击 允许，允许应用程序生成的通过各自的 IP 协议和端口从本地主机到任何目标位置所有通讯（入站和出站）。如果您点击 阻止，超出各自 IP 协议的应用程序将被拒绝访问互联网。

根据您的应答，一项规则将被创建，应用和列于表格中。下次应用程序试图连接，这条规则将被默认应用。

重要
允许传入的连接尝试，只有来自您明确地信任的 IP 或域名。

3.2.4. 反网络钓鱼警报

反网络钓鱼保护启用后，当您访问的网页试图窃取您的个人资料时，BitDefender 会用警报给您提示。 在您访问这样一个网页之前，BitDefender 将阻止该网页，并显示一个通用的警报网页：



反网络钓鱼警报

检查您的浏览器地址栏中的网页地址。 寻找表明该网页可能是用来网络钓鱼的线索。 如果网页地址是可疑的，建议您不要打开它。

这里有一些提示，可能对您有用：

- 如果您键入一个合法网站的地址，检查地址是否正确。 如果地址是正确的，重新键入并再次转到网页。
- 如果您已单击了一个电子邮件或即时消息上的链接，请检查是谁发送给您的。 如果发件人是未知的，这就可能是一个网络钓鱼的尝试。 如果您知道发件人，您应该检查这个人真的向您发送了链接。
- 如果您已经通过互联网访问了网页，检查您是在哪里发现的这个链接（在您的浏览器上单击返回按钮）。

如果您想要查看网页，单击相应的链接并采取这些操作之一：

- 只本次浏览网页。. 您不在网页上提交任何信息，就不会有风险。 如果网页是合法的，您可以添加它到白名单(单击 BitDefender 反网络钓鱼工具栏 ，然后选择添加到白名单)。
- 添加网页到白名单。. 网页将会立即显示，BitDefender 也不再发出警报。 该选项只在超级用户模式下可用。

重要

只有完全值得信赖的网页才可以添加到白名单（例如，银行网址，已知的在线商店等等）。 BitDefender 不会对白名单中的网页进行反网络钓鱼检查。

您可以使用 BitDefender 反网络钓鱼工具栏管理反网络钓鱼保护和白名单。 欲了解更多信息，请参阅 “反网络钓鱼工具栏”（第 50 页）。

3.2.5. 注册表警报

Windows 操作系统有个非常重要的组件叫 注册表，Windows 在此记录其设置选项、已安装的程序、用户信息及其他很多信息。

注册表 还被用作定义哪些程序在 Windows 启动时会自动启动，病毒经常利用这一点以便在用户重启电脑时自动加载。

注册表控制 保持关注 Windows 注册表–有效地检测特洛伊木马。 警报提醒有新的程序试图修改 Windows 注册表启动项。

注册表警报

您可以看到该程序试图设置它本身到 Windows 的启动项中. 如果您认为程序是安全的，建议允许这种设置。

注意

BitDefender 通常会在安装新的电脑软件时警觉您的电脑是否要以后电脑开机时后启动它。在许多情况下，这些软件是合法的，可以被信任。

如果您不清楚该程序，或者该程序看起来可疑，请点击 拦截 防止它修改 Windows 注册表。

如果您想 BitDefender 记住您的应答，检查 总是运用这一操作到这个程序。 通过这种方式，一个规则将创建，并且同样的操作将应用对于这个程序试图修改注册表的启动项，以便在 Windows 启动时程序自动运行。

3.2.6. 脚本警报

脚本 及 ActiveX 控件和Java applets 等代码被用于创建交互式网页，它们可被编写为具有危害行为。例如，ActiveX 控件可以获取对您计算机数据的完全控制，可以读取您的数据、删除信息、截获密码并截取您上网时的邮件。您应当只接受来自您信赖网站的脚本。

Bitdefender 可让您选择运行此类脚本或阻止其执行。

脚本控制 您将对该网站的信任和不信任进行管理。 BitDefender 将询问您是否同意网站激活脚本或其他活动内容:

脚本警报

您可看到脚本资源的名称。

选中 记住我的选择 选项并点击 是 或 否 会在规则表中创建一条规则并应用它。下次当同一个网站试图执行活动内容时将不会再提示您。

3.2.7. Cookie 警报

Cookie 在互联网中非常常见。它们是存储在您计算机上的小文件，您访问的网站在您的计算机上创建 Cookie 文件以记录您的特定信息。

Cookie 的主要目的是让您访问网站更方便，例如，网站可以借助 Cookie 记住您的姓名和偏好，这样您不必在每次访问该网站时都输入这些信息。

但是 Cookie 同样可以被用作跟踪您的上网习惯，从而触及您的隐私。 这是 Cookie 控制帮助。 当启用后，Cookie 控制 询问您是否许可新的网站尝试设置 Cookie：

Cookie 警报

您能看到试图设置或发送 Cookie 文件的程序名。

选中 记住我的选择 选项并点击是 或 否，就会在规则表中创建一条规则并应用它。下次您访问此网站时将不会被提示。

您可用这个功能选择信任和不信任的网站。

注意

由于互联网上巨量的 Cookie 被使用，Cookies 控制 开始使用时可能相当烦人，因为开始时它会询问很多有关某网站要在您的计算机上设置 Cookie 的问题。不过当您把您常用的网站都添加到规则表中后，上网就会变得和以前一样方便。

3.2.8. 用户控制警报

BitDefender 用户控制 可以由网络安全管理员配置阻止访问：

- 如游戏，聊天程序，文件共享程序及其他应用程序。
- 某些时段或全时段访问互联网。
- 不良网页。
- 网页和电子邮件，如果它们包含某些关键字。

BitDefender 将通过具体的警报通知您，您的行动不符合配置的用户访问规则。

重要

需要改变用户控制规则，请联系网络安全管理员。

4. 反垃圾邮件集成到邮件客户端

BitDefender Business Client 包括一个反垃圾邮件模块。 反垃圾邮件模块验证您收到的电子邮件并找出垃圾邮件。 BitDefender 检测出的垃圾邮件，会在主题行标记 [spam] 前缀。

注意
反垃圾邮件提供所有 POP3/SMTP 电子邮件客户端的保护。

BitDefender 通过一个直观易用的工具条直接集成到下列邮件客户端:

- Microsoft Outlook
- Outlook Express
- Windows Mail
- Mozilla Thunderbird

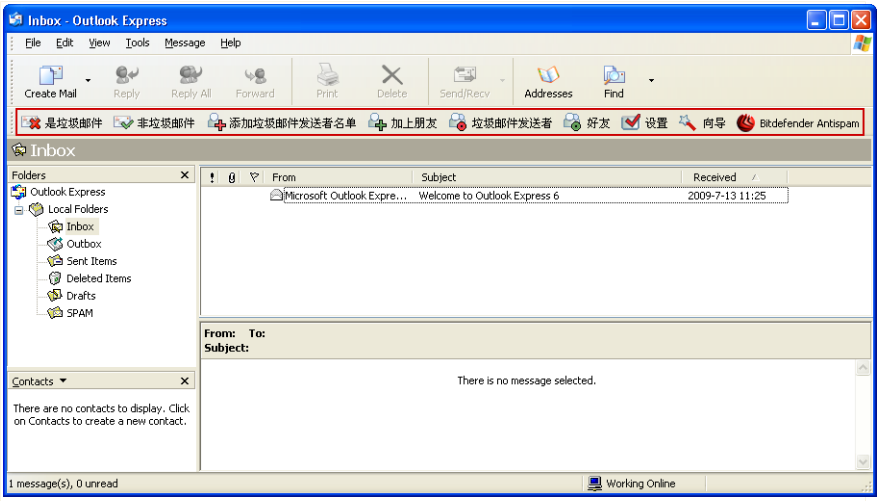
BitDefender 自动将垃圾邮件转移到一个特定文件夹，如下:

- 在 Microsoft Outlook 中，垃圾邮件被转移到一个 Spam 文件夹，位于 已删除邮件 文件夹。
- 在 Outlook Express 和 Windows Mail 中，垃圾邮件被直接移动到 已删除邮件 中。
- 在 Mozilla Thunderbird 中， 垃圾邮件被移动到 Spam 文件夹，位于 废件箱 文件夹中。

如果您使用其他邮件客户端，您必须创建一条规则，指定将由 BitDefender 标记为 [spam] 的邮件移动到一个您指定的垃圾邮件文件夹。

4.1. 反垃圾邮件工具栏

在您邮件客户端窗口的上部，您可以看到反垃圾邮件工具条。 反垃圾邮件工具条帮助您从邮件客户端直接管理反垃圾防护功能。 如果您发现 BitDefender 把正常邮件标记为垃圾邮件，您可以方便地进行纠正。



反垃圾邮件工具栏

BitDefender 工具栏中的每个按钮将被解释如下:

- 是垃圾邮件 – 发送一个邮件到贝叶斯模块表明所选的电子邮件是垃圾邮件。电子邮件将标记为[SPAM]并移至 Spam 文件夹。

  以后，适合相同方式的电子邮件将被标记为[SPAM] 。

  注意
  您可以选择一个或多个电子邮件。

- 非垃圾邮件 – 发送一个信息到贝叶斯模块说明所选的电子邮件不是垃圾邮件，BitDefender 不应该标记它。电子邮件将从Spam 文件夹移动到 收件箱 目录。

  以后，适合相同方式的电子邮件将不再被标记为 SPAM。

  注意
  您可以选择一个或多个电子邮件。

重要

The 非垃圾邮件 按钮便激活，当您选择一则消息由 BitDefender 被标记作为 SPAM 时(这些消息通常位于 Spam 文件夹)。

- 添加到垃圾邮件发送者列表 – 添加被选择的电子邮件的发件人 垃圾邮件发送者列表。

添加垃圾邮件发送者名单

选择 不要再次显示消息 如果您不想要被提示，当您添加垃圾邮件发送者地址到名单中时。

点击 确定 来关闭窗口。

以后，从那个地址发出的电子邮件将被标记作为 SPAM。

注意

您能选择一个或多个发件人。

- 添加好友 – 添加被选择的电子邮件的发件人到 好友列表。

加上朋友

选择 不要再次显示这条消息 如果您不想要被提示，当您添加好友的地址到名单中时。

点击 确定 来关闭窗口。

您将总是接收来自这个地址的电子邮件，而不管其包含什么内容。

注意

您能选择一个或多个发件人。

● 垃圾邮件发送者 – 打开 垃圾邮件发送者列表 包含所有不想接收其电子邮件的地址，而不管所包含的内容。

注意
任何来自包含在 垃圾邮件发送者清单 的电子邮件，将自动标记为 SPAM，而不做进一步处理。

垃圾邮件发送者清单

这里，您可以在 垃圾邮件发送者清单 中添加或删除项目。

如果您想要添加电子邮件，选中 电子邮件地址 选项，键入地址并点击按钮 。地址将出现在 垃圾邮件发送者列表。

重要
语法：name@domain.com.

如果您想要增加一个域，选中 域名 选项，键入域名并点击按钮 。域名将出现在垃圾邮件发送者列表。

重要
语法：

- @domain.com，*domain.com 和 domain.com – 所有从 domain.com 收到的电子邮件将被标记作为SPAM；
- *domain* – 所有从 域名（无论域名后缀）收到的电子邮件将被标记为 SPAM；

- *com – 所有收到域名以 com 为结尾的电子邮件将被标记作为 SPAM。

警告

请不要添加正常的网页邮箱服务域名（如 163 邮箱、Hotmail、新浪邮箱等）到垃圾邮件发送者列表。否则，使用这些邮箱的用户发给您的邮件都将会被当作垃圾邮件。 例如，您添加 163.com 到垃圾邮件发送者列表，则所有从 163.com 发出的邮件都会被标记为 [spam]。

要将电子邮件地址从 Windows 地址薄 / Outlook Express 文件夹导入到 Microsoft Outlook / Outlook Express / Windows Mail，请从从导入电子邮件地址从 下拉式菜单中选择合适的选项。

Microsoft Outlook Express / Windows Mail，将会出现一个新窗口，您从那里您可以选择包含需要添加到垃圾邮件发送者列表上的电子邮件地址。选择并单击 选择。

在这两个情况下电子邮件地址将出现在导入列表。选择其中一个并点击 添加他们到 垃圾邮件发送者列表。如果您点击 所有电子邮件将加到这个列表中。

要删除列表中的一个项目，选择它并点击 删除 按钮。如果您点击 清除列表 按钮您将会删除名单中的所有项目，但注意：这是不可恢复的。

使用 保存/ 载入 按钮保存/载入 垃圾邮件发送者列表 到一个期望的位置。文件将有 .bwl 扩展名.

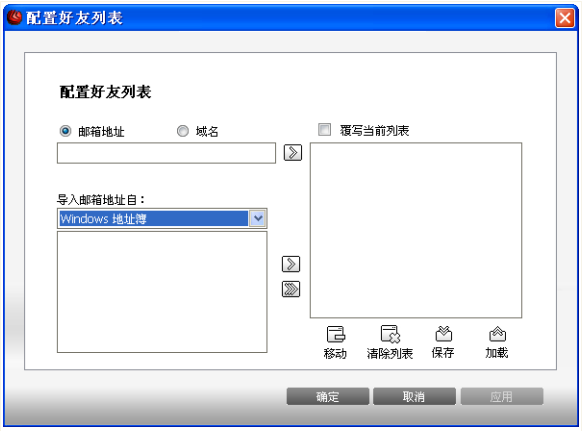
选择 加载时清空现有名单 能在加载以前保存的名单时,重设现有名单的内容。

点击 应用 和 确定 保存和关闭 垃圾邮件发送者清单。

- 好友 – 打开 好友清单 包含所有要接收其电子邮件的地址，而不管所包含的内容。

注意

任何来自包含在 好友清单 中的电子邮件，将自动传送到收件箱，而不做进一步处理。



好友清单

这里，您可以在 好友清单 中添加和删除项目。

如果您想要添加一个电子邮件地址，选中 Email 地址 选项，键入地址并单击 按钮。 该地址将出现在 好友清单。

重要
语法: name@domain.com.

如果您想要添加一个域名，选中 域名 选项，键入域名并单击 按钮。 域名将出现在 好友清单。

重要
语法:

- @domain.com, *domain.com 和domain.com – 不管他们的内容如何，所有从 domain.com 收到的电子邮件将到达您的 收件箱 ；
- *domain* – 不管内容，所有从 域名 收到的电子邮件(无论域名后缀)将到达您的 收件箱;
- *com – 不论内容，所有收到以 com 结尾的电子邮件将到达您的 收件箱 ；

要将电子邮件地址从 Windows 地址薄 / Outlook Express 文件夹导入到 Microsoft Outlook / Outlook Express / Windows Mail，请从从导入电子邮件地址从 下拉式菜单中选择合适的选项。

For Microsoft Outlook Express / Windows Mail 一个新窗口将出现，从那里您可以选择包含电子邮件地址的文件夹，您想要添加到 好友清单. 选择他们并单击选择。

在这两种情况下的电子邮件地址将出现在导入列表。选择其中一个并点击 添加 他们到 好友清单。 如果您单击 ，所有电子邮件地址将被添加到列表。

要删除列表中的一个项目，选择它并点击 删除 按钮。如果您点击 清除列表 按钮您将会删除名单中的所有项目，但注意：这是不可恢复的。

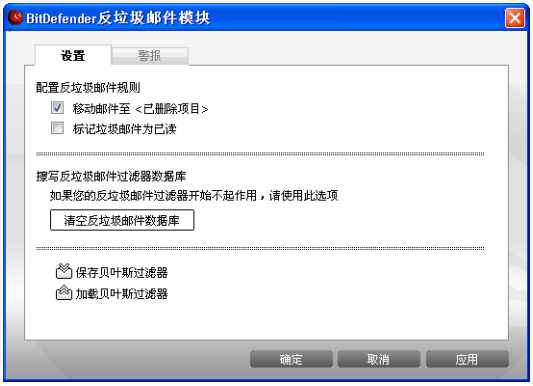
使用 保存/ 载入 按钮来保存/载入 好友清单到期望的位置。文件将有.bwl 扩展名。

选择 加载时清空现有名单 能在加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添加到 好友清单。BitDefender 不会阻止来自清单中的邮件。因此，把朋友加入好友清单能确保收到合法的邮件。

点击 应用 和 确定 保存和关闭 好友清单。

- 设置 – 打开 设置 窗口，您可以为 反垃圾邮件 模块指定一些选项。



设置

您可做以下选择：

- 移动邮件到已删除项目 – 移动垃圾邮件到 已删除项目 （只适用于微软Microsoft Outlook Express / Windows Mail）；

- 标记邮件为“已读” – 标记所有垃圾邮件消息为已读，以便不干扰到达的新垃圾邮件。

如果您的垃圾邮件过滤器是非常不精确的，您可能需要擦除过滤器数据库和再培训 贝叶斯过滤器。 点击 擦除反垃圾邮件数据库 重新设置 贝叶斯数据库。

使用 保存贝叶斯过滤器/ 载入贝叶斯过滤器 按钮以保存/加载 贝叶斯数据库 名单到期望的位置。该文件将有.dat 扩展名。

点击 警报 页签，如果您想要访问这个单元，禁用确认窗口 添加垃圾邮件发送者 和 添加好友 按钮。

注意

在 警报 窗口，您可以启用/禁用 请选择一个电子邮件信息 警报。 当您选择一个分组而不是一个电子邮件时，这个警报将出现。

- 向导 – 打开 向导 指引您逐步训练 贝叶斯过滤器， BitDefender 反垃圾邮件将逐步增加。 您也可以从 地址薄 添加地址到 好友清单 / 垃圾邮件发送者清单。
- BitDefender 反垃圾邮件 – 打开 BitDefender 用户界面。

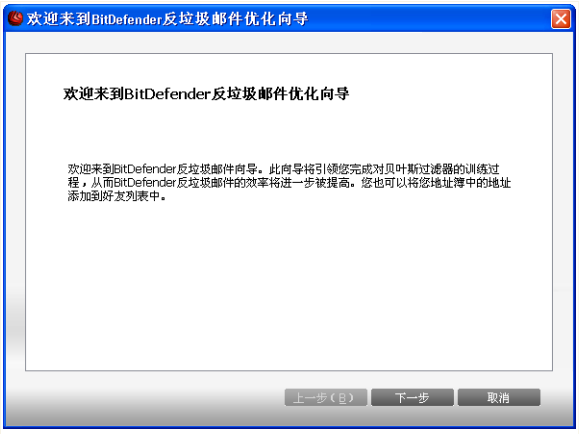
4.2. 反垃圾邮件配置向导

安装 BitDefender 后，第一次运行您的邮件客户端，将出现一个向导帮助您配置好友清单 和 垃圾邮件发送者清单 并培训 贝叶斯过滤器 ，以便提高反垃圾邮件过滤器的效率。

注意

这个向导也可以在任何时候通过单击 向导 按钮启动，在 反垃圾邮件工具条。

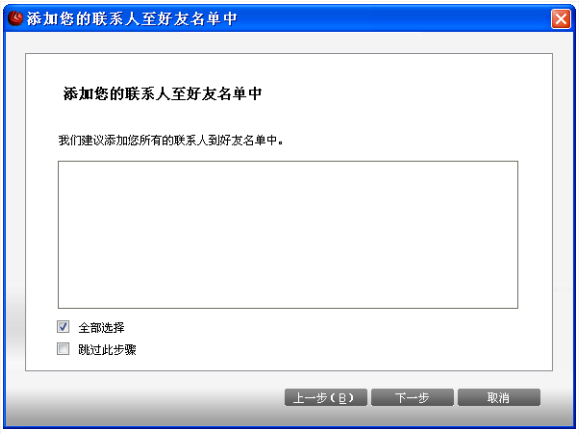
4.2.1. 步骤 1/6 - 欢迎窗口



欢迎窗口

点击 下一步。

4.2.2. 步骤 2/6 - 填充好友清单



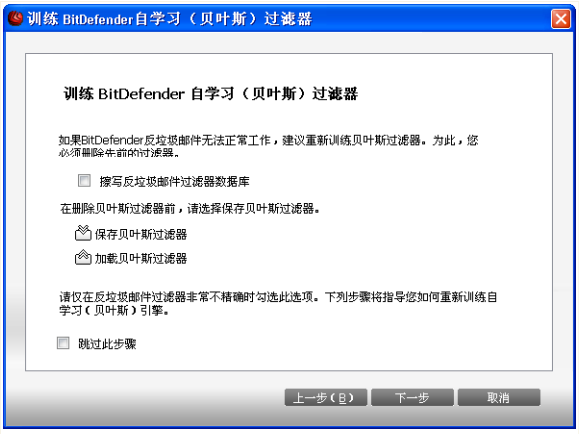
填充好友清单

这里，您能从您的 地址薄上看到所有的地址。请选择那些您想要增加到好友清单中的地址(我们推荐选择他们全部)。您将接收来自这些地址所有邮件，而不论内容。

要加入您所有的联系地址到好友清单，选中 选择全部。

如果您想要忽略这步，选择 跳过这一步。点击 后退 回到前一步或点击 下一步 继续向导。

4.2.3. 步骤 3/6 - 删除贝叶斯数据库



删除贝叶斯数据库

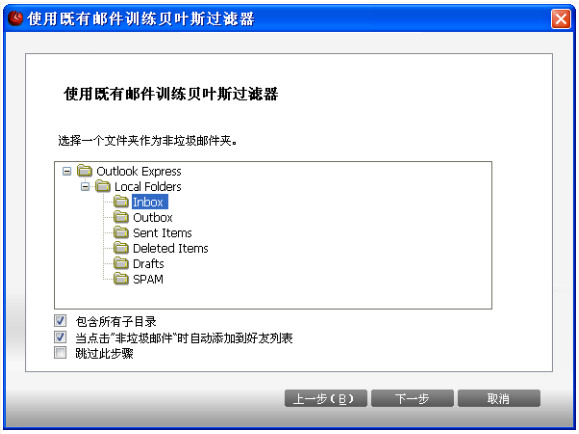
您可以发现您的反垃圾邮件过滤器开始没有效率。这也许是因为不正当的训练(例如，即您错误地标记了一定数量合法的消息作为垃圾，或反之亦然)。如果您的过滤器是非常不精确的，您可能需要擦除过滤器数据库并通过后续的向导再次培训。

选择 擦除反垃圾邮件过滤器数据库，如果您想要重新设置贝叶斯数据库。

使用 保存贝叶斯 或 加载贝叶斯 按钮来保存/加载 贝叶斯数据库 列表到一个指定的地点。文件将有 .dat 扩展名。

如果您想要忽略这步，选择 跳过这一步。点击 后退 回到前一步或点击 下一步 继续向导。

4.2.4. 步骤 4/6 - 使用合法的电子邮件训练贝叶斯过滤



使用合法的电子邮件训练贝叶斯过滤器

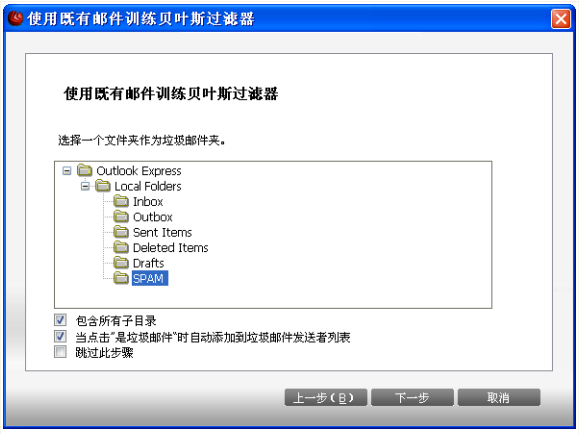
请选择一个包含合法电子邮件的文件夹。这些邮件将用来训练反垃圾邮件过滤器。

在目录列表下有两个高级选项:

- 包括子文件夹 - 包括您选择文件夹的子文件夹。
- 自动添加到好友清单 - 添加发件人到 好友清单。

如果您想要忽略这步，选择 跳过这一步。点击 后退 回到前一步或点击 下一步 继续向导。

4.2.5. 步骤 5/6 – 用垃圾邮件训练贝叶斯过滤器



训练 Bayesian 过滤反垃圾邮件

请选择一个包含垃圾电子邮件的文件夹。这些邮件将用来训练垃圾邮件过滤器。

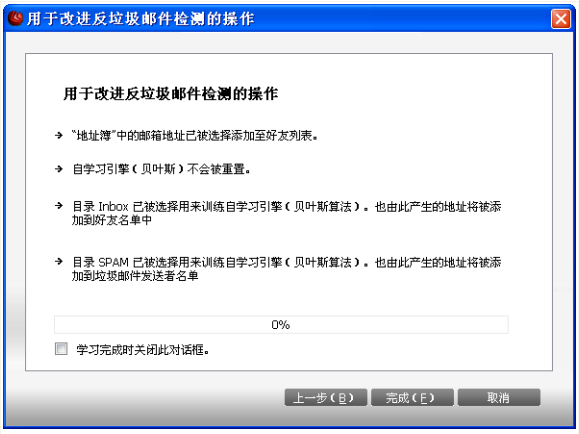
重要
请确定您选择的文件夹不包含合法的电子邮件，否则，识别垃圾邮件的能力将会大大下降。

在目录列表下有两个高级选项:

- 包括子文件夹 – 包括您选择文件夹的子文件夹。
- 自动添加到垃圾邮件发送者清单 – 添加发件人到 垃圾邮件发送者清单。

如果您想要忽略这步，选择 跳过这一步。点击 后退 回到前一步或点击 下一步 继续向导。

4.2.6. 步骤 6/6 - 总结



总结

这里，您能看到该向导的所有的设置。可以返回上一步做任何修改(点击 后退)。如果您不想要做任何改动，点击 完成 结束向导。

5. 反网络钓鱼工具栏

您在 Internet 上浏览时，BitDefender 将会保护您免受网络钓鱼软件的攻击。 它扫描您浏览的网页，并在发现网络钓鱼网站时提醒您。 您可以配置一个网站白名单，BitDefender 将不会扫描白名单中的网站。

您可以使用集成到 Internet ExplorerBitDefender 反网络钓鱼工具栏，很容易和有效地管理反网络钓鱼保护和使用白名单。 反网络钓鱼工具栏，所代表的 BitDefender 图标，是在 Internet Explorer 的顶部。 点击打开工具条菜单。

注意
如果您没有看到工具条，打开 视图 菜单，指向 工具栏 并选中 BitDefender 工具栏。

反网络钓鱼工具栏

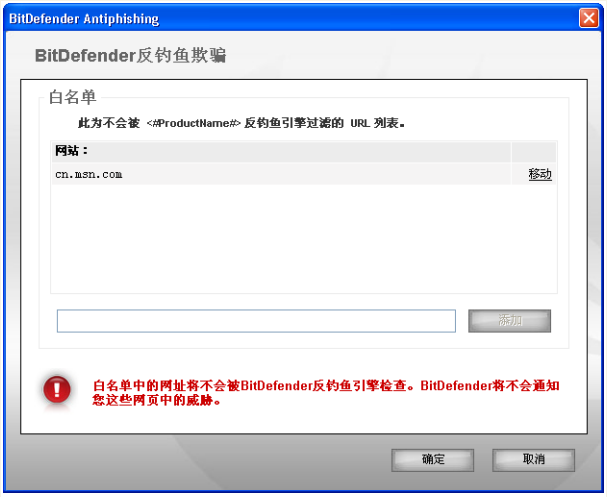
工具栏包含下面的命令菜单:

- 启用/禁用 Bitdefender 反网络钓鱼工具栏。 如果您选择禁用反网络钓鱼工具栏，您将不再受到反网络钓鱼攻击的保护。
- 设置 – 打开一个窗口，您可以指定反网络钓鱼工具栏的设置。 您可做以下选择:
  - 启用扫描 – 启用反网络钓鱼扫描。
  - 添加白名单之前询问 – 当您添加网站到白名单时询问您。

●添加至白名单 – 添加当前网站到白名单。

注意
添加网站到白名单中后，Bitdefender 将不会扫描该网站是否有网络钓鱼企图。我们建议您只添加您完全信任的网站到白名单中。

●查看白名单 – 打开白名单查看。



反网络钓鱼白名单

您可以看到名单上不被 BitDefender 反网络钓鱼引擎检查的所有网站列表。

如果您要从白名单中删除某地址，以便通知您任何该网页上的网络钓鱼威胁，点击旁边的 移除 按钮。

您可以将您完全信任的网站添加到白名单中，从而让 Bitdefender 反网络钓鱼引擎跳过扫描这些网站。 要向白名单中添加网站，请在对应的编辑框中输入网址，然后点击 添加。

●帮助 – 打开帮助文件。
●关于 – 打开一个包含 Bitdefender 及支持信息的窗口。

高级管理

6. 概览

BitDefender Business Client 可以在受限模式，也可以在超级用户模式下进行操作，开始 章节已经提到这一点。 您的网络安全管理员可以设置 BitDefender 操作超级用户模式。 在这种情况下，您可以详细配置 BitDefender，更重要的是，您还可以使用整套备份选项。

要检查或配置 BitDefender 的设置，您必须将界面可视化模式改为高级视图模式。要做到这一点，点击位于基本视图顶部的 切换到高级视图 按钮。

重要

在受限用户模式下，BitDefender Business Client 的配置和管理都完全取决于网络安全管理员。 您将无法配置任何设置，但只能看到 BitDefender Business Client 组件配置和各种操作方面的统计。 如果您对 BitDefender 配置有任何异议，请直接联系网络安全管理员。

高级视图模式下的主界面

高级视图是由 BitDefender 组件所组成。 这样，您就可以轻松地管理 BitDefender，基于各种类型安全性问题的处理。

要配置或检查设置和特定 BitDefender 组件的统计，使用左边的菜单：

- 快速任务 – 在本节您可以运行手动任务。
- 反病毒 – 在本节您可以设置 反病毒 模块。
- 防火墙 – 在本节您可以设置 防火墙 模块。
- 反垃圾邮件 – 在本节您可以设置 反垃圾邮件 模块。
- 隐私控制 – 在本节您可以配置 隐私控制 模块。
- 用户控制 – 在本节您可以配置 用户控制 模块。
- 更新 – 在本节您可以设置 更新 模块。

重要
如果网络安全管理员选择从项目中移除一些组件，这些组件可能会丢失。

您可以返回到基本视图，通过点击相应的 切换到基本视图 按钮。

如果你需要更多的帮助，请点击窗口底部的 帮助 链接。 上下文帮助页面会显示您提供详细资料。

6.1. 快速任务

如果您只想执行基本操作，请转入左边的菜单上的快速任务。 快速任务同基本视图的手动任务是一样的。

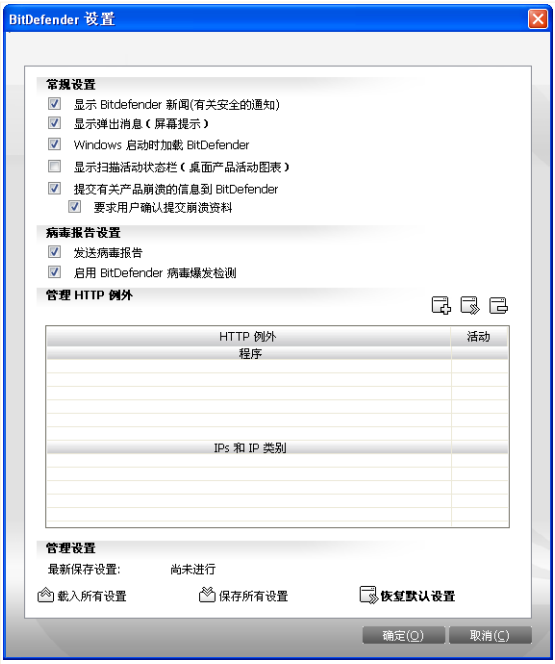
- 立即升级 – 立即开始升级产品。
- 扫描“我的文档” – 扫描“我的文档”目录。
- 深度系统扫描 – 开始对您的电脑进行一次全面扫描(包括存档)。
- 全面系统扫描 – 开始对您的电脑进行一次全面的扫描(不包括存档)。
- 启动备份向导 – 启动一个简易的 5 步向导程序备份你的数据。
- 备份设置 – 打开 BitDefender 备份，您可以 建立和执行备份详细操作。 仅适用于超级用户模式！
- 启动恢复向导 – 启动一个简易的4步向导程序恢复你的数据。

重要
如果网络安全管理员选择从项目中移除备份和恢复选项，这些选项可能会丢失。

要执行这些任务，请点击 立即运行 按钮，立即运行相应的任务。 欲了解更多信息，请参阅 “手动任务”（第 9 页）.

6.2. 配置常规设置

要配置 BitDefender Business Client 的常规设置和管理其设置，请点击 高级设置。 显示一个新窗口。



常规设置

这里，您可以设定 BitDefender 的所有行为。 默认情况下，BitDefender 在 Windows 启动时自动加载并且最小化运行于任务栏中。

6.2.1. 常规设置

- 显示 BitDefender 资讯（安全相关的通知） – 不定期显示由 BitDefender 服务器发送的病毒爆发通知。
- 显示弹出消息（屏幕便笺） – 显示产品状态相关的弹出式窗口。
- 系统启动时加载 BitDefender – 在系统启动时自动运行 BitDefender。 我们建议您选中这个选项。
- 显示扫描活动工具条(屏幕产品活动图) – 无论您何时登陆 Windows，都将显示 扫描活动工具条。 如果您不想显示扫描活动工具条，取消选择该复选框。
- 将产品受损信息提交给 BitDefender – 如果产品无法工作，错误日志将被发送到 BitDefender 实验室，同时 BitDefender 服务将被再次初始化。

  如果还选择了要求用户确认提交受损信息，那么登陆到工作站的用户将被通知产品已受损。这样，用户必须确认发送错误日志，并重启 BitDefender 服务。

6.2.2. 病毒报告设置

- 发送病毒报告 – 把在您的计算机发现的病毒报告递交给 BitDefender 实验室，这有助于我们掌握和追踪病毒的爆发。

  该报告将不包含机密数据，例如您的名字，IP 地址或其它资料。也不会用于商业目的。提供的信息只包含病毒名称，将完全用于建立统计报告。
- 启用病毒爆发报告 – 将潜在的病毒爆发报告发送给 BitDefender 实验室。

  该报告将不含有机密数据，例如您的名字，IP 地址或其它资料。也不会用于商业目的。提供的信息只包括病毒名称，将完全用于侦测新的病毒。

6.2.3. 管理 HTTP 例外

BitDefender Business Client 阻止 HTTP 通讯，以便进行恶意软件扫描，并应用相关的身份控制和用户控制策略。 不遵循 HTTP 标准的 HTTP 通讯会被自动拦截，而不进行任何提示。

HTTP 例外自动允许包含特定应用程序或 IP 地址的 HTTP 通讯。

HTTP 例外只由 IT 管理员使用或完全理解例外目的的专家用户使用。 普通用户不应该使用这些设置。

警告
定义 HTTP 例外时，需要小心。HTTP 例外可能会让工作站对病毒和其他恶意软件，变得脆弱。
只能添加您信任的应用程序和 IP 地址到 HTTP 例外。在添加 HTTP 例外之前，最好先请教您的网络安全管理员。

应用程序

当一个应用程序添加到了 HTTP 例外，该应用程序的 HTTP 通讯不再被 BitDefender 拦截。这意味着：

- 各自的通讯不会进行病毒扫描。
- 相关的身份控制和用户控制策略不会被应用到各自的通讯上。

这是一个可能添加为 HTTP 例外的应用程序实例：一个专有的应用程序，生成的 HTTP 通讯不符合 HTTP 标准，部署 BitDefender Business Client 之后无法工作。

警告
不要添加网页浏览其为 HTTP 例外，除非由 BitDefender 技术支持劝告的！HTTP 扫描排除一个网页浏览器，将使病毒扫描失效，身份控制和用户控制策略会对通过该浏览器发送和接收的内容失去其应有的能力。

添加例外

要添加一个例外，单击 添加 按钮并按照向导步骤进行。 右键单击应用程序栏上的一个空白项，选择 编辑 并完成向导的最后一步，这样更快捷。

步骤 1/2 – 选择例外类型

例外类型

选择“不扫描文件或路径”。

点击 下一步。

步骤 2/2 – 指定排除的路径

排除的路径

单击 浏览，选择被排除的应用程序，然后单击 添加。

路径将出现在列表中，您可添加任意多的路径。 要从列表中删除一个对象，请选择它然后点击 删除 按钮。

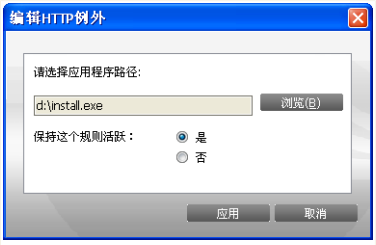
单击 完成 添加例外。

编辑例外

要编辑例外，做下列任何操作之一：

- 右键单击例外并从菜单中选择 编辑。
- 选择例外并单击 编辑 按钮。

显示一个新窗口。



编辑应用程序例外

按需要更改应用程序路径。 如果您想要暂时禁用例外，选择 否。

点击 应用 保存修改。

例外失效

要暂时使例外失效，右键单击活动栏上的相关区域，并在菜单上选择 否。要重新激活例外，按照相同的步骤并在菜单上选择 是。

您也能通过编辑规则进行这些变动。

删除例外

要删除例外，做下列任何操作之一：

- 右键单击例外并从菜单中选择 删除。
- 选择例外并单击 删除 按钮。

IP 地址和 IP 子网

当一个 IP 地址添加到 HTTP 例外时，该 IP 地址的 HTTP 通讯不再被 BitDefender 拦截。同理，当整个 IP 子网增加作为 HTTP 例外时，属于子网的 IP 地址的 HTTP 通讯不再被 BitDefender 拦截。这意味着：

- 各自的通讯不会进行病毒扫描。
- 相关的身份控制和用户控制策略不会被应用到各自的通讯上。

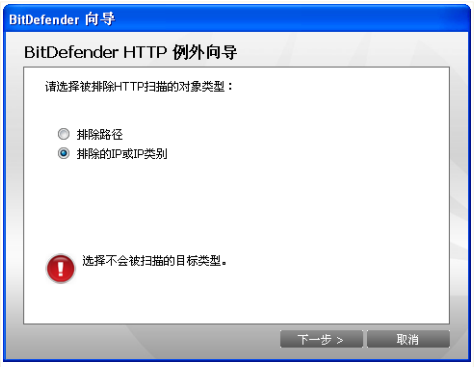
这里是一些添加 IP 地址或子网作为 HTTP 例外的案例：

- 身份控制规则已被配置，以防止个人或机密信息从工作站通过 HTTP 发送。要允许这样的信息通过 HTTP 在内部交换，您可以添加内部网页服务器的 IP 地址作为 HTTP 例外。
- 要禁用已知安全的特定 IP 地址的 HTTP 病毒扫描（例如，企业内部网 HTTP 服务器的 IP 地址）。

添加例外

要添加一个例外，单击 添加 按钮并按照向导步骤进行。 右键单击 IP 地址和 IP 类别列上的空白项，选择 编辑 并完成向导的最后一步，这样更快捷。

步骤 1/2 – 选择例外类型

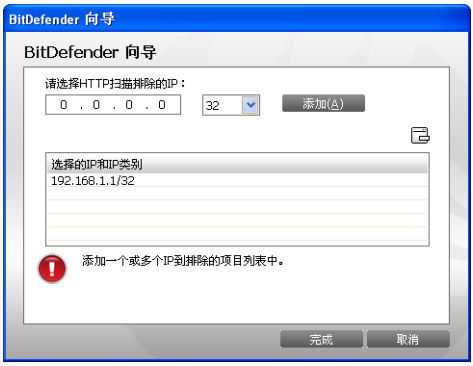


例外类型

选择排除一个 IP 或一个 IP 子网扫描的选项。

点击 下一步。

步骤 2/2 – 指定要排除的 IP



排除的 IP

要排除单一 IP 地址，在编辑框中键入，从菜单中选择一个32位子网掩码，然后单击 添加。

要排除整个子网，在编辑栏键入子网地址，从菜单中选择子网掩码，然后单击 添加。

您添加的那些 IP 地址或子网将会出现在列表中。如果您需要，您可以添加更多的例外。 要从列表中删除一个对象，请选择它然后点击 删除 按钮。

单击 完成 添加例外。

编辑例外

要编辑例外，做下列任何操作之一：

- 右键单击例外并从菜单中选择 编辑。
- 选择例外并单击 编辑 按钮。

显示一个新窗口。

编辑 IP 例外

如果有需要，更改 IP 地址或 IP 子网。 如果您想要暂时禁用例外，选择 否。

点击 应用 保存修改。

例外失效

要暂时使例外失效，右键单击活动栏上的相关区域，并在菜单上选择 否。要重新激活例外，按照相同的步骤并在菜单上选择 是。

您也能通过编辑规则进行这些变动。

删除例外

要删除例外，做下列任何操作之一：

- 右键单击例外并从菜单中选择 删除。
- 选择例外并单击 删除 按钮。

6.2.4. 管理设置

使用 保存所有设置 / 加载所有设置 按钮保存/加载您已保存到期望位置的设置。 这样您可以在重新安装或修复 BitDefender 后使用相同的设置。

要加载默认设置，请点击 恢复默认设置。

7. 反病毒

Bitdefender 保护您的电脑免受各类的恶意软件侵害（如病毒、木马、间谍软件、rootkit 等）。

除了典型的基于病毒库的扫描，BitDefender 还对扫描文件执行启发式分析。启发式分析的目的是在找到病毒特征码之前，根据特定的算法和模式识别新的病毒。有时会出现错误警报。此文件将被归为可疑文件。在这种情况下，我们建议您将文件发送到给 BitDefender 实验室进行进一步的分析。

BitDefender 病毒保护分为两类:

- 实时扫描 – 防止新的恶意威胁进入您的系统。这也是所谓的实时保护，文件在使用时被实时扫描。 举例来说，Bitdefender 会在您打开一个 Word 文档时扫描其中是否存在病毒，或者在您接受电子邮件时对其进行扫描。
- 请求式扫描 – 允许检测和删除已经存在于您系统内的恶意威胁。 这是由用户启动的传统扫描方式 – 用户手动选择BitDefender 应该要扫描的磁盘、文件夹或文件，然后由 BitDefender 执行请求式扫描。 扫描任务允许您创建自定义的扫描例程，并按时间表定期执行。

反病毒 模块的用户指南中包括下列内容:

7.1. 实时扫描

实时扫描，也称为实时防护，通过扫描所有访问文件，电子邮件和即时通讯应用程序（ICQ，NetMeeting，雅虎通，MSN）的通信，让您的计算机免除各种恶意软件威胁。

要配置和监控实时防护，请转入高级视图反病毒>防护。

实时防护

重要

为防止病毒感染您的计算机，请保持启用 实时防护。

在这个单元的底部，您可以看到关于文件和电子邮件的实时防护统计信息。如果您想要看到更多有关统计数据的解释， 请点击 更多统计资料。

要启动快速系统扫描，请点击 立即扫描。

7.1.1. 设置防护级别

您可以选择最符合您的防护需求的安全级别，上下拖动滚动条设置合适的防护级别。

共有 3 个防护级别:

防护级别	描述
宽松	覆盖基本安全需求，系统资源占用很低。

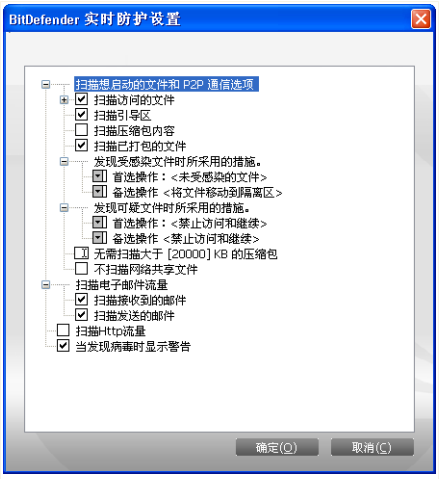
防护级别	描述
	只扫描程序和邮件信息中的病毒。除了传统的基于特征码的扫描，还使用了启发式分析。对感染文件采取的措施为：清除文件/禁止访问。
默认	提供标准安全级别，资源消耗级别较低。 扫描所有文件和邮件信息中的病毒和间谍软件。除了传统的基于特征码的扫描，还使用了启发式分析。对感染文件采取的措施为：清除文件/禁止访问。
严格	提供高级安全级别，资源消耗级别中等。 扫描所有文件、邮件信息和网页通信中的病毒和间谍软件。除了传统的基于特征码扫描之外，还使用了启发式分析。对感染文件采取的措施为：清除文件/禁止访问。

要启用默认的实时防护设置，请点击 默认级别。

7.1.2. 自定义级别

高级用户可以利用 BitDefender 提供扫描设置。该扫描程序可设置为只扫描特定文件扩展名，搜索特定的恶意软件威胁或跳过存档。这可能会大大减少扫描时间，提高您的电脑在扫描时的反应。

您可以通过点击 自定义级别，自定义 实时保护。下列窗口将显示：



实时防护设置

扫描选项以可扩展菜单的形式展现，和 Windows 中的类似。 按"+"的可以展开选项，按 “–” 收起选项。

注意
您会看到有些扫描选项虽然有"+"格子但却无法展开，因为这些格子尚未选定。 当您选择它们后就可以展开了。

●扫描访问文件和P2P传输选项 – 扫描访问文件和即时通信软件程序（ICQ、NetMeeting、雅虎通、MSN）的通讯。下一步，选择您想要扫描的文件类型。

选项		描述
扫描访问的文件	扫描所有文件	扫描所有被访问的文件，无论是何种类型。
	只扫描应用程序	只扫描带有下列扩展名的程序文件: .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;

选项		描述
		.lnk; .pif; .prc; .url; .smm; .pdf; .msi; .ini; .csc; .cmd; .bas; .eml and .nws。
	只扫描用户指定的文件扩展名	只扫描带有用户指定的文件扩展名的文件，请用“; ”分隔各个文件扩展名。
	扫描风险软件	扫描风险软件。 检测到的文件将被作为感染文件处理，启用此选项后，包含广告软件组件的软件可能会停止运行。 选择 跳过拨号软件和应用软件扫描 ，如果您想排除这些类型的文件扫描。
扫描引导扇区		扫描系统的引导扇区。
扫描压缩包内容		扫描被访问的压缩文档，启用此选项后，计算机速度会变慢。
扫描加壳文件		所有的加壳文件将会被扫描。
首选操作		从下拉菜单中选择对受感染文件及可疑文件所采取的首选操作。
	拒绝访问并继续	如果发现感染的文件，会阻止对该文件的访问。
	清理文件	从感染文件中移除恶意代码。
	删除文件	没有任何警告下立即删除受感染的文件。
	移动文件至隔离区	受感染的文件移到隔离区。
备选操作		从下拉菜单中选择备选操作，在首选操作失败后，会对受感染文件采取第二次操作。
	拒绝访问并继续	如果发现感染的文件，会阻止对该文件的访问。
	删除文件	没有任何警告下立即删除受感染的文件。
	移动文件至隔离区	受感染的文件移到隔离区。
不扫描大于[x]Kb 的文件。		输入要扫描的文件的最大尺寸，如果设置为 0Kb，则所有文件都会被扫描。
不扫描共享文件夹		如果您选择了这个选项， BitDefender 不会扫描网络共享文件夹，使网络访问速度更快。

选项	描述
	如果您所在的网络已经有反病毒解决方案，建议您启用此选项。

●扫描电子邮件通信 – 扫描电子邮件通信。

您可做以下选择：

选项	描述
扫描接收的邮件	扫描所有接收到的电子邮件信息。
扫描发送的邮件	扫描所有发送的电子邮件信息。

●扫描 HTTP 通信

●发现病毒时显示警告 – 当在文件或电子邮件中发现病毒是显示警告窗口。

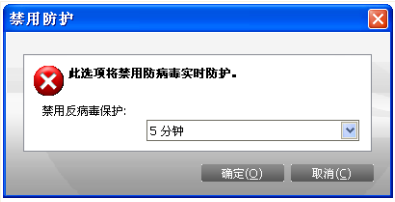
如果是被感染文件，警告窗口会包含病毒名称、文件路径、BitDefender 所采取的操作，以及一个指向 BitDefender 网站更多信息的链接。如果是被感染的电子邮件，警告窗口还会包含发件人和收件人信息。

如果您发现有可疑文件，您可以从警报视窗启动向导，帮助您把该文件传给 BitDefender 实验室作进一步分析。您可以输入电子邮件地址来接收该文件有关的信息。

点击 确定 保存修改并关闭窗口。

7.1.3. 禁用实时防护

如果您要禁用实时防护， 会出现一个警告窗口。



禁用实时防护

您必须从菜单上选择您想实时保护的禁用时间，来确认您的选择。您可以禁用实时保护 5，15或30分钟，一小时，永久或直到系统重新启动。

警告
这是一个重要的安全问题。我们建议您尽可能不要禁用实时保护。如果禁用实时保护，您将不会受到保护，免遭恶意威胁。

7.2. 请求式扫描

BitDefender 的主要目标是使您的计算机不受病毒的侵害。这首先是通过阻止新病毒入侵您的计算机，并扫描您的电子邮件信息和任何新下载或复制到系统的文件来实现的。

在您安装 BitDefender 之前，有可能病毒已经存在于您的系统。因此最好在您安装 BitDefender 后，立即扫描您的计算机。经常扫描计算机检查病毒是一个良好的习惯。

要配置并启动手动扫描，请到高级视图中的 反病毒>病毒扫描。

扫描任务

请求式扫描是基于任务的扫描，扫描任务应指定扫描选项以及扫描对象。 您可以在任何时候扫描计算机，使用默认的任务或者自己定义的扫描任务（用户自定义任务）。您也可以定期或当系统处于闲置状态时扫描您的系统，以便不干扰您的工作。

7.2.1. 扫描任务

BitDefender 自带几个默认的任务，涵盖了常见的安全问题。您也可以创建自定义的扫描任务。

每个任务有属性窗口，您可以配置任务并查看扫描结果。了解更多信息，请参见“配置扫描任务”（第 73 页）。

扫描任务可分三类：

- 系统扫描任务 – 包含以下默认的系统扫描任务：

系统扫描任务	描述
深度系统扫描	扫描整个系统，包括压缩文档。 在默认配置下，它扫描威胁到您系统安全的所有类型的恶意软件，如病毒，间谍软件，广告软件， rootkit 和其他。
全面系统扫描	扫描整个计算机，不扫描压缩文档。 在默认配置下，它扫描威胁到您系统安全的所有类型的恶意软件，如病毒，间谍软件，广告软件， rootkit 和其他。
快速扫描	扫描 Windows ， Program Files 和 All Users 文件夹。 在默认配置下，扫描除 rootkit 之外的所有类型恶意软件，但不扫描内存、注册表和 Cookie。

注意

因为 深度系统扫描和全面系统扫描 任务将分析整个系统，扫描可能需要持续一段时间。因此，我们建议您以低优先级方式，最好是在系统空闲的时候运行这些任务。

- 用户扫描任务 包含用户自定义的扫描任务。

  提供的任务名称为我的文档。 使用这项任务，扫描当前用户的重要文件夹，包括：我的文档，桌面 和 启动项 。它能确保您的文档、工作空间，以及系统启动时运行的应用程序的安全。

- 其他扫描任务－包含其他扫描任务列表。这些任务指的是无法在此窗口运行的其它扫描类型。您只能修改它们的设置，或查看扫描报告。 以下任务可用：

系统扫描任务	描述
上下文扫描	当通过 Windows 上下文目录扫描或使用扫描活动栏时使用此任务。 您可以更改扫描选项，使其更好地满足您的需要。
设备扫描	当有新的存储设备连接到计算机时，BitDefender Business Client 将自动检测并扫描它。 使用该操作配置存储设备（CD/DVD，USB 存储设备或映射网络驱动器）的自动检测和扫描选项。 了解更多关于此操作的信息，请参见 “设备扫描中” （第 91 页）。

在每个任务的右边有 3 个按钮：

- 计划表– 表明选中的任务随后将按计划执行。点击此按钮打开属性窗口， 计划制定页签，在那里您可以看到任务计划并进行修改。
- 删除 – 删除所选任务。

注意
仅对用户创建的任务可用，您无法移除默认的任务。

- 立即扫描 – 运行扫描任务，启动 实时扫描。

在每一个任务的左边，您可以看到 属性 按钮，可让您设定任务，并查看扫描日志。

7.2.2. 快捷菜单

每个扫描任务都有快捷菜单，在任务上单击鼠标右键就可打开快捷菜单。

快捷菜单

对于系统及用户定义扫描任务，在快捷菜单上会显示如下的命令:

- 立即扫描 – 运行选定的扫描任务，启用实时扫描。
- 改变扫描对象 – 打开 属性 窗口， 扫描路径 页签，在那里您可以改变选择任务的扫描目标。

注意
如果是系统任务，这个选项被 显示任务路径替换，您只能看到他们的扫描目标。

- 计划任务 – 打开 属性 窗口， 计划制定 页签，在那里您可以计划选择的任务。
- 查看扫描日志 – 打开 属性 窗口， 扫描日志 页签，在那里您可以看到选择任务被运行后生成的报告。
- 复制 – 复制选择的扫描任务。 这在建立新任务时非常有用，因为您可通过复制并修改已有的扫描任务快速创建一个新任务。
- 删除 – 删除指定的扫描任务。

注意
仅对用户创建的任务可用，您无法移除默认的任务。

- 属性 – 打开 属性 窗口， 浏览 页签，在那里您可以改变选定任务的配置。

关于上下文扫描任务，仅 属性 和 查看扫描日志 选项可用。

关于设备扫描任务，仅 属性 和 设备扫描选项可用。 第二个选项允许您为此操作配置特定的设置。 了解更多关于此操作的信息，请参见 “设备扫描中” （第 91 页）。

7.2.3. 创建扫描任务

您可以使用下列方法之一来创建扫描任务：

- 复制 一个现有任务并重新命名，然后在 属性 窗口进行必要的修改。
- 点击 新建任务 创建一个新任务并进行配置。

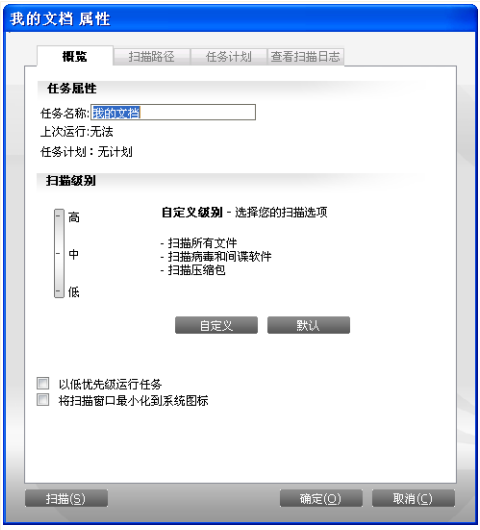
7.2.4. 配置扫描任务

每个扫描任务都有 属性 窗口，用户可以设置扫描选项、扫描对象、计划任务或查看扫描日志。 要打开属性窗口，请点击任务右侧的 打开 按钮，或者右键点击任务并点击快捷菜单中的 打开。

注意
欲了解更多有关在 日志 标签页中查看扫描日志的信息，请参阅 “查看扫描日志” （第 89 页）。

设置扫描选项

要为某个扫描任务设置扫描选项，请右键点击该任务，并选择 属性。 就会出现下面的窗口：



概览

您可在此查看该任务的信息（名称、上次运行时间及任务计划状态），并设置扫描选项。

扫描级别

您可通过选择一个扫描级别轻松配置扫描选项，请拖动滚动条选择合适的扫描级别。

共有三个扫描级别:

防护级别	描述
低	提供合理的检测效率，资源消耗水平低。 只扫描程序中的病毒。除了经典的特征码病毒扫描外，还使用了启发式分析。
中	提供良好的检测效率，中等资源消耗水平。 扫描所有文件中的病毒和间谍软件。除了经典的特征码病毒扫描外，还使用了启发式分析。
高	提供极高的检测效率，资源消耗水平很高。

防护级别	描述
	扫描所有文件和压缩文档中的病毒和间谍软件。除了经典的特征码病毒扫描外，还使用了启发式分析。

还有下列适用于扫描进程的常规选项：

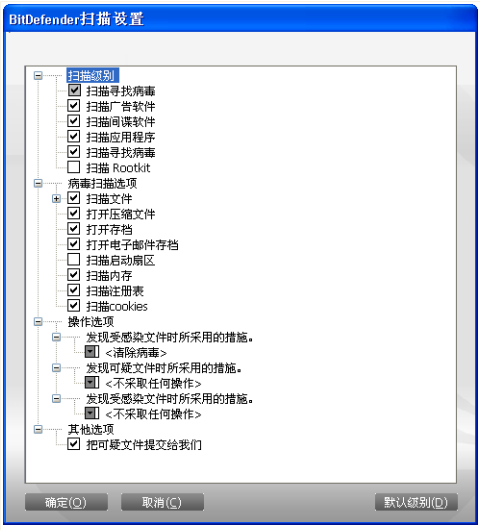
选项	描述
以低优先级运行任务	调低扫描过程的优先级，这将让其他程序运行速度更快，并增加扫描进程完成的时间。
最小化扫描窗口到系统托盘	将扫描窗口最小化到 系统托盘，双击 BitDefender 系统托盘图标可以打开窗口。

点击 确定 保存更改并关闭窗口。要运行任务，请点击 扫描。

自定义扫描级别

高级用户可以利用 BitDefender 提供扫描设置。该扫描程序可设置为只扫描特定文件扩展名，搜索特定的恶意软件威胁或跳过存档。这可能会大大减少扫描时间，提高您的电脑在扫描时的反应。

单击 自定义 设置您自己的扫描选项。 将会出现一个新的窗口。



扫描级别设置

扫描选项以可扩展菜单的形式展现，和 Windows 中的类似。 按"+"的可以展开选项，按 “–” 收起选项。

扫描分为四类选择:

- 扫描级别
- 病毒扫描选项
- 操作选项
- 其他选项

- 指定您希望 BitDefender 扫描的恶意软件类型，可通过从 扫描级别 分类中选择合适的选项完成。

  您可做以下选择:

选项	描述
扫描病毒	扫描已知的病毒。 BitDefender 可以检测不完整的病毒体，因此可以清除任何威胁您的系统安全的恶意软件。

选项	描述
扫描广告软件	扫描广告软件，检测到的文件将被作为感染文件处理。如果启用此选项，包含广告组件的软件可能会停止工作。
扫描间谍软件	扫描已知间谍软件的威胁。检测出的文件将会被作为感染文件处理。
扫描非法程序	扫描应用程序(.exe and .dll 文件)。
扫描拨号程序	扫描拨打高额花费电话号码的应用程序。检测到的文件将被作为感染文件处理，如果启用此选项，包含拨号器组件的软件可能会停止工作。
扫描的 rootkit	扫描隐藏对象（文件及进程），通常被称为 rootkit。

- 选定将扫描对象的类别(存档、电子邮件信息等)和其他选项。 这是通过 扫描选择类别选择某些选项。

  您可做以下选择:

选项		描述
扫描文件	扫描所有文件	所有可访问文件将被扫描，而无论其类型。
	只扫描程序文件	进扫描带有下述文件扩展名的程序文件: 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.
	只扫描用户指定的文件扩展名	只扫描带有用户指定的文件扩展名的文件，请用“; ”分隔各个文件扩展名。
扫描加壳文件		扫描加壳文件。
扫描压缩包内容		扫描压缩包内部的文件。
扫描电子邮件文件内部		扫描邮件存档内部。

选项	描述
扫描引导扇区	扫描系统的引导扇区。
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 Cookie	扫描 Cookie 文件。

- 指定对于受感染文件，可疑文件或隐藏文件所采取的操作，在 操作选项 类别。您可以为每个类别指定一个不同的操作。
  - 选择对检测到的感染文件所采取的操作。 您可做以下选择：

操作	描述
已处理	已处理，这些文件将被记录在扫描报告中。
清除病毒	从感染文件中移除恶意代码。
删除文件	没有任何警告下立即删除受感染的文件。
移至隔离区	受感染的文件移到隔离区。 被隔离的文件将不能被执行或打开，因此不存在感染其他文件的风险。

  - 选择对检测到的可疑文件所采取的操作。 您可做以下选择：

操作	描述
已处理	已处理，这些文件将会被记录在扫描报告中。
删除文件	直接删除可疑文件，不进行任何提示。
移至隔离区	移动可疑文件到隔离区。 被隔离的文件将不能被执行或打开，因此不存在感染其他文件的风险。

注意
可疑文件是由启发式分析程序检测出来的，我们建议您将这些可疑文件发送给 BitDefender 实验室。

  - 选择对所检测到的隐藏对象（Rootkit）所采取的操作。 您可做以下选择：

操作	描述
已处理	已处理，这些文件将会被记录在扫描报告中。
重命名名称	通过追加 .bd.ren 在他们的名称后面更改隐藏文件的名称。 因此，您将能够在您的计算机上搜索和找到这些文件。

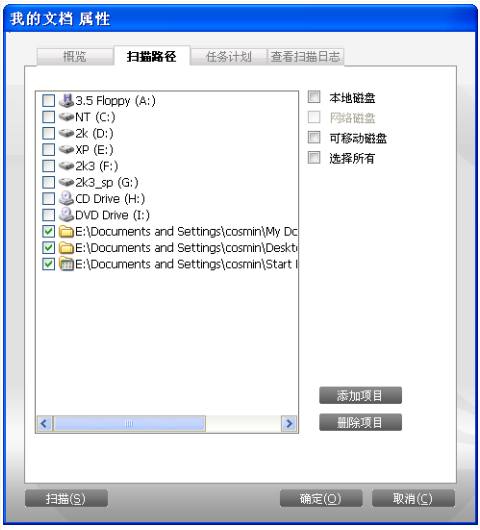
注意
如果您选择忽略检测出的文件，或者选择的操作失败，您必须在扫描向导中选择一个操作。

●扫描过程完毕后，要想提示提交所有可疑文件到 Bitdefender 实验室，请选中其他选项类别中的提交可疑文件到 BitDefender 实验室。

点击 默认 可载入默认设置选项。 点击 确定 保存修改并关闭窗口。

设置扫描对象

要设置特定用户扫描任务的扫描目标，右键单击该任务并选择 更改扫描目标。 就会出现下面的窗口：



扫描目标

您可以看到本地磁盘、网络磁盘、可移动磁盘，以及之前添加的文件或文件夹(如果有的话)的列表。当运行这个任务时，将扫描所有选中的项目。

本部分包含以下按钮:

●添加项目 – 打开一个浏览窗口，您可以选择想要扫描的文件/文件夹。

注意
您也可以使用拖放功能向列表中添加文件/文件夹。

●删除项目 – 删除列表中之前添加的文件/文件夹。

注意
只能删除后来添加的文件/文件夹，BitDefender 自动“发现”的对象不能被删除。

除了上面说明的按钮之外，还有一些其他选项可以帮您快速选择扫描对象。

●本地磁盘 – 扫描本地磁盘。

●网络磁盘 – 扫描所有的网络磁盘。
●可移动驱动器 – 扫描可移动驱动器（光盘、软盘、U 盘等）。
●所有项目 – 扫描所有驱动器，无论是本地、网络或可移动驱动器。

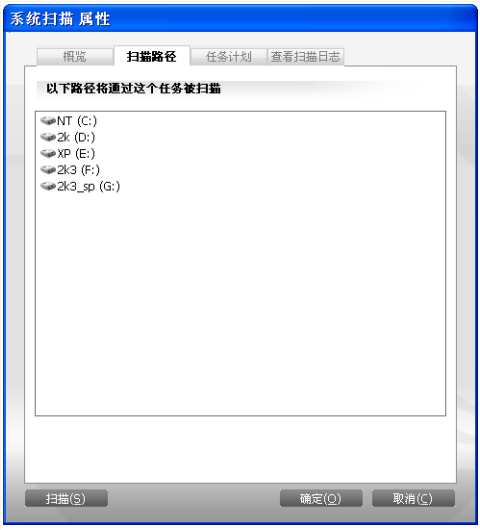
注意
如果您想扫描整个计算机，请选择对应 所有项目 的复选框。

点击 确定 保存更改并关闭窗口。要运行任务，请点击 扫描。

查看系统扫描任务的扫描对象

您不能在系统任务上修改任务的扫描目标。 您只能查看系统扫描任务的扫描对象。

要查看一个指定扫描任务的扫描目标，右键单击任务并选择 显示任务路径。 全面系统扫描 – 例如，将显示下列窗口：



全面系统扫描的扫描对象

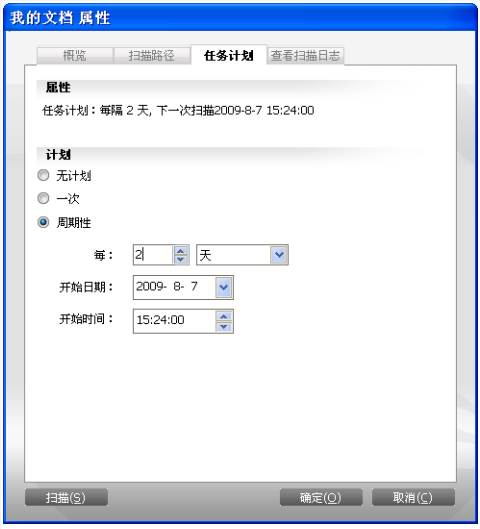
全面系统扫描 和 深度系统扫描将扫描所有磁盘，而 快速系统扫描 将只扫描 Windows 和 Program Files 文件夹。

点击 确定 来关闭窗口。 要运行任务，请点击 扫描。

设置扫描任务运行计划

如果任务复杂，扫描过程将需要较长时间才能完成，且您最好关闭所有其他程序。这也是为什么您应当计划在计算机空闲时段运行这些任务的原因所在。

要查看一个扫描任务的运行计划或对其进行修改，请右键点击该任务并选择 任务计划。 就会出现下面的窗口：



任务计划

您可以看到计划任务，如果有的话。

在设置任务的运行计划时，您需要选择下列选项之一：

- 没有计划 – 仅在用户请求时启动任务。
- 一次 – 仅在特定时间运行该任务一次。指请在 开始日期/开始时间 设置开始运行的日期和时间。
- 周期性 – 从某个特定日期开始，定时周期性运行该扫描任务（每小时、每天、每周、每月或每年）。

  如果您想要在某个时间间隔内重复扫描，选择 周期性地 并在 每隔 编辑栏输入一个 分/小时/天/周/月/年 的数字，表示这个扫描过程的频率。 您也必须在 开始日期/时间 编辑栏指定起始日期和时间。

点击 确定 保存更改并关闭窗口。要运行任务，请点击 扫描。

7.2.5. 扫描对象

在开始启动扫描过程之前，您应该确保 BitDefender 已更新到最新的病毒库。使用旧的病毒库扫描计算机，自从上次更新后可能会有新的恶意软件被 BitDefender 发现。要确认已更新到最新病毒库，请在高级视图上点击 更新>更新。

注意
为了能让 BitDefender 进行完整的扫描，您必须关闭所有的程序。尤其是您的电子邮件客户端(如 Outlook，Outlook Express 或 Eudora)必须关闭。

扫描方式

BitDefender 提供四种手动扫描方式：

- 即时扫描 – 从系统扫描任务或用户扫描任务中运行一个任务。
- 上下文扫描 – 右键单击一个文件或文件夹并选择 BitDefender Business Client。
- 拖放扫描 – 拖放文件或文件夹 到 扫描活动工具条。
- 手动扫描 – 使用 Bitdefender 手动扫描，直接选取要扫描的文件或文件夹。

即时扫描

要全部或部分扫描您的计算机，您可运行默认的扫描任务或您自己创建的任务。 这被称作即时扫描。

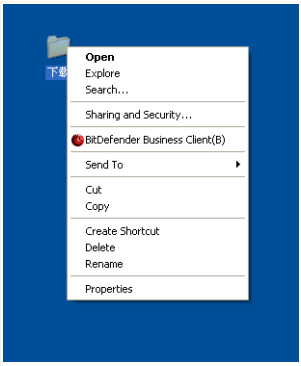
要运行一个扫描任务，您可以使用下列方法之一：

- 在列表中双击希望运行的扫描任务。
- 点击对应此任务的 立刻扫描 按钮。
- 选择该任务并点击 运行任务。

Bitdefender 扫描程序将会显示并启动扫描过程。 欲了解更多信息，请参阅 “BitDefender 扫描程序” (第 85 页)。

右键菜单扫描

如果想不创建扫描任务就扫描一个文件或文件夹，您可以使用右键菜单扫描。 这被称为右键菜单扫描。



右键菜单扫描

右键单击您想要扫描的文件或文件夹并选择 BitDefender Business Client。

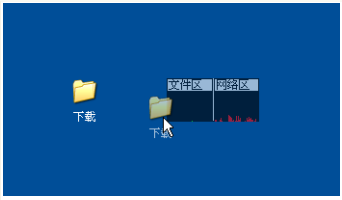
Bitdefender 扫描程序将会显示并启动扫描过程。 欲了解更多信息，请参阅 “BitDefender 扫描程序”(第 85 页)。

您可通过 右键菜单扫描 任务的 属性 窗口查看扫描报告，或修改扫描选项。

拖放方式扫描

拖动您想扫描的文件或文件夹，将其放到 扫描活动工具条上，如下图所示。

拖放扫描



放下文件

Bitdefender 扫描程序将会显示并启动扫描过程。 欲了解更多信息，请参阅 “BitDefender 扫描程序”（第 85 页）。

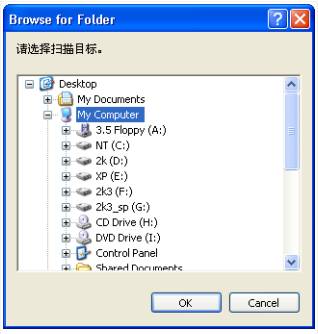
手工扫描

手工扫描需要从 BitDefender 的程序组中选择手工扫描程序，然后直接指定要扫描的对象。

注意
手动扫描非常有用，因为它可以运行在 Windows 的安全模式下。

要使用 BitDefender 扫描选择的对象，在 Windows 开始菜单上，按以下路径：开始 → 程序 → BitDefender Business Client → BitDefender 手动扫描。

就会出现下面的窗口：



手工扫描

选择您想扫描的对象并点击 确定。

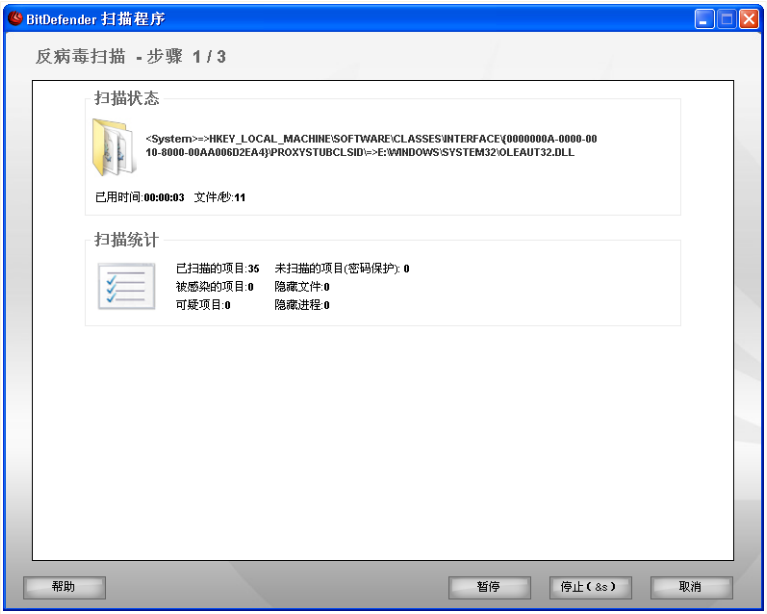
Bitdefender 扫描程序将会显示并启动扫描过程。欲了解更多信息，请参阅 “BitDefender 扫描程序”（第 85 页）。

BitDefender 扫描程序

当您启动一个请求式扫描过程，BitDefender 扫描程序就会出现。 请遵循向导程序的三个步骤来完成扫描过程。

步骤 1/3 — 正在扫描

Bitdefender 将开始扫描选定的对象。



正在扫描

您可以看到扫描的状态和统计(扫描速度，消耗时间，扫描/感染/可疑/隐藏对象的数量及其他)。

注意
扫描过程可能需要较长时间，取决于扫描的复杂程度。

要暂停扫描，只要点击 暂停 ，您需要点击 继续 恢复扫描。

可以在任何时候停止扫描，点击 停止&是. 您将直接跳到向导的最后一步。

请等待 Bitdefender 完成扫描。

步骤 2/3 — 选择操作

当扫描完成后，一个新的窗口将出现，就您可以看到扫描的结果。

操作

您可以看到有多少问题影响到您的系统。

被感染的对象根据它们所感染的病毒分组显示。 点击对应某个病毒的链接，可以看到感染对象的更多信息。

您可为每个问题组选择一个整体的操作，或者为每个问题选择单独的操作。

您可以通过菜单选择:

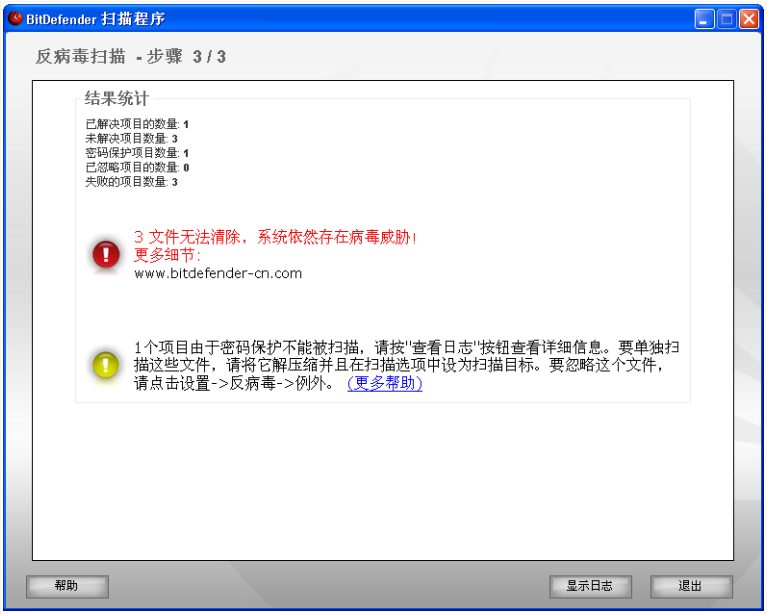
操作	描述
已处理	已处理检测出的文件。
清除病毒	从感染文件中移除恶意代码。
删除文件	删除检测出的文件。
移动到隔离区	移动受感染文件到隔离区。

操作	描述
重命名名称	通过追加 .bd.ren 在他们的名称后面更改隐藏文件的名称。 因此，您将能够在您的计算机上搜索和找到这些文件。

点击 继续 执行所选的操作。

步骤 3/3 — 查看结果

当 BitDefender 完成处理检测出的问题后，将会在一个新窗口显示扫描结果。



总结

您可看到扫描结果的总结。 报告文件在 日志 单元自动保存，根据各自任务的 属性 窗口。

重要
如有需要，请重新启动系统以完成清除过程。

点击 退出 关闭结果窗口。

Bitdefender 未能解决部分问题

在大多数情况下，Bitdefender 能成功清除受感染的文件或隔离受感染的文件。 但是，有些问题当时不能得到解决。

警告
如果有未解决的问题，建议您联系网络安全管理员。

Bitdefender 检测密码保护项目

密码保护的类别有两种类型：存档和安装程序。 除非它们含有受感染的文件并执行，否则他们将不会威胁系统安全性。

确保这些项目都是要清除的：

- 如果密码保护项目是一个有保护密码的存档，解压这个文件并单独对他们进行扫描。 最简单的扫描方法是右键点击，并从菜单中选择 BitDefender Business Client。
- 如果密码保护的项目是安装程序，在执行这个安装程序之前，确保 实时防护 被启用。 如果安装程序被感染，BitDefender 将检测和隔离感染源。

如果您不想让这些文件再次被 BitDefender 检测，您必须将它们添加到扫描例外。要添加扫描例外，切换到高级视图，然后转到 反病毒> 例外。 欲了解更多信息，请参阅 扫描排除的对象。

重要
如果 BitDefender 操作在受限模式下，请要求您的网络安全管理员配置扫描例外。

Bitdefender 检测到可疑文件

可疑文件是被启发式分析程序检测为可能感染了未知的病毒特征码。

如果在扫描期间发现可疑文件，您会被要求提交给 BitDefender 实验室。 点击 确认 发送这些文件给 Bitdefender 实验室进行分析。

7.2.6. 查看扫描日志

要查看任务运行后的扫描结果，右键单击任务并选择 查看扫描日志。 就会出现下面的窗口：

查看扫描日志

在这里，您可以看到执行的每一个任务所生成的报告文件。

提供给您的每一个文件包含记录的扫描过程状态信息，扫描执行的日期和时间，扫描结果的统计。

有两个可用按钮：

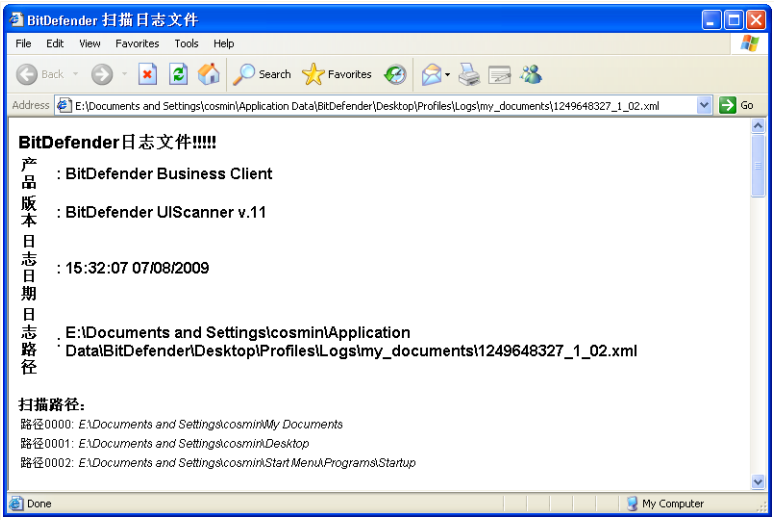
- 删除日志 – 删除选中的扫描日志。
- 显示日志 – 查看选中的扫描日志。 扫描日志会在默认浏览器中打开。

注意
此外，要查看或删除一个日志文件，可以右键点击该文件然后从右键菜单中选择对应的选项。

点击 确定 保存更改并关闭窗口。要运行任务，请点击 扫描。

扫描日志示例

下图是扫描日志的一个示例：



扫描日志示例

扫描日志包含扫描过程的详细信息，如扫描选项、扫描对象、发现的病毒，以及针对各个文件采取的操作等。

7.2.7. 设备扫描中

设备扫描是一个特殊任务，可允许您配置存储设备（CD/DVD，USB 存储设备或映射网络驱动器）的自动检测和扫描。

配置常规扫描设置

要配置该任务的扫描选项和操作方法，请右键单击它并选择属性。 这些设置与所有扫描任务的设置都非常相似。 更多信息 请翻阅 “设置扫描选项”（第 73 页）.

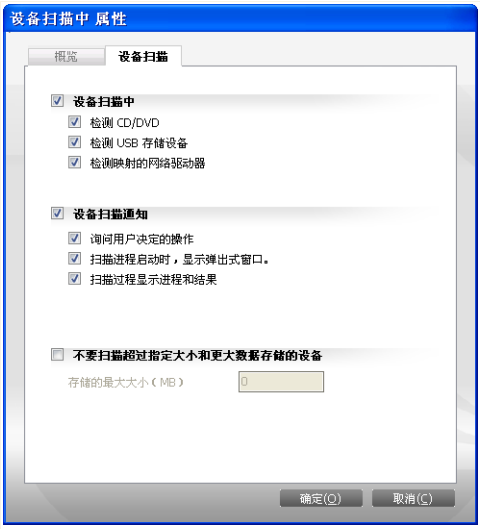
区别如下：

- 没有 rootkit 扫描和处理方法选项。
- 没有启动区、注册表、内存和 cookie 的扫描选项。

应当考虑到，对于 CD/DVD 上检测到的已感染和可疑文件，无法采取任何措施。同样，如果您有没有适当的权限，对于映射网络驱动器上检测到的已感染和可疑的文件，也无法采取任何措施。

配置任务的具体设置

要配置此扫描任务的具体设置，请右键单击它并选择设备扫描。 就会出现下面的窗口：



设备扫描

您可做以下选择：

- 设备扫描中. 选择此选项启用存储设备的自动检测和扫描。 如果您不想检测和扫描特定类型的存储设备（CD/DVD，USB 存储或映射网络驱动器），请清除相应选项。
- 设备扫描通知. 如果您希望检测存储设备时通知用户登陆到计算机，请选择此项。否则，检测的设备将自动被扫描，而无需通知用户（仅在系统托盘上显示扫描进度图标）。扫描进行时用户可以访问。

  您可以选择下列选项：

- 询问用户决定的操作. 一个警报窗口通知用户已检测到一个存储设备并提示用户是否要扫描该设备。
- 扫描进程启动时，显示弹出式窗口。. 开始扫描已检测到的存储设备时，将会有一个小窗口提示用户。
- 扫描过程显示进程和结果. 为了检查进度和扫描结果，用户可以单击系统托盘上的扫描进度图标打开扫描向导。

●不要扫描超过指定大小和更大数据存储的设备. 选择该选项后，将只扫描已检测到的存储数据量小于指定文件大小的设备。 在相应的位置填写文件大小限值（MB）。 0 表示未做任何限制

注意
该选项仅适用于 CD/DVD 和 USB 存储设备。

点击 确定 保存修改。

7.3. 不进行扫描的对象（白名单）

有些时候您可能需要排除某些文件的扫描。例如，您可能想在实时扫描的时候排除一个 eicar 测试文件或者请求式扫描时排除 .avi 文件。

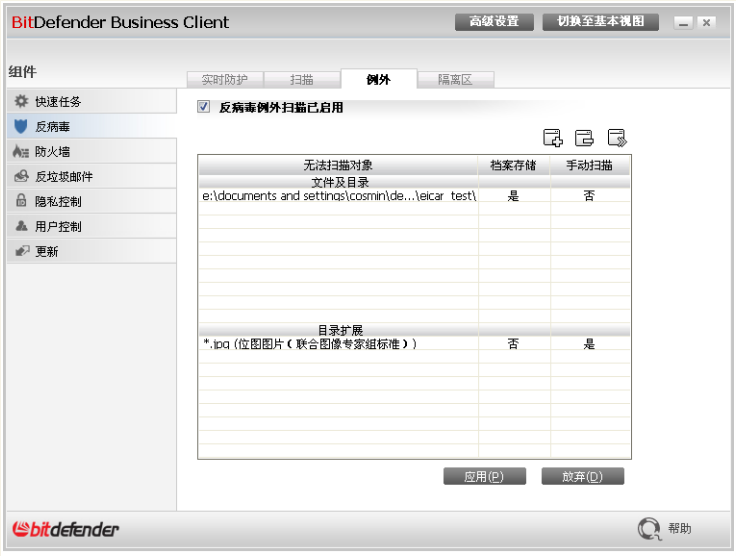
BitDefender 允许从实时扫描或请求式扫描时排除对象，或从两种扫描中排除。这项功能是为了减少扫描时间，以避免干扰您的工作。

有两种类型的对象可以被排除扫描:

●路径 – 由一个路径表示的文件或文件夹（包括其中的所有对象）将会被扫描程序排除扫描。
●文件扩展名 – 所有带有指定文件扩展名的文件将会被排除扫描。

注意
从即时扫描中排除的对象将不会被扫描，不管他们是由您访问还是由一个应用程序访问。

要查看和管理排除扫描的对象，请到高级视图中的 反病毒>白名单。



例外

您可以看到排除扫描的对象(文件，文件夹，扩展名)。对于您可以看到的每个对象，它是被即时扫描所排除，请求式扫描所排除或者两者所排除。

注意
此处指定的白名单不会影响右键菜单扫描。

要从列表中删除一个对象，请选择它然后点击 删除 按钮。

要修改一个条目，请选中它并点击 编辑 按钮。 一个新的窗口将出现，您可以改变被排除的扩展名或路径和您希望他们在必要时被排除扫描的类型。作必要的修改，然后单击 确定。

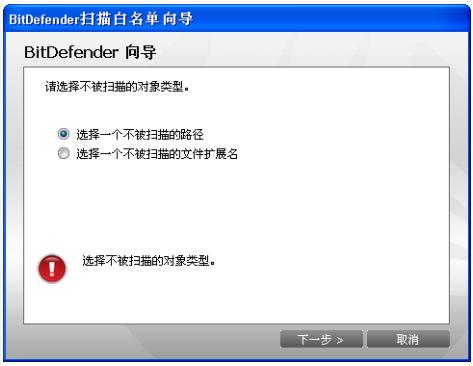
注意
您也可以右键点击一个对象，并使用快捷菜单上的选项进行编辑或删除。

您可以单击 放弃 恢复在规则表上所作的修改，通过点击 应用 来进行保存。

7.3.1. 排除扫描的路径

要排除扫描路径，请点击 添加 按钮。 将会显示配置向导，引导您完成设置要排除扫描的路径。

步骤 1/3 — 选择对象类型



选择对象类型

选择“不扫描文件或路径”。

点击 下一步。

步骤 2/3 — 指定排除的路径

排除的路径

要指定排除扫描的路径，请使用下述方法之一：

- 点击 浏览，然后选择要被排除的文件或路径，接着点击 添加。
- 在编辑栏输入您想要排除扫描的路径，并单击 添加。

注意
如果提供的路径并不存在，将会显示错误信息。点击确定 并检查路径是否有效。

路径将出现在列表中，您可添加任意多的路径。

要从列表中删除一个对象，请选择它然后点击 删除 按钮。

点击 下一步。

步骤 3/3 — 选择扫描类型

扫描类型

您可以看到一个包含了被排除扫描路径的列表，以及采用何种扫描方式被排除。

默认情况下，选定的路径被排除在实时防护和手动扫描。要更改何时应用排除规则，请点击右边的栏并选择你希望的选项。

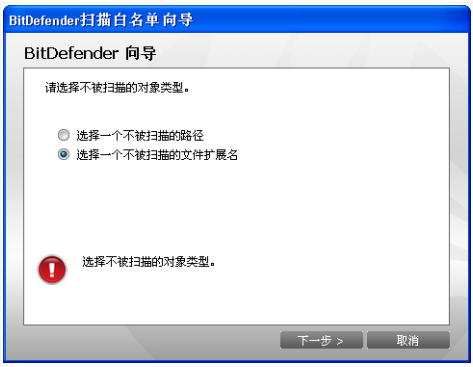
点击完成。

点击 应用 保存修改。

7.3.2. 排除扫描文件扩展名

要排除扫描文件扩展名，请点击 添加 按钮。 将出现一个向导窗口，指引您配置排除的文件扩展名。

步骤 1/3 — 选择对象类型

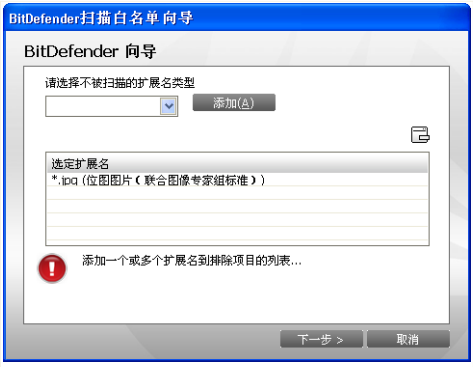


选择对象类型

选择“不扫描文件扩展名”。

点击 下一步。

步骤 2/3 — 指定排除的文件扩展名



排除的文件扩展名

要指定排除的文件扩展名，请采用下述方法之一：

●从下拉列表中选择您想排除的文件扩展名，并点击 添加。

注意
该菜单包含所有在您系统内注册的扩展名列表。当您选择一个文件扩展名，您可以看到它的描述（如果有的话）。

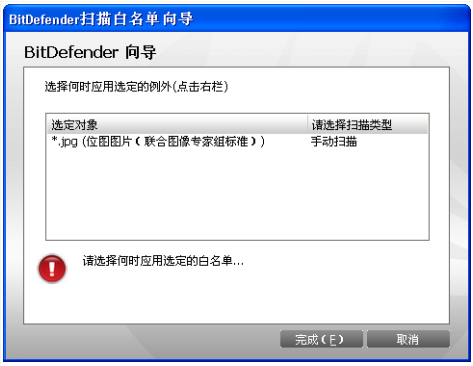
●在编辑框中输入您想排除的文件扩展名并点击 添加。

文件扩展名将出现在表中，您可添加任意多的文件扩展名。

要从列表中删除一个对象，请选择它然后点击 删除 按钮。

点击 下一步。

步骤 3/3 — 选择扫描类型



扫描类型

您可以看到一个表，包括被排除在扫描外的文件扩展名以及采用何种扫描时它们将被排除。

默认情况下，选定的文件扩展名被排除于实时防护和手动扫描，要修改何时应用排除规则，请点击右侧栏并选择所需选项。

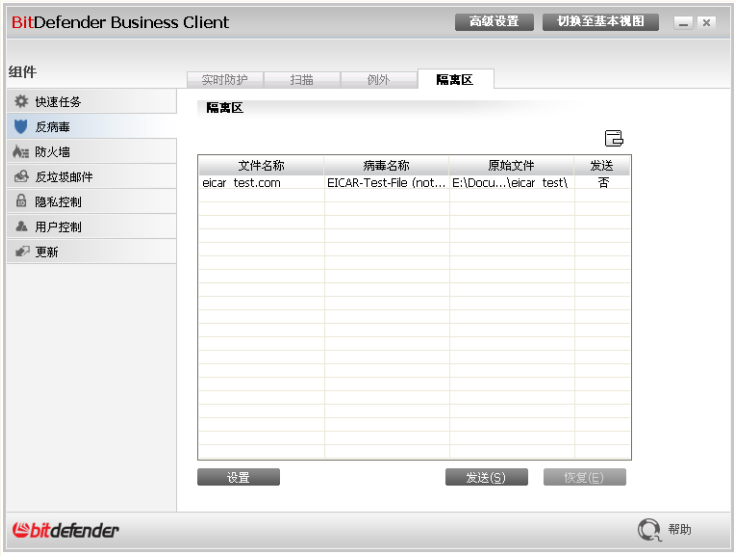
点击完成。

点击 应用 保存修改。

7.4. 隔离区

BitDefender 允许将被感染文件或可疑文件到一个名叫“隔离区”的安全区域。文件被放到隔离区后，将不能感染其他文件，同时您可将它们发送给 BitDefender 实验室做进一步分析。

要查看和管理隔离的文件或配置隔离区，请到高级视图中的反病毒>隔离区。



隔离区

隔离区显示所有当前被隔离的文件。 对于每一个隔离的文件，您可以看到它的名称，检测出的病毒名称，路径，原始位置和提交的日期。

注意

当一个病毒被隔离后，就不再有任何危害，因为它将不能被执行和打开。

7.4.1. 管理被隔离的文件

要从隔离区删除选定文件，请点击 删除 按钮。如果您将文件恢复到其原始路径，请点击 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。

右键菜单。. 上下文菜单，可让您轻松管理隔离的文件。前面提到的数据可以用于相同的选项。您也可以选择 刷新 来刷新隔离单元。

7.4.2. 配置隔离区设置

要配置隔离区设置，请点击 设置。 显示一个新窗口。

隔离区设置

使用隔离区设置，您可以设置 BitDefender 自动执行下列操作:

删除旧文件。. 要自动删除旧的被隔离文件，请选中相应的选项。 您必须指定被隔离的文件将保留的天数，以及 BitDefender 检查旧文件的频率。

注意
默认情况下， BitDefender 每天都会将检查旧文件并删除30天以上的文件。

删除重复文件。. 要自动删除重复的被隔离文件，请选中相应的选项。 您必须在两次检查重复之间有明确的间隔天数。

注意
默认情况下，BitDefender 每天检查重复的隔离文件。

自动提交文件。. 要自动提交被隔离的文件，请选中相应的选项。 您必须指定提交文件的频率。

注意
默认情况下，BitDefender 每隔 60 分钟提交一次隔离区的文件。

点击 确定 保存修改并关闭窗口。

8. 防火墙

防火墙保护您的计算机免除未经允许的进站和出站连接尝试。它类似于门卫--它将密切关注您的互联网连接，并允许或阻止互联网访问。

注意
如果您使用宽频或 DSL 连接互联网，防火墙是必不可少的。

在保密模式中，您的计算机对于恶意软件和黑客是"隐藏的"。防火墙模块能自动检测和保护端口扫描(通常，黑客在准备攻击计算机之前，会对电脑发送许多程序包以发现"进入点"，找出系统的漏洞，从而进行攻击)。

用户指南的防火墙单元包含以下主题:

- 防火墙识别
- 防火墙状态
- 通讯保护
- 高级设置
- 防火墙活动
- 网络区

8.1. 防火墙识别

BitDefender 防火墙将会给您的网络/互联网连接提供最佳的保护，而不需要进行配置。不管您是直接连接到互联网、单一的网络还是多个网络(以太网，无线网络，VPN 或其他网络类型)，无论可信与否，防火墙为了适应不同的情况将进行自我配置。

默认情况下，BitDefender 将自动检测您计算机的网络配置，创建一个合适的基本防火墙配置方案。它也能根据配置将检测到的网络添加到可信任网络区或不可信网络区的配置方案中。

8.1.1. 什么是防火墙的配置方案?

防火墙配置方案是一套控制应用程序网络/互联网访问的规则。

根据您计算机的网络配置，BitDefender 自动创建一个特定类型的配置方案。这个创建的基本配置方案包含系统应用程序和 BitDefender 组件所需要的网络访问规则或基本的 Internet 访问规则。

注意
不论您网络连接的数量，只需要创建单一的防火墙配置方案。

有 3 种类型的基本配置方案:

配置方案	描述
直接连接	包含基本互联网访问规则，建议网络配置允许直接访问互联网。 此规则既不允许网络用户访问您的计算机，也不允许您浏览网络。
不可信任	包含网络访问规则，适合连接不可信任网络的网络配置。 规则允许您浏览网络，但阻止其他网络成员访问您的计算机。
可信任	包含网络访问规则，适合连接可信任网络的网络配置。不限制任何网络访问。这意味着您可以访问网络共享，网络打印机和其他网络资源。同时，网络成员也可以连接到您的计算机并访问您的共享资源。

应用程序试图连接到互联网时，将添加合适的规则到配置方案。 您可以选择允许或拒绝默认情况下没有配置地应用程序访问互联网，默认情况下，只允许白名单上的应用程序，其他应用程序则会询问许可。

注意
要指定应用程序第一次尝试连接互联网的访问策略，请转到 状态 单元设置防护级别。 要编辑现有的配置方案，请转到 通讯 单元并单击 编辑配置方案。

8.1.2. 什么是网络区?

网络区是指网络内部的一台计算机或完全独立于您的计算机的整个网络，同时它能侦测到计算机并进行连接。实际上，网络区是一个允许或拒绝访问您的计算机的 IP 地址或IP 地址范围。

默认情况下，BitDefender 自动添加区为特定的网络配置。一个区是通过建立一个适当的网络访问规则而增加，在当前配置方案下，适用于整个网络。

有 2 种类型的区域:

区域类型	描述
可信任网络	计算机可以连接到可信任网络的计算机，并且它们也能连接到您的计算机。 所有来自这样区域的连接尝试，以及您的计算机连接到这样区域的尝试都是允许的。 如果一个网络被增加为可信任网络，您就可以不受限制地访问网络共享，网络打印机和其他网络资源。同时，网络成员也可以连接到您的计算机，并访问您的共享资源。
不可信任网络	计算机不能连接到不可信任网络里的计算机，并且它们也不能连接到您的计算机。 所有来自这样区域的连接尝试，以及您的计算机连接这样区域的尝试都是被阻止的。 由于 ICMP 通讯被拒绝和保密模式被启用，您的计算机在这个网络区域中几乎是不可见的。

注意

要编辑一个区域，请转到 网络区 单元。 要编辑一个区域相关的规则，请转到 通讯 单元并单击 编辑配置方案。

8.1.3. 防火墙操作

安装完毕重新启动系统后，BitDefender 会自动侦测您的网络配置，然后创建一个合适的基本配置方案，并根据检测到的网络添加一个区域。

注意

如果您直接连接到互联网，尚未为相应的网络配置创建网络区域。 如果您连接到一个以上的网络，添加的区域取决于各自的网络。

网络配置的每变化一次，无论您是连接到另一个网络，还是禁用了网络连接，都将创建一个新的防火墙配置方案。同时，网络区域也会作相应的更改。

新的防火墙配置方案创建后，原有的配置方案将被保存起来。这样，当您返回相应的网络配置时，它将被重新加载。

根据网络配置的不同，BitDefender 将自动调整配置。 默认情况下，BitDefender 防火墙是这样进行配置的：

- 如果您直接连接到互联网，无论您是否也连接到其他网络，都将创建一个直接连接的配置方案。否则，BitDefender 会创建一个不可信任的防火墙配置方案。

注意

作为一种安全策略，可信任的配置方案不是默认建立的。 要创建一个可信任的配置方案，您必须重置现有的配置方案。欲了解更多信息，请参阅 “重设配置方案”(第 116 页)。

- 区域的添加取决于网络配置。

区域类型	网络配置
可信任网络	私有 IP且没有网关 – 计算机是局域网(LAN)的一部分，不连接到互联网。 例如，创建家庭网络允许家庭成员共享文件、打印机或其它资源。
	域控制器检测的私有IP – 计算机是局域网(LAN)的一部分，并连接到一个域。 例如办公室网络，允许用户共享域内部的文件或其他资源。 一个域意味着存在一套成员计算机必须遵循的策略。
不可信任网络	打开(不安全的)无线网络 – 计算机是本地无线网络(WLAN)的一部分。 例如您使用公共场所的免费接入点访问互联网。

注意

在某些网络配置情况下，区域是不会创建的，例如:

- 公网(路由)IP – 计算机直接连接到互联网。
- 私有 IP，有网关，但未检测到域控制器 – 计算机是局域网(LAN)的一部分，但没有加入域，且通过网关连接互联网。 例如学校的校园网，允许用户访共享文件或其他资源。

- 保密模式已启用。
- VPN 和路由连接被允许。
- Internet 连接共享不允许用于不可信任的网络区域。
- 白名单中的应用程序自动允许访问，而其他应用程序，首次尝试连接时需要征询意见。

8.2. 防火墙状态

要配置防火墙保护，请转到高级视图的 防火墙>状态。

防火墙状态

在此单元，您可以启用/禁用 防火墙， 阻止所有的网络/互联网通讯，并对新事件设置默认行为。

重要
要保护免受互联网攻击，请保持 防火墙 被启用。

要阻止所有网络/互联网通讯，单击 阻止通讯 然后点击 是 进行确认。这将把您的计算机与其它计算机隔离开。

稍后要允许通讯，只要单击 允许通讯。

在此单元底部，可以看到 BitDefender 传入和传出通讯的统计信息。本图显示两分钟内的互联网通信流量。

注意
即使禁用防火墙，图表仍会显示。

8.2.1. 设置防护级别

您可以选择最符合您的防护需求的安全级别，上下拖动滚动条设置合适的防护级别。

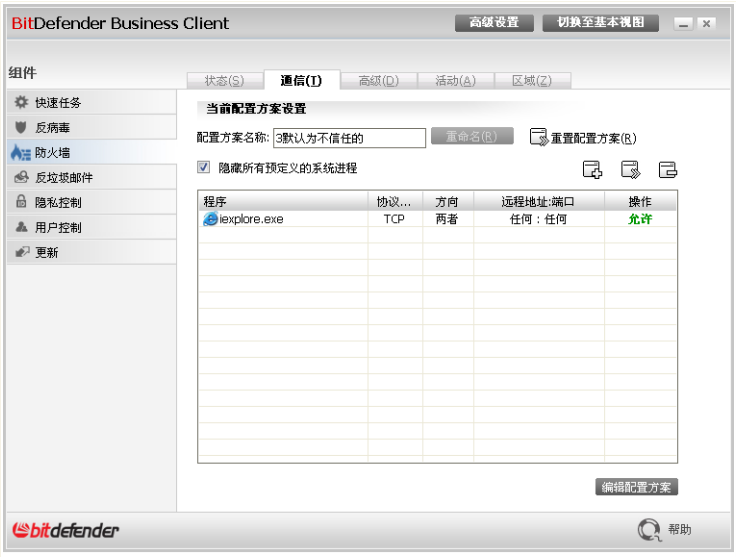
共有 3 个防护级别:

防护级别	描述
游戏模式	应用当前规则并允许所有通讯请求，包括那些不符合当前规则的请求，而不进行提示。 强烈不建议使用该策略，但对网络管理员和游戏玩家可能有用。
允许推荐	应用当前规则，允许所有应用程序发出的连接请求，这些连接必须是 BitDefender 认定为合法的(白名单)。对于其它的连接请求，BitDefender 会征求您的同意。您可以在 通讯 单元看到已创建的通讯规则。 白名单中的程序是世界范围内最常用的应用程序。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，以及服务器客户端和操作系统应用程序。 如果您想看到哪些程序在白名单，单击 显示白名单。
询问	应用当前规则，所有不匹配现行规则的连接请求都要征求您的同意。

单击 默认级别 设置默认策略（允许推荐)。

8.3. 通讯控制

要管理当前配置文件的防火墙规则，请转到高级视图的 防火墙>通讯。



通讯控制

在此单元，您可以通过创建特定协议、端口，应用程序和/或远程地址的规则，指明允许/拒绝哪些传入或传出的连接。

规则可以通过警报窗口被自动加入或单击 添加 按钮并选择规则参数手动添加。

8.3.1. 自动添加条例

由于 防火墙 已启用，每次与互联网的建立连接时，BitDefender 都将征求您的同意：

防火墙警报

您能看到的信息如下：试图访问互联网的应用程序，应用程序文件路径，访问目标，访问协议和应用程序试图连接的端口。

点击 允许，允许应用程序生成的通过各自的 IP 协议和端口从本地主机到任何目标位置所有通讯（入站和出站）。如果您点击 阻止，超出各自 IP 协议的应用程序将被拒绝访问互联网。

根据您的应答，一项规则将被创建，应用和列于表格中。下次应用程序试图连接，这条规则将被默认应用。

重要
允许传入的连接尝试，只有来自您明确地信任的 IP 或域名。

8.3.2. 手动添加规则

单击 添加规则 按钮并选择规则参数。 就会出现下面的窗口：

添加规则

要添加一个新的防火墙规则，请按照下列步骤操作:

1. 选择将创建新的防火墙规则的应用程序。

   要选择一个应用程序，点击 浏览，找到它并点击 确定。

   如果您想为所有应用程序创建一个规则，只要选中应用此规则到所有应用程序即可。
2. 选择规则应用的协议。

   最通用的协议列表可供您选择特定的协议。从相应的下拉菜单中选择指定的协议(规则应用的协议)或选择 任何 选择所有协议。

   下表列出了协议以及每个协议的简短描述，您可以选择:

协议	描述
ICMP	网际控制信息协议 – 是对互联网协议(IP)的延伸 。ICMP 支持数据包包含错误、控制，和信息性消息。PING 命令，例如，使用 ICMP 测试互联网连接。
TCP	TCP(传输控制协议) – TCP 使两个主机建立连接并且交换数据流。TCP 保证数据传输，同时保证那数据包将按照原样被转送。

协议	描述
UDP	UDP(用户数据协议) – 是基于 IP 传输设计的高性能协议。游戏和其他视频程序经常使用 UDP 传输数据。

3. 从相应的菜单选择规则操作。

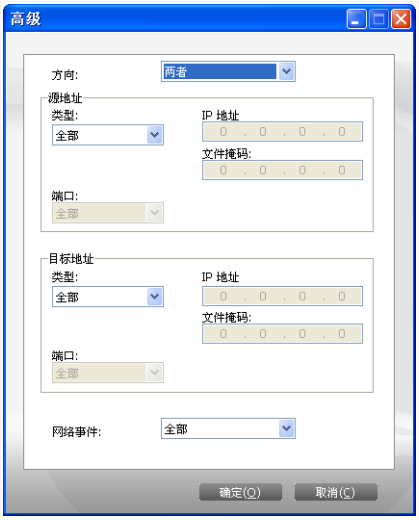
操作	描述
允许	在指定的情况下，应用程序被允许网络/互联网访问。
拒绝	在指定的情况下，应用程序被拒绝网络/互联网访问。

4. 如果先前选定的协议是 TCP 或 UDP，您可以指定规则是否应用于应用程序，使它作为服务器程序或不是。

   选中 允许其他计算机连接到此应用程序，对所有网络事件都应用此操作。此操作意味着您可以允许或拒绝此应用程序开放端口的权利。

   如果您想要只应用这个操作到 UDP 通讯和 TCP 通讯与连接，清除相关的复选框。

如果您想要配置规则的更多高级设置，单击 高级。 将出现一个新的窗口：



高级规则设置

您可以配置下列行动:

●方向 – 选择通信的方向。

类型	描述
传出	规则只应用于传出的通讯。
传入	规则只应用于传入的通讯。
两者	规则对发送和接收的 Cookie 都生效。

●源地址 – 指定源地址。

要指定源地址，从菜单中选择地址类型，并指定所需的数据。 您可做以下选择:

类型	描述
任何	规则应用任何源地址。
主机	规则只允许这个主机地址。 您必须键入主机的 IP 地址。
家庭网络	规则只允许指定的源网络。 您必须键入网络的 IP 地址和子网掩码。
本地主机	规则只允许本地主机。 如果您使用一个以上的网络界面，从菜单中选择规则应用的网络界面。如果您想要应用规则到所有本地主机，选择 任何。
本地网络	规则只允许本地网络。 如果您连接到一个以上的网络，从菜单中选择规则应用的网络。如果您想要使用规则应用于所有本地网络，选择 任何。

如果您已经选择了 TCP 或 UDP 作为协议，您可以设置一个特定的端口或一个介于 0 到 65535 之间的范围 。如果您想要规则应用于所有端口，选择 任何。

●目标地址 – 指定目标地址。

要指定目标地址，从菜单中选择地址类型，并指定所需的数据。 您可做以下选择:

类型	描述
任何	规则适用于任何目标地址。
主机	规则只允许指定的目的主机。 您必须键入主机的 IP 地址。

类型	描述
家庭网络	规则只允许指定的目的网络。 您必须键入网络的 IP 地址和子网掩码。
本地主机	规则只允许目的本地主机。 如果您使用一个以上的网络界面，从菜单中选择规则应用的网络界面。如果您想要应用规则到所有本地主机，选择 任何。
本地网络	规则只允许目的本地网络。 如果您连接到一个以上的网络，从菜单中选择规则应用的网络。如果您想要使用规则应用于所有本地网络，选择 任何。

如果您已经选择了 TCP 或 UDP 作为协议，您可以设置一个特定的端口或一个介于 0 到 65535 之间的范围 。如果您想要规则应用于所有端口，选择 任何。

- 网络事件 – 如果您已经选择了 TCP 或 UDP 作为协议，选择规则应用的网络事件。

点击 确定 关闭高级设置窗口。

点击 添加 添加防火墙规则。

8.3.3. 管理规则

您可以在当前配置方案表格中看到目前已经创建的规则。

选中复选框 隐藏系统进程 隐藏关于系统或 BitDefender 进程的规则。

规则列表是根据优先级进行的排序，第一个规则具有最高优先级。 单击 编辑配置方案 进入 详细视图 ，这里您可以通过上移和下移来改变规则的优先级。

要删除一个规则，只要选择它并单击 删除规则 按钮。

要修改规则，选择它并单击 修改规则 按钮或双击规则。

注意
一个上下文菜单也是可用的，它包含下列选项：添加规则，删除规则 和 编辑规则。

8.3.4. 修改配置方案

您可以修改一个配置方案，通过点击 编辑配置方案。 将出现下列窗口：

浏览视图

规则分为两个部分：传入规则和传出规则。您可以查看每个规则的应用程序和规则的参数(源地址、目标地址、源端口、目的端口、操作等)。

要删除一个规则，只要选择它并单击 删除规则 按钮。 要删除所有规则，单击 清空列表 按钮。 要修改一个规则，选择它并单击 编辑规则 按钮或双击它。 要暂时停用一个规则而不删除它，清除相应的复选框。

您可以提升或降低规则的优先级。 单击 在列表中上移 按钮提升选择规则一个等级的优先级， 或单击 在列表中下移 按钮降低选择规则一个等级的优先级。 要分配一个规则到最高优先级，单击 移到最前 按钮。 要分配一个规则到最低优先级，单击 移到最后 按钮。

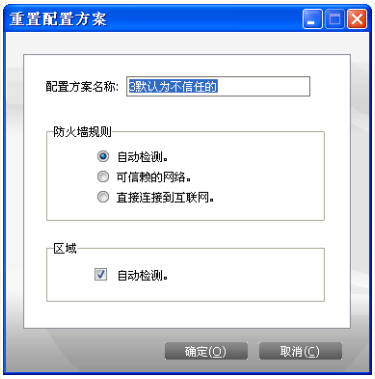
注意

一个上下文菜单也是可用的，它包含下列选项: 添加规则，编辑规则，删除规则，上移，下移，移到最前，移到最后 和 清空列表。

点击 确定 来关闭窗口。

8.3.5. 重设配置方案

高级用户可以选择重新配置防火墙配置方案，以优化防火墙防护或根据他们的需要进行定制。 要重设防火墙配置方案，单击 重设配置方案。 就会出现下面的窗口：



重设配置方案

您可以配置下列行动：

●配置方案名称 – 在编辑栏键入一个新名称。
●规则 – 指定应该为系统应用程序创建什么类型的规则。

您可做以下选择：

选项	描述
自动检测	让 BitDefender 检测网络配置并创建一套合适的基本规则。
可信任网络	建立一套适合可信任的网络的基本规则。
直接网络连接	建立一套适合直接连接互联网的基本视图。

●区域 – 选中 自动检测 让 BitDefender 为检测的网络创建合适的区域。

点击 确定 关闭窗口并重设配置方案。

重要
如果您选择重设配置方案，所有在这个单元添加的规则都将丢失。

8.4. 高级设置

要配置 BitDefender 防火墙的高级设置，请转到高级视图的 防火墙>高级。

高级设置

在这一单元，您可以配置 BitDefender 防火墙的高级设置。 高级设置允许您指定 ICMP 通讯的过滤规则(ICMP 设置) 和阻止多播信息，共享您的互联网连接或使您的计算机对于恶意软件和黑客不可见(设置)。

8.4.1. 配置 ICMP 过滤设置

在菜单中，您可以选择下列策略之一对 ICMP 过滤进行设置:

- 允许所有 ICMP 通讯 – 允许所有 ICMP 通讯。
- 阻止所有 ICMP 通讯 – 阻止所有 ICMP 通讯。

●自定义 ICMP 过滤 – 自定义的方式是过滤 ICMP 通讯。 您将可以选择允许何种类型的 ICMP 数据包。

您可做以下选择:

选项	描述
Echo	这个选项使 Echo 回复和 Echo 请求消息生效。Echo 请求是发送数据小包到主机的 ICMP 消息中并且等待数据被送回到 Echo 的回复。主机必须回应所有的 Echo 请求，并且在请求消息中包含确切的数据。Echo 回复是 ICMP 消息引起同时回应 ICMP Echo 请求消息，必须是给所有主机和路由器。
重定向	这是通知一个主机改变 ICMP 消息的路由选择信息方向(发送数据包的替代路线) 。如果主机试图通过路由器(R1)发送数据，并且通过其它路由器(R2)送达主机，并且从主机对 R2 有一个直接的连接是可用的，重定向将通知主人关于这个线路。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，即使有一条更好的可用路线，消息仍然不会被送出。
目的地不能到达	如果目的地主机不能找到，路由器将生成 ICMP 消息通知客户端，除非数据图有一个多点传送地址。这条消息的原因包括与主机的连接不存在(距离是无限的)，表明协议或端口不是活跃的，或数据必须被分割，但'不要分割' 的提示是开启的。
任何其他类型包	启用这个选项，任何其他包在 Echo，目的地不能到达 或 重定向 将通过。

8.4.2. 配置高级防火墙设置

以下的高级防火墙设置可供选择:

●阻拦所有多播通讯 – 丢弃所有的收到的多播数据包。

多播通讯是一种把信息同时传递给网络中一个特定组的通讯方式。只要多点传输被用户允许，数据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)视频流。听到多播地址的计算机用户可以接收或拒接这个数据包.如果选择接收，多播用户就能收看该视频了。

过多的多播通讯将占用带宽和资源。如果开启了这个选项，任何收到的多播数据包都将抛弃。然而，我们不建议选择这个选项。

- 启用 Internet 连接共享(ICS)支持 – 可以支持 Internet 连接共享(ICS)。

注意

此选项不会在您的系统自动启用 ICS，但只允许这种类型的连接的情况下，才在您的操作系统中启用它。

互联网连接共享使本地网络成员能通过您的计算机连接到互联网。当您受益于某种特定/特殊的互联网连接方式(如无线网络连接)，并让其他成员也共享您的网络时，它是十分有用的。

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。这还将打开您计算机上的一些端口(被使用您计算机连接的成员打开)。

- 保密模式 – 让您的计算机对于恶意软件和黑客是隐形的。

找出您的计算机是否易受攻击的一种简单方法是它尝试连接端口，然后检查是否有回应，这称为端口扫描。

恶意个体或软件程序不需要发现您的计算机是否存在，更不用说对网络提供服务的计算机。 保密模式 选项将停止任何想查出您的计算机端口是否开放，或确切知道端口情况的回应尝试。

- 监察程序文件与防火墙规则相匹配的变化 – 检查每一个试图连接到互联网的应用程序，看看自动添加规则控制以来是否已经改变。如果该应用程序已改变了，会出现一个警告提示您是否允许或阻止应用程序到互联网的连接。

一般情况下，应用程序会在更新后改变。但是，有一种风险，是由恶意软件改变的，其目的是感染您的计算机和其它计算机网络。

注意

我们建议您保持选中这个选项，并允许进入的只是自从他们的访问规则控制创建以来，那些预计改变的应用程序。

标记的应用程序都应该是值得信赖的和有较高安全性。 您可以选中 忽略标记进程的改变，以便允许标记的进程改变后可以连接互联网，而不会出现警告提示事件。

- 启用 Wi-Fi 通知 – 启用 Wi-Fi(无线网络) 通知。

●应用相同的配置方案到所有新网络 – 创建一个默认(通用) 防火墙配置方案，命名 通用网络，并应用它到检测的新网络进行配置。 如果您回到已经存在防火墙配置方案的旧网络，相关的防火墙配置方案将加载代替通用配置方案。

8.5. 连接控制

要通过应用程序监控当前网络/互联网活动(TCP 和 UDP)，并打开 BitDefender 防火墙日志，请转到高级视图的 防火墙>活动。

连接控制

您可以看到根据应用程序分类的总通信。对于每一个应用程序，您可以看到连接和打开的端口，以及关于传入与传出通讯的速度、总接收和总发送的统计信息。

这个窗口实时呈现了当前网络/互联网活动。如果连接或端口关闭，您可以看到相应的统计是为灰色，并最终消失。 同样的事情发生在所有相应的应用数据所产生的传输或打开一个您关闭的端口。

单击 阻止 创建规则限制选择应用程序、端口和连接的通信。 您将被要求确认您的选择。该规则可访问 通讯 单元作进一步微调。

注意
要阻止一个应用程序、端口或连接，您也可以右键单击它并选择 阻止。

点击 关闭 以结束选定进程的所有实例。 您将被要求以确认您的选择。

注意
要关闭一个进程，您也可以右键单击它并选择 关闭。

单击 导出快照 导出这个文件到一个 .txt 文件。

制订一个全面的事件清单，关于防火墙模块的使用(启用/停用防火墙，阻止通讯，启用保密模式，修改设置，应用配置方案)或所产生的活动检测(扫描端口，阻止连接尝试或根据规则的通讯)，检查 bitdefender 防火墙日志文件，可以通过点击 查看日志进行浏览。该文件位于当前 Windows 用户的公共文件夹，路径是: ... bitdefender \ bitdefender Firewall\ bdfirewall.txt.

8.6. 网络区

一个区域是一个 IP 地址或一个 IP 地址范围，创建在配置方案内的特殊规则。规则既可以允许网络成员不受限制地访问您的计算机(可信任网络)，或与此相反，从网络中完全孤立您的计算机(不可信任网络)。

默认情况下，BitDefender 自动侦测您的网络连接，并根据网络配置添加一个区域。

注意
如果您连接到几个网络，根据它们的配置，会添加多个区域。

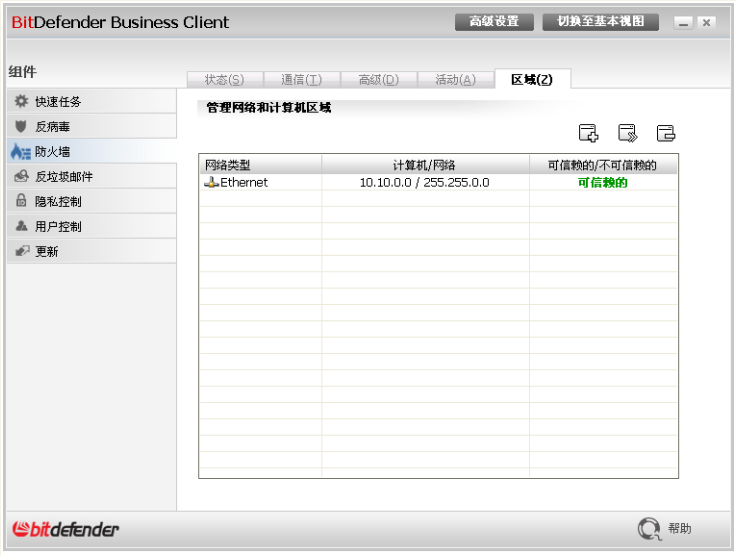
可信任的网络，在下列网络配置下默认添加:

●私有 IP，没有网关 – 计算机是局域网(LAN)的一部分，并且没有连接到互联网。
●域控制器检测的私有IP – 计算机是局域网(LAN)的一部分，并连接到一个域。

不可信任网络，下列网络配置下默认加入:

●打开(不安全的)无线网络 – 计算机是本地无线网络(WLAN)的一部分。

要管理网络区域，请转到高级视图的 防火墙>网络区。



网络区

您可以在表格中看到当前配置文件相关的网络区。 对于每一个区域，您可以看到的网络类型(局域网，无线网络，点对点通讯网络等等)，计算机或网络相关的区域是否可信。

要修改一个区域，选择它并单击 编辑区域 按钮或双击它。

注意

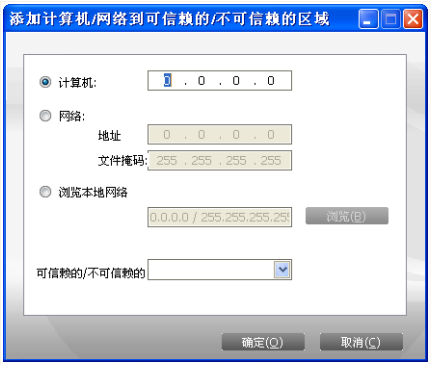
默认情况下，BitDefender 添加开放的无线网络为不可信任的网络。 如果您是连接到一个特定的开放式无线网络与可信赖的电脑(在家里或一对夫妇的朋友)，您可能要编辑相关的区域。为了能够与其他网络成员实现资源共享，就必须设定为一个可信赖的网络。

要删除一个区域，选择它并单击 删除区域 按钮。

8.6.1. 添加区域

您可以手动添加区域。 举例来说，这可以让您只跟您的朋友在一个开放式无线网使用共享文件(加入他们的计算机为可信赖的网络)，或阻止计算机连接一个可信赖的网络(加入它作为一个不可信赖的网络)。

要加入一个新的区域，单击 添加区域 按钮。 就会出现下面的窗口：



添加地带

要添加区域，按照下列步骤操作：

1. 从本地网络指定一台计算机或指定整个本地网，添加作为一个区域。 您可以选择下列方法之一：
   - 要加入一个指定的计算机，选择 计算机，并提供其 IP 地址。
   - 要加入一个指定的网络，选择 网络，并提供其 IP 地址和子网掩码。
   - 浏览本地网络，以查找并添加计算机或网络。

     要浏览本地网络，选择 浏览本地网络，然后点击 浏览。将出现一个新的窗口，您可以看到您连接的所有网络，以及网络内的所有成员。

     从列表中选择您想要添加区域的计算机或网络，并点击 确定。
2. 从菜单中选择想要创建的区域类型(可信赖网络或不可信赖网络)。
3. 点击 确定 添加到区域。

9. 反垃圾邮件

BitDefender 反垃圾邮件采用一流的创新技术和标准的反垃圾邮件过滤器，将垃圾邮件在到达用户的收件箱之前清除。

用户指南的 反垃圾邮件 单元包含以下议题:

- 反垃圾邮件识别
- 反垃圾邮件状态
- 反垃圾邮件设置

9.1. 反垃圾邮件认知

对个人和企业来说，垃圾邮件问题日趋严重。这并非一件美好的事情，您不希望孩子看到它，您可能应此而被老板炒掉(浪费太多时间或您的办公邮箱接受色情邮件)，但您却不能阻止他人发送垃圾邮件。 退而求其次，只能阻止接收垃圾邮件。然而不幸的是，垃圾邮件没有一定的形状和大小，而且数目繁多。

9.1.1. 反垃圾邮件过滤器

BitDefender 反垃圾邮件引擎包含多种不同过滤器以保护您的收件箱不受垃圾邮件侵扰: 好友列表，垃圾邮件发送者列表，字符集过滤器，图像过滤器，URL过滤器，NeuNet(启发式)过滤器 及 贝叶斯过滤器。

注意
反垃圾邮件 模块的 设置 单元，您可以启用/禁用每一个过滤器。

好友列表/垃圾邮件发送者列表

大多数人经常与特定群组的人保持联络，或收到来自公司和集团内部员工的信息。通过使用 好友或垃圾邮件发送者清单，您能轻松将想要接收的电子邮件(好友)和永远不想接收的电子邮件(垃圾邮件发送者)进行分类。

好友/垃圾邮件发送者列表可以被管理，从 高级视图 或从集成到大多数公共邮件客户端的 反垃圾邮件工具条 进行管理。

注意
我们建议您将朋友的名字和电子邮件邮址添加到 好友清单。BitDefender 不会阻止来自清单中的邮件。因此，把朋友加入好友清单能确保收到合法的邮件。

字符集过滤器

许多垃圾邮件都是用斯拉夫字符和/或亚洲字符写成的。字符集过滤器检测这种类型的信息并标记为 SPAM。

图像过滤器

由于避开启发性过滤器的现象越来越多，如今的收件箱充斥着许多包含不请自来的邮件信息。为了应对这一现象，BitDefender 采用了图像过滤器。此过滤器将邮件内的图像特征和 BitDefender 数据库进行对比。如果发现有类似，BitDefender 将在邮件上标记 SPAM。

URL 过滤器

几乎所有的垃圾邮件都包含各种网址的链接，这些网址通常是包含广告和购物信息，还有可能用于网络钓鱼。

BitDefender 拥有一个这种链接的数据库。 URL 过滤器根据它的数据库检查邮件中每一个 URL 连接。如果匹配的话，用[SPAM]标记这个邮件为垃圾邮件。

NeuNet(启发式)过滤器

NeuNet(启发式)过滤器 在所有邮件组件上执行一系列测试(不仅仅是邮件主题，也包括 HTML 或文本格式的邮件正文)，寻找字词，短语，链接或其他特征的垃圾邮件。根据分析的结果，增加一个垃圾邮件评分到邮件信息。

过滤器还可以在主题栏标记检测的邮件为 SEXUALLY-EXPLICIT: 并标记[SPAM]。

注意

从2004年5月19日起，含有色情内容的垃圾邮件都必须在标题内加入SEXUALLY-EXPLICIT:的词句进行警告。

贝叶斯过滤器

贝叶斯过滤器 模块会根据指定文字出现的次数的统计资料进行邮件分类。若指定的文字在邮件内的次数符合垃圾邮件的，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，要是有四个字母的单词在垃圾邮件里经常出现，那后续含有这单词的邮件是垃圾邮件的可能性将会提高。所有邮件内的相关单词都会经过过滤器的计算。垃圾邮件的可能性将以统计资料决定。

该模块提供另一个有趣的特点：它是能够接受训练的。它能快速的适应用户所收到的邮件类型并存入所有的相关资料。为了有效地发挥作用，过滤器必须经过培训，这意味着，将提交垃圾邮件和合法邮件的样品，就像狗是根据气味进行追查。有时，过滤器必须予以纠正，作出错误的决定后，提示进行调整。

重要

您可以在 反垃圾邮件工具条 使用 是垃圾邮件 和 非垃圾邮件 按钮调整贝叶斯过滤器。

9.1.2. 反垃圾邮件操作

BitDefender 反垃圾引擎使用组合使用所有的反垃圾邮件过滤器来决定一封电子邮件爱你是否应该进入您的 Inbox。

重要

BitDefender 检测出的垃圾邮件，会在主题行标记 [spam] 前缀。 BitDefender 自动将垃圾邮件转移到一个特定文件夹，如下：

- 在 Microsoft Outlook 中，垃圾邮件被转移到一个 Spam 文件夹，位于 已删除邮件 文件夹。
- 在 Outlook Express 和 Windows Mail 中，垃圾邮件被直接移动到 已删除邮件 中。
- 在 Mozilla Thunderbird 中， 垃圾邮件被移动到 Spam 文件夹，位于 废件箱 文件夹中。

如果您使用其他邮件客户端，您必须创建一条规则，指定将由 BitDefender 标记为 [spam] 的邮件移动到一个您指定的垃圾邮件文件夹。

每封来自互联网的电子邮件首先会被 好友列表/垃圾邮件发送者 过滤器检查。 如果发送者的地址存在于 好友列表，邮件会被直接移动到您的 收件箱。

否则 垃圾邮件发送者列表 过滤器会继续检查发送者的地址是否在其列表中。 如果发送者地址在垃圾邮件发送者列表中，则邮件会被标记为"垃圾邮件"并被移动到 垃圾邮件 文件夹（位于 Microsoft Outlook）。

同时， 字符集过滤器 将检查电子邮件是否是由斯拉夫字符或亚洲字符书写的。如果是，电子邮件将标记[SPAM]，并移动到 Spam 文件夹。

如果电子邮件不是由斯拉夫字符或亚洲字符书写的， 就会交给 图像过滤器。 图像过滤器 将检查所有的电子邮件与附件图像是否含有垃圾内容。

URL 过滤器 会寻找链接，并将发现的链接和 BitDefender 数据库比较。如果有相匹配的链接，BitDefender 将增加一个垃圾邮件评分到这封电子邮件。

NeuNet(启发式)过滤器 将接管电子邮件和将进行一系列测试，寻找字词、短语或其他垃圾邮件特点。如果是，它也会增加垃圾邮件评分到这封电子邮件。

注意
如果电子邮件在主题栏被标记为色情，BitDefender 会认为是垃圾邮件。

贝叶斯过滤器 模块将进一步分析邮件，根据特定字词出现的次数统计信息分类为垃圾邮件或非垃圾邮件。它会增加垃圾邮件评分到这封电子邮件。

如果总得分(URL 评分+启发式评分+贝叶斯评分)超过了垃圾邮件评分(用户在 状态 单元设置的安全级别)，该邮件被判定是垃圾邮件。

9.1.3. 反垃圾邮件升级

每当您进行更新：

- 新的图像特征会加入到 图像过滤器。
- 新的链接会加入到 URL 过滤器。
- 新的规则将加入到 NeuNet(启发式)过滤器。

这将会提高反垃圾邮件引擎的效率。

要保护您的计算机免受垃圾邮件发送者的攻击，BitDefender 可以执行一个自动更新。保持 自动更新 选项启用。

9.2. 反垃圾邮件状态

要配置反垃圾邮件保护，请转到高级视图的 反垃圾邮件>状态。

反垃圾邮件状态

在这个单元您可以配置 反垃圾邮件 模块并且可以查看它的活动信息。

重要
要防止垃圾邮件进入您的 收件箱 ，保持 反垃圾邮件过滤器 的启用状态。

在 统计 单元，您可以查看每个会话的反垃圾邮件活动的结果(您的计算机开机以来)或总结(BitDefender 安装以来)。

为了配置 反垃圾邮件 模块，必须按以下步骤操作:

9.2.1. 步骤 1/2 - 设置安全级别

您可以选择最符合您的防护需求的安全级别，上下拖动滚动条设置合适的防护级别。

共有 5 个安全级别:

安全级别	描述
宽松	为收到大量合法商业邮件的账户提供保护。 过滤器将允许大部分邮件通行，但可能产生一些错误信息(垃圾邮件被认为是合法邮件)。
适度宽松	为收到合法商业邮件的账户提供保护。 过滤器将允许大部分邮件通行，但可能产生一些错误信息(垃圾邮件被认为是合法邮件)。
中等	为常规账户提供保护。 为了避免把合法邮件过滤，过滤器只会阻止大多数垃圾邮件。
适度严格	为定期收到大量垃圾邮件的账户提供保护。 过滤器会让少量垃圾邮件通行，但可能会产生一些错误(合法信息被错误地标示为垃圾邮件)。 配置 好友/垃圾邮件发送者清单 并培训 智能学习引擎(贝叶斯)，以便减少误报数量。
严格	为定期收到大量垃圾邮件的账户提供保护。 过滤器会让少量垃圾邮件通行，但可能会产生一些错误(合法信息被错误地标示为垃圾邮件)。 添加联系人到 好友清单，以便减少误报数量。

设置缺省防护级别(适度严格)，单击 默认级别。

9.2.2. 步骤 2/2 – 填充地址列表

地址列表包含了发送合法的电子邮件的地址以及垃圾邮件的地址信息。

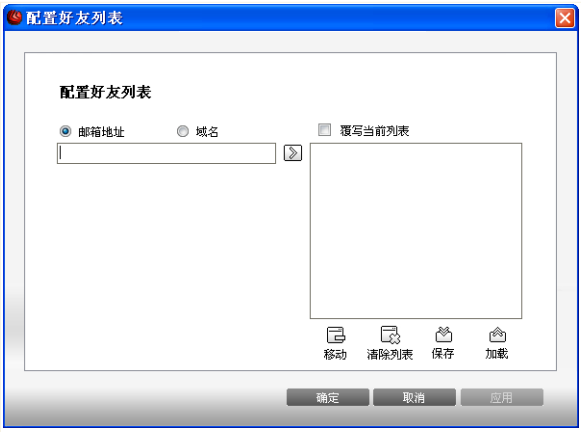
好友清单

好友清单 是一个您总是同意接收邮件的所有地址列表，不论内容。您的好友邮件不会被标记为垃圾邮件，即使内容疑似垃圾邮件。

注意

任何来自包含在 好友清单 中的电子邮件，将自动传送到收件箱，而不做进一步处理。

要配置好友清单，单击 管理好友（或在 反垃圾邮件工具条上单击 好友 按钮）。



好友清单

这里，您可以在 好友清单 中添加和删除项目。

如果想要添加一个电子邮件地址，选中 Email地址 选项，输入地址并单击 。这个地址将出现在 好友清单。

重要
语法：name@domain.com.

如果您想要添加一个域，选中 域名 选项，输入域名并单击 。 域名将出现在 好友清单。

重要
语法：

- @domain.com, *domain.com 和domain.com – 不管他们的内容如何，所有从 domain.com 收到的电子邮件将到达您的 收件箱 ；
- *domain* – 不管内容，所有从 域名 收到的电子邮件(无论域名后缀)将到达您的 收件箱；
- *com – 不论内容，所有收到以 com 结尾的电子邮件将到达您的 收件箱 ；

要删除列表中的一个项目，选择它并点击 删除 按钮。如果您点击 清除列表 按钮您将会删除名单中的所有项目，但注意：这是不可恢复的。

使用 保存/ 载入 按钮来保存/载入 好友清单到期望的位置。文件将有.bwl 扩展名。

选择 加载时清空现有名单 能在加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添加到 好友清单。BitDefender 不会阻止来自清单中的邮件。因此，把朋友加入好友清单能确保收到合法的邮件。

点击 应用 和 确定 保存和关闭 好友清单。

垃圾邮件发送者清单

垃圾邮件发送者清单 是一个不论其内容，您都不想接收的邮件发送者地址的列表。

注意
任何来自包含在 垃圾邮件发送者清单 的电子邮件，将自动标记为 SPAM，而不做进一步处理。

要配置垃圾邮件发送者列表，单击 管理垃圾邮件发送者 (或在 反垃圾邮件工具条 上单击 垃圾邮件发送者 按钮).

垃圾邮件发送者清单

这里，您可以在 垃圾邮件发送者清单 中添加或删除项目。

如果您想要添加一个电子邮件地址，选中 Email 地址 选项，输入地址并单击 。地址将出现在 垃圾邮件发送者清单。

重要
语法：name@domain.com.

如果您想要添加一个域名，选中 域名 选项，输入域名并单击 。 域名将出现在垃圾邮件发送者列表。

重要
语法：

- @domain.com，*domain.com 和 domain.com – 所有从 domain.com 收到的电子邮件将被标记作为SPAM；
- *domain* – 所有从 域名（无论域名后缀）收到的电子邮件将被标记为 SPAM；
- *com – 所有收到域名以 com 为结尾的电子邮件将被标记作为 SPAM。

警告
请不要添加正常的网页邮箱服务域名（如 163 邮箱、Hotmail、新浪邮箱等）到垃圾邮件发送者列表。否则，使用这些邮箱的用户发给您的邮件都将会被当作垃圾邮件。例如，您添加 163.com 到垃圾邮件发送者列表，则所有从 163.com 发出的邮件都会被标记为 [spam]。

要删除列表中的一个项目，选择它并点击 删除 按钮。如果您点击 清除列表 按钮您将会删除名单中的所有项目，但注意：这是不可恢复的。

使用 保存/ 载入 按钮保存/载入 垃圾邮件发送者列表 到一个期望的位置。文件将有 .bwl 扩展名.

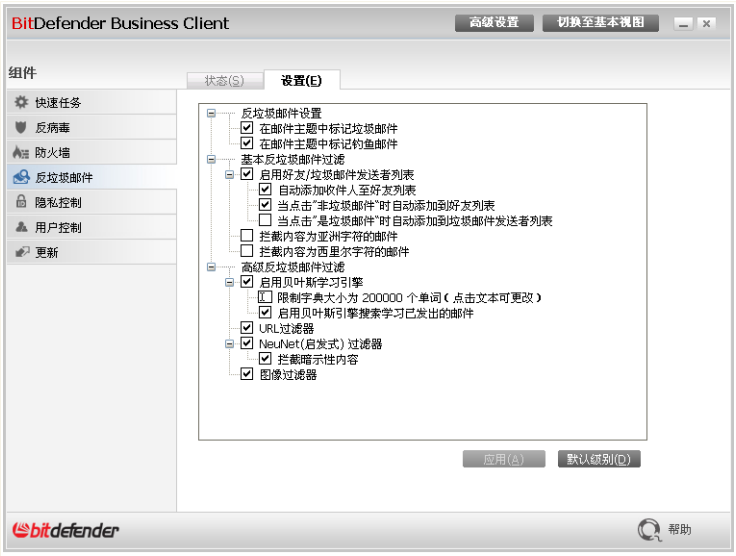
选择 加载时清空现有名单 能在加载以前保存的名单时,重设现有名单的内容。

点击 应用 和 确定 保存和关闭 垃圾邮件发送者清单。

重要
如果您想要重新安装 BitDefender，安装之前保存 好友 / 垃圾邮件发送者 列表是一个好想法，在安装完成后可以加载这些列表。

9.3. 反垃圾邮件设置

要配置反垃圾邮件设置及过滤器，请前往高级视图中的 反垃圾邮件>设置。



反垃圾邮件设置

这里，您可以启用/禁用每一个反垃圾邮件过滤器，并且可以指定反垃圾邮件模块的一些其他设置。

有3类类似于 Windows 的可伸展菜单选项可用（反垃圾邮件设置， 基础反垃圾邮件过滤器 和 高级反垃圾邮件过滤器）。

注意
点击"+" 展开类别或点击"-"收起它。

9.3.1. 反垃圾邮件设置

●在主题栏标记垃圾邮件 – 所有被认为是垃圾邮件的电子邮件信息将在主题栏标记[SPAM]。

●在主题栏标记网络钓鱼 – 所有的被认为是网络钓鱼的电子邮件会在主题行标记[SPAM]。

9.3.2. 基础反垃圾邮件过滤器

●好友/垃圾邮件发送者列表 – 使用 好友/垃圾邮件发送者列表 过滤电子邮件。
- 自动添加收件人到好友清单 – 自动添加发送的邮件收件人到好友清单。
- 自动添加到好友清单 – 当您单击 反垃圾邮件工具条 上的 非垃圾邮件 按钮，所选择的电子邮件发件人会自动添加到好友清单。
- 自动添加到垃圾邮件发送者清单 – 当您在 反垃圾邮件工具条 上单击 是垃圾邮件 按钮，所选择的电子邮件发件人会自动添加到垃圾邮件发送者清单。

注意
非垃圾邮件 和 是垃圾邮件 按钮用于培训 贝叶斯过滤器。

●阻止用亚洲字符书写的邮件 – 阻止用亚洲字符书写的邮件。
●阻止用斯拉夫字符书写的邮件 – 阻止用 斯拉夫字符 书写的邮件。

9.3.3. 高级反垃圾邮件过滤器

●启用智能学习引擎(贝叶斯) – 开启/关闭 智能学习引擎(贝叶斯)。
- 限制字典大小在 200000 字以内 – 置贝叶斯过滤器的字典大小 – 越小越快速，越大越准确。

注意
推荐大小：200.000 词。

- 用传出的电子邮件培训智能学习引擎(贝叶斯) – 用传出的电子邮件培训智能学习引擎(贝叶斯)。

●URL 过滤器 – 开启/关闭 URL 过滤器。
●NeuNet(启发式)过滤器 – 开启/关闭 NeuNet(启发式)过滤器。
- 阻止色情内容 – 开启/关闭在主题栏检测邮件带有色情内容。

●图像过滤器 – 开启/关闭 图像过滤器。

注意
选择/清除相关的复选框来启用/禁用它。

单击 应用 保存修改或单击 默认级别 加载默认设置。

10. 隐私控制

BitDefender 监控着您系统中可能被间谍软件利用的“热点”，同时检查所有对您的系统和软件的修改。这可有效阻止黑客安装在系统中的木马和其他恶意软件，保护您的私密信息不被窃取（如信用卡号码等）。

BitDefender 也扫描您访问的网站，如果有网络钓鱼威胁被检测到将会及时提醒您。

用户指南的 隐私控制 单元包含以下议题:

- 隐私控制状态
- 高级设置 – 身份识别控制
- 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

10.1. 隐私控制状态

要配置隐私控制或查看其信息，请到高级视图中的 隐私控制>状态。

隐私控制状态

10.1.1. 隐私控制

您可以查看隐私是启用还是禁用。 如果您想更改隐私控制状态，请清除或选中对应的复选框。

重要
为防止您的私密资料失窃，保护您的隐私，请保持启用 隐私控制。

隐私控制采用下列的防护控制保护您的计算机：

- 身份识别控制 – 根据您在 身份识别 单元创建的规则，对所有传出的 HTTP 和 SMTP 通讯进行过滤，保护您的机密资料。
- 注册表控制 – 程序要达到在 Windows 启动时自动运行的目的，而试图修改注册表项，需要询问您的许可。
- Cookie 控制 – 新的网站试图设置一个 cookie 时，询问您的许可。
- 脚本控制– 每次网站试图激活一个脚本或其他活动内容，都将经过您同意。

要配置这些控制的设置，单击 高级设置。

在这个单元底部，您可以看到 隐私控制统计。

设置防护级别

您可以选择最符合您的防护需求的安全级别，上下拖动滚动条设置合适的防护级别。

共有 3 个防护级别:

防护级别	描述
严格	所有隐私控制组件可用。 您必须配置合适的身份控制规则，以防止未经授权的机密信息发送。
默认	注册表控制 和 个人信息控制 启用。 您必须配置合适的身份控制规则，以防止未经授权的机密信息发送。
宽松	仅注册表控制 启用。

您也可点击 自定义级别 自己定义防护级别。 会出现一个窗口，选择您想要启用的防护控制并单击 确定。

点击 默认级别 将滚动条放到默认级别位置。

10.1.2. 反网络钓鱼保护

网络钓鱼是一种犯罪活动，在互联网上使用社会工程学技术，以诱骗人们提供私人信息。

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。

网络钓鱼邮件通常是一个涉及到您的网上账户的问题。它试图说服您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，是伪造的）输入私人资料的要求。例如，为了确认账户信息，如用户名和密码，提供您的银行账户或社保号码。 有时，为了增强说服力，假信息可假装如果您不使用提供的链接，您的账户会暂停使用等。

网络钓鱼还利用间谍软件，如木马键盘记录程序，直接从您的电脑上窃取账户信息。

主网页网络钓鱼的目标是顾客的在线支付服务，例如 eBay 和 PayPal，以及银行提供的网上服务。 最近，用户的社交网络网站也已针对网络钓鱼，以取得个人识别资料用于身份盗用。

为了防止您在网上冲浪时受到网络钓鱼软件侵袭，请保持 反网络钓鱼 为启用状态。这样，BitDefender 将在您访问网站时进行网络钓鱼扫描，如果存在任何网络钓鱼威胁，它会及时提醒您。 您可以配置一个网站白名单，BitDefender 将不会扫描白名单中的网站。

为了更容易管理反网络钓鱼保护和白名单，使用集成到 Internet Explorer 的 BitDefender 反网络钓鱼工具栏。 欲了解更多信息，请参阅 “反网络钓鱼工具栏”（第 50 页）。

如果您想要 BitDefender 反网络钓鱼工具条，您可以清除 显示反网络钓鱼工具条 复选框。当您试图访问窃取个人信息时，您将会被警告。

10.2. 高级设置 – 身份识别控制

保证私密数据的安全是一个困扰我们的大问题。数据失窃随着互联网通讯的发展而愈加严重，并利用最新技术欺骗用户交出私密信息。

无论是您的电子邮件或信用卡号码，只要它们落入了恶意之手，就会给您带来损失：您可能会发现自己淹没在垃圾邮件中，或者发现巨额的信用卡消费。

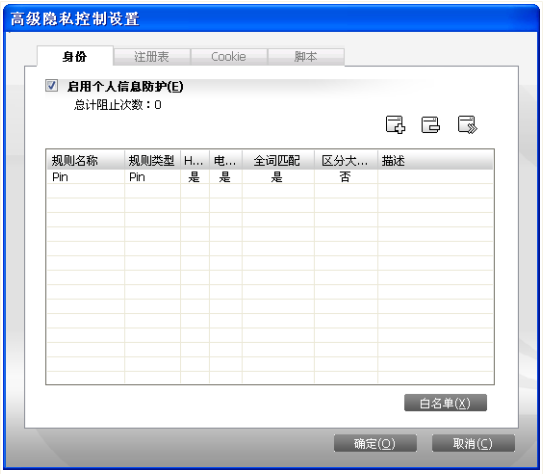
隐私控制保护您的敏感数据免受在线窃取。 基于您创建的规则，隐私控制扫描从您计算机发出的网页、电子邮件和即时通讯通信中是否包含特定字符串（例如，您的信用卡号码）。如果发现匹配，则对应的网页、电子邮件或即时讯息会被阻止。

您可创建规则来保护您认为需要保密的任何信息，比如电话号码、身份证号码、银行卡号、电子邮件地址等。 本功能支持多用户，使用不同的 Windows 用户账户登录可以设置不同的个人信息防护规则。 只有当您登录到自己的 Windows 用户账户后，您所创建的规则才会被应用和访问。

在 身份识别 单元可以配置隐私规则。 要访问这个单元，打开 高级隐私控制设置 窗口并单击 身份识别 页签。

注意

要打开 高级隐私控制设置 窗口，在高级视图单击 隐私控制>状态 并单击 高级设置。



个人信息控制

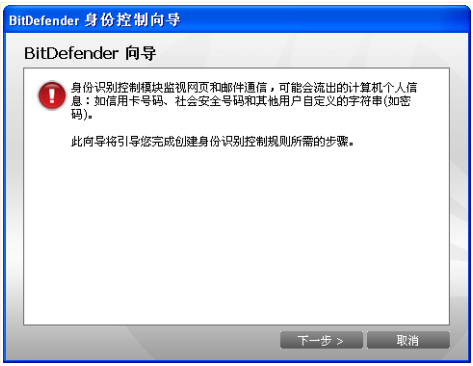
如果您想要使用的隐私控制，请执行下列步骤：

1. 选中 启用身份识别保护 复选框。
2. 创建规则以保护您的敏感数据。 欲了解更多信息，请参阅 “创建个人信息控制规则”（第 139 页）。
3. 如果有需要，在您已创建的规则下，定义特定的例外。 欲了解更多信息，请参阅 “定义例外”（第 142 页）。

10.2.1. 创建个人信息控制规则

要创建个人信息保护规则，请点击 添加 按钮，并按照配置向导的引导进行操作。

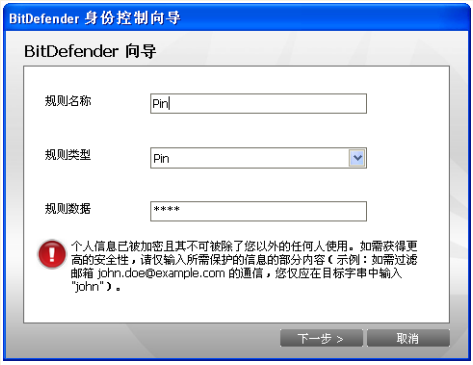
步骤 1/4 - 欢迎窗口



欢迎窗口

点击 下一步。

步骤 2/4 - 设置规则类型和规则数据



设置规则类型和规则数据

您必须设置下列参数:

●规则名称 - 请在此输入规则的名称。

●规则类型 – 选择规则类型（地址、姓名、信用卡、身份证等）。

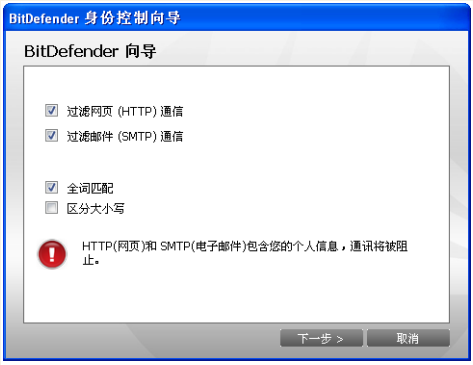
●规则数据 – 请输入您希望保护的数据。 例如，如果您要保护您的信用卡号码，在这里输入全部或部分号码。

注意
如果您输入少于三个字符，系统会提示您验证数据。我们推荐您至少输入三个字符，以避免造成误堵的讯息及网页。

所有您输入的数据都会被加密，为了加强安全性，请不要输入您要保护的信息的全部数据。

点击 下一步。

步骤 3/4 – 选择要检查的通信类型



选择通信类型

选择您希望 BitDefender 扫描的通信类型。 您可做以下选择：

●过滤 Web（HTTP）通讯 – 扫描 web(HTTP)通讯并阻止匹配该规则的外传数据。
●过滤邮件（SMTP）通讯 – 扫描电子邮件 （SMTP）通讯并阻止包含有匹配规则的数据的外传电子邮件。

您可以仅当规则全部匹配字符串或大小写匹配字符串时应用此规则。

点击 下一步。

步骤 4/4 - 规则说明

规则说明

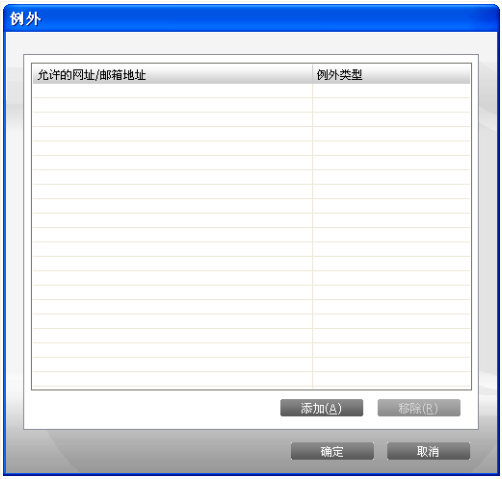
在编辑框中输入对此规则的简短说明。 由于当您查看规则时，需要被被阻止的数据（字符串）不是明文显示的，规则说明能帮助您了解该规则的用途。

点击完成。

10.2.2. 定义例外

在有些情况下，您需要为特定的识别规则定义例外。 当您创建规则时，防止您的信用卡号码不被发送的 HTTP(网页)。每当您的信用卡号码，从您的用户账号中提交到一个网站时，相关的网页会被阻止。例如，您想在一个在线商店购买鞋类(您知道是安全的)，您需要在相关的规则下指定一个例外。

要打开管理例外的窗口，请点击例外。



例外

要添加例外，按照下列步骤进行：

1. 点击 添加 在表中添加一个新条目。
2. 双击 指定允许的地址，并提供您想要添加例外的网址或电子邮件地址。
3. 双击选择类型，并从菜单中选择和之前输入的地址对应的类型。
   - 如果您指定的是一个网站地址，请选择HTTP。
   - 如果您指定的是一个电子邮件地址，请选择SMTP。

要删除一个例外条目，请从列表中选中它然后点击 删除。

点击 确定 保存修改。

10.2.3. 管理规则

您能看到表格中的规则列表。

要删除一个规则，只要选择它并单击 删除 按钮。 要暂时禁用一个规则而不删除它，清除相关的复选框。

要编辑规则，请选中并点击 "编辑" 按钮或双击它，一个新的窗口会出现。

编辑条例

在这里，您可以更改规则名称，描述和参数(类型,数据和通讯)。 单击 确定 以保存更改。

点击 确定 保存修改并关闭窗口。

10.3. 高级设置 – 注册表控制

Windows 操作系统有个非常重要的组件叫 注册表，Windows 在此记录其设置选项、已安装的程序、用户信息及其他很多信息。

注册表 还被用作定义哪些程序在 Windows 启动时会自动启动，病毒经常利用这一点以便在用户重启电脑时自动加载。

注册表控制 对 Windows 注册表保持关注 – 对于检测木马是十分有效的。程序需要在 Windows 启动时自动运行而修改注册表项时，会及时提醒您。

注册表警报

您可以拒绝这个修改，通过点击 否 或者您通过点击 是 允许它可以修改。

如果您想 BitDefender 记住您的应答，检查 总是运用这一操作到这个程序。 通过这种方式，一个规则将创建，并且同样的操作将应用对于这个程序试图修改注册表的启动项，以便在 Windows 启动时程序自动运行。

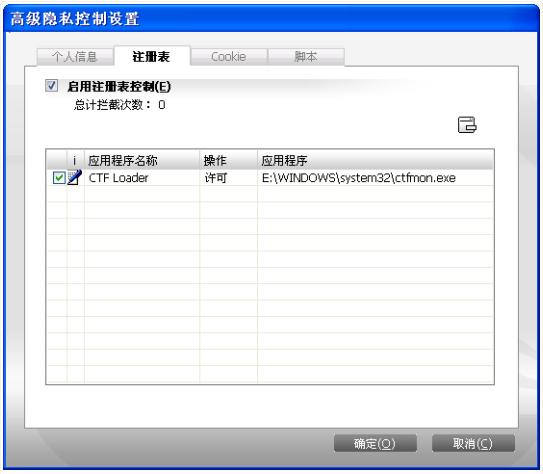
注意

通常在您安装需要在下次系统重启时运行的新软件时，BitDefender 都会警告您。绝大多数情况下，这些程序是合法的，可以被信任。

每一个设置的规则都可以在 注册表 单元作进一步微调。 要访问这个单元，打开 高级隐私控制设置 窗口并单击 注册表 页签。

注意

要打开 高级隐私控制设置 窗口，在高级视图单击 隐私控制>状态 并单击 高级设置。



注册表控制

您可以在表格中看到已创建的规则列表。

要删除一个规则，只要选择它并单击 删除 按钮。 要暂时禁用规则而不删除它，清除相关的复选框。

要更改一个规则的操作，双击操作栏并从菜单中选择合适的选项。

点击 确定 来关闭窗口。

10.4. 高级设置 - Cookie 控制

Cookie 在互联网中非常常见。它们是存储在您计算机上的小文件，您访问的网站在您的计算机上创建 Cookie 文件以记录您的特定信息。

Cookie 的主要目的是让您访问网站更方便，例如，网站可以借助 Cookie 记住您的姓名和偏好，这样您不必在每次访问该网站时都输入这些信息。

但是 Cookie 同样可以被用作跟踪您的上网习惯，从而触及您的隐私。

这就是 Cookie 控制 的作用。启用 Cookie 控制 后，每当一个新网站试图在您的计算上设置 Cookie 时，都会征询您的许可：

Cookie 警报

您能看到试图设置或发送 Cookie 文件的程序名。

选中 记住我的选择 选项并点击是 或 否，就会在规则表中创建一条规则并应用它。下次您访问此网站时将不会被提示。

您可用这个功能选择信任和不信任的网站。

注意

由于互联网上巨量的 Cookie 被使用，Cookies 控制 开始使用时可能相当烦人，因为开始时它会询问很多有关某网站要在您的计算机上设置 Cookie 的问题。不过当您把您常用的网站都添加到规则表中后，上网就会变得和以前一样方便。

每一个设置的规则，可以在 Cookie 单元作进一步微调。 要访问这个单元，打开高级隐私控制设置 窗口并单击 Cookie 页签。

注意

要打开 高级隐私控制设置 窗口，在高级视图单击 隐私控制>状态 并单击 高级设置。

Cookie 控制

您可以在表格中看到已创建的规则列表。

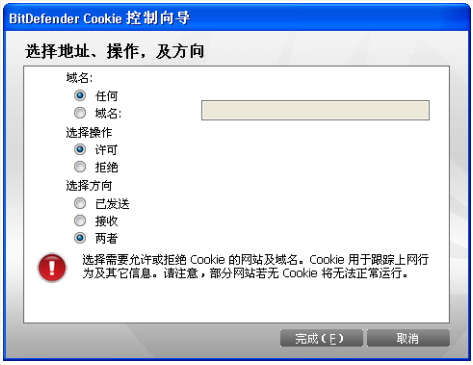
要删除一个规则，只要选择它并单击 删除 按钮。 要修改一个规则的参数，只要双击它并作预期的修改。 要暂时禁用一个规则而不删除它，清除相关的复选框。

这些规则可以自动输入(通过警报窗口)或手动(单击 添加 按钮并选择规则参数)。配置向导就会出现。

10.4.1. 配置向导

配置向导仅一个步骤。

步骤 1/1 – 选择地址，操作和方向



选择地址、操作，及方向

您可以设定下述参数:

- 域名 – 输入要应用规则的域名。
- 操作 – 选择规则的操作。

操作	描述
允许	允许该域名上的 Cookie 操作。
拒绝	不允许域名上的 Cookie 操作。

- 方向 – 选择通信的方向。

类型	描述
发送	规则只对发向网站的 Cookie 生效。
接收	规则只对接收自网站的 Cookie 生效。
两者	规则对发送和接收的 Cookie 都生效。

点击完成。

注意
您可以接受 cookies，但不返回他们，通过设置操作 拒绝 和方向 传出。

点击 确定 保存修改并关闭窗口。

10.5. 高级设置 – 脚本控制

脚本 及 ActiveX 控件和Java applets 等代码被用于创建交互式网页，它们可被编写为具有危害行为。例如，ActiveX 控件可以获取对您计算机数据的完全控制，可以读取您的数据、删除信息、截获密码并截取您上网时的邮件。您应当只接受来自您信赖网站的脚本。

Bitdefender 可让您选择运行此类脚本或阻止其执行。

由于使用 脚本控制，您将管理信任的和不信任的网站。每次某网站试图激活一个脚本或其他活动内容时，BitDefender 都会征求您的同意:

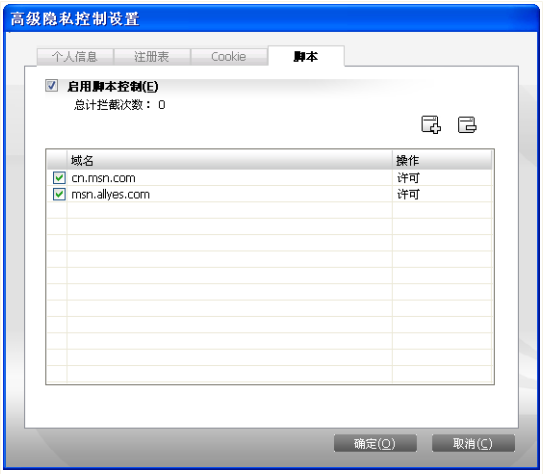
脚本警报

您可看到脚本资源的名称。

选中 记住我的选择 选项并点击 是 或 否 会在规则表中创建一条规则并应用它。下次当同一个网站试图执行活动内容时将不会再提示您。

每一个设置的规则，可以在 脚本 单元作进一步微调。 要访问这个单元，打开 高级隐私控制设置 窗口并单击 脚本 页签。

注意
要打开 高级隐私控制设置 窗口，在高级视图单击 隐私控制>状态 并单击 高级设置。



脚本控制

您可以在表格中看到已创建的规则列表。

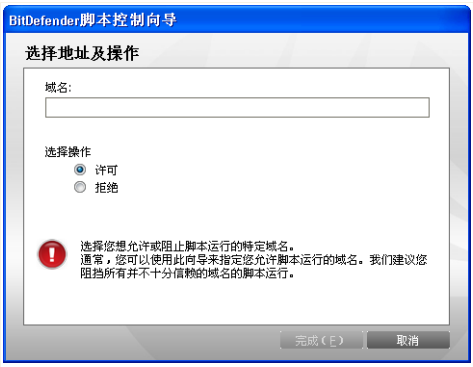
要删除一个规则，只要选择它并单击 删除 按钮。 要修改一个规则的参数，只要双击它并作预期的修改。 要暂时禁用一个规则而不删除它，清除相关的复选框。

这些规则可以自动输入(通过警报窗口)或手动(单击 添加 按钮并选择规则参数)。配置向导就会出现。

10.5.1. 配置向导

配置向导仅一个步骤。

步骤 1/1 – 选择地址和操作



选择地址及操作

您可以设定下述参数:

- 域名 – 输入要应用规则的域名。
- 操作 – 选择规则的操作。

操作	描述
允许	该域名上的脚本将被执行。
拒绝	该域名上的脚本将不会执行。

点击完成。

点击 确定 保存修改并关闭窗口。

10.6. 系统信息

BitDefender 可以让您从单一位置查看所有的系统设置和注册在 Windows 启动运行时的应用程序。这样，您可以监控系统的活动和安装的应用程序以及找出可能的系统感染。

要获取系统信息，请转到高级视图的 隐私控制>系统信息。

系统信息

列表包含所有在系统启动时自动加载的项目，以及有各个应用程序加载的项目。

根据选择的项目，有4个按钮可用:

●移除 – 删除选择的项目。 您必须单击 是 以确认您的选择。

注意

如果您不想在当前会话，被提示再次确认您的选择，单击 本次会话中不要再次询问我。

●恢复 – 将当前的文件关联恢复到默认值。 仅适用 文件关联 设置!

●转到 – 打开一个窗口，显示所选的项目（例如 注册表）。

●刷新 – 重新打开 系统信息 部分。

11. 用户控制

用户控制能阻止访问:

- 不良网页。
- 某些时段可以连接到互联网(例如网上培训的时间)。
- 含有某些关键词的网页和电子邮件。
- 应用程序，如游戏，聊天程序，文件共享程序或其他程序。

用户指南的 用户控制 单元包含以下议题:

- 用户控制状态
- 网页控制
- 应用程序控制
- 关键词过滤
- 网络限时器

11.1. 用户控制状态

要配置所选用户的用户控制，请转到高级视图的 用户控制>状态。

用户控制状态

您可以为每个 Windows 用户账号设置用户控制。 要启用一个指定用户账号的用户控制，从菜单中选择用户账号并选择相关的复选框。

11.1.1. 选择保护控制

要配置防护级别，必须首先选择想要应用设置的用户。 然后使用下列控制配置防护级别:

- 网页控制 – 根据您在 网页 单元设置的规则过滤网页导航。
- 应用程序控制 – 阻止访问您在 应用程序 单元指定的应用程序。
- 网络限时器 – 允许根据在 限时器 单元设置的时间表进行网页访问。
- 网页访问 – 阻止访问所有网站(不只是那些在 网页 单元的网页)。
- 关键词过滤 – 根据您设定的规则过滤网页和电子邮件，在 关键词 选项卡中。
- 启发式网页过滤 – 根据预建立的规则过滤网页访问。

注意

为了从用户控制模式下获得最大功效，您必须配置选定的控制。 要了解如何配置它们，请参阅本章的下列议题。

11.1.2. 配置启发式网页过滤

启发式网页过滤分析网页，并阻止那些匹配模式的潜在不良内容的网页。

要根据预先定义的规则集过滤网页访问，您必须指定一个安全级别。 沿着标尺拖曳滑块指定用户设置安全级别。

共有 3 个安全级别:

安全级别	描述
低	儿童 阻止含有对儿童可能有害内容的网页(色情、性、毒品、暴力等）。
中	青少年 阻止所有关于性、色情作品或成人内容的网页。
高	无论网页内容是什么，不限制访问所有网页。

点击 默认级别 设置滑块为默认级别。

11.2. 网页控制

网页控制 帮助您阻止访问有不良内容的网站。BitDefender 会提供一份要阻止的站点和网页的列表，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。

要配置网页访问，请转到高级视图的 用户控制>网页。

网页控制

要启用这个保护，请选中相应的 启用网页控制。

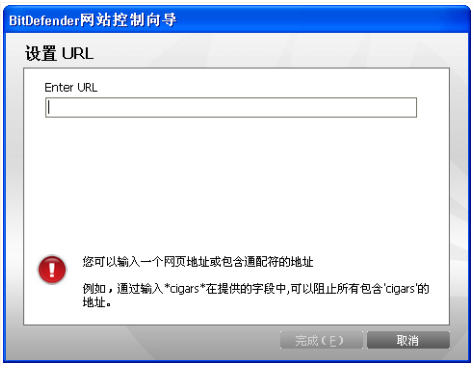
选择 允许访问这些网页/阻止访问这些网页，查看允许/阻止的网站列表。单击 例外... 访问补充列表的窗口。

规则必须手动输入。 首先，选择 允许访问这些网页/阻止访问这些网页 来允许/阻止访问您在向导中指定的网页站点。 然后，单击 添加... 按钮开启配置向导。

11.2.1. 配置向导

配置向导仅一个步骤。

步骤 1/1 - 指定网站



指定网站

输入将要应用规则的网页站点并单击 完成。

重要
语法:

- *.xxx.com - 这个规则的操作将应用到所有以 .xxx.com 作为结尾的网页站点;
- *porn* - 这个规则的操作将应用到包含 porn 的网页站点地址;
- www.*.com - 这个规则的操作将应用到所有以 com 作为后缀的网页站点;
- www.xxx.* - 这个规则的操作将应用到所有以 www.xxx. 为前缀的网页站点，而不论其后缀如何。

点击 应用 保存修改。

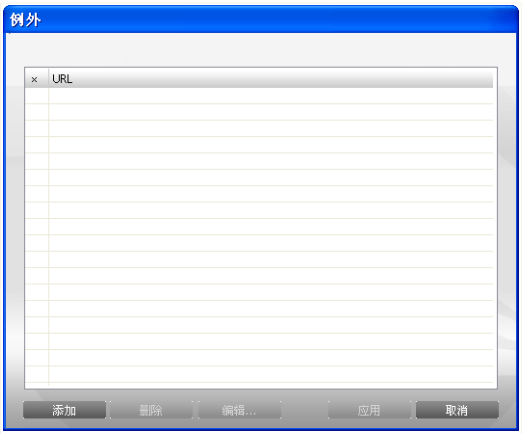
要删除一个规则，只要选择它并单击 删除 按钮。 要修改一个规则，选择它并单击 编辑... 按钮或双击它。 要暂时禁用一个规则而不删除它，清除相关的复选框。

11.2.2. 指定例外

有时您可能需要指定特定的例外规则。 例如，您设置一个规则来阻止网址包含关键词"killer"的站点(语法: *killer*)。 您也知道存在着所谓的网站killer-music 在那

里访问者可以在线听音乐。 要在前面创建的规则上制造一个例外，访问 例外 窗口定义一个例外规则。

单击 例外...。 将会出现下列窗口：



指定例外

单击 添加... 以指定例外。 配置向导 将出现。 完成向导来设置例外。

点击 应用 保存修改。

要删除一个规则，只要选择它并单击 删除。 要修改一个规则，选择它并单击 编辑... 或双击它。 要暂时禁用一个规则而不删除它，清除相应的复选框。

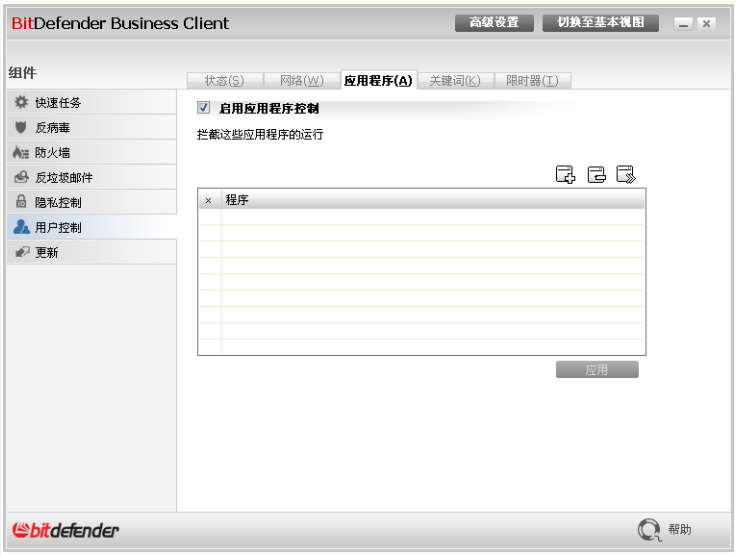
11.2.3. BitDefender 网页黑名单

BitDefender 提供包含不良内容或可能危险内容的网站的黑名单使用 BitDefender 提供的应阻止的网页清单。

11.3. 应用程序控制

应用程序控制 帮助您阻止任何应用程序运行。游戏，多媒体和即时通讯软件，以及其他类型的软件和恶意软件都会被阻止。用这样的方式阻止的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。

要配置应用程序控制，请转到高级视图的 用户控制>应用程序。



应用程序控制

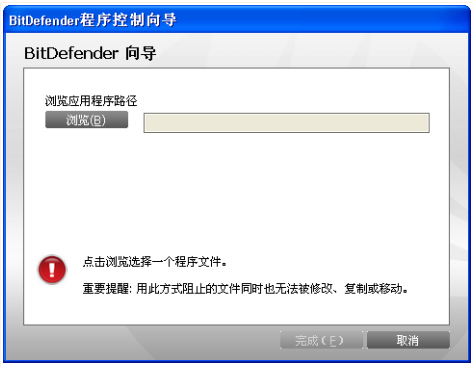
要启用这个保护，选择相应的复选框 启用应用程序控制。

这个规则必须手动输入。 单击 添加... 按钮启动配置向导。

11.3.1. 配置向导

配置向导仅一个步骤。

步骤 1/1 - 选择阻止的应用程序



选择阻止的应用程序

单击 浏览，选择需要阻止的应用程序并单击 完成。

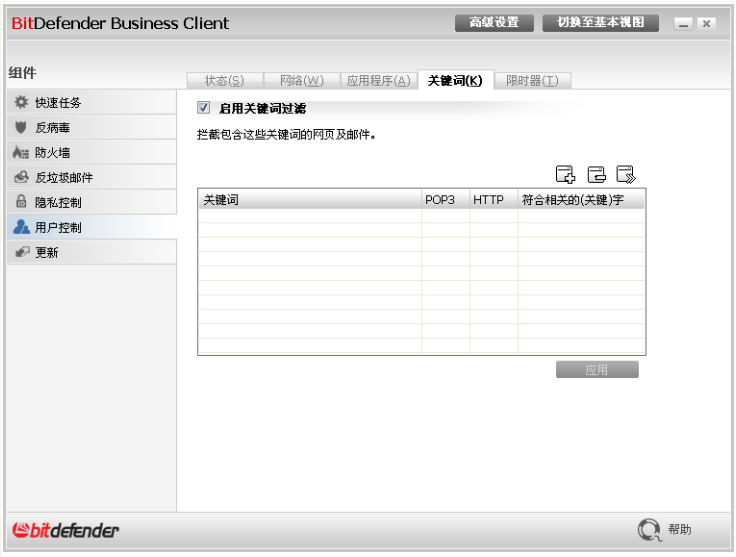
点击 应用 保存修改。

要删除一个规则，只要选择它并单击 删除 按钮。 要修改一个规则，选择它并单击 编辑... 按钮或双击它。 要暂时禁用一个规则而不删除它，清除相关的复选框。

11.4. 关键词过滤

关键词过滤 帮助您阻止访问包含了特定关键词的电子邮件信息或网页。 通过这种方式，您可以防止用户看到不恰当的词语或短语。

要配置关键词过滤，请转到高级视图的 用户控制>关键词。



关键词过滤

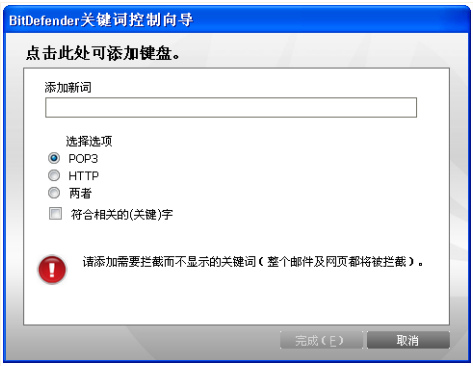
要启用这项保护，选择相应的复选框 关键词过滤。

这个规则必须手动输入。 单击 添加... 按钮启动配置向导。

11.4.1. 配置向导

配置向导包含 1 步操作过程。

步骤 1/1 – 输入关键词



输入关键词

您必须设置下列参数:

- 关键词 – 在编辑栏输入想要阻止的词语或短语。
- 协议 – 选择 BitDefender 扫描指定关键词的协议。

您可做以下选择:

选项	描述
POP3	含有关键词的电子邮件将被阻止。
HTTP	含有关键词的网页将被阻止。
两者	含有关键词的网页和邮件都将被阻止。

点击 应用 保存修改。

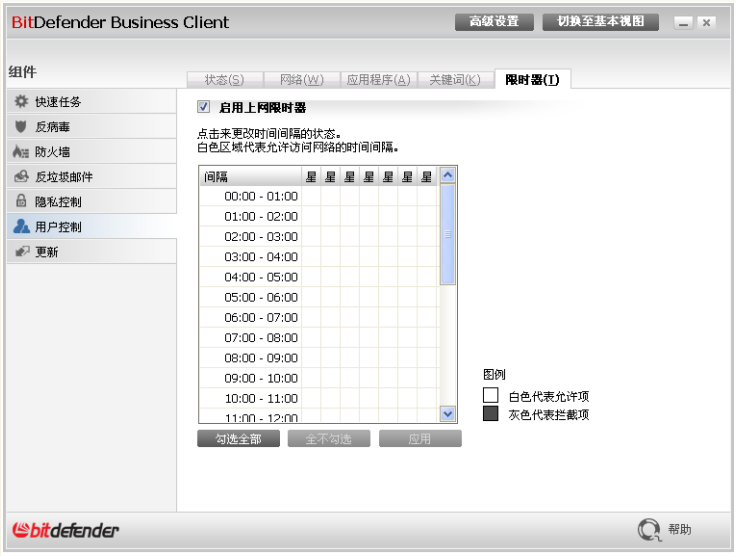
要删除一个规则，只要选择它并单击 删除 按钮。 要修改一个规则，选择它并单击 编辑... 按钮或双击它。 要暂时禁用一个规则而不删除它，清除相关的复选框。

11.5. 网页限时器

网页限时器 帮助您允许或阻止用户或程序在指定时段内的网页访问。

注意
BitDefender 将会不时更新，无论 网页限时器 设置如何。

要配置网页限时器，请转到高级视图 用户控制>限时器。



网页限时器

要启用这项保护，选择相应的复选框 启用网页限时器。

当所有网络连接全被阻止时，选择这个时段。 您可以单击个别的格子，或单击并拖动鼠标覆盖更多的时段。 同时，您可以单击 全时段禁止 来选择所有的格子阻止所有网页访问。 如果您单击 全时段允许，互联网连接将在任何时间被允许。

重要
灰色的格子代表这个时段禁止所有互联网连接访问。

点击 应用 保存修改。

12. 更新

更新可以分为两类：

- 病毒特征库更新 保持已知恶意软件程序数据库为最新。保护您的计算机和数据，免受最新的威胁。 病毒特征库更新还包括垃圾邮件特征更新，改善反垃圾邮件的保护。
- 产品文件更新 添加各种程序改进，包括新的特征和扫描技术。

如果您通过宽带或 DSL 连接到互联网，您可以配置 BitDefender 自动更新。 要配置自动更新，请转到 更新 页签并选择 更新已禁用 复选框。

注意
自动更新可以由您的网络安全管理员进行配置。

自动更新启用后，计算机开启时，BitDefender 会每小时检查更新。 如果发现了新升级包，可能会要求您确认进行升级，也可能自动进行升级，这取决于自动升级设置 里面的设置选项。

升级过程是逐步执行的，需要被更新的文件会被逐步替换，因此升级过程不会影响产品的正常运行，同时又可减少系统漏洞。

用户指南的 更新 章节包括以下内容：

- 自动更新
- 更新设置

12.1. 自动升级

要查看更新相关的信息或开始更新，在高级视图中请转到 更新>更新 。

自动升级

在这里，您可以看到最近检测时间和最近更新时间，以及最近检测更新执行信息(如果成功或错误发生)。此外，还有当前引擎版本信息和病毒库的数量显示。

通过点击 显示病毒名单，您可以查看 BitDefender 的病毒库。网页浏览器将创建并打开一个包含所有病毒特征的 HTML 文件。您可以通过这个病毒库检索指定病毒或者单击 BitDefender 病毒名单 转到 BitDefender 在线病毒库。

要配置自动更新，选择 更新已禁用 复选框。

重要
要想免受最新威胁的侵害，请保持启用 自动升级。

如果您在更新期间打开这个单元，就可以看到更新下载状态。

12.1.1. 进行升级

自动更新可以在任何时候进行，只要您单击 立即更新。 这种更新也称为 用户请求更新。

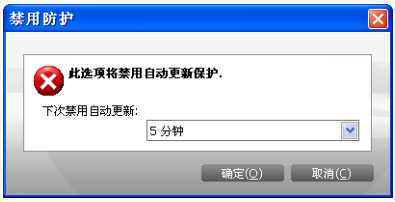
升级 模块会连接到 BitDefender 更新服务器并检查是否有可用更新，如果发现了可用更新，则会根据在 手动升级设置 里的选择，提示您确认升级或者直接自动进行升级。

重要
升级完成后，可能有必要重新启动计算机。建议立刻重新启动。

注意
如果您通过拨号方式连接到网络，建议您定期手动升级产品。

12.1.2. 禁用自动升级

如果您禁用自动升级，会出现一个警告窗口。



禁用自动升级

您必须从列表中选择您想禁用自动升级多长时间以确认您的操作，您可禁用自动升级 5 分钟、15 分钟、30 分钟、1 小时或直到下次系统重启。

警告
这是一个重大安全问题。我们建议您尽可能不要禁用自动升级。如果 BitDefender 不能定时升级，则无法保护您免受最新的威胁。

12.2. 更新设置

升级可通过本地网络、互联网进行，可直接连接或通过代理服务器连接。 默认情况下， BitDefender 每小时通过互联网检查更新，并在不通知您的情况下安装新的升级包。

要配置升级设置及管理代理服务器，请前往高级视图的 升级>设置。

更新设置

升级设置选项分为四个功能组（升级服务器设置，自动升级设置，手动升级设置 和高级设置）。 以下将分别说明每个功能组。

12.2.1. 设置更新服务器

要设置升级服务器，请使用 升级服务器设置 部分的选项。 要拥有更快速可靠的升级，您可以指定两个升级服务器：一个 首选升级服务器 和一个 备选升级服务器。默认情况下，两个升级服务器是相同的：http://upgrade.bitdefender.com。 这是一个通用网址，从您最近的区域存储 BitDefender 病毒库的服务器上自动下载。 如果您看到不同的更新位置，则程序已配置为从本地更新服务器更新。

您将需要配置这些设置在下列情况下：

- 在本地更新服务器上有可用的 BitDefender Business Client 更新文件。 在这种情况下，使用以下任意的语法规则更改初始更新位置：
  - http://update_server_ip:port
  - http://update_server_name:port

默认端口是 7074。

您可以从网络管理员处获取这些设置。

注意
建议替代更新位置保持不变，当本地更新服务器不可用时作为一项备用计划。

- 计算机通过代理服务器连接到 Internet。 在这种情况下，选择初始更新位置相对应的使用代理复选框，然后单击管理代理并配置代理设置。 欲了解更多信息，请参 阅 “管理代理服务器” （第 170 页）

12.2.2. 设置自动升级

要向让 BitDefender 自动进行升级，请设置 自动升级设置 中的选项。

您可以在 时间间隔 编辑栏指定两次更新检测的时间间隔。默认情况下，更新时间间隔为 1 小时。

要指定自动升级过程如何进行，请选择下述选项之一：

- 静默升级 – BitDefender 将自动下载和安装更新。
- 下载升级包之前提示 – 每次发现可用升级包时，会提示您下载。
- 安装升级包之前提示 – 每次下载一个升级包之后，系统会在安装前提示您。

12.2.3. 手动升级设置

指定手动升级（用户请求的升级）如何执行，您可在 手动升级设置 组中指定一个选项：

- 静默升级 – 手动升级将自动在后台进行，无需用户干预。
- 下载升级包之前提示 – 每次发现可用升级包时，会提示您下载。

12.2.4. 设置高级设置选项

为防止 BitDefender 升级过程打扰您的工作，您可在 高级设置 组中设置相关的选项：

- 等待重启而不提示 – 如果升级后需要重启，产品会继续用旧文件运行，直到系统重启。用户不会被提示进行重启，用户的工作不会被打扰。

●您能从菜单中指定选择将下载和安装哪些合适的更新:
- 更新产品文件和病毒特征库
- 只更新产品文件
- 只更新病毒特征库

病毒特征库更新使 BitDefender 检测并阻止 BitDefender 实验室识别的最新恶意软件和垃圾邮件。这是为什么保持最新病毒特征库的重要原因。

病毒特征库更新不更新扫描引擎，但是这不会对扫描过程产生任何问题。

注意

该设置主要是由网络安全管理员根据企业内部安全策略进行使用。 例如，病毒特征库将每小时自动更新，当产品文件是手动更新的，每星期一次。

12.2.5. 管理代理服务器

如果您的公司使用代理服务器连接到互联网，您必须要指定代理服务器设置，以便 BitDefender 进行更新。否则，它将使用管理员安装产品时设置的代理设置或当前用户的默认浏览器的代理设置(如果有的话)。

要修改代理服务器设置，请点击 管理代理服务器，会出现 代理服务器设置 窗口。

代理服务器管理器

代理服务器设置分为三组:

- 管理员的代理服务器设置（检测于安装时） – 在安装时检测到的系统管理员的代理服务器设置，只有在您以系统管理员账户登录时才可设置。如果代理服务器需要用户名和密码，您必须在对应的编辑框中输入它们。
- 当前用户的代理服务器设置（来自默认浏览器） – 从默认浏览器中获取的当前用户的代理服务器设置。如果代理服务器需要用户名和密码，您必须在对应的编辑框中指定。

> **注意**
> 支持的浏览器为 Internet Explorer、Mozilla Firefox 和 Opera。如果您使用其他浏览器，BitDefender 将无法获取当前用户的代理服务器设置。

- 个人代理设置 – 代理服务器设置，如果您以管理员身份登录就可以配置。 需要指定如下设置选项:
  - 地址 – 输入代理服务器IP地址。
  - 端口 – 输入代理服务器端口。

- 用户名 – 输入代理服务器用户名。
- 密码 – 输入以上指定用户名的密码。

在试图连接到互联网时，BitDefender 会尝试每一组代理服务器设置，直到连接成功。

首先会尝试您自己的代理服务器设置，如果连接不成功，则会尝试安装时检测的管理员代理服务器设置，如果还不能成功，则会尝试从默认浏览器中检测到的当前用户代理服务器设置。

点击 确定 保存修改并关闭窗口。

点击 应用 保存更改或点击 默认 加载默认设置。

13. 备份设置

如果您需要执行更复杂的备份和恢复操作，您可以使用功能齐全的 BitDefender 备份解决方案。 BitDefender 备份提供:

- 各种各样的备份选项，如压缩、加密、过滤文件备份或设置备份速度。
- 恢复文件的完善控制(例如，您可以在某一特定时间点恢复您的数据备份)。
- 先进的调度功能(例如，您可以选择当计算机处于闲置状态时，启动备份作业)。
- 日志浏览器，它可以帮助您跟踪备份，恢复您执行的操作和排除故障。

在这一单元，为您提供详细资料，图形用户界面和 BitDefender 备份功能。

重要

BitDefender 备份只有在超级用户模式下可用。 如果您是一个受限用户但需要更多的备份选项，请联系您的网络安全管理员。

要打开 BitDefender 备份，请执行下列操作之一:

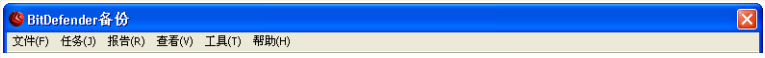
- 单击基本视图上的 备份设置。
- 在高级视图，请转到 快速任务 并运行备份设置任务，通过点击相应的 立即运行 按钮。

BitDefender 备份工具

有两种方法可以用来建立和执行备份操作。您可以进入上层 菜单栏 或点击某个页签的 导航工具条。

13.1. 菜单栏

有六个菜单选项，您可以使用并执行 BitDefender 备份解决方案提供的所有功能。



菜单栏

文件

- 创建新任务：显示一个对话框，以创建一个新备份任务或其他任务。
- 打开备份设置：出现一个对话框，以便打开用于恢复的备份集或目录集。

●退出：允许退出 Bitdefender 备份单元。

任务

●备份：执行选中的备份任务。如果选择一个以上任务，则执行所有选定任务。
●恢复文件： 恢复选择的任务。如果有超过一个的选择任务，执行所有选择的任务。
●恢复时间点的数据： 恢复选择的任务到某一个时间点。如果有超过一个的选择任务，它将执行所有选择的任务。
●任务计划：创建或修改任务计划。
●删除任务计划：删除选定的任务计划。
●删除：删除选定的任务。如果选中了多个任务，则删除所有选中任务。
●删除所有：删除任务管理器中的所有任务。
●浏览目的地：允许查看备份数据所选择的任务目的地。
●修改选项：修改选定的任务选项。
●属性：允许修改选定任务的属性，包括任务资料来源、名称、目的地等。

报告

●查看报告： 如果选择的任务有安全设置，这个选项允许查看的任务报告的内容。
●另存为：保存选定的报告内容到指定的文件。
●打印：打印选中的报告内容。
●清除所有：清除选定的任务报告内容。
●刷新：刷新选定的任务报告内容。

查看

●新手上路：如果开始窗口没有显示，该选项可以打开它。
●任务管理器：如果任务管理器窗口没有显示，该选项可以打开它。
●日志查看器：如果日志查看窗口没有显示，该选项可以打开它。
●工具箱：如果这个窗口没有显示，该选项可以打开它。
●显示菜单栏：隐藏菜单栏。需要显示按 Alt键。
●显示网格线：显示或隐藏网格线。它适用于日志查看器和任务管理器窗口。

工具

●备份向导：开启备份向导。
●恢复向导：开启恢复向导。
●刻录：开启刻录 CD/DVD/ISO 刻录工具或一个刻录管理工具。
  - CD/DVD 刻录
  - ISO 文件刻录
  - 查看刻录器信息
●导出所有任务：导出所有创建的任务到指定的文件。
●导入任务：从一个 .JOB 文件，一个 .TXT 文件，或一个 .XML 文件导入任务。

- ●导出日志: 导出日志到一个 .TXT 文件或一个 .XML 文件。
  - 到一个 TXT 文件
  - 到一个 XML 文件
- ●导入日志: 从一个 .TXT 文件或一个 .XML 文件导入日志。
  - 从一个 TXT 文件
  - 从一个 XML 文件
- ●选项: 修改全局备份选项。
  - 常规
  - 报告&日志
  - 任务计划

帮助

- ●帮助主题: 显示帮助主题。
- ●搜索: 允许输入或选择关键词搜索帮助主题。
- ●在线搜索: 允许在互联网上搜索帮助主题。
- ●BitDefender 网站: 允许访问 BitDefender 的互联网主页, 浏览 BitDefender 新闻和在线支持。
- ●支持信息: 显示可以使用获得支持的联系信息。
- ●关于 Bitdefender 备份: 显示版权, 版本与 BitDefender 备份相关的信息。

13.2. 导航工具条

导航工具条, 显示在主窗口的上方和在 菜单栏 的下方, 能够访问四个单元:

- ●新手上路
- ●任务管理器
- ●日志查看器
- ●工具箱

13.2.1. 新手上路

开始 帮助您轻松备份电子邮件, 聊天记录和数据。

新手上路

您可以进入到 开始 通过下列步骤:

- 在 导航工具条 点击 新手上路。
- 在 菜单栏 中点击 查看 并选择 新手上路。
- 使用快捷键 CTRL+A1t+S.

要在同一个任务中备份您的重要文档、照片、电子邮件和聊天记录，点击 备份我的数据 按钮，并按照后续 3 个步骤操作。

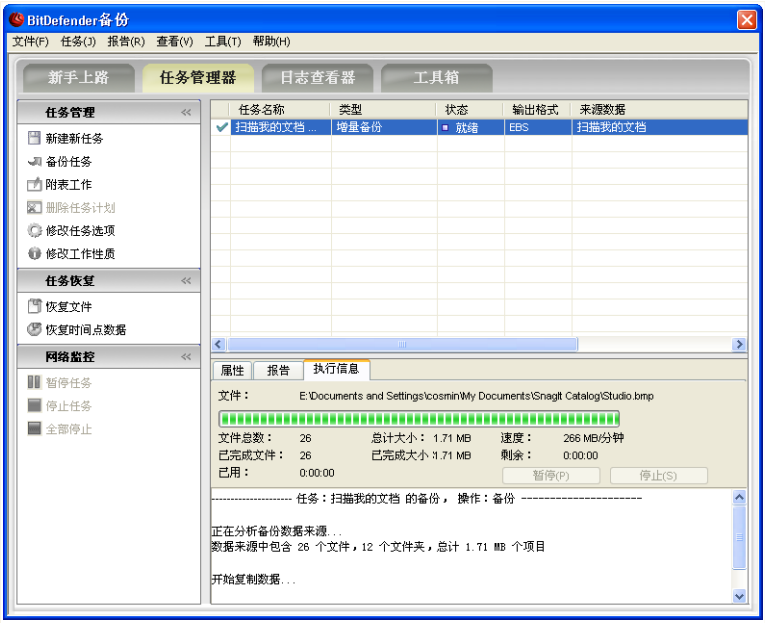
要只备份您的电子邮件，单击 备份我的电子邮件 按钮，并按照后续 3 个步骤操作。

要备份您的聊天记录，点击 备份我的聊天记录 按钮，并按照后续 3 个步骤操作。

注意
这三个步骤也在 创建新任务 进行了描述。

13.2.2. 任务管理器

任务管理器 是用来查看和管理备份任务，查看任务属性和任务报告，以及监督任务执行速度。任务管理器 可以检查任务属性和当前状态，修改任务设置，以及执行任务备份或恢复。



任务管理器

您可以通过下列步骤进入 任务管理器:

- 在 导航工具条 点击 任务管理器。
- 在 菜单栏 中点击 查看，并选择 任务管理器。
- 使用快捷键 CTRL+A1t+M.

在左侧，您会看到一个快速运行连接的列表，具体情况如下:

任务管理器
- 创建任务

- ●备份任务
- ●计划任务
- ●删除任务计划表
- ●修改任务方案
- ●修改任务属性

任务恢复

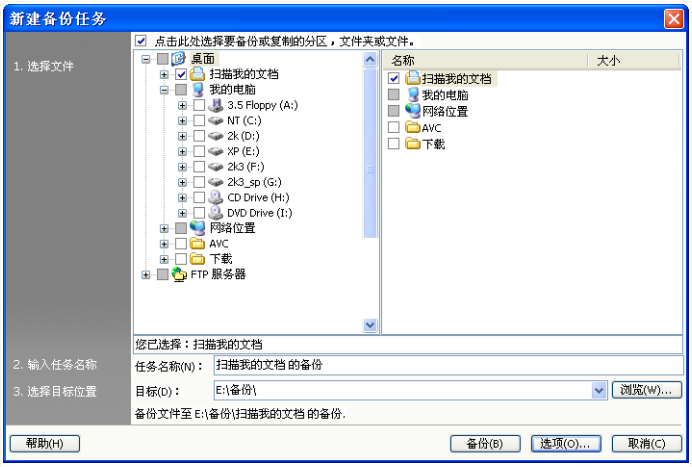
- ●恢复文件
- ●恢复时间点数据

工作控制

- ●暂停任务
- ●停止工作
- ●全部停止

新建新任务

要在同一任务中备份您的重要文档、照片、电子邮件和聊天记录，点击 创建新任务 按钮，并按照后续三个步骤操作。



新建新任务

1. 点击复选框，选择驱动盘、目录或文件进行备份。

当您在左侧窗口中选择一个项目，其内容就会显示在右侧窗口，以便完善您的选择。

2. 为您的备份任务输入名称或使用默认任务名称。

   默认的任务名是在文件或目录被选择备份时自动生成的，但是它是可以被修改的。

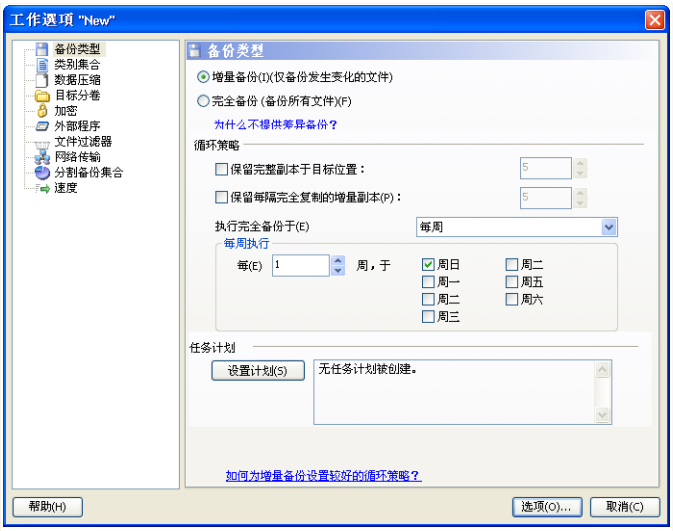
3. 点击 浏览，选择保存您的备份任务位置。

注意

不要忘了点击 备份 开始任务或点击 取消 来取消任务。
要完善您的设置，点击 选项。

备份选项对话框

在选项 对话框有几个子选项。



备份选项对话框

备份类型

BitDefender 备份支持两种备份类型。

●完整备份　　备份选定的所有数据源到指定的目标位置。执行完整备份时，BitDefender 备份不只备份更改的数据，而是整个数据源。

●增量备份: 第一次执行时，增量备份和完整备份一样，需要完全备份数据源到指定的目标文件上的备份集。之后，它只是备份新创建或修改过的文件。增量备份执行一次，就生成一个备份目录集。

整量备份和完整备份也可以结合成为一个 轮换备份。例如，您可以设置一个任务的增量备份，同时制定一个每周一次的完整备份，假设是周日。应该这样操作: 从下拉菜单中选择每周，每周区域内选择 1并选择周日。这样每周日进行完整备份，将取代所有之前的备份并且会成为新的增量备份的基础。

目录集

它是用来为每个备份制作文档信息的目录，它是增量备份和恢复进程的基础。目录集*.ecs包含一系列的目录，这些目录在备份集里代表所有文件索引目录。这种目录包括数据备份时间、备份目录、文件名及属性。数据可以从目录集进行恢复。

一个目录集文件名由任务目的地自动生成。要修改任务的目录集，按照下列步骤操作:

1. 点击 目录集.
2. 在相应的编辑栏输入一个文件名称。
3. 单击 浏览 选择目录，以保存目录集文件。
4. 点击 确定。

数据压缩

当执行备份到保存的空间时，BitDefender 备份允许压缩和保存数据到备份集。它支持快速压缩、标准压缩、高强度压缩。例如，要启动标准压缩、在中等压缩率和速度，按照下列步骤进行:

1. 点击 数据压缩。
2. 点击 标准压缩.
3. 点击 确定。

目标分卷

BitDefender 备份允许分发备份集到不同的目标地址。这样，即使某一个目标位置没有足够的可用空间，数据备份仍可继续执行。

使用下列的一个方法，您可以添加一个或多个目标位置继续备份、修改或移除他们:

1. 点击 目标分卷。
2. 单击 添加 选择一个新的目的地，以保存备份数据。
3. 单击 编辑 修改所选备份目的地。
4. 单击 删除 以删除选择的备份的目的地。
5. 点击 全部删除 以删除所有备份目的地。
6. 点击 确定。

加密

bitdefender 备份在保存到备份集之前，通过加密保证备份的数据安全。一个任务的安全设置包括密码保护。

要在备份前对数据进行加密，请按照下列步骤操作:

1. 点击 加密。
2. 从下拉菜单中选择加密类型。
3. 在相应的编辑栏输入您的密码。
4. 在相应的编辑栏重输密码。
5. 点击 确定。

外部程序

这个任务可以在备份前后运行其它命令，并且这些命令可以是 .exe，.com 或 .bat，或某一事件的特定类型，如"备份完成后关闭计算机"。

要在备份开始时执行命令，按照下列步骤操作:

1. 点击 外部程序
2. 选择 在任务执行之前 选项。
3. 单击 浏览，选择执行的命令文件。
4. 点击 确定。

要在备份完毕后执行命令，按照下列步骤操作:

1. 点击 外部程序
2. 选择 在任务执行之后 选项。
3. 点击 浏览 选择执行的命令文件。
4. 或者点击 关闭计算机，当备份完成后。
5. 或者点击 重新启动计算机，当备份完成后。
6. 或者点击 登出当前用户，当备份完成后。
7. 点击 确定。

注意

如果您想要配置在备份失败的情况下仍然生效，选中复选框 即使任务执行失败，仍运行外部程序。

文件过滤

BitDefender 备份提供了强大的过滤功能，以排除或包含指定的文件、文件类型或目录，以节省储存空间，并提高备份速度。

指定文件类型，可以过滤通过以下步骤:

1. 点击 文件过滤。
2. 单击 过滤类型。

3. 弹出选择文件类型对话框，通过选择 仅包含选定的文件类型 或 排除选定的文件类型 选项。
4. 如有必要，自定义类型编辑栏键入另一个文件类型但要确保使用.abc 格式。当您输入超过一个以上的自定义类型时，使用 ，(逗号)作为分隔符。在相应的编辑栏添加简短描述。
5. 点击 确定。

通过以下步骤，指定可以被过滤的文件：

1. 点击 文件过滤。
2. 单击 过滤文件。
3. 在弹出选择文件类型对话框中，选择仅包含规则指定的文件或排除规则指定的文件选项。
4. 单击 浏览并选择所需的文件。文件位置的路径将会自动添加到 应用到下列目录 编辑栏。 要包含或配出文件，而不论其位置，单击 应用到所有目录。
5. 点击 确定。

通过以下步骤过滤指定的目录：

1. 点击 文件过滤。
2. 单击 过滤目录.
3. 在弹出式对话框排除或包含指定的目录，通过选中 只包含规则指定的目录 或 排除规则指定的目录 选项。
4. 单击 浏览 并选择目录。 这个目录位置路径将会自动添加到 应用到下列目录 编辑栏。 要包含或排除目录，而不论其位置，单击 应用到所有目录。
5. 点击 确定。

过滤器可以通过以下步骤进行修改：

1. 点击 文件过滤。
2. 点击您希望修改的过滤器，然后点击 编辑。
3. 在对话框修改您的选项。
4. 点击 确定。

过滤器可以删除通过以下步骤：

1. 点击 文件过滤。
2. 点击您想删除的过滤器，并单击 删除。
3. 或者直接点击 删除所有 删除所有过滤器。
4. 点击 确定。

网络传输

BitDefender 备份允许备份和彻底恢复共享在工作组网络上的数据。如果没有网络连接，它有时将再次尝试备份数据。要明确重新尝试备份的频率与次数，请遵循这些步骤。

1. 点击 网络传输.

2. 点击 因为网络断开而导致读取网络文件失败时，请尝试重新连接。
3. 输入您想重新数据备份的频率(秒)。
4. 输入多少次的备份尝试。
5. 点击 确定。

注意

为了避免被网络错误的信息所覆盖，点击 当网络不可用时，不生成错误报告。

分割备份集.

生成的备份集可以被分割为几个备份集，使备份可正常执行，即时目标位置或文件系统有限。Bitdefender 备份提供了两种分割方法：自动分割和文件大小分割。

备份任务的分割设置可作如下修改:

1. 点击 分割备份集.
2. 选择 按目标位置空间自动分割。
3. 或选择 指定分割大小 并从下拉菜单中选择理想的尺寸。
4. 点击 确定。

速度

BitDefender 备份支持三种速度。速度越快，中央处理器(CPU)被占用的资源越多。

备份速度可指定由以下这些步骤。

1. 点击 速度.
2. 选择 快速,中速或慢速.
3. 点击 确定。

数据验证

为了确保您的备份数据始终安全，请遵循这些步骤。

1. 点击 数据核查。
2. 点击 备份过程中核查数据.
3. 点击 确定。

备份任务

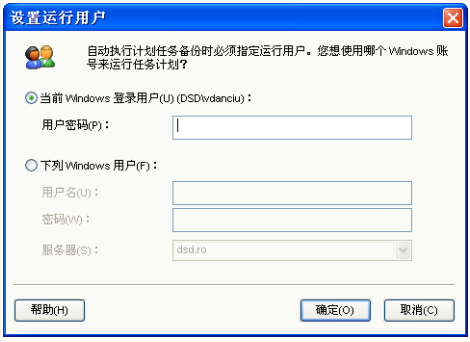
一旦任务被建立，备份会被自动执行。但是，您仍然可以进入 任务管理器 通过选择建立的任务来执行备份并在菜单中点击 备份任务。

为了在恢复文件时得到备份细节，您必须在弹出的窗口键入一个简短的说明。单击 取消 不理会弹出窗口或 确定 继续。通过点击 取消备份 按钮，备份任务也可以被取消。

注意
在窗口的状态条上可以看到 属性，报告 和任务 执行信息 的详细信息。

附表工作

这里，您可以把备份工作放在在方便的时候。您可排定工作，每天，每周，每月或在任何特定时间(例如，在系统启动时)。 计划任务 是自动备份的基础。



附表工作

如果您的计算机是域网络成员，需要补充一系列额外的步骤到任务计划表中。

1. 选择任务并单击 计划任务。
2. 运行的用户 对话框就会出现。如果您是域用户，请输入域密码。
3. 否则，选择以下列 Windows 用户来运行。
4. 输入用户名称，密码和域名。
5. 点击 确定。

一旦您设定了运行的用户，BitDefender 备份将显示 计划 对话框，让您可以设置一个方便的时间来执行任务。

这里，您可以指定任务运行的频率：每日，每周，每月，一次，在系统启动，在登录，当计算机处于闲置状态。如果任务被排定每日，每周，每月或只有一次，您还可以指定开始时间。您还可以选择每隔多久预定任务被运行（表示为天数或周数，一个月的某一天或日期） 。另一种可能设置是任务开始后的闲置时间长度（分钟）。

我们也可以为同一个任务配置多个时间表，通过点击 显示多个时间表。 通过点击高级，您可以设置额外的调度选项。例如，您可以定义任务的开始和结束的日期。

要进一步完善时间表，点击 设置 页签。 选项.三个子选项可供选择。

●计划任务已完成
- 删除不需要再次运行的计划任务。

  这项工作只对运行一次的计划任务有用。
- 停止工作，如果运行过程中：

  指定任务开始后多长时间内应当停止。

●空闲时间
- 只在计算机已经被闲置了至少一段时间的情况下开始任务：

  指定鼠标或键盘未使用有多长时间（分钟）在的情况下，计划任务才开始。
- 如果计算机没有被闲置那么久，则重新计时：

  指定有多长（分钟），任务会保持检查，看看计算机是否在闲置状态。
- 停止工作，如果计算机不再被闲置。

  指定是否任务应该停止，如果您开始使用计算机，而任务还正运行中。

●电源管理
- 如果计算机上使用电池运行，则不开始执行任务。

  指定您的计算机在电池运行模式下是否阻止这项工作。选择此复选框，可以延长电池使用寿命。
- 停止工作，如果电池模式开始。

  指定是否任务应该停止，您的计算机开始运行在电池模式下。
- 唤醒计算机以运行此任务。

  指定计算机是否运行时间表上的任务，即便是在睡眠模式下。

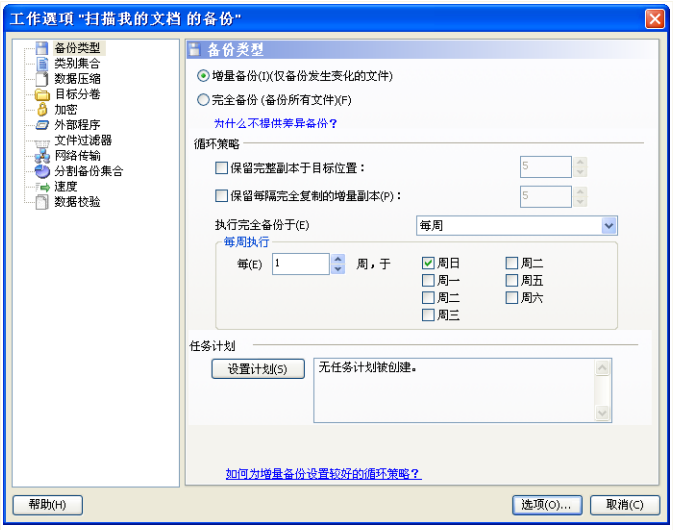
删除任务计划

要删除一个任务计划，选择它并单击 删除任务计划，在 任务管理 单元。

如果这项任务是无计划的，删除任务计划 将显示为灰色，也就是表示不能使用。

修改任务选项

要修改任务选项，选择任务并单击 修改任务选项，在 任务管理 单元。

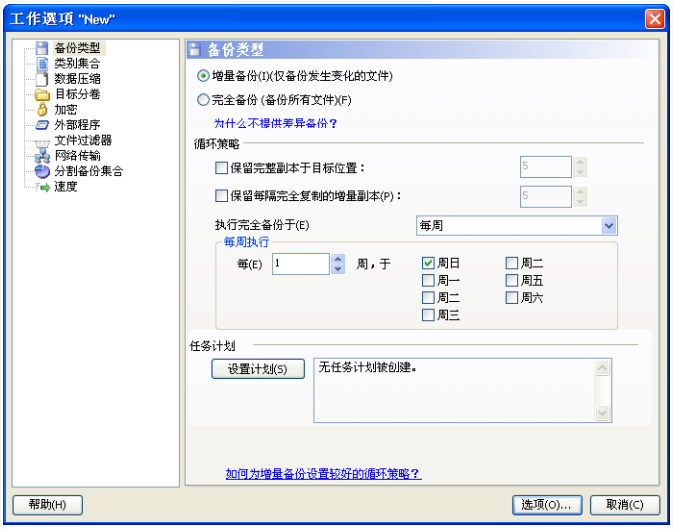


修改任务选项

选定的任务可以是一个备份任务，也可以是一个刻录任务。让我们将他们一次一个的来。

备份选项对话框

在选项 对话框有几个子选项。



备份选项对话框

备份类型

BitDefender 备份支持两种备份类型。

- 完整备份　　备份选定的所有数据源到指定的目标位置。执行完整备份时，BitDefender 备份不只备份更改的数据，而是整个数据源。
- 增量备份: 第一次执行时，增量备份和完整备份一样，需要完全备份数据源到指定的目标文件上的备份集。之后，它只是备份新创建或修改过的文件。增量备份执行一次，就生成一个备份目录集。

整量备份和完整备份也可以结合成为一个 轮换备份。例如，您可以设置一个任务的增量备份，同时制定一个每周一次的完整备份，假设是周日。应该这样操作: 从下拉菜单中选择每周，每周区域内选择 1并选择周日。这样每周日进行完整备份，将取代所有之前的备份并且会成为新的增量备份的基础。

目录集

它是用来为每个备份制作文档信息的目录，它是增量备份和恢复进程的基础。目录集*.ecs包含一系列的目录，这些目录在备份集里代表所有文件索引目录。这种目录包括数据备份时间、备份目录、文件名及属性。数据可以从目录集进行恢复。

一个目录集文件名由任务目的地自动生成。要修改任务的目录集，按照下列步骤操作:

1. 点击 目录集.
2. 在相应的编辑栏输入一个文件名称。
3. 单击 浏览 选择目录，以保存目录集文件。
4. 点击 确定。

数据压缩

当执行备份到保存的空间时，BitDefender 备份允许压缩和保存数据到备份集。它支持快速压缩、标准压缩、高强度压缩。例如，要启动标准压缩、在中等压缩率和速度，按照下列步骤进行:

1. 点击 数据压缩。
2. 点击 标准压缩.
3. 点击 确定。

目标分卷

BitDefender 备份允许分发备份集到不同的目标地址。这样，即使某一个目标位置没有足够的可用空间，数据备份仍可继续执行。

使用下列的一个方法，您可以添加一个或多个目标位置继续备份、修改或移除他们:

1. 点击 目标分卷。
2. 单击 添加 选择一个新的目的地，以保存备份数据。
3. 单击 编辑 修改所选备份目的地。
4. 单击 删除 以删除选择的备份的目的地。
5. 点击 全部删除 以删除所有备份目的地。
6. 点击 确定。

加密

bitdefender 备份在保存到备份集之前，通过加密保证备份的数据安全。一个任务的安全设置包括密码保护。

要在备份前对数据进行加密，请按照下列步骤操作:

1. 点击 加密。
2. 从下拉菜单中选择加密类型。
3. 在相应的编辑栏输入您的密码。
4. 在相应的编辑栏重输密码。
5. 点击 确定。

外部程序

这个任务可以在备份前后运行其它命令，并且这些命令可以是 .exe，.com 或 .bat，或某一事件的特定类型，如"备份完成后关闭计算机"。

要在备份开始时执行命令，按照下列步骤操作：

1. 点击 外部程序
2. 选择 在任务执行之前 选项。
3. 单击 浏览，选择执行的命令文件。
4. 点击 确定。

要在备份完毕后执行命令，按照下列步骤操作：

1. 点击 外部程序
2. 选择 在任务执行之后 选项。
3. 点击 浏览 选择执行的命令文件。
4. 或者点击 关闭计算机，当备份完成后。
5. 或者点击 重新启动计算机，当备份完成后。
6. 或者点击 登出当前用户，当备份完成后。
7. 点击 确定。

注意

如果您想要配置在备份失败的情况下仍然生效，选中复选框 即使任务执行失败，仍运行外部程序。

文件过滤

BitDefender 备份提供了强大的过滤功能，以排除或包含指定的文件、文件类型或目录，以节省储存空间，并提高备份速度。

指定文件类型，可以过滤通过以下步骤：

1. 点击 文件过滤。
2. 单击 过滤类型。
3. 弹出选择文件类型对话框，通过选择 仅包含选定的文件类型 或 排除选定的文件类型 选项。
4. 如有必要，自定义类型编辑栏键入另一个文件类型但要确保使用.abc 格式。当您输入超过一个以上的自定义类型时，使用 ，(逗号)作为分隔符。在相应的编辑栏添加简短描述。
5. 点击 确定。

通过以下步骤，指定可以被过滤的文件：

1. 点击 文件过滤。
2. 单击 过滤文件。
3. 在弹出选择文件类型对话框中，选择仅包含规则指定的文件或排除规则指定的文件选项。
4. 单击 浏览并选择所需的文件。文件位置的路径将会自动添加到 应用到下列目录 编辑栏。 要包含或配出文件，而不论其位置，单击 应用到所有目录。
5. 点击 确定。

通过以下步骤过滤指定的目录:

1. 点击 文件过滤。
2. 单击 过滤目录.
3. 在弹出式对话框排除或包含指定的目录，通过选中 只包含规则指定的目录或 排除规则指定的目录 选项。
4. 单击 浏览 并选择目录。 这个目录位置路径将会自动添加到 应用到下列目录 编辑栏。 要包含或排除目录，而不论其位置，单击 应用到所有目录。
5. 点击 确定。

过滤器可以通过以下步骤进行修改:

1. 点击 文件过滤。
2. 点击您希望修改的过滤器，然后点击 编辑。
3. 在对话框修改您的选项。
4. 点击 确定。

过滤器可以删除通过以下步骤:

1. 点击 文件过滤。
2. 点击您想删除的过滤器，并单击 删除。
3. 或者直接点击 删除所有 删除所有过滤器。
4. 点击 确定。

网络传输

BitDefender 备份允许备份和彻底恢复共享在工作组网络上的数据。如果没有网络连接，它有时将再次尝试备份数据。要明确重新尝试备份的频率与次数，请遵循这些步骤。

1. 点击 网络传输.
2. 点击 因为网络断开而导致读取网络文件失败时，请尝试重新连接。
3. 输入您想重新数据备份的频率(秒)。
4. 输入多少次的备份尝试。
5. 点击 确定。

注意

为了避免被网络错误的信息所覆盖，点击 当网络不可用时，不生成错误报告。

分割备份集.

生成的备份集可以被分割为几个备份集，使备份可正常执行，即时目标位置或文件系统有限。Bitdefender 备份提供了两种分割方法: 自动分割和文件大小分割。

备份任务的分割设置可作如下修改:

1. 点击 分割备份集.

2. 选择 按目标位置空间自动分割。
3. 或选择 指定分割大小 并从下拉菜单中选择理想的尺寸。
4. 点击 确定。

速度

BitDefender 备份支持三种速度。速度越快，中央处理器(CPU)被占用的资源越多。

备份速度可指定由以下这些步骤。

1. 点击 速度.
2. 选择 快速,中速或慢速.
3. 点击 确定。

数据验证

为了确保您的备份数据始终安全，请遵循这些步骤。

1. 点击 数据核查。
2. 点击 备份过程中核查数据.
3. 点击 确定。

修改刻录任务选项

在刻录任务对话框，有几个子选项可用。

刻录

这里您可以设置磁盘在被刻录后被弹出，完成（如果您打算与他人共用）或使用 Joliet 文件系统书写（减少文件名限制）。

如果您想制定任务时间表，点击 设定计划表。

这里，您可以把备份工作放在在方便的时候。您可排定工作，每天，每周，每月或在任何特定时间(例如，在系统启动时)。 计划任务 是自动备份的基础。

如果您的计算机是域网络成员，需要补充一系列额外的步骤到任务计划表中。

1. 选择任务并单击 计划任务。
2. 运行的用户 对话框就会出现。如果您是域用户，请输入域密码。
3. 否则，选择以下列 Windows 用户来运行。
4. 输入用户名称，密码和域名。
5. 点击 确定。

一旦您设定了运行的用户，BitDefender 备份将显示 计划 对话框，让您可以设置一个方便的时间来执行任务。

这里，您可以指定任务运行的频率：每日，每周，每月，一次，在系统启动，在登录，当计算机处于闲置状态。如果任务被排定每日，每周，每月或只有一

次，您还可以指定开始时间。您还可以选择每隔多久预定任务被运行（表示为天数或周数，一个月的某一天或日期）。另一种可能设置是任务开始后的闲置时间长度（分钟）。

我们也可以为同一个任务配置多个时间表，通过点击 显示多个时间表。 通过点击 高级，您可以设置额外的调度选项。例如，您可以定义任务的开始和结束的日期。

要进一步完善时间表，点击 设置 页签。 选项.三个子选项可供选择。

●计划任务已完成

- 删除不需要再次运行的计划任务。

  这项工作只对运行一次的计划任务有用。
- 停止工作，如果运行过程中：

  指定任务开始后多长时间内应当停止。

●空闲时间

- 只在计算机已经被闲置了至少一段时间的情况下开始任务：

  指定鼠标或键盘未使用有多长时间（分钟）在的情况下，计划任务才开始。
- 如果计算机没有被闲置那么久，则重新计时：

  指定有多长（分钟），任务会保持检查，看看计算机是否在闲置状态。
- 停止工作，如果计算机不再被闲置。

  指定是否任务应该停止，如果您开始使用计算机，而任务还正运行中。

●电源管理

- 如果计算机上使用电池运行，则不开始执行任务。

  指定您的计算机在电池运行模式下是否阻止这项工作。选择此复选框，可以延长电池使用寿命。
- 停止工作，如果电池模式开始。

  指定是否任务应该停止，您的计算机开始运行在电池模式下。
- 唤醒计算机以运行此任务。

  指定计算机是否运行时间表上的任务，即便是在睡眠模式下。

外部程序

这个任务可以在备份前后运行其它命令，并且这些命令可以是 .exe，.com 或 .bat，或某一事件的特定类型，如"备份完成后关闭计算机"。

要在备份开始时执行命令，按照下列步骤操作：

1. 点击 外部程序
2. 选择 在任务执行之前 选项。
3. 单击 浏览，选择执行的命令文件。

4. 点击 确定。

要在备份完毕后执行命令，按照下列步骤操作：

1. 点击 外部程序
2. 选择 在任务执行之后 选项。
3. 点击 浏览 选择执行的命令文件。
4. 或者点击 关闭计算机，当备份完成后。
5. 或者点击 重新启动计算机，当备份完成后。
6. 或者点击 登出当前用户，当备份完成后。
7. 点击 确定。

注意

如果您想要配置在备份失败的情况下仍然生效，选中复选框 即使任务执行失败，仍运行外部程序。

文件过滤

BitDefender 备份提供了强大的过滤功能，以排除或包含指定的文件、文件类型或目录，以节省储存空间，并提高备份速度。

指定文件类型，可以过滤通过以下步骤：

1. 点击 文件过滤。
2. 单击 过滤类型。
3. 弹出选择文件类型对话框，通过选择 仅包含选定的文件类型 或 排除选定的文件类型 选项。
4. 如有必要，自定义类型编辑栏键入另一个文件类型但要确保使用.abc 格式。当您输入超过一个以上的自定义类型时，使用 ，(逗号)作为分隔符。在相应的编辑栏添加简短描述。
5. 点击 确定。

通过以下步骤，指定可以被过滤的文件：

1. 点击 文件过滤。
2. 单击 过滤文件。
3. 在弹出选择文件类型对话框中，选择仅包含规则指定的文件或排除规则指定的文件选项。
4. 单击 浏览并选择所需的文件。文件位置的路径将会自动添加到 应用到下列目录 编辑栏。 要包含或配出文件，而不论其位置，单击 应用到所有目录。
5. 点击 确定。

通过以下步骤过滤指定的目录：

1. 点击 文件过滤。
2. 单击 过滤目录.

3. 在弹出式对话框排除或包含指定的目录，通过选中　只包含规则指定的目录 或 排除规则指定的目录 选项。
4. 单击 浏览 并选择目录。 这个目录位置路径将会自动添加到 应用到下列目录 编辑栏。 要包含或排除目录，而不论其位置，单击 应用到所有目录。
5. 点击 确定。

过滤器可以通过以下步骤进行修改:

1. 点击 文件过滤。
2. 点击您希望修改的过滤器，然后点击 编辑。
3. 在对话框修改您的选项。
4. 点击 确定。

过滤器可以删除通过以下步骤:

1. 点击 文件过滤。
2. 点击您想删除的过滤器，并单击 删除。
3. 或者直接点击 删除所有 删除所有过滤器。
4. 点击 确定。

数据验证

为了确保您的备份数据始终安全，请遵循这些步骤。

1. 点击 数据核查。
2. 点击 备份过程中核查数据.
3. 点击 确定。

修改工作性质

要修改任务属性，选择相关的任务并单击 修改任务属性，在 任务管理 单元。

修改工作性质

1. 点击复选框，选择驱动盘、目录或文件进行备份。

   当您在左侧窗口中选择一个项目，其内容就会显示在右侧窗口，以便完善您的选择。
2. 为您的备份任务输入名称或使用默认任务名称。

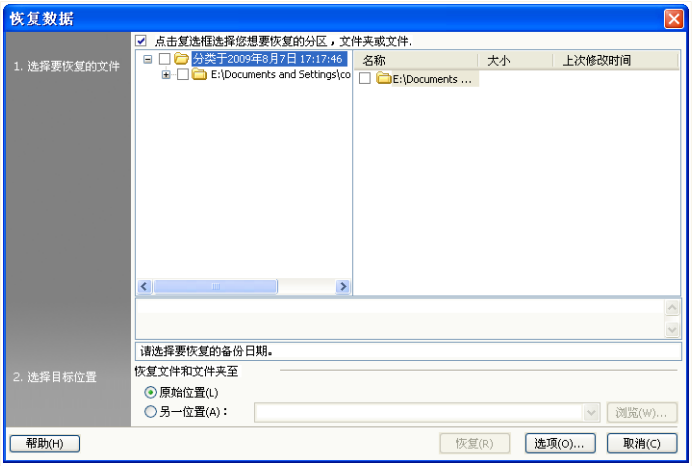
   默认的任务名是在文件或目录被选择备份时自动生成的，但是它是可以被修改的。
3. 点击 浏览，选择保存您的备份任务位置。

注意

不要忘了点击 备份 开始任务或点击 取消 来取消任务。
要完善您的设置，点击 选项。

恢复文件

要恢复您的备份数据，选择从哪里恢复数据，单击 恢复文件，在 恢复任务 菜单并按照这些步骤操作。



恢复文件

1. 选中要被恢复的分区，目录，或文件的复选框。

   当您在左侧窗口选择一个项目，其内容将显示在右侧窗口，以便完善您的选择。
2. 在 选择恢复位置 窗口，您可以使用没有任何改变的原始位置，或指定另一个位置，以恢复该文件。

   点击 浏览，选择保存您的备份任务位置。

注意

不要忘记点击 恢复 开始恢复或 取消 停止恢复。
要完善您的设置，点击 选项。

恢复选择对话框

恢复选项允许您指定一些文件在预定的时间被恢复并更新每个恢复文件的修改时间。

当恢复的文件已经存在

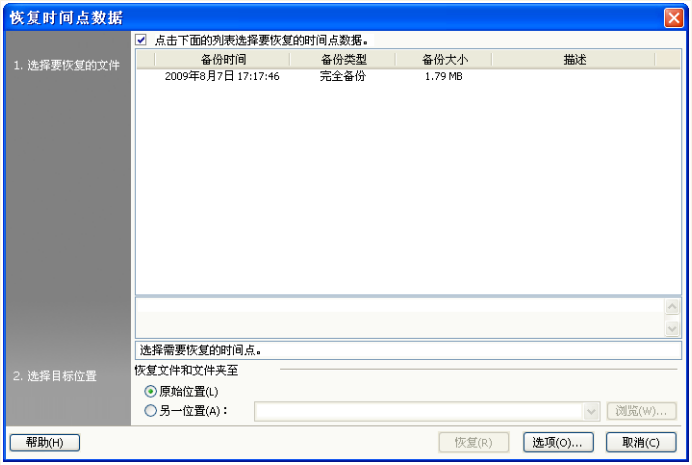
- 跳过文件BitDefender 将跳过相关的文件。
- 询问用户 BitDefender 询问是否替换现有的文件。
- 直接替换 BitDefender 会在没有询问您的情况下直接替换文件。
- 替换旧文件 BitDefender 只替换旧文件。旧文件是根据修改的日期来定义的。

文件修改日期
如果选中该选项，当文件和目录结构被恢复时 BitDefender 使用当前的日期作为显示的日期。如果没有选择该选项，BitDefender 使用备份时的日期作为文件或目录的修改日期。

目录结构
它只会在您选择另一个位置来恢复数据时被激活。您也可以保存您数据的目录结构。

恢复时间点数据

想要在一个特定的时间点恢复您的备份数据，选择需要数据恢复任务，点击 在 恢复任务 菜单中的恢复时间点数据，然后依照下列步骤操作。



恢复时间点数据

1. 从列表中选择一个特定时间点的备份集。备注将显示在它下面。
2. 在 选择恢复位置 窗口中，您既可以使用原始位置，而不作任何改变，也可以指定另一个位置，以恢复该文件。

   点击 浏览，选择保存您的备份任务位置。

注意
不要忘记点击 恢复 开始恢复或 取消 停止恢复。

要完善您的设置，点击 选项。

恢复选择对话框

恢复选项允许您指定一些文件在预定的时间被恢复并更新每个恢复文件的修改时间。

当恢复的文件已经存在

●替换旧文件 BitDefender 只替换旧文件。旧文件是根据修改的日期来定义的。

文件修改日期

如果选中该选项，当文件和目录结构被恢复时 BitDefender 使用当前的日期作为显示的日期。如果没有选择该选项，BitDefender 使用备份时的日期作为文件或目录的修改日期。

目录结构

它只会在您选择另一个位置来恢复数据时被激活。您也可以保存您数据的目录结构。

任务控制

有三种方式来任务控制：暂停任务、停止任务、和停止所有。

暂停

要暂停一个正在进行的备份或恢复任务，单击 暂停任务 按钮，在 任务控制 菜单。

停止

要停止正在进行的备份或恢复任务，单击 停止任务 按钮，在 任务控制 菜单。

全部停止

如果有一个以上的备份或恢复任务在运行，没有必要一个接一个去停止他们。点击停止所有 按钮，在 任务控制 菜单，以立刻全部停止他们。

13.2.3. 日志查看器

本节显示了如何查看，导入，导出和清除日志。日志选项可以帮助您记住您备份或恢复的内容，时间，它也显示运行过程中的警告或错误的行动。例如，如果一个文件执行过程中发生了错误，BitDefender 将把它当作一个警告讯息记录下来。

日志查看器

您可以进入 日志查看器，通过以下方式:

- 在 导航工具条 上点击 日志查看器。
- 在 菜单栏 上单击 查看 并选择 日志查看器。
- 使用快捷键 CTRL+A1t+L.

查看日志

观察日志选项允许追溯您的行动，寻找该行动失败的原因。

描述 BitDefender 备份的一个日志项目包含下列元素:

类型

日志项目严重性的分类。BitDefender 备份按严重程度分四类:

- 致命的: 一个妨碍 BitDefender 备份正常工作的重大问题。举例来说，BitDefender 备份的配置文件已损坏。

- ●错误: 一个导致操作失败的问题。例如，一个备份到一台服务器的任务，但服务器不能被访问。
- ●警告: 一个不影响操作的问题，但可以归类为一个事件。举例来说，备份时一个文件无法读取。
- ●信息: 它描述了一个成功的操作。举例来说，一个任务被成功删除。

日期
项目发生日期日志。

时间
日志文件生成的本地时间。

资源
来源记录了相关的项目，可能是一个任务或者是 BitDefender 备份程序。例如，一个系统标记的项目提示，它是由 BitDefender 备份程序记录的。其他可能的标记是 BitDefender 备份任务已经记录到相关的项目。

用户
被日志记录下来的用户名称和其他相关的操作。

描述
介绍详细内容登录项目。

清晰的条目

bitdefender 备份可提供清晰的两种方式: 自动和手动。

重要
一旦登陆记录已被清除的，它不能追回。因此，最好是把所有的出口条目到一个文件并保存，为下一步协商。

自动清晰
当 BitDefender 备份开始后，会比较现有的日志大小和默认日志大小。BitDefender 备份会自动清除所有超出默认日志大小的文件。

注意
要查询或修改默认日志大小，按照下列步骤进行:
1. 在菜单栏 点击 工具。
2. 点击 选项，然后选择 报告&日志。
3. 键入想要的大小限制(MB)到相应的编辑栏。当日志大小已经达到这个限额，BitDefender 备份将清除所有日志。

手动清楚

遵循这些步骤来手动清除日志。

1. 在 日志管理 菜单点击 清除所有。
2. 点击 确定，以在清除之前导出某些日志，或点击 否，如果您不想保留任何日志。

导入和导出日志

bitdefender 备份目前支持文件导入和导出的两种格式：.TXT 和 .XML

注意

我们建议您清除之前，导出和保存日志文件。

要导出日志到指定的文件，按照下列步骤进行：

1. 单击 导出到.TXT文件 或在 日志管理 菜单选择 导出到.TXT文件。
2. 键入文件名并选择一个地点来保存您的文件。
3. 点击 保存。

要从一个指定的文件导入日志，按照下列步骤进行：

1. 点击 从.TXT 文件导入 或在 日志管理 菜单选择 从.TXT 文件导入。
2. 找到您的文件。
3. 点击打开.

注意

在 日志管理 菜单点击 刷新 按钮，以确保您看到最新的日志。

13.2.4. 工具箱

本节说明如何使用 BitDefender 备份数据刻录到 CD/DVD 或刻录 ISO 映象文件。它涉及的主题，如刻录 CD-R/RW、DVD-R/RW/RAM、DVD+R/RW/DL 和离线保存备份数据。

工具箱

您可以进入 工具箱，通过下列方法之一：

- 在 导航工具条 点击 工具箱。
- 在 菜单栏 中点击 查看，并选择 工具箱。
- 使用快捷键 CTRL+A1t+T.

刻录 CD/DVD

要手动刻录数据到 CD/DVD，请按照下列步骤：

1. 点击 刻录数据到 CD/DVD。
2. 点击 擦除，如果您想重用可擦写光盘。如果您想快速擦除，点击 快速。如果您需要完全擦除信息记录，点击 完全，但是这可能需要较长时间。
3. 单击 刻录对话框。

这里您可以设置磁盘在被刻录后被弹出，完成（如果您打算与他人共用）或使用 Joliet 文件系统书写（减少文件名限制）。

4. 点击 文件 或 目录，在弹出式对话框中添加您要刻录的数据。
5. 数据添加后，选择刻录器和输入光碟的名称来刻录资料，然后点击 刻录。

刻录 ISO 映像文件到 CD/DVD

刻录一个 ISO 映像文件到 CD/DVD，按照这些步骤进行：

1. 点击 刻录 ISO 映像文件到 CD/DVD.
2. 点击 擦除，如果您想重用可擦写光盘。如果您想快速擦除，点击 快速。如果您需要完全擦除信息记录，点击 完全，但是这可能需要较长时间。
3. 单击 刻录对话框。

   在这里您可以设置光盘刻录后被弹出，以最后完成光盘（如果您打算与他人共用）或用 Joliet 文件系统刻录数据（减少文件名限制）。
4. 点击 添加。
5. 选择一个刻录的 ISO 映像文件并点击 打开。
6. 点击 刻录.

管理我的刻录器

这有助于您在当前系统管理并查看录入设备和媒体。它包含以下链接：

- 弹出设备，弹出选择的录入设备。
- 关闭设备 关闭选择的录入设备。
- 媒体信息，允许查看录入设备的媒体信息。
- 设备信息，允许查看录入设备以及资料。
- 功能 允许查看媒体录制功能。
- 擦除媒体 擦除光碟内容。

联系方式

14. 联系信息:

我们相信高效的沟通是业务成功的关键，十年以来，BitDefender 已经建立起了一套超出用户期望的沟通体系。如果您有任何问题，请随时联系我们。

14.1. 网址

销售部: sales@bitdefender.com
技术支持: http://kb.bitdefender.com
文档: documentation@bitdefender.com
合作伙伴项目: partners@bitdefender.com
市场部: marketing@bitdefender.com
媒体关系: pr@bitdefender.com
工作机会: jobs@bitdefender.com
提交病毒: virus_submission@bitdefender.com
垃圾邮件提交: spam_submission@bitdefender.com
报告不当使用: abuse@bitdefender.com
产品网址: http://www.bitdefender.com
产品 FTP 存档: ftp://ftp.bitdefender.com/pub
当地分销商: http://www.bitdefender.com/site/Partnership/list/
BitDefender 知识库: http://kb.bitdefender.com

14.2. BitDefender 各国办事处

BitDefender 的分公司都非常乐意在它们的业务区回答您的任何咨询，以下是它们的地址以及电话号码。

14.2.1. 北美

BitDefender, LLC
PO Box 667588
Pompano Beach, Fl 33066
电话（销售和技术支持）: 1-954-776-6262
销售: sales@bitdefender.com
网址: http://www.bitdefender.com
网上自助服务: http://kb.bitdefender.com/site/KnowledgeBase/showMain/2/

14.2.2. 德国

BitDefender GmbH
Airport Office Center
Robert-Bosch-Straße 2
59439 Holzwickede
Deutschland
电话（办事处&销售）: +49 (0)2301 91 84 222
电话（技术支持）： +49 (0)2301 91 84 444
销售： vertrieb@bitdefender.de
网站： http://www.bitdefender.de
网上自助服务： http://www.bitdefender.de/site/KnowledgeBase/showMain/2/

14.2.3. 英国和爱尔兰

Business Centre 10 Queen Street
Newcastle, Staffordshire
ST5 1ED
UK
电话（销售和技术支持）： +44 (0) 8451-305096
电子邮件： info@bitdefender.co.uk
销售： sales@bitdefender.co.uk
网站： http://www.bitdefender.co.uk
网上自助服务： http://kb.bitdefender.com/site/KnowledgeBase/showMain/2/

14.2.4. 西班牙和拉丁美洲

BitDefender España SLU
C/ Balmes, 191, 2º, 1ª
08006 Barcelona
España
传真： +34 932179128
电话（办事处&销售）: +34 902190765
电话（技术支持）： +34 935026910
销售： comercial@bitdefender.es
网站： http://www.bitdefender.es
网上自助服务： http://www.bitdefender.es/site/KnowledgeBase/showMain/2/

14.2.5. 罗马尼亚

BITDEFENDER SRL
West Gate Park, Building H2, 24 Preciziei Street
Bucharest, Sector 6
传真: +40 21 2641799
电话（销售和技术支持）: +40 21 2063470
销售: sales@bitdefender.ro
网站: http://www.bitdefender.ro
网上自助服务: http://www.bitdefender.ro/site/KnowledgeBase/showMain/2/

14.2.6. EMEA 和 APAC 企业单元

BITDEFENDER SRL
West Gate Park, Building H2, 24 Preciziei Street
Bucharest, Sector 6
Romania
传真: +40 21 2641799
电话（销售和技术支持）: +40 21 2063470
销售: sales@bitdefender.com
网站: http://www.bitdefender.com
网上自助服务: http://www.bitdefender.com/site/KnowledgeBase/showMain/2/

词汇表

ActiveX

ActiveX 是一种写入程序的模型，因此其他的程序和操作系统可以调用它。ActiveX 技术被用于和 Microsoft Internet Explorer 浏览器一起使用，来创建和计算机程序类似的交互型网页。使用 ActiveX 用户可以提问或回答问题、使用按钮并可和网页用其他方式交互。ActiveX 控件通常使用 Visual Basic 编写。

值得注意的是 Active X 完全缺少安全控制；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程序目的的授权说明协议之后才进行安装，因此并不算冒犯用户。

但是，弹出的广告可能非常恼人，有时甚至影响系统性能。此外，某些此类程序收集的信息可能侵犯用户隐私。

归档文件（压缩包）

含有已经被备份文件的磁盘，磁带或是目录。

它是一个含有一个或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。这样的漏洞的动机不一定总是恶意的，例如，有的操作系统在出厂时就留有给技术支持人员或维护人员特权账户。

Boot sector（引导扇区）

它是一个在每一个磁盘的头部的扇区，用以说明磁盘的体系结构（扇区大小、簇大小等等）。为了引导磁盘，引导扇区还包含载入操作系统的一段程序。

Boot virus（引导扇区病毒）

它是一个可以感染硬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。因此，当每次您启动您的系统时，病毒将会在内存里活动。

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应用程序。两个最受欢迎的浏览器是：Netscape Navigator 和微软 Internet Explorer）。这两个浏览器都是图形界面，也就是说它们可以显示图像和文字。另外，现代多

数的浏览器可以显示多媒体信息，包括声音和视频，当然它们需要一些格式的插件。

Command line （命令行）
在命令行界面下，用户使用命令行语言在屏幕上直接输入命令。

Cookie
在互联网行业，Cookies 是指您计算机上包含可被广告商用来追踪您的兴趣和爱好的信息的小文件。Cookie 技术仍处于不断发展中，其目的是直接向您展示您感兴趣的广告。不过对很多人来说，这是一把双刃剑。一方面，您可有效地看到符合您兴趣的广告，另一方面，Cookie 会跟踪并记录您访问了什么网页以及点击了什么地方。可以理解，会有有关隐私的争论，而且很多用户觉得 Cookie 被用作类似“条形码”的用途而感觉被冒犯。虽然此观点可能有点极端，但在某些情况下的确如此。

Disk drive （磁盘驱动器）
这是一个从磁盘上读写数据的设备。

硬盘驱动器可在硬盘上读写数据。

软盘驱动器可在软盘上读写数据。

磁盘驱动器可以是内置的（在计算机内部），也可以是外置的（连接到计算机上的外置设备）。

Download （下载）
从源主机往外围设备复制数据（通常是一个文件）的过程，此术语通常用来描述从在线服务向个人计算机复制文件的过程。此外，下载还可以指从网络文件服务器向网络中的计算机复制文件的过程。

电子邮件
Electronic mail 的缩写。一种通过局域网或广域网在计算机上发送消息的服务。

事件
由程序检测到的操作或发生的事情。事件可能是用户操作，例如点击鼠标按钮或按下键盘等，也可能是系统中发生的事情，如内存溢出。

False positive （误报）
是指扫描程序将正常文件认定为受感染的文件。

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，它通常在一到三个字母之间。例如C源程序的“c”，PostScript 语言的"ps"，文本文件的"txt"。

Heuristic（启发式）
它是一个用来检测新病毒的基于规则的方法。该方式的扫描不需要依靠病毒库。启发式扫描的好处是不会被现存病毒的变种所欺骗。但是，它有可能报告一个正常程序中含有可疑代码，从而导致所谓的“误报”（"false positive"）。

IP
网际网络协议（Internet Protocol） – 在 TCP/IP 协议组里的一个路由协议，主要处理 IP 寻址、路由、分解及组装 IP 包。

Java applet（Java 小程序）
它是一个只在网页上运行的 Java 程序。要想在网页上用 Java 小程序，您需要指明这个 Java 小程序的名称和 Java 小程序可以利用的大小（长和宽，以像素为单位）。访问含有 Java 小程序的网页时，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，它由一个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，但是它不可以读写客户端计算机。另外，小程序被进一步的约束着，所以它只可以在它所来自域名里进行数据读写。

Macro virus（宏病毒）
一种以宏命令方式嵌入文档中的电脑病毒，许多应用程序，如 Word 和 Excel，支持强大的宏语言。

这些程序允许在文档中嵌入宏，每次打开文档就将执行宏。

Mail client（电子邮件客户端程序）
电子邮件应用程序使用户可以编写、接收和发送邮件。

内存
计算机的内部存储区域，术语“内存”指以芯片方式存放的数据，“存储”是指存在于磁带或磁盘上的内存。每台计算机都带有一定数量的物理内存，通常被称为主存或 RAM。

Non-heuristic(非启发式)
这种扫描方式依赖病毒特征库，其优点是不会被看起来像是病毒的文件欺骗，因此很少产生误报。

加壳程序

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以便减少内存使用。比如，一个文本文件包含 10 个连续的空格字符，通常就会需要 10 个字节存储。

但是，一个压缩程序会将空格字符替换为一个特殊的空格序列字符，然后跟上被替换的空格数。这样，10 个空格字符只需两个字节存储。这只是一种加壳方式，还有很多其他的加壳方式。

路径

指打开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。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有一个通道，如两台计算机之间的通讯渠道。

网络钓鱼

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，在此对资料进行偷窃。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个人资料（比如密码、信用卡、身份证号码和银行户口帐号），这个网站是欺骗的工具。

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。

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、显示屏和键盘的端口。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。

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，以及受感染和可疑文件的报告文件。

Rootkit（黑客工具）

Rootkit 是一套提供管理员级别系统访问的软件工具。这个名词首次出现在 UNIX 操作系统中，指的是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。它们可以监控通信、创建系统的后门，更改文件以及日志以避免被发现。

脚本
是宏或批量处理文件的另外一种名称。运用脚本不需用户者指令。

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。

间谍软件
它是一种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。

间谍软件和木马程序一样，都是在用户不知情的情况下安装其它软件的同时进行安装的。一般来说，成为间谍软件的攻击对象都是由于下载了当前特定的点对点文件转换产品。

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宽带，长期内会使用户系统运行不顺畅，甚至是系统崩溃。

Startup items （启动项）
在这文件夹内的任何文件都会在系统启动时自行启动。启动时的屏幕，音响效果，日志或任何应用程序都能成为启动项。通常在此文件夹内的文件都是别名文件。

系统栏
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 （传输控制协议/互联网协议）
传输控制/互联网协议 – 这是一套广泛应用于互联网的网络协议，满足各种硬件结构和操作系统的计算机的互联网络通信。TCP/IP 包括计算机通信原理和网络连接和路由流量方面的约定。

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。

该术语源自于荷马史诗中的《伊利亚特》，指的是希腊人送给他们的敌人一个大型的木马，假装与对方和解。但是木马被拖进城之后，希腊士兵就偷偷从马的空心腹部跑出来，打开城门让同胞们蜂拥而入，并很快占领了特洛伊。

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。

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自我繁殖。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。它能够用尽系统的内存，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。

Virus definition （病毒库）
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。

A. 修复和卸载 BitDefender

要想修复或移除 BitDefender Business Client，需满足以下条件：

1. 您必须使用管理员账号登录到计算机。
2. BitDefender Business Client 必须在超级用户模式下操作。 否则，您需要有管理密码。

如果您想修复或移除 BitDefender Business Client，请依照以下路径从 Windows 开始菜单进入：开始 → 程序 → BitDefender Business Client → 修复或移除。

您将被要求按下下一步确认您的选择，之后会出现一个新窗口供您选择：

- 修复 – 重新安装上一次安装中所选的程序组件。 如果程序在受限用户模式下操作，您必须提供管理密码。

  如果您选择修复 BitDefender，新的窗口会出现。 点击修复 开始修复过程。

  当看到重启提示时，请重启计算机，随后单击 安装重新安装 BitDefender Business Client。

  安装过程完成后会显示一个新窗口。 点击完成。

- 卸载 – 卸载所有已经安装的组件。 如果程序在受限用户模式下操作，您必须提供管理密码。

  如果您选择删除 BitDefender，新的窗口会出现。 单击移除开始移除操作。

  卸载过程完成后，会显示一个新窗口。 点击完成。