



AVG Internet Security 2011

用户手册

文档修订 2011.21 (16.5.2011)

版权所有 AVG Technologies CZ, s.r.o. 保留所有权利。
所有其它商标均是其各自所有者的财产。

本产品采用 RSA Data Security, Inc. 在 1991 年创立的 MD5 信息摘要算法（版权所有 (C) 1991-1992 RSA Data Security, Inc.）。

本产品采用 C-SaCzech 库中的代码（版权所有 (c) 1996-2001 Jaromir Dolecek (dolecek@ics.muni.cz)）。

本产品采用压缩库 Zlib（版权所有 (c) 1995-2002 Jean-loup Gailly and Mark Adler）。

本产品采用压缩库 libbzip2（版权所有 (c) 1996-2002 Julian R. Seward）。



目录

1. 简介	8
2. AVG 安装要求	9
2.1 支持的操作系统	9
2.2 最低和推荐硬件要求	9
3. AVG 安装选项	10
4. AVG 安装过程	11
4.1 欢迎使用	11
4.2 激活您的 AVG 许可证	11
4.3 选择安装类型	12
4.4 自定义选项	13
4.5 安装 AVG Security Toolbar	14
4.6 安装进度	15
4.7 安装已成功	15
5. 安装后	17
5.1 产品注册	17
5.2 访问用户界面	17
5.3 扫描整个计算机	17
5.4 Eicar 测试	17
5.5 AVG 默认配置	18
6. AVG 用户界面	19
6.1 系统菜单	20
6.1.1 文件	20
6.1.2 组件	20
6.1.3 历史记录	20
6.1.4 工具	20
6.1.5 帮助	20
6.2 安全状态信息	22
6.3 快速链接	23
6.4 组件概览	24
6.5 统计信息	25
6.6 系统任务栏图标	25
6.7 AVG 小工具	26



7. AVG 组件	29
7.1 Anti-Virus	29
7.1.1 Anti-Virus 原理	29
7.1.2 Anti-Virus 界面	29
7.2 Anti-Spyware	30
7.2.1 Anti-Spyware 原理	30
7.2.2 Anti-Spyware 界面	30
7.3 Anti-Spam	32
7.3.1 Anti-Spam 原理	32
7.3.2 Anti-Spam 界面	32
7.4 Firewall	33
7.4.1 Firewall 原理	33
7.4.2 Firewall 配置文件	33
7.4.3 Firewall 界面	33
7.5 Link Scanner	36
7.5.1 Link Scanner 原理	36
7.5.2 Link Scanner 界面	36
7.5.3 Search-Shield	36
7.5.4 Surf-Shield	36
7.6 Resident Shield	40
7.6.1 Resident Shield 原理	40
7.6.2 Resident Shield 界面	40
7.6.3 Resident Shield 检测	40
7.7 Family Safety	44
7.8 AVG LiveKive	45
7.9 电子邮件扫描程序	45
7.9.1 电子邮件扫描程序原理	45
7.9.2 电子邮件扫描程序界面	45
7.9.3 电子邮件扫描程序检测	45
7.10 更新管理器	48
7.10.1 更新管理器原理	48
7.10.2 更新管理器界面	48
7.11 许可证	50
7.12 远程管理	51
7.13 Online Shield	52
7.13.1 Online Shield 原理	52
7.13.2 Online Shield 界面	52



7.13.3 Online Shield 检测	52
7.14 Anti-Rootkit	55
7.14.1 Anti-Rootkit 原理	55
7.14.2 Anti-Rootkit 界面	55
7.15 系统工具	57
7.15.1 进程	57
7.15.2 网络连接	57
7.15.3 自动启动	57
7.15.4 浏览器扩展	57
7.15.5 LSP 查看器	57
7.16 PC Analyzer	62
7.17 ID Protection	64
7.17.1 ID Protection 原理	64
7.17.2 ID Protection 界面	64
7.18 Security Toolbar	66
8. AVG Security Toolbar	68
8.1 AVG Security Toolbar 界面	68
8.1.1 AVG 徽标按钮	68
8.1.2 采用 AVG Secure Search (powered by Google) 的搜索框	68
8.1.3 页面状态	68
8.1.4 AVG 新闻	68
8.1.5 新闻	68
8.1.6 删除历史记录	68
8.1.7 电子邮件通知程序	68
8.1.8 天气信息	68
8.1.9 Facebook	68
8.2 AVG Security Toolbar 选项	75
8.2.1 ‘常规’选项卡	75
8.2.2 ‘有用的按钮’选项卡	75
8.2.3 ‘安全’选项卡	75
8.2.4 ‘高级选项’选项卡	75
9. AVG 高级设置	79
9.1 外观	79
9.2 声音	81
9.3 忽略故障状况	82
9.4 Identity Protection	83
9.4.1 Identity Protection 设置	83



9.4.2 ‘已允许’列表	83
9.5 病毒库	87
9.6 PUP 特例	87
9.7 Anti-Spam	89
9.7.1 设置	89
9.7.2 性能	89
9.7.3 RBL	89
9.7.4 白名单	89
9.7.5 黑名单	89
9.7.6 高级设置	89
9.8 Online Shield	99
9.8.1 Web 保护	99
9.8.2 即时通讯	99
9.9 Link Scanner	102
9.10 扫描	103
9.10.1 扫描整个计算机	103
9.10.2 外壳扩展扫描	103
9.10.3 扫描特定的文件或文件夹	103
9.10.4 可移动设备扫描	103
9.11 计划	108
9.11.1 计划的扫描	108
9.11.2 病毒数据库更新计划	108
9.11.3 程序更新计划	108
9.11.4 Anti-Spam 更新计划	108
9.12 电子邮件扫描程序	119
9.12.1 验证	119
9.12.2 邮件过滤	119
9.12.3 服务器	119
9.13 Resident Shield	127
9.13.1 高级设置	127
9.13.2 排除的项目	127
9.14 缓存服务器	131
9.15 Anti-Rootkit	132
9.16 更新	133
9.16.1 代理	133
9.16.2 拨号	133
9.16.3 URL	133
9.16.4 管理	133



9.17 暂时禁用 AVG 保护	140
9.18 产品改进计划	140
10. Firewall 设置	143
10.1 常规	143
10.2 安全	144
10.3 区域和适配器配置文件	145
10.4 IDS	146
10.5 日志	148
10.6 配置文件	149
11. AVG 扫描	151
11.1 扫描界面	151
11.2 预定义扫描	152
11.2.1 扫描整个计算机	152
11.2.2 扫描特定的文件或文件夹	152
11.2.3 Anti-Rootkit 扫描	152
11.3 扫描 Windows 资源管理器	161
11.4 命令行扫描	162
11.4.1 CMD 扫描参数	162
11.5 扫描计划	164
11.5.1 计划设置	164
11.5.2 扫描方式	164
11.5.3 扫描内容	164
11.6 扫描结果概览	172
11.7 扫描结果详细信息	173
11.7.1 ‘结果概览’选项卡	173
11.7.2 ‘感染’选项卡	173
11.7.3 ‘间谍软件’选项卡	173
11.7.4 ‘警告’选项卡	173
11.7.5 ‘Rootkit’选项卡	173
11.7.6 ‘信息’选项卡	173
11.8 病毒库	180
12. AVG 更新	182
12.1 更新级别	182
12.2 更新类型	182
12.3 更新过程	182



13. 事件历史记录	183
14. 常见问题解答和技术支持	185



1. 简介

本用户手册提供全面的 **AVG Internet Security 2011** 文档。

祝贺您购买 AVG Internet Security 2011 !

AVG Internet Security 2011 是一系列屡获殊荣的 AVG 产品之一，旨在全面保护 PC，让用户高枕无忧。与所有其它 AVG 产品一样，**AVG Internet Security 2011** 经过了彻头彻尾的完全重新设计，以一种更具用户友好性、更高效的新方式提供 AVG 享有盛名、备受信赖的安全保护。新 **AVG Internet Security 2011** 产品的界面经过优化，同时兼具更为严格、速度更快的扫描功能。为方便您使用，更多的安全功能实现了自动化；此外还引入了新的智能型用户选项，以便您可以根据自己的生活方式来调整我们的安全功能。不再为提升安全性而牺牲易用性！

AVG 旨在保护您的计算和网络活动。请尽享 AVG 的全面保护。

所有 AVG 产品均可提供

- 适合您的计算机和 Internet 使用方式的保护：网上银行和网上购物、冲浪和搜索、聊天和收发电子邮件，或文件下载和交友 –AVG 总有一款适合您的产品
- 无障碍的保护，深受全世界 1.1 亿多用户的信赖，依托一个由经验丰富的研究人员组成的全球网络
- 以全天候提供服务的专家支持为后盾的保护



2. AVG 安装要求

2.1. 支持的操作系统

AVG Internet Security 2011 意在保护运行以下操作系统的工作站：

- Windows XP Home Edition SP2
- Windows XP Professional SP2
- Windows XP Professional x64 Edition SP1
- Windows Vista (x86 和 x64, 所有版本)
- Windows 7 (x86 和 x64, 所有版本)

(应用了更高 Service Pack 版本的特定操作系统可能也适用)

注意：Windows XP x64 不支持 [ID Protection](#) 组件。仅可在此操作系统中安装不带 IDP 组件的 AVG Internet Security 2011。

2.2. 最低和推荐硬件要求

对 **AVG Internet Security 2011** 的最低硬件要求：

- Intel Pentium CPU 1,5 GHz
- 512 MB RAM 内存
- 750 MB 可用硬盘空间 (用于安装)

对 **AVG Internet Security 2011** 的推荐硬件要求：

- Intel Pentium CPU 1,8 GHz
- 512 MB RAM 内存
- 1400 MB 可用硬盘空间 (用于安装)



3. AVG 安装选项

可用安装光盘中的安装文件安装 AVG，也可从 AVG 网站 (<http://www.avg.com/>) 上下载最新的安装文件。

在开始安装 AVG 之前，我们强烈建议您访问 AVG 网站 (<http://www.avg.com/>)，查看是否有新的安装文件。这样可确保安装的是最新版 AVG Internet Security 2011。

在安装过程中，系统将要求您提供您的许可证/销售号码。请确保在开始安装前将其准备好。销售号码可在光盘包装上找到。如果您是以在线方式购买 AVG 副本的，那么已通过电子邮件向您发送了许可证号码。



4. AVG 安装过程

要将 **AVG Internet Security 2011** 安装到计算机中，需要获得最新的安装文件。您可以使用您的盒装版所含光盘中的安装文件，但此文件可能已过时。因此我们建议在线获取最新的安装文件。可以从 AVG 网站 (<http://www.avg.com/>) 上的 **“支持中心”** / **“下载”** 部分中下载该文件。

安装过程就是一系列对话框窗口，各个窗口中显示了有关每一步该如何操作的简短说明。下面，我们提供了对各个对话框窗口的说明：

4.1. 欢迎使用

开始安装时会显示 **“欢迎”** 对话框窗口。您将在此窗口中选择要在安装过程中使用的语言，以及 AVG 用户界面的默认语言。此对话框窗口上方部分有一个下拉菜单，其中包含语言列表，您可以从中进行选择：



注意：此处选择的是用于安装过程的语言。您选择的语言将安装为 AVG 用户界面的默认语言，同时还会自动安装英语。如果想要为用户界面安装其它语言，请在下面名为 **自定义选项** 的设置对话框中指定其它语言。

另外，此对话框还提供了 AVG 许可协议的完整文本。请仔细阅读该协议。若要确认您已阅读、了解并接受该协议，请单击 **“接受”** 按钮。如果您不同意该许可协议，请单击 **“拒绝”** 按钮，安装过程会立即终止。

4.2. 激活您的 AVG 许可证

在 **“激活您的许可证”** 对话框中，您需要将您的许可证号码填入所提供的文本字段。

销售号码可在 **AVG Internet Security 2011** 包装盒内的光盘包装上找到。许可证号码将在您在线购买 **AVG Internet Security 2011** 之后通过确认电子邮件发送给您。您必须完全按照如图所示键入号码。如果存在数字形式的许可证号码（在电子邮件中），建议使用复



制和粘贴方法插入它。



按“**下一步**”按钮继续执行安装过程。

4.3. 选择安装类型



“**选择安装类型**”对话框提供了以下两个安装选项供您选择：**“快速安装”**和**“自定义安装”**。

对于大多数用户而言，强烈建议执行标准的**“快速安装”**；该安装方式会采用程序供应商预定义的设置以完全自动的方式安装 AVG。这种配置可提供最佳的安全性，同时又会使



资源得到最优利用。今后如果需要更改配置，您始终都可以直接在 AVG 应用程序中完成。如果选择了 **“快速安装”** 选项，单击 **“下一步”** 按钮可进入以下 [“安装 AVG Security Toolbar”](#) 对话框。

“自定义安装” 只应由经验丰富的用户在确有必要不以标准设置安装 AVG 时使用；例如，为满足特定的系统要求。选择此选项后，单击 **“下一步”** 按钮可进入 [“自定义选项”](#) 对话框。

在该对话框的右侧，您可以找到与 [AVG 小工具](#)（在 Windows Vista/Windows 7 上受支持）相关的复选框。如果想要安装此小工具，可选中对应的复选框。然后就可以从 Windows 边栏访问 [AVG 小工具](#)，从而使您能够立即访问最重要的 **AVG Internet Security 2011** 功能，即 [扫描](#) 和 [更新](#)。

4.4. 自定义选项

“自定义选项” 对话框允许您设置两个安装参数：



目标文件夹

在该对话框的 **“目标文件夹”** 部分，您应该指定要安装 **AVG Internet Security 2011** 的位置。默认情况下，AVG 会被安装到 C: 驱动器上的 Program Files 文件夹中。如果您要更改此位置，请使用 **“浏览”** 按钮来显示驱动器结构，然后选择相应的文件夹。

组件选择

“组件选择” 部分提供所有可安装的 **AVG Internet Security 2011** 组件的概览。如果默认设置不适合您，您可以删除/添加特定的组件。



不过，您只能从您购买的 AVG 版本所包含的组件中进行选择！

突出显示 **‘组件选择’** 列表中的任何项，此部分右侧将会显示对应组件的简要说明。有关每个组件的功能的详细信息，请参见本文档的 [‘组件概览’](#) 一章。若要恢复至软件供应商预设的默认配置，请使用 **‘默认’** 按钮。

按 **‘下一步’** 按钮以继续。

4.5. 安装 AVG Security Toolbar



在 **‘安装 AVG Security Toolbar’** 对话框中，您可以决定是否想要安装 [AVG Security Toolbar](#)。如果不更改默认设置，则会将此组件自动安装到 Internet 浏览器（*目前受支持的浏览器包括 Microsoft Internet Explorer v. 6.0 或更高版本，以及 Mozilla Firefox v. 3.0 或更高版本*）中，以便在上网冲浪时提供全面的在线保护。

此外，也可决定是否要将 AVG Secure Search (powered by Google) 作为默认搜索提供程序。如果是，则将相应复选框保持选中状态。



4.6. 安装进度

‘**安装进度**’对话框显示安装过程的进度，不需要任何人工干预：



安装过程结束后会重定向到下一对话框。

4.7. 安装已成功



‘**安装已成功**’对话框确认 **AVG Internet Security 2011** 已经完整安装并配置完成。



请在此对话框中提供您的联系信息，以便接收所有与产品相关的信息和新闻。下方是注册表格，其中包含两个选项：

- **“是，让我通过电子邮件随时了解安全新闻和 AVG 2011 特惠”**选中此复选框即表明您愿意了解 Internet 安全领域的最新动态，并希望接收关于 AVG 产品特惠、改进和升级等的信息。
- **“我同意参加 AVG 2011 Web 安全和产品改进计划...”**选中此复选框即确认您希望参加产品改进计划（有关详细信息，请参阅 [AVG 高级设置/产品改进计划](#) 一章），该计划将收集关于检测到的威胁的匿名信息，以便提高总体 Internet 安全级别。

若要结束安装过程，您需要重新启动计算机：选择您是希望 **“立即重新启动”**，还是希望推迟此操作 - **“稍后重新启动”**。

注意：如果是使用任何 AVG 商业许可证，在您以前选择了安装远程管理项（请参见 [自定义选项](#)）的情况下，安装已成功对话框会显示以下界面：

您需要指定 AVG DataCenter 参数 - 请提供到 AVG DataCenter 的连接字符串，格式为 **“服务器:端口”**。如果此时尚不能提供此信息，请将此字段留空，稍后可以在 **“高级设置/远程管理”**对话框中设置此配置。有关 AVG Remote Administration 的详细信息，请参阅 AVG Business Edition 用户手册；可从 AVG 网站 (<http://www.avg.com/>) 下载该手册。



5. 安装后

5.1. 产品注册

安装完 **AVG Internet Security 2011** 之后，请在 AVG 网站 (<http://www.avg.com/>) 中的“注册”页面上在线注册您的产品（直接在该页面中按提供的说明操作）。注册之后，您就可以完全访问您的 AVG 用户帐户、AVG 更新新闻稿，还可以享受专为注册用户提供的其它服务。

5.2. 访问用户界面

[AVG 用户界面](#) 可通过以下几种方式进行访问：

- 双击 [AVG 系统任务栏图标](#)
- 双击桌面上的 AVG 图标
- 双击位于 [AVG 小工具](#) 底部的状态行（[如果已安装](#)；在 Windows Vista/Windows 7 上受支持）
- 从菜单“开始”“程序”“AVG 2011”“AVG 用户界面”
- 从 [AVG Security Toolbar](#) 通过选项“启动 AVG”

5.3. 扫描整个计算机

存在一种潜在风险，即计算机病毒在 **AVG Internet Security 2011** 安装之前就已传播到您的计算机上。因此，您应运行“[扫描整个计算机](#)”这一功能以确保您的 PC 上不存在感染。

有关运行 [扫描整个计算机](#) 这一功能的说明，请参阅 [AVG 扫描](#) 一章。

5.4. Eicar 测试

要确保 **AVG Internet Security 2011** 已安装妥当，可执行 EICAR 测试。

EICAR 测试是用于测试防病毒系统运行情况的标准且绝对安全的方法。它可以安全地进行分发，因为它并非真正的病毒，且不包含任何病毒代码段。大多数产品都会将它当成病毒而作出反应（尽管它们在报告它时通常使用一个清楚明白的名称，例如 EICAR-AV-Test）。您可以从 EICAR 网站 (www.eicar.com) 下载 EICAR 病毒，该网站上还提供了所有必要的 EICAR 测试信息。

请尝试下载 eicar.com 文件并将其保存到您的本地磁盘上。确认下载该测试文件后，[Online Shield](#) 会立即对此作出反应，显示一则警告。这则通知表明 AVG 已在计算机中安装妥当。



也可从网站 <http://www.eicar.com> 中下载压缩版 EICAR 病毒”(例如，以 `ecar_com.zip` 的形式下载)。通过 [Online Shield](#) 可下载此文件，将其保存在本地磁盘中，但随后尝试对其进行解压缩时，[Resident Shield](#) 就会检测到该病毒”。如果 AVG 未能将 EICAR 测试文件当成病毒识别出来，则您应重新检查程序配置！

5.5. AVG 默认配置

AVG Internet Security 2011 的默认配置（即应用程序在刚安装完后的设置）由软件供应商设置，这样所有组件和功能都会经过调整达到最佳性能。

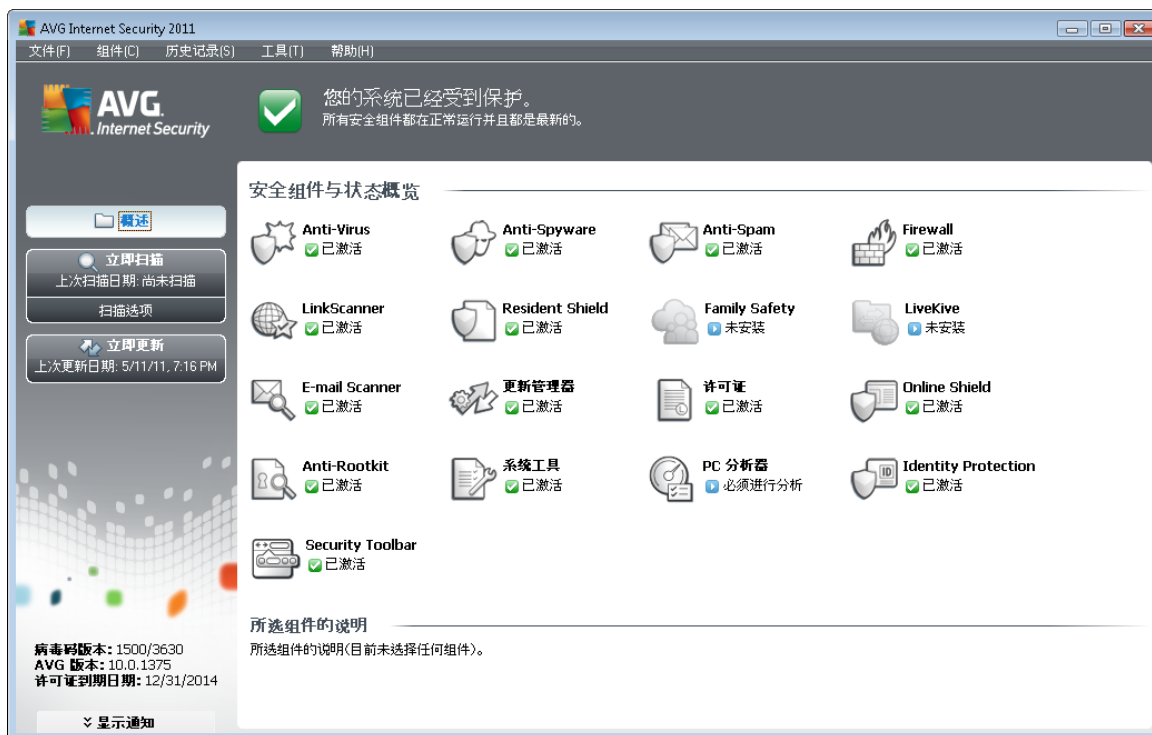
除非必要，否则请勿更改 AVG 配置！对设置的更改只应当由经验丰富的用户执行。

对 [AVG 组件](#) 设置的某些细微编辑可直接从特定组件的用户界面中进行。如果您认为需要更改 AVG 配置以便更好地满足自己的需要，请转至 [“AVG 高级设置”](#)：选择“工具”“高级设置”系统菜单项，然后在新打开的 [“AVG 高级设置”](#) 对话框中编辑 AVG 配置。



6. AVG 用户界面

AVG Internet Security 2011 打开时会显示主窗口：



该主窗口分为若干区域：

- **系统菜单**（窗口顶部的系统行）提供了标准的导航方式，可用来访问所有 AVG 组件、服务和功能 - [详细信息 >>](#)
- **安全状态信息**（窗口上方区域）提供了有关 AVG 程序当前状态的信息 - [详细信息 >>](#)
- **快速链接**（窗口左侧区域）用于快速访问最重要和最常用的 AVG 任务 - [详细信息 >>](#)
- **组件概览**（窗口中央区域）提供了已安装的所有 AVG 组件的概览 - [详细信息 >>](#)
- **统计信息**（窗口左下方区域）提供了有关程序运行情况的所有统计数据 - [详细信息 >>](#)
- **系统任务栏图标**（显示器右下角，系统任务栏上）指示 AVG 的当前状态 - [详细信息 >>](#)
- **AVG 小工具**（Windows 边栏，在 Windows Vista/7 中受支持）允许快速访问 AVG 扫描和更新 - [详细信息 >>](#)



6.1. 系统菜单

系统菜单是所有 Windows 应用程序中都采用的标准导航方式。它横放在 **AVG Internet Security 2011** 主窗口的最顶部。使用系统菜单可访问特定的 AVG 组件、功能和服务。

系统菜单分为五个主要部分：

6.1.1. 文件

- **“退出”** - 关闭 **AVG Internet Security 2011** 的用户界面。不过，AVG 应用程序将在后台继续运行，因而您的计算机仍将受到保护！

6.1.2. 组件

系统菜单的 **“组件”** 菜单项包含指向已安装的所有 AVG 组件的链接，单击这些链接可在用户界面中打开这些组件的默认对话框页面：

- **系统概览** - 切换到默认的用户界面对话框，其中提供了 [已安装的所有组件及其状态的概览](#)
- **Anti-Virus**，可确保您的计算机免受企图进入您计算机的病毒侵害 - [详细信息 >>](#)
- **Anti-Spyware**，可确保您的计算机免受间谍软件和广告软件侵害 - [详细信息 >>](#)
- **Anti-Spam**，检查所有传入的电子邮件并将不需要的电子邮件标记为“垃圾邮件” - [详细信息 >>](#)
- **Firewall**，控制您的计算机与 Internet 或本地网络上的其它计算机交换数据的方式 - [详细信息 >>](#)
- **Link Scanner**，检查在您的 Internet 浏览器中显示的搜索结果 - [详细信息 >>](#)
- **电子邮件扫描程序**，检查所有传入和传出的邮件是否携带病毒 - [详细信息 >>](#)
- **Family Safety** 有助于监视子女的在线活动，并且防止他们受到不当网站内容的侵害 - [详细信息 >>](#)
- **LiveKive** 用于自动在线备份数据 - [详细信息 >>](#)
- **Resident Shield**，在后台运行并在文件被复制、打开或保存时扫描它们 - [详细信息 >>](#)
- **更新管理器**，控制所有 AVG 更新 - [详细信息 >>](#)
- **许可证**，用于显示许可证号、类型和到期日期 - [详细信息 >>](#)
- **Online Shield**，用于扫描正在通过 Web 浏览器下载的所有数据 - [详细信息 >>](#)
- **Anti-Rootkit**，检测企图掩饰恶意软件的程序和技术 - [详细信息 >>](#)
- **系统工具**，提供 AVG 环境和操作系统信息的详细摘要 - [详细信息 >>](#)



- **PC Analyzer**, 提供有关您的计算机状态的信息 - [详细信息 >>](#)
- **Identity Protection** - 是一种防恶意软件组件, 主要用于防止身份窃贼窃取宝贵的个人数字资料 - [详细信息 >>](#)
- **Security Toolbar** 可用于直接通过 Internet 浏览器使用所选 AVG 功能 - [详细信息 >>](#)
- **Remote Administration** 仅当已在 [安装过程](#) 中指定要安装此组件时, 才会显示在 AVG Business Edition 中

6.1.3. 历史记录

- **“扫描结果”** - 切换到 AVG 测试界面, 具体而言, 即切换到 **“扫描结果概览”** 对话框
- **Resident Shield 检测** - 用于打开一个对话框, 从中大概了解 **Resident Shield**
- **E-mail Scanner 检测** - 用于打开一个对话框, 从中大概了解 **E-mail Scanner** 组件检测后断定有危险的邮件附件
- **“通过Online Shield发现的威胁”** - 用于打开一个对话框, 从中大概了解 **Online Shield**
- **“病毒库”** 打开隔离区 (**病毒库**) 的界面, AVG 会将已检测到但因故无法自动修复的所有受感染文件移到隔离区中。受感染文件会在隔离区中隔离起来, 从而保证计算机的安全, 同时也会将受感染文件存储下来, 以备日后修复
- **事件历史记录日志** - 用于打开历史记录日志界面, 其中有全部已记录的 **AVG Internet Security 2011** 操作的概况
- **Firewall** - 用于打开 Firewall 设置界面中的 **日志** 选项卡, 其中有全部 Firewall 操作的详细概况

6.1.4. 工具

- **扫描计算机** - 可以切换到 **AVG 扫描界面** 并启动对整个计算机的扫描。
- **扫描所选文件夹** - 可以切换到 **AVG 扫描界面**, 还可以在计算机的树结构中定义应扫描的文件和文件夹。
- **扫描文件** - 可以按需对从磁盘树结构中选择的单个文件执行测试。
- **更新** - 自动启动 **AVG Internet Security 2011** 的更新进程。
- **从目录更新** - 从位于您本地磁盘上指定文件夹中的更新文件执行更新过程。不过, 建议仅将此选项用于应急情况, 例如不存在 Internet 连接的情况 (例如, 您的计算机受到感染且已从 Internet 断开; 您的计算机连接到无权访问 Internet 的网络, 等等)。在新打开的窗口中, 请选择您之前将更新文件放置到的文件夹, 然后启动更新过程。
- **高级设置** - 打开 **“AVG 高级设置”** 对话框, 在此对话框中您可以对 **AVG Internet Security 2011** 配置进行编辑。一般而言, 建议保留由软件供应商定义的应用程序



默认设置。

- **Firewall 设置** - 打开一个独立的对话框，以便对 **Firewall** 组件进行高级配置。

6.1.5. 帮助

- **目录** - 打开 AVG 帮助文件
 - **获取在线帮助** - 打开 AVG 网站 (<http://www.avg.com/>) 中的客户支持中心页面
 - **您的 AVG Web** - 打开 AVG 网站 (<http://www.avg.com/>)
 - **“关于病毒和威胁”** - 打开在线 **病毒百科全书**，您可以在其中查找关于所识别到的病毒的详细信息
 - **重新激活** - 用于打开 **“激活 AVG”** 对话框，其中有 **安装过程** 中在 **“对 AVG 进行个性化设置”** 对话框中输入的数据。在此对话框中，您可以输入您的许可证号码来替换销售号码（您安装 AVG 时使用的号码）或替换原来的许可证号码（例如在升级到新的 AVG 产品时）。
 - **立即注册** - 用于连接到 AVG 网站 (<http://www.avg.com/>) 的注册页面。请填写您的注册数据；只有注册了自己的 AVG 产品的客户才能享受到免费的技术支持。
- 注：**如果使用的是试用版 **AVG Internet Security 2011**，后两个选项会显示为 **“立即购买”** 和 **“激活”**；这样就可以立即购买该程序的完整版。对于通过销售号码安装的 **AVG Internet Security 2011**，这两个选项显示为 **“注册”** 和 **“激活”**。有关更多信息，请见本文档的 **许可证** 一节。
- **关于 AVG** - 打开 **“信息”** 对话框，此对话框包含五个选项卡，提供了有关程序名称、程序和病毒数据库版本、系统信息、许可协议以及 **AVG Technologies CZ** 联系信息的数据。

6.2. 安全状态信息

“安全状态信息” 区域位于 AVG 主窗口的上部。在此区域中，始终可以找到 **AVG Internet Security 2011** 当前安全状态的信息。下面概述了此区域中可能显示的图标以及各自所代表的含义：



- 绿色图标表示 AVG 的运行完全正常。您的计算机受到全面保护、已及时更新且已安装的所有组件均正常工作。



- 橙色图标警告，一个或多个组件配置不当，您应对其属性/设置加以注意。AVG 中未出现严重问题，您可能出于某种原因已决定将某些组件关闭。但您仍然受 AVG 保护。不过，请对问题组件的设置加以注意！**“安全状态信息”** 区域中将提供其名称。

如果您出于某种原因决定 **忽略一组件的错误状态**（可通过在 AVG 主窗口的组件概览中右键单击相应组件的图标打开上下文菜单，从中即可选择 **忽略组件状态** 选项



），此图标也会显示。在特定情况下您可能需要使用此选项，但极力建议尽快禁用“**忽略组件状态**”选项。



- 红色图标表示 AVG 出现严重状况！一个或多个组件无法正常工作，因而 AVG 无法保护您的计算机。请立刻加以注意，以修复所报告的问题。如果您自己无法纠正错误，请与 [AVG 技术支持](#) 团队联系。

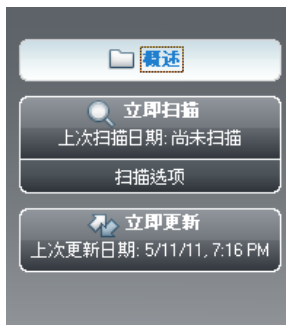
在 AVG 未设置为达到最佳性能的情况下，安全状态信息旁边会显示一个名为“**修复**”（或在问题涉及多个组件的情况下为“**全部修复**”）的新按钮。按此按钮可启动自动的程序检查和配置过程。这是将 AVG 设置为最佳性能并达到最高安全级别的简便方法！

强烈建议您注意“**安全状态信息**”，如果所报告的内容表示出现任何问题，请立即设法予以解决。否则您的计算机将面临风险！

注：AVG 状态信息也可以随时通过 [系统任务栏图标](#) 获得。

6.3. 快速链接

快速链接（在 [AVG 用户界面](#) 的左侧区域中）用于直接访问最重要且最常用的 AVG 功能：



- **概览** - 使用此链接可从当前打开的任何 AVG 界面切换到包含所有已安装组件概览的默认界面 - 请参见 [“组件概览”一章 >>](#)
- **“立即扫描”** 默认情况下，此按钮提供上次启动的扫描的信息（**扫描类型**、**上次启动的日期**）可以执行 **立即扫描** 命令以再次启动相同的扫描，也可以单击 **扫描选项** 链接打开 AVG 扫描界面，您可以在其中运行扫描、对扫描进行计划或编辑其参数 - 请参见 [AVG 扫描一章 >>](#)
- **“立即更新”** 此链接提供上次启动更新过程的日期。按此按钮可打开更新界面并立即启动 AVG 更新过程 - 请参见 [“AVG 更新”一章 >>](#)

上述链接可随时从用户界面中进行访问。一旦您使用某一快速链接运行特定进程，GUI 便会切换到一个新对话框，但这些快速链接依然可用。此外，还会进一步以图形方式描述正在运行的进程。



6.4. 组件概览

“**组件概览**”区域位于 [AVG 用户界面](#) 的中央位置。该区域分为两个部分：

- 已安装的所有组件的概览，它由一个面板组成，其中显示了组件的图标以及关于相应组件是否已激活的信息
- 所选组件的说明

在 **AVG Internet Security 2011** 中，“**组件概览**”部分中含有关于以下组件的信息：

- **Anti-Virus**，可确保您的计算机免遭企图进入您计算机的病毒侵害 - [详细信息 >>](#)
- **Anti-Spyware**，可确保您的计算机免受间谍软件和广告软件侵害 - [详细信息 >>](#)
- **Anti-Spam**，检查所有传入的电子邮件并将不需要的电子邮件标记为“垃圾邮件” - [详细信息 >>](#)
- **Firewall**，控制您的计算机与 Internet 或本地网络上的其它计算机交换数据的方式 - [详细信息 >>](#)
- **Link Scanner**，检查在您的 Internet 浏览器中显示的搜索结果 - [详细信息 >>](#)
- **电子邮件扫描程序**，检查所有传入和传出的邮件是否携带病毒 - [详细信息 >>](#)
- **Resident Shield**，在后台运行并在文件被复制、打开或保存时扫描它们 - [详细信息 >>](#)
- **Family Safety** 有助于监视子女的在线活动，并且防止他们受到不当网站内容的侵害 - [详细信息 >>](#)
- **LiveKive** 用于自动在线备份数据 - [详细信息 >>](#)
- **更新管理器**，控制所有 AVG 更新 - [详细信息 >>](#)
- **许可证**，用于显示许可证号、类型和到期日期 - [详细信息 >>](#)
- **Online Shield**，用于扫描正在通过 Web 浏览器下载的所有数据 - [详细信息 >>](#)
- **Anti-Rootkit**，检测企图掩饰恶意软件的程序和技术 - [详细信息 >>](#)
- **系统工具**，提供 AVG 环境和操作系统信息的详细摘要 - [详细信息 >>](#)
- **PC Analyzer**，提供有关您的计算机状态的信息 - [详细信息 >>](#)
- **Identity Protection** - 是一种防恶意软件组件，主要用于防止身份窃贼窃取宝贵的个人数字资料 - [详细信息 >>](#)
- **Security Toolbar** 可用于直接通过 Internet 浏览器使用所选 AVG 功能 - [详细信息 >>](#)
- **Remote Administration** 仅当已在 [安装过程](#) 中指定要安装此组件时，才会显示在



AVG Business Edition 中

单击任何组件的图标即可在组件概览中突出显示它。同时，该组件的基本功能说明也会显示在用户界面的底部。双击该图标可打开对应组件自身的界面，其中列出了一些基本的统计数据。

在组件图标的上方右键单击鼠标可展开一个上下文菜单；除了打开该组件的图形界面之外，您还可以选择 **“忽略组件状态”**。选择此选项可表明已经知道该组件的错误状态，但出于某种原因想要保持 AVG 的这种状态，而且不想通过 [系统任务栏图标](#) 收到警告。

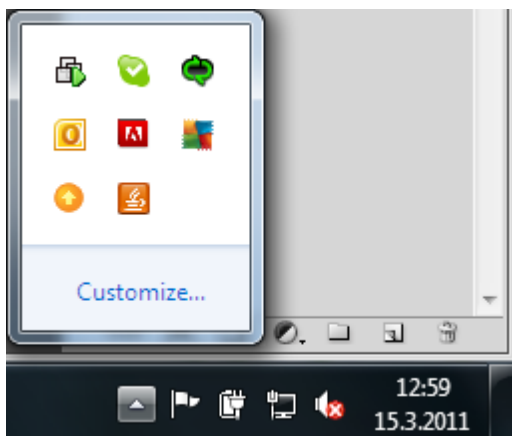
6.5. 统计信息

“统计信息” 区域位于 [AVG 用户界面](#) 的左下部。它提供了关于此程序运行情况的一系列信息：

- **“病毒数据库”** – 告知您当前安装的病毒数据库版本情况
- **“AVG 版本”** – 告知您所安装的 AVG 版本情况（版本号采用的格式为 10.0.xxxx，其中 10.0 是产品系列版本，xx 代表内部版本号）
- **“许可证到期日期”** – 提供了您的 AVG 许可证的到期日期

6.6. 系统任务栏图标

系统任务栏图标（在 Windows 任务栏中）用于指示 **AVG Internet Security 2011** 的当前状态。不论 AVG 主窗口是处于打开状态还是关闭状态，此图标在系统任务栏中始终都是可见的：



如果图标是彩色的 ，则 **系统任务栏图标** 表示所有 AVG 组件均已激活且完全正常运行。此外，如果 AVG 处于错误状态，但您完全清楚这种情况并有意决定 **“忽略组件状态”**，也会显示彩色的 AVG 系统任务栏图标。带感叹号的图标  表示有问题（组件已停用，处于错误状态等）。双击 **系统任务栏图标** 可打开主窗口并对组件进行编辑。

系统任务栏图标还会通过从 AVG 系统任务栏图标打开的弹出窗口，通知当前的 AVG 活动情况以及此程序中可能发生的状态变化情况（例如，计划的扫描或更新自动启动、



Firewall 配置文件切换、组件状态变化、出现错误状态……) :



系统任务栏图标还可以用作可随时访问 AVG 主窗口的快速链接 - 双击此图标即可。通过右键单击 **系统任务栏图标**，可以打开一个简短的上下文菜单，其中提供了以下选项：

- **打开 AVG 用户界面** - 单击此选项可打开 [AVG 用户界面](#)
- **扫描** - 单击可打开
- **Firewall** - 单击可打开 [Firewall](#) 设置选项的上下文菜单，您可以在其中编辑主要参数：[Firewall 状态](#)（*Firewall 已启用 / Firewall 已禁用 / 紧急模式*）、[游戏模式切换](#)和 [Firewall 配置文件](#)
- **运行 PC Analyzer** - 单击可启动 [PC Analyzer](#) 组件
- **运行扫描** - 仅当计算机上当前有扫描正在运行时才会显示此项。对于该扫描，您可以设置其优先级，或者停止或暂停正在运行的扫描。此外，可以使用以下操作：*设置所有扫描的优先级*、*暂停所有扫描*或*停止所有扫描*。
- **立即更新** - 用于立即启动[更新](#)
- **帮助** - 可在起始页上打开帮助文件

6.7. AVG 小工具

AVG 小工具显示在 Windows 桌面上（Windows 边栏）。此应用程序仅在 Windows Vista 和 Windows 7 操作系统中受支持。**AVG 小工具**提供了对最重要的 **AVG Internet Security 2011** 功能的即时访问权限，即[扫描](#)和[更新](#)：



AVG 小工具提供以下快速访问选项：

- **“立即扫描”** - 单击 **“立即扫描”** 链接可直接启动 **“扫描整个计算机”**。您可以在小工具的交替用户界面中观察扫描过程的进度。简要的统计信息概览提供了关于已扫描的对象数量、检测到的威胁和已修复的威胁的信息。在扫描过程中，您随时可



以暂停  或停止  扫描过程。有关扫描结果的详细数据，请参见标准 [扫描结果概览](#) 对话框，该对话框可直接在小工具中通过 [显示详细信息](#) 选项打开（各项扫描结果都将会列在 [边栏小工具扫描](#) 下）。



- “立即更新”单击 [立即更新](#) 链接可直接从该小工具启动 AVG 更新：



- “Twitter 链接” 打开一个新的 [AVG 小工具](#) 界面，其中提供 Twitter 上发布的最新 AVG 馈送的概览。单击 [查看所有 AVG Twitter 馈送](#) 链接可在新窗口中打开 Internet 浏览器，并直接重定向到 Twitter 网站，确切地说是重定向到专用于与 AVG 相关的新闻的网页：



- “Facebook 链接” 在 Internet 浏览器中打开 Facebook 网站，确切地说是打开 [“AVG 社区”](#) 网页



- **LinkedIn**  - 只有网络安装中才有此选项（即前提是已用某个 AVG 企业版许可证安装 AVG）；用其可打开 Internet 浏览器，显示 **AVG SMB 社区** 网站中 LinkedIn 社交网络中的内容
- **PC Analyzer**  - 打开 [PC Analyzer](#) 组件中的用户界面
- **搜索框** - 键入关键字后立即就会用默认 Web 浏览器在新打开的窗口中显示搜索结果



7. AVG 组件

7.1. Anti-Virus

7.1.1. Anti-Virus 原理

防病毒软件的扫描引擎会扫描所有文件和文件操作（打开/关闭文件，等等）是否携带已知病毒。对于检测到的任何病毒，都会阻止其执行任何操作，然后将其清除或隔离。大多数防病毒软件也都采用启发式扫描方法，这种方法会扫描文件有无典型的病毒特征，即所谓的病毒签名。这意味着，如果新病毒包含现有病毒的一些典型特征，则防病毒扫描程序便可以检测到新的未知病毒。

防病毒保护软件的一项重要功能就是不让任何已知病毒在计算机上运行！

由于仅凭一项技术可能不足以检测或识别病毒，因此 **Anti-Virus** 综合运用了多项技术以确保您的计算机不受病毒侵害：

- 扫描 - 搜索表示给定病毒特征的字符串
- 启发式分析 - 在虚拟的计算机环境中对已扫描对象的指令进行动态模拟
- 常规检测 - 检测给定病毒/病毒种群的指令特征

AVG 还能够分析和检测系统中可能不需要的可执行应用程序或 DLL 库。我们将此类威胁称为“可能不需要的程序”（各种间谍软件、广告软件等）。此外，AVG 还会扫描系统注册表是否含有可疑条目，扫描 Internet 临时文件以及跟踪 Cookie，并允许您像处理任何其它感染一样处理所有可能有害的内容。



7.1.2. Anti-Virus 界面



Anti-Virus 组件的界面提供了有关该组件功能的一些基本信息，有关该组件当前状态的信息（**Anti-Virus 组件已激活。**），以及对 **Anti-Virus** 统计信息的简要概述：

- **“病毒定义数量”**—此数字提供了在最新版病毒数据库中定义的病毒计数
- **“数据库发布”**指定数据库上次更新的日期和时间
- **“数据库版本”**定义当前安装的病毒数据库版本号；此版本号将随病毒库的每次更新而递增

此组件的界面中仅有一个操作按钮（**“后退”**）- 按该按钮可返回默认的 [AVG 用户界面](#)（**组件概览**）。

7.2. Anti-Spyware

7.2.1. Anti-Spyware 原理

间谍软件通常定义为一种恶意软件，即在用户不知情或未同意的情况下从用户计算机中收集信息的软件。有些间谍软件应用程序也可能是有意安装的，并且通常包含广告、弹出窗口或其它类型的令人讨厌的软件。

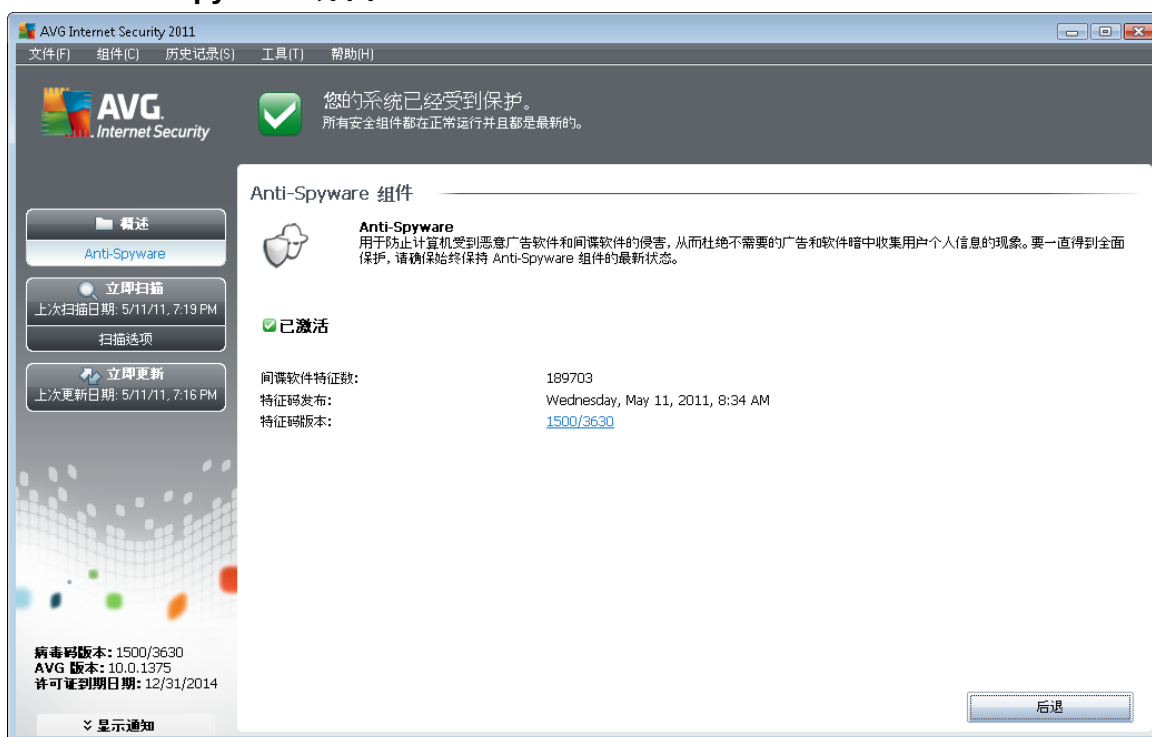
目前，最常见的感染来源是包含具有潜在危险内容的网站。其它一些传播方法，例如通过电子邮件，或通过蠕虫和病毒传播也很普遍。最重要的防护措施是使用始终发挥作用



的后台扫描程序 **Anti-Spyware**，它就像一个常驻保护盾一样，当您运行应用程序时它会在后台对它们进行扫描。

还有一种潜在风险，即恶意软件已在安装 AVG 之前传播到您的计算机中，或者由于疏忽大意，您未将 **AVG Internet Security 2011** 与最新的 [数据库和程序更新](#) 保持同步。因此，AVG 允许您使用扫描功能对计算机进行全面扫描，以检查是否存在恶意软件/间谍软件。它还能够检测休眠和非活动的恶意软件，即已经下载但尚未激活的恶意软件。

7.2.2. Anti-Spyware 界面



Anti-Spyware 组件的界面简要概述了该组件的功能，提供了有关该组件当前状态的信息以及一些 **Anti-Spyware** 统计信息：

- **“间谍软件定义”** - 此数字提供了在最新的间谍软件数据库版本中定义的间谍软件样本计数
- **“数据库发布”** 指定间谍软件数据库的更新日期及时间
- **“数据库版本”** - 定义最新的间谍软件数据库版本号；此版本号将随病毒库的每次更新而递增

此组件的界面中仅有一个操作按钮（**“后退”**） - 按该按钮可返回默认的 [AVG 用户界面](#)（组件概览）。

7.3. Anti-Spam

垃圾邮件是指未经请求的电子邮件，大多以宣传产品或服务为目的，采取群发方式，每次寄给大量的电子邮件地址，充斥收件人的邮箱。垃圾邮件并不包括那些已征得消费者同意而发送的合法的商业电子邮件。垃圾邮件不仅令人厌烦，而且往往含有诈骗信息、病毒或冒犯性内容。

7.3.1. Anti-Spam 原理

AVG Anti-Spam 会检查传入的所有电子邮件，并将不需要的电子邮件标记为垃圾邮件。**AVG Anti-Spam** 可以通过添加特殊的文本字符串来修改电子邮件（已被识别为垃圾邮件的电子邮件）的主题。然后就能在电子邮件客户端中轻松地过滤电子邮件。

AVG Anti-Spam 组件采用多种分析方法来处理每一封电子邮件，可在最大程度上阻止不需要的电子邮件。**AVG Anti-Spam** 使用定期更新的数据库进行垃圾邮件检测。还可以使用 [RBL 服务器](#)（存储着已知的垃圾邮件发送者电子邮件地址的公共数据库），以及向 [白名单](#)（绝不会被标记为垃圾邮件）和 [黑名单](#)（始终都会被标记为垃圾邮件）手动添加电子邮件地址。

7.3.2. Anti-Spam 界面



在 **Anti-Spam** 组件的对话框中，有描述该组件功能的简短文字说明、有关其当前状态的信息，以及以下统计信息：

- **数据库版本** –指定垃圾邮件数据库的更新和发布日期及时间
- **Spamcatcher 版本** –定义反垃圾邮件引擎的最新版本号



- **“已处理的电子邮件数量”** 指定自从上次启动反垃圾邮件引擎以来已处理的电子邮件数量
- **“垃圾电子邮件数量”** 指定所有已扫描的电子邮件中，标记为垃圾电子邮件的邮件数量
- **“网络钓鱼电子邮件数量”** 指定所有已扫描的电子邮件中，确定为网络钓鱼尝试的邮件数量

“Anti-Spam”对话框进一步提供了 [“工具”/“高级设置”](#) 链接。使用该链接可重定向到用于对所有 AVG Internet Security 2011 组件进行高级配置的环境。

请注意：所有 AVG 组件均已由软件供应商设置完毕，可提供最佳性能。除非必要，否则请勿更改 AVG 配置。对设置的所有更改均应由经验丰富的用户执行。

此组件的界面中仅有一个操作按钮（**“后退”**）- 按该按钮可返回默认的 [AVG 用户界面](#)（组件概览）。

7.4. Firewall

防火墙是一个系统，用于通过阻止/允许通信在两个或更多网络之间强制执行访问控制策略。防火墙包含一组用于保护内部网络免受外来攻击（通常来自 Internet）的规则，并控制着通过每个网络端口的所有通信。根据定义的规则对这些通信进行评估，然后决定是允许还是禁止它们。如果防火墙识别到任何入侵企图，它会阻止这种企图，不允许入侵者访问计算机。

防火墙经过配置后会允许或拒绝通过指定端口的或指定软件应用程序的内部/外部通信（双向、传入或传出）。例如，防火墙可以配置为仅允许 Web 数据使用 Microsoft Explorer 流入和流出。通过任何其它浏览器传送 Web 数据的任何企图都会被阻止。

防火墙会保护可据以识别您个人身份的信息，以免在未经您同意的情况下将它们从您的计算机中发出。它控制着您的计算机与 Internet 或本地网络上的其它计算机交换数据的方式。在组织中，防火墙还保护着每台计算机免遭网络中其它计算机上的内部用户发起的攻击。

建议：一般而言，建议不要在一台计算机上使用多个防火墙。安装更多的防火墙并不能增强计算机的安全性。更有可能的是，这两个应用程序之间反倒会发生一些冲突。因此，我们建议在您的计算机上仅使用一个防火墙，停用所有其它防火墙，从而消除可能发生冲突的风险以及与此相关的任何问题。

7.4.1. Firewall 原理

在 AVG 中，**Firewall** 组件控制着通过计算机每个网络端口的所有通信。**Firewall** 会根据定义的规则，对您计算机上运行的要连接至 Internet/本地网络的应用程序，以及尝试从计算机外部连接至您的 PC 的应用程序进行评估。对于每个应用程序，**Firewall** 都会确定是否允许其通过这些网络端口进行通信。默认情况下，如果应用程序处于未知状态（即未定义相应的 **Firewall** 规则），**Firewall** 将询问您是允许还是阻止其通信尝试。

注：AVG Firewall 不可用于服务器平台！



AVG Firewall 的功能包括：

- 自动允许或阻止已知应用程序的通信尝试，或提示您进行确认
- 根据您的需要应用包含预定义规则的完整[配置文件](#)
- [在连接至不同的网络或使用不同的网络适配器时自动切换配置文件](#)

7.4.2. Firewall 配置文件

[Firewall](#) 允许基于以下情况定义特定的安全规则：您的计算机是域成员、独立的计算机，还是笔记本电脑。其中每个选项都需要设置一种不同的保护级别，具体级别可在各自的配置文件中查看。简言之，[Firewall](#) 配置文件就是 [Firewall](#) 组件的一项特定配置，您可以使用多项此类预定义配置。

可用配置文件

- **全部允许** - 是制造商预先设置好的 [Firewall](#) 系统配置文件，始终都会显示出来。激活此配置文件后，将允许所有网络通信而不应用任何安全策略规则，就如同关闭 [Firewall](#) 保护一样（即允许所有应用程序，但仍检查数据包 -若要完全禁用所有过滤功能，您需要禁用 Firewall）。您不得复制或删除此系统配置文件，也不得修改其设置。
- **全部阻止** - 是制造商预先设置好的 [Firewall](#) 系统配置文件，始终都会显示出来。激活此配置文件后，所有网络通信都将被阻止，计算机既不能从外部网络进行访问，也不能与外部进行通信。您不得复制或删除此系统配置文件，也不得修改其设置。
- **自定义配置文件：**
 - **直连到 Internet** - 适用于直接连接到 Internet 的普通家用台式计算机，或在安全的公司网络以外连接到 Internet 的笔记本电脑。如果您是在家中进行连接的或者是在没有中央控制措施的小型公司网络中，请选择此选项。此外，在旅行中或从多种未知且可能有危险的场所（网吧、酒店房间等）将笔记本电脑联网时，也请选择此选项。在这种情况下将创建更具限制性的规则，因为会假定这些计算机未采取额外的保护措施，因此需要得到最大程度的保护。
 - **域中的计算机** - 适用于本地网络（如学校或公司网络）中的计算机。假定网络受某些其它措施保护，因此其安全级别可低于独立计算机。
 - **小型家庭或办公网络** - 适用于小型网络（如家庭或小型企业）中的计算机，这种网络通常只有几台计算机连在一起，没有中央管理员。

配置文件切换

借助于配置文件切换功能，[Firewall](#) 可在使用特定网络适配器或在连接到特定类型的网络



时自动切换到预定义的配置文件。如果尚未为某一网络区域分配配置文件，则在下次连接到此区域时，[Firewall](#) 将显示一个对话框，要求您分配配置文件。

可在“[区域和适配器配置文件](#)”对话框中对所有本地网络接口或区域指定配置文件并指定其它设置；如果不想使用该功能，还可从中将其禁用（然后会对任何类型的连接使用默认配置文件）。

通常，使用多种连接的笔记本电脑用户会发现此功能十分有用。如果您使用的是台式机，并且始终只使用一种类型的连接（例如有线连接到 Internet），则无需费力去设置配置文件切换，因为您大概永远都不会用到它。

7.4.3. Firewall 界面



Firewall 的界面提供了有关该组件的功能及其状态的一些基本信息，以及简要的 **Firewall** 统计信息概览：

- **Firewall 已启用** – Firewall 上次启动至今所经过的时间
- **已阻止的数据包数** – 检查的数据包总数中已阻止的数据包数
- **数据包总数** – 在 Firewall 运行期间检查的数据包总数

Firewall 设置

- “**选择 Firewall 配置文件**” – 请从下拉菜单中选择预定义的配置文件之一 – 有两个配置文件始终都提供（名为“**全部允许**”和“**全部阻止**”的默认配置文件），其它配



置文件是您在 [“Firewall 设置”](#) 中的 [“配置文件”](#) 对话框中通过编辑配置文件手动添加的。

- **启用游戏模式** - 选中此选项可确保在运行全屏应用程序（玩游戏、播放演示文稿、看电影等）时，[Firewall](#) 不会显示对话框询问是允许还是阻止不明应用程序的通信。如果此时有未知应用程序企图通过网络进行通信，[Firewall](#) 将自动根据当前配置文件中的设置允许或阻止这一企图。**注：**在启用了游戏模式的情况下，所有计划的任务（扫描、更新）都将推迟执行，直到全屏应用程序关闭为止。
- **Firewall 状态：**
 - **“已启用 Firewall”** - 选中此选项可允许与所选 [Firewall](#) 配置文件中定义的那套规则中指定为 允许 的那些应用程序通信
 - **已禁用 Firewall** - 此选项用于彻底禁用 [Firewall](#)，会允许传输所有网络通信内容，但不会对其进行检查！
 - **紧急模式(阻止所有 Internet 通信)** - 选中此选项将阻止通过每个网络端口的所有通信内容；[Firewall](#) 仍在运行，但所有网络通活动信都会被停止

请注意：所有 AVG 组件均已由软件供应商设置完毕，可提供最佳性能。除非必要，否则请勿更改 AVG 配置。对设置的任何更改只应当由经验丰富的用户执行。如果需要更改 Firewall 配置，请选择系统菜单项 **“工具”“Firewall 设置”**；然后在新打开的 [“Firewall”设置](#) 对话框中编辑 Firewall 配置。

控制按钮

- **“重新生成配置”** 单击此按钮将覆盖当前 **Firewall** 配置，并恢复到基于自动检测的默认配置。
- **“保存更改”** - 按此按钮可保存并应用在此对话框中所做的任何更改
- **“取消”** - 按此按钮可返回默认的 [AVG 用户界面](#)（组件概览）

7.5. Link Scanner

7.5.1. Link Scanner 原理

LinkScanner 可以为您防范 Web 上数量日益增加的 昙花一现 式威胁。这些威胁可隐藏在任何类型的网站上，从政府到大型知名品牌乃至小型企业的网站，并且它们很少在那些网站上逗留超过 24 小时。**LinkScanner** 分析您所查看的任何网页上的所有链接背后的网页，并确保它们在唯一重要的时刻（即在您即将点击该链接时）是安全的，从而为您提供保护。

LinkScanner 技术包括两项功能，即 [Search-Shield](#) 和 [Surf-Shield](#)：

- [Search-Shield](#) 包含已知危险的网站（URL 地址）列表。在通过 Google、Yahoo! JP、WebHledani、Yandex、百度、Bing、AOL、Altavista、EarthLink、Ask、Seznam、



eBay、Twitter、Digg 或 SlashDot 进行搜索时，会按此列表对所有搜索结果进行检查，并显示评判图标（对于 Yahoo! 搜索结果，仅会显示 遭到漏洞利用的网站 评判图标）。

- **Surf-Shield** 用于扫描用户正在访问的网站的内容，而不考虑网站地址。即使某些网站未受到 **Search-Shield** 的保护（例如，创建新的恶意网站时，或以前清除的网站现在包含某种恶意软件时），**Surf-Shield** 也会在您尝试访问该网站时进行检测和阻止。

注意： Link Scanner 不适用于服务器平台！

7.5.2. Link Scanner 界面

LinkScanner 组件的界面简要说明了该组件的功能，并提供了有关该组件当前状态的信息。此外，其中还包含关于最新 **LinkScanner** 数据库版本号的信息（**LinkScanner** 版本）。



LinkScanner 设置

在此对话框的底部，您可以对若干选项进行编辑：

- **启用 Search-Shield** - （默认情况下已启用）：在对 Google、Yahoo!JP、WebHledani、Yandex、百度、Bing、AOL、AltaVista、EarthLink、Ask、Seznam、eBay、Twitter、Digg 或 SlashDot 等搜索引擎所返回的网站内容进行事先检查后，就所执行的搜索显示警告通知图标。
- **启用 Surf-Shield** - （默认情况下已启用）：主动（实时）防范访问网站时遇到的



漏洞利用网站。当用户通过 Web 浏览器（或任何其它使用 HTTP 的应用程序）访问已知的恶意网站连接及其漏洞利用内容时，将会对这些网站及其内容进行阻止。

7.5.3. Search-Shield

如果启用 **Search-Shield** 后在 Internet 上进行搜索，则会对最常用的搜索引擎返回的所有搜索结果（Google、Yahoo!JP、WebHledani、Yandex、百度、Bing、AOL、AltaVista、EarthLink、Ask、Seznam、eBay、Twitter、Digg 和 SlashDot）返回的所有搜索结果进行评估，看是否为危险或可疑链接。通过检查这些链接并标记恶意链接，[AVG Link Scanner](#) 在您点击危险或可疑链接前就发出警告，从而可以确保您只访问安全网站。

评估搜索结果页面上的某个链接时，将在该链接旁边显示一个图形符号，用以通知正在进行链接验证。评估完成时，将显示各自的信息图标：

 所链接的页面安全（这种图标不会对安全的 Yahoo! JP 搜索结果显示）。

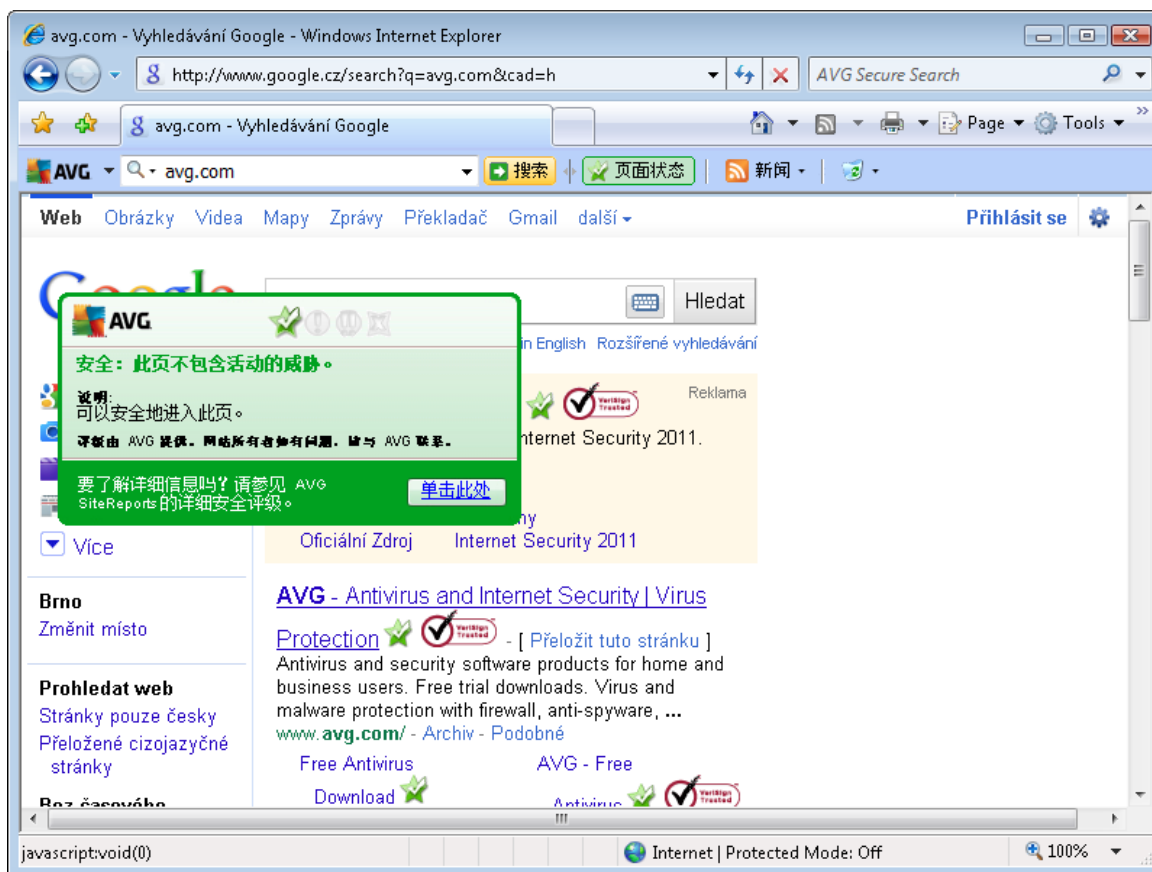
 所链接的页面不包含威胁，但有些可疑（来源或动机可疑，因此不建议进行电子购物等）。

 所链接的页面本身是安全的，但包含指向确实危险的页面的链接；或者，虽然此刻未直接施用任何威胁，但代码可疑。

 所链接的页面含有活动的威胁！为您的安全考虑，不允许访问此页面！

 无法访问所链接的页面，因此无法扫描。

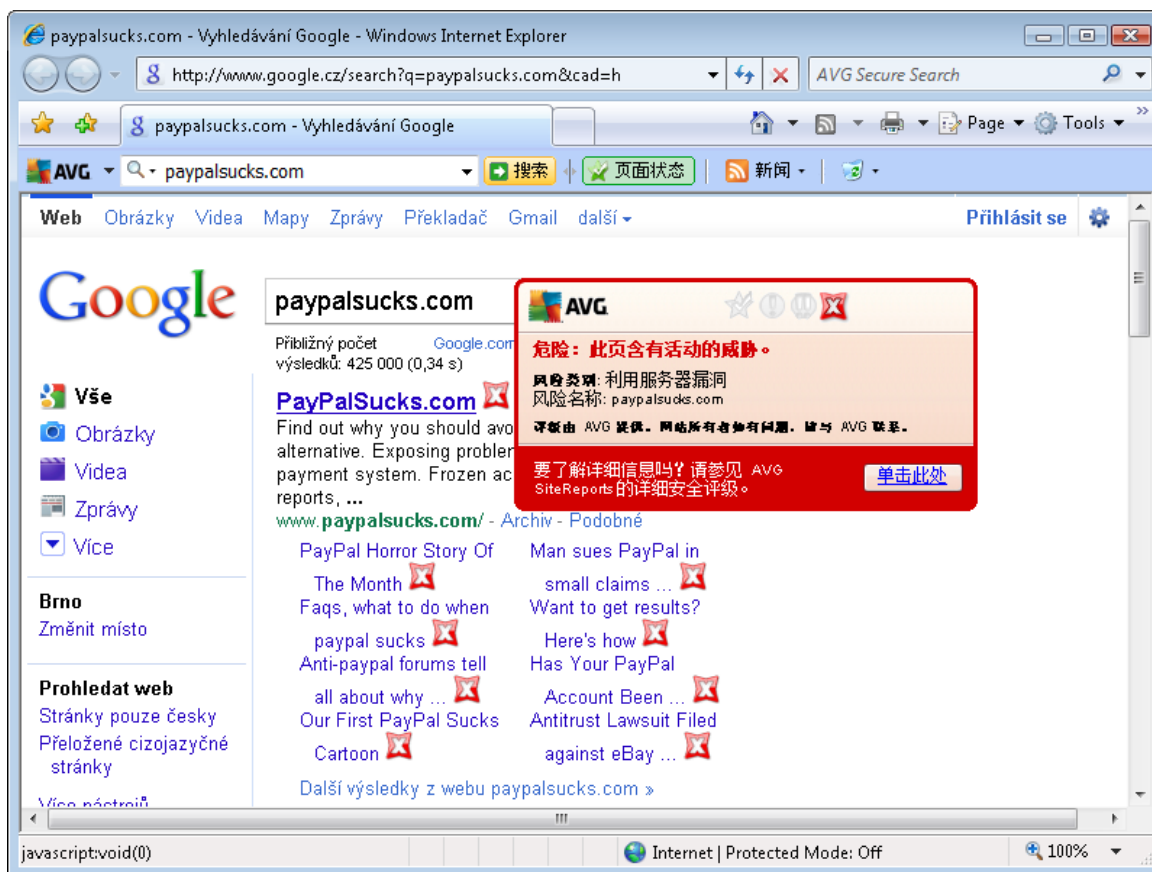
悬停在某个等级图标上时，将显示有关存在问题的特定链接的详细信息。显示出来的信息包括有关威胁的其它详细信息（如果有）：



7.5.4. Surf-Shield

此功能强大的防护工具可阻止您尝试打开的任何网页上的恶意内容，防止其被下载到您的计算机上。启动该功能后，当您单击指向危险站点的链接或键入其 URL 时将自动阻止您打开该网页，从而保护您的系统免遭意外感染。需要牢记的是，只要访问受感染站点，被利用的网页就可能会感染您的计算机。因此，当您访问包含漏洞利用或其它严重威胁的危险网页时，[AVG Link Scanner](#) 将阻止您的浏览器显示该网页。

如果您确实遇到恶意网站，那么在您的 Web 浏览器中，[AVG Link Scanner](#) 将使用类似下面的屏幕警告您：



进入此类网站会带来很大的风险，建议不要进入！

7.6. Resident Shield

7.6.1. Resident Shield 原理

Resident Shield 组件可对计算机进行持续的保护。它会扫描正在被打开、保存或复制的每一个文件，并守护计算机系统区域。当 **Resident Shield** 在被访问的文件中发现病毒时，它会停止当前正在执行的操作，不允许病毒激活自身。一般情况下，您甚至觉察不到这一过程，因为它在后台运行，只会在发现威胁时通知您；同时，**Resident Shield** 还会阻止威胁激活并将其删除。**Resident Shield** 是在系统启动期间被加载到计算机内存中的。

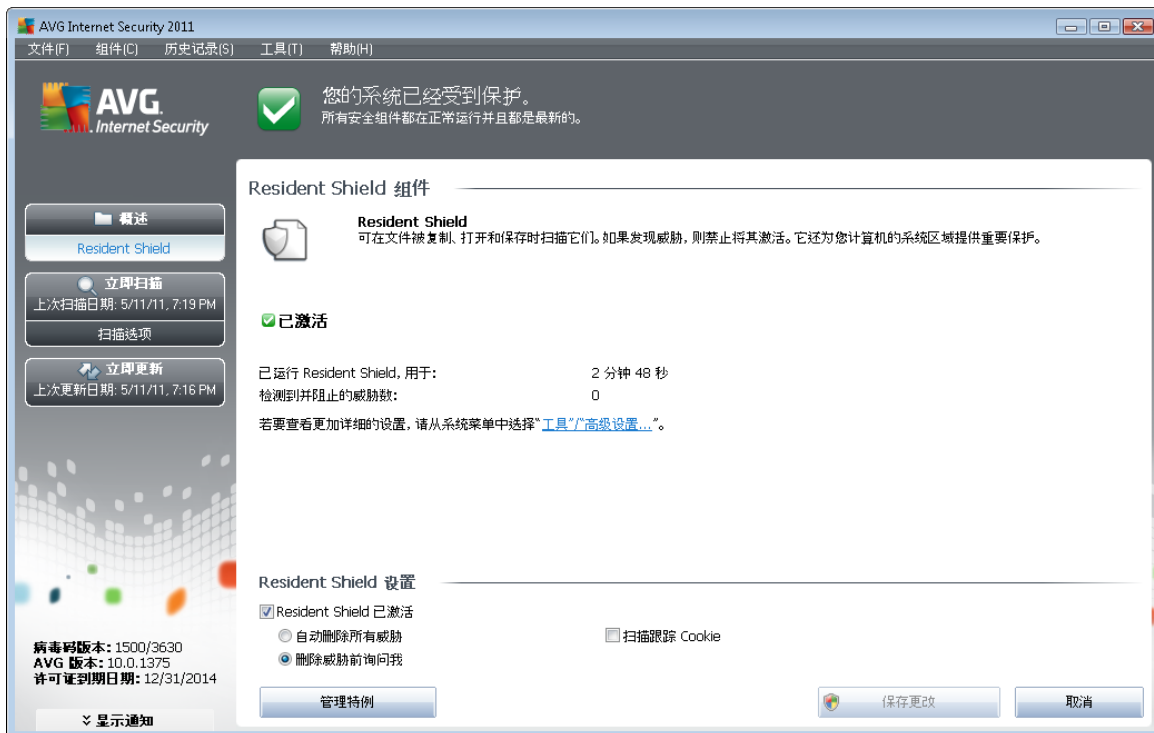
Resident Shield 的功能包括：

- 扫描是否存在特定类型的可能威胁
- 扫描可移动介质（闪存盘等）
- 扫描带有特定扩展名或根本不带扩展名的文件
- 允许存在不纳入扫描范围内的特例 – 永远都不应被扫描的特定文件或文件夹



警告：*Resident Shield* 在计算机启动期间被加载到计算机内存中，请务必让它始终保持启用状态，这一点至关重要！

7.6.2. Resident Shield 界面



除了 **Resident Shield** 功能的概览以及关于该组件状态的信息外，**Resident Shield** 界面还提供了某些统计数据：

- **Resident Shield 运行所持续的时间** - 提供了自最近一次启动该组件以来经过的时间
- **检测到并阻止的威胁数** - 被阻止运行/打开的检测到的感染数（如果需要，可重置此值；例如出于统计需要重置此值 - 为此请单击 **重置值**）

Resident Shield 设置

此对话框的底部有一个名为 **“Resident Shield 设置”** 的区域，在此区域中您可以编辑该组件功能的一些基本设置（与所有其它组件一样，其详细配置可通过系统菜单的 **“工具”/“高级设置”** 项进行访问）。

通过 **“Resident Shield 已激活”** 选项可轻松启用/禁用常驻保护功能。默认情况下，此功能已启用。在启用了常驻保护功能的情况下，您可以进一步决定应如何处理（删除）可能检测到的感染：

- o 自动删除（**“自动删除所有威胁”**）



- o 或在用户同意后方可删除（**“删除威胁前询问我”**）

此选项对安全级别无影响，只是体现了您的使用偏好而已。

无论选择二者中的哪一个，您都仍然可以选择是否要**“扫描跟踪 Cookie”**。在特定的情况下，您可以启用此选项以达到最高的安全级别，但默认情况下它已禁用。（Cookie 是服务器发送到 Web 浏览器的文本块，之后浏览器每次访问该服务器时都会将其原封不动地发回。HTTP Cookie 用于验证、跟踪和维护有关用户的特定信息，例如网站首选项或电子购物车中的内容）。

请注意：所有 AVG 组件均已由软件供应商设置完毕，可提供最佳性能。除非必要，否则请勿更改 AVG 配置。对设置的任何更改只应当由经验丰富的用户执行。如果需要更改 AVG 配置，请选择系统菜单项**工具/高级设置**，然后在新打开的[AVG 高级设置](#)对话框中编辑 AVG 配置。

控制按钮

Resident Shield 界面中提供的控制按钮如下：

- **管理特例** - 打开 **“Resident Shield - 排除项目”** 对话框，在此对话框中您可以定义应被排除在 [Resident Shield](#) 扫描范围之外的文件夹和文件
- **保存更改** - 按此按钮可保存并应用在此对话框中所做的任何更改
- **取消** - 按此按钮可返回默认的 [AVG 用户界面](#)（组件概览）

7.6.3. Resident Shield 检测

Resident Shield 可在文件被复制、打开或保存时扫描它们。当检测到病毒或任何类型的威胁时，系统会立即通过下面的对话框向您发出警告：



在此警告对话框中，您将找到关于经检测被认定为受感染的文件的数据（文件名）、识



别到的感染的名称（*威胁名称*），以及指向[病毒百科全书](#)的链接，如果所检测到感染是已知的，您可以在病毒百科全书中找到关于该感染的详细信息（*更多信息*）。

另外，您必须决定应立即采取什么操作 - 可用选项如下：

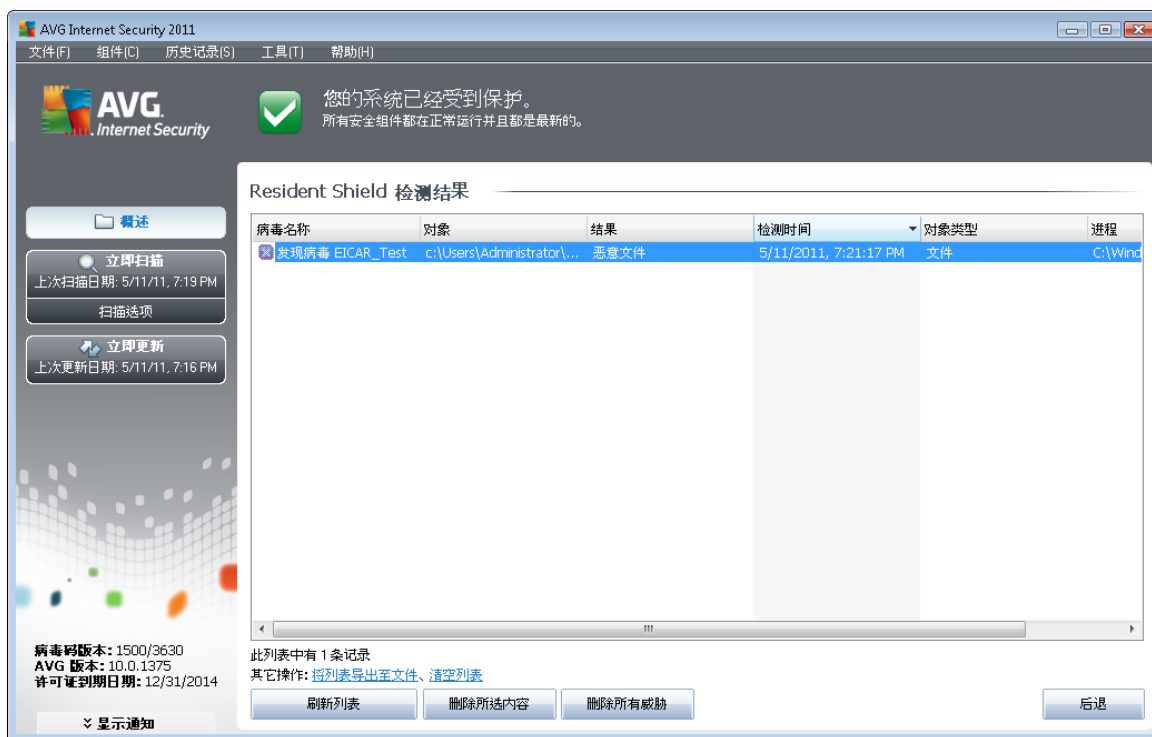
请注意，并非所有选项都始终出现，这取决于具体条件（受感染文件的类型及其位置）！

- **“以超级用户身份删除威胁”** - 如果您认为您作为普通用户可能没有足够的权限来删除此威胁，请选中此框。超级用户拥有很高的访问权限，如果威胁位于某个系统文件夹中，那么您可能需要选中此复选框才能成功删除它。
- **“修复”** - 仅当检测到的感染可修复时才会显示此按钮。然后将感染从文件中删除，并将文件恢复原始状态。如果文件本身是病毒，使用此功能可将其删除（即转移到[病毒库](#)）
- **“移至库”** - 将病毒移至 AVG [病毒库](#)
- **“转至文件”** - 此选项用于将您重定向到可疑对象的确切位置（打开一个新的 Windows 资源管理器窗口）
- **“忽略”** - 我们极力建议，若非绝对必要，请勿使用此选项！

注：检测到的对象可能会大于病毒库中的可用空间。如果情况如此，则会在尝试将已受到感染的对象移到病毒库中时弹出警告消息，就所发生的问题发出通知。但病毒库大小可以编辑。病毒库大小指定为硬盘实际大小的可调比例。要加大病毒库，请通过 [AVG 高级设置](#) 中的 **限制病毒库大小** 选项，转到 [病毒库](#) 对话框。

此对话框的底部有一个链接 **“显示详细信息”** 单击此链接可打开一个弹出式窗口，其中包含关于检测到感染时正在运行的进程的详细信息，以及该进程的识别号。

[Resident Shield](#) 检测到的所有威胁的完整概览可在 **“Resident Shield 检测”** 对话框中找到，可通过系统菜单选项 [“历史记录”](#) / **“Resident Shield 检测”** 访问该对话框：



“Resident Shield 检测” 提供了经 **Resident Shield** 检测而被评估为有危险并且已被修复或移至 **病毒库** 的对象概览。对于检测到的每个对象，提供了以下信息：

- **“感染”**–对检测到的对象的描述（甚至可能就是其名称）
- **“对象”**–对象的位置
- **“结果”**–对检测到的对象执行的操作
- **“检测时间”**–检测到此对象的日期和时间
- **“对象类型”**–检测到的对象的类型
- **“进程”**–通过执行何种操作来调出有潜在危险的对象以便能够检测到它

在此对话框底部的列表下方，显示了上面列出的检测到的对象总数信息。此外，您还可以将检测到的对象的整个列表导出到一个文件中（**“将列表导出至文件”**），以及删除所有检测到的对象条目（**“清空列表”**）。单击 **“刷新列表”** 按钮将更新 **Resident Shield** 检测到的结果列表。按 **“后退”** 按钮可切换回默认的 **AVG 用户界面**（组件概览）。

7.7. Family Safety

AVG Family Safety 有助于防止子女访问不当网站，查看不当媒体内容，以及执行不当在线搜索，也可以就子女的在线活动向家长提供报告。可对每个子女设置相应保护级别，通过各不相同的登录信息分别对其进行监控。

仅当计算机中装有 **AVG Family Safety** 产品时，该组件才会处于活动状态。如果未安装



AVG Family Safety 产品，请单击 **AVG Internet Security 2011** 用户界面中的相应图标，然后就会重定向到该产品的网站，从中可找到全部所需详细信息。

7.8. AVG LiveKive

AVG LiveKive 可将所有文件、照片和音乐自动备份到一个安全的位置，这样就可以将其与家人和朋友分享，通过任何能上网的设备对其进行访问，包括 iPhone 和 Android 设备。

仅当计算机中装有 **AVG LiveKive** 产品时，该组件才会处于活动状态。如果未安装 **AVG LiveKive** 产品，请单击 **AVG Internet Security 2011** 用户界面中的相应图标，然后就会重定向到该产品的网站，从中可找到全部所需详细信息。

7.9. 电子邮件扫描程序

电子邮件是最常见的病毒和特洛伊木马来源之一。网络钓鱼和垃圾邮件更加剧了电子邮件存在的风险。免费电子邮件帐户更有可能收到此类恶意电子邮件（因为它们极少利用反垃圾邮件技术），而家庭用户则非常依赖此类电子邮件。此外，家庭用户在不明网站上冲浪以及在在线表单中填写个人数据（例如他们的电子邮件地址）时，会增加遭受通过电子邮件发起的攻击的风险。公司通常使用企业电子邮件帐户并利用反垃圾邮件过滤器等技术来降低风险。

7.9.1. 电子邮件扫描程序原理

个人电子邮件扫描器可自动扫描传入/传出的电子邮件。您可以将它与在 AVG 中没有自己的插件的电子邮件客户端搭配使用（但也可用于扫描 AVG 通过特定插件来支持的电子邮件客户端的电子邮件，即 Microsoft Outlook 和 The Bat）。它主要与 Outlook Express、Mozilla、Incredimail 等电子邮件应用程序搭配使用。

在 AVG [安装](#)期间，自动创建了用于实施电子邮件控制的服务器：一个用于检查传入的电子邮件，另一个用于检查传出的电子邮件。通过这两个服务器可自动在端口 110 和端口 25（用于发送/接收电子邮件的标准端口）上检查电子邮件。

电子邮件扫描程序担当电子邮件客户端与 Internet 上的电子邮件服务器之间的接口。

- **对于传入的邮件：**从服务器收到邮件时，**电子邮件扫描程序**组件会测试它是否携带病毒，删除受感染的附件并添加验证信息。检测到病毒后，会立即将其隔离在**病毒库**中。随后再将邮件传递给电子邮件客户端。
- **对于传出的邮件：**电子邮件客户端将邮件发送到电子邮件扫描程序；电子邮件扫描程序测试该邮件及其附件是否携带病毒，然后将该邮件发送至 SMTP 服务器（默认情况下已禁用扫描传出邮件的功能，可以手动加以设置）。

注：AVG E-mail Scanner 不可用于服务器平台！



7.9.2. 电子邮件扫描程序界面



在 **电子邮件扫描程序** 组件的对话框中，您可以找到描述该组件功能的简要文本、有关其当前状态的信息，以及以下统计信息：

- **已扫描的电子邮件总数** - 自 **电子邮件扫描程序** 上次启动以来扫描了多少封电子邮件（如果需要则可重置此值；例如，可出于统计目的重置此值，单击 **重置值** 即可）
- **“发现并阻止的威胁数”** - 提供自 **电子邮件扫描程序** 上次启动以来在电子邮件中检测到的感染数目
- **“已安装的电子邮件保护插件”** - 有关特定电子邮件保护插件（指您默认安装的电子邮件客户端）的信息

电子邮件扫描程序设置

此对话框的底部有一个名为 **“电子邮件扫描程序设置”** 的区域，在此区域中您可以编辑该组件功能的一些基本设置：

- **“扫描传入的邮件”** - 选中此项可指定应对被传递到您帐户的所有电子邮件进行病毒扫描。默认情况下已启用此项，建议不要更改此设置！
- **“扫描传出的邮件”** - 选中此项可确认应对从您的帐户发出的所有电子邮件进行病毒扫描。默认情况下，此项已禁用。



- **“扫描电子邮件时显示通知窗口”** 选中此选项可确认自己想要在通过 [电子邮件扫描程序](#) 组件扫描邮件的过程中，通过显示在系统任务栏中的 AVG 图标上的通知对话框得到通知。默认情况下已启用此项，建议不要更改此设置！

电子邮件扫描程序 组件的高级配置可通过系统菜单的 **“工具”/“高级设置”** 项进行访问；但建议仅限经验丰富的用户使用高级配置！

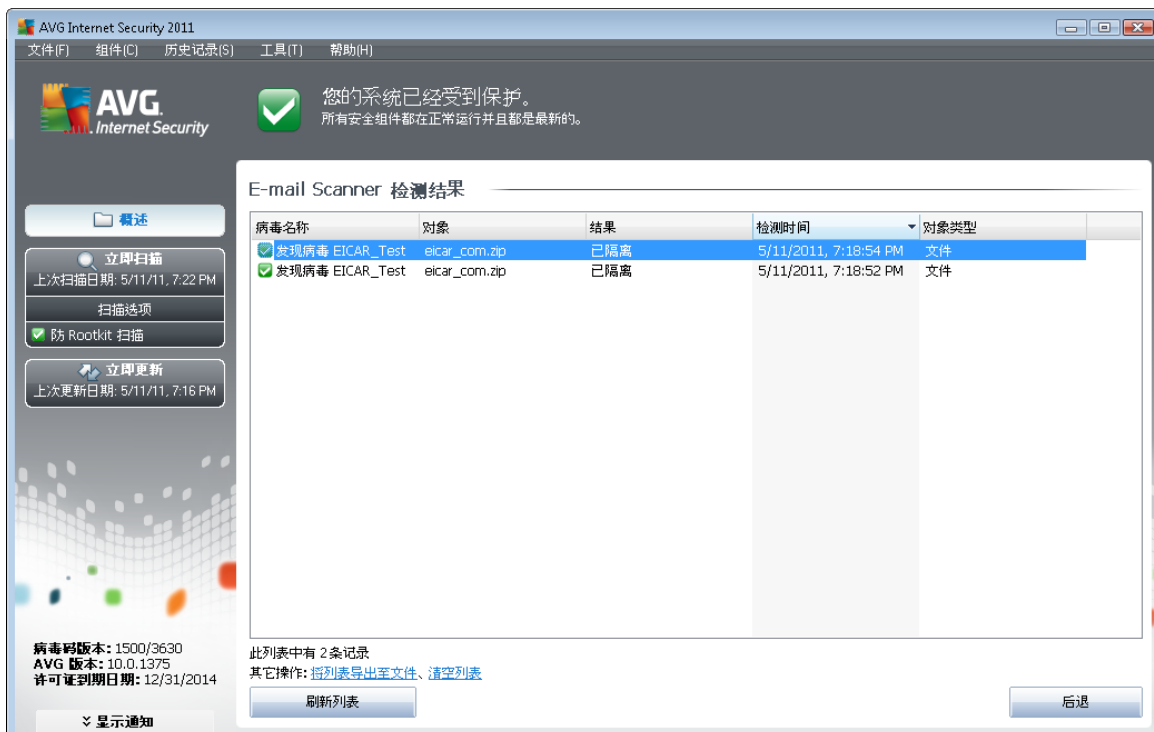
请注意：所有 AVG 组件均已由软件供应商设置完毕，可提供最佳性能。除非必要，否则请勿更改 AVG 配置。对设置的任何更改只应当由经验丰富的用户执行。如果需要更改 AVG 配置，请选择系统菜单项 **工具/高级设置**，然后在新打开的 [AVG 高级设置](#) 对话框中编辑 AVG 配置。

控制按钮

电子邮件扫描程序 界面中提供的控制按钮如下：

- **保存更改** - 按此按钮可保存并应用在此对话框中所做的任何更改
- **取消** - 按此按钮可返回默认的 [AVG 用户界面](#)（组件概览）

7.9.3. 电子邮件扫描程序检测



在 **“电子邮件扫描程序检测”** 对话框（可通过系统菜单选项 **历史记录/“电子邮件扫描程序检测”** 来访问）中，您可以看到 [电子邮件扫描程序](#) 组件检测到的所有结果的列表。对于检测到的每个对象，提供了以下信息：

- **“感染”** - 对检测到的对象的描述（甚至可能就是其名称）



- **“对象”**–对象的位置
- **“结果”**–对检测到的对象执行的操作
- **“检测时间”**–检测到此可疑对象的日期和时间
- **“对象类型”**–检测到的对象的类型

在此对话框底部的列表下方，显示了上面列出的检测到的对象总数信息。此外，还可以将列出的所有检测到的对象都导出到文件中（**“将列表导出至文件”**），也可删除检测到的对象的所有相关条目（**“清空列表”**）。

控制按钮

“电子邮件扫描程序检测”界面中提供的控制按钮如下：

- **“刷新列表”**–更新检测到的威胁列表
- **“返回”**–切换回之前显示的对话框

7.10. 更新管理器

7.10.1. 更新管理器原理

如果不能得到定期更新，任何一款安全软件都无法保证能够真正防范各种类型的威胁！病毒编写者一直在寻找软件和操作系统中可以利用的新漏洞。每天都会出现新的病毒、新的恶意软件、新的黑客攻击。因此，软件供应商都在不断地发布更新和安全补丁，以修复被发现的任何安全漏洞。

定期更新 AVG 至关重要！

更新管理器可帮助您管理定期更新。在此组件中，您可以计划从 Internet 或本地网络自动下载更新文件。如果可能，每天都应进行基本病毒定义更新。不太急需的程序更新可以每周进行一次。

注：请留意 [AVG 更新](#) 一章，了解有关更新类型和更新级别的更多信息！



7.10.2. 更新管理器界面



更新管理器的界面显示有关该组件的功能及其当前状态的信息，并提供相关统计数据：

- **最新更新** - 用于详细说明上次数据库更新的日期和时间
- **病毒数据库版本** - 定义当前安装的病毒数据库版本号；此版本号将随病毒库的每次更新而递增
- **下次计划更新** - 用于详细说明下次数据库更新的日期和时间

更新管理器设置

在此对话框的底部，可以找到 **“更新管理器设置”** 区域，在此区域中，您可以对更新过程启动规则进行一些更改。您可以定义是希望自动下载更新文件（**“启动自动更新”**）还是希望仅在需要时下载。默认情况下，**启动自动更新**选项已启用，我们建议将其保留此状态！定期下载最新的更新文件对于任何安全软件的正常运行都是至关重要的！

此外，您还可以定义应在何时启动更新：

- **“定期”** - 定义时间间隔
- **“按特定时间间隔”** - 定义应启动更新的确切日期和时间

默认情况下，更新设置为每 4 小时启动一次。强烈建议保留此设置，若非必要，请勿更改！



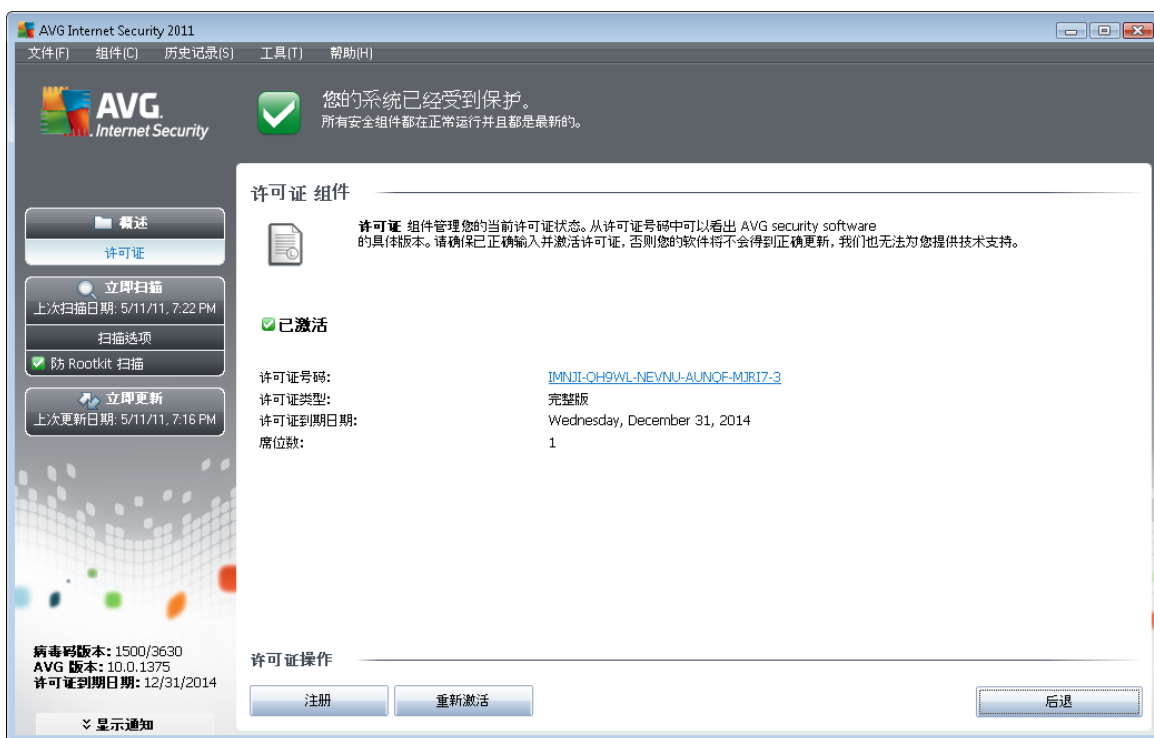
请注意：所有 AVG 组件均已由软件供应商设置完毕，可提供最佳性能。除非必要，否则请勿更改 AVG 配置。对设置的任何更改只应当由经验丰富的用户执行。如果需要更改 AVG 配置，请选择系统菜单项**工具/高级设置**，然后在新打开的 [AVG 高级设置](#) 对话框中编辑 AVG 配置。

控制按钮

更新管理器界面中提供的控制按钮如下：

- **立即更新** - 用于在需要时启动 [立即更新](#)
- **保存更改** - 按此按钮可保存并应用在此对话框中所做的任何更改
- **取消** - 按此按钮可返回默认的 [AVG 用户界面](#)（组件概览）

7.11. 许可证



在 **许可证** 组件的界面中，有描述该组件功能的简短文字说明、有关其当前状态的信息，以及以下信息：

- **许可证号码** - 提供您的许可证号码的截短形式（出于安全考虑，不显示最后四个符号）。当输入您的许可证号码时，您必须确保其绝对精确并完全按照如图所示键入它。因此，我们强烈建议在对许可证号码进行任何操作时始终使用 **复制和粘贴** 方法。
- **许可证类型** - 指定所安装产品的类型。



- **许可证到期日期** - 此日期决定了您的许可证的有效期。如果您希望在此日期后继续使用 **AVG Internet Security 2011**，您必须更新您的许可证。许可证更新可在 [AVG 网站](http://www.avg.com/) 上在线进行。
- **席位** - 您有权在多少个工作站上安装您的 **AVG Internet Security 2011**。

控制按钮

- **注册** - 用于连接到 AVG 网站 (<http://www.avg.com/>) 的注册页面。请填写您的注册数据；只有注册了自己的 AVG 产品的客户才能享受到免费的技术支持。
- **重新激活** - 用于打开“**激活 AVG**”对话框，其中有 [安装过程中](#) 在“**对 AVG 进行个性化设置**”对话框中输入的数据。在此对话框中，您可以输入您的许可证号码来替换销售号码（您安装 AVG 时使用的号码）或替换原来的许可证号码（例如在升级到新的 AVG 产品时）。

注：如果使用的是试用版 **AVG Internet Security 2011**，这两个按钮会显示为“**立即购买**”和“**激活**”，以便您立即购买该程序的完整版。对于通过销售号码安装的 **AVG Internet Security 2011**，这两个按钮显示为“**注册**”和“**激活**”。

- **返回** - 按该按钮可返回默认的 [AVG 用户界面](#)（组件概览）。

7.12. 远程管理



仅当已安装产品的企业版时，**远程管理**组件才会显示在 **AVG Internet Security 2011** 的用户界面中（请参见 [组件许可证](#)）。在“**远程管理**”对话框中，您可以找到关于该组件是否



处于活动状态并连接到服务器的信息。**远程管理**组件的所有设置都将在 **“高级设置”** **“远程管理”** 中进行。

有关该组件在 AVG Remote Administration 系统中的选项和功能的详细说明，请参阅专门用于此主题的特定文档。该文档在 [AVG 网站 \(www.avg.com\)](http://www.avg.com) 上的 **“支持中心”** **“下载”** **“文档”** 部分可供下载。

控制按钮

- **“返回”** 按该按钮可返回默认的 [AVG 用户界面](#) (组件概览)。

7.13. Online Shield

7.13.1. Online Shield 原理

Online Shield 是一种实时常驻保护功能；它甚至可以在所访问的网页（以及其中可能包含的文件）在您的 Web 浏览器中显示或下载到您的计算机前便扫描它们的内容。

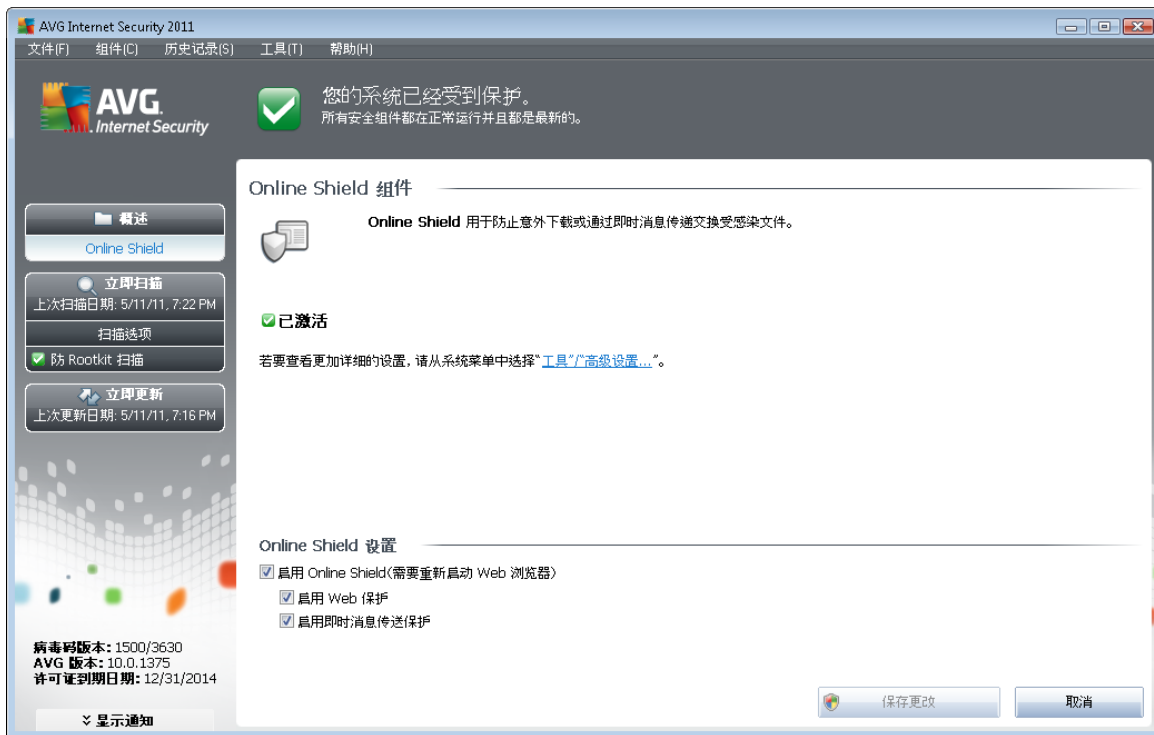
Online Shield 可以检测到您即将访问的页面包含一些危险的 javascript，并阻止该页面显示。另外，它还会识别页面中包含的恶意软件，发现它们后会立即停止下载，使其绝不可能进入您的计算机。

注：AVG Online Shield 不适用于服务器平台！



7.13.2. Online Shield 界面

Online Shield 组件的界面描述了这种保护的行为。另外，您还可以找到关于该组件当前状态的信息。在此对话框的底部，您可以找到该组件功能的基本编辑选项：



Online Shield 设置

首先，您可以通过选中/取消选中 **“启用 Online Shield”** 项来直接启用/禁用 **Online Shield**。默认情况下此选项已启用，因而 **Online Shield** 组件已激活。不过，若非必要，请勿更改此设置，建议将此组件保留为激活状态。如果选中此项，并且 **Online Shield** 正在运行，则会激活另外两个配置选项：

- **“启用 Web 保护”** 此选项确认 **Online Shield** 应对网站内容执行扫描。
- **启用即时消息传递保护** - 如果您希望 **Online Shield** 验证即时消息通信（例如，ICQ、MSN Messenger.....）没有病毒，请选中此选。

请注意：所有 AVG 组件均已由软件供应商设置完毕，可提供最佳性能。除非必要，否则请勿更改 AVG 配置。对设置的任何更改只应当由经验丰富的用户执行。如果需要更改 AVG 配置，请选择系统菜单项 **工具/高级设置**，然后在新打开的 [AVG 高级设置](#) 对话框中编辑 AVG 配置。

控制按钮

Online Shield 界面中有下列控制按钮：



- **“保存更改”** - 按此按钮可保存并应用在此对话框中所做的任何更改
- **“取消”** 按此按钮可返回默认的 [AVG 用户界面](#) (组件概览)

7.13.3. Online Shield 检测

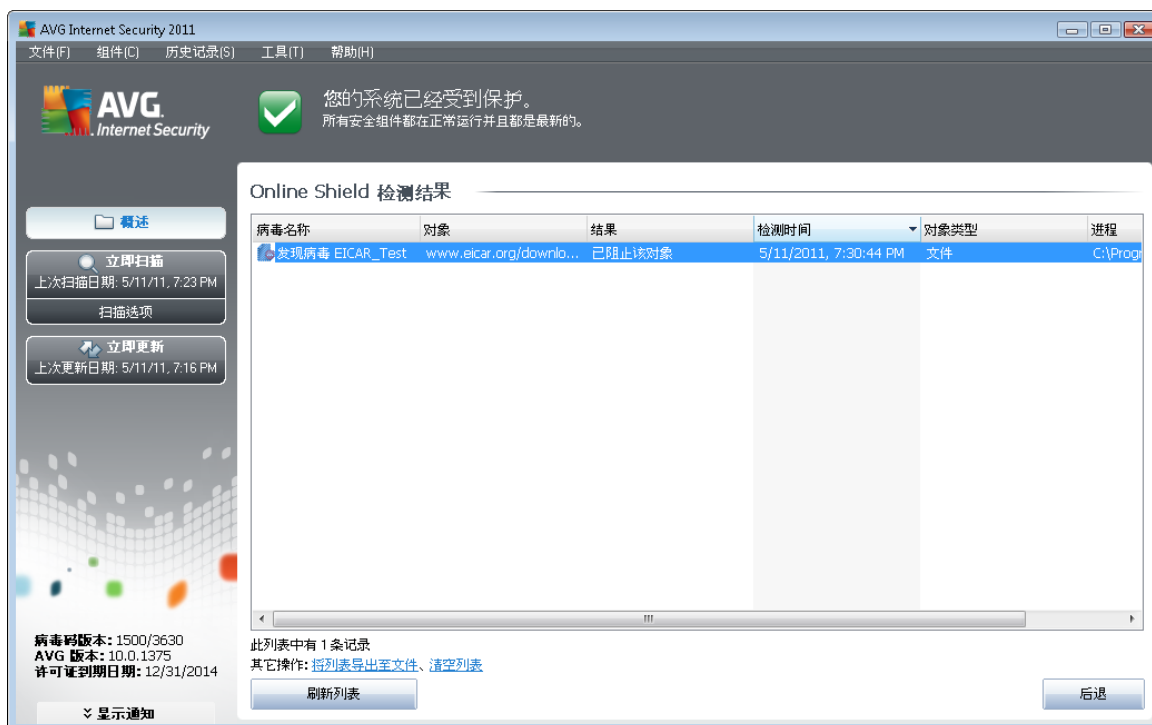
Online Shield 会扫描所访问的网页的内容以及这些网页中可能包含的文件，甚至在这些内容被显示在 Web 浏览器中之前或这些文件被下载到计算机之前便进行扫描。如果检测到威胁，便会立即通过下面的对话框向您发出警告：



在此警告对话框中，您将找到关于经检测被认定为受感染的文件的数据（**文件名**）、识别到的感染的名称（**威胁名称**），以及指向 [病毒百科全书](#) 的链接，您可以在病毒百科全书中找到关于该感染的详细信息（*如果已知*）。该对话框提供了以下按钮：

- **“显示详细信息”** 单击 **“显示详细信息”** 按钮可打开一个弹出式窗口，其中包含关于检测到感染时正在运行的进程的详细信息，以及该进程的识别号。
- **“关闭”** 单击此按钮可关闭警告对话框。

可疑网页将不会打开，检测到的威胁也会记入 **“通过 Online Shield 发现的威胁”** 列表 - 可通过系统菜单 [“历史记录”](#) **“通过 Online Shield 发现的威胁”** 了解检测到的威胁。



对于检测到的每个对象，提供了以下信息：

- **“感染”**–对检测到的对象的描述（甚至可能就是其名称）
- **“对象”**–对象来源（网页）
- **“结果”**–对检测到的对象执行的操作
- **“检测时间”**–检测到并阻止此威胁的日期和时间
- **“对象类型”**–检测到的对象的类型
- **“进程”**–通过执行何种操作来调出有潜在危险的对象以便能够检测到它

在此对话框底部的列表下方，显示了上面列出的检测到的对象总数信息。此外，您还可以将检测到的对象的整个列表导出到一个文件中（**“将列表导出至文件”**），以及删除所有检测到的对象条目（**“清空列表”**）。单击**“刷新列表”**按钮将更新 **Online Shield** 检测结果列表。按**“后退”**按钮可切换回默认的 **AVG 用户界面**（组件概览）。

7.14. Anti-Rootkit

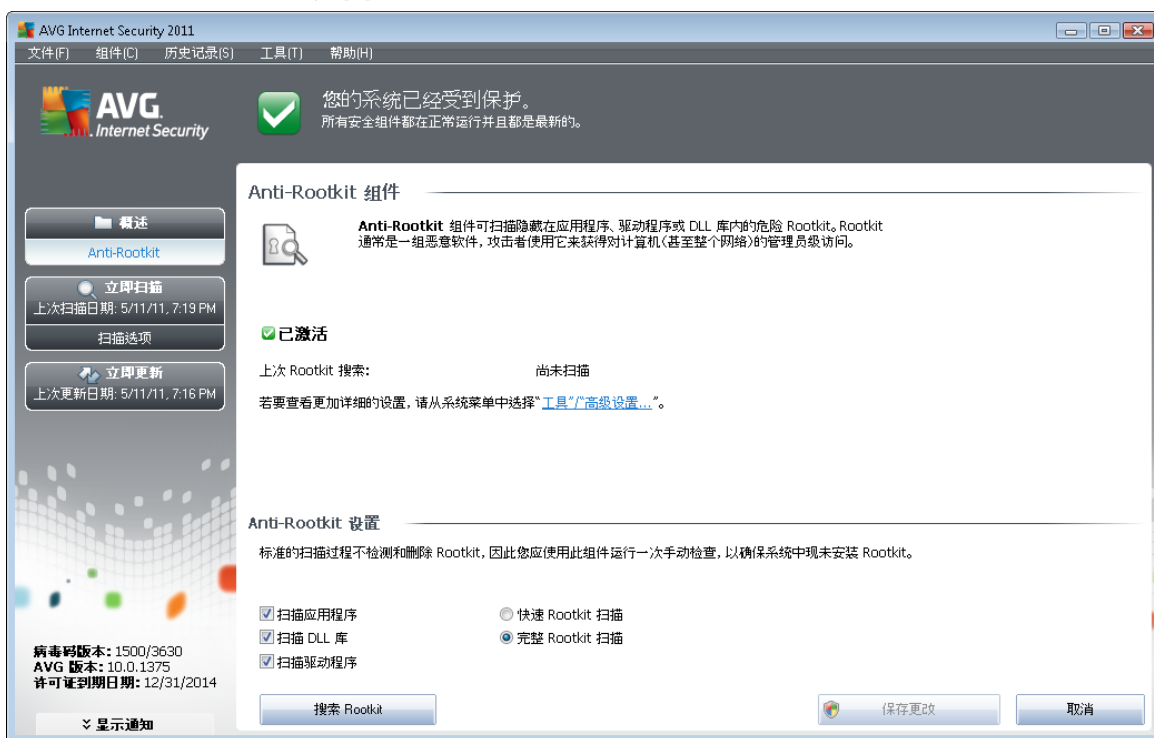
Rootkit 是一种程序，旨在在未经计算机系统所有者及合法管理员授权的情况下获得对计算机系统的基本控制。Rootkit 基本上不需要访问硬件，因为它的目的就是要控制硬件上运行的操作系统。通常情况下，Rootkit 通过破坏或避开标准操作系统安全机制来掩饰它们存在于系统中。它们往往又是特洛伊木马，因而会骗取用户的信任，使其认为在系统中运行它们是安全的。用来实现此目的的方法可能包括隐藏正在运行的进程以使监测程序无法发现它们，或者隐藏文件或系统数据以使操作系统无法发现它们。



7.14.1. Anti-Rootkit 原理

AVG Anti-Rootkit 是一款专门用来检测和有效删除危险 Rootkit（即可在您的计算机中掩饰恶意软件存在的程序和技术）的工具。**AVG Anti-Rootkit** 可以根据一组预定义的规则来检测 Rootkit。请注意，所有 Rootkit 都会被检测出来（而不仅仅是受感染的 Rootkit）。如果 **AVG Anti-Rootkit** 发现一个 Rootkit，则不一定意味着该 Rootkit 已受到感染。有时，Rootkit 会被用作驱动程序，或者是正确应用程序的组成部分。

7.14.2. Anti-Rootkit 界面



Anti-Rootkit 用户界面简要说明了该组件的功能，告知该组件的当前状态，还提供了关于 **Anti-Rootkit** 测试上次启动时间的信息（**上次 Rootkit 搜索时间**）。“**Anti-Rootkit**”对话框还提供了 **“工具”/“高级设置”** 链接。使用此链接可重定向到用于对 **Anti-Rootkit** 进行高级配置的环境。

请注意：所有 AVG 组件均已由软件供应商设置完毕，可提供最佳性能。除非必要，否则请勿更改 AVG 配置。对设置的所有更改均应由经验丰富的用户执行。

Anti-Rootkit 设置

此对话框的底部有一个 **“Anti-Rootkit 设置”** 区域，在此区域中可以设置 Rootkit 扫描的某些基本功能。首先，选中相应的复选框可指定应扫描的对象：

- **扫描应用程序**
- **扫描 DLL 库**



- **扫描驱动程序**

此外，还可以选择 Rootkit 扫描模式：

- **快速 Rootkit 扫描** - 用于扫描所有正在运行的进程、已加载的驱动程序和系统文件夹（通常是 c:\Windows）
- **完整 Rootkit 扫描** - 用于扫描所有正在运行的进程、已加载的驱动程序、系统文件夹（通常是 c:\Windows），以及所有本地磁盘（包括闪存磁盘，但不包括软盘/CD 驱动器）

控制按钮

- **“搜索 Rootkit”** - 由于 Rootkit 扫描并不隐含在 [“扫描整个计算机”](#) 中，因此可以直接从 **Anti-Rootkit** 界面中使用此按钮运行 Rootkit 扫描
- **“保存更改”** - 按此按钮可保存在此界面中所做的所有更改并返回默认的 [AVG 用户界面](#)（组件概览）
- **“取消”** - 按此按钮可返回默认的 [AVG 用户界面](#)（组件概览）而不保存您所做的任何更改

7.15. 系统工具

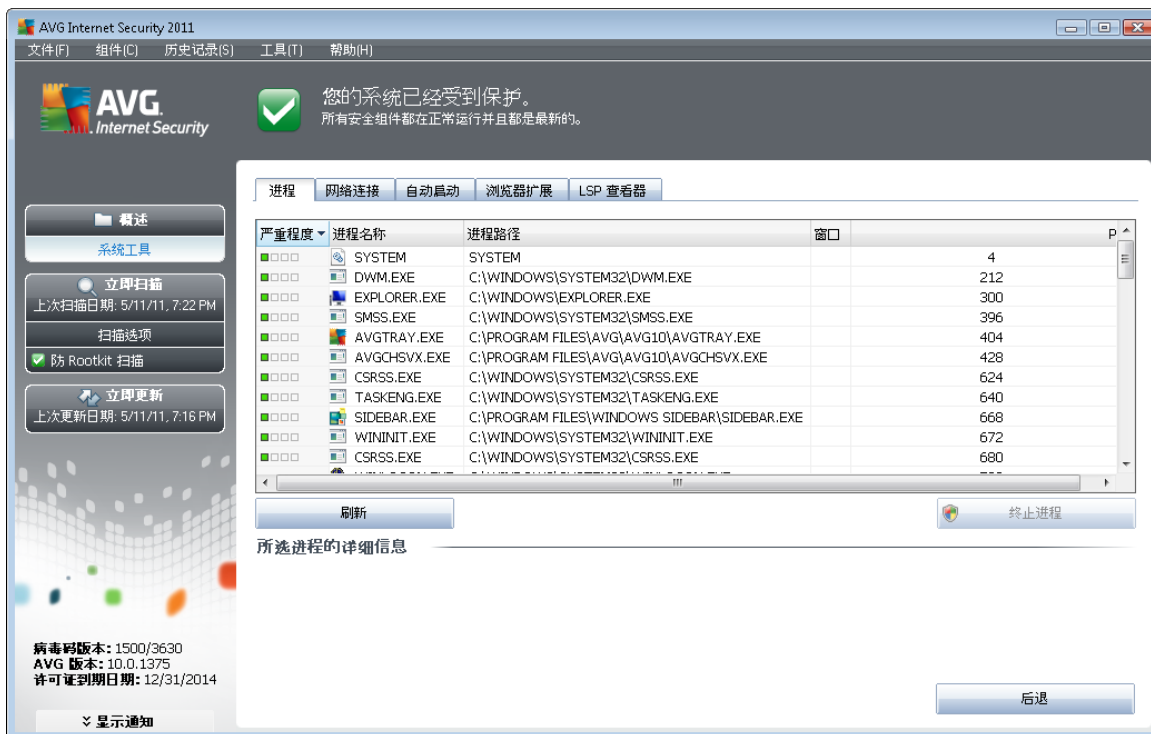
系统工具是指可以显示 **AVG Internet Security 2011** 环境和操作系统详细摘要的工具。该组件显示了以下各项的概览：

- [进程](#) - 您计算机上当前活动进程（即正在运行的应用程序）的列表
- [网络连接](#) - 当前活动连接的列表
- [自动启动](#) - 在 Windows 系统启动期间执行的所有应用程序的列表
- [浏览器扩展](#) - 您的 Internet 浏览器中安装的插件（即应用程序）列表
- [LSP 查看器](#) - 分层服务提供程序 (LSP) 的列表

您还可以对特定的概览进行编辑，但建议仅限经验丰富的用户进行编辑！



7.15.1. 进程



“**进程**”对话框包含您计算机上当前活动进程（即正在运行的应用程序）的列表。此列表分为若干列：

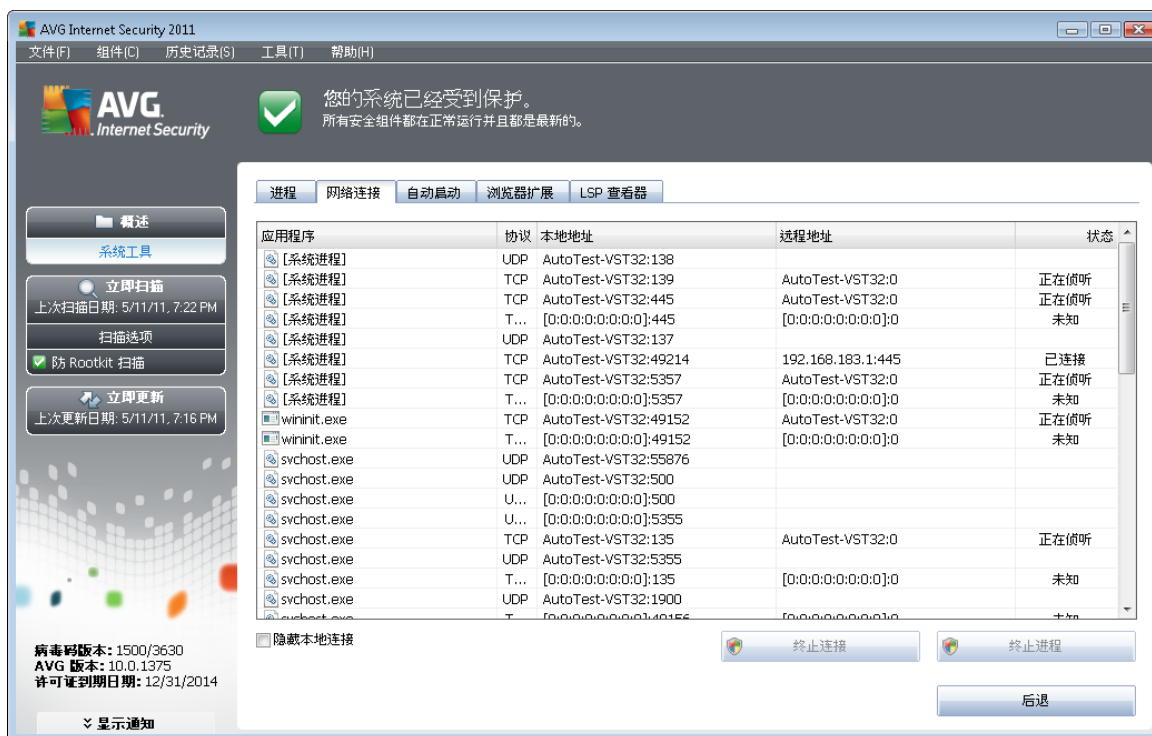
- “**严重程度**”以图形方式显示相应进程的严重程度，划分为 4 个等级：从不太重要（□□□□）到至关重要（■ ■ ■ ■）
- “**进程名称**”-正在运行的进程的名称
- “**进程路径**”-正在运行的进程的物理路径
- “**窗口**”-指示应用程序的窗口名称（如果适用）
- “**PID**”-即进程识别号，是具备唯一性的 Windows 内部进程标识符

控制按钮

系统工具界面中提供的控制按钮如下：

- “**刷新**”-根据当前状态更新进程列表
- “**终止进程**”-您可以选择一个或多个应用程序，然后按此按钮将其终止。**我们强烈建议不要终止任何应用程序，除非您完全确定它们是真正的威胁！**
- “**返回**”-切换回默认的 [AVG 用户界面](#)（组件概览）

7.15.2. 网络连接



“**网络连接**”对话框包含了当前活动连接的列表。此列表分为以下几列：

- “**应用程序**”-与相应连接相关的应用程序的名称（除了 Windows 2000，其中没有提供此信息）
- “**协议**”-用于连接的传输协议类型：
 - o TCP -与 Internet 协议 (IP) 一起用来通过 Internet 传输信息的协议
 - o UDP -TCP 协议的备用协议
- “**本地地址**”-本地计算机的 IP 地址及所用的端口号
- “**远程地址**”-远程计算机的 IP 地址及所连接到的端口号。如果可能，它还将查找远程计算机的主机名。
- “**状态**”-指示当前最有可能的状态（已连接、服务器应关闭、侦听、已完成、主动关闭、被动关闭、主动关闭）

若要仅列出外部连接，请勾选位于对话框底部区域列表下方的“**隐藏本地连接**”复选框。

控制按钮

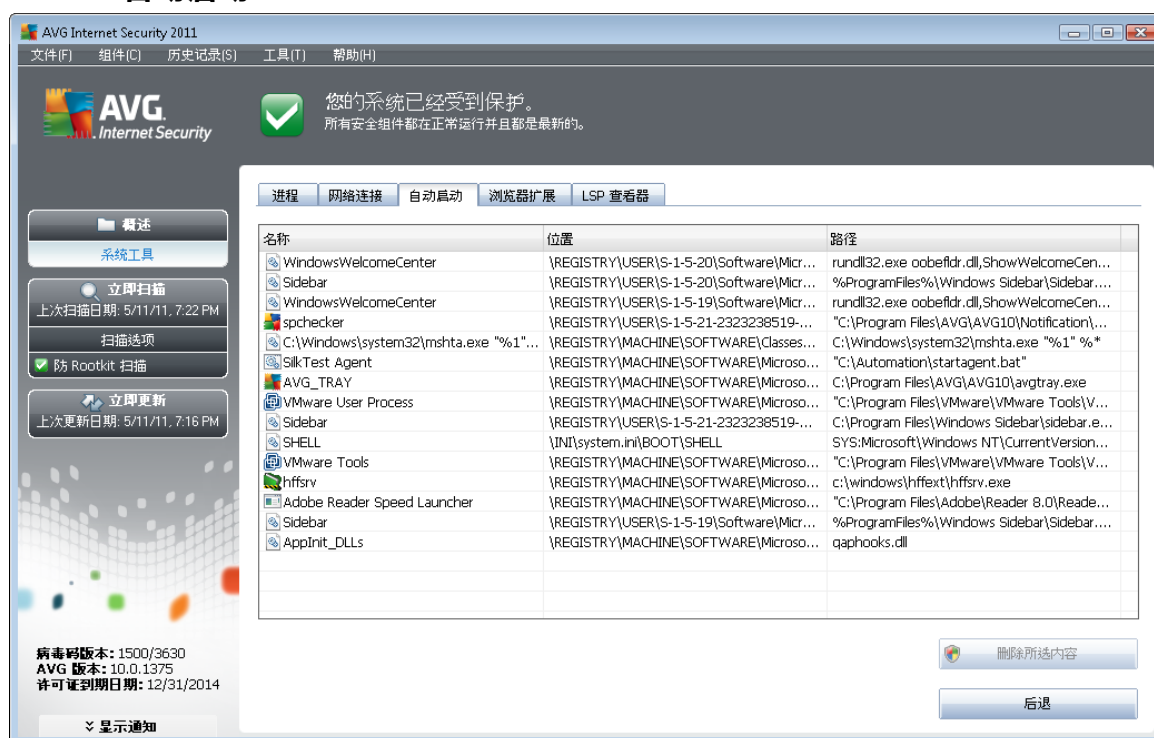
可用的控制按钮有：



- **‘终止连接’** - 关闭列表中选定的一个或多个连接
- **‘终止进程’** - 关闭列表中所选连接的一个或多个相关应用程序
- **‘后退’** - 切换回默认的 [AVG 用户界面](#)（组件概览）。

有时，可能只终止当前处于连接状态的应用程序。我们强烈建议不要终止任何连接，除非您完全确定它们是真正的威胁！

7.15.3. 自动启动



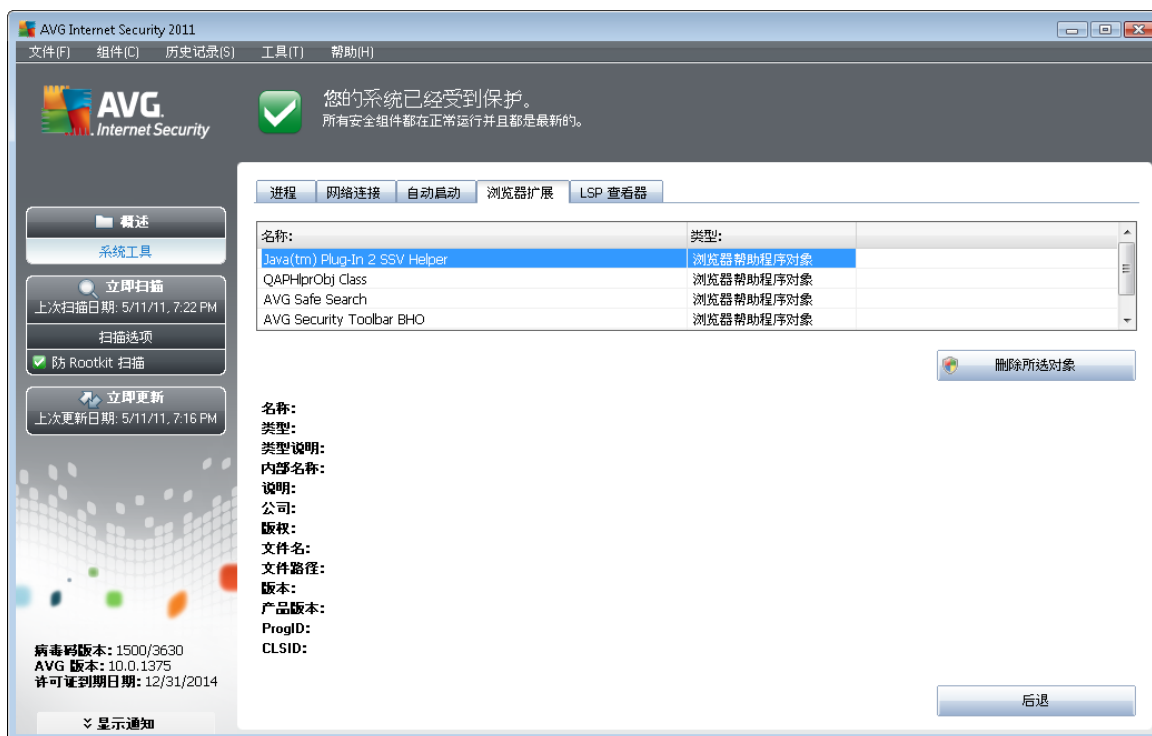
自动启动对话框显示在 Windows 系统启动过程中执行的所有应用程序的列表。一些恶意应用程序通常会自动将自身添加到注册表启动项中。

您可以删除一项或多项，方法是将其选中，然后按 **‘删除所选内容’** 按钮。按 **‘后退’** 按钮可恢复默认 [AVG 用户界面](#)（组件概览）。

强烈建议不要从此列表中删除任何应用程序，除非您完全确定它们是真正的威胁！



7.15.4. 浏览器扩展



“**浏览器扩展**”对话框包含您的 Internet 浏览器中安装的插件（即应用程序）列表。此列表既可能包含常规的应用程序插件，也可能包含潜在的恶意程序。单击此列表中的一个对象可获得有关所选插件的详细信息，这些信息将被显示在此对话框的底部。

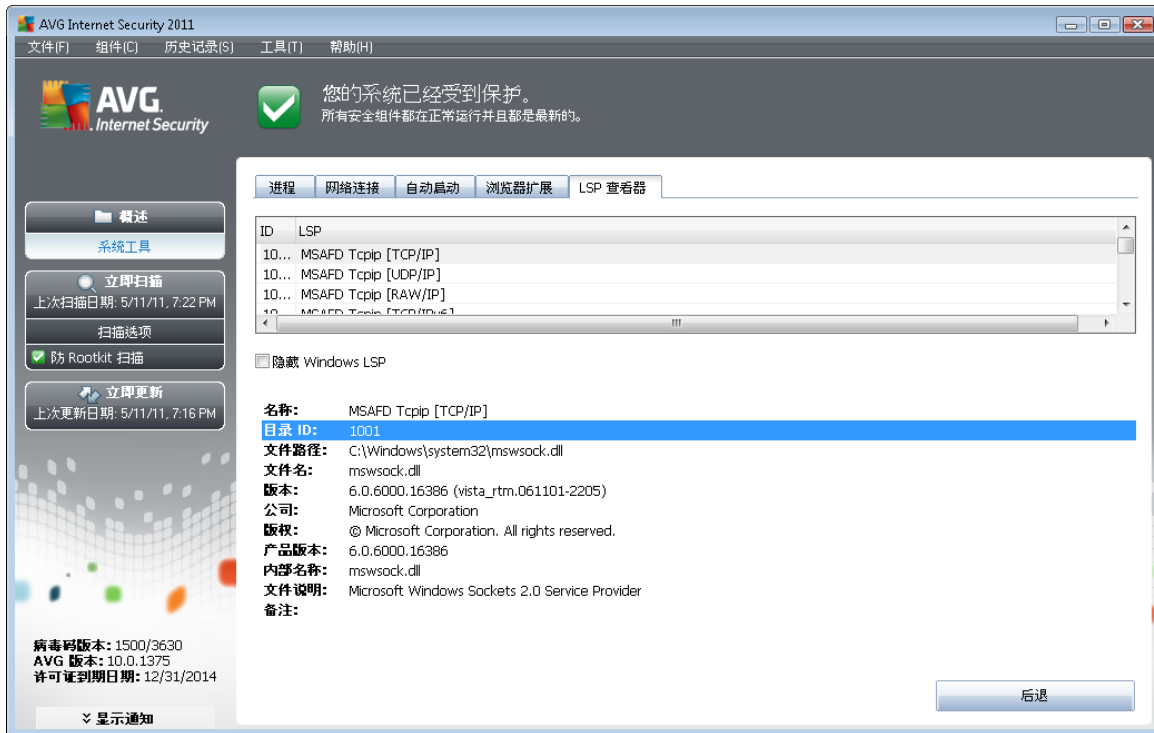
控制按钮

“**浏览器扩展**”选项卡中提供的控制按钮如下：

- “**删除所选对象**”-删除此列表中当前突出显示的插件。**强烈建议不要从此列表中删除任何插件，除非您完全确定它们是真正的威胁！**
- “**后退**”-切换回默认的 [AVG 用户界面](#)（组件概览）



7.15.5. LSP 查看器



“**LSP 查看器**”对话框显示了分层服务提供程序 (LSP) 的列表。

分层服务提供程序 (LSP) 是一种系统驱动程序，它链接到 Windows 操作系统的网络服务。它能够访问进出计算机的所有数据，并可以修改这些数据。需要使用某些 LSP 才能使 Windows 连接至其它计算机，包括 Internet。但某些恶意软件应用程序也可能将它们自身作为 LSP 来安装，从而得以访问您的计算机传输的所有数据。因此，审查此列表可能有助于您检查所有可能的 LSP 威胁。

在某些情况下，还可以修复已断开的 LSP（例如当文件已被删除而注册表项仍然不变时）。一旦发现可修复的 LSP，便会显示一个用来修复此问题的新按钮。

若要使此列表中包含 Windows LSP，请取消选中 “**隐藏 Windows LSP**”复选框。按 “**后退**”按钮可恢复默认 [AVG 用户界面](#)（组件概览）。

7.16. PC Analyzer

PC Analyzer 组件能够扫描计算机上的系统问题，并提供可能正在使计算机总体性能恶化的问题的透明概览。在该组件的用户界面中，有一个图表划分为四行，分别对应于四个类别：注册表错误、垃圾文件、碎片和损坏的快捷方式：



- **注册表错误** - 将显示 Windows 注册表中的错误数。修复注册表要求具有较专业的知识，我们建议不要尝试自行修复注册表。
- **垃圾文件** - 将显示几乎不需要的文件的数量。通常，垃圾文件包括各种格式的临时文件以及回收站中的文件。
- **碎片** - 将计算零碎硬盘空间的百分比，即使用很长一段时间后，大部分文件会分散在物理磁盘的各个位置。可以使用某种碎片整理工具来修复此问题。
- **损坏的快捷方式** - 将提示不再有效、指向不存在位置的快捷方式。

若要开始分析您的系统，请单击 **立即分析** 按钮。可以直接在该图表中观察分析进度及其结果：



结果概览提供了检测到的系统问题（**错误**）数量，并按照所测试的对应类别来划分：分析结果还会以图形方式显示在 **严重程度** 列中的轴上。

控制按钮

- **立即分析**（在分析开始之前显示）- 按此按钮可立即启动对计算机的分析
- **“立即修复”**（在分析结束后显示）- 按此按钮可转到 AVG 网站 (<http://www.avg.com/>) 上提供与 **PC Analyzer** 组件相关的最新详细信息的页面
- **“取消”** 按此按钮可停止运行分析，或在分析完成后返回默认的 [AVG 用户界面](#)（组件概览）

7.17. ID Protection

AVG Identity Protection 是一款防恶意软件产品，旨在阻止身份盗用者通过针对您的 PC 的各种恶意软件窃取您的密码、银行帐户详细信息、信用卡号码和其它个人数字财富。它确保在您的 PC 上运行的所有程序都正确地运行。**AVG Identity Protection** 持续地识别和阻止可疑行为，并保护您的计算机免遭所有新恶意软件侵害。

7.17.1. ID Protection 原理

AVG Identity Protection 是一款防恶意软件组件，采用行为学技术为您抵御各种恶意软件（间谍软件、僵尸程序、身份盗用等），并针对新的病毒提供零时差保护（Zero Day Protection）。恶意软件日趋复杂，通过伪装成正常程序使您的 PC 暴露给远程攻击者，以便进行身份盗用。**AVG Identity Protection** 可为您抵御这些基于执行的新恶意软件。该组



件提供的保护是对 [AVG Anti-Virus](#) 的补充，后者通过签名机制和扫描措施来防止受到基于文件的已知病毒的侵害。

我们强烈建议您同时安装 [AVG Anti-Virus](#) 和 AVG Identity Protection 组件，以便为您的 PC 提供完整保护。

7.17.2. ID Protection 界面



Identity Protection 组件的界面简要说明了该组件的基本功能、其状态以及某些统计数据：

- “**已删除的恶意软件项目**”-提供了经检测而被认定为恶意软件并被删除的应用程序数目
- “**受监控的进程**”-IDP 正在监控的当前正在运行的应用程序数目
- “**受监控的行为**”-受监控的应用程序中执行的特定操作数目

下方是 [“显示受到监控的进程和活动监控”](#) 链接，单击该链接可转到 [系统工具](#) 组件的用户界面，您可以在其中找到所有受监控进程的详细概览。

Identity Protection 设置

在该对话框的底部有一个 “**Identity Protection 设置**” 区域，在此区域中您可以编辑该组件功能的一些基本设置：

- “**激活 Identity Protection**”（默认情况下已启用）：选中此项可激活 IDP 组件并打



开进一步的编辑选项。

有些情况下，**Identity Protection** 可能会报告某一合法文件可疑或有危险。由于 **Identity Protection** 是根据威胁的行为来检测威胁的，因此当某一程序试图监控按键操作、安装其它程序时或者计算机上安装了新的驱动程序时，通常会出现这种情况。因此，请通过选择以下选项之一指定在检测到可疑活动时 **Identity Protection** 组件应采取何种行为：

- o **“始终提示”** - 如果某应用程序被检测为恶意软件，则会询问是否应该阻止该应用程序（默认情况下已启用此选项，强烈建议不要更改，除非更改有真正的原因。）
- o **“自动隔离检测到的威胁”** - 将自动阻止经检测而被认定为恶意软件的所有应用程序
- o **“自动隔离已知威胁”** - 仅会阻止检测后认为一定是恶意软件的应用程序

控制按钮

Identity Protection 界面中有下列控制按钮：

- **保存更改** - 按此按钮可保存并应用在此对话框中所做的任何更改
- **取消** - 按此按钮可返回默认的 [AVG 用户界面](#)（组件概览）

7.18. Security Toolbar

Security Toolbar 是一个可选的 Web 浏览器工具栏，用于在网上冲浪时提供增强的 AVG 保护和各种功能及工具。目前 **Security Toolbar** 受 Internet Explorer（6.0 或更高版本）和 Mozilla Firefox（3.0 或更高版本）Web 浏览器支持：



Security Toolbar 组件的所有设置，都能直接在 Web 浏览器中的 [Security Toolbar](#) 中显示。



8. AVG Security Toolbar

AVG Security Toolbar 是一款新的工具，它与 [LinkScanner](#) 组件搭配使用。**AVG Security Toolbar** 可用于控制 [LinkScanner](#) 的功能以及调整其行为。

如果选择在安装 **AVG Internet Security 2011** 过程中安装此工具栏，系统会自动将它添加到 Web 浏览器中（*Internet Explorer 6.0 或更高版本*，以及 *Mozilla Firefox 3.0 或更高版本*）。目前尚不支持其它 Internet 浏览器。

注：如果您使用的是某种备选的 Internet 浏览器（例如 Avant Browser），则您可能会遇到意外行为。

8.1. AVG Security Toolbar 界面

AVG Security Toolbar 旨在与 **MS Internet Explorer**（6.0 版或更高版本）和 **Mozilla Firefox**（version 3.0 或更高版本）配合使用。在您决定要安装 **AVG Security Toolbar**（在 [AVG 安装过程](#)中，系统会让您决定是否要安装该组件）后，该组件将位于您 Web 浏览器中，恰好在地址栏下方：



AVG Security Toolbar 由以下部分组成：

8.1.1. AVG 徽标按钮

此按钮提供了对一般工具栏项目的访问功能。单击此徽标按钮可重定向到 [AVG 网站](#)。单击 AVG 图标旁边的指针可打开以下内容：

- **“Toolbar 信息”** - 指向 **AVG Security Toolbar** 主页的链接，该主页详细介绍了此工具栏提供的保护情况
- **“启动 AVG”** - 打开 **AVG Internet Security 2011** [用户界面](#)
- **“AVG 信息”** - 打开一个上下文菜单，其中包含以下指向相关重要安全信息 **AVG Internet Security 2011** 的链接：
 - o **关于威胁** - 打开 [AVG 网站](#) 上提供关于威胁榜的最重要数据、病毒删除建议、AVG 更新信息、对 [病毒数据库](#) 的访问以及其它相关信息的页面
 - o **AVG 新闻** - 打开提供与 AVG 相关的最新新闻发布稿的网页
 - o **当前威胁级别** - 打开相应的病毒实验室网页，其中以图形方式显示了当前网页上的威胁级别
 - o **AVG 威胁实验室** - 打开 [AVG 站点报告](#) 网站，您可以在那里按名称搜索特定威胁，并获得有关每个威胁的详细信息

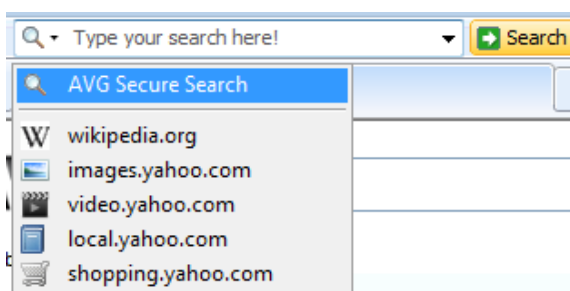


- **“选项”** - 打开一个配置对话框，您可以在此对话框中调整 **AVG Security Toolbar** 设置以满足您的需要 - 请参见后面的章节 [“AVG Security Toolbar 选项”](#)
- **删除历史记录** - 允许您在 **AVG Security Toolbar** 中删除全部历史记录，或单独删除搜索历史记录、删除浏览器历史记录、删除下载历史记录和删除 Cookie。
- **“更新”** - 检查 **AVG Security Toolbar**
- **“帮助”** - 提供用于打开帮助文件、联系 [AVG 技术支持部门](#)、发送与产品相关的反馈或查看该工具栏的当前版本详细信息的选项

8.1.2. 采用 AVG Secure Search (powered by Google) 的搜索框

使用 **AVG Secure Search (powered by Google)** 框是一种用 AVG Secure Search (powered by Google) 搜索 Web 的简单安全的方法。无论目前显示的是什么页面，将词语或短语输入该搜索框，然后按 **搜索** 按钮或 **Enter** 键，均可直接通过 AVG Secure Search (powered by Google) 服务器开始执行搜索。搜索框还会列出您的搜索历史记录。通过搜索框进行的搜索会使用 [Search-Shield](#) 保护来进行分析。

您也可以在搜索字段中切换到 Wikipedia 或某种其它特定的搜索服务 - 请参见图：



8.1.3. 页面状态

此按钮用于直接在工具栏中显示根据 [Surf-Shield](#) 组件的标准得出的正在显示的网页的评估结果：

- - 所链接的页面是安全的
- - 页面有些可疑。
- - 页面包含指向确定有风险的页的链接。
- - 所链接的页面含有活动威胁！为您的安全考虑，不允许访问此页面！
- - 无法访问该页面，因此无法扫描。

单击该按钮可打开一个信息面板，其中有关于特定网页的详细数据。



8.1.4. AVG 新闻

此按钮直接从 **AVG Security Toolbar** 中打开与 AVG 相关的最新 **标题新闻** 的概览，同时包括来自媒体和公司新闻发布的新闻：



在右上角，可以看到两个红色控制按钮：

-  - 此按钮打开编辑对话框，您可以在其中指定用来在 **AVG Security Toolbar** 中显示 **“AVG 新闻”** 按钮的参数：



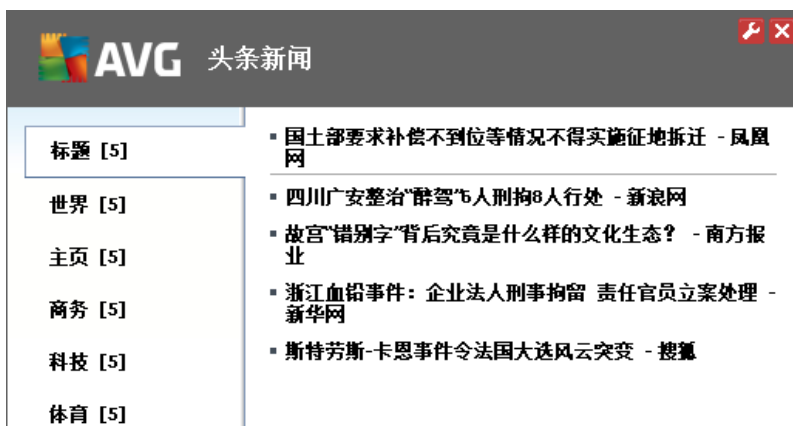
- o **“显示消息”** 更改希望一次显示的消息数量



- o **“RSS 设计”** 为新闻概览的当前显示选择 **高级** 或 **基本** 模式（默认选择了 **高级** 模式 - 请参见上图）
- o **“隐藏已读消息”** 标记此项将确认不应再显示每条已读消息，以便能够提供新的消息
-  - 单击此按钮可关闭当前打开的新闻概览

8.1.5. 新闻

类似地，此按钮直接从 **AVG Security Toolbar** 中打开来自所选媒体的最新新闻概览，并划分为若干个部分：



在右上角，可以看到两个红色控制按钮：

-  - 此按钮打开编辑对话框，您可以在其中指定用来在 **AVG Security Toolbar** 中显示 **“新闻”** 按钮的参数：



- **“按钮名称”** 您可以选择更改在 **AVG Security Toolbar**
- **“新闻版本”** 从列表中选择国家/地区以显示来自所选地区的新闻
- **“显示消息”** 指定希望一次显示的消息数量
- **“RSS 设计”** 在 **基本** / **高级** 选项之间切换以选择新闻概览的设计 (**默认情况下已设置为高级设计, 请参见上图**)
- **“隐藏已读消息”** 选中此项将确认不应再在新闻概览中显示所有已读消息, 而应替换为新的新闻标题
- **“显示按钮”** 可以在此字段中指定应在 **AVG Security Toolbar** 新闻概览中显示的新闻类型
 -  - 单击此按钮可关闭当前打开的新闻概览

8.1.6. 删除历史记录

使用此按钮可以删除浏览器历史记录, 就像通过 **AVG 徽标** -> **“删除历史记录”** 选项进行的操作一样。

8.1.7. 电子邮件通知程序

“电子邮件通知程序” 按钮允许您直接在 [AVG Security Toolbar](#) 界面中激活在新电子邮件到达时向您发出通知的选项。该按钮打开如下编辑对话框, 您可以在其中定义电子邮件帐户参数和电子邮件显示规则。请按照对话框中的说明进行操作:

配置: "电子邮件通知程序按钮"

AVG 电子邮件通知程序设置

只需输入您的电子邮件帐户详细信息，即可轻松访问您的所有电子邮件。

帐户类型: ☒ Gmail ☐ POP3
☐ 其它:

电子邮件地址
密码

☒ 自动登录(登录到我的帐户时将不要求提供密码)

每隔以下时间检查一次有无新电子邮件 分钟

☒ 允许提醒有新电子邮件

☒ 有新电子邮件送达时播放一段声音
☐ 5 秒后关闭通知窗口

- **“帐户类型”** 指定您的电子邮件帐户使用的协议类型。可在以下备选选项中进行选择：“Gmail”、“POP3”，也可通过 **其它** 选项中的下拉菜单选择服务器名称（目前，如果您的帐户在 Yahoo! JP Mail 或 Hotmail 中，则可使用此选项）。如果不确定您的帐户使用的电子邮件服务器类型，可设法从电子邮件提供商或 Internet 服务提供商处找到该信息。
- **登录** - 下面这一部分中有 **电子邮件地址** 及其相应 **密码** 的确切形式。请将 **自动登录** 选项保持选中状态，这样就不必重复地填写数据。
- **测试帐户** - 可用此按钮测试输入的详细信息。
- **重置设置** - 用于快速删除在上面输入的电子邮件地址详细信息。
- **检查新电子邮件的间隔时间(分钟)** - 定义用于检查新电子邮件的时间间隔（范围介于 5 至 120 分钟），并指定您是否以及想要如何接收有关新电子邮件到达的通知。
- **允许新电子邮件提醒** - 取消选中此复选框可禁用收到新电子邮件时发出的可视化通知。
 - **有新电子邮件送达时播放一段声音** - 取消选中此复选框可禁用收到新电子邮件时发出的声音通知。
 - **5 秒后关闭通知窗口** - 选中此复选框可在收到新电子邮件 5 秒后自动关闭



可视化通知窗口。

8.1.8. 天气信息

通过“天气”按钮，可直接在 **AVG Security Toolbar** 界面中显示关于所选目的地的当前气温的信息（每 3 至 6 个小时更新一次）。单击该按钮可打开新的信息面板，其中包含详细天气概览：

Brno, CZ
[更改地点]

14° C

风速: 16,09 公里/小时
日出: 05:08
日落: 20:29

周一
最高温度: 17 °C
最低温度: 8 °C

周二
最高温度: 21 °C
最低温度: 9 °C

已更新 05/16/2011 11:02:30

YAHOO! NEWS

全面预报 >

提供的编辑选项如下：

- **“更改地点”** 单击 **“更改地点”** 文本可显示一个名为 **“搜索您的地点”** 的新对话框。在文本字段中填入所需地点的名称，然后单击 **“搜索”** 按钮予以确认。下一步，在具有相同名称的所有地点的列表中，选择您要寻找的目的地。最后，信息面板会再次显示，以提供所选地点的天气信息。
- **“华氏温标/摄氏温标转换器”** 在信息面板的右上角，您可以在华氏温标与摄氏温标之间做出选择。根据您的选择，将会以所选温标显示气温信息，
- **全面预报** - 如果对全面和详细的预报感兴趣，则可使用 **全面预报** 链接访问专门的网站。

8.1.9. Facebook

“Facebook” 按钮用于直接从 **AVG Security Toolbar** 连接到 [Facebook](#) 社交网络。单击此按钮将显示登录邀请，再次打击将打开 **“Facebook 登录”** 对话框。提供您的登录凭据，然后单击 **“连接”** 按钮。如果您还没有 [Facebook](#) 帐户，可以使用 **“注册 Facebook”** 链接直接创建一个。

完成 [Facebook](#) 注册过程后，将会请求您允许 **AVG 社交扩展** 应用程序。此应用程序的功能对 [Facebook](#) 连接工具栏至关重要，因此建议您确保允许它运行。然后，[Facebook](#) 连接将会激活，**AVG Security Toolbar** 中的 **“Facebook”** 按钮现在将提供标准 [Facebook](#) 菜单选项。

8.2. AVG Security Toolbar 选项

AVG Security Toolbar 的所有参数配置都可以直接在“AVG Security Toolbar”面板中进行访问。通过 AVG / 选项 工具栏菜单项可在一个名为 **“Toolbar 选项”** 的新对话框中打开其编辑界面，此对话框分以下四个部分：

8.2.1. ‘常规’选项卡



在此选项卡中，可以指定在“AVG Security Toolbar”面板中应显示或隐藏的工具栏控制按钮。如果要相应按钮显示出来，请标记任一选项。以下说明的是各个工具栏按钮的功能：

- **‘页面状态’按钮** - 使用该按钮可在 **AVG Security Toolbar**
- **‘AVG 新闻’按钮** - 该按钮用于打开一网页，其中有关于 AVG 的最新新闻
- **‘新闻’按钮** - 通过该按钮可分门别类地大概了解媒体每天发布的最新新闻
- **‘删除历史记录’按钮** - 通过该按钮可以直接从‘AVG Security Toolbar 面板中 删除整个历史记录’、删除搜索历史记录’、删除浏览器历史记录’、删除下载历史记录或 删除 Cookie”
- **‘电子邮件通知程序’按钮** - 该按钮允许您在 **AVG Security Toolbar** 界面中显示新到达的电子邮件
- **‘天气’按钮** - 此按钮提供关于所选位置的天气情况的即时信息
- **‘Facebook’按钮** - 该按钮提供到 [Facebook](https://www.facebook.com) 社交网络的直接连接

8.2.2. ‘有用的按钮’选项卡



通过 **‘有用的按钮’** 选项卡，可从列表中选择应用程序，然后将其图标显示在工具栏界面中。然后就能将该图标用作快速链接，这样就能直接启动相应的应用程序。

8.2.3. ‘安全’选项卡



‘安全’ 选项卡划分为 **‘AVG 浏览器安全’** 和 **‘等级’** 这两个区域，在此选项卡中您可以通过选中特定的复选框将您要使用的功能分配给 **AVG Security Toolbar**：



- “**浏览器安全**”-选中此项可激活或禁用 [AVG Search-Shield](#) 和/或 [Surf-Shield](#) 服务
- **等级** - 选择供您要使用的 [Search-Shield](#) 组件用来评定搜索结果等级的图形符号：
 - o 页面是安全的
 - o 页面有些可疑
 - o 页面包含指向确实危险的页面的链接
 - o 页面含有活动的威胁
 - o 无法访问页面，因此无法扫描

请选中相应的选项以确认您希望获得关于此特定威胁级别的通知。不过，无法禁止显示为包含活动威胁和危险威胁的页面分配红色标记。**再次说明，对于程序供应商设置的默认配置，除非确有必要更改，否则建议保留。**

8.2.4. ‘高级选项’选项卡



在 **高级选项** 选项卡中，首先选择要用作默认搜索引擎的搜索引擎。可在 *AVG Secure Search (powered by Google)*、*百度*、*WebHledani*、*Yandex* 和 *Yahoo! JP* 中进行选择。更改默认搜索引擎后，请重新启动 Internet 浏览器，以使所作的更改生效。

此外，还可激活或禁用其它特定 **AVG Security Toolbar** 设置（所列标题有关默认 AVG



Secure Search (powered by Google) 设置) :

- **将 AVG Secure Search (powered by Google) 设置并一直作为地址栏的搜索提供程序** - 如果将其选中，则可通过此选项直接在 Internet 浏览器地址栏中键入搜索关键字，还会自动用 Google 服务搜索相关网站。
- **让 AVG 就浏览器导航错误(404/DNS)提出建议** - 如果在网上搜索时遇到不存在的页面或无法显示的页面（404 错误），则会自动重定向到一个网页，用其可从与主题相关的备选页面的概览中进行选择。
- **将 AVG Secure Search (powered by Google) 设置并一直作为默认搜索提供程序** - Google 是在 **AVG Security Toolbar** 中用于执行 Web 搜索的默认搜索引擎，此选项激活后也会成为 Web 浏览器的默认搜索引擎。

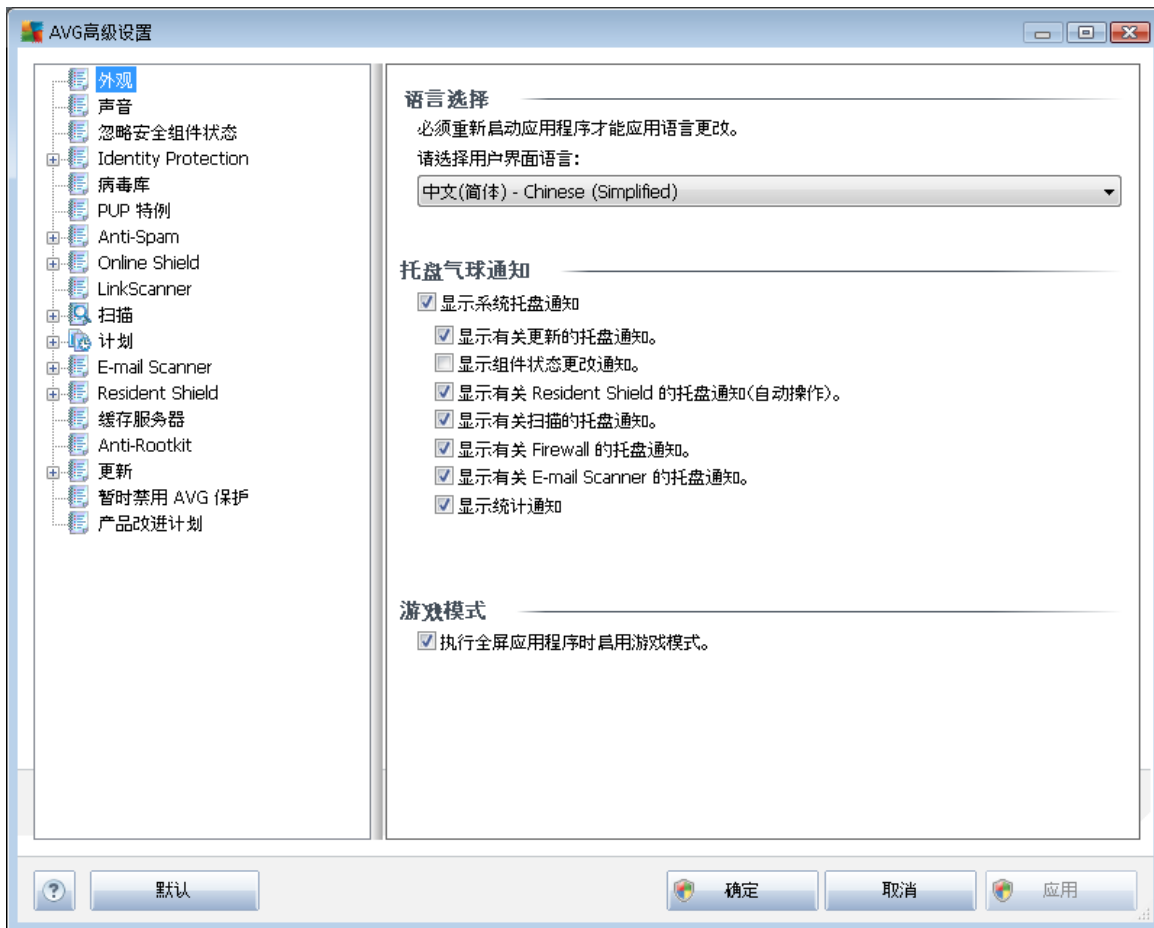


9. AVG 高级设置

会在名为 **“高级 AVG 设置”** 的新窗口中打开 **AVG Internet Security 2011** 的高级配置对话框。此窗口划分成两个区域：左侧部分提供一个树形导航结构，用于访问程序的配置选项。选择您要更改其配置的组件（或其特定组成部分）即可在该窗口的右侧区域中打开编辑对话框。

9.1. 外观

导航树的第一项内容（**“外观”**）是指 [AVG 用户界面](#) 的常规设置，以及有关应用程序行为的几个基本选项：

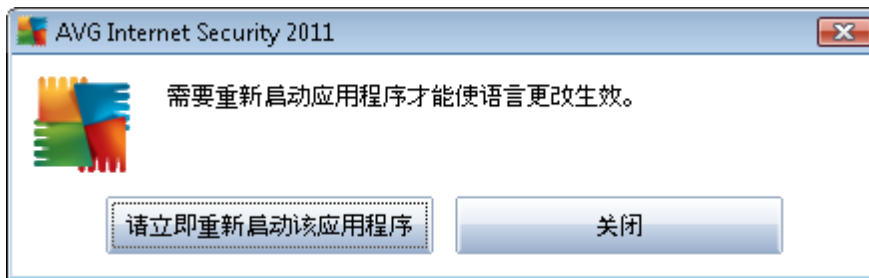


语言选择

在 **“语言选择”** 区域中，可以从其中的下拉菜单中选择所需的语言；然后整个 [AVG 用户界面](#) 都将使用该语言。此下拉菜单仅提供您之前在 [安装过程](#) 中选择安装的那些语言（请参见 [自定义选项](#) 一章）以及英语（这是默认安装的语言）。不过，您必须重新启动用户界面才能完成将应用程序切换到其它语言的过程；请按以下步骤操作：

- 选择所需的应用程序语言，然后按 **“应用”** 按钮（位于右下角）确认您所作的选择

- 按 **确定** 按钮进行确认
- 随即会弹出一个新的对话框窗口，告知您更改 AVG 用户界面语言需要重新启动应用程序：



任务栏气球通知

在此区域中，您可以禁止显示有关应用程序状态的系统任务栏气球通知。默认情况下，允许显示气球通知，建议保留此配置！这些气球通知通常用来告知 AVG 组件的某种状态变化情况，因此您应加以注意！

不过，如果您出于某种原因决定不希望显示这些通知，或者希望仅显示某些通知（与特定 AVG 组件相关），则您可以通过选中/取消选中以下选项来定义并指定您的使用偏好：

- **显示系统任务栏通知** - 默认情况下此项已选中（**启用**），因而通知会显示。取消选中此项可完全禁止显示所有气球通知。启用此项后，您可以进一步选择应显示哪些特定通知：
 - **显示有关 更新 的任务栏通知** - 决定是否应显示有关 **AVG 更新过程的启动、进度及完成情况** 的信息；
 - **显示组件状态变更通知** - 决定是否应显示有关组件的活动/不活动状态或其可能存在的问题的信息。在报告组件的故障状态时，此选项相当于 **系统任务栏图标**（颜色变化）的通知功能，该功能用来报告任何 AVG 组件中存在的问题；
 - **显示有关 Resident Shield 的任务栏通知（自动操作）** - 用于决定是应显示还是禁止有关文件保存、复制和打开进程的信息（仅当已启用 **Resident Shield 自动修复** 选项时才会显示此配置）；
 - **“显示有关 扫描 的任务栏通知”** - 决定是否应显示有关计划的扫描的自动启动、进度及结果的信息；
 - **“显示有关 Firewall 的任务栏通知”** - 决定是否应显示有关 Firewall 状态和进程的信息，例如该组件的启用/停用警告、可能的通信阻止等信息；
 - **显示有关 电子邮件扫描程序 的任务栏通知** - 决定是否应显示有关所有传入和传出电子邮件的扫描信息。
 - **显示统计通知** - 保持此选项的选中状态可允许在系统任务栏中定期显示统



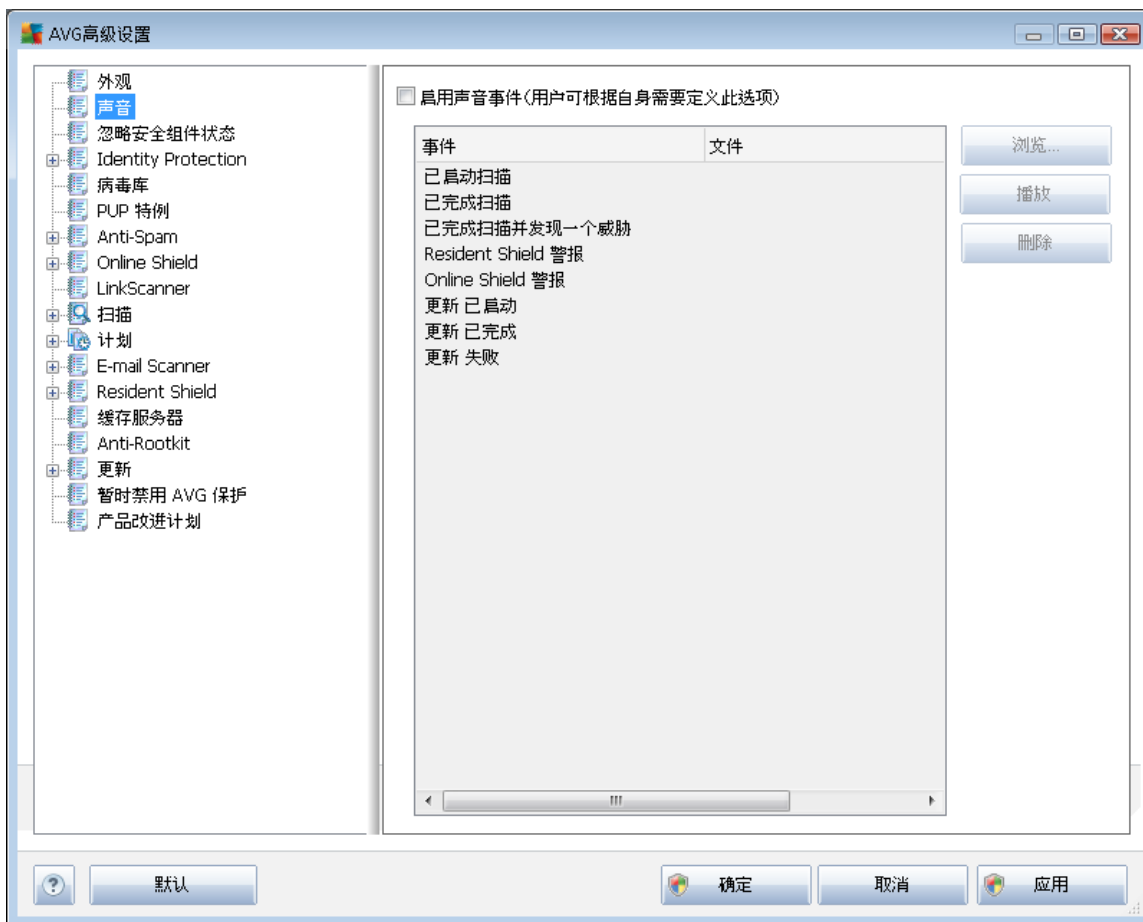
计复查通知。

游戏模式

此 AVG 功能旨在用于有可能受到 AVG 信息提示（例如，开始执行计划扫描时出现的信息提示）干扰（可能将全屏应用程序最小化，或破坏其图形）的全屏应用程序。要避免出现这种情况，请保持 **‘执行全屏应用程序时启用游戏模式’** 选项的复选框的选中状态（默认设置）。

9.2. 声音

在 **‘声音’** 对话框中，您可以指定是否要通过声音通知来获知特定 AVG 操作的情况。如果是，请选中 **‘启用声音事件’** 选项（默认情况下已禁用）以激活 AVG 操作的列表：

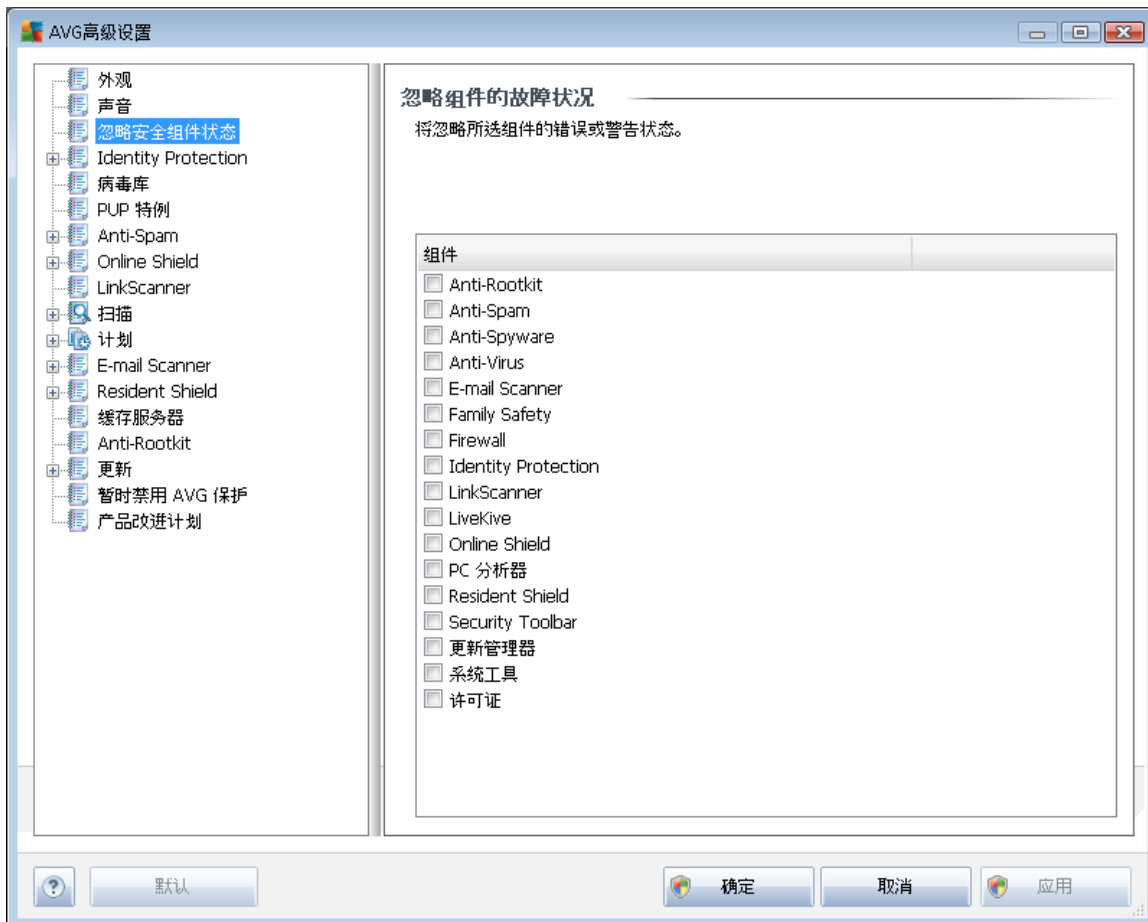


接着，请从此列表中选择相应的事件，然后在磁盘中通过浏览（**‘浏览’**）查找要为此事件分配的合适声音。若要听一下所选的声音，请突出显示此列表中的相应事件，然后按 **‘播放’** 按钮。使用 **‘删除’** 按钮可删除为特定事件分配的声音。

注：仅支持 *.wav 格式的声音！

9.3. 忽略故障状况

在“**忽略组件故障状况**”对话框中，您可以勾选您不想获知哪些组件的情况：



默认情况下，此列表中未选定任何组件。这意味着，如果有任何组件出现错误状态，系统会立即通过以下方式将此情况告知您：

- **系统任务栏图标** - 当 AVG 的所有组件都正常运行时，此图标以四种颜色显示；但是，如果出现错误，此图标会显示一个黄色的感叹号；
- AVG 主窗口的“**安全状态信息**”区域中对现有问题的文字说明

可能存在您由于某种原因而需要暂时禁用某一组件的情况（*不建议这样做，您应让所有组件都永远处于启用状态并保持默认配置；但这种情况还是有可能发生的*）。在这种情况下，系统任务栏图标会自动报告该组件的错误状态。但对于这种特殊的情况，我们不能将其算作真正的错误，因为这是您自己故意引起的，并且您也知道这带来的潜在危险。同时，一旦此图标以灰色显示，它实际上就无法报告可能出现的任何其它错误。

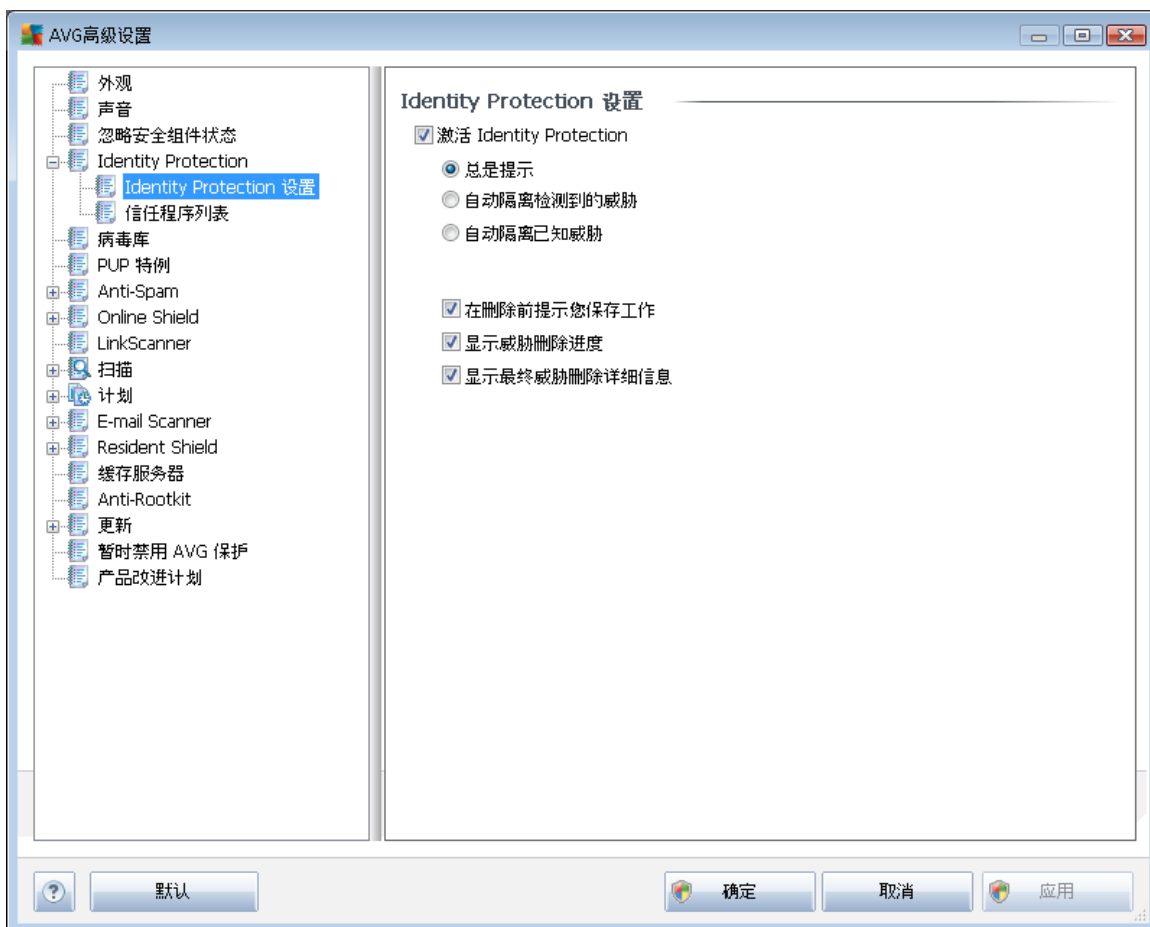
对于这种情况，您可以在上面的对话框中选择可能处于错误状态（或已禁用）但您不希望获知其情况的组件。在 [AVG 主窗口中的组件概览](#) 中，也可直接对特定组件使用同样的选项，即“**忽略组件状态**”。



9.4. Identity Protection

9.4.1. Identity Protection 设置

通过 [“Identity Protection 设置”](#) 对话框，可启用/禁用 [Identity Protection](#) 组件的以下基本功能：



“激活 Identity Protection”（默认情况下已启用）- 取消选中此项可禁用 [Identity Protection](#) 组件。

如无必要，强烈建议不要取消选中此框！

激活 [Identity Protection](#) 后，您可以指定在检测到威胁时应如何处理：

- **“始终提示”**（默认情况下已启用）- 检测到威胁时会询问是否要将其移到隔离区中，以确保不会移除所要运行的应用程序。
- **“自动隔离检测到的威胁”** - 选中此复选框可指定要将可能会检测到的所有威胁都立即移到 [AVG 病毒库](#) 的安全空间中。如果保留默认设置，则在检测到威胁时，程序将询问您是否应将其移至隔离区，以确保不会移除您要运行的程序。



序。

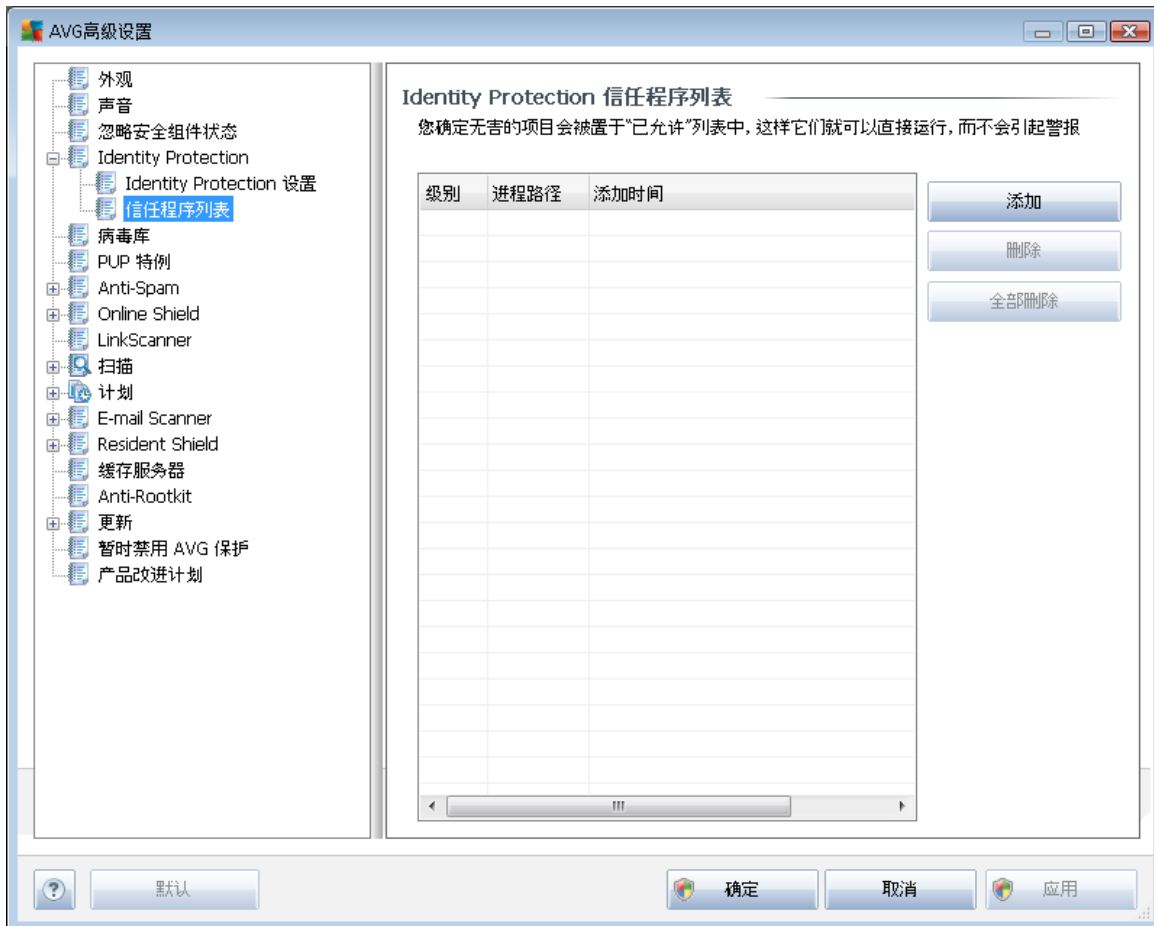
- **“自动隔离已知威胁”** - 如果想将检测后认为是疑似恶意软件的所有应用程序都自动直接移到 [AVG 病毒库](#) 中，请保持此选项的选中状态。

还可指定具体选项，有选择性地激活更多 [Identity Protection](#) 功能：

- **“删除前提示保存您的工作”** - (默认情况下已启用) - 如果想在将检测后认为是疑似恶意软件的应用程序移到隔离区中之前收到警告，请保持此选项的选中状态。如果您正在使用该应用程序，您需要先保存项目以防丢失。默认情况下已启用此选项，强烈建议保持其已启用状态。
- **“显示恶意软件删除进度”** - (默认情况下已启用) - 启用此选项后，一检测到潜在恶意软件就会打开新对话框，显示将恶意软件移到隔离区的进度。
- **“显示最终的恶意软件删除详细信息”** - (默认情况下已启用) - 启用此选项后，[Identity Protection](#) 会显示关于移到隔离区中的各个项目的详细信息（严重程度、位置等）。

9.4.2. ‘已允许’列表

在 **“Identity Protection 设置”** 对话框内，如果决定保留 **“自动隔离检测到的威胁”** 项目的未选中状态，则在每次检测到可能有危险的恶意软件时，系统都将询问您是否应删除该软件。然后，如果您将可疑应用程序（*根据其行为检测到的*）指定为安全，并且确认应该在您的计算机上保留它，则该应用程序将被添加至所谓的 **Identity Protection ‘已允许’列表**，并且将不再被报告为有潜在危险：



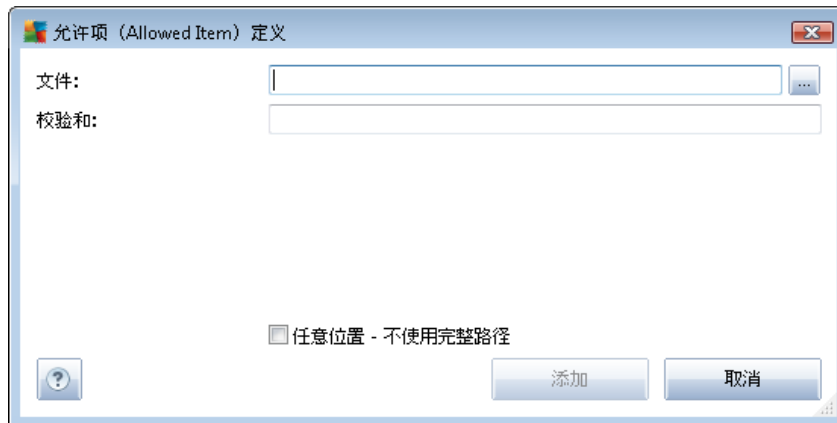
Identity Protection ‘已允许’列表提供有关各个应用程序的以下信息：

- **级别** - 以图形方式显示相应进程的严重程度，划分为四个等级：从不太重要（   ) 到至关重要（   )
- **进程路径** - 应用程序（进程）可执行文件的位置路径
- **允许的日期** - 手动将此应用程序指定为安全应用程序的日期

控制按钮

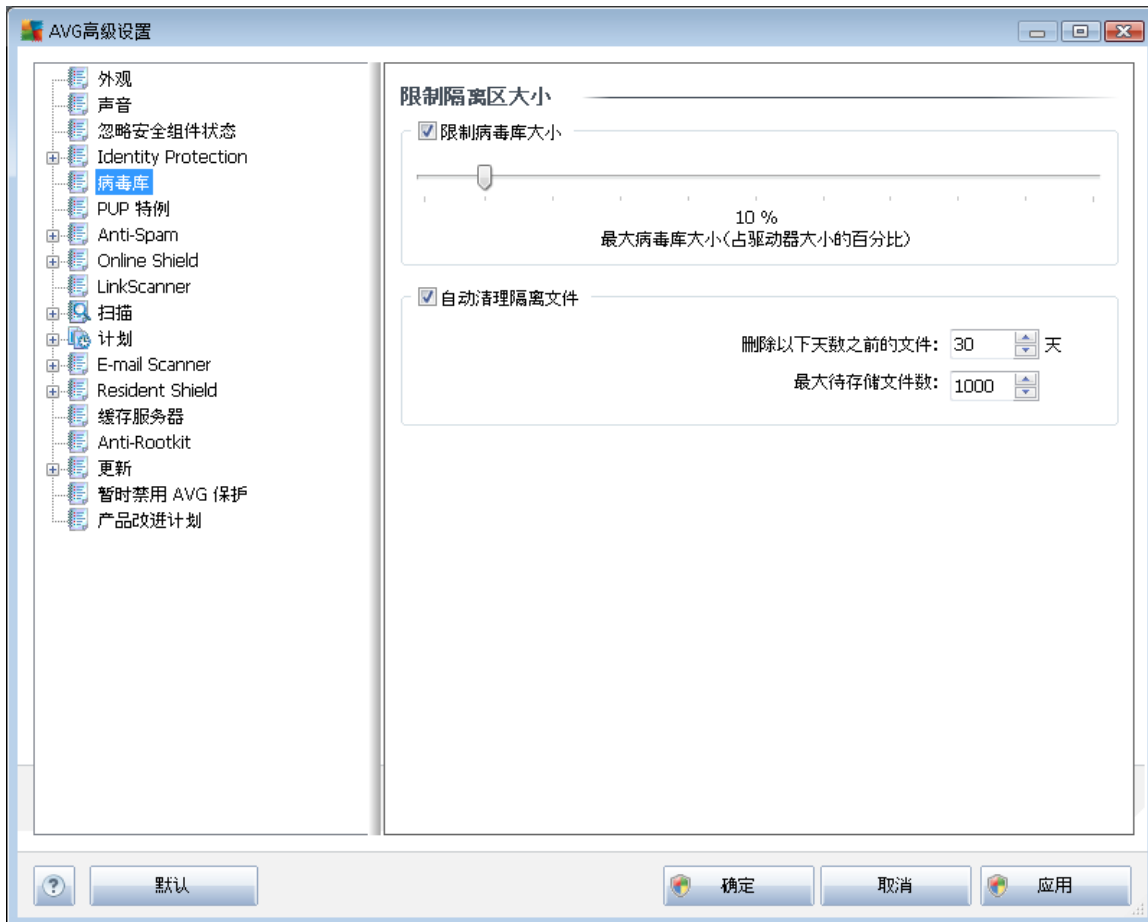
Identity Protection ‘已允许’列表对话框中的控制按钮包括：

- **添加** - 按此按钮可向 ‘已允许’ 列表添加新应用程序。随即会弹出以下对话框：



- o **文件** - 键入要标记为特例的文件（应用程序）的完整路径
- o **校验和** - 显示所选文件的唯一 签名 ”。此校验和是一个自动生成的字符串，AVG 通过它可明确地将所选文件与其它文件区分开来。此校验和在成功添加文件后生成并显示。
- o 任意位置 - 不使用完整路径 - 如果您希望将此文件仅定义为特定位置的特例，那么请将此复选框保留为未选中状态
- **移除** - 按此按钮可从列表中移除所选应用程序
- **全部移除** - 按此按钮可移除列出的所有应用程序

9.5. 病毒库

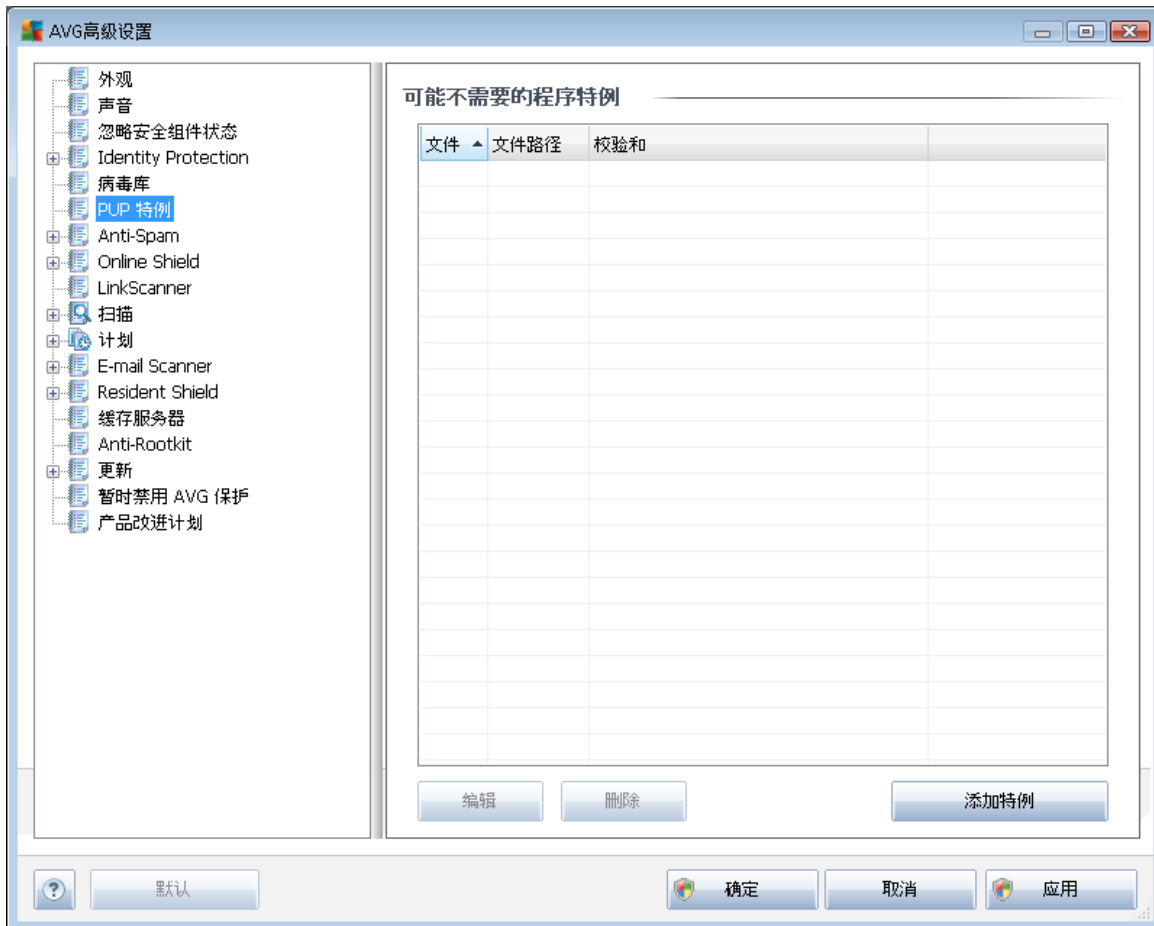


通过 **“病毒库维护”** 对话框，可定义关于管理 **病毒库** 中存储的对象的若干参数：

- **“限制病毒库大小”**—使用滑块可设置 **病毒库** 的最大大小。此大小根据您本地磁盘的大小按比例指定。
- **“自动删除文件”**—在此区域中，请定义对象应被存储在 **病毒库** 中的最大时长（**“删除存储时间超过 ... 天的文件”**），以及 **病毒库** 中最大待存储文件数（**“最大待存储文件数”**）

9.6. PUP 特例

AVG Internet Security 2011 能够分析和检测系统中可能不需要的可执行应用程序或 DLL 库。在某些情况下，用户可能希望让某些不需要的程序留在计算机上（这些程序是有意安装的）。有些程序（特别是免费程序）包含广告软件。AVG 可能会检测到此类广告软件并将它们报告为 **可能不需要的程序**。如果您希望将这样的程序保留在您的计算机上，则可以将它定义为可能不需要的程序特例：



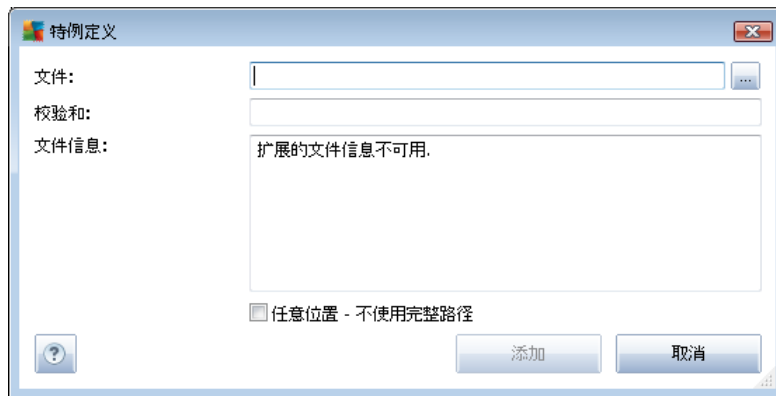
“可能不需要的程序特例”对话框列出了已定义且当前有效的 可能不需要的程序 的特例。您可以对此列表进行编辑，删除现有项，或添加新特例。此列表中提供了有关每个特例的以下信息：

- **文件** - 提供相应应用程序的名称
- **文件路径** - 显示该应用程序的位置路径
- **校验和** - 显示所选文件的唯一 签名”。此校验和是一个自动生成的字符串，AVG 通过它可明确地将所选文件与其它文件区分开来。此校验和在成功添加文件后生成并显示。

控制按钮

- **编辑** - 打开已定义特例的编辑对话框（与用于定义新特例的对话框完全相同，见下图），在此对话框中您可以更改特例的参数
- **删除** - 从特例列表中删除所选项
- **添加特例** - 打开一个编辑对话框，您可以在该对话框中定义要创建的新特例的参数

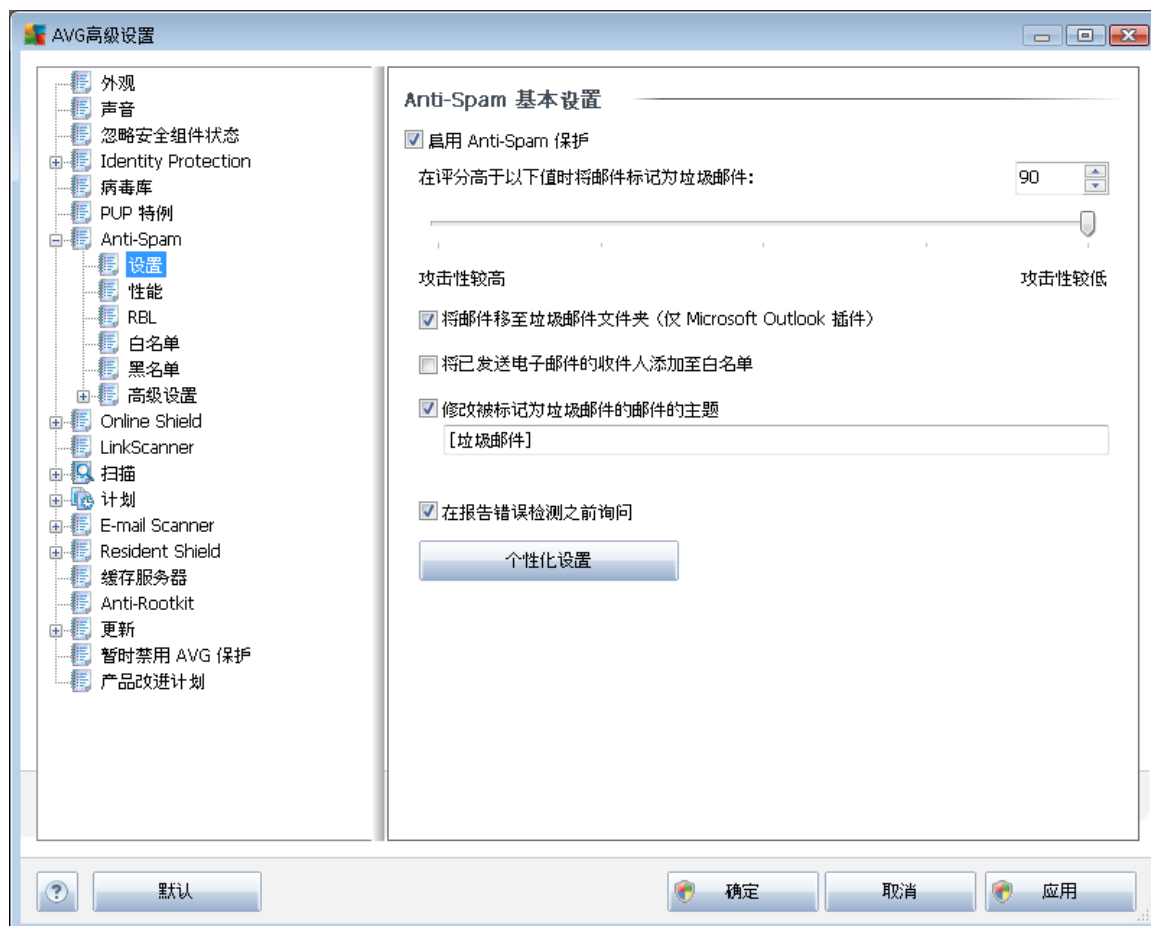
数：



- o **文件** - 请键入您要标记为特例的文件的完整路径
- o **校验和** - 显示所选文件的唯一“签名”。此校验和是一个自动生成的字符串，AVG通过它可明确地将所选文件与其它文件区分开来。此校验和在成功添加文件后生成并显示。
- o **文件信息** - 显示关于此文件的任何其它可用信息（许可证/版本信息等）
- o **任意位置 - 不使用完整路径** - 如果您希望将此文件仅定义为特定位置的例外，那么请将此复选框保留为未选中状态。如果选中此复选框，指定的文件无论其位置在何处，都会被定义为例外（不过，您无论如何都必须填写特定文件的完整路径；然后倘若您的系统中出现两个具有相同名称的文件，该文件将用作唯一示例）。

9.7. Anti-Spam

9.7.1. 设置



在“**Anti-Spam 基本设置**”对话框中，您可以选中/取消选中“**启用 Anti-Spam 保护**”复选框以允许/禁止对电子邮件通信进行反垃圾邮件扫描。此选项在默认情况下已启用，照例建议，除非确有必要更改此配置，否则请予以保留。

接下来，您还可以选择较为严格或较为宽松的评分措施。**Anti-Spam** 过滤器根据多项动态扫描技术为每封邮件指定一个分值（即该邮件的内容与垃圾邮件的相似度）。可调整“**在评分高于以下值时将邮件标记为垃圾邮件**”设置，方法是键入值，或者向左或向右移动滑块（使用滑块时，值限制在 50-90 的范围内）。

一般而言，我们建议将阈值设置在 50 至 90 之间，如果您确实不知道设为何值，建议设置为 90。下面对评分阈值进行了大致介绍：

- **介于 80 和 90 之间的值** - 将过滤掉很有可能是垃圾邮件的电子邮件。有些并非垃圾邮件的邮件也可能被错误地过滤掉。
- **介于 60 和 79 之间的值** - 这些值被认为是相当严格的配置。将过滤掉可能是垃圾邮件的电子邮件。并非垃圾邮件的邮件也可能被捕获到。
- **介于 50 和 59 之间的值** - 非常严格的配置。并非垃圾邮件的电子邮件很有可能会被当成真正的垃圾邮件而被捕获到。正常使用时不推荐此阈值范围。



在 **“Anti-Spam 基本设置”** 对话框中，可进一步定义检测到的[垃圾邮件](#)的处理方式：

- **“将邮件移至垃圾邮件文件夹”**—选中此复选框可指定应将检测到的每封垃圾邮件自动移至您的电子邮件客户端中的特定垃圾邮件文件夹中；
- **“将已发送电子邮件的收件人添加至白名单”**—勾选此复选框可确认，已发送电子邮件的所有收件人都是可信的，来自他们的电子邮件帐户的所有电子邮件都可以传递；
- **“修改被标记为垃圾邮件的邮件的主题”**—如果您想在所有被检测为[垃圾邮件](#)的邮件的主题字段中添加特定词语或字符作为标记，请勾选此复选框；可以在激活的相应文本字段中键入所需的文本。
- **“在报告错误检测之前询问”**—前提是您在[安装过程](#)中同意了参与[产品改进计划](#)。如果是这样，将允许您向 AVG 报告检测到的威胁。系统会自动处理报告过程。不过，您可以选中此复选框，确认您希望在向 AVG 报告任何检测到的垃圾邮件之前向您询问，以确保该邮件确实应该分类为垃圾邮件。

控制按钮

“Anti-Spam 培训” 按钮用于打开 [Anti-Spam 培训向导](#)，在[下一章](#)中会对其进行详细说明。

Anti-Spam 培训向导 的第一个对话框要求您选择打算用于培训的电子邮件来源。通常情况下，您需要使用已被误标记为垃圾邮件的电子邮件，或尚未被识别出来的垃圾邮件。



有以下选项可供选择：

- **特定的电子邮件客户端** - 如果您使用的是所列出的电子邮件客户端（MS Outlook、Outlook Express、The Bat!）之一，只需选择对应的选项即可

- **“包含 EML 文件的文件夹”**–如果您使用的是任何其它电子邮件程序，首先应将这些邮件保存至特定文件夹（以 .eml 格式），或者确保您知道电子邮件客户端邮件文件夹的位置。然后选择 **“包含 EML 文件的文件夹”**；这样您下一步就能找到所需的文件夹

为加快并简化培训过程，最好事先对各文件夹中的电子邮件进行整理，以使您将用于培训的文件夹仅包含培训邮件（要么是需要的邮件，要么是不需要的邮件）。但并非必需进行整理，因为您可以稍后对这些电子邮件进行过滤。

选择相应选项，然后单击 **“下一步”** 继续按向导提示操作。

本步骤中显示的对话框取决于您之前所作的选择。

包含 EML 文件的文件夹



在此对话框中，请选择您要用于培训的邮件所在的文件夹。按 **“添加文件夹”** 按钮以找到包含 .eml 文件（已保存的电子邮件）的文件夹。所选的文件夹随后便会显示在此对话框中。

在 **“文件夹包含”** 下拉菜单中，设置以下两个选项之一：所选文件夹包含的是需要的电子邮件（非垃圾邮件），还是未经请求便发来的电子邮件（垃圾邮件）。请注意，在下一步中您可以过滤这些邮件，所以该文件夹现在不必仅包含培训电子邮件。您还可以通过单击 **“删除文件夹”** 按钮从此列表中删除不需要的选定文件夹。

完成后，单击 **“下一步”**，然后接着设置 [邮件过滤选项](#)。

特定的电子邮件客户端

在您确认其中一个选项后，将显示新的对话框。



注：对于 Microsoft Office Outlook，系统会提示您先选择 MS Office Outlook 配置文件。

在“**文件夹包含**”下拉菜单中，设置以下两个选项之一：所选文件夹包含的是需要的电子邮件（**非垃圾邮件**），还是未经请求便发来的电子邮件（**垃圾邮件**）。请注意，在下一步中您可以过滤这些邮件，所以该文件夹现在不必仅包含培训电子邮件。所选电子邮件客户端的导航树已被显示在此对话框的主体区域。请在此树中找到所需的文件夹，然后用鼠标突出显示它。

完成后，单击“**下一步**”，然后接着设置 [邮件过滤选项](#)。



在此对话框中，您可以进行电子邮件过滤设置。

如果您确定所选文件夹仅包含您要用于培训的邮件，请选择“**所有邮件（无过滤）**”选项。



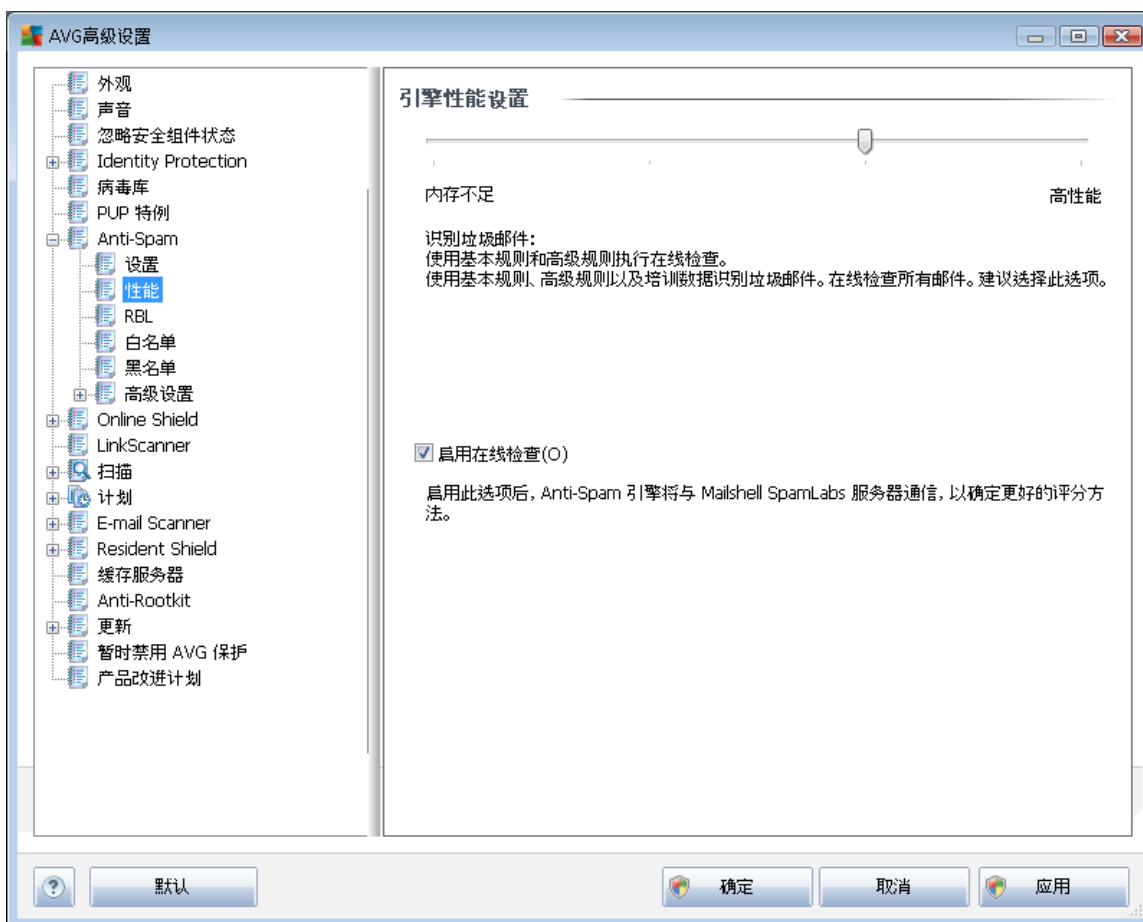
如果您不确定此文件夹中包含哪些邮件，并且希望此向导对每一封邮件都向您询问（以便您决定是否要将其用于培训），请选择 **“对每封邮件均进行询问”** 选项。

若要进行更高级的过滤，请选择 **“使用过滤器”** 选项。您可以填写要在电子邮件主题和/或发件人字段中搜索的一个词（名称）、词的一部分或词组。与所输入的条件完全匹配的所有邮件都将被用于培训，不再进行提示。

注意！：当您在两个文本字段中都填入内容时，只与其中一个条件匹配的地址也将被用于培训。

选择适当的选项后，请单击 **“下一步”**。接下来显示的对话框将仅用于提供信息，告知您此向导已做好邮件处理准备。若要开始培训，请再次单击 **“下一步”** 按钮。随后便依据前面选择的条件开始培训。

9.7.2. 性能



“引擎性能设置”对话框（通过左侧导航区域中的**“性能”**项链接到此对话框）提供了 **Anti-Spam** 组件的性能设置。向左或向右移动滑块可更改扫描性能的高低，最左侧为**“低内存占用”**模式，最右侧为**“高性能”**模式。

- **低内存占用** - 在扫描过程中识别[垃圾邮件](#)时，不使用任何规则。只使用培训数据进行识别。在一般使用情形中不建议采用此模式，除非计算机硬件配置非常低。



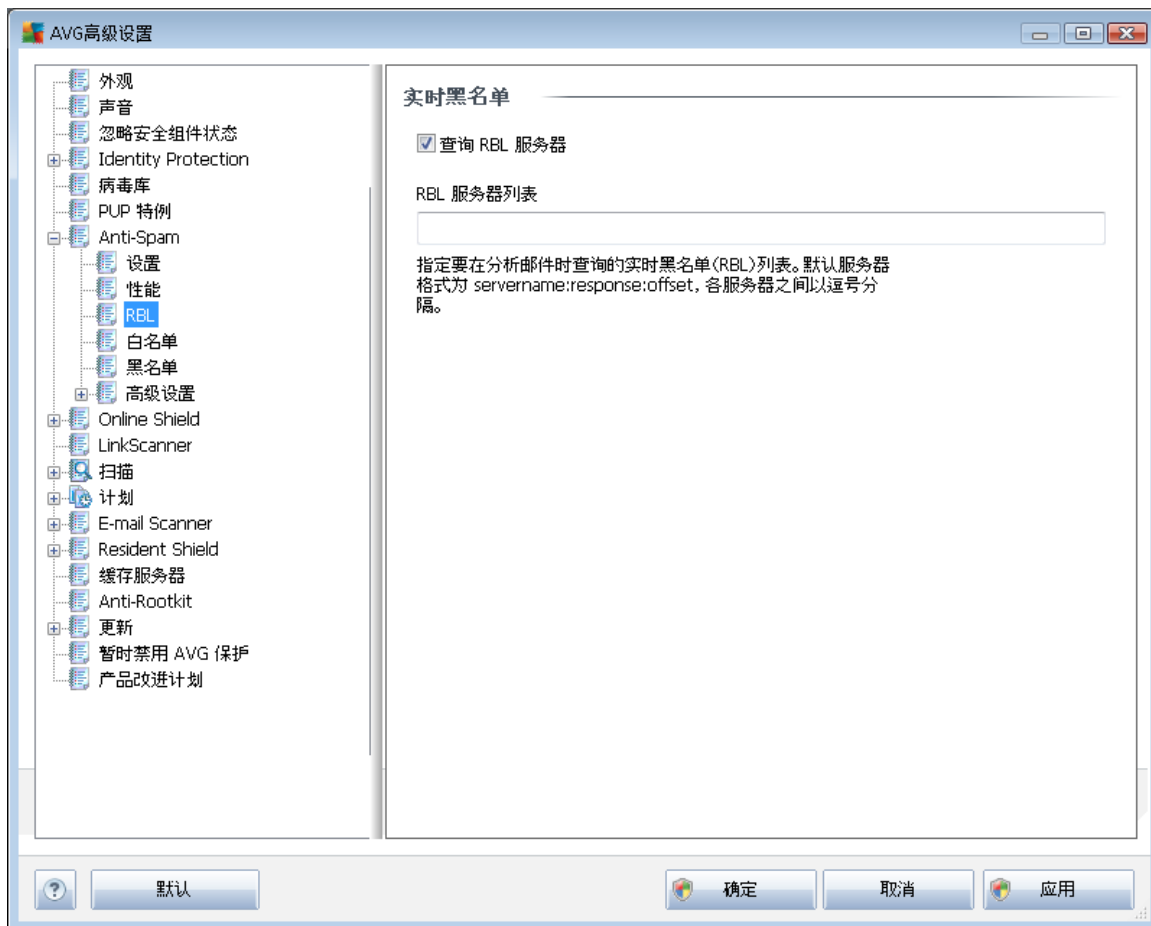
- **高性能** - 采用此模式时将占用大量内存。在扫描过程中，将使用以下功能来识别垃圾邮件：规则和垃圾邮件数据库缓存、基本规则和高级规则、垃圾邮件制造者的 IP 地址和垃圾邮件制造者数据库。

默认情况下，‘**启用在线检查**’项已启用。这样可通过与 [Mailshell](#) 服务器进行通信（即，将扫描到的数据与在线的 [Mailshell](#) 数据库进行比较），实现更为精确的垃圾邮件检测效果。

通常情况下，若非必要，建议保留默认设置。对此配置的任何更改都只应由专家级用户进行！

9.7.3. RBL

“RBL”项用于打开一个名为‘**实时黑名单**’的编辑对话框：



在此对话框中，您可以启用/禁用 ‘**查询 RBL 服务器**’ 功能。

RBL（实时黑名单）服务器是一台承载着一个大型数据库的 DNS 服务器，该数据库中存储着已知的垃圾邮件发件人。启用此功能后，会对照此 RBL 服务器数据库验证所有电子邮件，如果有邮件与该数据库中的任何条目相同，则会将该邮件标记为垃圾邮件。RBL 服务器数据库包含最新的垃圾邮件指纹，以便进行最佳、最准确的垃圾邮件检测。如果用户收到 [Anti-Spam](#) 引擎通常无法检测到的大量垃圾邮件，则此功能对他们来说尤为有



用。

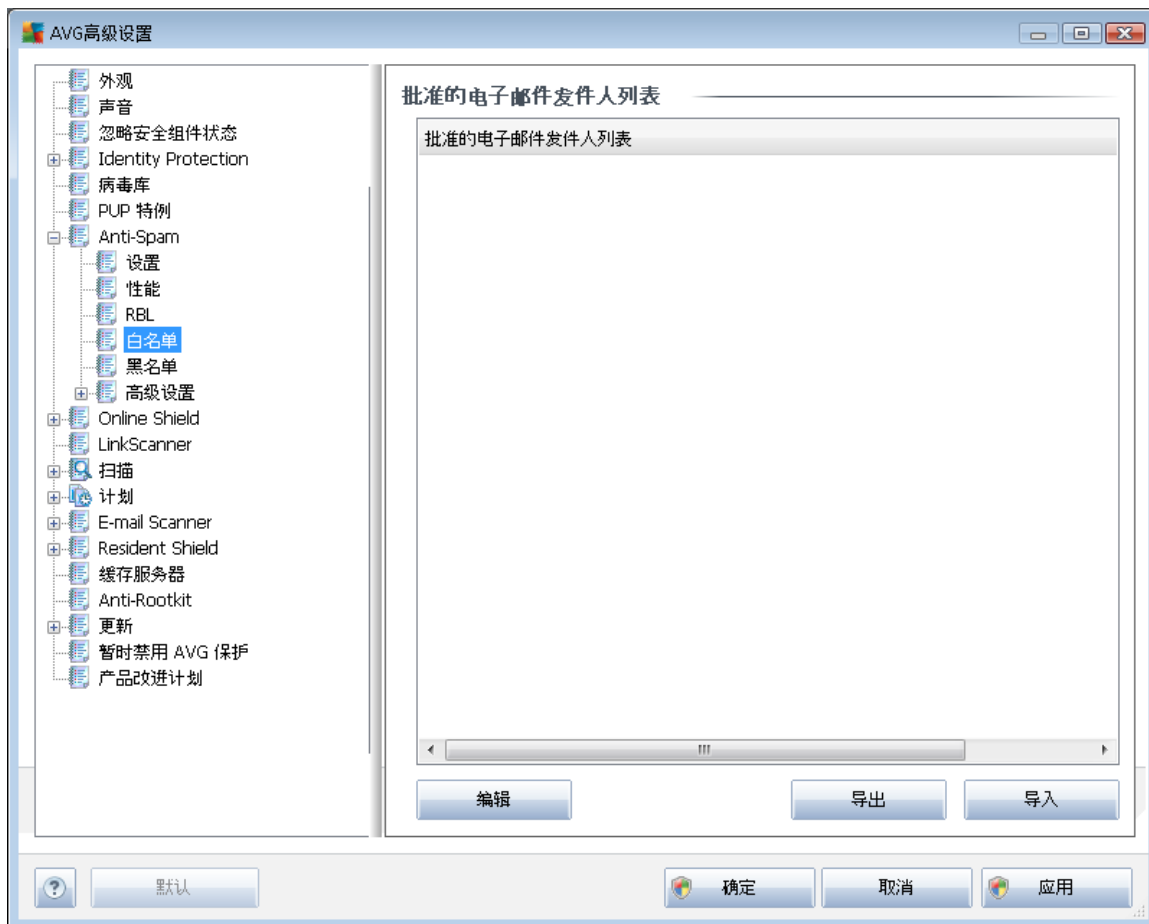
可在 **“RBL 服务器列表”** 中定义特定 RBL 服务器位置。

注：在有些系统上以及有些配置条件下，启用此功能可能会降低电子邮件接收速度，因为每一封邮件都必须对照 RBL 服务器数据库进行验证。

不会将任何个人数据发送到此服务器！

9.7.4. 白名单

“白名单” 选项用于打开一个名为 **“批准的电子邮件发件人列表”** 的对话框，其中列有全部经过批准的发件人电子邮件地址和域名，这些发件人发送的邮件绝不会被标记为 [垃圾邮件](#)。



在此编辑界面中，您可以整理一个您确定绝不会向您发送不需要的邮件（[垃圾邮件](#)）的发件人名单。您还可以整理一个您知道不会产生垃圾邮件的完整域名（如 [avg.com](#)）列表。

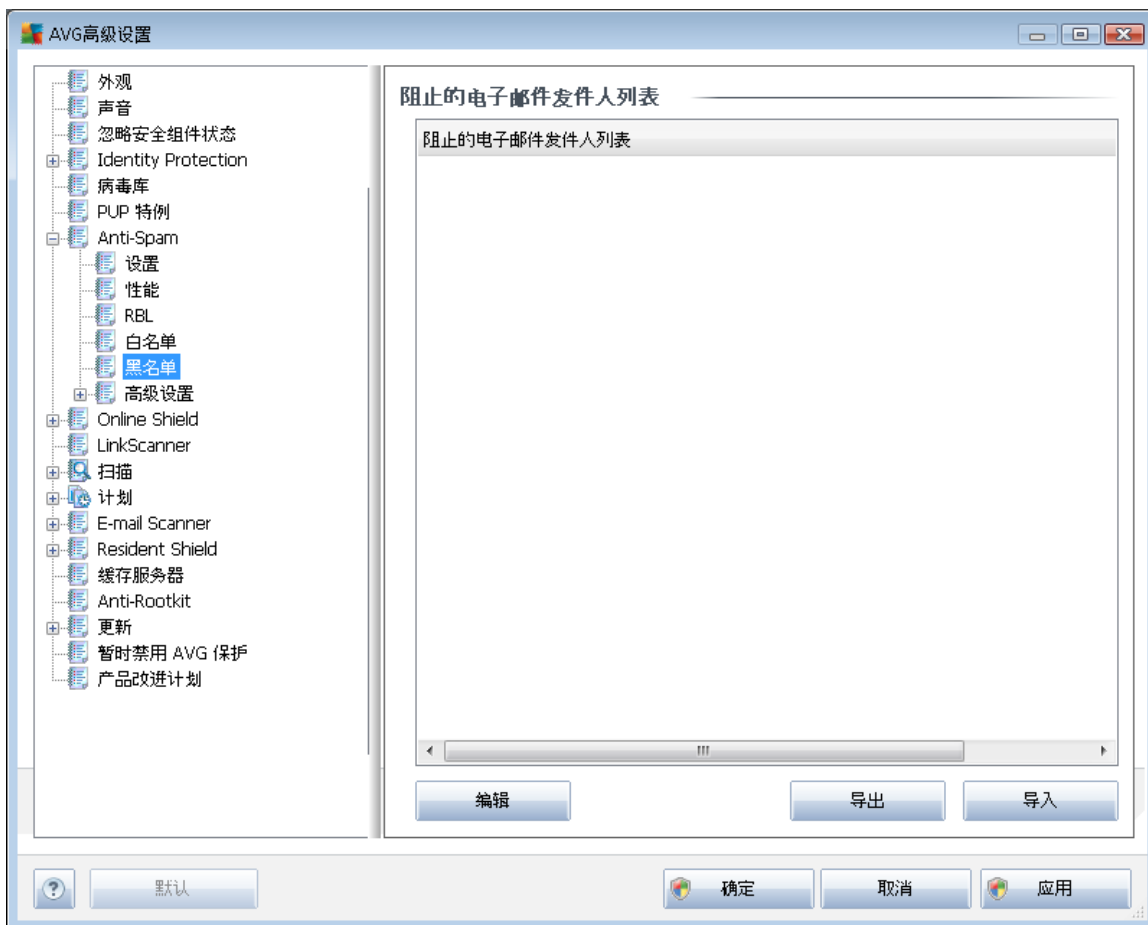
准备好一个这样的发件人和/或域名列表之后，您就可以通过以下任一方法输入它们：直接输入每个电子邮件地址或一次性导入整个地址列表。有下列控制按钮可供使用：



- **编辑** - 按此按钮可打开一个对话框，从中可手动列出地址（也可使用复制和粘贴功能）。每行请插入一项内容（发件人或域名）。
- **导出** - 如果您决定导出这些记录以用于某种用途，您可以按此按钮进行导出。所有记录都将被保存到一个纯文本文件中。
- **导入** - 如果您已经准备好一个包含电子邮件地址/域名的文本文件，您可以通过选择此按钮直接将其导入。文件内容每行只得包含一项信息（地址、域名）。

9.7.5. 黑名单

黑名单 选项用于打开一个对话框，其中列有已阻止的发件人的所有电子邮件地址和域名，这些发件人发送的邮件始终都会标记为 [垃圾邮件](#)。



在此编辑界面中，您可以整理一个预期会向您发送不需要的邮件（[垃圾邮件](#)）的发件人名单。您还可以整理一个您预期会发来垃圾邮件的完整域名（如 *spammingcompany.com*）列表。来自所列出的地址/域的所有电子邮件都将被标识为垃圾邮件。

准备好一个这样的发件人和/或域名列表之后，您就可以通过以下任一方法输入它们：直接输入每个电子邮件地址或一次性导入整个地址列表。有下列控制按钮可供使用：

- **编辑** - 按此按钮可打开一个对话框，从中可手动列出地址（也可使用复制和粘贴

功能)。每行请插入一项内容（发件人或域名）。

- **“导出”** - 如果您决定导出这些记录以用于某种用途，您可以按此按钮进行导出。所有记录都将被保存到一个纯文本文件中。
- **导入** - 如果您已经准备好一个包含电子邮件地址/域名的文本文件，您可以通过选择此按钮直接将其导入。

9.7.6. 高级设置

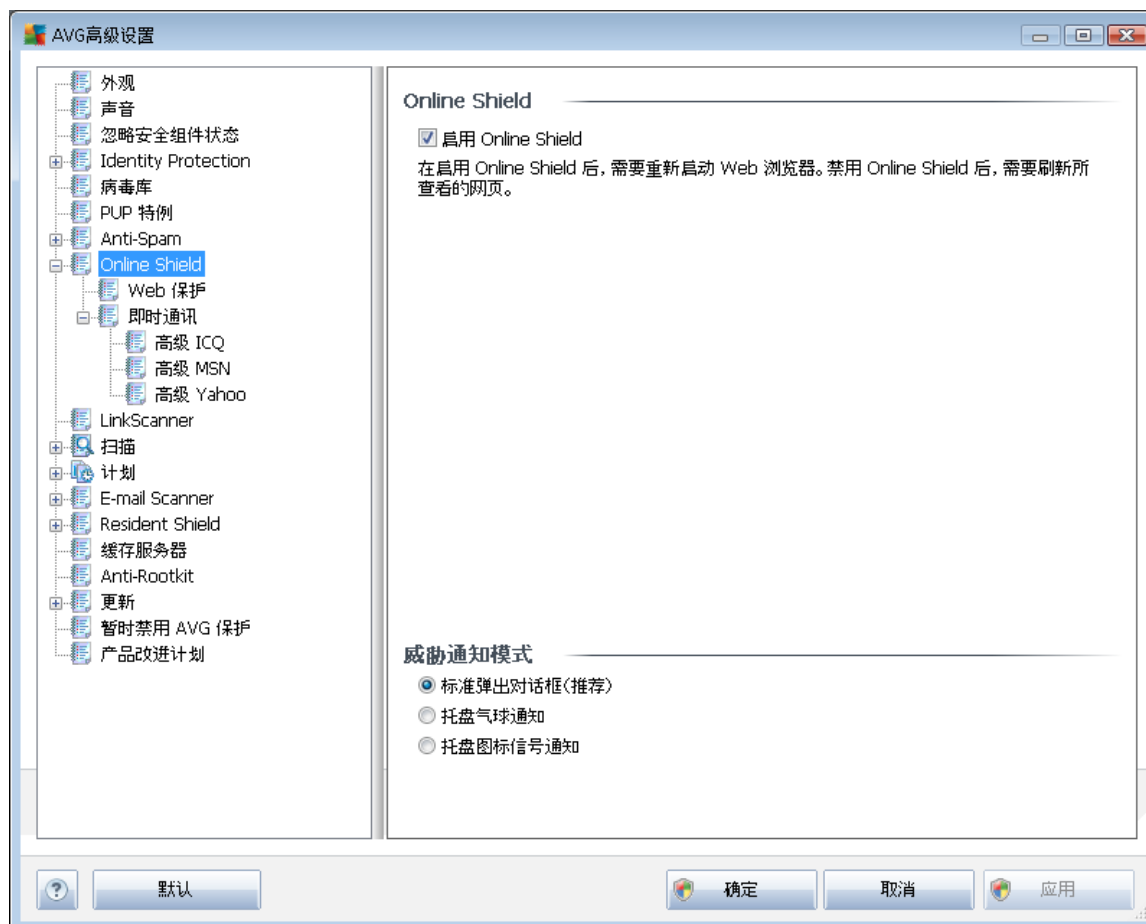
“高级设置”分支包含大量针对 Anti-Spam 组件的设置选项。这些设置旨在面向经验丰富的用户，尤其是需要全面配置反垃圾邮件保护从而实现最佳的电子邮件服务器保护的网管员。因此，我们未对各个对话框提供其它帮助信息；不过，在用户界面中直接提供了有关每个选项的简短说明。

如果您对 Spamcatcher (MailShell Inc.) 的高级设置不是非常熟悉，强烈建议您不要更改任何设置。更改不当可能会导致性能严重降低或组件功能失常。

如果您依然认为自己需要对 [Anti-Spam](#) 配置进行高级更改，请遵照在用户界面中直接提供的说明操作。一般而言，在每一个对话框中都会有一项特定的功能，您可以对其进行编辑 - 其说明总是被包含在该对话框本身中：

- **缓存** - 指纹、域声誉、LegitRepute
- **培训** - 词语条目上限、自动培训阈值、权重
- **过滤** - 语言列表、国家/地区列表、批准的 IP、阻止的 IP、阻止的国家/地区、阻止的字符集、冒牌发件人
- **RBL** - RBL 服务器、多重攻击、阈值、超时、最大 IP 数
- **Internet 连接** - 超时、代理服务器、代理服务器身份验证

9.8. Online Shield



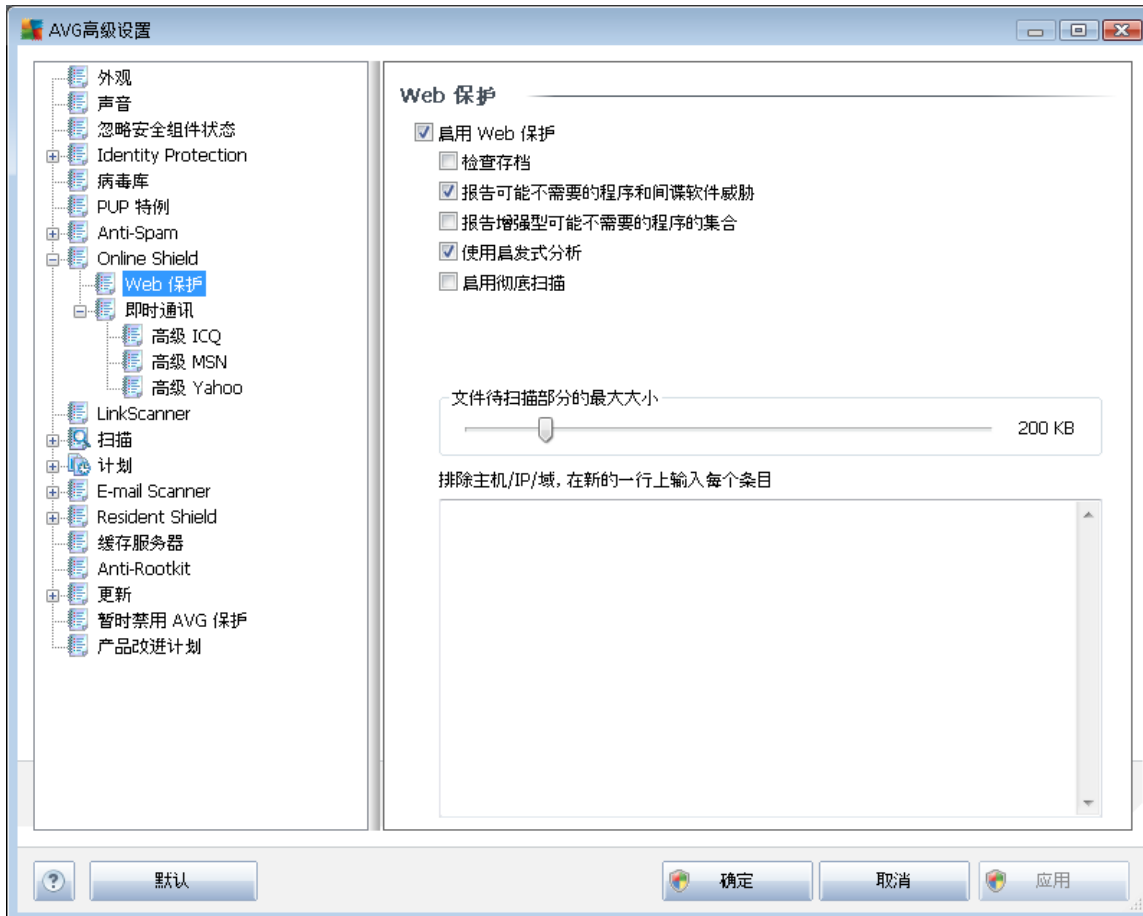
“Online Shield”对话框允许通过 **“启用 Online Shield”** 选项激活/停用整个 **Online Shield** 组件（默认情况下已启用）。有关此组件的进一步高级设置，请继续访问导航树中列出的后续对话框：

- [Web 保护](#)
- [即时通讯](#)

威胁通知模式

在此对话框的底部区域，请选择您希望通过哪种方式获知可能检测到的威胁的情况：通过标准的弹出对话框、通过任务栏气球通知，还是通过任务栏图标信息。

9.8.1. Web 保护



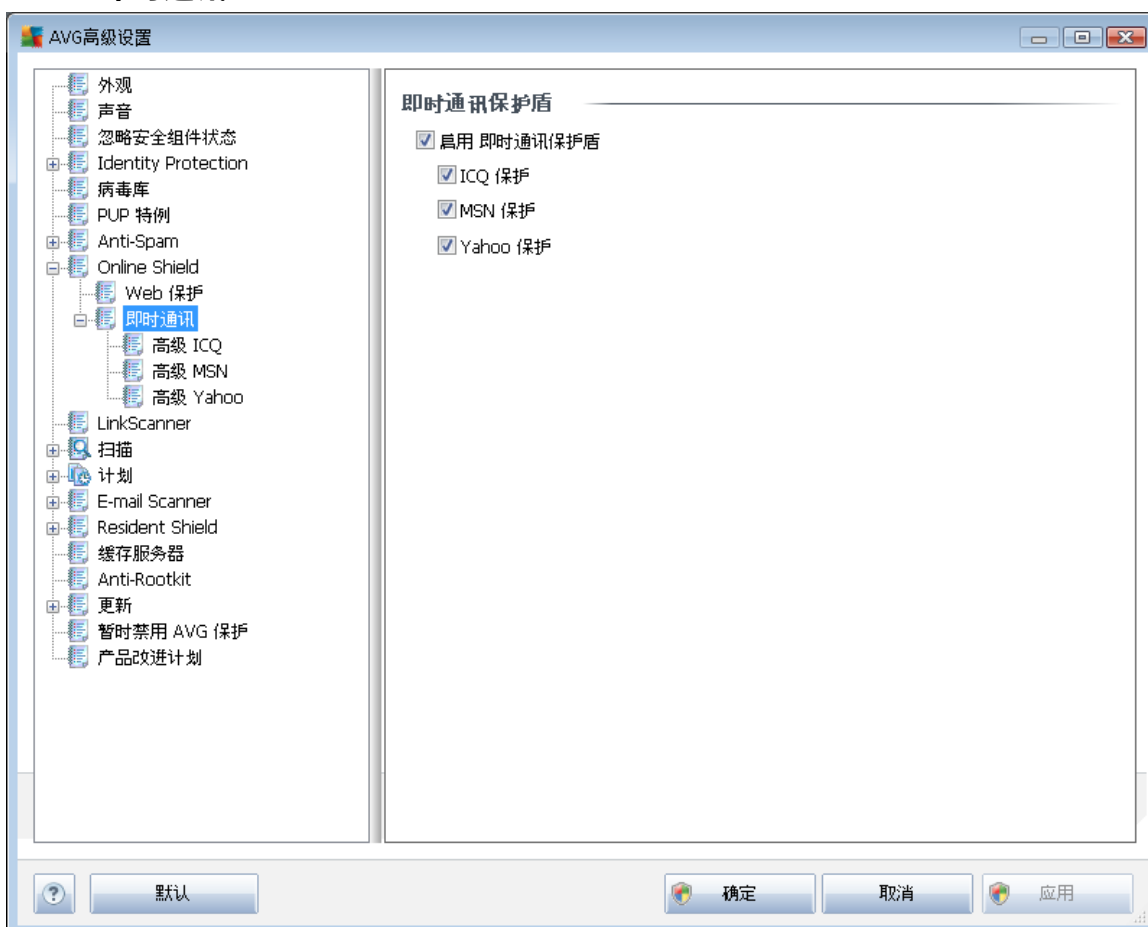
在 **“Web 保护”** 对话框中，您可以编辑该组件的与网站内容扫描有关的配置。在编辑界面中，可以配置下列基本选项：

- **“启用 Web 保护”** - 此选项用于确认 [Online Shield](#) 应对 www 页面内容进行扫描。如果启用此选项（默认情况下已启用），则您可以进一步启用/禁用以下项：
 - **“检查存档”**（默认情况下已禁用）：扫描要显示的 www 页面中可能包含的存档的内容。
 - **“报告可能不需要的程序和间谍软件威胁”** -（默认情况下已启用）：选中此框可激活 [Anti-Spyware](#) 引擎，进行间谍软件和病毒扫描。[间谍软件属于疑似恶意软件类软件：虽然它通常代表了安全风险，但有些程序也可能是被特意安装的。](#)建议保持此功能的激活状态，因为此功能会使计算机更加安全。
 - **“报告更多可能不需要的程序”**（默认情况下已禁用）：选中此框可检测更多 [间谍软件](#)：程序直接从制造商处获得时极其安全而无害，但之后却可能被滥用以达到恶意目的。这项附加措施可以进一步提高计算机的安全性，但也可能会阻止合法程序，因此默认情况下已将其禁用。



- **“使用启发式分析”**（默认情况下已启用）：使用 [启发式分析](#) 方法（在虚拟的计算机环境中对已扫描对象的指令进行动态模拟）扫描要显示的页面的内容。
- **“启动彻底扫描”**（默认情况下已禁用）- 在特定情况下（怀疑计算机受到感染），您可以选中此选项以激活最全面的扫描算法，该算法甚至会对计算机上极难被感染的区域进行扫描以确保绝对安全。不过要记住，此方法相当耗时。
- **“文件待扫描部分的最大大小”**-如果显示的页面中包含文件，您甚至可以在将这些文件下载至计算机之前对其内容进行扫描。但是，扫描大型文件需要一段时间，网页的下载过程可能会显著变慢。可用滑块指定仍然需要使用 [Online Shield](#) 扫描的文件的大小上限。即使所下载的文件大于指定大小，因而不会经过 Online Shield 扫描，您仍会受到保护：如果此文件受到感染，[Resident Shield](#) 会立即检测到它。
- **“排除主机/IP/域”**- 在此文本字段中您可以键入 [Online Shield](#) 不应扫描的服务器的确切名称（主机、IP 地址、带掩码的 IP 地址或 URL）或其不应扫描的域。因此，只应排除您可以完全确定绝不会提供危险网站内容的主机。

9.8.2. 即时通讯



在 **“即时通讯保护盾”** 对话框中，可编辑涉及即时通讯扫描的 [Online Shield](#) 组件设置。目前支持以下三种即时消息传递程序：**ICQ**、**MSN** 和 **Yahoo** - 如果要让 [Online Shield](#) 验证在

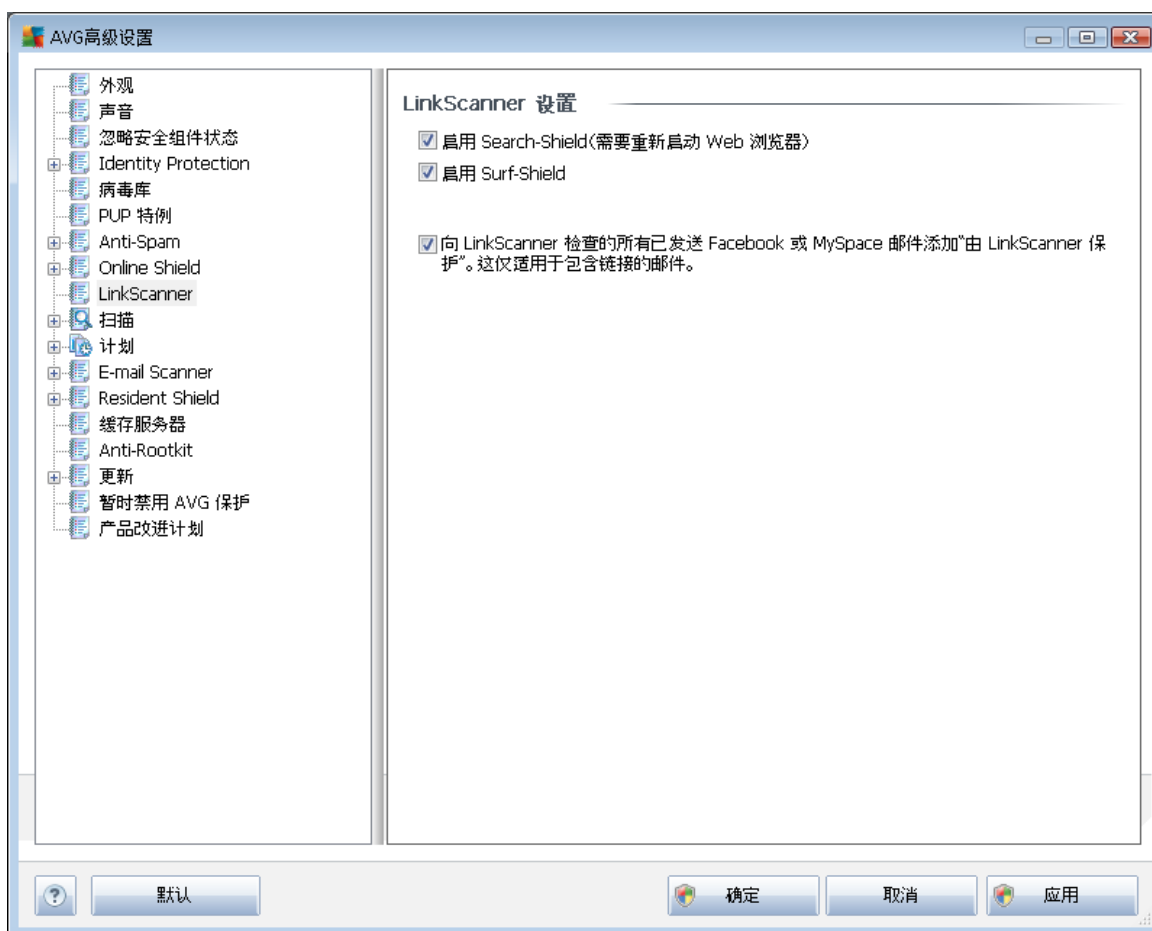


线通信内容是否无病毒，请勾选上述每种程序的相应选项。

如果要进一步指定允许/阻止的用户，则可查看和编辑相应的对话框（**“高级 ICQ”**、**“高级 MSN”**、**“高级 Yahoo”**），然后指定**白名单**（允许与您通信的用户名单）和**黑名单**（应被阻止的用户）。

9.9. Link Scanner

通过 **LinkScanner 设置** 对话框，可启用/禁用 **LinkScanner** 的以下基本功能：



- **启用 Search-Shield** - （默认情况下已启用）：在对 Google, Yahoo! JP、WebHledani、Yandex、百度、Bing、AOL、AltaVista、EarthLink、Ask、Seznam、eBay、Twitter、Digg 或 SlashDot 等搜索引擎所返回的网站内容进行事先检查后，就所执行的搜索显示警告通知图标。
- **启用 Surf-Shield** - （默认情况下已启用）：主动（实时）防范访问网站时遇到的漏洞利用网站。当用户通过 Web 浏览器（或任何其它使用 HTTP 的应用程序）访问已知的恶意网站连接及其漏洞利用内容时，将会对这些网站及其内容进行阻止。
- **添加通过 LinkScanner 保护...** 选中此项可确认您希望将关于 **Link Scanner** 检



查的验证通知输入从 Facebook 和 MySpace 社交网络发送且包含活动的超链接的所有消息。

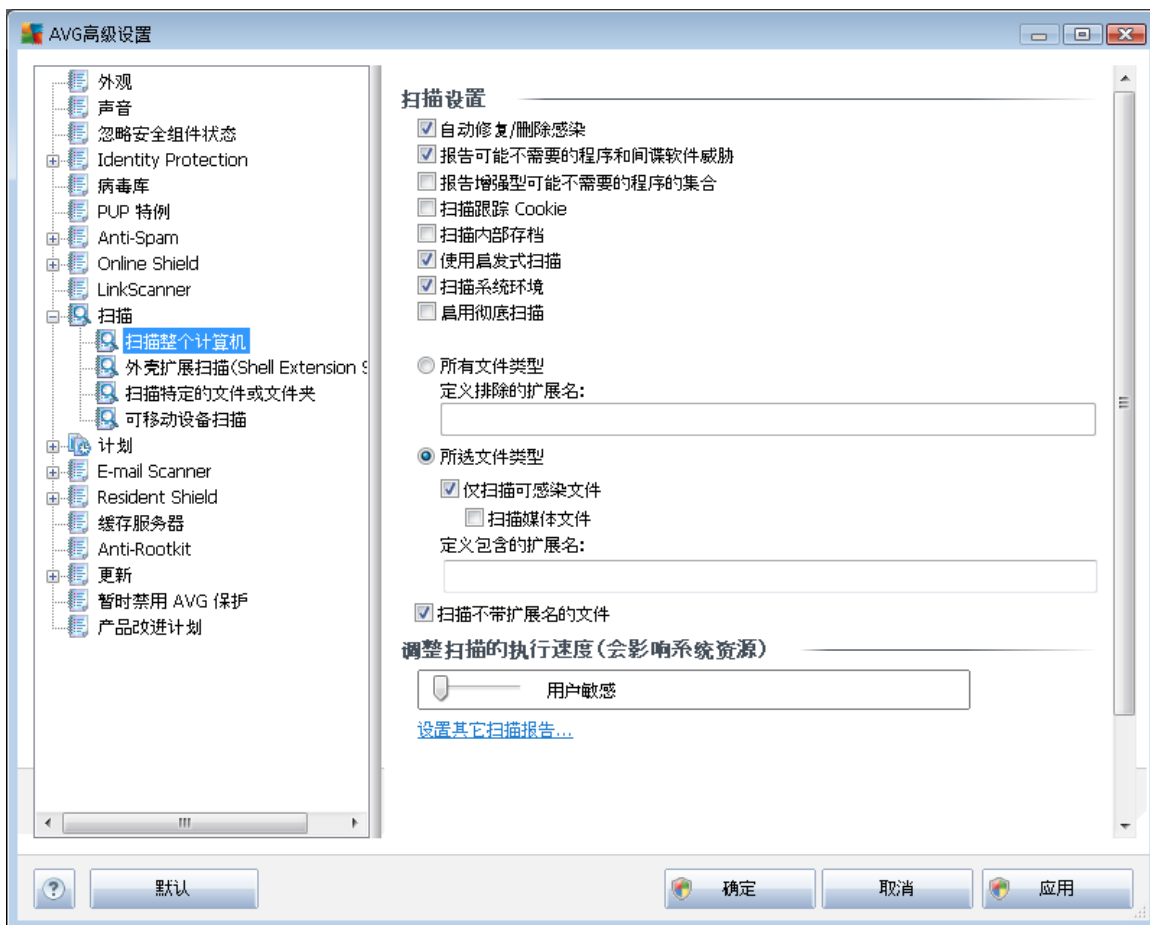
9.10. 扫描

高级扫描设置分为四种类别，分别对应软件供应商定义的以下特定扫描类型：

- **扫描整个计算机** - 对整个计算机进行的标准预定义扫描
- **外壳扩展扫描** - 直接从 Windows 资源管理器环境中对选定对象进行的特定扫描
- **扫描特定的文件或文件夹** - 对计算机的选定区域进行的标准预定义扫描
- **可移动设备扫描** - 对连接到计算机的可移动设备进行的特定扫描

9.10.1. 扫描整个计算机

通过“**扫描整个计算机**”选项，您可以编辑软件供应商预定义的其中一项扫描（即“**扫描整个计算机**”）的参数：



扫描设置

“扫描设置”区域提供了可以选择启用/禁用的扫描参数的列表：

- **自动修复/移除感染**（默认情况下已启用）- 如果在扫描期间发现病毒并且有修复方案，则可以自动对其进行修复。如果不能自动修复受感染文件，则会将受感染对象移到 **病毒库** 中。
- **报告可能不需要的程序和间谍软件威胁**（默认情况下已启用）- 选中此框可激活 **Anti-Spyware** 引擎以及针对间谍软件和病毒的扫描。间谍软件属于疑似恶意软件类软件：虽然它通常代表了安全风险，但有些程序也可能是被特意安装的。建议保持此功能的激活状态，因为此功能会使计算机更加安全。
- **报告更多可能不需要的程序**（默认情况下已禁用）- 选中此框可检测更多 **间谍软件**：程序直接从制造商处获得时极其安全而无害，但之后却可能被滥用以达到恶意目的。这项附加措施可以进一步提高计算机的安全性，但也可能会阻止合法程序，因此默认情况下已将其禁用。
- **扫描跟踪 Cookie**（默认情况下已启用）- **Anti-Spyware** 组件的此参数用于定义在扫描期间应检测 Cookie（HTTP Cookie 用于验证、跟踪和维护有关用户的特定信息，例如网站首选项或电子购物车中的内容）
- **扫描压缩包**（默认情况下已禁用）- 此参数定义扫描时应检查存储在压缩包（如 ZIP 和 RAR 等）中的所有文件。
- **使用后发式扫描**（默认情况下已启用）- 启发式分析（在虚拟的计算机环境中对已扫描对象的指令进行动态模拟）将成为在扫描期间用来进行病毒检测的方法之一；
- **扫描系统环境**（默认情况下已启用）- 扫描时还将检查您计算机的系统区域。
- **启动彻底扫描**（默认情况下已禁用）- 在特定情况下（怀疑计算机受到感染），您可以选中此选项以激活最全面的扫描算法，该算法甚至会对计算机上极难被感染的区域进行扫描以确保绝对安全。不过要记住，此方法相当耗时。

此外，您还应决定要扫描的文件类型：

- **所有文件类型**，选择此选项可以通过提供一系列由逗号分隔（保存后逗号会变成分号）、不应扫描的文件扩展名来定义一些排除在扫描范围之外的特例；
- **所选文件类型** - 可以指定希望仅扫描可能受到感染的文件（将不扫描不可能遭到感染的文件，例如某些纯文本文件或某些其它的非可执行文件），其中包括媒体文件（视频、音频文件 - 如果将此框保留为未选中状态，则会进一步缩短扫描时间，因为这些文件通常很大，不太可能受到病毒感染）。此外，您还可以通过扩展名指定哪些文件是始终应扫描的文件。
- 您也可以选择指定要 **扫描不带扩展名的文件** - 默认情况下此选项已启用；我们建议，除非确有必要更改，否则将其保持启用。不带扩展名的文件相当可疑，应随时对此类文件进行扫描。

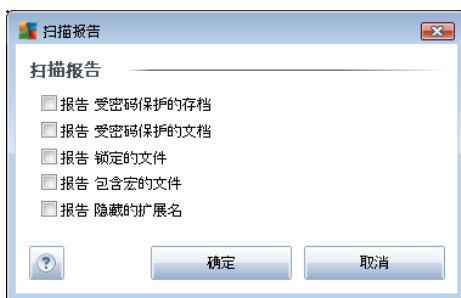


调整扫描的完成速度

在“**调整扫描的完成速度**”区域中，您可以根据系统资源的使用情况进一步指定所需的扫描速度。默认情况下，此选项值设为**用户敏感信息**级别，即自动确定资源的使用。如果您希望加快扫描运行速度，那么扫描所用的时间较少，但在扫描期间会大大增加对系统资源的占用，因而会降低 PC 上其它活动的速度（当**计算机处于打开状态但当前无人使用时可以采用此选项**）。另一方面，通过延长扫描的持续时间，可以减少对系统资源的使用。

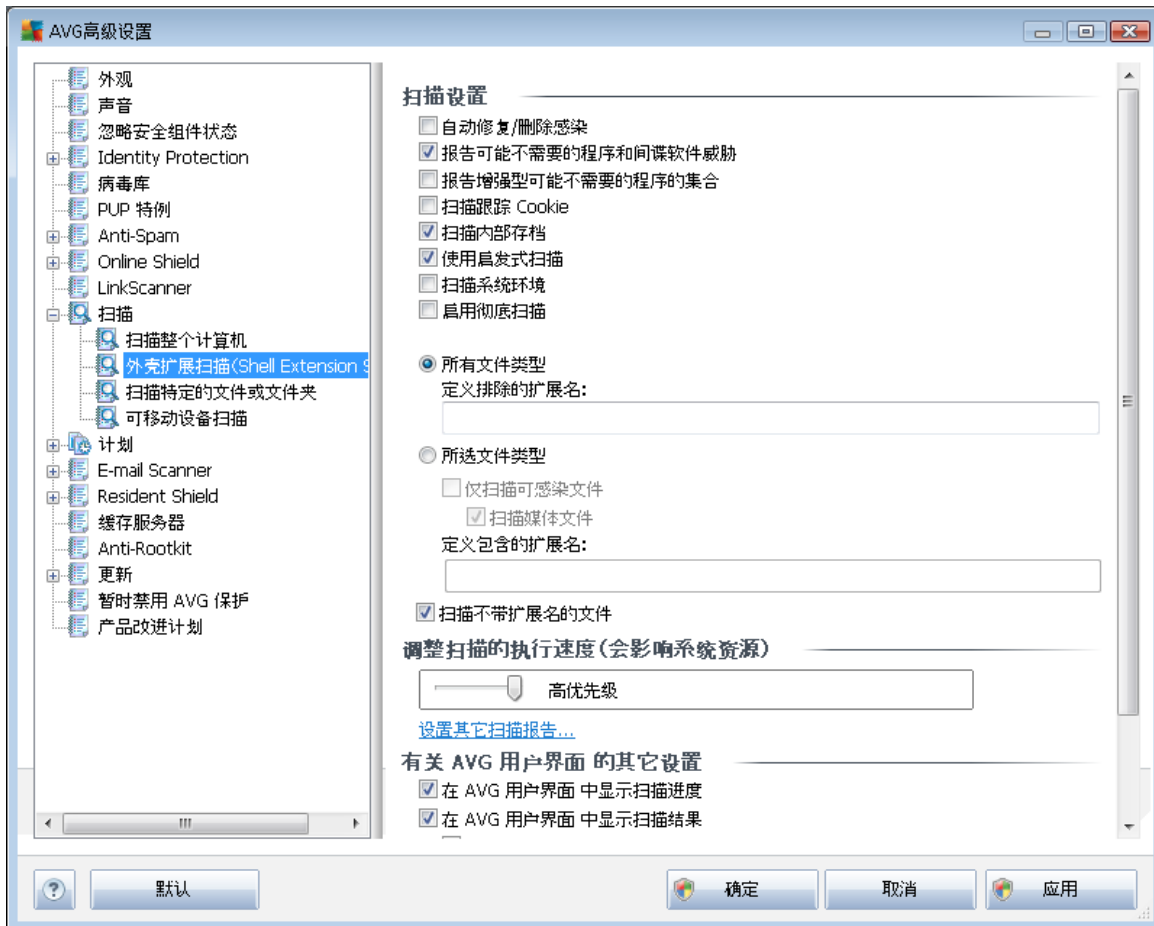
设置其它扫描报告...

单击“**设置其它扫描报告...**”链接可打开一个名为“**扫描报告**”的独立对话框窗口，在此窗口中您可以通过勾选若干项来定义应报告哪些扫描结果：



9.10.2. 外壳扩展扫描

与前面的“**扫描整个计算机**”项类似，名为“**外壳扩展扫描**”的此项也提供了若干选项，用以编辑由软件供应商预定义的扫描。这一次，配置则与[直接从 Windows 资源管理器中对特定对象启动的扫描](#)（此启动环境即为外壳扩展）相关，请参见[“在 Windows 资源管理器中扫描”](#)一章：



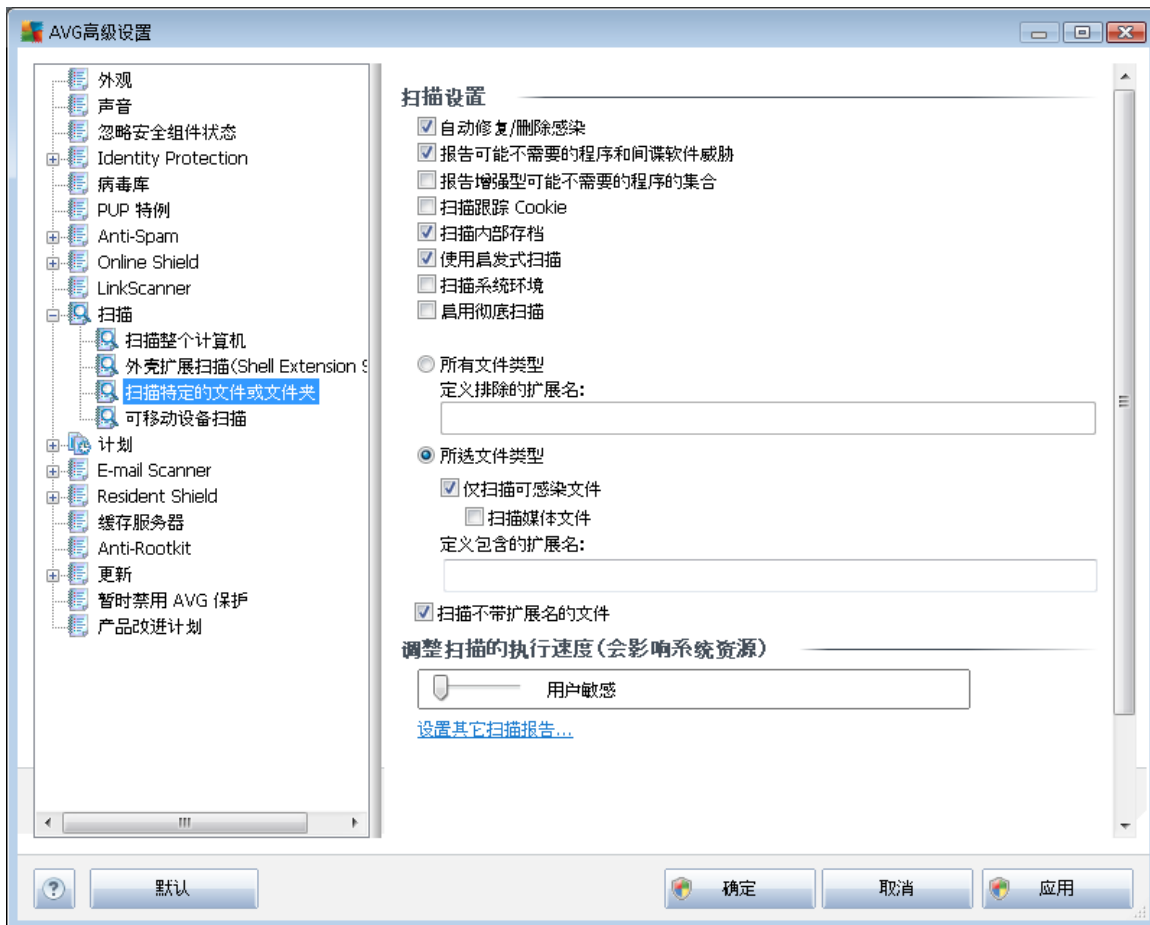
相应的参数列表与可用于“[扫描整个计算机](#)”的参数列表相同。不过，二者的默认设置是不同的（例如，扫描整个计算机默认情况下不检查压缩包，但是会扫描系统环境，而外壳扩展扫描则相反）。

注意：有关特定参数的说明，请参阅“[AVG 高级设置/扫描/扫描整个计算机](#)”一章。

与“[扫描整个计算机](#)”对话框相比，“[外壳扩展扫描](#)”对话框还包含名为“**与 AVG 用户界面相关的其它设置**”部分，您可以在其中指定是否希望能够从 AVG 用户界面中访问扫描进度和扫描结果。此外，您还可以定义仅当在扫描期间检测到感染的情况下才应显示扫描结果。

9.10.3. 扫描特定的文件或文件夹

‘扫描特定的文件或文件夹’的编辑界面与‘扫描整个计算机’编辑对话框完全相同。所有配置选项都一样；不过，‘扫描整个计算机’的默认设置更为严格：

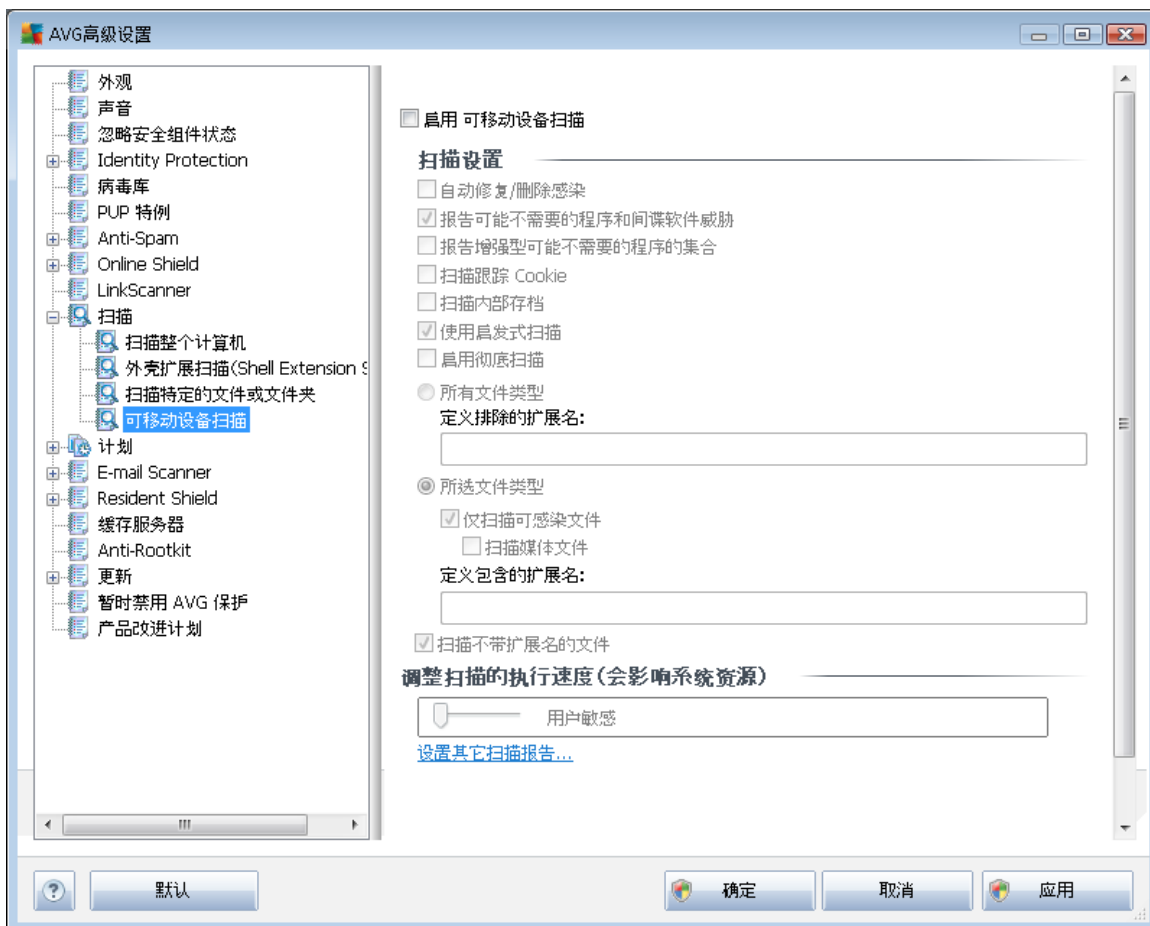


在此配置对话框中设置的所有参数都仅适用于选定使用‘扫描特定的文件或文件夹’功能进行扫描的区域！

注意：有关特定参数的说明，请参阅“AVG 高级设置/扫描/扫描整个计算机”一章。

9.10.4. 可移动设备扫描

“可移动设备扫描”的编辑界面也非常类似于 [“扫描整个计算机”](#) 编辑对话框：



当您将任何可移动设备连接到您的计算机时，“可移动设备扫描”会自动启动。默认情况下，此扫描已禁用。不过，扫描可移动设备有无潜在威胁非常重要，因为它们是一大感染来源。若要让此扫描准备就绪并在需要时自动启动，请选中 **“启用可移动设备扫描”** 选项。

注意：有关特定参数的说明，请参阅 [“AVG 高级设置/扫描/扫描整个计算机”](#) 一章。

9.11. 计划

在 **“计划”** 区域中，您可以编辑以下各项的默认设置：

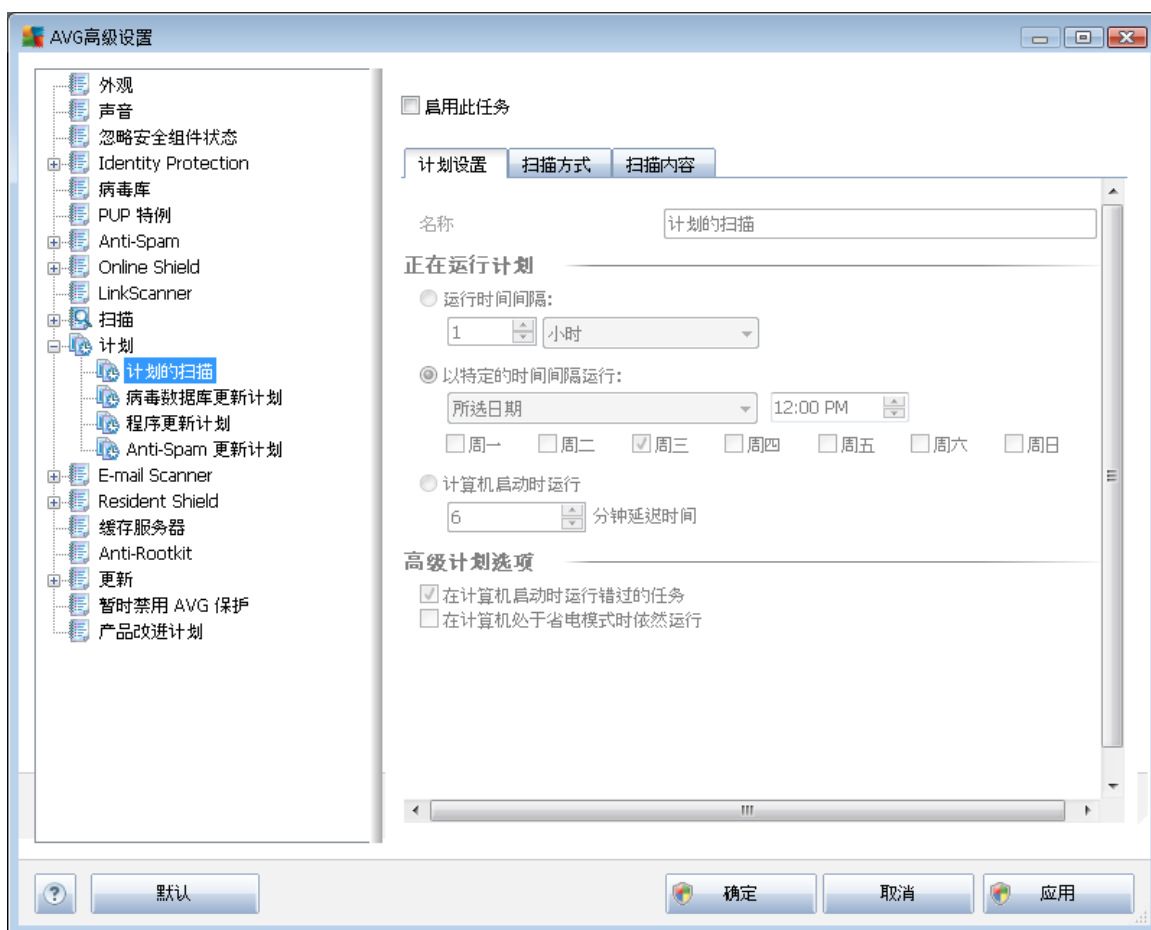
- [计划的扫描](#)
- [病毒数据库更新计划](#)
- [程序更新计划](#)



- [Anti-Spam 更新计划](#)

9.11.1. 计划的扫描

可在三个选项卡上编辑（或设置新计划）计划内扫描的参数。在每个选项卡中，都可以先选中/取消选中 **启用此任务** 选项，以便直接暂时停用计划内测试，然后按需启用计划内测试：



然后，在名为 **名称** 的文本字段（已对所有默认计划停用此字段）中，有程序供应商对此计划指定的名称。对于新添加的计划（可以通过在左侧导航树中的 **计划的扫描** 项上单击鼠标右键来添加新计划），您可以自行指定名称，在这种情况下此文本字段将可供编辑。请尽量始终对扫描使用简洁、适当的描述性名称，以便以后更容易将其与其它扫描辨别开来。

例如：将扫描命名为 **新扫描** 或 **我的扫描** 并不适当，因为这些名称并未指出扫描实际检查的内容。相反，**系统区域扫描** 等名称就可以称得上是不错的描述性名称。此外，没有必要的在扫描的名称中指定它是对整个计算机的扫描还是仅扫描选定的文件或文件夹 - 您自己创建和计划的扫描始终都属于 [扫描选定的文件或文件夹](#)。

在此对话框中，可以进一步定义下列扫描参数：



计划执行

可在此指定新计划的扫描启动任务的时间间隔。此时间间隔的定义方式有三种：指定经过一段特定的时间后重新启动扫描（**‘每隔...运行一次’**；或定义确切的日期和时间（**‘以特定的时间间隔运行...’**；也可以定义扫描启动操作应关联的事件（**‘操作条件：计算机启动时’**）。

高级计划选项

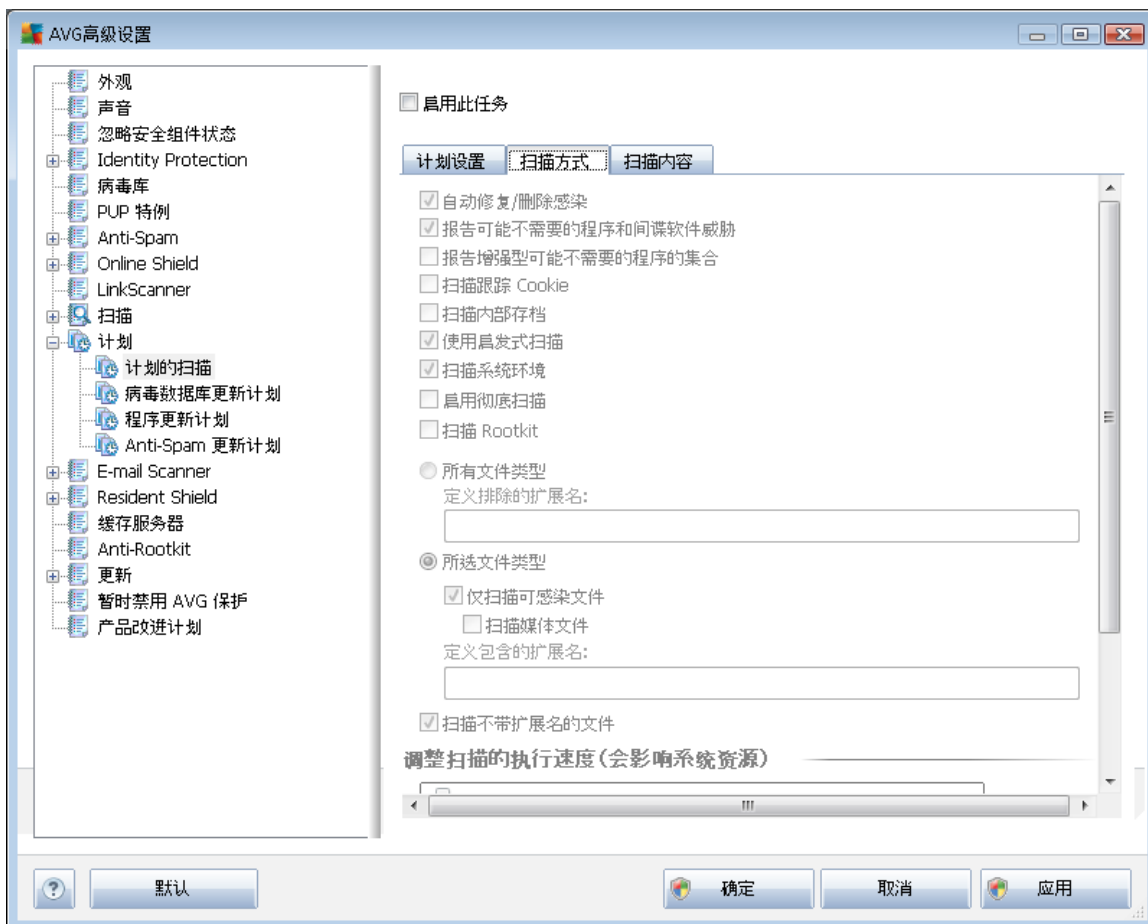
在此区域中，可以定义当计算机处于省电模式或完全关闭时，应该/不应启动扫描的条件。

每当计划的扫描在您指定的时间启动时，都会在 [AVG 系统任务栏图标](#) 上方打开一个弹出窗口，以此方式将这种情况通知您：



随即便会出现一个新的 [AVG 系统任务栏图标](#)（以彩色显示并带闪光），告诉您计划的扫描正在运行。右键单击这个表示正在运行扫描的 AVG 图标可打开一个上下文菜单，在此菜单中您可以决定暂停甚至停止正在运行的扫描，还可以更改当前运行的扫描的优先级：





‘扫描方式’选项卡上包含一个扫描参数列表，可以选择启用/禁用这些参数。默认情况下，大多数参数都处于启用状态，并将在扫描过程中发挥作用。除非有必要更改这些设置，否则我们建议保留预定义的配置：

- **自动修复/移除感染**（默认情况下已启用）：如果在扫描期间发现病毒并且有修复方案，则可以自动对其进行修复。如果不能自动修复受感染文件，则会将受感染对象移到 [病毒库](#) 中。
- **报告可能不需要的程序和间谍软件威胁**（默认情况下已启用）：选中此框可激活 [Anti-Spyware](#) 引擎以及针对间谍软件和病毒的扫描。[间谍软件属于疑似恶意软件类软件：虽然它通常代表了安全风险，但有些程序也可能是被特意安装的。](#)建议保持此功能的激活状态，因为此功能会使计算机更加安全。
- **报告更多可能不需要的程序**（默认情况下已禁用）：选中此框可检测更多 [间谍软件](#)：程序直接从制造商处获得时极其安全而无害，但之后却可能被滥用以达到恶意目的。这项附加措施可以进一步提高计算机的安全性，但也可能会阻止合法程序，因此默认情况下已将其禁用。
- **扫描跟踪 Cookie**（默认情况下已禁用）：[Anti-Spyware](#) 组件的此参数用于定义在扫描期间应检测 Cookie ([HTTP Cookie 用于验证、跟踪和维护有关用户的特定信](#)



息，例如网站首选项或电子购物车中的内容)

- **扫描压缩包** (默认情况下已禁用)：此参数定义扫描时应检查所有文件，即使这些文件被存储在压缩包 (如 ZIP 和 RAR 等) 内也不例外
- **使用后发式扫描** (默认情况下已启用)：后发式分析 (在虚拟的计算机环境中对已扫描对象的指令进行动态模拟) 将成为在扫描期间用来进行病毒检测的方法之一；
- **扫描系统环境** (默认情况下已启用)：扫描时还将检查您计算机的系统区域；
- **启动彻底扫描** (默认情况下已禁用) - 在特定情况下 (怀疑计算机受到感染)，您可以选中此选项以激活最全面的扫描算法，该算法甚至会对计算机上极难被感染的区域进行扫描以确保绝对安全。不过要记住，此方法相当耗时。
- **扫描 Rootkit** (默认情况下已禁用)：如果您要将 Rootkit 检测纳入对整个计算机的扫描，请勾选此项。在 [Anti-Rootkit](#) 组件中，Rootkit 检测功能也可单独作为一项功能供用户使用；

此外，您还应决定要扫描的文件类型：

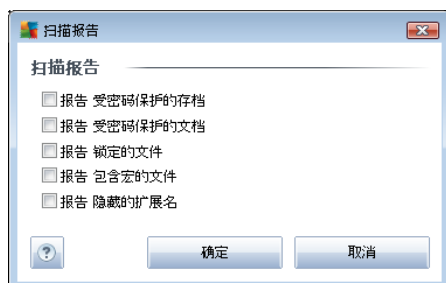
- **所有文件类型**，选择此选项可以通过提供一系列由逗号分隔 (保存后逗号会变成分号)、不应扫描的文件扩展名来定义一些排除在扫描范围之外的特例；
- **所选文件类型** - 可以指定希望仅扫描可能受到感染的文件 (将不扫描不可能遭到感染的文件，例如某些纯文本文件或某些其它的非可执行文件)，其中包括媒体文件 (视频、音频文件 - 如果将此框保留为未选中状态，则会进一步缩短扫描时间，因为这些文件通常很大，不太可能受到病毒感染)。此外，您还可以通过扩展名指定哪些文件是始终应扫描的文件。
- 您也可以选择指定要**扫描不带扩展名的文件** - 默认情况下此选项已启用；我们建议，除非确有必要更改，否则将其保持启用。不带扩展名的文件相当可疑，应随时对此类文件进行扫描。

调整扫描的完成速度

在“**调整扫描的完成速度**”区域中，您可以根据系统资源的使用情况进一步指定所需的扫描速度。默认情况下，此选项值设为**用户敏感信息**级别，即自动确定资源的使用。如果您希望加快扫描运行速度，那么扫描所用的时间较少，但在扫描期间会大大增加对系统资源的占用，因而会降低 PC 上其它活动的速度 (当计算机处于打开状态但当前无人使用时可以采用此选项)。另一方面，通过延长扫描的持续时间，可以减少对系统资源的使用。

设置其它扫描报告

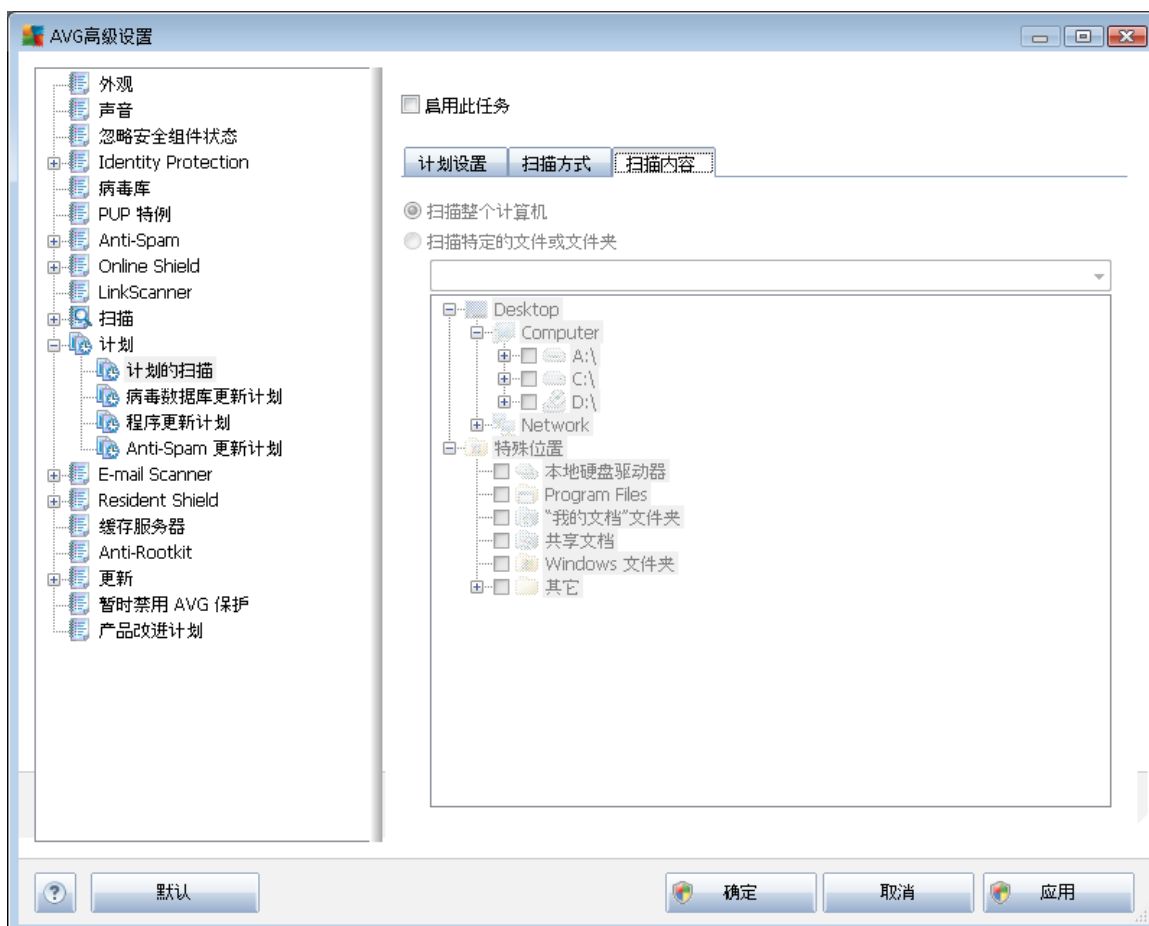
单击“**设置其它扫描报告...**”链接可打开一个名为“**扫描报告**”的独立对话框窗口，在此窗口中您可以通过勾选若干项来定义应报告哪些扫描结果：



其它扫描设置

单击 **其它扫描设置...** 可打开新的 **计算机关闭选项** 对话框，在此可以决定当扫描进程运行结束后，是否应自动关闭计算机。在确认此选项（**扫描完成时关闭计算机**）后，将激活一个新选项（**强制关闭锁定的计算机**），通过该选项，即使目前已锁定计算机也可关机。

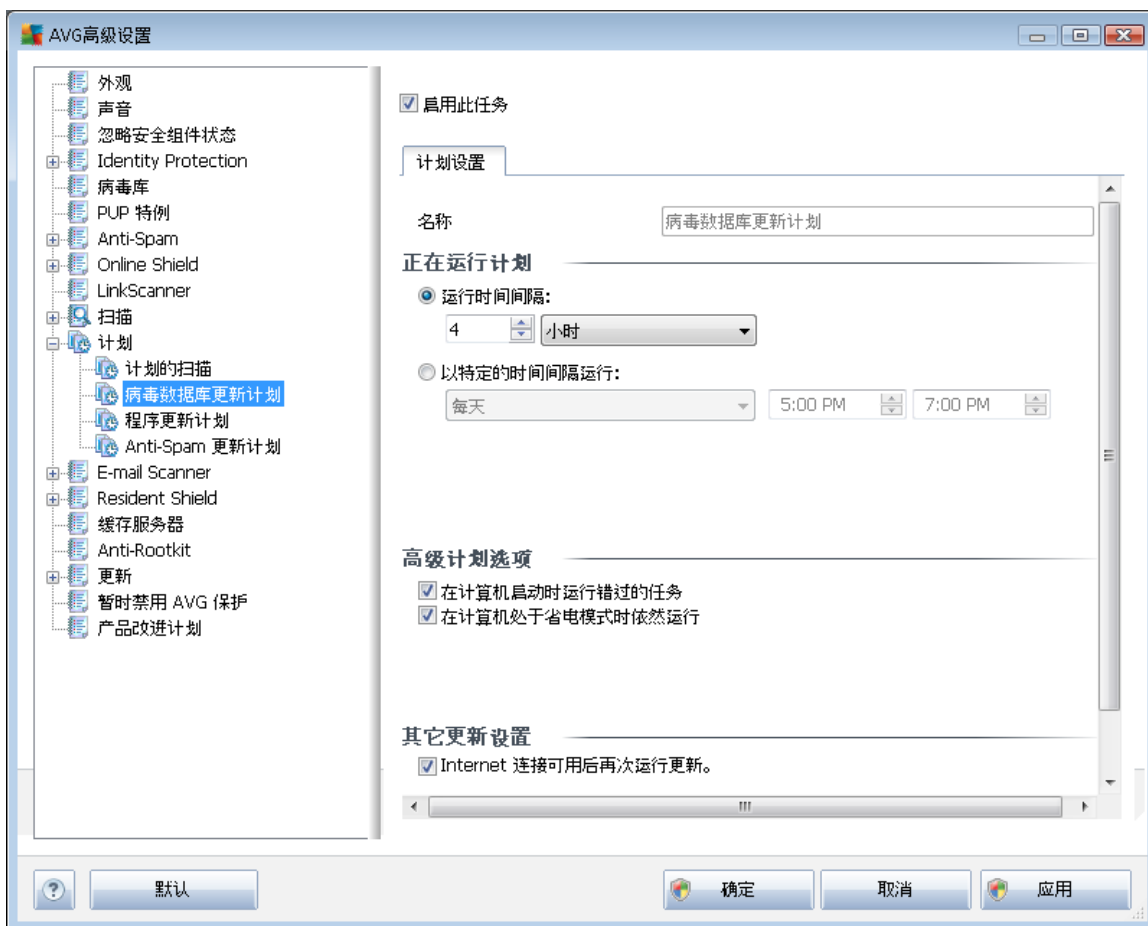




在“**扫描内容**”选项卡上，您可以定义您要计划的是 [扫描整个计算机](#) 还是 [扫描特定的文件或文件夹](#)。如果您选择的是“扫描特定的文件或文件夹”，则在此对话框底部将激活如图所示的树结构，您可以利用它来指定要扫描的文件夹。

9.11.2. 病毒数据库更新计划

如果**确实有必要**，则可取消选中**启用此任务**选项，以便直接暂时停用计划病毒数据库更新，然后再将其启用：



更新管理器组件有基本病毒数据库更新计划功能。在此对话框中，您可以设置病毒数据库更新计划的某些详细参数。在名为**‘名称’**的文本字段（已对所有默认计划停用此字段）中，有程序供应商对此计划指定的名称。

计划执行

在此区域中，请指定新计划的病毒数据库更新启动任务的时间间隔。通过指定反复在经过一段时间后启动更新（**‘每隔...运行一次’**），或通过指定确切的日期和时间（**‘在特定的时间运行...’**），均可定时。

高级计划选项

在此区域中，可以定义当计算机处于省电模式或完全关闭时，应该/不应启动病毒数据库更新的条件。



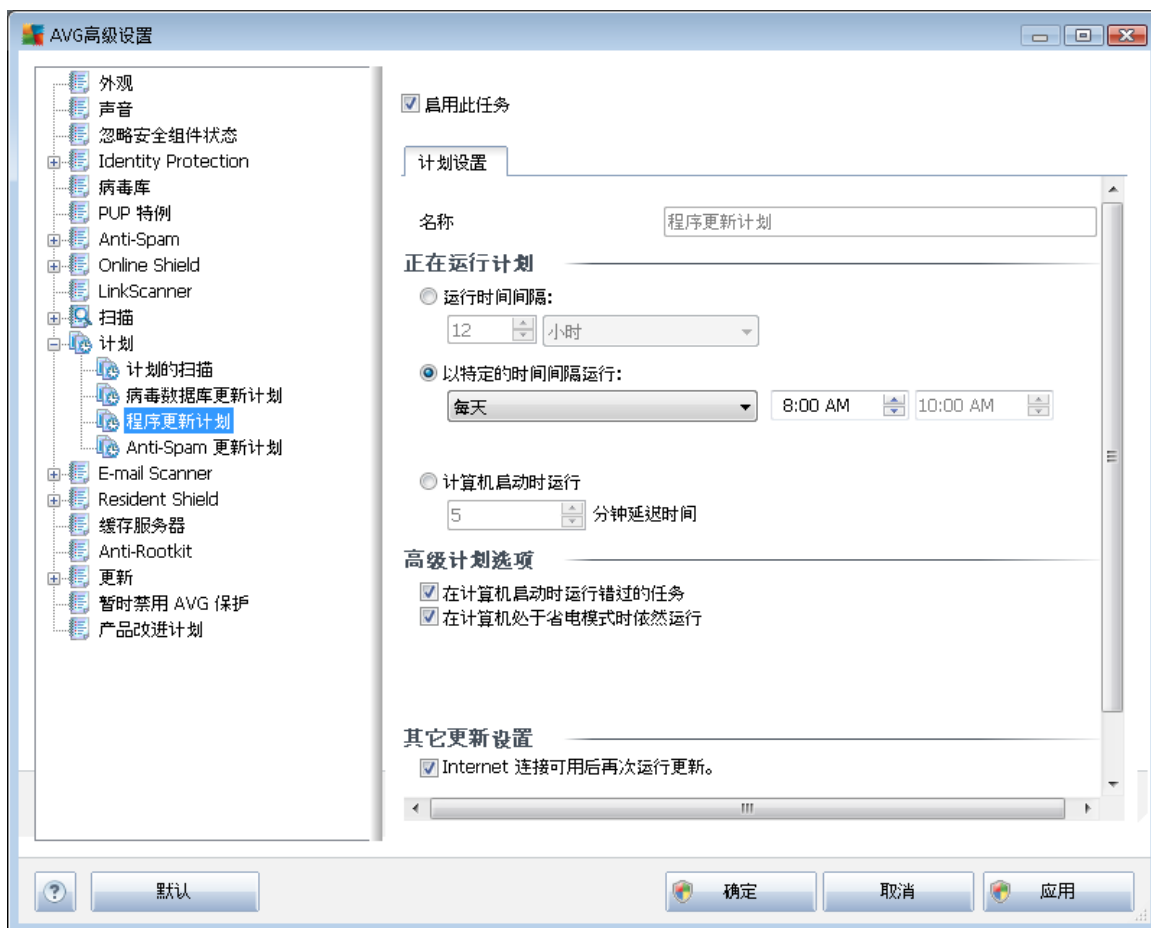
其它更新设置

最后，选中“**一旦 Internet 连接可用就再次运行更新**”选项可确保：如果 Internet 连接断开，导致更新过程失败，则在 Internet 连接恢复后更新过程会立即重新启动。

一旦计划的更新在您指定的时间启动，系统便会通过在 [AVG 系统任务栏图标](#) 上方打开的一个弹出窗口将此情况告知您（前提是您保留了 [高级设置/外观](#) 对话框的默认配置）。

9.11.3. 程序更新计划

如果**确实有必要**，则可取消选中**启用此任务**选项，以便直接暂时停用计划程序更新，然后再将其启用：



在名为**名称**的文本字段（已对所有默认计划停用此字段）中，有程序供应商对此计划指定的名称。

计划执行

请在此指定新计划的程序更新启动任务的时间间隔。此时间间隔的定义方式有三种：指



定经过一段特定的时间后重复启动更新（**‘每隔...运行一次’**，定义确切的日期和时间（**‘在特定的时间运行...’**），也可以定义更新启动操作应关联的事件（**‘计算机启动时的操作’**）。

高级计划选项

在此区域中，可以定义当计算机处于省电模式或完全关闭时，应该/不应启动程序更新的条件。

其它更新设置

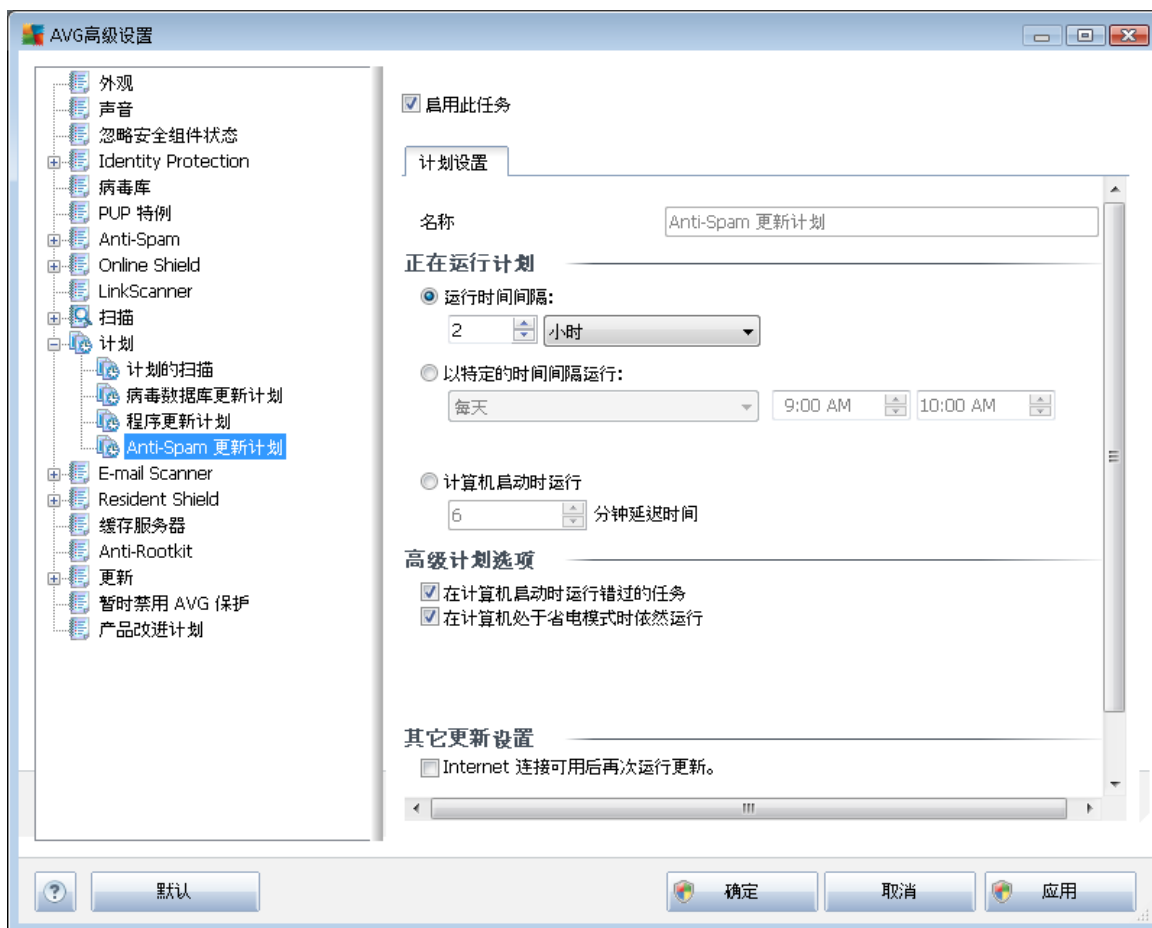
选中 **“一旦 Internet 连接可用就再次运行更新”** 选项可确保：如果 Internet 连接断开，导致更新过程失败，则在 Internet 连接恢复后更新过程会立即重新启动。

一旦计划的更新在您指定的时间启动，系统便会通过在 [AVG 系统任务栏图标](#) 上方打开的一个弹出窗口将此情况告知您（前提是您保留了 [高级设置/外观](#) 对话框的默认配置）。

注：如果计划程序更新和计划扫描同时执行，则更新进程优先，扫描会中断。

9.11.4. Anti-Spam 更新计划

如果**确实有必要**，则可取消选中**启用此任务**选项，以便直接暂时停用计划内 [Anti-Spam](#) 更新，然后再将其启用：



更新管理器 组件中有基本 Anti-Spam 更新计划功能。可在此对话框中设置更新计划的某些详细参数。在名为“名称”的文本字段（已对所有默认计划停用此字段）中，有程序供应商对此计划指定的名称。

计划执行

请在此指定新计划的 [Anti-Spam](#) 更新启动任务的时间间隔。通过指定反复在经过一段时间后启动 [Anti-Spam](#) 更新（**“每隔...运行一次”**），或定义确切的日期和时间（**“在特定的时间运行...”**），或可能定义要将更新启动操作与其关联起来的事件（**“计算机启动时的操作”**），均可定时。

高级计划选项

通过此部分，可定义计算机处于省电模式中或已彻底关闭时应该/不应该启动 [Anti-Spam](#)



更新的情况。

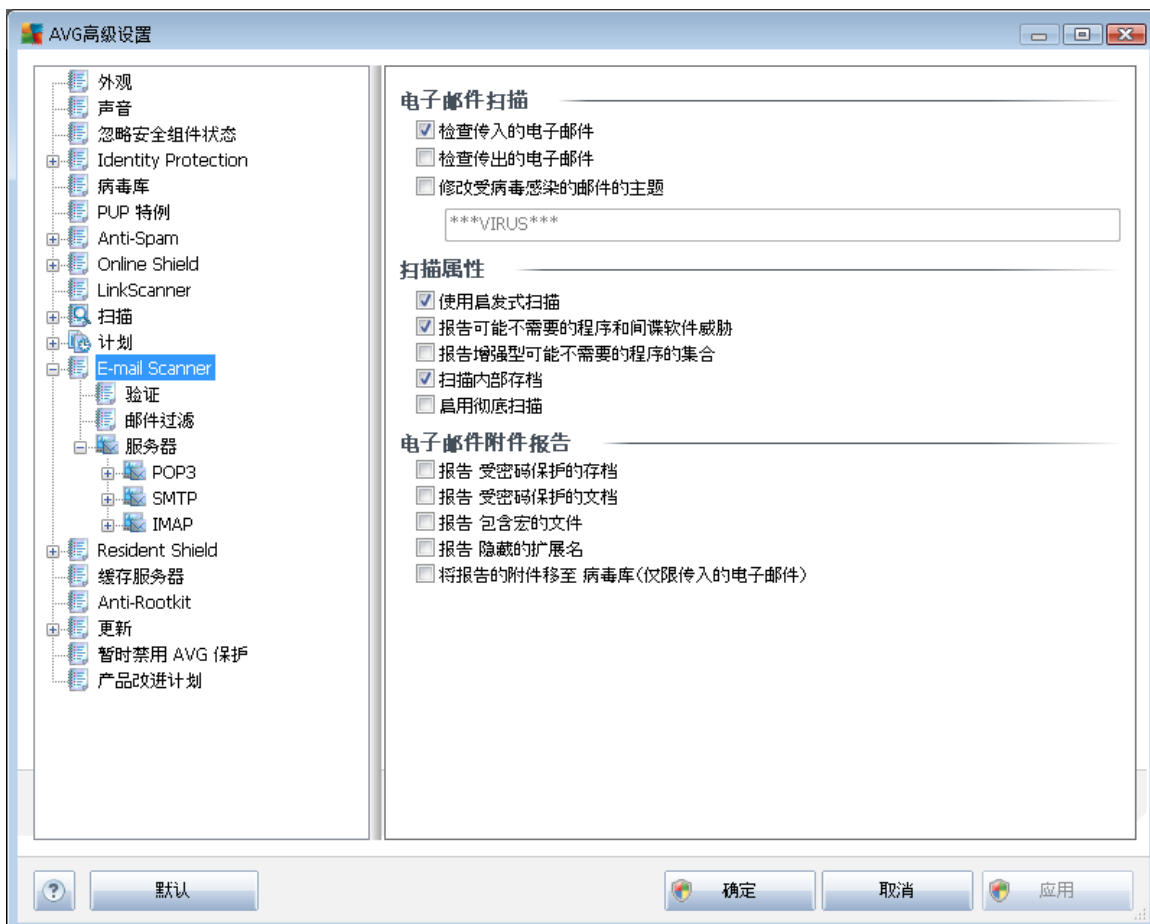
其它更新设置

选中 **“一旦 Internet 连接可用便重新运行更新”** 选项可确保：如果 Internet 连接中断，导致 **Anti-Spam** 更新进程失败，则会在 Internet 连接恢复后立即重新启动更新进程。

一旦在所指定的时间启动计划扫描，就会通过在 **AVG 系统任务栏图标** 上方打开的弹出窗口就此情况发出通知（前提是已保留 **高级设置/外观** 对话框的默认配置）。

9.12. 电子邮件扫描程序

“电子邮件扫描程序” 对话框分为三个区域：



电子邮件扫描

在此部分中，您可以进行有关传入和/或传出电子邮件的以下基本设置：

- **“检查传入电子邮件”** (默认情况下已启用) - 选中或取消选中以启用/禁用对传送到您的电子邮件客户端的所有电子邮件进行扫描的选项
- **“检查传出电子邮件”** (默认情况下已禁用) - 选中或取消选中以启用/禁用对从您的帐户发出的所有电子邮件进行扫描的选项
- **“修改受病毒感染的邮件的主题”** (默认情况下已禁用) - 如果希望在扫描的电子邮件检测到感染时收到警告, 请选中此项并在文本字段中填写所需文本。然后此文本将被添加到每个检测到感染的邮件的“主题”字段, 以便于识别和过滤。默认值为: ***VIRUS***, 建议保留此值。

扫描属性

在此部分, 您可以指定扫描电子邮件的方式:

- **“使用启发式”** (默认情况下已启用) - 选中此框将在扫描电子邮件时使用 [启发式检测方法](#)。启用此选项时, 不仅可以按扩展名过滤电子邮件附件, 还可以检测附件的实际内容。过滤设置可在 [“邮件过滤”](#) 对话框中完成。
- **“报告可能不需要的程序和间谍软件威胁”** (默认情况下已启用) - 选中此框以激活 [Anti-Spyware](#) 引擎以及针对间谍软件和病毒的扫描。[间谍软件属于疑似恶意软件类软件: 虽然它通常代表了安全风险, 但有些程序也可能是被特意安装的。](#) 建议保持此功能的激活状态, 因为此功能会使计算机更加安全。
- **“报告更多可能不需要的程序”** (默认情况下已禁用) - 选中此框可检测更多 [间谍软件](#): 程序直接从制造商处获得时极其安全而无害, 但之后却可能被滥用以达到恶意目的。这项附加措施可以进一步提高计算机的安全性, 但也可能会阻止合法程序, 因此默认情况下已将其禁用。
- **“扫描压缩包”** (默认情况下已启用) - 选中此框可扫描电子邮件附件中的压缩包的内容。
- **“启动彻底扫描”** (默认情况下已禁用) - 在特定情况下 (例如, 怀疑计算机受到病毒或漏洞利用的感染), 您可以选中此选项以激活最全面的扫描算法, 该算法甚至会对计算机上极难被感染的区域进行扫描以确保绝对安全。不过要记住, 此方法相当耗时。

电子邮件附件报告

可在此部分中就有潜在危险或可疑的文件设置其它报告。请注意, 不会显示警告对话框, 而只是在电子邮件的末尾添加一段验证文本, 所有此类报告都会列在 [电子邮件扫描程序检测](#) 对话框中:

- **“报告受密码保护的压缩包”** 受密码保护的压缩包 (ZIP、RAR 等) 不能进行病毒扫描; 选中此框可将这类压缩包报告为具有潜在危险。
- **“报告受密码保护的文档”** 受密码保护的文档不能进行病毒扫描; 选中此框可将这类文档报告为有潜在危险。
- **“报告包含宏的文件”** 宏是一个预定义的操作序列, 旨在为用户简化某些任务的

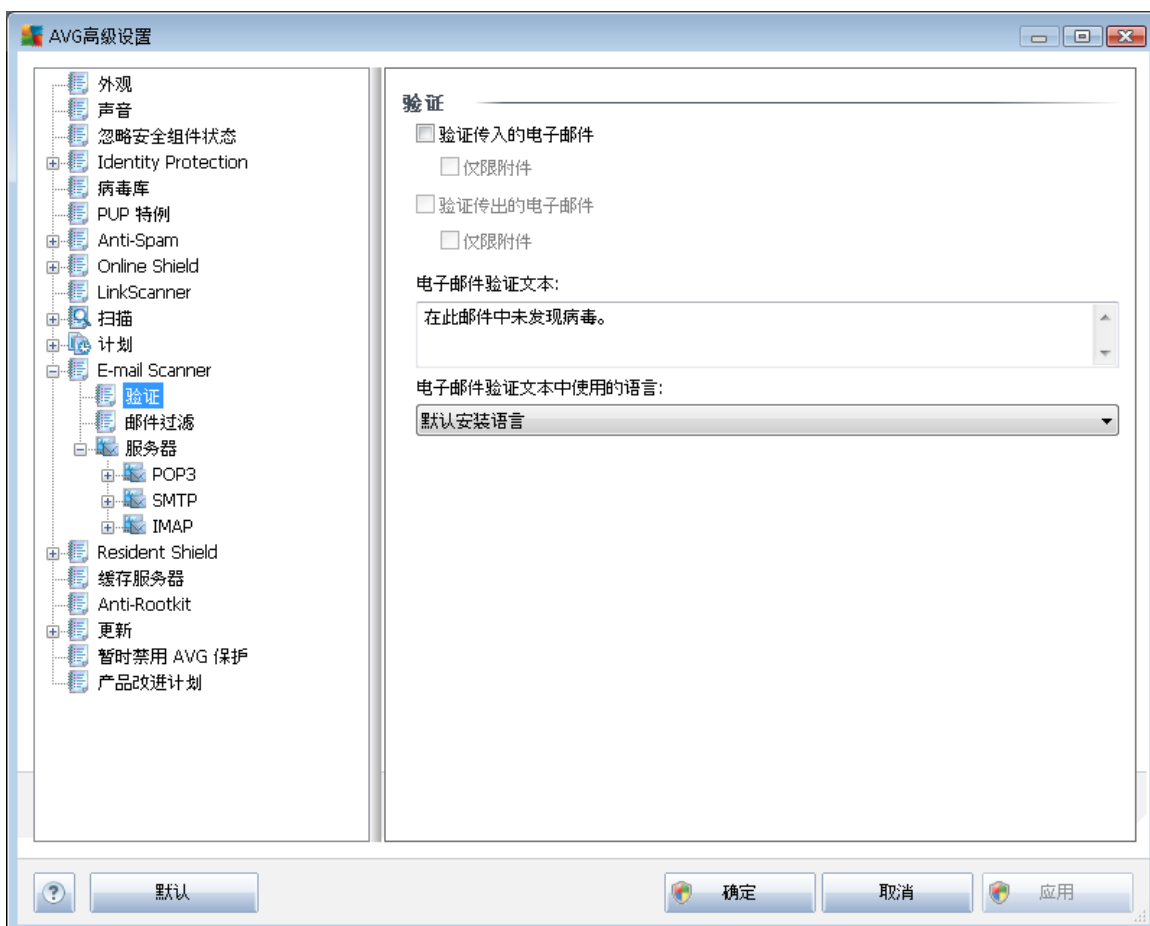


执行过程（MS Word 宏已为大家所熟悉）。因此，宏可能包含有潜在危险的指令，您可能需要选中此框，以确保将包含宏的文件报告为可疑。

- **报告隐藏的扩展名** - 隐藏的扩展名能使可疑的可执行文件看起来像没有危险的纯文本文件（如 Something.txt.exe 伪装成 Something.txt）；选中此框可将这类文件报告为有潜在危险。
- **“将报告的附件移至病毒库”** - 指定电子邮件经过扫描后发现其附件是受密码保护的存档、受密码保护的文档、含有文件的宏和/或隐藏了扩展名的文件时是否要通过电子邮件就相关情况发出通知。如果在扫描期间识别到此类邮件，请指定是否应将检测到的受感染对象移至 **病毒库**。

9.12.1. 验证

在 **“验证”** 对话框中，您可以为传入邮件和传出邮件指定验证文本和语言：



验证文本包括两个部分，即用户部分和系统部分 - 请参见下面的示例：第一行表示用户部分，其余内容是自动生成的：

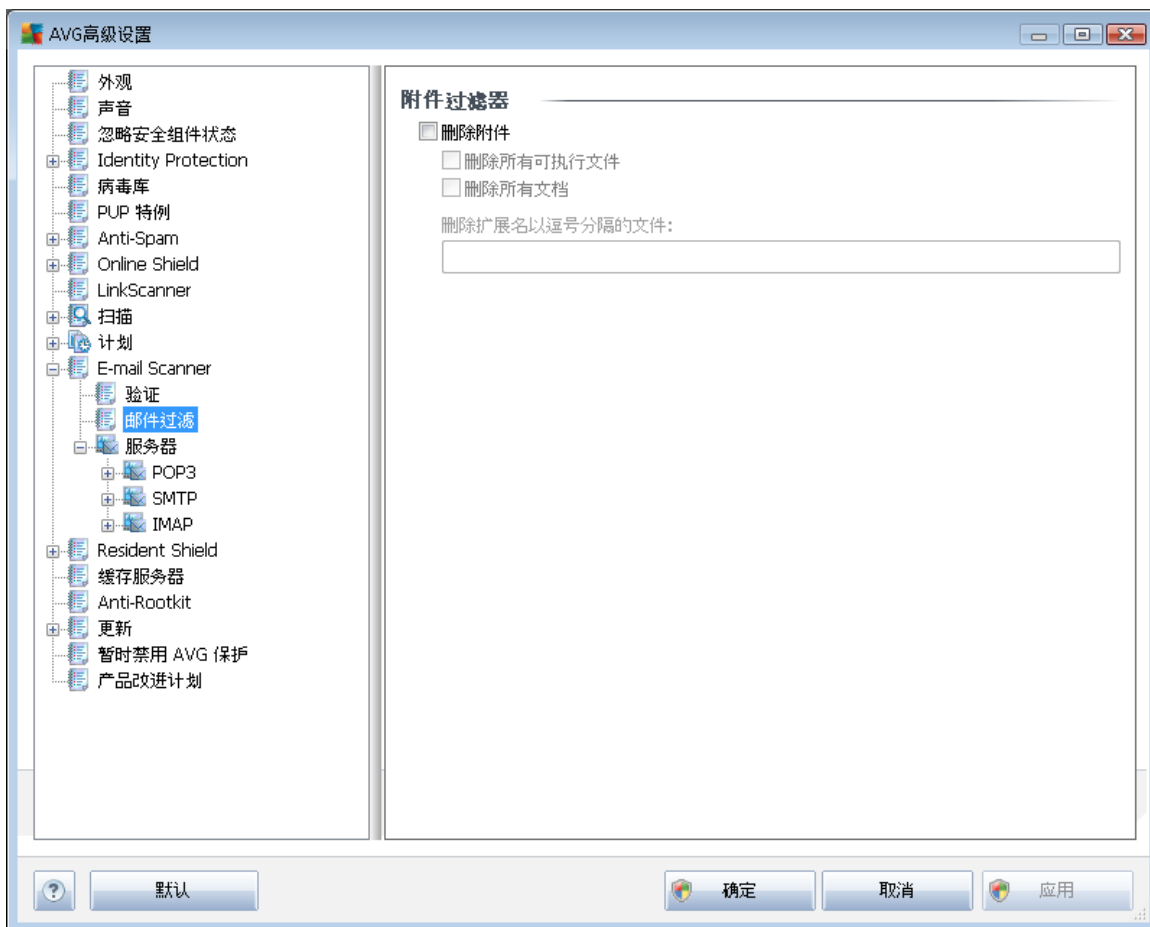
在此邮件中未发现病毒。

检查工具：AVG。

版本：x.y.zz / 病毒数据库：xx.y.z - 发布日期：2010/9/12

如果决定对传入或传出电子邮件使用验证，可以在此对话框中进一步指定验证文本用户部分的确切措辞（**电子邮件验证文本**），并选择应对自动生成的验证文本系统部分使用什么语言（**用于电子邮件验证文本的语言**）。

9.12.2. 邮件过滤

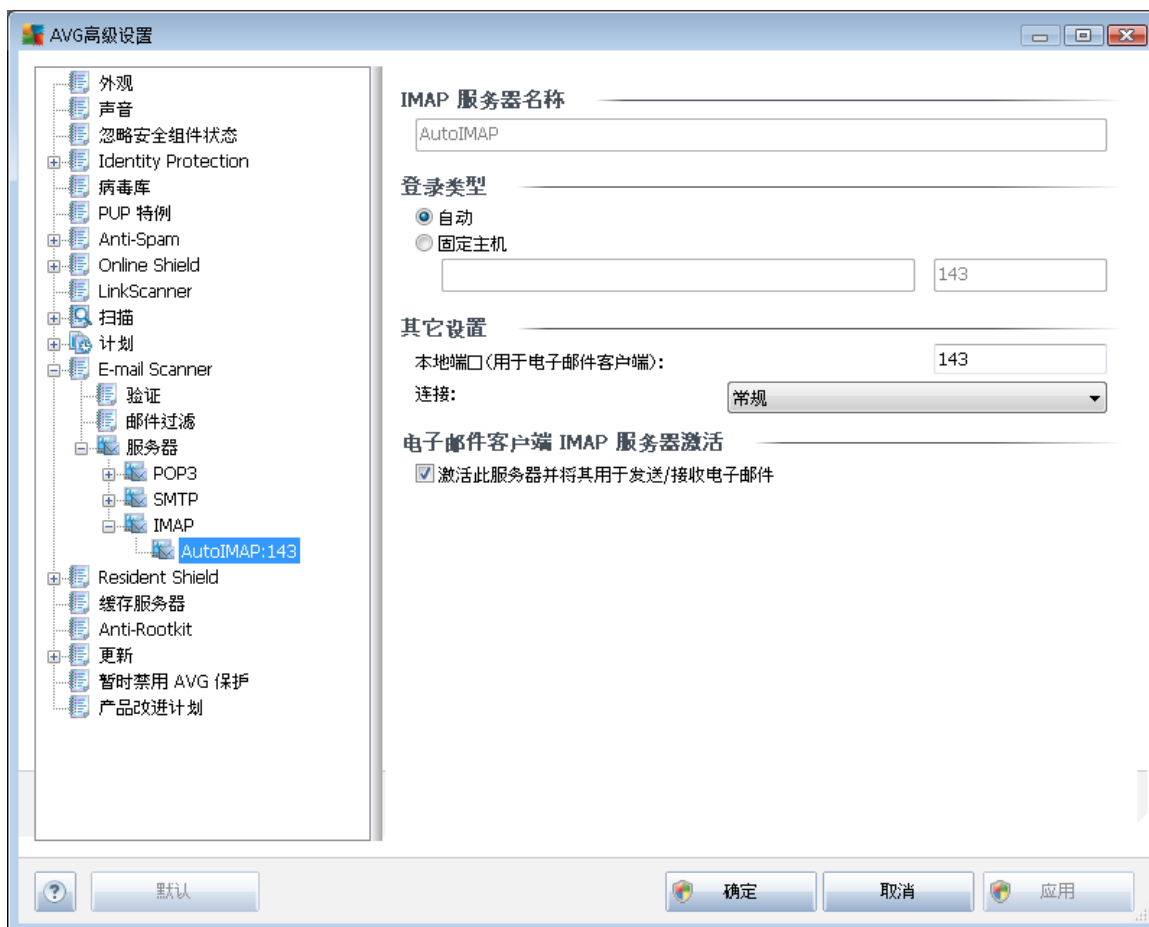


在 **‘附件过滤器’** 对话框中，您可以设置用于扫描电子邮件附件的参数。默认情况下，**‘删除附件’** 选项已禁用。如果您决定激活此选项，那么经检测而被认定为受感染或有潜在危险的所有电子邮件附件将被自动删除。如果您要定义应删除特定类型的附件，请选择相应的选项：

- **移除所有可执行文件** - 将删除所有 *.exe 文件
- **移除所有文档** - 将删除所有 *.doc、*.docx、*.xls、*.xlsx 文件
- **移除带有以下扩展名（用逗号分隔）的文件** - 将移除具有所定义扩展名的所有文件

9.12.3. 服务器

在‘**服务器**’区域中，您可以编辑 [E-mail Scanner](#) 组件服务器的参数，或使用‘**添加新服务器**’按钮设置新服务器。



在此对话框（通过**服务器/POP3**打开）中，您可以设置使用 POP3 协议接收邮件的新 [电子邮件扫描程序](#) 服务器：

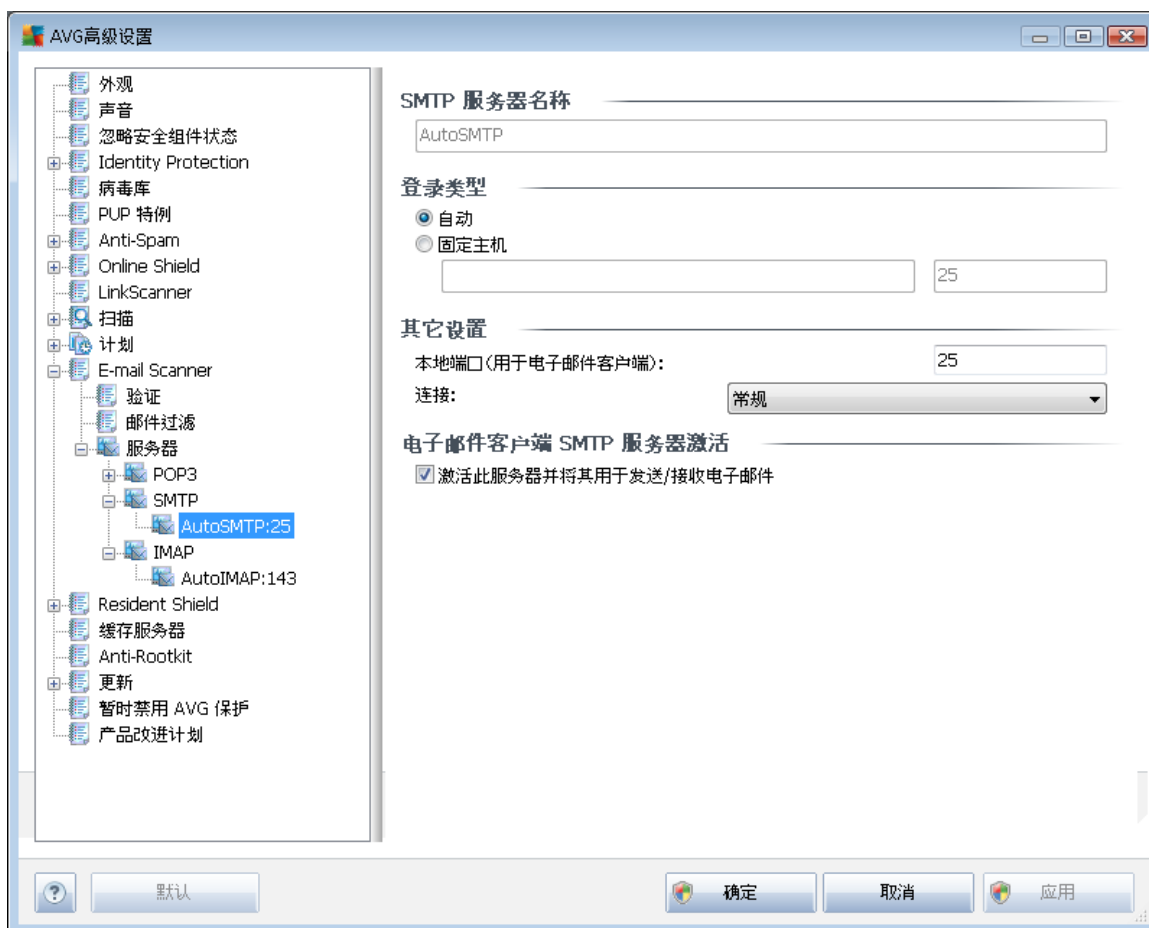
- **POP3 服务器名称** - 您可以在此字段中指定新添加的服务器的名称（若要添加 POP3 服务器，请在左侧导航菜单的 POP3 菜单项上单击鼠标右键）。对于自动创建的‘AutoPOP3 服务器’，此字段已禁用。
- **登录类型** - 定义用于接收邮件的邮件服务器的确定方法：
 - **自动** - 将自动根据您的电子邮件客户端设置进行登录。
 - **固定主机** - 这种情况下，程序将始终使用此处指定的服务器。请指定邮件服务器的地址或名称。登录名保持不变。可以使用域名（例如，*pop.acme.com*）以及 IP 地址（例如，*123.45.67.89*）来表示名称。如果此邮件服务器使用非标准端口，则您可以在服务器名称后面指定此端口，二者之间用冒号

隔开（例如，`pop.acme.com:8200`）。POP3 通信的标准端口为 110。

- **其它设置** - 用于指定更为详细的参数：

- **本地端口** - 指定应在哪个端口允许来自邮件应用程序的通信。随后必须在您的邮件应用程序中指定此端口作为 POP3 通信端口。
- **连接** - 在此下拉菜单中，您可以指定要使用何种连接（*常规/SSL/SSL 默认*）。如果选择 SSL 连接，则数据以加密方式发送，因而没有被第三方跟踪或监视的风险。此功能也是只有在目标邮件服务器支持它时才可用。

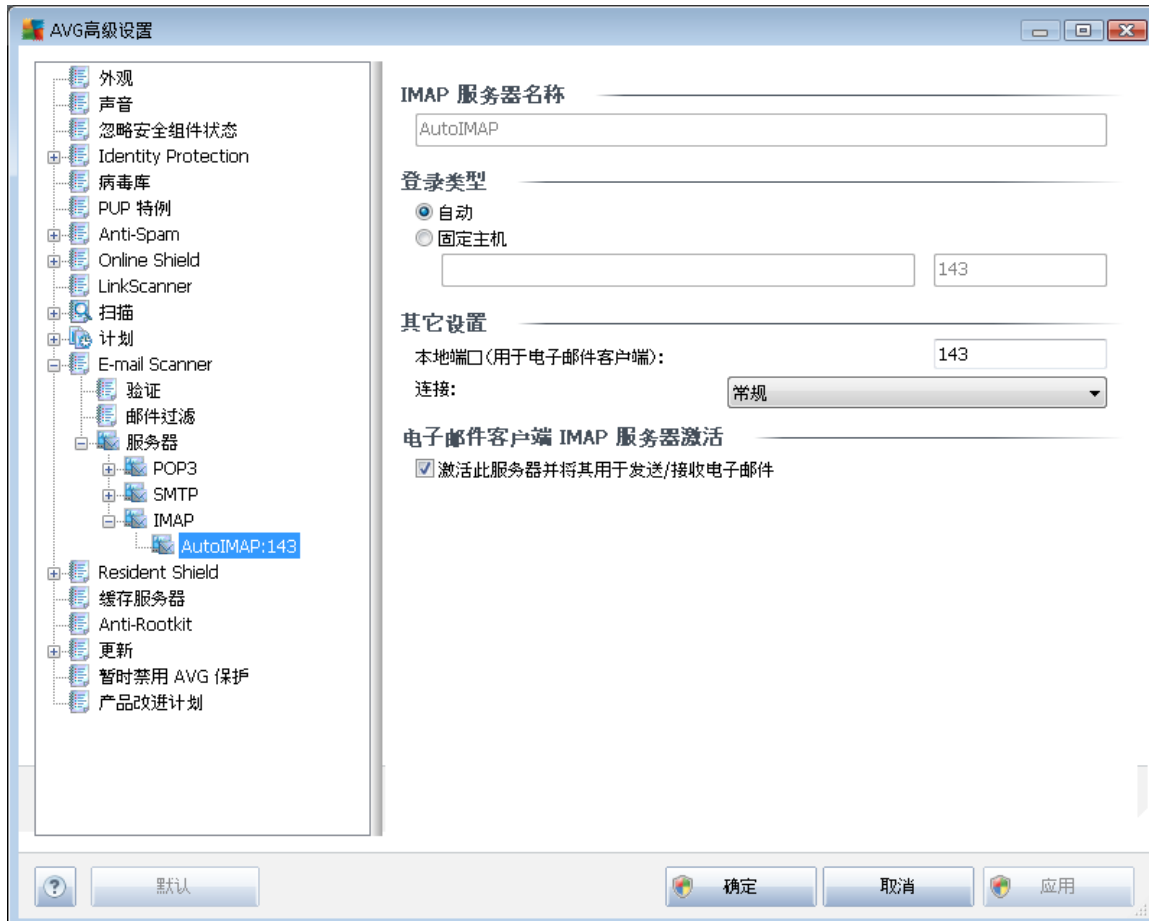
- **电子邮件客户端 POP3 服务器激活** - 选中/取消选中此项可激活或停用指定的 POP3 服务器



在此对话框（通过 **服务器/SMTP** 打开）中，您可以设置使用 SMTP 协议发送邮件的新 **电子邮件扫描程序** 服务器：

- **SMTP 服务器名称** - 您可以在此字段中指定新添加的服务器的名称（若要添加 SMTP 服务器，请在左侧导航菜单的 **SMTP** 菜单项上单击鼠标右键）。对于自动创建的 'AutoSMTP' 服务器，此字段已禁用。

- **登录类型** - 定义应采用何种方法来决定用于发送邮件的邮件服务器：
 - **自动** - 将自动根据您的电子邮件客户端设置进行登录
 - **固定主机** - 这种情况下，程序将始终使用此处指定的服务器。请指定邮件服务器的地址或名称。可以使用域名（例如，smtp.acme.com）以及 IP 地址（例如，123.45.67.89）来表示名称。如果此邮件服务器使用非标准端口，则您可以在服务器名称后面键入此端口，二者之间用冒号隔开（例如，smtp.acme.com:8200）。SMTP 通信的标准端口为 25。
- **其它设置** - 用于指定更为详细的参数：
 - **本地端口** - 指定应在哪个端口允许来自邮件应用程序的通信。然后必须在对应的邮件应用程序中指定此端口作为用于 SMTP 通信的端口。
 - **连接** - 在此下拉菜单中，可以指定要使用的连接类型（常规/SSL/SSL 默认）。如果选择 SSL 连接，则数据以加密方式发送，因而没有被第三方跟踪或监视的风险。只有在目标邮件服务器支持此功能时，此功能才可用。
- **电子邮件客户端 SMTP 服务器激活** - 选中/取消选中此框可激活/停用上面指定的 SMTP 服务器

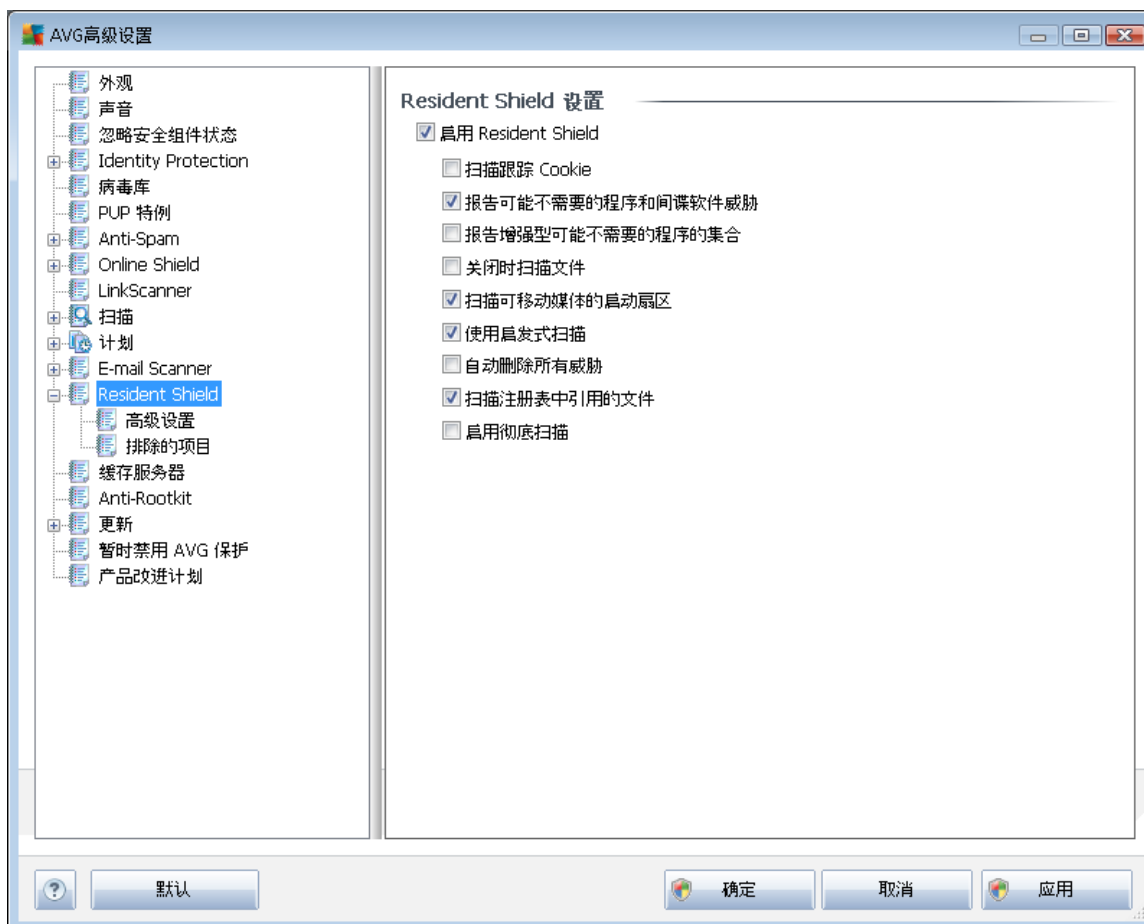


在此对话框（通过 **服务器/IMAP** 打开）中，您可以设置使用 IMAP 协议发送邮件的新 [电子邮件扫描程序](#) 服务器：

- **“IMAP 服务器名称”** - 您可以在此字段中指定新添加的服务器的名称（若要添加 IMAP 服务器，请在左侧导航菜单的 IMAP 菜单项上单击鼠标右键）。对于自动创建的 AutoIMAP 服务器，此字段已禁用。
- **登录类型** - 定义应采用何种方法来决定用于发送邮件的邮件服务器：
 - o **自动** - 将自动根据您的电子邮件客户端设置进行登录
 - o **固定主机** - 这种情况下，程序将始终使用此处指定的服务器。请指定邮件服务器的地址或名称。可以使用域名（例如，*smtp.acme.com*）以及 IP 地址（例如，*123.45.67.89*）来表示名称。如果此邮件服务器使用非标准端口，则您可以在服务器名称后面键入此端口，二者之间用冒号隔开（例如，*imap.acme.com:8200*）。用于 IMAP 通信的标准端口为 143。
- **其它设置** - 用于指定更为详细的参数：
 - o **本地端口** - 指定应在哪个端口允许来自邮件应用程序的通信。然后必须在对应的邮件应用程序中指定此端口作为用于 IMAP 通信的端口。
 - o **连接** - 在此下拉菜单中，可以指定要使用的连接类型（*常规/SSL/SSL 默认*）。如果选择 SSL 连接，则数据以加密方式发送，因而没有被第三方跟踪或监视的风险。只有在目标邮件服务器支持此功能时，此功能才可用。
- **电子邮件客户端 IMAP 服务器激活** - 选中/取消选中此框可激活/停用上面指定的 IMAP 服务器

9.13. Resident Shield

Resident Shield 组件用于实时保护文件和文件夹免遭病毒、间谍软件及其它恶意软件侵害。



在 **“Resident Shield 设置”** 对话框中，您可以通过选中/取消选中 **“启用 Resident Shield”** 项（默认情况下此选项已启用）来完全激活或停用 **Resident Shield** 保护。此外，您还可以选择应激活哪些 **Resident Shield** 功能：

- **“扫描跟踪 Cookie”**（默认情况下已禁用） - 此参数用于指定在扫描期间应对 Cookie 进行检测。（HTTP Cookie 用于验证、跟踪和维护有关用户的特定信息，例如网站首选项或电子购物车中的内容）
- **“报告可能不需要的程序和间谍软件威胁”**（默认情况下已启用）：选中此框可激活 **Anti-Spyware** 引擎，进行间谍软件和病毒扫描。间谍软件属于疑似恶意软件类软件：虽然它通常代表了安全风险，但有些程序也可能是被特意安装的。建议保持此功能的激活状态，因为此功能会使计算机更加安全。
- **“报告更多可能不需要的程序”**（默认情况下已禁用） - 选中此框可检测更多 **间谍软件**：程序直接从制造商处获得时极其安全而无害，但之后却可能被滥用以达到恶意目的。这项附加措施可以进一步提高计算机的安全性，但也可能会阻止合法



程序，因此默认情况下已将其禁用。

- **“关闭时扫描文件”** (默认情况下已禁用) - 关闭时执行的扫描可确保 AVG 在活动的对象（如应用程序、文档等）被打开和关闭时对它们进行扫描；此功能可帮助您保护您的计算机免遭某些类型的复杂病毒侵害
- **“扫描可移动介质的启动扇区”** (默认情况下已启用)
- **“使用启发式扫描”** (默认情况下已启用) 将使用 [启发式分析](#) 方法进行检测（在虚拟的计算机环境中对已扫描对象的指令进行动态模拟）
- **自动删除所有威胁** (默认情况下已禁用) - 对于检测到的任何受感染文件，如果有修复方案，则会自动对其进行修复，所有无法修复的受感染文件都会被删除。
- **“扫描注册表中引用的文件”** (默认情况下已启用) - 此参数定义 AVG 将扫描添加到 Startup 注册表项的所有可执行文件，以避免在计算机下次启动时执行已知的感染。
- **“启动彻底扫描”** (默认情况下已禁用) - 特定情况下（在极其紧急的状态下），您可以选中此选项以激活最彻底的算法，该算法将深度检查所有可能的威胁对象。不过要记住，此方法相当耗时。

9.13.1. 高级设置

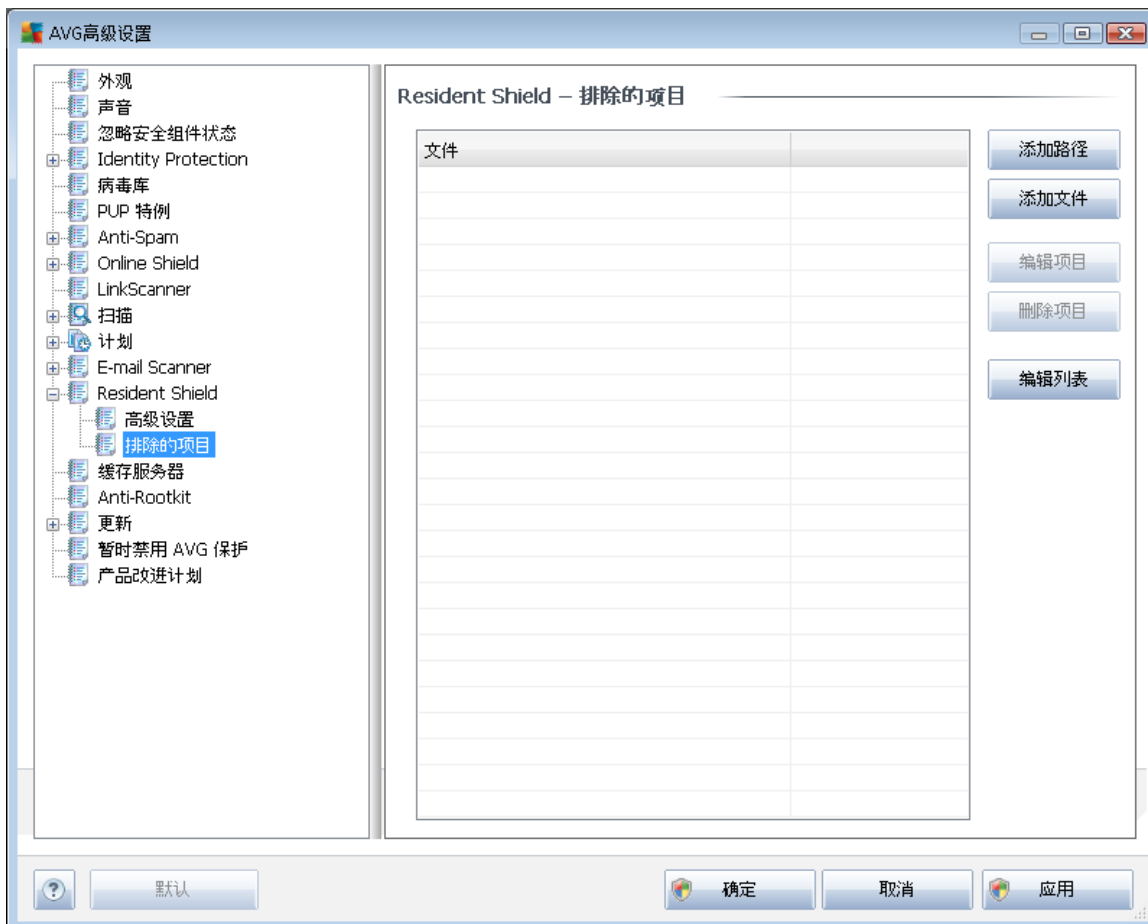
在 **‘Resident Shield 扫描的文件’** 对话框中，可以配置所要扫描的文件（通过特定扩展名）：



决定是要扫描所有文件还是仅扫描可感染文件 – 如果选择后者，则可以进一步指定一个扩展名列表以定义应排除在扫描范围之外的文件，还可以指定另一个文件扩展名列表以定义在所有情况下都必须扫描的文件。

下方名为 **‘Resident Shield 将扫描’** 的部分对当前设置进行了进一步汇总，其中显示 [Resident Shield](#) 实际扫描内容的详细概览。

9.13.2. 排除的项目



可通过 **‘Resident Shield - 排除项目’** 对话框定义应排除在 [Resident Shield](#) 扫描范围之外的文件和/或文件夹。

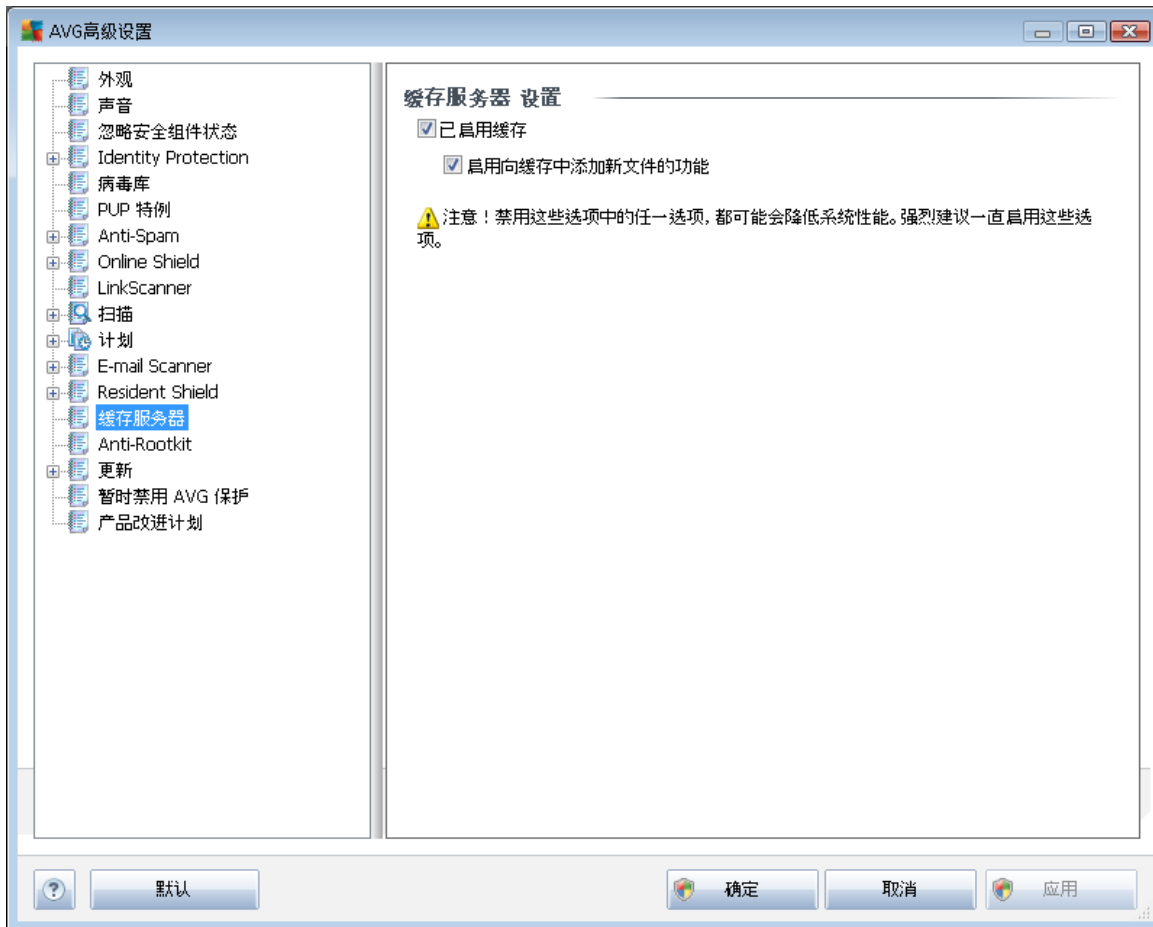
我们强烈建议，若非必要，不要排除任何项目！

此对话框提供了以下控制按钮：

- **‘添加路径’** – 通过在本地磁盘导航树中逐一选择目录来指定要排除在扫描范围之外的目录
- **‘添加文件’** – 通过在本地磁盘导航树中逐一选择文件来指定要排除在扫描范围之外的文件
- **‘编辑项目’** – 用于编辑选定文件或文件夹的指定路径
- **‘删除项目’** – 用于从列表中删除选定项目的路径

9.14. 缓存服务器

‘缓存服务器’是一种流程，旨在提高任何扫描（**按需扫描**、**计划全盘扫描**、**Resident Shield 扫描**）的速度。该流程用于收集并保存值得信赖的文件（有数字签名的系统文件等）的信息：然后就会将这些文件视为安全文件，会在扫描过程中将其略过。



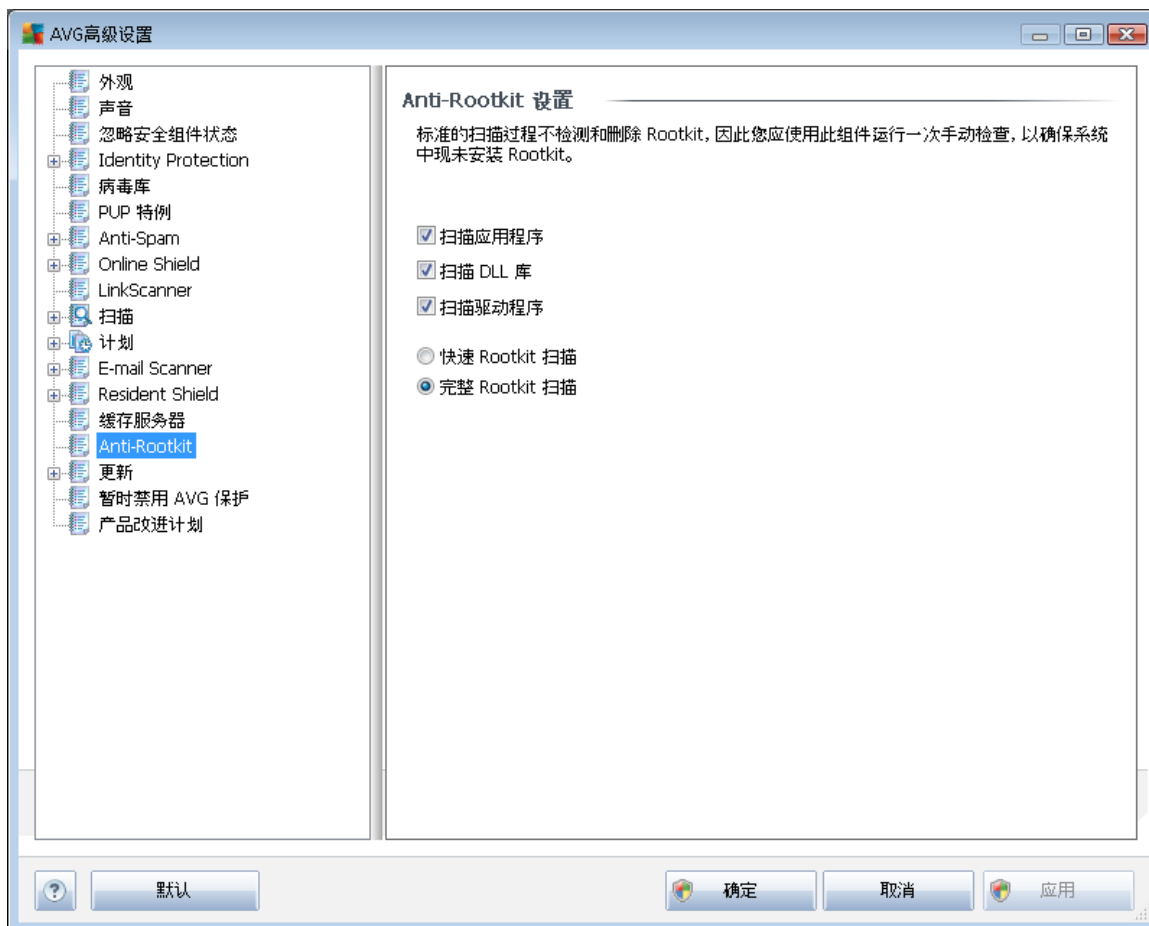
设置对话框中有两个选项：

- **已启用缓存**（默认情况下已启用）- 取消选中该框可禁用**缓存服务器**，清空缓存。请注意，扫描速度可能会减慢，计算机的总体性能会降低，因为会先对每个正在使用的文件进行病毒和间谍软件扫描。
- **启用向缓存中添加新文件的功能**（默认情况下已启用）- 取消选中该框可停止向缓存中添加更多文件。会保留并使用所有已存入缓存的文件，直到彻底禁用缓存功能为止，或直到下次更新病毒数据库为止。



9.15. Anti-Rootkit

在此对话框中，可以编辑 [Anti-Rootkit](#) 组件的配置：



可在此对话框中对 [Anti-Rootkit](#) 组件的所有功能执行的编辑操作，也都可以直接在 [Anti-Rootkit 组件的界面](#) 中执行。

选中相应的复选框可指定应扫描的对象：

- **扫描应用程序**
- **扫描 DLL 库**
- **扫描驱动程序**

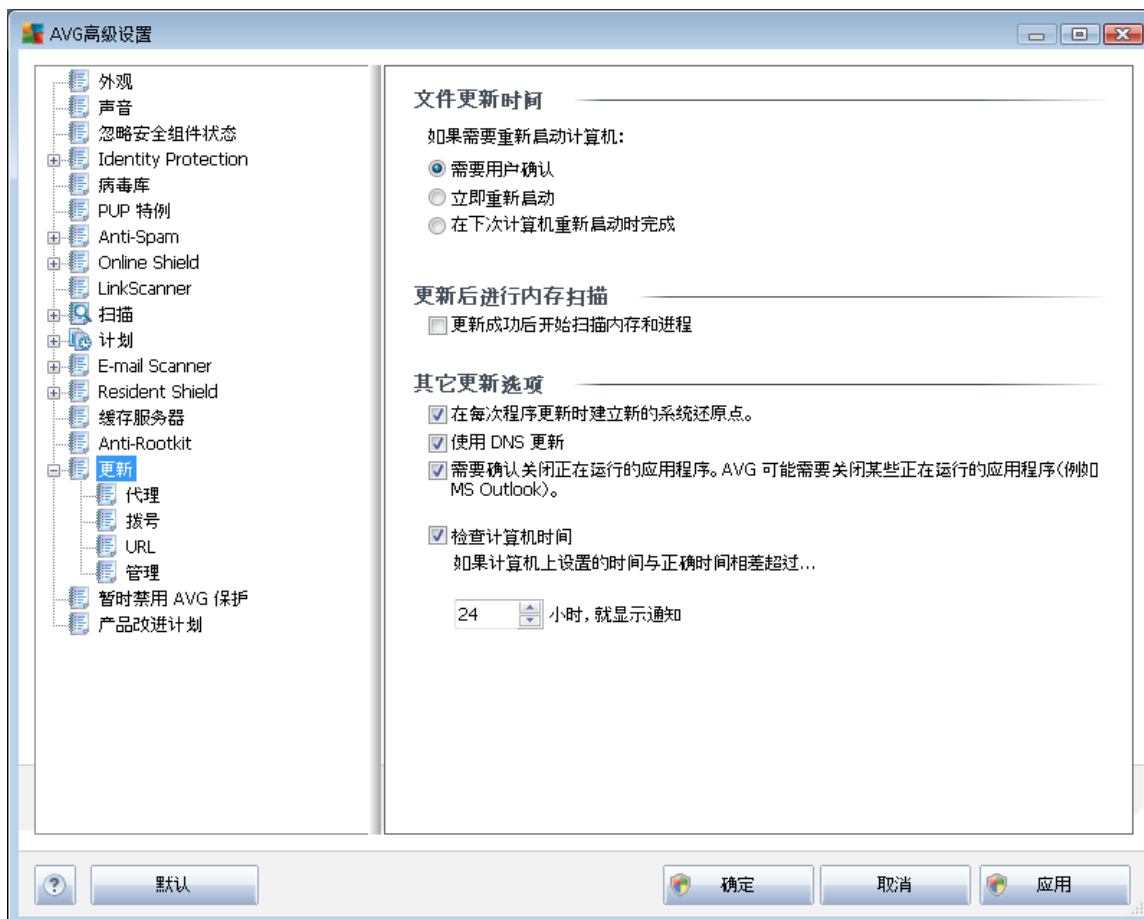
此外，还可以选择 Rootkit 扫描模式：

- **快速 Rootkit 扫描** - 用于扫描所有正在运行的进程、已加载的驱动程序和系统文件夹（通常是 c:\Windows）
- **完整 rootkit 扫描** - 用于扫描所有正在运行的进程、已加载的驱动程序、系统文件



夹（通常是 c:\Windows），以及所有本地磁盘（包括闪存磁盘，但不包括软盘/CD 驱动器）

9.16. 更新



‘更新’导航选项用于打开一个新对话框，从中可指定与 [AVG 更新](#) 有关的常规参数：

文件更新时间

在本节中，可从三个选项中选择用在必须重新启动 PC 才能执行更新过程时的选项。可计划在下次重新启动 PC 时完成更新，也可立即重新启动：

- **需要用户确认**（默认设置）- 会询问用户是否同意重新启动 PC，而重新启动是完成 [更新过程](#)
- **立即重新启动** - [更新过程](#) 结束后计算机将立即自动重新启动，不需要用户同意
- **下次重新启动计算机时完成更新** - [更新过程](#) 会推迟到下次重新启动计算机时才完成。请记住，此选项仅当确信计算机定期重新启动时才建议使用，至少每天重新启动一次！



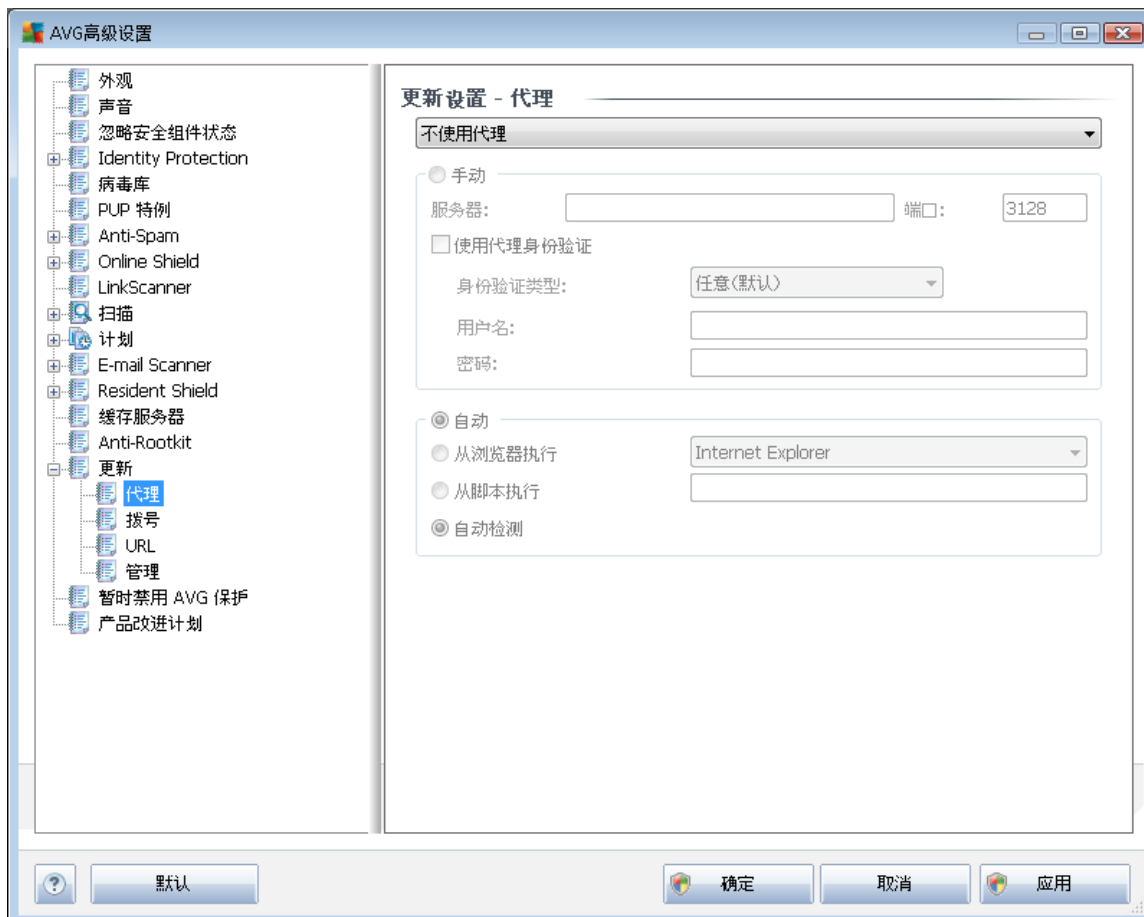
更新后进行内存扫描

选中此复选框可指定，您希望在每次成功完成更新后启动新的内存扫描。最新下载的更新可能包含新的病毒定义，这些定义会被立即应用在扫描中。

其它更新选项

- **在每次程序更新时建立新的系统还原点** - 在每次启动 AVG 程序更新前，都会创建一个系统还原点。万一更新过程失败并且您的操作系统崩溃，那么您始终都可以利用此还原点将您的操作系统还原成其原始配置。可通过开始/所有程序/附件/系统工具/系统还原访问此选项，但建议仅限经验丰富的用户进行任何更改！如果您要利用此功能，请将此复选框保持选中状态。
- **使用 DNS 更新**（默认情况下已启用）- 选中此选项后，一启动更新，**AVG Internet Security 2011** 就会在 DNS 服务器中查找有关最新病毒数据库版本和最新程序版本的信息。然后就会仅下载并应用最小的不可或缺的所需更新文件。这样会最大程度地减小下载的数据总量，更新过程也会加快。
- **‘需要确认才能关闭正在运行的应用程序’**（默认情况下已启用）有助于您确保，在需要关闭当前正在运行的应用程序才能完成更新过程的情况下，未经您同意不会关闭任何此类程序；
- **‘检查计算机时间’** - 选中此选项可表示，在计算机时间与正确时间之差大于指定的小时数时，您希望显示通知。

9.16.1. 代理



代理服务器是一台独立的服务器或运行在 PC 上的一项服务，用于保证与 Internet 的连接更加安全。根据指定的网络规则，您可以直接访问 Internet 或通过代理服务器进行访问；也可以允许同时使用这两种方法。接着，在 **“更新设置 - 代理”** 对话框的第一项内容中，您必须从组合框菜单中的以下选项中进行选择：

- **“使用代理”**
- **“不使用代理服务器”** - 默认设置
- **“先尝试使用代理连接，若代理连接失败则直接连接”**

如果您选择了使用代理服务器的任何选项，则您还必须进一步指定一些数据。服务器设置可手动配置，也可自动配置。

手动配置

如果您选择手动配置（选中 **“手动”** 选项以激活对话框的相应区域），则您必须指定以下项：



- **服务器** - 指定服务器的 IP 地址或服务器的名称
- **端口** - 指定用于进行 Internet 访问的端口号（默认情况下此端口号设置为 3128，但可以设置为其它值 - 如果您不知道该如何设置，请联系您的网络管理员）

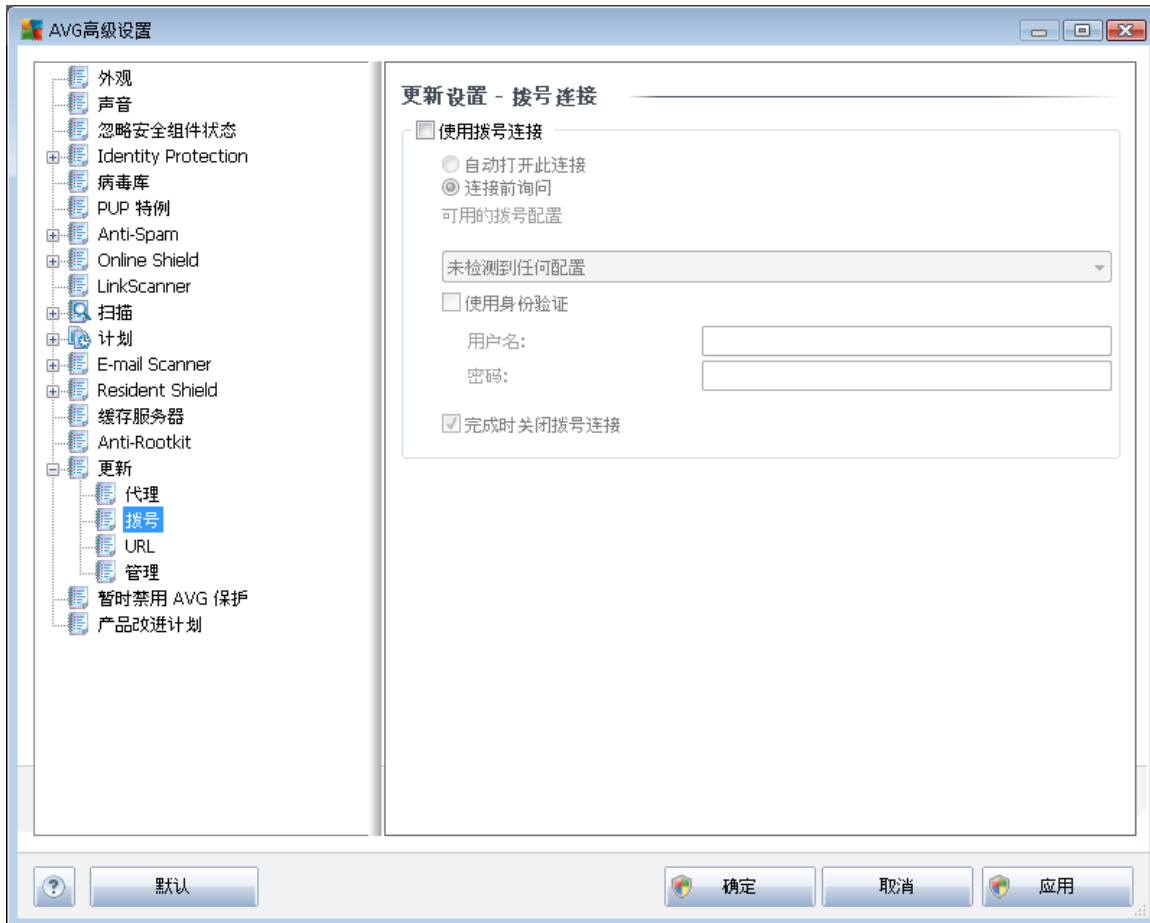
代理服务器也可以针对每个用户配置特定的规则。如果您的代理服务器是这样设置的，请选中 **“使用代理身份验证”** 选项以验证您的用户名和密码是否有效，即能否通过代理服务器连接到 Internet。

自动配置

如果您选择自动配置（选中 **“自动”** 选项以激活对话框的相应区域），请选择应从何处获得代理配置：

- **“从浏览器”** - 将从您的默认 Internet 浏览器中读取配置
- **从脚本** - 将从下载的具有返回代理地址功能的脚本中读取配置
- **自动检测** - 将直接从代理服务器中自动检测配置

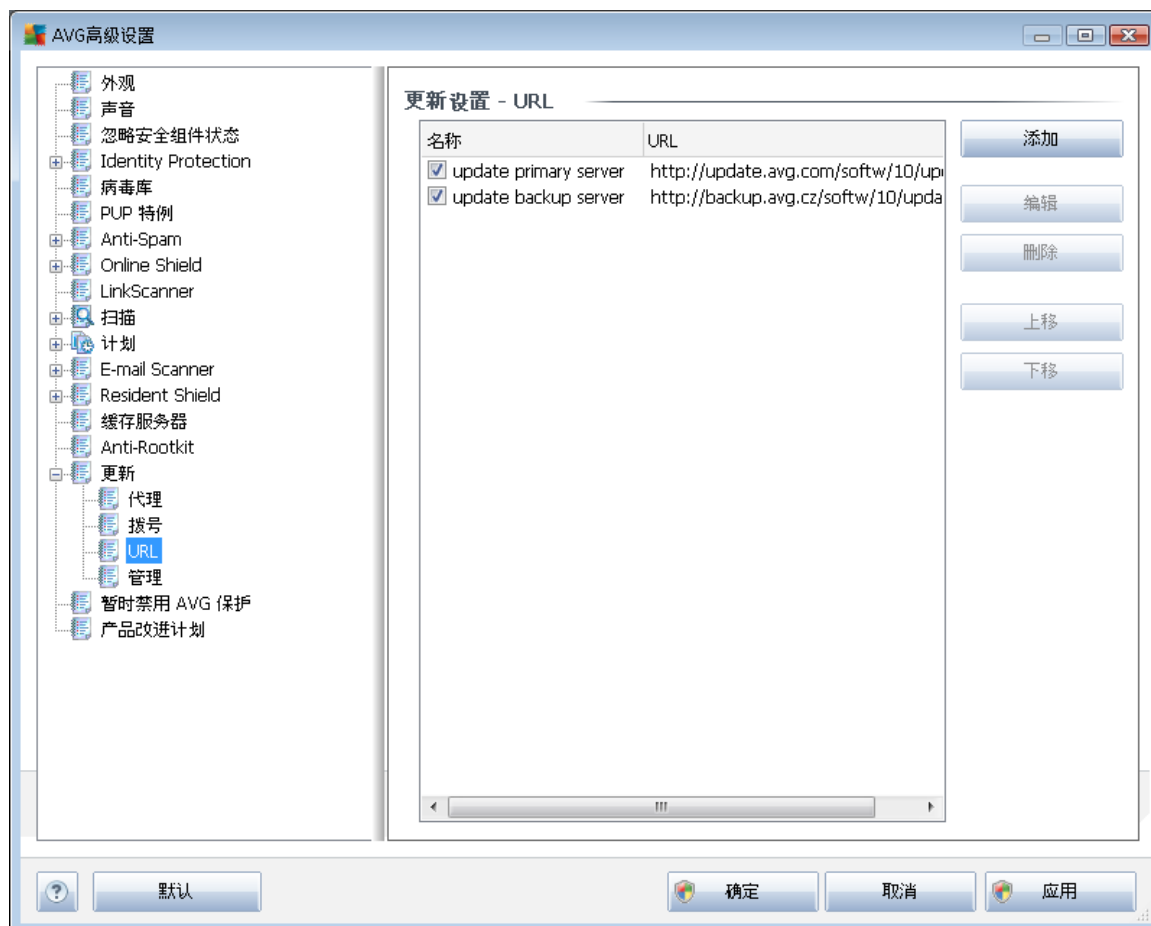
9.16.2. 拨号



在 **“更新设置 - 拨号连接”** 对话框中定义（可选）的所有参数都涉及拨号连接至 Internet。该对话框中的字段均未激活，在您选中 **“使用拨号连接”** 选项后，才会激活这些字段。

请指定您是希望自动连接到 Internet（**“自动打开此连接”**）还是希望每次都手动确认连接（**“连接前询问”**）。对于自动连接，还应选择更新完成后是否要关闭连接（**“完成时关闭拨号连接”**）。

9.16.3. URL

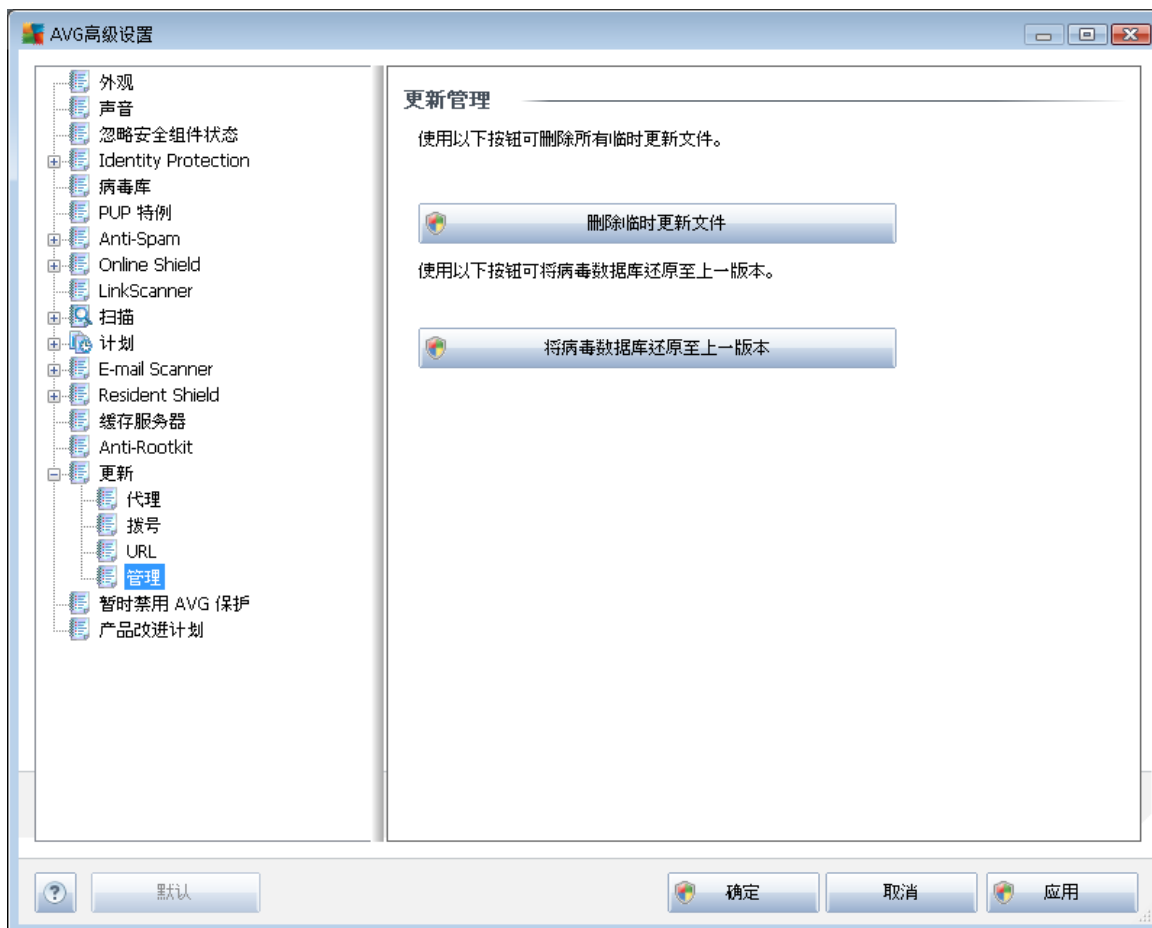


“URL”对话框提供了可从中下载更新文件的 Internet 地址列表。可以使用以下控制按钮修改此列表及其中的各项：

- **“添加”**—打开一个对话框，在此对话框中您可以指定要添加到此列表中的新 URL
- **“编辑”**—打开一个对话框，在此对话框中您可以编辑选定的 URL 参数
- **“删除”**—从此列表中删除选定的 URL
- **“上移”**—在列表中将选定的 URL 上移一个位置
- **“下移”**—在列表中将选定的 URL 下移一个位置

9.16.4. 管理

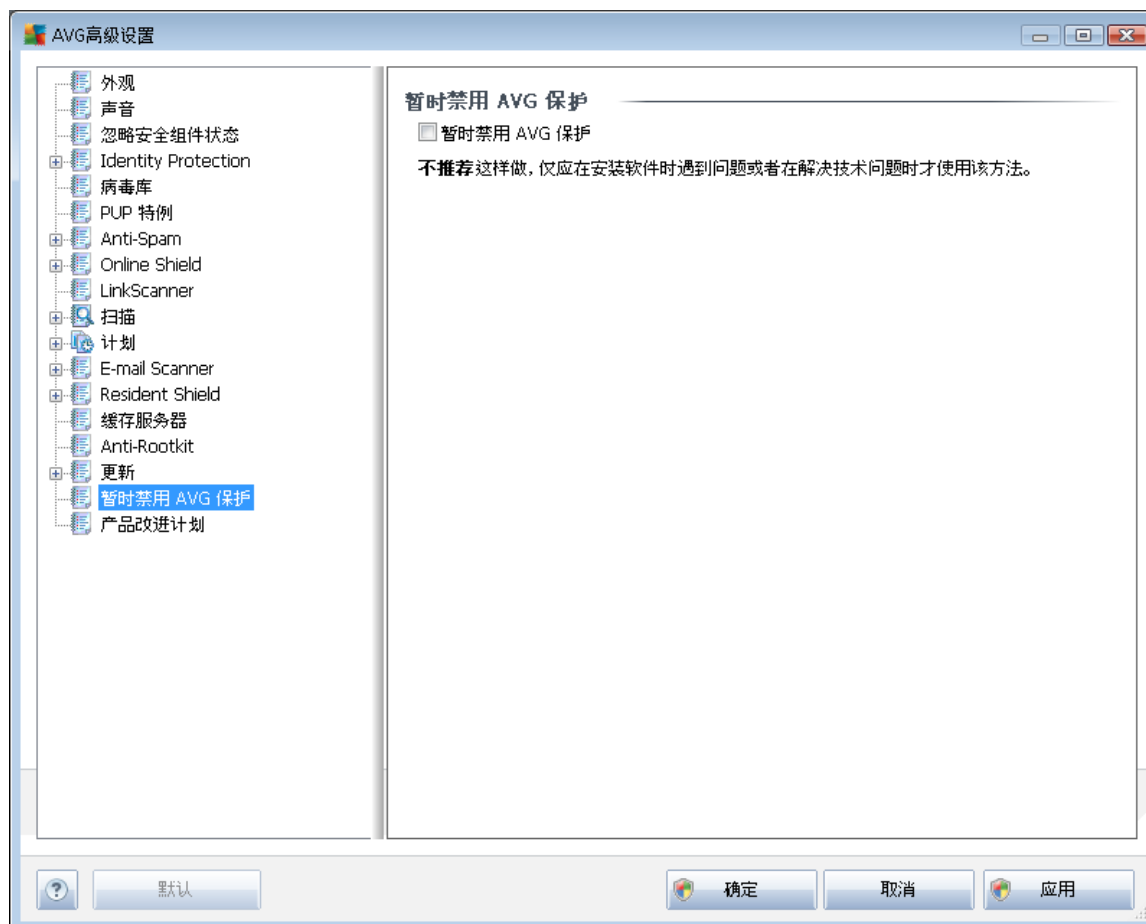
“**管理**”对话框提供了两个选项，这两个选项分别可通过以下两个按钮进行访问：



- **“删除临时的更新文件”**–按此按钮可从硬盘上删除所有多余的更新文件（默认情况下，这些文件的存储期限为 30 天）
- **“将病毒数据库恢复为上一版本”**–按此按钮可从硬盘上删除最新的病毒库版本，并恢复为以前保存的版本（下次更新将包括新的病毒数据库版本）



9.17. 暂时禁用 AVG 保护



在 **‘暂时禁用 AVG 保护’** 对话框中，您可以选择一次性关闭由 **AVG Internet Security 2011** 实施的整个保护。

请记住，只有在绝对必要的情况下才使用此选项！

在大多数情况下，**不必**在安装新软件或驱动程序之前禁用 AVG，即使安装程序或软件安装向导建议先关闭正在运行的程序和应用程序以确保在安装过程中不发生意外中断也如此。如果确实在安装过程中遇到问题，应尽量先停用 **Resident Shield** 组件。如果必须暂时禁用 AVG，您应该在完成后尽快将其重新启用。如果在防病毒软件被禁用的过程中连接到 Internet 或网络，计算机很容易受到攻击。

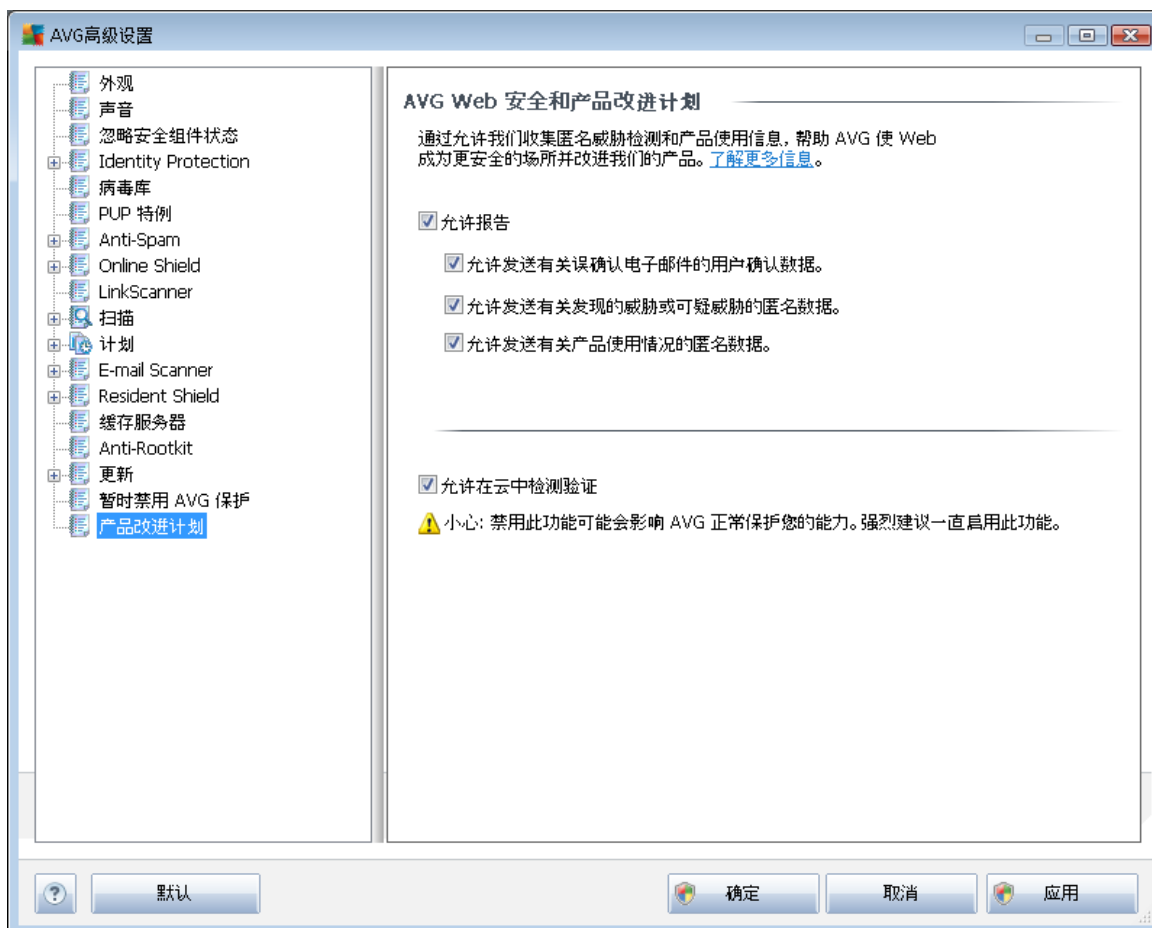
9.18. 产品改进计划

‘AVG Web 安全和产品改进计划’ 邀请您参加 AVG 产品改进，并帮助我们提升 Internet 总体安全级别。选中 **‘允许报告’** 选项可允许向 AVG 报告检测到的威胁。这有助于我们从世界各地的所有参与者处收集有关最新威胁的最新信息，然后我们就会以更严密的保护回报大家。

报告会自动进行，因此不会引起不便，也不会向报告中添加个人数据。 报告检测到



的威胁是可选操作，但我们也确实希望您启用此功能，因为这有助于我们为所有 AVG 用户改善保护功能。



如今，威胁已远远超过普通病毒。恶意代码和危险网站的编写者创新能力很强，新型威胁时常出现，其中绝大多数都是在 Internet 上肆虐。以下是一些最常见的威胁：

- **病毒**是一种自我复制和传播的恶意代码，通常直到造成破坏时才会被发觉。有些病毒是严重的威胁，它们在传播途中会删除或有意更改文件；而有些病毒则会执行一些看似无害的操作，例如播放一段音乐。但所有病毒都有危险性，因为它们都有基本的繁殖能力。即使是一个简单的病毒也能很快耗尽所有计算机内存，从而造成崩溃。
- **蠕虫**是病毒的一个子类别，与普通病毒不同的是，它不需要依附于一个载体对象；它将自身作为一个独立的对象发送到其它计算机（通常通过电子邮件发送），因此往往会造成电子邮件服务器和网络系统过载。
- **间谍软件**通常被定义为一类包含程序（通常是特洛伊木马），旨在窃取个人信息、密码、信用卡号码或潜入计算机以使攻击者得以对其进行远程控制的恶意软件（恶意软件 = 任何有恶意的软件，包括病毒）；当然，所有这些行径都是在计算机所有者不知情或未同意的情况下实施的。



- **可能不需要的程序**是一类间谍软件，它们可能但不一定不会对您的计算机产生危险。广告软件就是 PUP 的一个具体例子，这种软件用于分发广告，分发途径通常是显示弹出广告；虽然惹人讨厌，但其实是无害的。
- **跟踪 Cookie** 视为一类间谍软件，因为这些小型文件（存储在 Web 浏览器中并在您再次访问其父网站时会自动发送至该网站）可能会包含诸如您的浏览历史记录等数据以及其它一些类似信息。
- **漏洞利用**是一种恶意代码，它利用操作系统、Internet 浏览器或其它基本程序中的缺陷或漏洞进行攻击。
- **网络钓鱼**试图通过假冒可靠的知名组织骗取敏感的个人数据。潜在受害者往往被大量的电子邮件诱入圈套，这些电子邮件要求他们执行银行帐户详细信息更新之类的操作。为执行这类操作，潜在受害者会受邀单击所提供的链接，然后就会被诱骗到假银行网站。
- **愚弄邮件**是一种批量发送的电子邮件，其中含有危险信息、恐吓信息或是纯粹的骚扰和无用信息。以上所列的许多威胁都用愚弄邮件来传播。
- **恶意网站**会故意在访客的计算机中安装恶意软件，已被攻陷的站点的行径完全一样，只是这些站点是已被传播威胁的访客侵入的合法网站。

为保护您免遭上述所有不同类型威胁的侵扰，AVG 包含了以下这些专用组件：

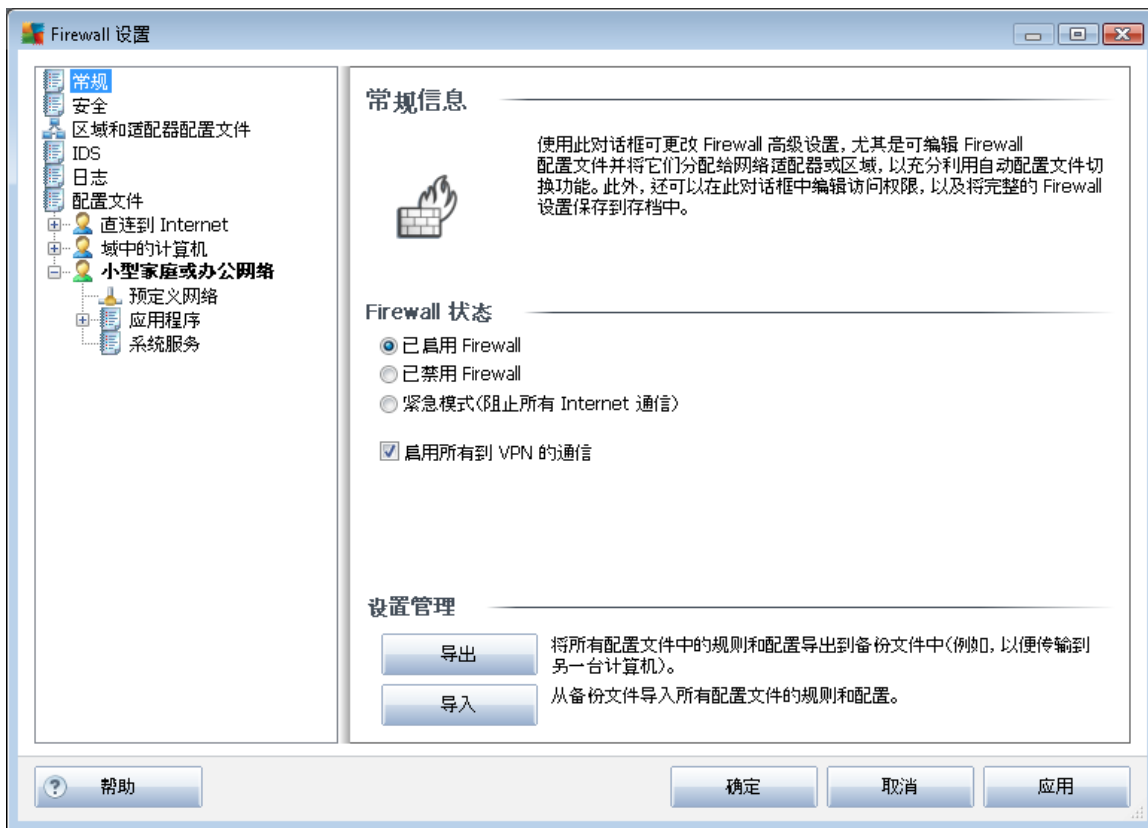
- [**Anti-Virus**](#)，用来保护您的计算机免遭病毒入侵；
- [**Anti-Spyware**](#)，用来为您的计算机防范间谍软件；
- [**Online Shield**](#)，用来为您在 Internet 上冲浪时防范病毒和间谍软件；
- [**LinkScanner**](#)，用来保护您免遭本章提到的其它在线威胁的侵扰。

10. Firewall 设置

Firewall 配置在一个新窗口中打开，可以在此窗口中的多个对话框中设置该组件非常高级的参数。不过，高级配置只能由专家及经验丰富的用户进行编辑。

10.1. 常规

‘常规信息’对话框划分为两个部分：



Firewall 状态

在 ‘Firewall 状态’ 部分，您可以在需要时切换 **Firewall** 状态：

- ‘**已启用 Firewall**’ 选中此选项可允许与所选 **Firewall 配置文件**
- ‘**已禁用 Firewall**’ 此选项用于彻底禁用 **Firewall**，会允许所有网络通信，但不会对其进行检查！
- ‘**紧急模式（阻止所有 Internet 通信）**’ 选中此选项将阻止通过每个网络端口的所有通信；**Firewall** 仍在运行，但所有网络通信都会被停止
- **启用所有向 VPN 传输的信息** - 例如，建议在用 VPN（虚拟专用网）连接在家连接办公室时选中此框。**AVG Firewall** 会自动在所有网络适配器中进行搜索，查找

用于 VPN 连接的网络适配器，并允许所有应用程序连接目标网络（仅适用于未对其指定具体 *Firewall* 规则的应用程序）。在装有普通网络适配器的普通系统中，执行这一简单步骤应该可以避免对需要通过 VPN 使用的每种应用程序都设置详细规则。

注：要启用 VPN 连接，就必须至少允许通过以下系统协议进行通信：GRE、ESP、L2TP、PPTP。可在 *系统服务* 对话框中执行上述操作。

设置管理

在“*设置管理*”部分，您可以 **导出/导入 *Firewall*** 配置；也就是将定义的 *Firewall* 规则和设置导出到备份文件中，或者导入整个备份文件。

10.2. 安全



在“*安全设置*”对话框中，您可以定义 *Firewall* 行为的通用规则（不管选定的配置文件如何，这些规则都适用）：

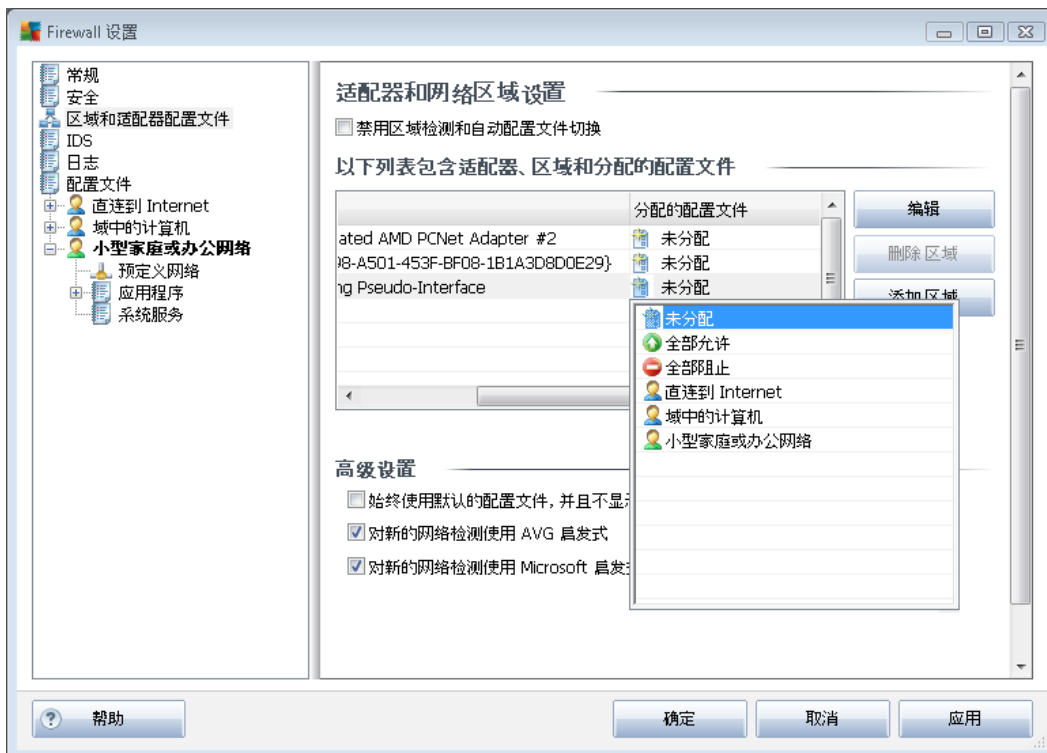
- “**允许以下用户修改设置**”-指定获允更改 *Firewall* 配置的用户
- “**为以下用户显示确认对话框**”-指定应为哪些用户显示确认对话框（在出现定义的 *Firewall* 规则所不适用的情况时要求用户作出决定的对话框）

在这两种情况下，您都可以将相应的特定权限分配给以下用户组之一：

- **管理员** - 对 PC 有完全控制权，有权将每位用户分配到拥有专门定义的权限的组中
- **管理员和超级用户** - 管理员可以将任何用户分配到指定组（*超级用户*）中并定义该组成员的权限
- **所有用户** - 未被分配到任何特定组中的其他用户

10.3. 区域和适配器配置文件

在 **‘适配器和网络区域设置’** 对话框中，您可以编辑与向特定适配器及相应网络分配定义的配置文件相关的设置：



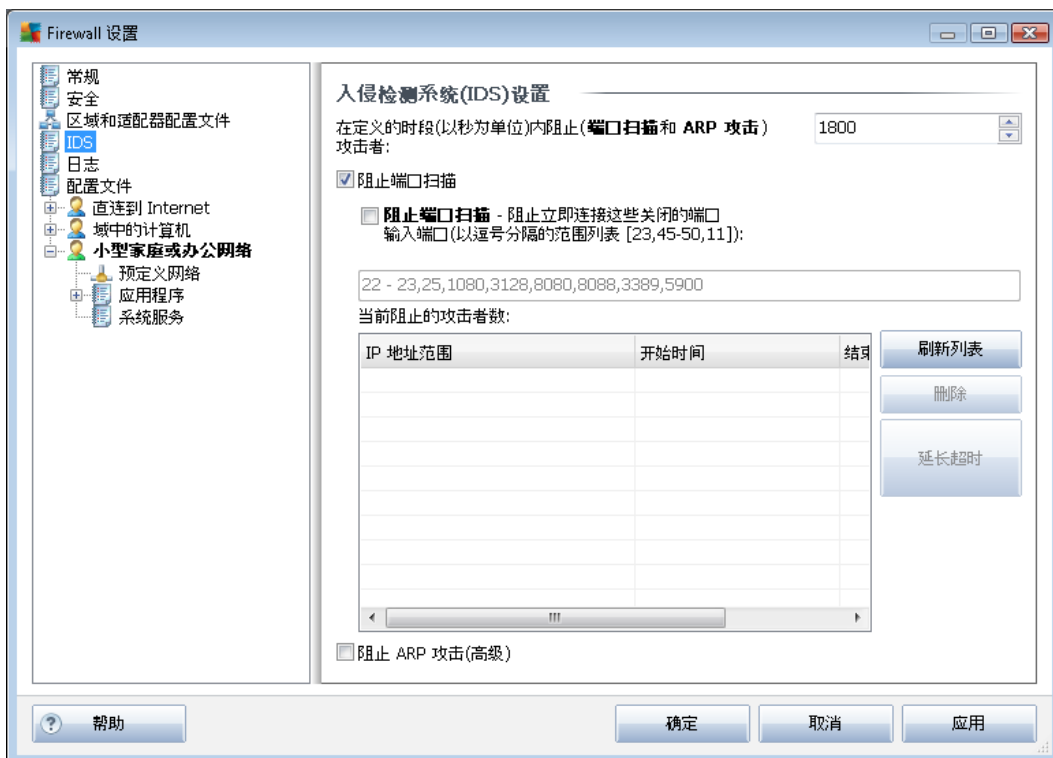
- **禁用区域检测和自动配置文件切换** - 对于每个区域，可分别对每种网络接口类型指定某个已定义的配置文件。如果不想定义特定配置文件，将会使用通用配置文件。不过，如果您决定区分配置文件并将它们分配给特定的适配器和区域，之后由于某种原因，您希望暂时改变这种安排，那么请勾选 **‘禁用区域检测和自动配置文件切换’** 选项。
- **‘适配器、区域及分配的配置文件列表’** 通过此列表可大概了解所检测到的适配器和区域。您可以为其中的每一项分配预定义配置文件菜单中的一个特定配置文件。若要打开此菜单，请单击适配器列表中的对应项，然后选择配置文件。

高级设置

- o **“始终使用默认配置文件且不显示新的网络检测区域”** 每当计算机连接到新的网络时，**Firewall** 都会发出警报，并显示一个对话框，提示您在其中选择网络连接的类型并为其分配 **Firewall 配置文件**。如果您不希望显示该对话框，可选中此框。
- o **使用 AVG 启发式检测新网络** - 用其能收集有关用 AVG 自己的机制检测到的新网络的信息（但是，此选项只能在 Vista 和版本更高的操作系统中使用）。
- o **使用 Microsoft 启发式检测新网络** - 用其能收集有关用 Windows 服务检测到的新网络的信息（此选项只能在 Windows Vista 及更高版本中使用）。

10.4. IDS

“入侵检测系统” 是一种特殊的行为分析功能，旨在发现和阻止计算机特定端口上的可疑通信尝试。您可以在以下界面中配置 IDS 参数：



“入侵检测系统 (IDS) 设置” 对话框提供以下配置选项：

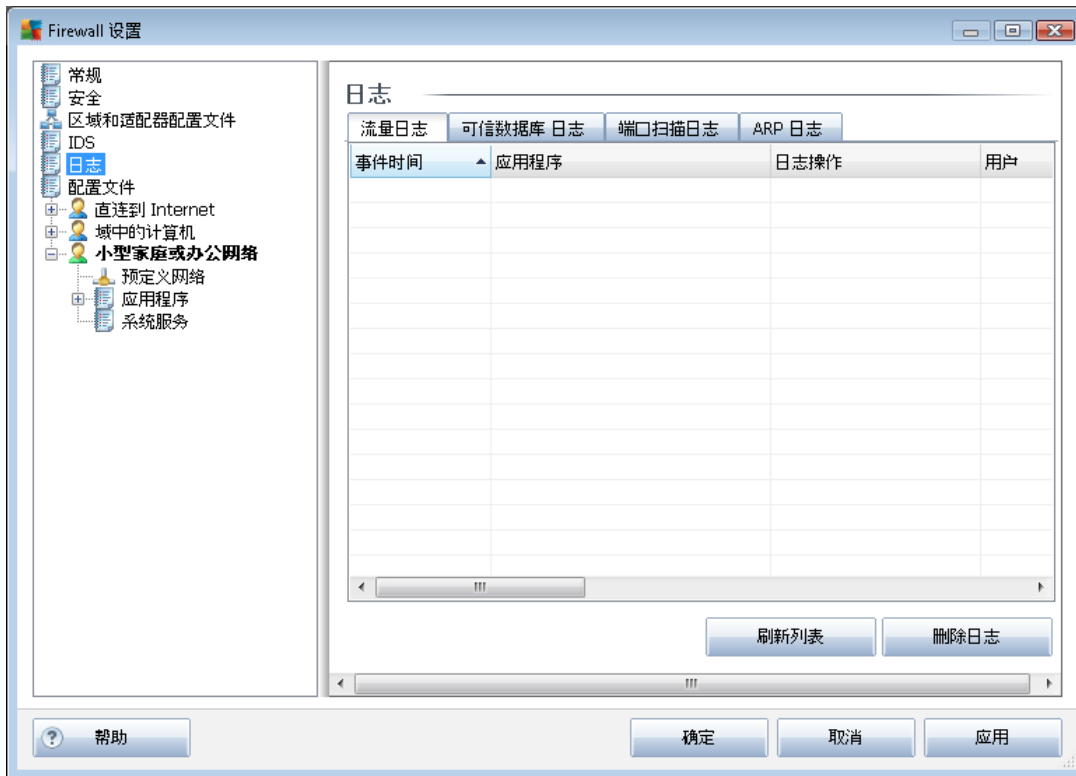
- **“在定义的时段内阻止攻击者”** 您可以在此处设置当某个端口上检测到可疑通信尝试时，应持续阻止该端口多少秒。默认情况下，该时间间隔设置为 1800 秒（30 分钟）。

- **“阻止端口扫描”** - 选中该框可以阻止从外部通过所有 TCP 和 UDP 端口向计算机进行的通信尝试。对于任何此类连接，仅允许进行五次尝试，第六次尝试将被阻止。
 - **“黑端口扫描”** - 选中此框可以立即阻止通过以下文本字段中指定的端口进行的任何通信尝试。各个端口或端口范围应使用逗号隔开。如果您希望使用此功能，这里提供了一个预定义的建议端口列表。
 - **“当前阻止的攻击者”** 此部分列出了 [Firewall](#) 当前阻止的任何通信尝试。完整的阻止尝试历史记录可以在 [“日志”](#) 对话框（[端口扫描日志](#) 选项卡）中查看。
- **“阻止 ARP 攻击”** 可阻止本地网络内被 *IDS* 检测为 有潜在危险 的特定类型的通信尝试。**“在定义的时段内阻止攻击者”** 中设置的时间在此适用。我们建议仅由熟悉本地网络类型和风险级别的高级用户使用此功能。

控制按钮

- **“刷新列表”** 单击此按钮可更新该列表（以包括任何最新阻止的尝试）
- **“删除”** 单击此按钮可取消选定的阻止
- **“延长超时”** 单击此按钮可延长阻止所选尝试的时段。将显示一个带延时选项的新对话框，可以在该对话框中设置特定的时间和日期或者不限时长。

10.5. 日志



在“日志”对话框中，您可以在四个选项卡上查看已记入日志的所有 [Firewall](#) 操作和事件的列表，以及对相关参数的详细说明：（事件时间、应用程序名称、相应的日志操作、用户名、PID、通信方向、协议类型、远程及本地端口号等）：

- “**通信日志**”-提供了所有尝试连接到网络的应用程序的活动信息。
- “**可信数据库日志**”-可信数据库是指收集有关经过验证的可信应用程序的信息的 AVG 内部数据库，始终都可以允许此类应用程序在线进行通信。新的应用程序首次尝试连接到网络时（即尚未为此应用程序指定防火墙规则时），有必要确定是否应允许相应应用程序进行网络通信。首先，AVG 会在可信数据库中进行搜索，如果其中列出了此应用程序，则会自动授予它网络访问权限。只有在经过搜索之后发现数据库中没有关于此应用程序的信息时，才会通过一个独立的对话框询问您是否要允许此应用程序访问网络。
- “**端口扫描日志**”-提供所有 [入侵检测系统](#) 活动的日志记录。
- “**ARP 日志**”-关于阻止本地网络内（[阻止 ARP 攻击](#) 选项）被 [入侵检测系统](#) 检测为有潜在危险的特定类型的通信尝试的日志记录信息。

控制按钮

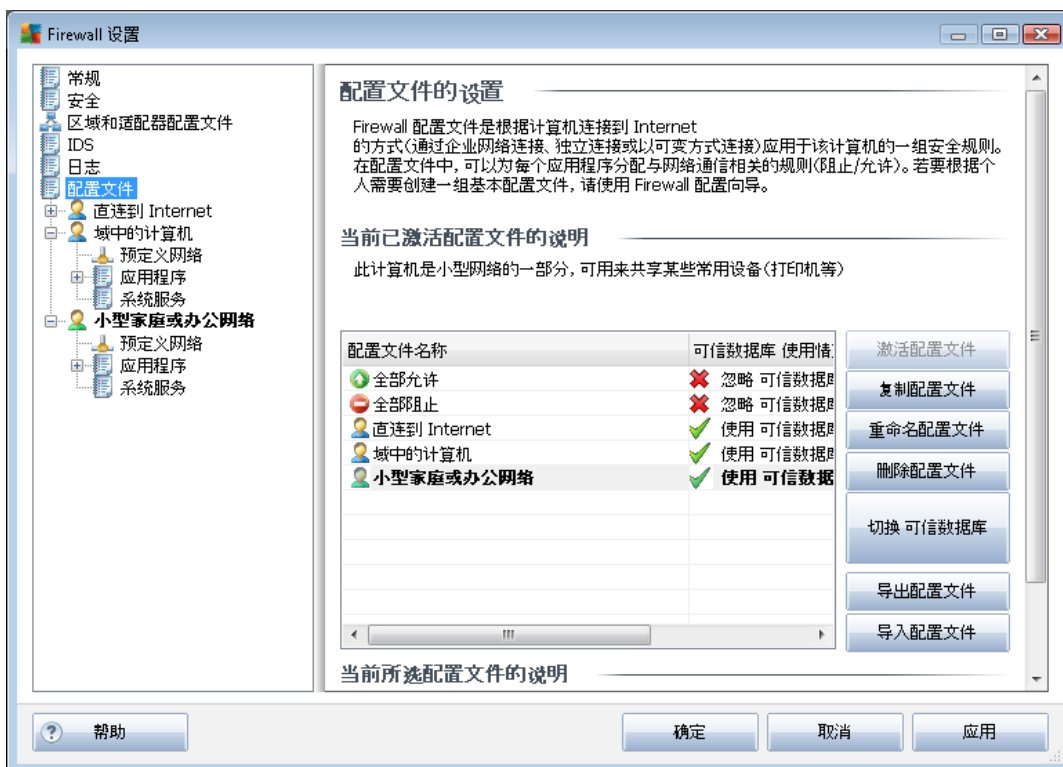
- “**刷新列表**”-可以按照所选属性对所有已记录的参数进行排列：按时间顺序排列

（日期）或按字母顺序排列（其它列）-只需单击相应列标题即可。使用 **刷新列表** 按钮可更新当前显示的信息。

- **“清空列表”**-删除图表中的所有条目。

10.6. 配置文件

“配置文件的设置”对话框中列有全部可用配置文件。



在此对话框中，使用以下控制按钮即可对系统 [配置文件](#) 以外的所有其它配置文件进行编辑：

- **“激活配置文件”**-此按钮用于将选定的配置文件设置为活动配置文件，这意味着 [Firewall](#) 将使用选定配置文件的配置来控制网络通信。
- **“复制配置文件”**-创建一份与选定配置文件完全相同的副本，随后您就可以对该副本进行编辑和重命名，以创建基于所复制的原始配置文件的新配置文件
- **“重命名配置文件”** 允许您为选定的配置文件定义新的名称
- **“删除配置文件”**-从列表中删除选定的配置文件
- **“切换可信数据库”** 对于所选的配置文件，您可以决定使用 [可信数据库](#) 信息（可信数据库是指收集有关经过验证的可信应用程序的数据的 AVG 内部数据库，始终都可以允许此类应用程序在线进行通信。）



- **“导出配置文件”**–将选定配置文件的配置记录到一个文件中，该文件将被保存下来以供以后可能使用
- **“导入配置文件”**–根据从备份配置文件中导出的数据来配置选定配置文件的设置

在此对话框的底部区域中，可以找到对上方列表中当前选定的配置文件的说明。

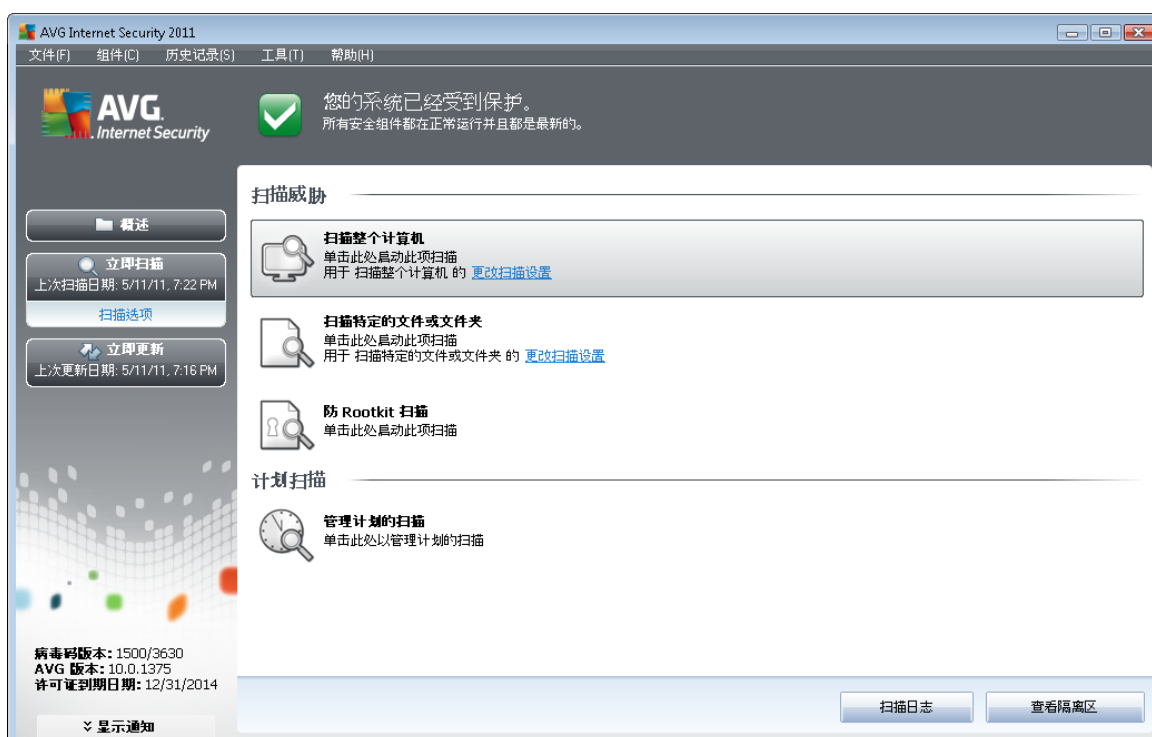
左侧导航菜单的结构将根据 **“配置文件”** 对话框中的相应列表所含的预定义配置文件数目而作出相应的改变。对于每个预定义配置文件，都会在 **“配置文件”** 项下方创建一个特定的分支。随后便可以在以下对话框（对所有配置文件而言都完全相同）中编辑特定的配置文件：



11. AVG 扫描

扫描是 **AVG Internet Security 2011** 功能的关键组成部分。您可以运行按需测试或[安排它们定期运行](#)（在方便的时间运行）。

11.1. 扫描界面



可通过 [扫描选项 快速链接](#) 访问 AVG 扫描界面。单击此链接可切换到 **‘扫描威胁’** 对话框。在此对话框中，您将找到以下内容：

- [预定义扫描](#) 的概览 – 提供了三种类型的扫描（由软件供应商定义），随时可供用户在需要时或按计划立即使用：
 - [扫描整个计算机](#)
 - [扫描特定的文件或文件夹](#)
 - [Anti-Rootkit 扫描](#)
- [扫描计划](#) 区域 – 在此区域中您可以根据需要定义新测试和创建新计划。

控制按钮

此测试界面内提供的控制按钮如下：

- **‘扫描历史记录’** – 显示 [‘扫描结果概览’](#) 对话框，该对话框中包含了完整的扫描



历史记录

- “**查看病毒库**” 在一个新窗口中打开 **病毒库** - 即用于隔离检测到的感染的区域

11.2. 预定义扫描

按需扫描是 **AVG Internet Security 2011** 的主要功能之一。按需测试旨在每当怀疑可能存在病毒感染时便对计算机的各个部分进行扫描。但是，强烈建议定期执行此类测试，即使您认为在您的计算机上找不到病毒，也应如此。

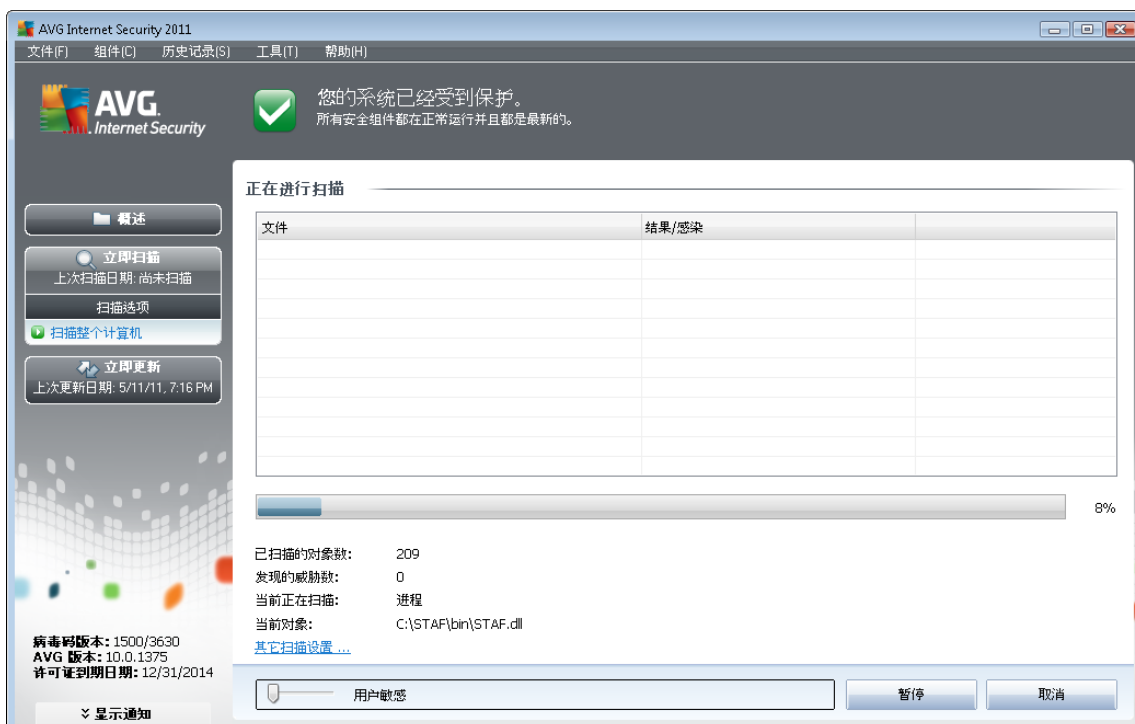
在 **AVG Internet Security 2011** 中提供了软件供应商预定义的以下扫描类型：

11.2.1. 扫描整个计算机

扫描整个计算机 - 扫描您的整个计算机是否存在感染和/或可能不需要的程序。此测试将扫描您计算机的所有硬盘驱动器，检测病毒并修复发现的任何病毒，或将检测到的感染移至 **病毒库**。在工作站上，对整个计算机的扫描应计划为每周至少运行一次。

启动扫描

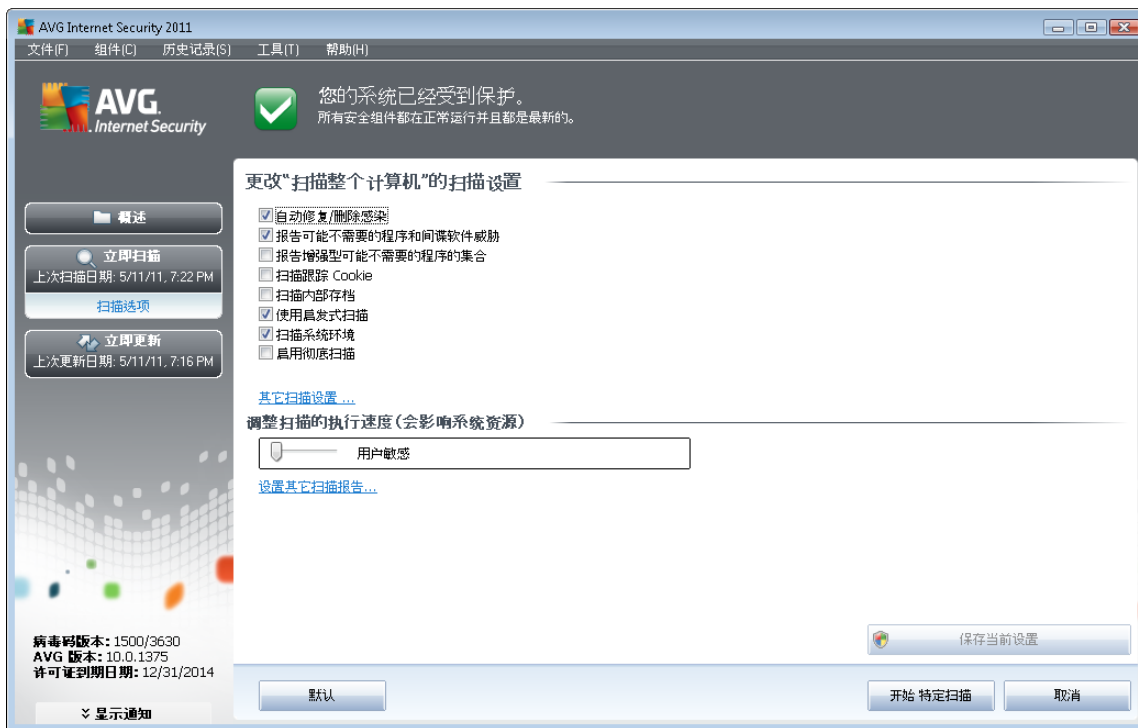
“**扫描整个计算机**”可直接从**扫描界面**中通过单击扫描图标来启动。对于此类型的扫描，无须进一步配置任何特定设置，扫描将立即开始并显示“**正在进行扫描**”对话框（见截图）。如果需要，可以暂时中断（“**暂停**”）或取消（“**停止**”）这种扫描。



编辑扫描配置



您可以选择编辑“**扫描整个计算机**”的预定义默认设置。按“**更改扫描设置**”链接可转到“**更改扫描整个计算机的扫描设置**”对话框（可从[扫描界面](#)中通过[扫描整个计算机](#)”的更改扫描设置链接来访问）。**建议保留默认设置，若非必要，请勿更改！**



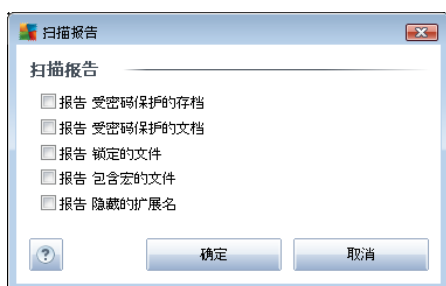
- **扫描参数** - 在扫描参数列表中，您可以根据需要启用/禁用特定参数：
 - **自动修复/移除感染**（默认情况下已启用）- 如果在扫描期间发现病毒并且有修复方案，则可以自动对其进行修复。如果不能自动修复受感染文件，则会将受感染对象移到 **病毒库** 中。
 - **报告可能不需要的程序和间谍软件威胁**（默认情况下已启用）- 选中此框可激活 **Anti-Spyware** 引擎以及针对间谍软件和病毒的扫描。**间谍软件属于疑似恶意软件类软件：虽然它通常代表了安全风险，但有些程序也可能是被特意安装的。**建议保持此功能的激活状态，因为此功能会使计算机更加安全。
 - **报告更多可能不需要的程序**（默认情况下已禁用）- 选中此框可检测更多 **间谍软件**：程序直接从制造商处获得时极其安全而无害，但之后却可能被滥用以达到恶意目的。这项附加措施可以进一步提高计算机的安全性，但也可能会阻止合法程序，因此默认情况下已将其禁用。
 - **扫描跟踪 Cookie**（默认情况下已禁用）- **Anti-Spyware** 组件的此参数用于定义在扫描期间应检测 Cookie（HTTP Cookie 用于验证、跟踪和维护有关用户的特定信息，例如网站首选项或电子购物车中的内容）。
 - **扫描压缩包**（默认情况下已禁用）- 此参数定义扫描时应检查存储在压缩包（如 ZIP 和 RAR 等）中的所有文件。

- **使用后发式扫描**（默认情况下已启用）- 启发式分析（在虚拟的计算机环境中对已扫描对象的指令进行动态模拟）将成为在扫描期间用来进行病毒检测的方法之一。
- **扫描系统环境**（默认情况下已启用）- 扫描时还将检查您计算机的系统区域。
- **启动彻底扫描**（默认情况下已禁用）- 在特定情况下（怀疑计算机受到感染），您可以选中此选项以激活最全面的扫描算法，该算法甚至会对计算机上极难被感染的区域进行扫描以确保绝对安全。不过要记住，此方法相当耗时。
- **其它扫描设置** - 该链接将打开新的 **其它扫描设置** 对话框，在此对话框中可以指定以下参数：



- **计算机关闭选项** - 决定在扫描过程完成时是否应自动关闭计算机。在确认此选项（**扫描完成时关闭计算机**）后，将激活一个新选项（**强制关闭锁定的计算机**），通过该选项，即使目前已锁定计算机也可关机。
- **定义要扫描的文件类型** - 应进一步决定要扫描的文件类型：
 - **所有文件类型**，选择此选项可以通过列出不应扫描的文件扩展名（由逗号分隔）指定特例，不对其进行扫描；
 - **所选文件类型** - 可以指定希望仅扫描可能受到感染的文件（将不扫描不可能遭到感染的文件，例如某些纯文本文件或某些其它的非可执行文件），其中包括媒体文件（视频、音频文件 - 如果将此框保留为未选中状态，则会进一步缩短扫描时间，因为这些文件通常很大，不太可能受到病毒感染）。此外，您还可以通过扩展名指定哪些文件是始终应扫描的文件。
 - 您也可以选择指定要**扫描不带扩展名的文件** - 默认情况下此选项已启用；我们建议，除非确有必要更改，否则将其保持启用。不带扩展名的文件相当可疑，应随时对此类文件进行扫描。

- **调整扫描的完成速度** - 您可以使用滑块更改扫描进程的优先级。默认情况下，此选项值设为用户敏感信息级别，即自动确定资源的使用。另外，您也可以使用较低的速度运行扫描进程，这意味着将最大限度地减少系统资源负荷（如果您需要使用计算机，而不在乎扫描过程所持续的时间，则此选项将十分有用）；也可以使用较快的速度运行扫描，这会增加对系统资源的需求（例如，在计算机暂时无人使用时）。
- **设置其它扫描报告** - 该链接将打开新的 **‘扫描报告’** 对话框，在此对话框中您可以选择应报告可能发现的哪些类型的结果：



警告： 这些扫描设置与新定义的扫描的参数相同 - 有关说明请参见 [‘AVG 扫描/扫描计划/扫描方式’](#) 章节。如果您决定更改 **‘扫描整个计算机’** 功能的默认配置，则您可以将您的新设置保存为默认配置，以用于今后对整个计算机进行的所有扫描。

11.2.2. 扫描特定的文件或文件夹

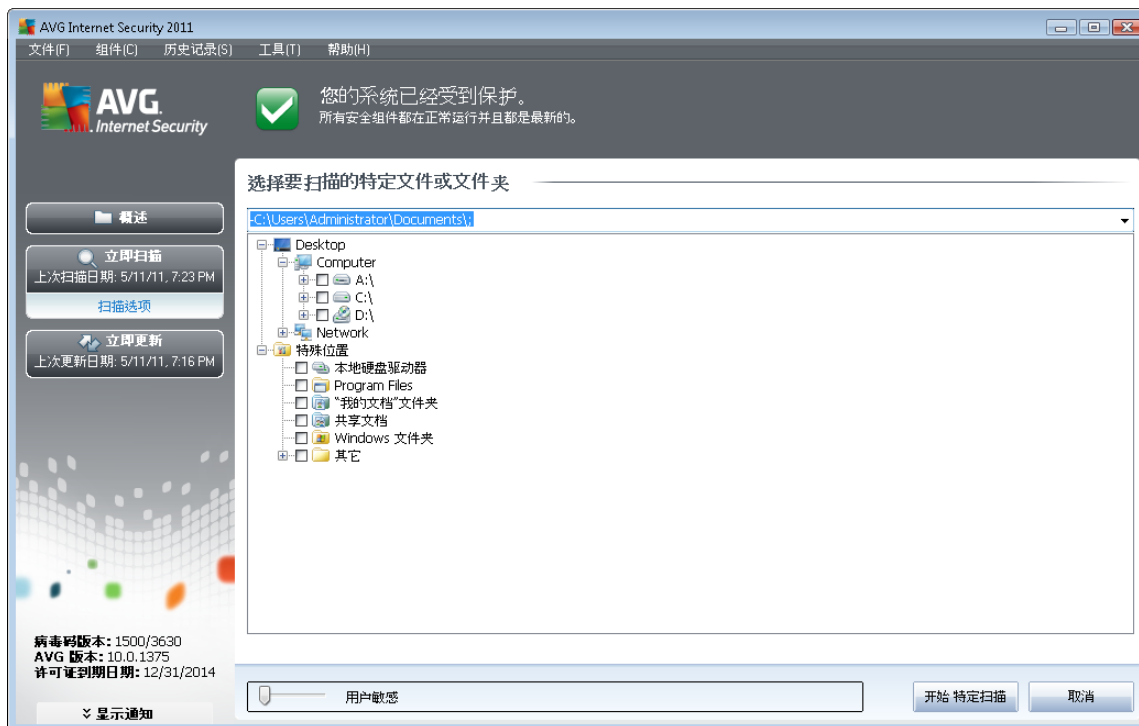
扫描特定的文件或文件夹 - 仅扫描您选定进行扫描的那些计算机区域（选定的文件夹、硬盘、软盘、CD 等）。在检测到病毒并对其进行处理时扫描的进程与采用 **扫描整个计算机** 这一功能处理此情况时相同：修复所发现的任何病毒或将其移至 [病毒库](#)。可以利用 **扫描特定的文件或文件夹** 这一功能来根据您的需要设置您自己的测试并计划这些测试的运行时间。

启动扫描

‘扫描特定的文件或文件夹’ 功能可直接从 [扫描界面](#) 中通过单击此扫描功能的图标来启动。随即便会打开一个名为 **‘选择要扫描的特定文件或文件夹’** 的新对话框。在您计算机的树结构中，选择您希望扫描的那些文件夹。每个选定文件夹的路径将自动生成，并显示在此对话框上部的文本框中。

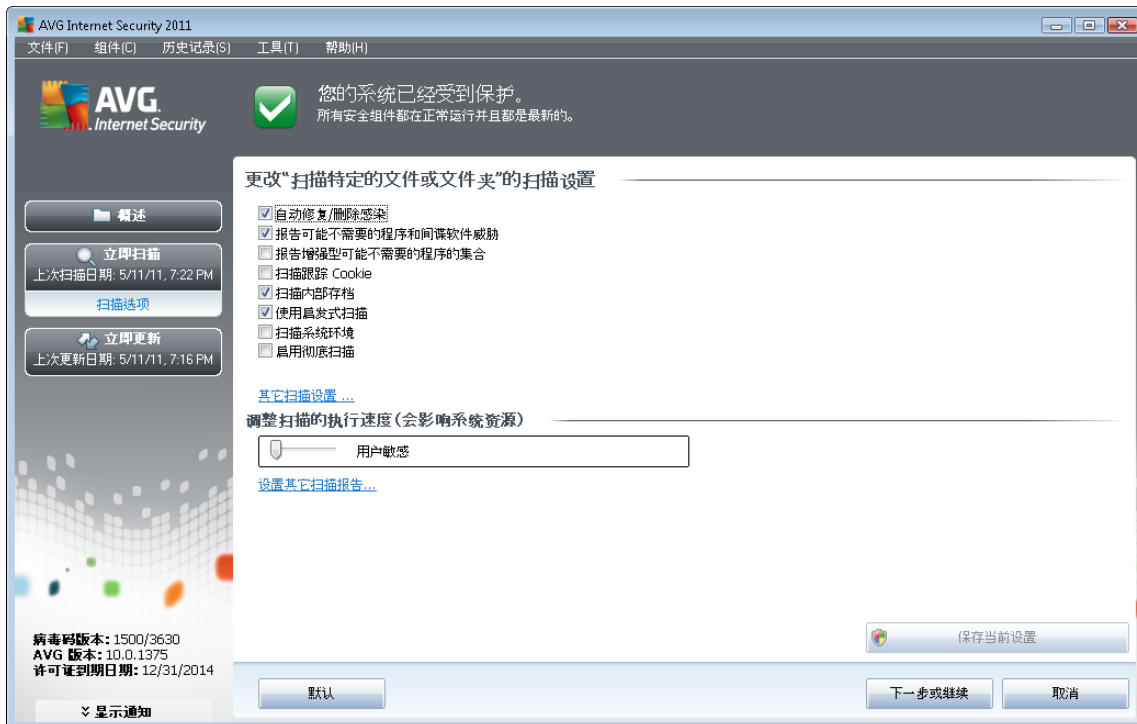
还可以只扫描特定文件夹本身而不扫描其所有子文件夹；为此，请在自动生成的路径前面写一个减号“-”（见截图）。若要将整个文件夹都排除在扫描范围之外，请使用“!”参数。

最后，若要启动扫描，请单击 **‘开始扫描’** 按钮，扫描过程本身与 [扫描整个计算机](#) 基本上完全相同。



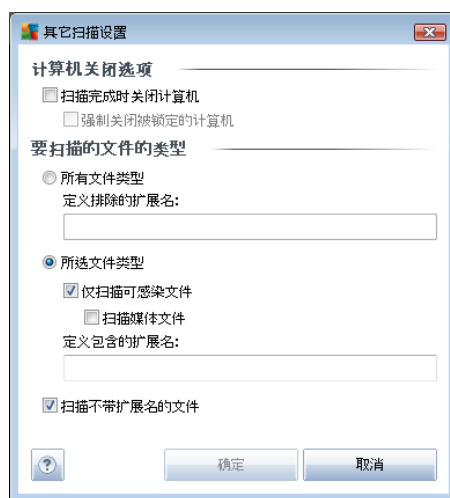
编辑扫描配置

您可以选择编辑 **‘扫描特定的文件或文件夹’** 的预定义默认设置。按 **‘更改扫描设置’** 链接可转到 **‘更改扫描特定的文件或文件夹的扫描设置’** 对话框。**建议保留默认设置，若非必要，请勿更改！**



- **扫描参数** - 在扫描参数列表中，您可以根据需要启用/禁用特定参数：
 - **自动修复/移除感染**（默认情况下已启用）- 如果在扫描期间发现病毒并且有修复方案，则可以自动对其进行修复。如果不能自动修复受感染文件，则会将受感染对象移到 **病毒库** 中。
 - **报告可能不需要的程序和间谍软件威胁**（默认情况下已启用）- 选中此框可激活 **Anti-Spyware** 引擎以及针对间谍软件和病毒的扫描。**间谍软件属于疑似恶意软件类软件：虽然它通常代表了安全风险，但有些程序也可能是被特意安装的。**建议保持此功能的激活状态，因为此功能会使计算机更加安全。
 - **报告更多可能不需要的程序**（默认情况下已禁用）- 选中此框可检测更多 **间谍软件**：程序直接从制造商处获得时极其安全而无害，但之后却可能被滥用以达到恶意目的。这项附加措施可以进一步提高计算机的安全性，但也可能会阻止合法程序，因此默认情况下已将其禁用。
 - **扫描跟踪 Cookie**（默认情况下已禁用）- **Anti-Spyware** 组件的此参数用于定义在扫描期间应检测 Cookie（HTTP Cookie 用于验证、跟踪和维护有关用户的特定信息，例如网站首选项或电子购物车中的内容）。
 - **扫描压缩包**（默认情况下已启用）- 此参数定义扫描时应检查存储在压缩包（如 ZIP 和 RAR 等）中的所有文件。
 - **使用启发式扫描**（默认情况下已禁用）- 启发式分析（在虚拟的计算机环境中对已扫描对象的指令进行动态模拟）将成为在扫描期间用来进行病毒检测的方法之一。

- **扫描系统环境**（默认情况下已禁用）- 扫描时还将检查您计算机的系统区域。
- **启动彻底扫描**（默认情况下已禁用）- 在特定情况下（怀疑计算机受到感染），您可以选中此选项以激活最全面的扫描算法，该算法甚至会对计算机上极难被感染的区域进行扫描以确保绝对安全。不过要记住，此方法相当耗时。
- **其它扫描设置** - 该链接将打开新的 **“其它扫描设置”** 对话框，在此对话框中可以指定以下参数：

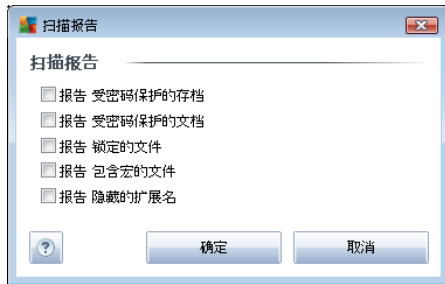


- **计算机关闭选项** - 决定在扫描过程完成时是否应自动关闭计算机。在确认此选项（**扫描完成时关闭计算机**）后，将激活一个新选项（**强制关闭锁定的计算机**），通过该选项，即使目前已锁定计算机也可关机。
- **定义要扫描的文件类型** - 应进一步决定要扫描的文件类型：
 - **所有文件类型**，选择此选项可以通过列出不应扫描的文件扩展名（由逗号分隔）指定特例，不对其进行扫描；
 - **所选文件类型** - 可以指定希望仅扫描可能受到感染的文件（将不扫描不可能遭到感染的文件，例如某些纯文本文件或某些其它的非可执行文件），其中包括媒体文件（视频、音频文件 - 如果将此框保留为未选中状态，则会进一步缩短扫描时间，因为这些文件通常很大，不太可能受到病毒感染）。此外，您还可以通过扩展名指定哪些文件是始终应扫描的文件。
 - 您也可以选择指定要**扫描不带扩展名的文件** - 默认情况下此选项已启用；我们建议，除非确有必要更改，否则将其保持启用。不带扩展名的文件相当可疑，应随时对此类文件进行扫描。
- **扫描进程优先级** - 您可以使用滑块更改扫描进程的优先级。默认情况下，此选项值设为**用户敏感信息**级别，即自动确定资源的使用。另外，您也可以使用较低的速度运行扫描进程，这意味着将最大限度地减少系统资源负荷（如果您需要使用计算机，而不在乎扫描过程所持续的时间，则此选项将十分有用）；也可以用较快



的速度运行扫描，这会增加对系统资源的需求（例如，在计算机暂时无人使用时）。

- **设置其它扫描报告** - 该链接将打开新的 **‘扫描报告’** 对话框，在此对话框中您可以选择应报告可能发现的哪些类型的结果：



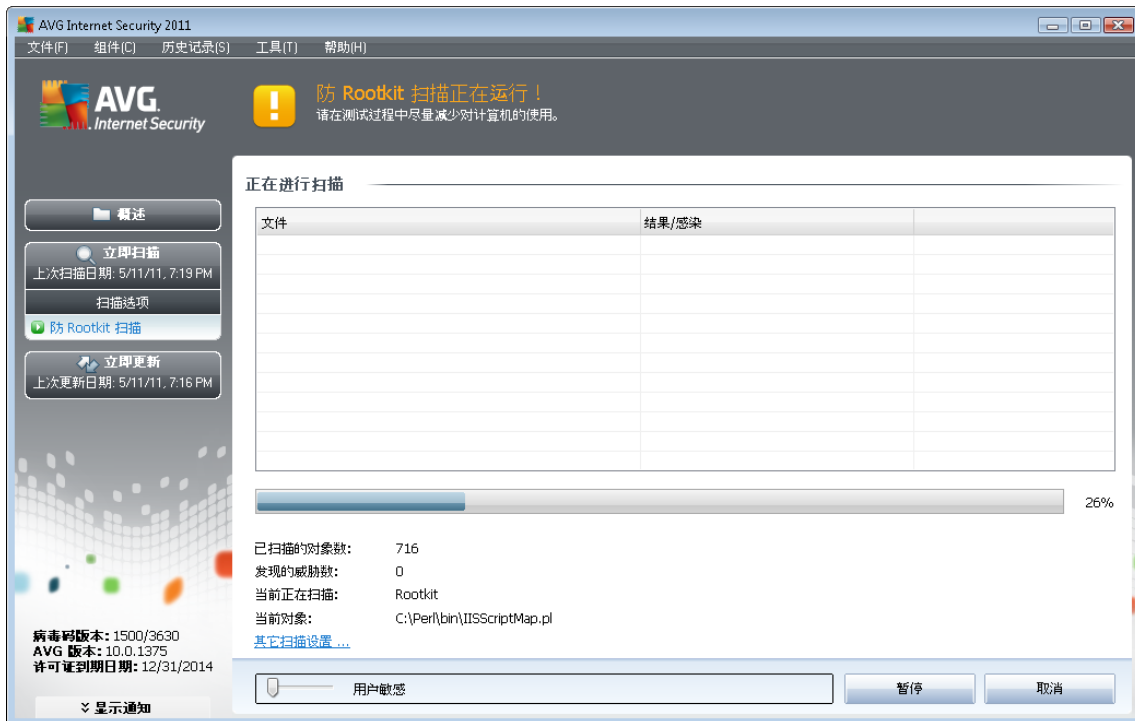
警告： 这些扫描设置与新定义的扫描的参数相同 - 有关说明请参见 [‘AVG 扫描/扫描计划/扫描方式’](#) 章节。如果您决定更改 **‘扫描特定的文件或文件夹’** 功能的默认配置，则您可以将您的新设置保存为默认配置，以用于今后对特定文件或文件夹进行的所有扫描。此外，此配置将被用作您新计划的所有扫描的模板（[所有自定义的扫描都基于扫描选定的文件或文件夹的当前配置](#)）。

11.2.3. Anti-Rootkit 扫描

Anti-Rootkit 扫描 用于在您的计算机中搜索是否可能存在 Rootkit（可以在您的计算机中掩盖恶意软件活动的程序和技术）。如果检测到 Rootkit，并不一定意味着您的计算机已受到感染。有些情况下，特定的驱动程序或正常应用程序的组成部分可能会被误检测为 Rootkit。

启动扫描

Anti-Rootkit 扫描 功能可以直接从 [扫描界面](#) 中通过单击此扫描功能的图标来启动。无须再对此类扫描配置任何特定设置，会立即开始扫描并显示 **‘正在进行扫描’** 对话框（见截图）。如果需要，可以暂时中断（**‘暂停’**）或取消（**‘停止’**）这种扫描。



编辑扫描配置

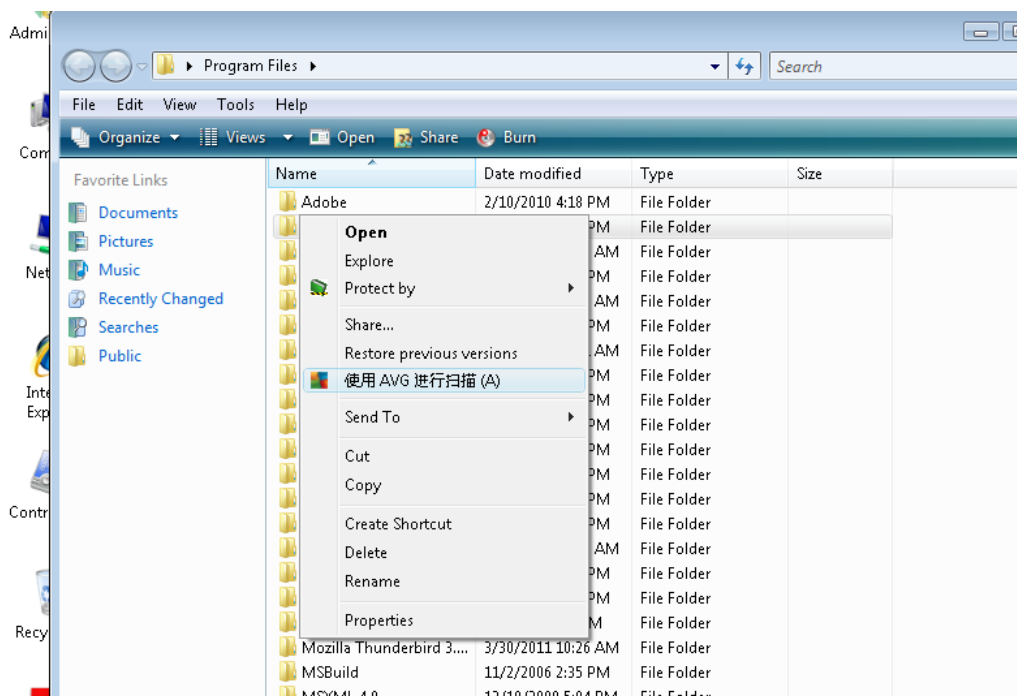
Anti-Rootkit 扫描始终以默认设置启动，且只能在 **“AVG 高级设置/Anti-Rootkit”**对话框中编辑相应的扫描参数。在扫描界面中，仅当正在扫描时才提供以下配置：

- **自动扫描** - 您可以使用滑块更改扫描进程的优先级。默认情况下，此选项值设为 **用户敏感信息** 级别，即自动确定资源的使用。另外，您也可以使用较低的速度运行扫描进程，这意味着将最大限度地减少系统资源负荷（如果您需要使用计算机，而不在乎扫描过程所持续的时间，则此选项将十分有用）；也可以使用较快的速度运行扫描，这会增加对系统资源的需求（例如，在计算机暂时无人值守时）。
- **其它扫描设置** - 该链接将打开新的 **“其它扫描设置”**对话框，在此对话框中，您可以定义可能与 **Anti-Rootkit 扫描**相关的计算机关机条件（**“扫描完成时关闭计算机”**，或 **“强制关闭锁定的计算机”**）：



11.3. 扫描 Windows 资源管理器

除了针对整个计算机或其选定区域启动的预定义扫描之外，**AVG Internet Security 2011** 还提供了直接在 Windows 资源管理器环境中快速扫描特定对象的选项。如果您要打开一个未知文件并且无法确定其内容，则您可能想在需要时对它进行检查。请按照以下步骤操作：



- 在 Windows 资源管理器中，突出显示您要检查的文件（或文件夹）
- 在此对象上单击鼠标右键以打开上下文菜单
- 选择 **“使用 AVG 扫描”** 选项以使用 AVG 扫描此文件



11.4. 命令行扫描

AVG Internet Security 2011 中有从命令行执行扫描的选项。例如，可以在服务器上使用此选项，或者在创建要在计算机启动后自动启动的批处理脚本时使用此选项。您可以使用 AVG 图形用户界面中提供的大多数参数从命令行启动扫描。

若要从命令行启动 AVG 扫描，请在 AVG 的安装文件夹中运行以下命令：

- **avgscanx**（用于 32 位操作系统）
- **avgscana**（用于 64 位操作系统）

命令语法

此命令的语法如下：

- **avgscanx /参数** ... 例如，**avgscanx /comp** 表示扫描整个计算机
- **avgscanx /参数 /参数** ... 如果有多个参数，则这些参数应位于一行中且相互之间用一个空格和一个斜杠字符分隔开来
- 如果需要为参数提供特定的值（例如 **/scan** 参数，此参数需要有关要扫描哪些选定计算机区域的信息，您必须提供选定区域的确切路径），则需用分号将这些值隔开，例如：**avgscanx /scan=C:\;D:**

扫描参数

若要显示可用参数的完整概述，请键入相应的命令，后跟参数 **/?** 或 **/HELP**（例如 **avgscanx /?**）。唯一一个不可缺少的参数就是 **/SCAN**，此参数用于指定应扫描的计算机区域。有关各个选项的详细说明，请参见[命令行参数概述](#)。

若要执行扫描，请按 **Enter**。在扫描过程中，按 **Ctrl+C** 或 **Ctrl+Pause** 可停止扫描过程。

从图形界面启动的 CMD 扫描

在 Windows 安全模式下运行计算机时，还可以从图形用户界面中启动命令行扫描。扫描本身将从命令行启动，“**命令行编译器**”对话框只是允许您在易用的图形界面中指定大多数扫描参数。

由于此对话框仅可以在 Windows 安全模式中访问，因此若要查看关于此对话框的详细说明，请参阅直接从此对话框中打开的帮助文件。

11.4.1. CMD 扫描参数

下面列出了可用于命令行扫描的所有参数：

- **/SCAN** [扫描特定的文件或文件夹](#) /SCAN=路径;路径（例如 /SCAN=C:\;D:\）



- **/COMP** [扫描整个计算机](#)
- **/HEUR** 使用 [启发式分析](#)
- **/EXCLUDE** 将路径或文件排除在扫描范围之外
- **/@** 命令文件 /文件名/
- **/EXT** 扫描这些扩展名 /例如 EXT=EXE,DLL/
- **/NOEXT** 不扫描这些扩展名 /例如 NOEXT=JPG/
- **/ARC** 扫描压缩包
- **/CLEAN** 自动清理
- **/TRASH** 将受感染的文件移至 [病毒库](#)
- **/QT** 快速测试
- **/MACROW** 报告宏
- **/PWDW** 报告受密码保护的文件
- **/IGNLOCKED** 忽略被锁定的文件
- **/REPORT** 将报告输出至文件 /文件名/
- **/REPAPPEND** 附加到报告文件
- **/REPOK** 将未受感染的文件报告为 “正常”
- **/NOBREAK** 不允许使用 Ctrl-Break 中止操作
- **/BOOT** 启用 MBR/BOOT 检查
- **/PROC** 扫描活动的进程
- **/PUP** 报告 [可能不需要的程序](#)”
- **/REG** 扫描注册表
- **/COO** 扫描 Cookie
- **/?** 显示有关此主题的帮助
- **/HELP** 显示有关此主题的帮助
- **/PRIORITY** 设置扫描优先级 /低、自动、高/ (请参见 [高级设置 /扫描](#))
- **/SHUTDOWN** 扫描完成时关闭计算机



- **/FORCESHUTDOWN** 扫描完成时强制关闭计算机
- **/ADS** 扫描备用数据流（仅限 NTFS）
- **/ARCBOMBSW** 报告重新压缩的存档文件

11.5. 扫描计划

通过 **AVG Internet Security 2011**，您可以根据需要（例如，当您怀疑您的计算机受到感染时）或按照制定的计划运行扫描。强烈建议按照计划运行扫描：这样您可以确保您的计算机受到保护而不存在任何受感染的可能性，并且您将无需担心是否要启动扫描以及何时启动扫描。

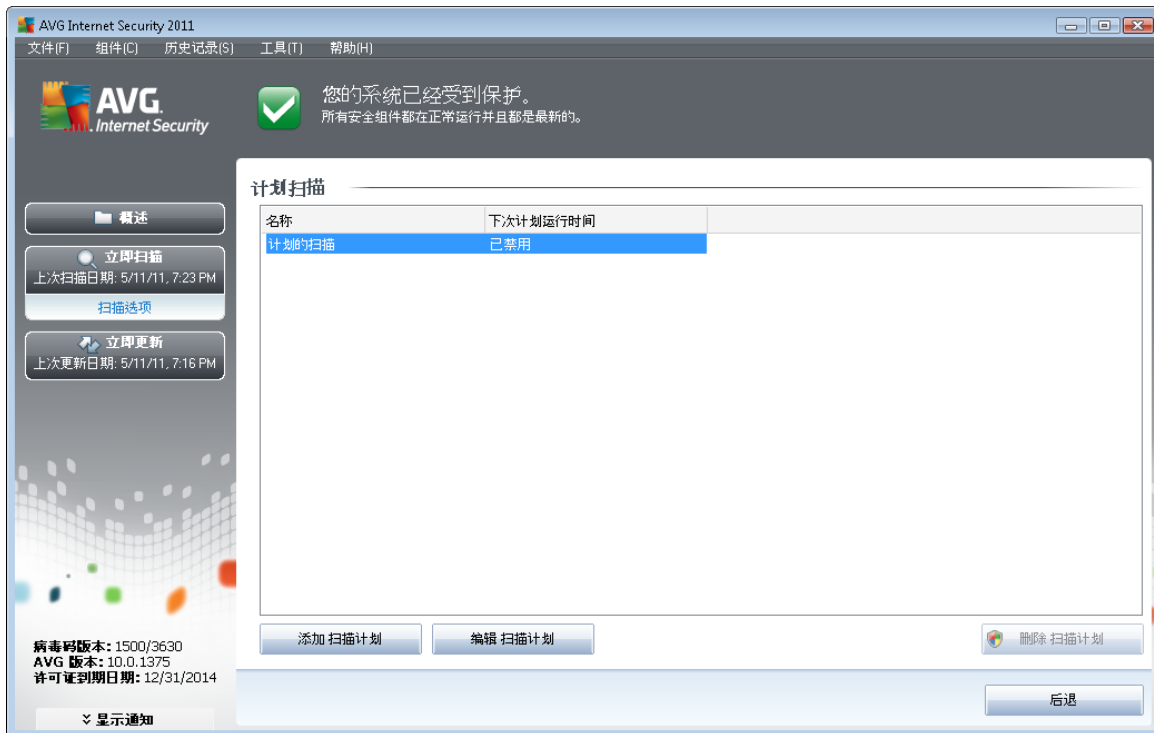
您应定期 **扫描整个计算机**，至少每周一次。不过，如果可能，对整个计算机的扫描应每日进行一次 - 扫描计划的默认配置中便是这样设置的。如果计算机“始终处于开机状态”，那么您可以将扫描安排在工作时间运行。如果计算机有时会关机，则可以这样安排扫描：**如果错过扫描任务，则在计算机启动时运行扫描**。

若要创建新的扫描计划，请查看 [AVG 扫描界面](#) 并在其底部找到名为 **“计划扫描”** 的区域：



计划扫描

单击 **“计划扫描”** 区域中的相应图标可打开一个新的 **“计划扫描”** 对话框，此对话框中列出了当前计划的所有扫描：

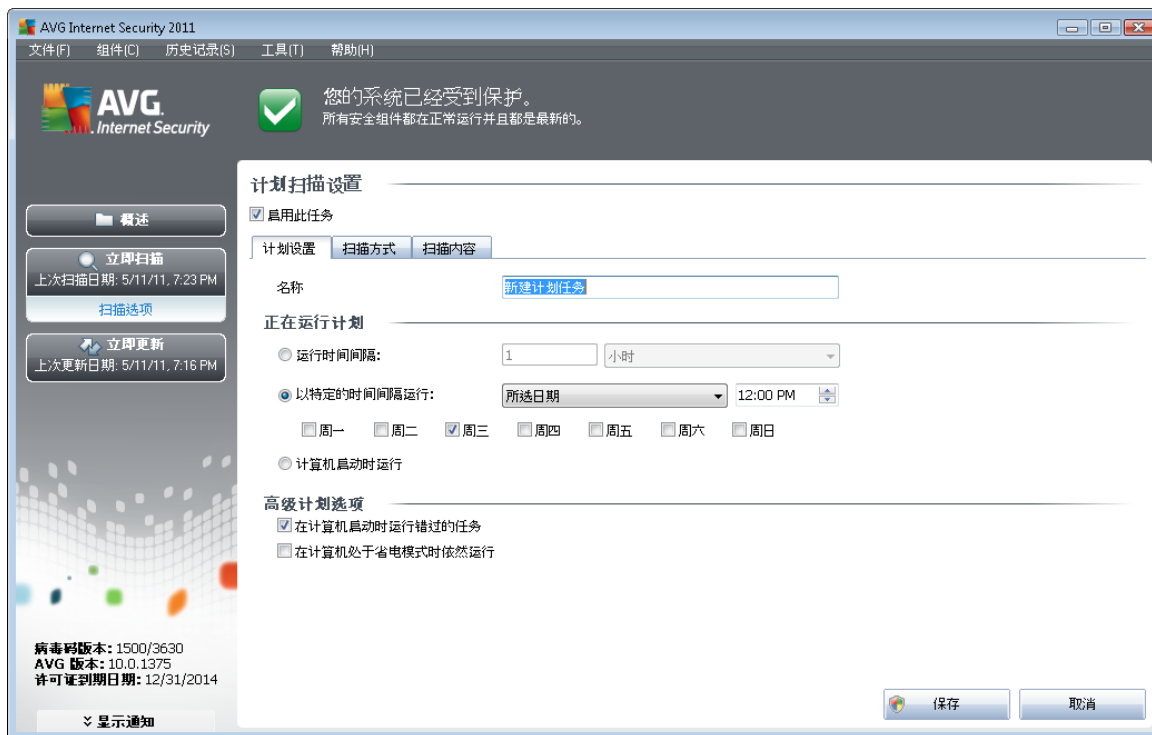


可以使用以下控制按钮来编辑/添加扫描：

- **添加扫描计划** - 按此按钮可打开 **计划的扫描设置** 对话框中的 **计划设置** 选项卡。在此对话框中，您可以指定新定义的测试的参数。
- **编辑扫描计划** - 仅当您之前已经从计划的测试列表中选择了现有测试的情况下，才可以使用此按钮。如果此按钮显示为已激活，则您可以单击它以切换到 **计划的扫描设置** 对话框中的 **计划设置** 选项卡。此选项卡中已经指定了选定测试的参数，您可以进行编辑。
- **删除扫描计划** - 如果您之前已经从计划的测试列表中选择了现有测试，则此按钮也已激活。按此控制按钮可以从列表中删除此测试。不过，您只能删除您自己的测试；在默认设置中预定义的 **整个计算机扫描计划** 是永远无法删除的。
- **后退** - 返回 [AVG 扫描界面](#)

11.5.1. 计划设置

如果要计划新的测试及其定期启动任务，请进入 **计划的测试设置** 对话框（单击 **计划扫描** 对话框中的 **添加扫描计划** 按钮）。此对话框分为以下三个选项卡：**计划设置**（见下图（系统将自动将您重定向到的默认选项卡））、**扫描方式** 和 **扫描内容**。



在“**计划设置**”选项卡中，可以先选中/取消选中“**启用此任务**”项以暂时停用计划的测试，在实际需要时再启用它。

接下来，为即将创建和计划的扫描提供一个名称。在“**名称**”项旁边的文本字段中键入名称。请尽量对扫描使用简洁、适当的描述性名称，以便以后更容易将其与其它扫描辨别开来。

例如：将扫描命名为 **新扫描** 或 **我的扫描** 并不适当，因为这些名称并未指出扫描实际检查的内容。相反，**系统区域扫描** 等名称就可以称得上是不错的描述性名称。此外，没有必要在扫描的名称中指定它是对整个计算机的扫描还是仅扫描选定的文件或文件夹 - 您自己创建和计划的扫描始终都属于 扫描选定的文件或文件夹。

在此对话框中，可以进一步定义下列扫描参数：

- “**计划执行**”-指定新计划的扫描启动任务的时间间隔。此时间间隔的定义方式有三种：指定经过一段特定的时间后重新启动扫描（“**每隔 ... 运行一次**”）；或定义确切的日期和时间（“**在特定的时间运行...**”）；也可以定义扫描启动操作应关联的事件（“**操作条件：计算机启动时**”）。
- “**高级计划选项**”-在此区域中，可以定义当计算机处于省电模式或完全关闭时，应该/不应启动扫描的条件。

“计划的扫描设置”对话框中的控制按钮

“计划的扫描设置”对话框的所有三个选项卡（“计划设置”、“扫描方式”和“扫描内容”）中都有两个控制按钮，无论目前使用的是哪个选项卡，这两个按钮的功能都相同：



- **保存** - 保存您在此选项卡或此对话框的任何其它选项卡中所执行的所有更改并返回 [AVG 扫描界面的默认对话框](#)。因此，如果您希望在所有选项卡上配置测试参数，请仅在您指定了所有要求之后才按此按钮以进行保存。
- **取消** - 取消您在此选项卡或此对话框的任何其它选项卡中所执行的任何更改并返回 [AVG 扫描界面的默认对话框](#)。

11.5.2. 扫描方式



‘扫描方式’选项卡上包含一个扫描参数列表，可以选择启用/禁用这些参数。默认情况下，大多数参数都处于启用状态，并将在扫描过程中发挥作用。除非有必要更改这些设置，否则我们建议保留预定义的配置：

- **自动修复/移除感染**（默认情况下已启用）：如果在扫描期间发现病毒并且有修复方案，则可以自动对其进行修复。如果受感染的文件无法自动修复，或者您决定禁用此选项，则会在检测到病毒时通知您，此时您必须决定要对检测到的感染作何处理。建议操作是将受感染的文件删除至 [病毒库](#)。
- **报告可能不需要的程序和间谍软件威胁**（默认情况下已启用）：选中此框可激活 [Anti-Spyware](#) 引擎以及针对间谍软件和病毒的扫描。[间谍软件属于疑似恶意软件类软件：虽然它通常代表了安全风险，但有些程序也可能是被特意安装的。](#)建议保持此功能的激活状态，因为此功能会使计算机更加安全。
- **报告更多可能不需要的程序**（默认情况下已禁用）：选中此框可检测更多 [间谍软件](#)：程序直接从制造商处获得时极其安全而无害，但之后却可能被滥用以达到恶意目的。这项附加措施可以进一步提高计算机的安全性，但也可能会阻止合法程序，因此默认情况下已将其禁用。

- **扫描跟踪 Cookie**（默认情况下已禁用）：[Anti-Spyware](#) 组件的此参数用于定义应在扫描期间检测 Cookie（HTTP Cookie 用于验证、跟踪和维护有关用户的特定信息，例如网站首选项或电子购物车中的内容）。
- **扫描压缩包**（默认情况下已禁用）：此参数定义扫描时应检查所有文件，即使这些文件被存储在某种压缩包（如 ZIP 和 RAR 等）内也不例外。
- **使用启发式扫描**（默认情况下已启用）：启发式分析（在虚拟的计算机环境中对已扫描对象的指令进行动态模拟）将成为在扫描期间用来进行病毒检测的方法之一。
- **扫描系统环境**（默认情况下已启用）：扫描时还将检查您计算机的系统区域。
- **启动彻底扫描**（默认情况下已禁用）- 在特定情况下（怀疑计算机受到感染），您可以选中此选项以激活最全面的扫描算法，该算法甚至会对计算机上极难被感染的区域进行扫描以确保绝对安全。不过要记住，此方法相当耗时。

接下来，您可以更改扫描配置，说明如下：

- **其它扫描设置** - 该链接将打开新的 **其它扫描设置** 对话框，在此对话框中可以指定以下参数：

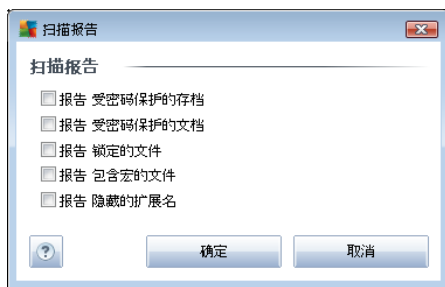


- **计算机关闭选项** - 决定在扫描过程完成时是否应自动关闭计算机。在确认此选项（**扫描完成时关闭计算机**）后，将激活一个新选项（**强制关闭锁定的计算机**），通过该选项，即使目前已锁定计算机也可关机。
- **定义要扫描的文件类型** - 应进一步决定要扫描的文件类型：
 - **所有文件类型**，选择此选项可以通过列出不应扫描的文件扩展名（由逗号分隔）指定特例，不对其进行扫描；
 - **所选文件类型** - 可以指定希望仅扫描可能受到感染的文件（将不扫描不可能遭到感染的文件，例如某些纯文本文件或某些其它的非可执行文件），其中包括媒体文件（视频、音频文件 - 如果将此框保留为未选中状态，则会进一步缩短扫描时间，因为这些文件通常很大，不太可能受到

病毒感染)。此外，您还可以通过扩展名指定哪些文件是始终应扫描的文件。

- 您也可以选择指定要**扫描不带扩展名的文件** - 默认情况下此选项已启用；我们建议，除非确有必要更改，否则将其保持启用。不带扩展名的文件相当可疑，应随时对此类文件进行扫描。

- **调整扫描的完成速度** - 您可以使用滑块更改扫描进程的优先级。默认情况下，此选项值设为**用户敏感信息级别**，即自动确定资源的使用。另外，您也可以使用较低的速度运行扫描进程，这意味着将最大限度地减少系统资源负荷（*如果您需要使用计算机，而不在乎扫描过程所持续的时间，则此选项将十分有用*）；也可以使用较快的速度运行扫描，这会增加对系统资源的需求（*例如，在计算机暂时无人使用时*）。
- **设置其它扫描报告** - 该链接将打开新的 **“扫描报告”** 对话框，在此对话框中您可以选择应报告可能发现的哪些类型的结果：



注：默认情况下，扫描配置已经过设置，可达到最佳性能。除非确有必要更改扫描设置，否则强烈建议保留预定义的配置。任何配置更改都仅应由经验丰富的用户执行。有关其它扫描配置选项，请参见 **“高级设置”** 对话框，可通过**文件/高级设置**系统菜单项访问此对话框。

控制按钮

“计划的扫描设置” 对话框的所有三个选项卡（**“计划设置”**、**“扫描方式”** 和 **“扫描内容”**）中都有两个控制按钮，无论目前使用的是哪个选项卡，这两个按钮的功能都相同：

- **保存** - 保存您在此选项卡或此对话框的任何其它选项卡中所执行的所有更改并返回 **AVG 扫描界面的默认对话框**。因此，如果您希望所有选项卡上配置测试参数，请仅在您指定了所有要求之后才按此按钮以进行保存。
- **取消** - 取消您在此选项卡或此对话框的任何其它选项卡中所执行的任何更改并返回 **AVG 扫描界面的默认对话框**。



11.5.3. 扫描内容



在 **“扫描内容”** 选项卡上，您可以定义您要计划的是 [扫描整个计算机](#) 还是 [扫描特定的文件或文件夹](#)。”

如果您选择的是“扫描特定的文件或文件夹”，则在此对话框底部将激活如图所示的树结构，您可以利用它来指定要扫描的文件夹（单击加号节点以展开各项，直到您找到要扫描的文件夹为止）。可以通过选中多个文件夹的对应框来选定这些文件夹。选定的文件夹将显示在对话框顶部的文本字段中，下拉菜单将保留所选扫描的历史记录以供日后使用。也可手动输入所需文件夹的完整路径（如果您输入多个路径，则必须用分号将它们隔开，不加空格）。

还可在树结构中看到名为 **“特殊位置”** 的分支。下表指出了在相应复选框被选中后会扫描的位置：

- **本地硬盘驱动器** - 计算机的所有硬盘驱动器
- **程序文件**
 - o C:\Program Files\
 - o 在 64 位版本中为 C:\Program Files (x86)
- **“我的文档”文件夹**
 - o 对于 Win XP 为：C:\Documents and Settings\Default User\My Documents\



o 对于 Windows Vista/7 为：C:\Users\user\Documents\

- **共享文档**

o 对于 Win XP 为：C:\Documents and Settings\All Users\Documents\

o 对于 Windows Vista/7 为：C:\Users\Public\Documents\

- **Windows 文件夹** - C:\Windows\

- **其它**

- o 系统驱动器 - 装有操作系统的硬盘驱动器（通常是 C:）

- o 系统文件夹 - C:\Windows\System32\

- o 临时文件文件夹 - C:\Documents and Settings\User\Local\ (Windows XP)；或 C:\Users\user\AppData\Local\Temp\ (Windows Vista/7)

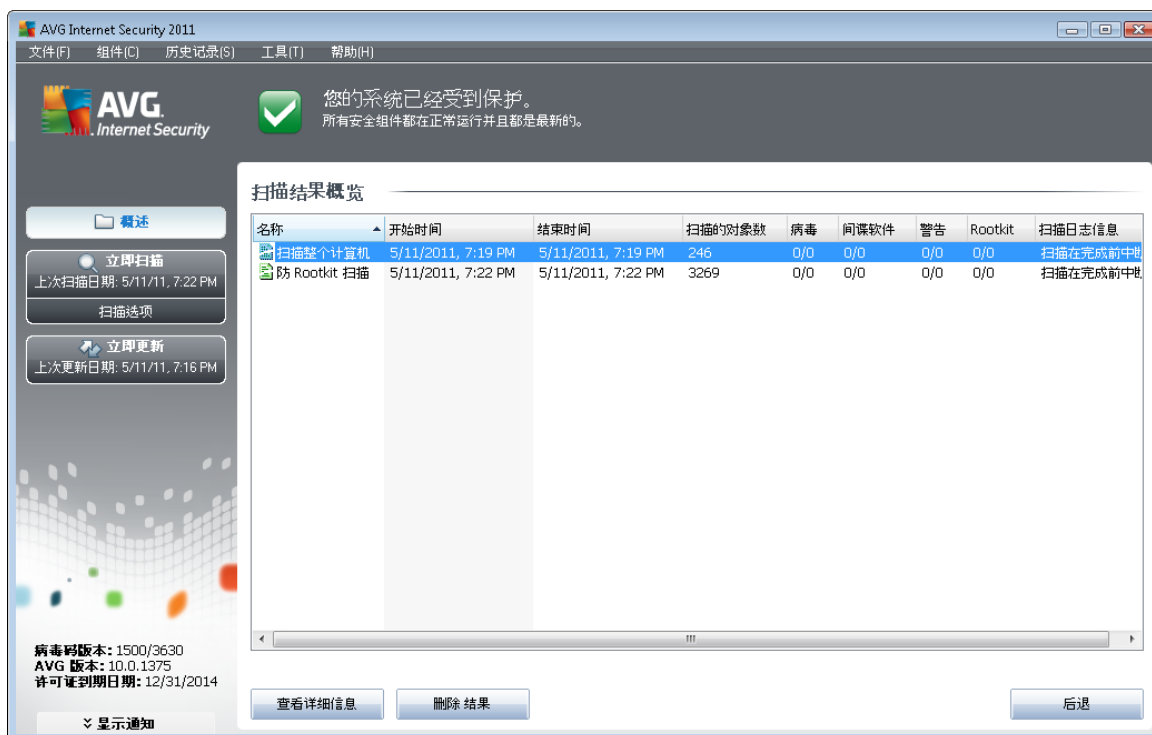
- o Internet 临时文件 - C:\Documents and Settings\User\Local Settings\Temporary Internet Files\ (Windows XP)；或 C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files (Windows Vista/7)

“计划的扫描设置”对话框中的控制按钮

“计划的扫描设置”对话框的所有三个选项卡（[“计划设置”](#)、[“扫描方式”](#)和 [“扫描内容”](#)）中都有两个控制按钮，无论目前使用的是哪个选项卡，这两个按钮的功能都相同：

- **保存** - 保存您在此选项卡或此对话框的任何其它选项卡中所执行的所有更改并返回 [AVG 扫描界面的默认对话框](#)。因此，如果您希望在所有选项卡上配置测试参数，请仅在您指定了所有要求之后才按此按钮以进行保存。
- **取消** - 取消您在此选项卡或此对话框的任何其它选项卡中所执行的任何更改并返回 [AVG 扫描界面的默认对话框](#)。

11.6. 扫描结果概览



“扫描结果概览”对话框可从 [AVG 扫描界面](#) 中通过 “[扫描历史记录](#)” 按钮进行访问。此对话框列出了以前启动的所有扫描及其结果的信息：

- “**名称**”-扫描名称；可以是其中一个[预定义扫描](#)的名称，也可以是您为[自己的计划扫描](#)指定的名称。每个名称都包含一个指示扫描结果的图标：

 -绿色图标表明在扫描期间未检测到感染

 -蓝色图标表示在扫描期间检测到感染，但受感染的对象已被自动删除

 -红色图标警告在扫描期间检测到感染，但无法将其删除！

每个图标要么是实心的，要么被切成两半 -实心图标表示该扫描已完成并正常结束；被切成两半的图标表示该扫描已被取消或中断。

注：有关每个扫描的详细信息，请参见 [“扫描结果”](#)对话框，可通过 [“查看详细信息”](#)按钮（在此对话框的底部）访问此对话框。

- “**开始时间**”-扫描开始的日期和时间
- “**结束时间**”-扫描结束的日期和时间
- “**测试的对象数**”-扫描期间检查的对象数
- “**感染**”-检测到/删除的[病毒感染](#)数



- **“间谍软件”** - 检测到/删除的 [间谍软件](#) 数
- **警告** - 检测到的 [可疑对象](#)
- **Rootkit** - 检测到的 [Rootkit](#)
- **“扫描日志信息”** - 与扫描过程和结果相关的信息（通常与其终止或中断有关）

控制按钮

“扫描结果概览” 对话框的控制按钮有：

- **“查看详细信息”** - 按此按钮可切换到 [“扫描结果”](#) 对话框，以查看有关所选扫描操作的详细数据
- **“删除结果”** - 按此按钮可从扫描结果概览中删除所选扫描结果
- **“后退”** - 返回 [AVG 扫描界面的默认对话框](#)

11.7. 扫描结果详细信息

如果在 [“扫描结果概览”](#) 对话框中选定了特定扫描，则您可以单击 **“查看详细信息”** 按钮切换到 [“扫描结果”](#) 对话框，此对话框提供了有关选定扫描的过程和结果的详细数据。

此对话框又分为若干选项卡：

- **“结果概览”** - 此选项卡始终显示，提供了描述扫描进度的统计数据
- **“感染”** - 仅当扫描期间检测到 [病毒感染](#) 的情况下，此选项卡才会显示
- **“间谍软件”** - 仅当扫描期间检测到 [间谍软件](#) 的情况下，此选项卡才会显示
- **警告** - 例如，如果扫描过程中发现 cookie，则会显示此选项卡
- **“Rootkit”** - 仅当扫描期间检测到 [Rootkit](#) 的情况下，此选项卡才会显示
- **信息** - 仅当检测到某些潜在威胁但这些威胁不能划归为上述任何类别时，此选项卡才会显示；此时此选项卡会就检测结果提供一则警告消息。此外，此选项卡中也有关于无法对其进行扫描的对象（如受密码保护的存档）的信息。



11.7.1. ‘结果概览’选项卡



在 **‘扫描结果’** 选项卡中，您可以找到有关以下内容的详细统计信息：

- 检测到的 [病毒感染/间谍软件](#)
- 已删除的 [病毒感染/间谍软件](#)
- 无法删除或修复的 [病毒感染/间谍软件](#) 的数量

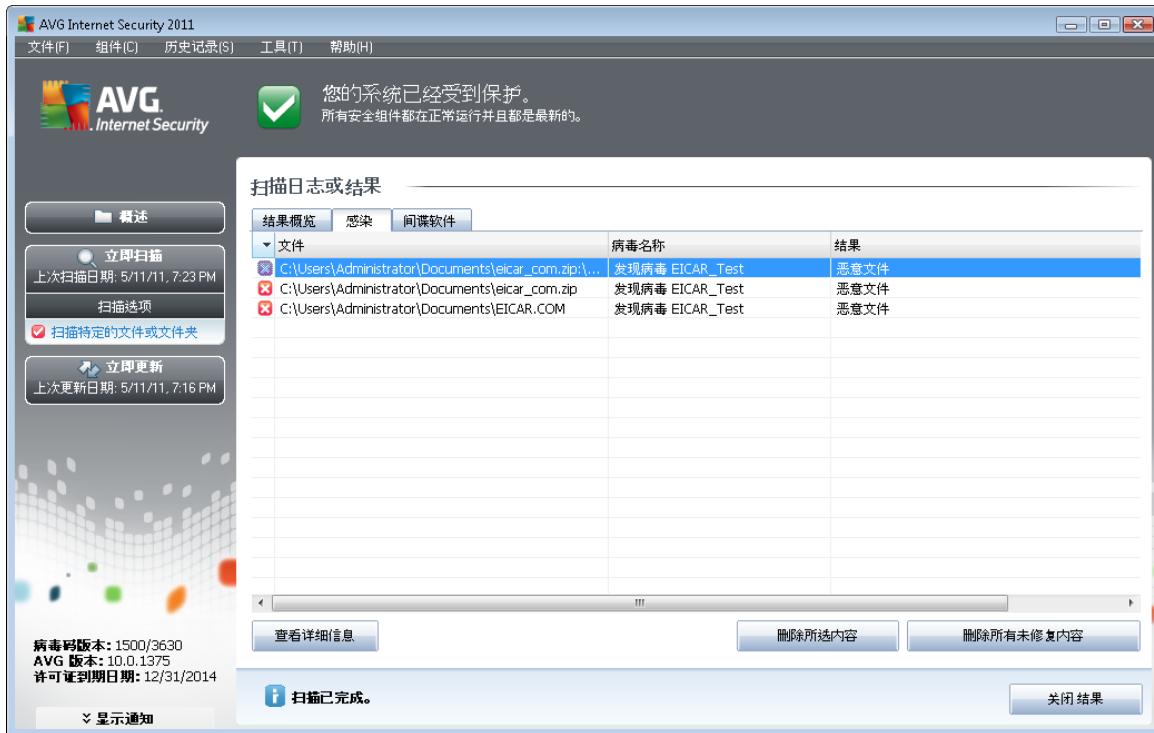
此外，您还将找到扫描启动的日期和确切时间、扫描的对象总数、扫描持续时间以及在扫描期间出现的错误数等信息。

控制按钮

此对话框中仅提供了一个控制按钮。按 **‘关闭结果’** 按钮可返回 [‘扫描结果概览’](#) 对话框。



11.7.2. ‘感染’选项卡



仅当在扫描期间检测到[病毒感染](#)时，‘扫描结果’对话框中才会显示‘感染’选项卡。此选项卡分为三个部分，分别提供下列信息：

- ‘文件’-受感染对象原始位置的完整路径
- ‘感染’-检测到的[病毒](#)的名称（有关特定病毒的详细信息，请参阅在线[病毒百科全书](#)）
- ‘结果’-定义在扫描期间检测到的受感染对象的当前状态：
 - ‘已感染’-已检测到受感染的对象并将其留在其原始位置（例如，如果您已在特定扫描设置中[关闭自动修复选项](#)）
 - ‘已修复’-已自动修复受感染的对象，并将其留在其原始位置
 - ‘已移至病毒库’-已将受感染的对象移至[病毒库](#)隔离区
 - ‘已删除’-已删除受感染的对象
 - ‘已添加至 PUP 特例’-已将发现结果评估为特例并已将其添加至 PUP 特例列表（在高级设置的‘[PUP 特例](#)’对话框中配置）中
 - ‘锁定的文件 -未测试’-相应对象已被锁定，因而 AVG 无法对它进行扫描
 - ‘有潜在危险的对象’-已检测到该对象有潜在危险，但未受感染（例如，

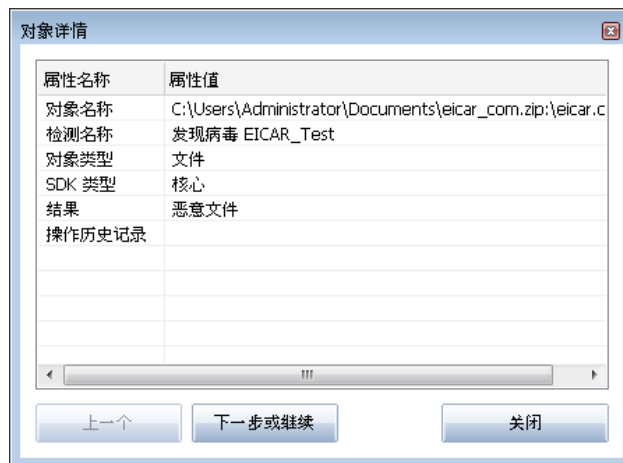
它可能包含宏)；此信息仅仅是一则警告

- o **“需要重新启动才能完成操作”**-无法删除受感染的对象，若要完全删除它，必须重新启动您的计算机

控制按钮

此对话框中有三个控制按钮：

- **“查看详细信息”**-此按钮用于打开一个名为 **“详细对象信息”** 的新对话框：

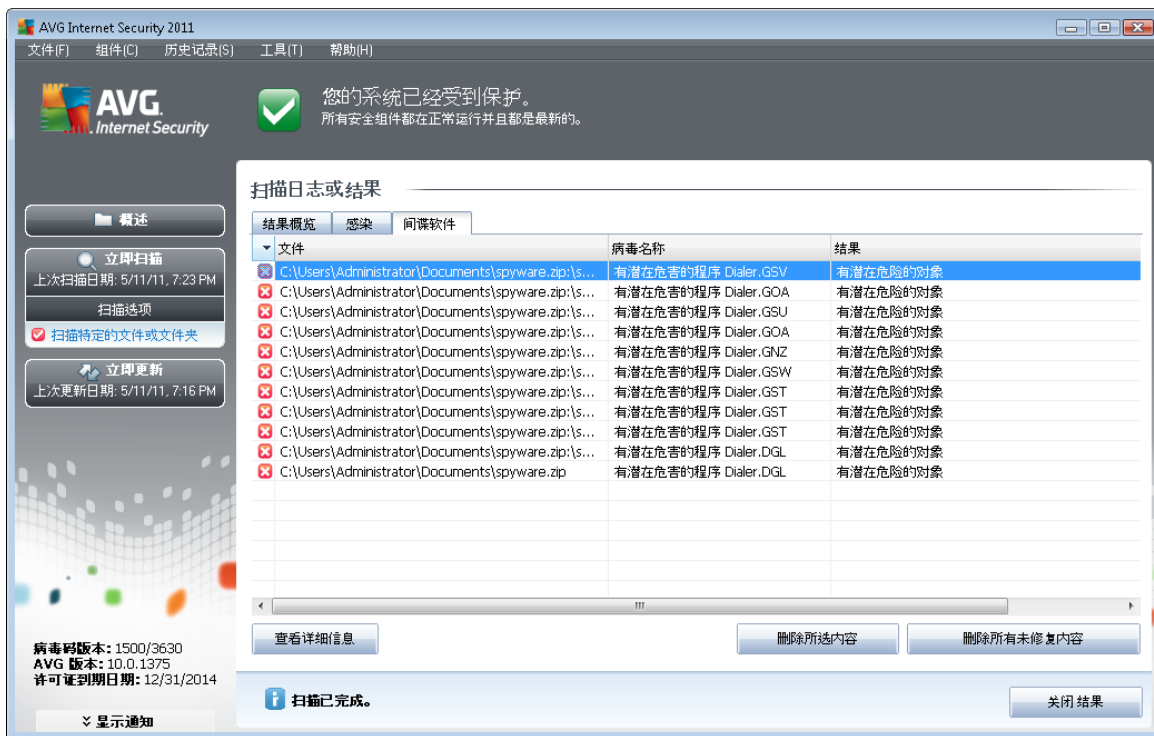


在此对话框中，可找到所检测到的受感染对象的详细信息（例如，受感染对象的名称和位置、对象类型、SDK 类型、检测结果以及与检测到的对象相关的操作历史记录）。用 **“上一个”** **“下一个”** 按钮可查看特定检测结果的相关信息。使用 **“关闭”** 按钮可关闭此对话框。

- **“删除选定的感染对象”** 使用此按钮可将选定的发现结果移至 [病毒库](#)
- **“删除所有未修复的感染对象”** 此按钮会删除无法修复的所有发现结果，或将其移至 [病毒库](#)
- **“关闭结果”**-终止详细信息概览并返回 [“扫描结果概览”](#) 对话框



11.7.3. ‘间谍软件’选项卡



仅当在扫描期间检测到[间谍软件](#)时，‘扫描结果’对话框中才会显示‘间谍软件’选项卡。此选项卡分为三个部分，分别提供下列信息：

- ‘文件’-受感染对象原始位置的完整路径
- ‘感染’-检测到的[间谍软件](#)的名称（有关特定病毒的详细信息，请参阅在线[病毒百科全书](#)）
- ‘结果’-定义在扫描期间检测到的对象的当前状态：
 - ‘已感染’-已检测到受感染的对象并将其留在其原始位置（例如，如果您已在特定扫描设置中[关闭自动修复选项](#)）
 - ‘已修复’-已自动修复受感染的对象，并将其留在其原始位置
 - ‘已移至病毒库’-已将受感染的对象移至[病毒库隔离区](#)
 - ‘已删除’-已删除受感染的对象
 - ‘已添加至 PUP 特例’-已将发现结果评估为特例并已将其添加至 PUP 特例列表（在高级设置的‘[PUP 特例](#)’对话框中配置）中
 - ‘锁定的文件 -未测试’-相应对象已被锁定，因而 AVG 无法对它进行扫描
 - ‘有潜在危险的对象’-已检测到该对象有潜在危险，但未受感染（例如，



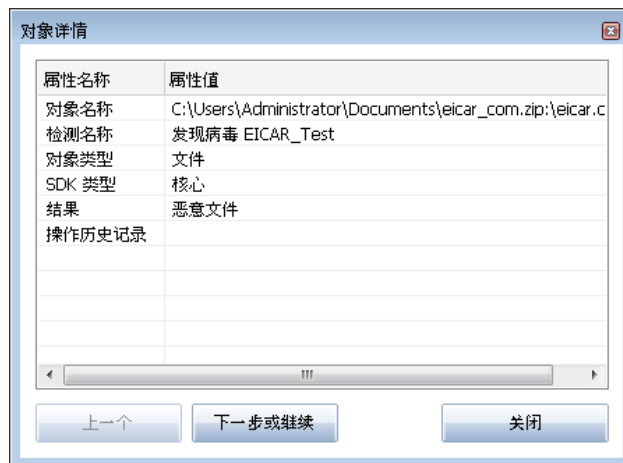
它可能包含宏）；此信息仅仅是一则警告

- o **“需要重新启动才能完成操作”**-无法删除受感染的对象，若要完全删除它，必须重新启动您的计算机

控制按钮

此对话框中有三个控制按钮：

- **“查看详细信息”**-此按钮用于打开一个名为 **“详细对象信息”** 的新对话框：



在此对话框中，可找到所检测到的受感染对象的详细信息（例如，受感染对象的名称和位置、对象类型、SDK 类型、检测结果以及与检测到的对象相关的操作历史记录）。用 **“上一个”** **“下一个”** 按钮可查看特定检测结果的相关信息。使用 **“关闭”** 按钮可离开此对话框。

- **“删除选定的感染对象”** 使用此按钮可将选定的发现结果移至 [病毒库](#)
- **“删除所有未修复的感染对象”** 此按钮会删除无法修复的所有发现结果，或将其移至 [病毒库](#)
- **“关闭结果”**-终止详细信息概览并返回 [“扫描结果概览”](#) 对话框

11.7.4. “警告”选项卡

“警告” 选项卡显示了在扫描期间检测到的可疑对象（通常是文件）的相关信息。[Resident Shield](#) 检测到这些文件时，会阻止对它们的访问。此类发现结果的典型例子有：隐藏的文件、Cookie、可疑的注册表项、受密码保护的文档或压缩包等。此类文件对您的计算机或安全不会构成任何直接威胁。如果在您的计算机上检测到了广告软件或间谍软件，则有关这些文件的信息通常会有用。如果 AVG 测试仅检测到严重程度为 **警告** 的内容，则不必采取任何操作。

下面简要说明了此类对象最常见的一些例子：

- **隐藏的文件** - 默认情况下隐藏的文件在 Windows 中是不可见的，因此有些病毒或



其它威胁可能会在存储自己的文件时为它们设置隐藏属性，以此方式企图逃避检测。如果您的 AVG 报告了一个隐藏的文件并且您怀疑它有恶意，则您可以将它移至 [AVG 病毒库](#)。

- **Cookie** - Cookie 是一些纯文本文件，网站使用它们来存储特定于用户的信息，之后会利用这些信息来加载具有定制特点的网站布局、预先填写用户名，等等。
- **可疑的注册表项** - 有些恶意软件会将其信息存储到 Windows 注册表中，以确保在启动时加载它，或扩大其在操作系统上的影响。

11.7.5. ‘Rootkit’选项卡

如果您启动了 [Anti-Rootkit 扫描](#)，“Rootkit”选项卡将显示扫描期间检测到的 Rootkit 信息。

Rootkit 是一种程序，旨在未经计算机系统所有者及合法管理员授权的情况下获得对计算机系统的基本控制。Rootkit 基本上不需要访问硬件，因为它的目的就是要控制硬件上运行的操作系统。通常情况下，Rootkit 通过破坏或避开标准操作系统安全机制来掩饰它们存在于系统中。它们往往又是特洛伊木马，因而会骗取用户的信任，使其认为在系统中运行它们是安全的。用来实现此目的的方法可能包括隐藏正在运行的进程以使监测程序无法发现它们，或者隐藏文件或系统数据以使操作系统无法发现它们。

此选项卡在结构上与 [‘感染’选项卡](#) 或 [‘间谍软件’选项卡](#) 基本相同。

11.7.6. ‘信息’选项卡

‘信息’ 选项卡包含有关那些不能被归为感染、间谍软件等类别的“发现结果”的数据。它们不能被肯定地标记为危险，但仍值得您注意。AVG 扫描功能可以检测到可能并未受感染但可疑的文件。会以 **‘警告’** 或 **‘信息’** 的形式报告这些文件。

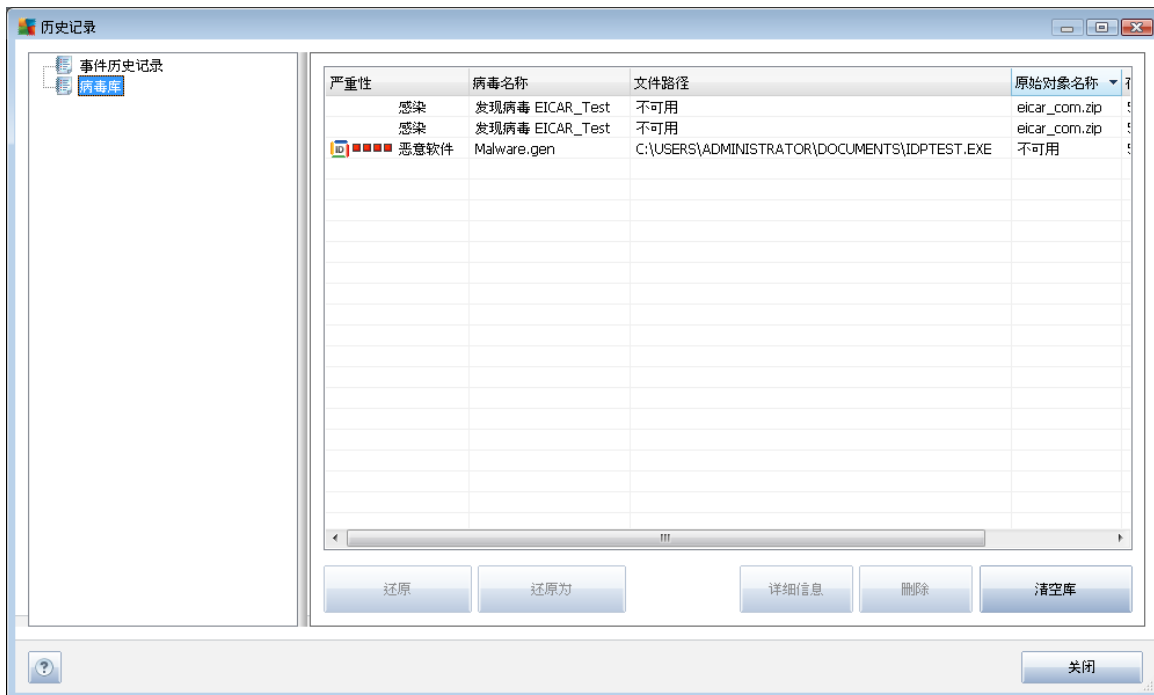
如果报告严重性为 **‘信息’** 的文件，则可能是由以下其中一个原因所致：

- **运行时间压缩** - 该文件是使用不太常见的某一运行时间压缩器 (Run-time Packer) 压缩的，这可能表示有防止扫描此类文件的企图。不过，并非每次报告此类文件时都表示存在病毒。
- **运行时间递归压缩** - 与上一项相似，不过在常用软件中不太常见。此类文件可疑，应考虑删除它们或提交它们以进行分析。
- **受密码保护的压缩包或文档** - AVG 无法扫描受密码保护的文件（一般而言，任何其它防恶意软件程序也都无法扫描）。
- **包含宏的文档** - 所报告的文档包含可能有恶意的宏。
- **隐藏的扩展名** - 隐藏了扩展名的文件可能似乎是图片等内容，但事实上它们是可执行文件（如 *picture.jpg.exe*）。默认情况下第二个扩展名在 Windows 中不可见，AVG 会将此类文件报告出来以防止无意中打开它们。
- **文件路径不正确** - 如果某一重要的系统文件是从非默认路径运行的（例如 *winlogon.exe* 从 Windows 文件夹以外的位置运行），AVG 会将这种不一致情况报告出来。有些情况下，病毒会使用标准系统进程的名称以使自己在系统中不太显眼。



- **锁定的文件** - 所报告的文件已被锁定，因而 AVG 无法对它进行扫描。这通常意味着某一文件正在不断地被系统使用（例如交换文件）。

11.8. 病毒库



病毒库是一种安全环境，用于管理在 AVG 测试期间检测到的可疑/受感染对象。一旦在扫描期间检测到受感染的对象并且 AVG 无法自动修复它，系统就会要求您决定要如何处理此可疑对象。建议的解决方法是将此对象移至**病毒库**以待进一步处理。**病毒库**的主要用途是将已删除的文件保留一段时间，以便您能确定不再需要将已删除的文件保留在其原始位置。如果发现该文件缺失会引起问题，则可发送受感染文件进行分析，或将其还原至原始位置。

病毒库界面在一个单独的窗口中打开，概述了有关被隔离的受感染对象的信息：

- **“严重程度”** 如果决定安装 **AVG Internet Security 2011** 中的 **Identity Protection** 组件，则会在此部分中以图形方式显示所发现的各个受感染对象的严重程度，共分四级，从无可非议 (□□□□) 到非常危险 (■ ■ ■ ■)；还会显示有关感染类型的信息（根据其感染程度分类，所有列出的对象要么肯定受到感染，要么可能受到感染）
- **“病毒名称”** 依据 **病毒百科全书**（在线）指定检测到的感染的名称
- **文件路径** - 所检测到的受感染文件的原始位置的完整路径
- **原始对象名称** - 此图表中列出的所有检测到的对象均已使用在扫描过程中由 AVG 提供的标准名称作为标签。如果相应对象具有已知的特定原始名称（例如，与电子邮件附件的实际内容不符的附件名称），则会在此列中提供此名称。
- **存储日期** - 检测到可疑文件并将其移至**病毒库**

控制按钮

可从**病毒库**界面中访问以下控制按钮：

- **还原** - 将受感染的文件移回其在磁盘上的原始位置
- **还原为** - 用于将受感染的文件移至选定的文件夹
- **详细信息** - 此按钮仅适用于 **Identity Protection** 检测到的威胁。单击该按钮可大概了解威胁详细信息（受感染的文件/进程、进程的特性等信息）。请注意，对于除 IDP 检测到的所有其它威胁，都会灰显并停用此按钮！



- **删除** - 将受感染的文件从**病毒库**中彻底移除
- **清空库** - 彻底删除**病毒库**中的所有内容。通过从**病毒库**中删除文件，将会以不可还原的方式从磁盘中删除这些文件（不是移动到回收站）。



12. AVG 更新

让您的 AVG 保持最新对于确保尽快检测到所有新发现的病毒至关重要。

由于 AVG 更新并非依据任何固定的时间安排进行发布，而是要视新威胁的数量和严重程度而定，因此建议至少每天检查一次或更频繁地检查是否有新的更新。只有这样，您才能确保 AVG Internet Security 2011 在日间也会保持最新。

12.1. 更新级别

AVG 提供了两种更新级别供选用：

- **‘定义更新’** 包含实现可靠的防病毒保护所需的更改。通常情况下，它不包含任何代码更改，仅更新定义数据库。此更新一旦可用，应立即加以应用。
- **‘程序更新’** 包含各种程序更改、修复及改进。

在 [计划更新](#) 时，可以选择应下载并应用哪种优先级别。

注：如果计划程序更新和计划扫描同时执行，则更新进程优先，扫描会中断。

12.2. 更新类型

您可以将以下两种类型的更新区分开来：

- **‘按需更新’** 是可随时在需要时立即执行的一种 AVG 更新。
- **计划的更新** - 在 AVG 中，还可以 [预设更新计划](#)。这样，计划的更新就会按照所设定的配置定期执行。只要在指定的位置存在新的更新文件，它们就会被直接从 Internet 上下载，或从网络目录中下载。当没有较新的更新可用时，不会执行任何操作。

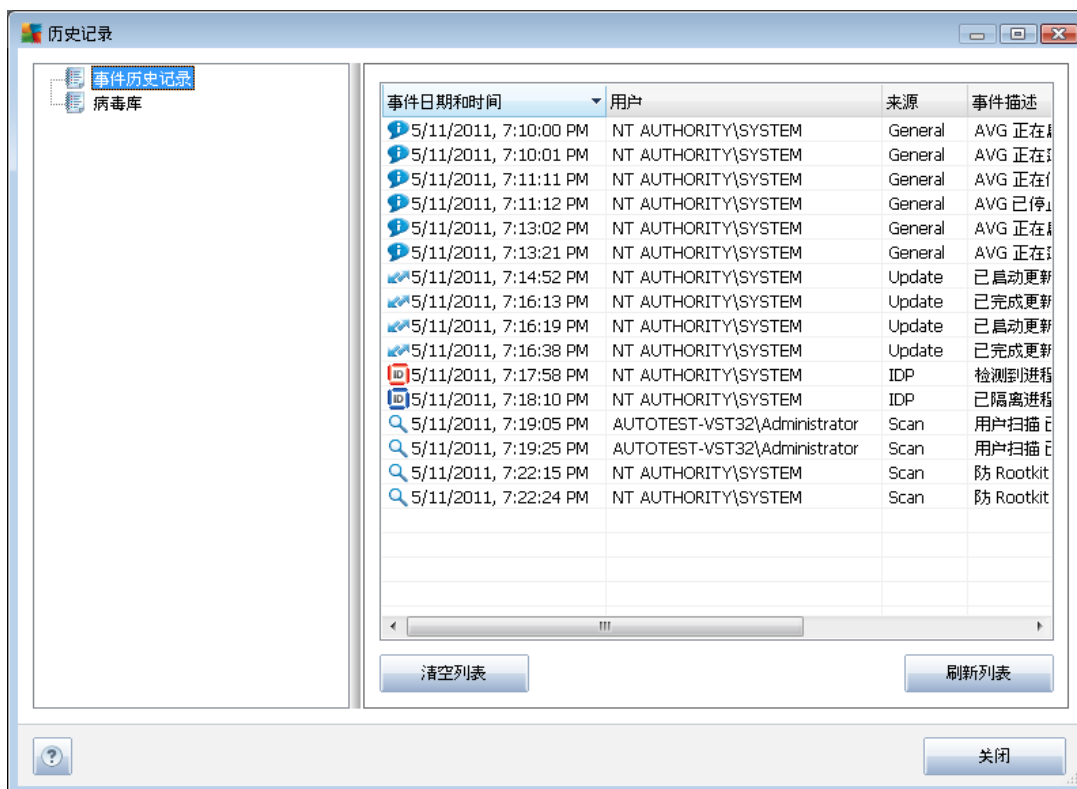
12.3. 更新过程

在需要更新时，可以通过 **‘立即更新’** [快速链接](#) 立即启动更新过程。所有 [AVG 用户界面](#) 对话框中都始终提供此链接。不过，仍强烈建议按照更新计划中的规定定期执行更新，更新计划可在 [更新管理器](#) 组件中进行编辑。

启动更新后，AVG 首先会核实是否有新的更新文件可用。如果有，AVG 会开始下载这些文件，然后自行启动更新过程。在更新过程中，系统会将您重定向到 **‘更新’** 界面，从中可查看以图形方式表示的更新过程进度，以及相关统计参数概览（更新文件的大小、接收到的数据、下载速度、经过的时间等）。

注：在 AVG 程序更新启动前，会创建一个系统还原点。万一更新过程失败并且您的操作系统崩溃，那么您始终都可以利用此还原点将您的操作系统还原成其原始配置。可通过 **开始 / 所有程序 / 附件 / 系统工具 / 系统还原** 显示此选项。仅建议有经验的用户使用！

13. 事件历史记录



“历史记录”对话框可从[系统菜单](#)中通过“历史记录”/“事件历史记录日志”项进行访问。此对话框中有 AVG Internet Security 2011 运行期间发生的重大事件的摘要。“历史记录”可记录以下类型的事件：

- 有关 AVG 应用程序更新的信息
- 扫描开始、结束或停止（包括自动执行的测试）
- 与病毒检测有关的事件（通过 [Resident Shield](#) 或 [扫描](#) 进行检测），包括发生位置
- 其它重要事件

对于每个事件，将列出以下信息：

- “事件日期和时间”提供事件发生的确切日期和时间
- “用户”指示启动事件的用户
- “来源”提供触发事件的源组件或 AVG 系统的其它部分
- “事件说明”提供实际情况的简短摘要



控制按钮

- **“清空列表”** - 删除事件列表中的所有条目
- **“刷新列表”** - 更新事件列表中的所有条目



14. 常见问题解答和技术支持

如果遇到有关 AVG 的问题，不论是商业方面还是技术方面的问题，都请参阅 AVG 网站 (<http://www.avg.com/>) 中的 **‘常见问题解答’** 部分。

如果按此方法无法找到帮助，请通过电子邮件与技术支持部门联系。请使用可在系统菜单中通过 **‘帮助’** **‘获取在线帮助’** 显示出来的联系信息表格。