AVG Internet Security 2012

用户手册

文档修订 2012.20 (3/29/2012)

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 7

2. AVG 安装要求 8

2.1 支持的操作系统 8
2.2 最低和推荐硬件要求 8

3. AVG 安装过程 9

3.1 欢迎使用：语言选择 9
3.2 欢迎使用：许可协议 10
3.3 激活您的许可证 11
3.4 选择安装类型 12
3.5 自定义选项 13
3.6 安装 AVG Security Toolbar 14
3.7 安装进度 15
3.8 安装已成功 16

4. 安装后 17

4.1 产品注册 17
4.2 访问用户界面 17
4.3 扫描整个计算机 17
4.4 Eicar 测试 17
4.5 AVG 默认配置 18

5. AVG 用户界面 19

5.1 系统菜单 20
5.1.1 文件 20
5.1.2 组件 20
5.1.3 历史记录 20
5.1.4 工具 20
5.1.5 帮助 20
5.1.6 支持 20
5.2 安全状态信息 27
5.3 快速链接 27
5.4 组件概览 28
5.5 系统任务栏图标 29
5.6 AVG Advisor 31
5.7 AVG 小工具 32

 2012 版权所有 AVG Technologies CZ, s.r.o. 保留所有权利。

6. AVG 组件 34

6.1 Anti-Virus 34
6.1.1 扫描引擎 34
6.1.2 常驻保护措施 34
6.1.3 Anti-Spyware 防护措施 34
6.1.4 Anti-Virus 界面 34
6.1.5 Resident Shield 检测结果 34
6.2 LinkScanner 39
6.2.1 LinkScanner 界面 39
6.2.2 Search-Shield 检测结果 39
6.2.3 Surf-Shield 检测结果 39
6.2.4 Online Shield 检测结果 39
6.3 电子邮件保护 45
6.3.1 E-mail Scanner 45
6.3.2 Anti-Spam 45
6.3.3 电子邮件保护界面 45
6.3.4 E-mail Scanner 检测结果 45
6.4 Firewall 48
6.4.1 Firewall 原理 48
6.4.2 Firewall 配置文件 48
6.4.3 Firewall 界面 48
6.5 Anti-Rootkit 51
6.5.1 Anti-Rootkit 界面 51
6.6 系统工具 53
6.6.1 进程 53
6.6.2 网络连接 53
6.6.3 自动启动 53
6.6.4 浏览器扩展 53
6.6.5 LSP 查看器 53
6.7 PC Analyzer 58
6.8 Identity Protection 60
6.8.1 Identity Protection 界面 60
6.9 Remote Administration 62

7. 我的应用程序 63

7.1 AVG Family Safety 63
7.2 AVG LiveKive 64
7.3 AVG Mobilation 64

 2012 版权所有 AVG Technologies CZ, s.r.o. 保留所有权利。

7.4 AVG PC Tuneup 65

8. AVG Security Toolbar 66

9. AVG Do Not Track 68

9.1 AVG Do Not Track 界面 68
9.2 有关跟踪进程的信息 69
9.3 阻止跟踪进程 70
9.4 AVG Do Not Track 设置 71

10. AVG 高级设置 74

10.1 外观 74
10.2 声音 77
10.3 暂时禁用 AVG 保护 78
10.4 Anti-Virus 79
10.4.1 Resident Shield 79
10.4.2 缓存服务器 79
10.5 电子邮件保护 84
10.5.1 电子邮件扫描程序 84
10.5.2 Anti-Spam 84
10.6 LinkScanner 100
10.6.1 LinkScanner 设置 100
10.6.2 Online Shield 100
10.7 扫描 104
10.7.1 扫描整个计算机 104
10.7.2 外壳扩展扫描 104
10.7.3 扫描特定的文件或文件夹 104
10.7.4 可移动设备扫描 104
10.8 计划 109
10.8.1 计划的扫描 109
10.8.2 指定更新计划 109
10.8.3 程序更新计划 109
10.8.4 Anti-Spam 更新计划 109
10.9 更新 118
10.9.1 代理 118
10.9.2 拨号 118
10.9.3 URL 118
10.9.4 管理 118
10.10 Anti-Rootkit 124

 2012 版权所有 AVG Technologies CZ, s.r.o. 保留所有权利。

10.10.1 特例 *124*
10.11 Identity Protection 125
10.11.1 Identity Protection 设置 *125*
10.11.2 “已允许”列表 *125*
10.12 可能不需要的程序 128
10.13 病毒库 131
10.14 产品改进计划 131
10.15 忽略错误状态 134
10.16 Advisor - 已知网络 135

11. Firewall 设置 **136**

11.1 常规 136
11.2 安全 137
11.3 区域和适配器配置文件 138
11.4 IDS 139
11.5 日志 141
11.6 配置文件 142
11.6.1 配置文件信息 *142*
11.6.2 预定义网络 *142*
11.6.3 应用程序 *142*
11.6.4 系统服务 *142*

12. AVG 扫描 **152**

12.1 扫描界面 152
12.2 预定义扫描 153
12.2.1 扫描整个计算机 *153*
12.2.2 扫描特定的文件或文件夹 *153*
12.3 扫描 Windows 资源管理器 160
12.4 命令行扫描 161
12.4.1 CMD 扫描参数 *161*
12.5 扫描计划 163
12.5.1 计划设置 *163*
12.5.2 扫描方式 *163*
12.5.3 扫描内容 *163*
12.6 扫描结果概览 172
12.7 扫描结果详细信息 173
12.7.1 “结果概览”选项卡 *173*
12.7.2 “感染”选项卡 *173*
12.7.3 “间谍软件”选项卡 *173*

 2012 版权所有 AVG Technologies CZ, s.r.o. 保留所有权利。

12.7.4 “警告”选项卡 *173*
12.7.5 “Rootkit”选项卡 *173*
12.7.6 “信息”选项卡 *173*
12.8 病毒库 180

13. AVG 更新 **182**

13.1 更新启动 182
13.2 更新进度 182
13.3 更新级别 183

14. 事件历史记录 **184**

15. 常见问题解答和技术支持 **186**

 2012 版权所有 AVG Technologies CZ, s.r.o. 保留所有权利。

1. 简介

本用户手册提供全面的 **AVG Internet Security 2012** 文档。

对于在网上的一举一动，AVG Internet Security 2012 可以提供多重保护，这意味着不必担心身份被盗、病毒或访问有害网站。其中包括 AVG 云保护技术和 AVG Community Protection Network，这意味着我们收集最新威胁信息并将其透露给我们的社区，以确保用户得到最严密的保护：

- 通过 AVG Firewall、AVG Anti-Spam 和 AVG Identity Protection，安全地在线购物和办理银行事务
- 通过 VG Social Networking Protection 在社交网络中一直平安无事
- 通过 LinkScanner 的实时保护功能放心地上网和搜索

 2012 版权所有 AVG Technologies CZ, s.r.o. 保留所有权利。

2. AVG 安装要求

2.1. 支持的操作系统

AVG Internet Security 2012 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 2012。*

2.2. 最低和推荐硬件要求

对 **AVG Internet Security 2012** 的最低硬件要求：

- Intel Pentium CPU 1,5 GHz
- 512 MB RAM 内存
- 1000 MB 可用硬盘空间（用于安装）

对 **AVG Internet Security 2012** 的推荐硬件要求：

- Intel Pentium CPU 1,8 GHz
- 512 MB RAM 内存
- 1550 MB 可用硬盘空间（用于安装）

 2012 版权所有 AVG Technologies CZ, s.r.o. 保留所有权利。

3. AVG 安装过程

何处可以获得安装文件？

要将 **AVG Internet Security 2012** 安装到计算机中，需要获得最新的安装文件。为了确保要安装的是最新版 **AVG Internet Security 2012**，建议从 AVG 网站 (http://www.avg.com/) 下载安装文件。通过***支持中心/下载*** 部分可分类综览各个 AVG 版本的安装文件。

如果无法确定需要下载并安装哪些文件，则可能需要使用该网页底部的***选择产品*** 服务。答完三个简单问题后，这种服务就会指定所需的确切文件。按***继续*** 按钮可重定向到按用户个人需要自定义的下载文件全表。

安装过程看起来如何？

将安装文件下载并保存到您的硬盘上之后，您就可以启动安装过程。安装过程中会显示一系列简单易懂的对话框。每个对话框都会简短说明执行安装过程的每个步骤时所要执行的操作。下面，我们会详细说明各个对话窗口：

3.1. 欢迎使用：语言选择

安装过程开始时会显示***欢迎使用 AVG 安装程序*** 对话框：

可在此对话框中选择要在安装过程中使用的语言。在该对话框的右上角中，单击其中的组合框以下拉语言菜单。选择所需语言，然后就会以所选语言继续执行安装过程。

注意：目前选择的只是用于安装过程的语言。会以所选语言和英语（始终都会自动安装）安装 AVG Internet Security 2012 应用程序。但也能安装更多语言，并以其中的任何一种语言使用 AVG Internet Security 2012。会在以下某个名为自定义选项的安装对话框中，请用户确认全部所选备选语言。

 2012 版权所有 AVG Technologies CZ, s.r.o. 保留所有权利。

3.2. 欢迎使用：许可协议

接下来，***欢迎使用 AVG 安装程序***对话框会提供 AVG 许可协议全文：

请仔细阅读全文。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。

AVG 隐私政策

除了许可协议，此安装对话框中还有用于详细了解 AVG 隐私政策的选项。可在该对话框的左下角中看到 ***AVG 隐私政策*** 链接。单击该链接即可重定向到 AVG 网站 (http://www.avg.com/)，其中有 AVG Technologies 隐私政策原则全文。

控制按钮

第一个安装对话框中只有两个控制按钮：

- ***可打印版本*** - 单击可打印 AVG 许可协议的全文。
- ***拒绝*** - 单击可拒绝接受许可协议。会立即退出安装过程。不会安装 **AVG Internet Security 2012**！
- ***上一步*** - 单击可后退一步，返回到上一安装对话框。
- ***接受*** - 单击可确认已阅读、理解并接受许可协议。会继续安装，还会前进一步，显示以下安装对话框。

 2012 版权所有 AVG Technologies CZ, s.r.o. 保留所有权利。

3.3. 激活您的许可证

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：

许可证号码位于何处？

销售号码可在 **AVG Internet Security 2012** 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 2012** 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。

如何使用复制粘贴法

通过 ***复制粘贴法*** 将 **AVG Internet Security 2012** 许可证号码输入程序，可确保输入的许可证号码正确无误。请按以下步骤操作：

- 打开包含许可证号码的电子邮件。
- 在许可证号码开头单击鼠标左键，按住并将鼠标光标拖到许可证号码末尾，然后松开鼠标左键。许可证号码现在应该已突出显示出来。
- 按住 ***Ctrl***，然后按 ***C***。这样会复制许可证号码。
- 指向并单击要从中粘贴已复制的许可证号码的位置。
- 按住 ***Ctrl***，然后按 ***V***。这样会将许可证号码粘贴到所选位置。

控制按钮

 2012 版权所有 AVG Technologies CZ, s.r.o. 保留所有权利。

如同在大多安装对话框中，其中也有三个控制按钮可用：

- ***取消*** - 单击可立即退出安装进程；不会安装 **AVG Internet Security 2012**！
- ***上一步*** - 单击可后退一步，返回到上一级安装对话框。
- ***下一步*** - 单击可继续安装，前往下一步。

3.4. 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***：

快速安装

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 Internet Security 2012** 包括 AVG 小工具）。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，您始终可以直接在 **AVG Internet Security 2012** 应用程序中完成。

在该选项中，您可以看到两个已预先被确认的复选框，系统强烈建议您选中两个选项：

- ***我想要将 AVG Secure Search 作为我的默认搜索提供程序*** - 选中该项可确认，您要使用与 Link Scanner 组件密切协作运行的 AVG Secure Search 引擎，以便在上网时获得最大安全性的保护。
- ***我想要安装 AVG Security Toolbar*** - 选中该项以安装用于在您上网时保护您最大安全性的 AVG Security Toolbar。

请按***下一步***按钮可进入接下来的安装 AVG Security Toolbar 对话框。

 2012 版权所有 AVG Technologies CZ, s.r.o. 保留所有权利。

自定义安装

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 Internet Security 2012** 时使用 ;如，为满足特定的系统要求。

如果您选择该选项，则名为***目标文件夹***的选项将会在该对话框中显示。此时，您应该指定要安装 **AVG Internet Security 2012** 的位置。默认情况下，按照该对话框中的文本所述，**AVG Internet Security 2012** 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。要恢复软件供应商预设的默认目标，请使用***默认***按钮。

然后，请按***下一步***按钮可进入自定义选项对话框。

控制按钮

如同在大多安装对话框中，其中也有三个控制按钮可用：

- ***取消*** - 单击可立即退出安装进程 ;不会安装 **AVG Internet Security 2012** !
- ***上一步*** - 单击可后退一步，返回到上一级安装对话框。
- ***下一步*** - 单击可继续安装，前往下一步。

3.5. 自定义选项

自定义选项对话框让您设置安装的详细参数：

组件选择部分提供所有可安装的 **AVG Internet Security 2012** 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。

 2012 版权所有 AVG Technologies CZ, s.r.o. 保留所有权利。

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。要恢复软件供应商预设的默认配置，请使用 ***默认*** 按钮。

控制按钮

如同在大多安装对话框中，其中也有三个控制按钮可用：

- ***取消*** - 单击可立即退出安装进程；不会安装 **AVG Internet Security 2012**！
- ***上一步*** - 单击可后退一步，返回到上一级安装对话框。
- ***下一步*** - 单击可继续安装，前往下一步。

3.6. 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 *(当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 和更高版本)* 中，以便在上网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。

控制按钮

如同在大多安装对话框中，其中也有三个控制按钮可用：

 2012 版权所有 AVG Technologies CZ, s.r.o. 保留所有权利。

- ***取消*** - 单击可立即退出安装进程；不会安装 **AVG Internet Security 2012**！
- ***上一步*** - 单击可后退一步，返回到上一级安装对话框。
- ***下一步*** - 单击可继续安装，前往下一步。

3.7. 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：

安装过程结束后会自动重定向到下一对话框。

控制按钮

此对话框中只有一个控制按钮，即***取消***。仅当想要停止安装进程的运行时，才应该使用此按钮。请注意，这种情况下不会安装 **AVG Internet Security 2012**！

2012 版权所有 AVG Technologies CZ, s.r.o. 保留所有权利。

3.8. 安装已成功

安装已成功 对话框用于确认 **AVG Internet Security 2012** 已经安装完毕并配置好：

产品改进计划

可在此处决定是否要参加产品改进计划 *(有关详细信息，请参见 AVG 高级设置/产品改进计划*一章)，该计划用于收集有关检测到威胁的匿名信息，以便提高 Internet 的整体安全程度。如果同意此声明，请保持***我同意参加 AVG 2012 Web 安全和产品改进计划...*** 选项的选中状态 *(默认情况下已确认该选项)*。

计算机的重新启动

要结束安装过程，需要重新启动计算机：选择是要***立即重新启动***，还是要推迟此操作，也就是***稍后重新启动***。

 2012 版权所有 AVG Technologies CZ, s.r.o. 保留所有权利。

4. 安装后

4.1. 产品注册

安装完 **AVG Internet Security 2012** 后，请在 AVG 网站 (http://www.avg.com/) 中在线注册您的产品。注册之后，您就可以得到 AVG 用户帐户最高访问权、查看所有 AVG 更新新闻稿，还可以享受专为注册用户提供的其它服务。

最简单的注册方法是直接在 **AVG Internet Security 2012** 用户界面中注册。请在主菜单中选择帮助/立即注册选项。会重定向到 AVG 网站 (http://www.avg.com/) 中的***注册*** 页面。请按该页面中的说明操作。

4.2. 访问用户界面

AVG 主对话框可通过以下几种方式显示：

- 双击 AVG 系统任务栏图标
- 双击桌面上的 AVG 图标
- 通过以下菜单：***开始/所有程序/AVG 2012***

4.3. 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 2012** 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。第一次扫描可能需要相当长的时间 *(大约一小时)*，但建议您启动第一次扫描，以确保您的计算机未受威胁而导致性能损耗。有关运行扫描整个计算机的说明，请参阅 AVG 扫描一章。

4.4. Eicar 测试

要确保 **AVG Internet Security 2012** 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 (*LinkScanner 组件的一部分*) 会立即进行警告以作出反应。这则通知表明 AVG 已在计算机中安装妥当。

 2012 版权所有 AVG Technologies CZ, s.r.o. 保留所有权利。

也可从网站 http://www.eicar.com 中下载压缩版 EICAR 病毒 "*例如，以 eicar_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(*在 Anti-Virus 组件内*)就会检测到该 病毒 "。

如果 AVG 未能将 EICAR 测试文件认定为病毒，则应该重新检查程序配置！

4.5. AVG 默认配置

AVG Internet Security 2012 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。

 2012 版权所有 AVG Technologies CZ, s.r.o. 保留所有权利。

5. AVG 用户界面

AVG Internet Security 2012 打开时会显示主窗口：

该主窗口分为若干区域：

- ***使用系统菜单*** *(窗口顶部的系统行)*是标准操作方式，通过系统菜单可使用所有 **AVG Internet Security 2012** 组件、服务和特性 - 详细信息 >>
- ***安全状态信息*** *(窗口顶部)*中有关于 **AVG Internet Security 2012** 当前状态的信息 - 详细信息 >>
- ***在脸谱 (Facebook) 上加入我们*** *(窗口右上区域)*按钮可让您加入到 Facebook 上的 AVG 社区。但是，该按钮仅在所有组件完全正常工作时才显示 *(有关如何识别 AVG 组件状态的详细信息，请参见安全状态信息)*
- ***快速链接*** *(窗口左侧)*用于快速执行最重要和最常用的 **AVG Internet Security 2012** 任务 - 详细信息 >>
- ***My Apps*** *(窗口左下部)*用于概览 **AVG Internet Security 2012** 的衍生应用程序：LiveKive、Family Safety 和 PC Tuneup
- ***组件概览*** *(窗口中部)*可用于概览已安装在 **AVG Internet Security 2012 中的所有组件** - 详细信息 >>
- ***系统任务栏图标*** *(在显示器右下角的系统任务栏中)*用于显示 **AVG Internet Security 2012 的当前状态** - 详细信息 >>
- ***AVG 小工具*** *(在 Windows 边栏中，在 Windows Vista/7 中受支持)*可用于在 **AVG**

2012 版权所有 AVG Technologies CZ, s.r.o. 保留所有权利。

Internet Security 2012 中快速执行扫描和更新 - 详细信息 >>

5.1. 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 2012** 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：

5.1.1. 文件

- ***"退出"***–关闭 **AVG Internet Security 2012** 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！

5.1.2. 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*** 用于检测系统中的病毒、间谍软件、蠕虫、特洛伊木马、不需要的可执行文件或库，也可以防止受到恶意广告软件的侵害 - 详细信息 >>
- ***LinkScanner*** 用于在 Internet 上搜索和上网时防止受到基于 Web 的攻击 - 详细信息 >>
- ***电子邮件保护*** 用于检查传入的电子邮件中的垃圾邮件，以及阻止病毒、仿冒攻击或其它威胁 - 详细信息 >>
- ***Firewall*** 用于控制通过每个网络端口传输的所有通讯内容，从而防止受到恶意攻击，并阻止所有入侵企图 - 详细信息 >>
- ***Anti-Rootkit*** 用于扫描隐藏在应用程序、驱动程序或库内的危险 Rootkit - 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*** 用于持续防止用户的数字财产遭到新威胁和不明威胁的破坏 - 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

5.1.3. 历史记录

- 扫描结果 - 用于切换到 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，从中可综览 Resident Shield

 2012 版权所有 AVG Technologies CZ, s.r.o. 保留所有权利。

- E-mail Scanner 检测结果 - 用于打开一个对话框，从中可综览电子邮件保护组件检测后断定有危险的邮件附件

- Online Shield 检测结果 - 用于打开一个对话框，从中可综览 LinkScanner 组件中 Online Shield 服务检测到的威胁

- 病毒库 - 用于打开隔离区（病毒库）的界面，AVG 会将已检测到但出于某种原因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 2012** 操作的概况

- Firewall 日志 - 用于打开 Firewall 设置界面中的日志选项卡，其中包含全部 Firewall 操作的详细概况

5.1.4. 工具

- 扫描计算机 - 启动扫描整个计算机。

- 扫描所选文件夹... - 可切换到 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...*** - 可以按需对单个文件执行测试。单击此选项可打开带有硬盘树结构的新窗口。选择所需的文件，然后确认启动扫描。

- 更新 - 自动启动 **AVG Internet Security 2012** 的更新过程。

- ***从目录更新...*** - 从位于您本地硬盘上指定的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诸如不存在 Internet 连接的紧急情况 *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... - 用于打开 AVG 高级设置对话框，您可以在此对话框中对 AVG Internet Security 2012 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... - 用于打开一个独立的对话框，以便对 Firewall 组件进行高级配置。

5.1.5. 帮助

- ***目录*** - 打开 AVG 帮助文件

- ***获取帮助*** - 用于打开 AVG 网站 (http://www.avg.com/)中的客户支持中心页面

- ***您的 AVG Web*** - 用于打开 AVG 网站 (http://www.avg.com/)

- ***关于病毒和威胁*** - 用于打开在线病毒百科全书，从中可查找关于已识别出的病毒的详细信息

- ***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

 2012 版权所有 AVG Technologies CZ, s.r.o. 保留所有权利。

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*），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；只有已注册各自 AVG 产品的客户才能享受免费技术支持。

注：*如果使用的是试用版* **AVG Internet Security 2012**，*则后两个选项会显示为****立即购买****和****激活****，以便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 2012**，*这两个选项显示为****注册****和****激活****。*

- ***关于 AVG*** - 用于打开***信息***对话框，该对话框包含六个选项卡，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。

5.1.6. 支持

通过***支持***链接可打开一个新***信息***对话框，其中有尝试寻求帮助时可能需要了解的各类信息。该对话框中有关于所安装的 AVG 程序的基本资料（*程序/数据库版本*）、许可证详细信息，以及快速支持链接列表：

信息对话框分为六个选项卡：

版本对话框分为三个区域：

- ***支持信息*** - 其中有关于 **AVG Internet Security 2012** 版本、病毒数据库版本、Anti-Spam 数据库版本和 LinkScanner 版本的信息。

 2012 版权所有 AVG Technologies CZ, s.r.o. 保留所有权利。

- ***用户信息*** - 其中有关于已得到授权的用户和公司的信息。
- ***许可证详细信息*** - 其中有关于许可证的信息 *(产品名称、许可证类型、许可证号码、到期日期、席位数)*。也可在此部分中用***注册*** 链接在线注册 **AVG Internet Security 2012** ;这样就可以享受所有 AVG 技术支持。此外，还可用***重新激活*** 链接打开***激活 AVG*** 对话框 :可将许可证号码填入相应字段，以替代销售号码 *(已在安装 AVG Internet Security 2012 的过程中用过的销售号码)*，也可将正在使用的许可证号码替换为另一个许可证号码 *(例如，向版本较高的 AVG 产品升级)*。

在***程序*** 选项卡中，可找到有关 **AVG Internet Security 2012** 程序文件版本的信息，以及有关用在该产品中的第三方代码的信息：

系统 *选项卡中列有操作系统参数（处理器类型，操作系统及其版本，内部版本号，已应用的 Service Pack，内存总量，以及可用内存量）：*

 2012 版权所有 AVG Technologies CZ, s.r.o. 保留所有权利。

在 ***许可协议*** 选项卡中，可阅读用户与 AVG Technologies 之间的许可协议全文：

支持 选项卡中列有客户支持部门的所有联系方式。此外，其中还有指向 AVG 网站 (http://www.avg.com/)、AVG 论坛、常见问题解答……的链接，还可找到可能会在联系客户支持团队时用到的信息：

2012 版权所有 AVG Technologies CZ, s.r.o. 保留所有权利。

联系人 选项卡中列有全部 AVG Technologies 联系人，还有 AVG 本地代表和经销商的联系人：

5.2. 安全状态信息

安全状态信息 区域位于 **AVG Internet Security 2012** 主窗口的上部。在此区域中，始终可以找到 **AVG Internet Security 2012** 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：

- 此绿色图标表示 ***AVG Internet Security 2012 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。

- 黄色图标警告***一个或多个组件配置不当，***您应对其属性/设置加以注意。**AVG Internet Security 2012** 中未出现严重问题，您可能出于某种原因已决定将某个组件关闭。用户仍处于受保护状态！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。

如果出于某种原因决定忽略组件的错误状态，也会显示黄色图标。***忽略组件状态*** 选项能通过 **AVG Internet Security 2012** 主窗口的组件概览中相应组件图标上的上下文菜单 *(通过单击鼠标右键打开)* 显示出来。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 Internet Security 2012** 的这种状态，而且不想通过系统任务栏图标收到警告。在特定情况下您可能需要使用此选项，但极力建议您尽快禁用***忽略组件状态*** 选项。

此外，如果您的 **AVG Internet Security 2012** 需要重新启动计算机 ***(需要重新启动)***，也会显示黄色图标。请注意该警告，并使用***立即重新启动***按钮重新启动 PC。

- 此橙色图标表示 ***AVG Internet Security 2012 处于严重状态***！一个或多个组件无法正常工作，因此 **AVG Internet Security 2012** 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 Internet Security 2012 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 Internet Security 2012 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！

注意：*AVG Internet Security 2012 状态信息也可以随时通过系统任务栏图标获得。*

5.3. 快速链接

快速链接位于 **AVG Internet Security 2012** 用户界面左侧。通过这些链接可直接使用该程序最重要和最常用的应用程序特性，如扫描和更新。快速链接能在用户界面的所有对话框中使用：

 2012 版权所有 AVG Technologies CZ, s.r.o. 保留所有权利。

快速链接 以图形方式分三个部分：

- ***立即扫描*** - 默认情况下，用该按钮可了解有关所启动的上一次扫描操作的信息 *（即扫描类型和上次启动日期）*。单击***立即扫描*** 命令可再次启动上一次扫描操作。如果要启动另一项扫描操作，请单击***扫描选项*** 链接。这样可以打开 AVG 扫描界面，从中可执行扫描，安排扫描，或编辑其参数。 *（对于详细信息，请参见 AVG 扫描一章）*
- ***扫描选项*** - 使用此链接可从当前打开的任何 AVG 对话框切换到包含所有已安装组件概览的默认对话框。 *（对于详细信息，请参见组件概览一章）*
- ***立即更新*** - 用该链接可了解上次启动更新的日期和时间。按该按钮可直接运行更新进程，还可密切关注其进度。 *（对于详细信息，请参见 AVG 更新一章）*

快速链接 随时均可在 AVG 用户界面中使用。一旦您使用某一快速链接运行特定进程（扫描进程或更新进程），该应用程序便会切换到一个新对话框，但这些快速链接依然可用。此外，还会在操作方法中进一步以图形方式显示正在运行的进程，这样就可以全面控制目前运行在 **AVG Internet Security 2012** 中的所有已启动进程。

5.4. 组件概览

组件概览部分

组件概览 部分位于 **AVG Internet Security 2012** 用户界面中部。该区域分为两个部分：

- ***所有已安装组件的概述*** 中包括全部已安装组件的图形面板。每个面板都标有相应组件的图标，还有关于相应组件目前是已激活还是已停用的信息。
- ***组件说明*** 位于此对话框底部。组件说明用于简短说明组件的基本功能。此外，其中还有关于所选组件当前状态的信息。

已安装组件的列表

在 **AVG Internet Security 2012 中，*组件概览*** 部分中含有关于以下组件的信息：

- ***Anti-Virus*** 用于检测系统中的病毒、间谍软件、蠕虫、特洛伊木马、不需要的可执行文件或库，也可以防止受到恶意广告软件的侵害 - 详细信息 >>

 2012 版权所有 AVG Technologies CZ, s.r.o. 保留所有权利。

- ***LinkScanner*** 用于在 Internet 上搜索和上网时防止受到基于 Web 的攻击 - 详细信息 >>
- ***电子邮件保护*** 用于检查传入的电子邮件中的垃圾邮件，以及阻止病毒、仿冒攻击或其它威胁 - 详细信息 >>
- ***Firewall*** 用于控制通过每个网络端口传输的所有通讯内容，从而防止受到恶意攻击，并阻止所有入侵企图 - 详细信息 >>
- ***Anti-Rootkit*** 用于扫描隐藏在应用程序、驱动程序或库内的危险 Rootkit - 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*** 用于持续防止用户的数字财产遭到新威胁和不明威胁的破坏 - 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

能执行的操作

- ***将鼠标光标移到任一组件的图标上*** 即可在组件概览中突出显示该组件。与此同时，该组件的基本功能说明也会显示在用户界面的底部。
- ***单击任一组件的图标*** 即可打开相应组件自身的界面，其中列有基本统计数据。
- ***在组件图标上单击鼠标右键***即可展开上下文菜单，其中有多个选项：
  - ***打开*** - 单击此选项可打开相应组件自身的对话框 *（与单击相应组件的图标的效果完全相同）*。
  - ***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这种状态，而且不想通过系统任务栏图标收到警告。
  - ***打开高级设置...*** - 仅可将此选项用于某些组件，即能用其使用高级设置的组件。

5.5. 系统任务栏图标

AVG 系统任务栏图标 *（在显示器右下角的 Windows 任务栏中）*用于显示 **AVG Internet Security 2012** 的当前状态。无论 **AVG Internet Security 2012** 用户界面是已打开还是已关闭，始终均可在系统任务栏中看到该图标：

 2012 版权所有 AVG Technologies CZ, s.r.o. 保留所有权利。

AVG 系统任务栏的显示方式

- 该图标处于全彩状态，而且没有附加元素，表明所有 **AVG Internet Security 2012** 组件都已激活，都运行完全正常。但是，如果某个组件的运行不完全正常，但用户已决定忽略组件状态，则也会这样显示该图标。 *确认忽略组件状态选项，就表示知道组件的错误状态，但出于某种原因想要保持这种状态，不想看到有关这种情况的警告。）*

- 该图标带有感叹号，表明某个组件 *（甚至更多组件）* 处于错误状态。始终都要注意此类警告，并且尽力解决组件未设置妥当的配置问题。为了能够执行组件配置更改，请双击 AVG 系统任务栏图标打开应用程序用户界面。对于有关哪些组件处于错误状态的详细信息，请查阅安全状态信息一节。

- AVG 系统任务栏图标还可以这样的方式显示，即处于全彩状态并且带有闪烁并旋转着的一束光。这种图形显示方式用于表示目前已启动更新进程。

- 显示全彩图标并且带有箭头，表示正在执行一项 **AVG Internet Security 2012** 扫描操作。

AVG 系统任务栏信息

AVG 系统任务栏图标还可以向您通知 **AVG Internet Security 2012** 中的当前活动，及通过在系统托盘图标中打开的弹出窗口，通知程序中的可能状态变化 *例如，自动启动计划内更新或扫描、Firewall 配置文件切换、组件状态变化、出现错误状态等*）：

可通过 AVG 系统任务栏图标执行的操作

也可将 ***AVG 系统任务栏图标*** 用作快速链接，以显示 **AVG Internet Security 2012** 用户界面，只须双击 AVG 系统任务栏图标即可。通过用鼠标右键单击 AVG 系统任务栏图标，可以打开一个简短的上下文菜单，其中有以下选项：

- ***打开 AVG 用户界面*** - 单击可打开 **AVG Internet Security 2012** 用户界面。

 2012 版权所有 AVG Technologies CZ, s.r.o. 保留所有权利。

- ***暂时禁用 AVG 保护*** - 使用该选项可以一次性关闭由**AVG Internet Security 2012**提供的整个保护。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 Internet Security 2012**，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。如果必须暂时禁用**AVG Internet Security 2012**，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。

- ***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（*已启用 Firewall/已禁用 Firewall/紧急模式*）、游戏模式切换和 Firewall 配置文件。

- ***扫描*** - 单击此项可打开预定义扫描的上下文菜单（*扫描整个计算机*和*扫描特定的文件或文件夹*），然后选择所需的扫描，该扫描会立即启动。

- ***正在运行扫描...*** - 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*。

- ***运行 PC Analyzer*** - 单击可启动 PC Analyzer 组件。

- ***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。

5.6. AVG Advisor

AVG Advisor 是一种可保持监控您 PC 中所有运行的进程以找到潜在的问题，并提示如何避免此问题发生的性能特征。***AVG Advisor*** 可在系统任务栏以滑动的弹出窗口形式出现。

AVG Advisor 可能会在以下情况中显示：

- 所使用的 Internet 浏览器的内存不足，可能会降低 PC 运行速度（*AVG Advisor 只支持 Internet Explorer、Chrome、Firefox、Opera 和 Safari 浏览器*）；

- 计算机上正在运行的某一进程在消耗大量的内存，从而降低 PC 的性能；

- 您的计算机将要自动连接到未知 WiFi。

在上述任何情况中，***AVG Advisor*** 会警告您可能发生的潜在问题，并提供冲突进程或应用

 2012 版权所有 AVG Technologies CZ, s.r.o. 保留所有权利。

程序的名称和图标。另外，***AVG Advisor*** 会建议采取何种措施来避免潜在的问题。

5.7. AVG 小工具

AVG 小工具 显示在 Windows 桌面（*Windows 边栏*）中。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 2012** 功能的即时访问权限，如扫描和更新：

快速执行扫描和更新

可立即用 ***AVG 小工具*** 根据您的需要发起扫描或更新：

- ***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*** **AVG Internet Security 2012**链接可直接从该小工具中启动更新：

 2012 版权所有 AVG Technologies CZ, s.r.o. 保留所有权利。

访问社交网络

AVG 小工具 中也有一个快速链接，可连接到主要社交网络。可用相应按钮连接到 Twitter、Facebook 或 LinkedIn 中的 AVG 社区：

- ***Twitter 链接*** - 打开一个新的 ***AVG 小工具*** 界面，上面提供 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*** - 只有网络安装中才提供此选项 *（即如果已用某个 AVG 企业版许可证安装 AVG）*；它可打开 Internet 浏览器，显示 LinkedIn 社交网络中的 ***AVG SMB 社区*** 网站。

能通过小工具使用的其它特性

- ***PC Analyzer*** - 用于打开 PC Analyzer 组件中的用户界面，并立即启动分析。

- ***搜索框*** - 键入关键字后立即用默认 Web 浏览器在新打开的窗口中显示搜索结果。

2012 版权所有 AVG Technologies CZ, s.r.o. 保留所有权利。

6. AVG 组件

6.1. Anti-Virus

Anti-Virus 组件是 **AVG Internet Security 2012 的基石，**该组件已将安全程序的多种基本特性集于一身：

- 扫描引擎
- 常驻保护措施
- Anti-Spyware 防护措施

6.1.1. 扫描引擎

扫描引擎是 ***Anti-Virus*** 组件的基础，用于扫描所有文件和文件活动 *（打开/关闭文件等活动）*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，然后在病毒库中将其清除或隔离。

AVG Internet Security 2012 的一项重要特性就是不让任何已知病毒在计算机上运行！

检测方式

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，即所谓的病毒特征。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。***Anti-Virus*** 采用以下检测方式：

- 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

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。**AVG Internet Security 2012** 也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 Internet Security 2012** 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。

AVG Internet Security 2012 可为计算机提供不间断保护！

6.1.2. 常驻保护措施

AVG Internet Security 2012 可以所谓的常驻保护措施的形式提供持续保护。***Anti-Virus*** 组件用于扫描正在打开、保存或复制的每一个文件 *（有特定扩展名或根本没有扩展名）*。该组件用于保护计算机的系统区和可移动介质（*闪存盘等介质*）。如果在所访问的文件中发现病毒，该组件会停止正在执行的操作，不许病毒激活自身。用户通常甚至不会注意到上述过

 2012 版权所有 AVG Technologies CZ, s.r.o. 保留所有权利。

程，因为常驻保护措施 在后台 运行。仅当发现威胁后才会得到通知 ;与此同时，***Anti-Virus*** 还会阻止所发现的威胁的激活，将其删除。

常驻保护措施在计算机启动期间被加载到计算机内存中。请务必始终保持其启用状态，这一点至关重要！

6.1.3. Anti-Spyware 防护措施

Anti-Spyware 含有间谍软件数据库，用于辨别类型已知的间谍软件定义。AVG 间谍软件专家会努力识别和描述刚刚涌现出来的最新间谍软件模式，并将其定义添加到间谍软件数据库中。这些新的定义将通过更新过程下载到计算机中，这样即使面对最新的间谍软件类型，也始终能够得到可靠的保护。通过 ***Anti-Spyware*** 可对计算机进行全面的恶意软件/间谍软件扫描。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。

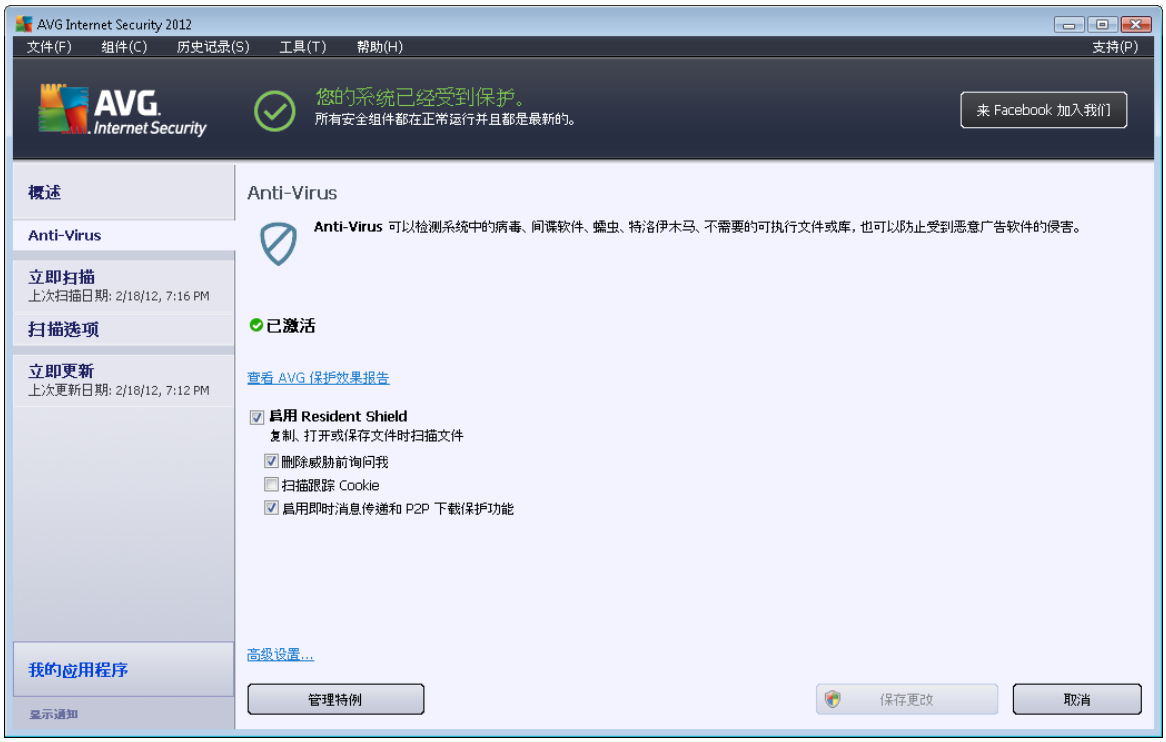
什么是间谍软件？

间谍软件通常是指一种恶意软件，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，往往含有广告、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的内容的网站。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。

 2012 版权所有 AVG Technologies CZ, s.r.o. 保留所有权利。

6.1.4. Anti-Virus 界面

Anti-Virus 组件的界面中包含该组件的功能的简短信息、该组件当前状态（*已激活*）的信息，以及该组件的基本配置选项：



配置选项

对于可在 ***Anti-Virus*** 组件中使用的特性，该对话框中有一些基本配置选项。以下是这些选项的概括说明：

- ***查看 AVG 如何进行保护在线报告*** - 该链接用于重定向到 AVG 网站 (http://www.avg.com/) 中的特定网页。对于在特定时段内在计算机中执行的所有 **AVG Internet Security 2012** 活动，该网页中有详细统计信息综览。
- ***启用 Resident Shield*** - 用此选项可轻松启用/禁用常驻保护措施。Resident Shield 可在复制、打开或保存文件时对其进行扫描。检测到病毒或任何类型的威胁时，都会立即发出警告。默认情况下已启用此功能，建议保持其启用状态！启用常驻保护措施后，可进一步决定要如何处理可能检测到的受感染文件：
  - ***删除威胁前询问我*** - 保持此选项的选中状态以确认在检测到的威胁移至病毒库之前的任何时候，都要询问我。此选项对安全级别无影响，仅为用户使用偏好。
  - ***扫描跟踪 Cookie*** - 可决定是否要扫描跟踪 Cookie（与上面的选项无关）。*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*

2012 版权所有 AVG Technologies CZ, s.r.o. 保留所有权利。

*户的特定信息，如网站首选项或电子购物车中的内容。)*特定情况下可启用此选项，以达到最高安全级别，但默认情况下已将其禁用。

- ***启用即时消息传递和 P2P 下载保护功能***- 如果您希望验证即时消息通信（*例如，ICQ、MSN Messenger 等*）没有病毒），请选中此选项。

- ***高级设置*** - 单击此链接可重定向到 **AVG Internet Security 2012** 高级设置中的相应对话框。从中可详细编辑该组件的配置。但请注意，设置所有组件的默认配置时，目的都是使 **AVG Internet Security 2012** 的性能和安全性达到最高程度。除非确实有理由如此，否则建议保留默认配置！

控制按钮

可在该对话框中使用以下控制按钮：

- ***管理特例*** - 用于打开 ***Resident Shield - 特例***的新对话框。Resident Shield 扫描中特例配置也可通过主菜单进行访问，请按以下顺序操作：依次单击高级设置/Anti-Virus/Resident Shield/特例 *有关详细说明，请参见相应章节)*。可在该对话框中指定要排除在 Resident Shield 扫描范围以外的文件和文件夹。我们强烈建议，若非必要，不要排除任何项目！此对话框中有以下控制按钮：
  - *添加路径* - 用于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一个 *(或多个)* 目录。
  - *添加文件* - 用于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* - 用其可编辑所选文件或文件夹的指定路径。
  - *删除项目* - 用其可从列表中删除所选项目的路径。
  - *编辑列表* - 用其可在新对话框（作用类似于标准文本编辑器）中编辑整个已定义特例的列表。
- ***应用*** - 用于保存在此对话框中对所有组件设置执行的更改，并返回到**AVG Internet Security 2012**的主用户界面（*组件概览*）。
- ***取消*** - 用于取消在此对话框中执行的所有组件设置更改。不会保存任何更改。会返回到 **AVG Internet Security 2012** 主用户界面（*组件概览*）。

6.1.5. Resident Shield 检测结果

已检测到威胁！

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：

 2012 版权所有 AVG Technologies CZ, s.r.o. 保留所有权利。

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*）、识别出的感染的名称（*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*）。

此外，还必须决定现在该执行什么操作。有几个选项可供选择。***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）！***

- ***修复*** - 仅当检测到的感染可修复时才会显示此按钮。然后会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（推荐）*** - 将病毒移至病毒库
- ***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*）
- ***忽略威胁*** - 我们极力建议，若非绝对必要，请勿使用此选项！

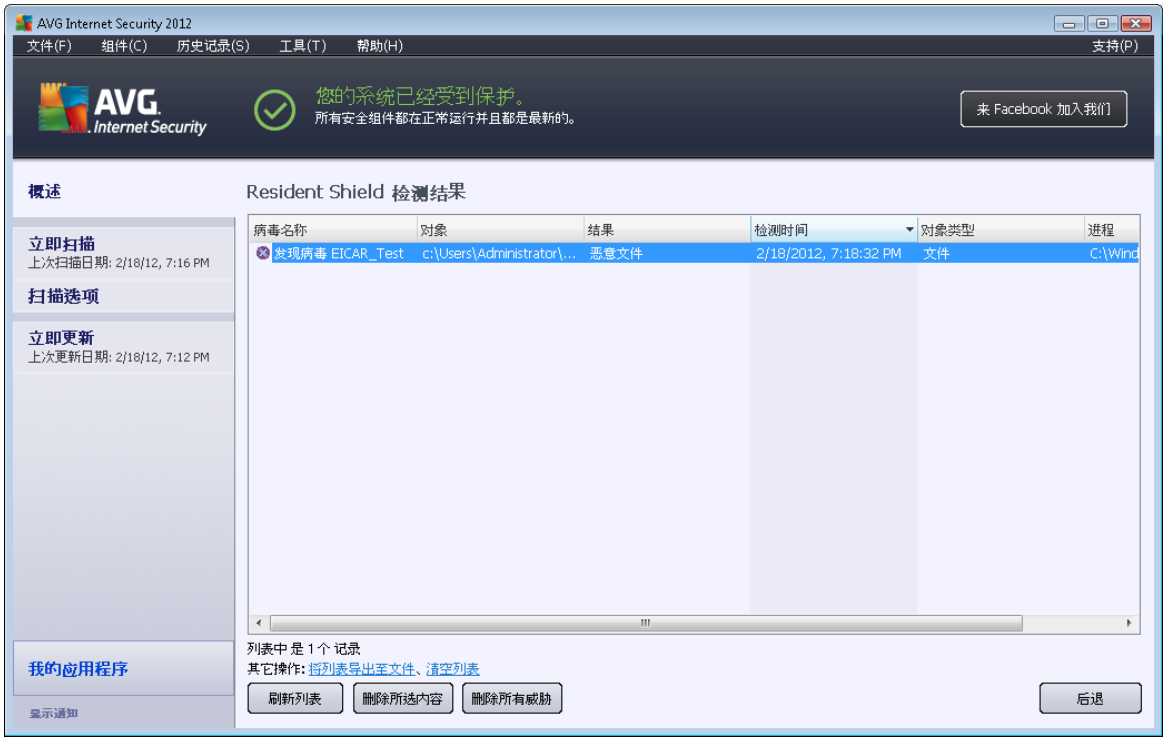
注：*检测到的对象可能会大于病毒库中的可用空间。如果情况如此，则会在尝试将已受到感染的对象移到病毒库中时弹出警告消息，就所发生的问题发出通知。但病毒库大小可以编辑。病毒库大小指定为硬盘实际大小的可调比例。要加大病毒库，请通过 AVG 高级设置 中的 限制病毒库大小 选项，转到病毒库对话框。*

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 检测结果概览

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：

 2012 版权所有 AVG Technologies CZ, s.r.o. 保留所有权利。



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 AVG 主对话框（*组件概览*）。

6.2. LinkScanner

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。

2012 版权所有 AVG Technologies CZ, s.r.o. 保留所有权利。

LinkScanner 保护措施不适用于服务器平台！

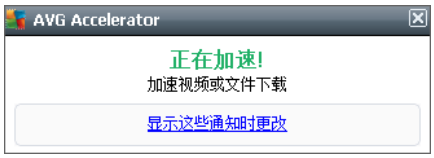
LinkScanner 技术由如下主要特性构成：

- Search-Shield 包含已知危险的网站 *（URL 地址）*列表。在通过 Google、Yahoo!JP、eBay、Twitter、Digg、SlashDot、WebHledani、Yandex、百度、Bing、AOL、AltaVista、EarthLink、Ask 和 Seznam 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。

- 上网时，Online Shield 以实时保护措施的形式运行。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。Online Shield 可检测到即将访问的页面中所含的病毒和间谍软件，还会立即停止下载，这样威胁从来都不会进入计算机。

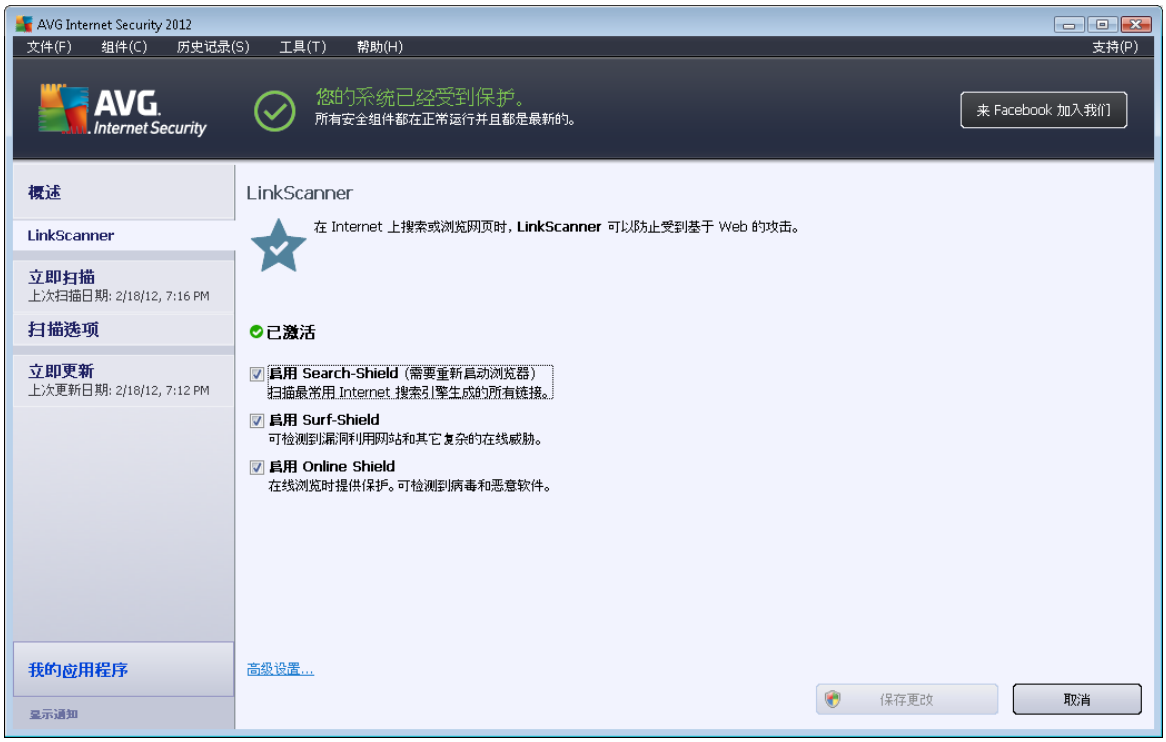
- ***通过 AVG Accelerator*** 可使在线视频播放更加流畅，还可使后续下载更加容易。视频加速进程运行时，会通过系统任务栏弹出窗口发出通知。



 2012 版权所有 AVG Technologies CZ, s.r.o. 保留所有权利。

6.2.1. LinkScanner 界面

LinkScanner 组件的主对话框简要说明了该组件的功能，并提供了有关该组件当前状态 *(已激活)* 的信息：



该对话框底部有该组件的一些基本配置：

- ***启用 Search-Shield*** *-(默认情况下已启用)*：仅当有正当理由禁用 Search Shield 功能时才取消选中该框。
- ***启用 Surf-Shield*** *-(默认情况下已启用)*：用于主动 *(实时)* 防范访问网站时遇到的漏洞利用网站。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。
- ***启用 Online Shield*** *-(默认情况下已启用)*：用于对即将访问的网页进行实时扫描，以检测潜在病毒或间谍软件。如果已发现这些威胁，则会立即停止下载，这样威胁从来都不会进入计算机。

6.2.2. Search-Shield 检测结果

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，LinkScanner 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：

2012 版权所有 AVG Technologies CZ, s.r.o. 保留所有权利。

所链接的页面是安全的.

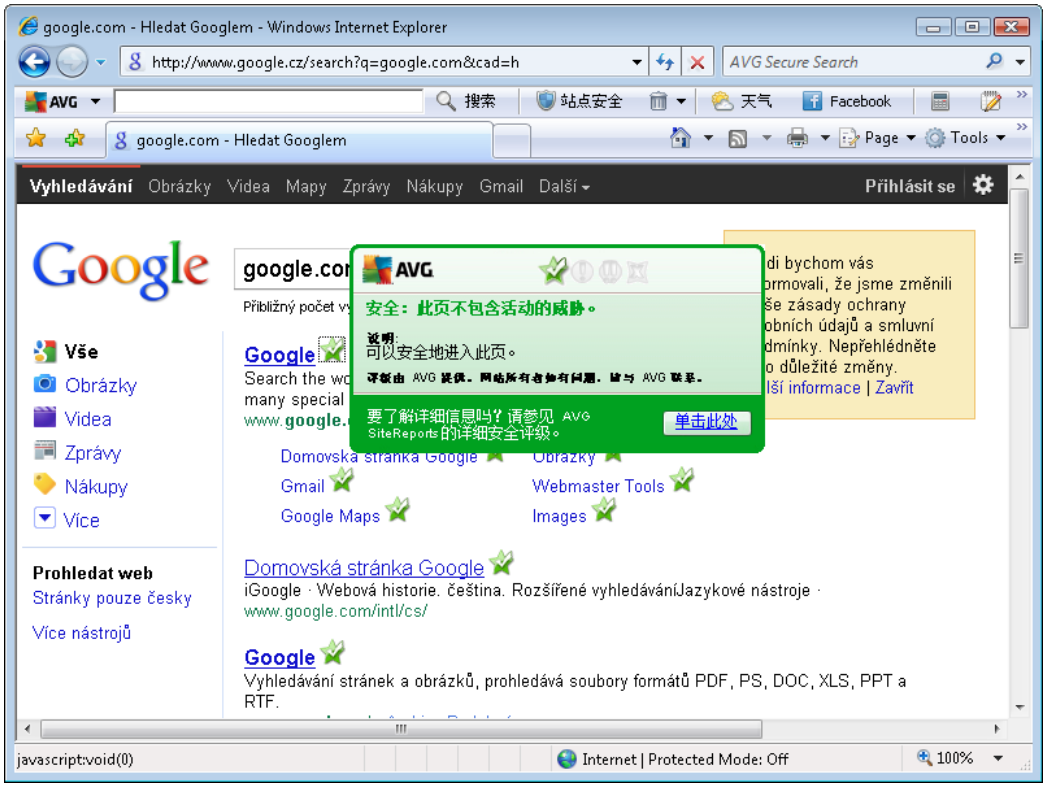
所链接的页面不包含威胁，但有些可疑 *(来源或动机可疑，因此不建议进行电子购物等)*。

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)*：



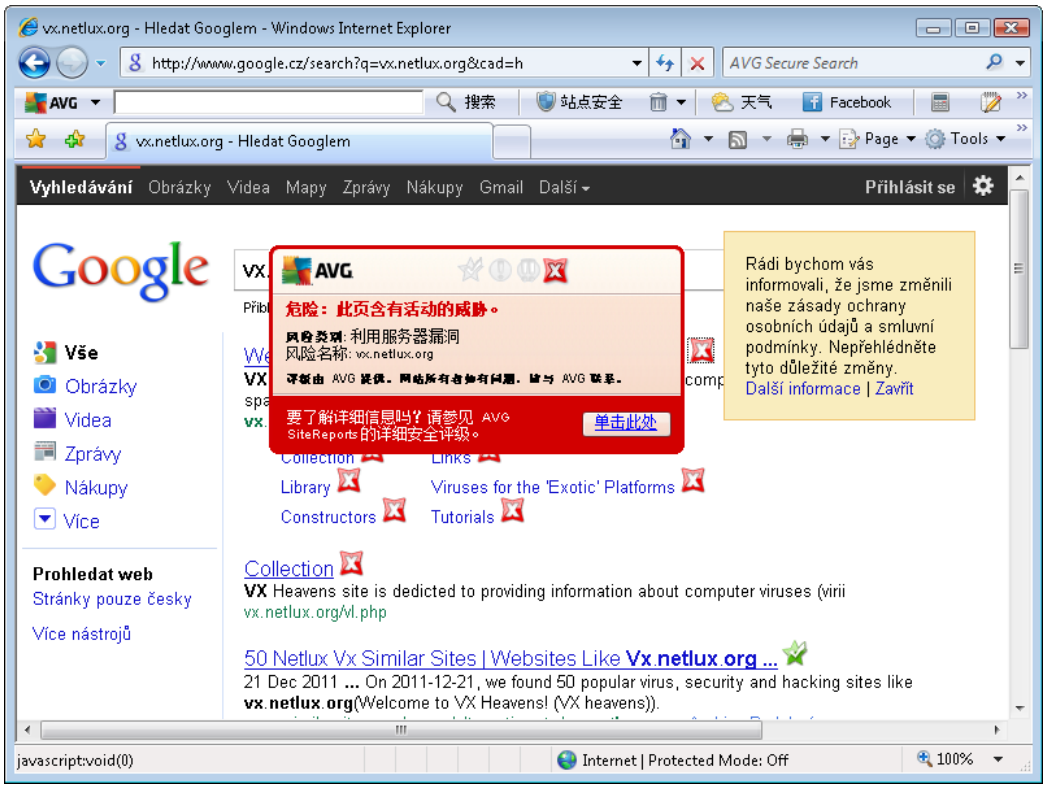
6.2.3. Surf-Shield 检测结果

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，当您要访问包含漏洞利用或其它严重威胁的危险网页时，LinkScanner 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，LinkScanner 将使用类似下面的屏

2012 版权所有 AVG Technologies CZ, s.r.o. 保留所有权利。

幕警告您：



进入此类网站会带来很大的风险，建议不要进入！

6.2.4. Online Shield 检测结果

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：

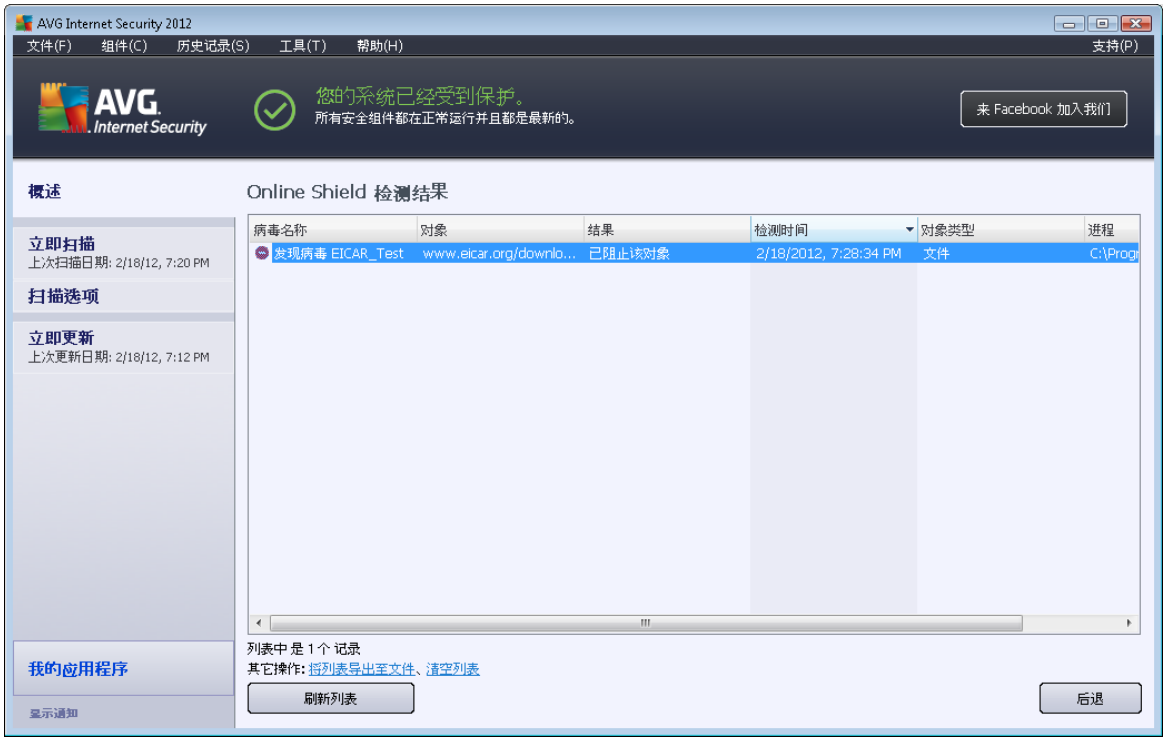
在此警告对话框中，您将找到关于经检测被认定为受感染的文件的数据（*文件名*）、识别到的感染的名称（*威胁名称*），以及指向病毒百科全书的链接，您可以在病毒百科全书中找到关于该感染的详细信息（*如果已知*）。该对话框提供了以下按钮：

- ***"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。

2012 版权所有 AVG Technologies CZ, s.r.o. 保留所有权利。

- ***"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"***）。

控制按钮

- ***刷新列表*** - 用于更新 ***Online Shield***

2012 版权所有 AVG Technologies CZ, s.r.o. 保留所有权利。

- ***后退*** - 用于切换回默认的 AVG 主对话框 *组件概览*）

6.3. 电子邮件保护

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会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。

电子邮件保护 组件用于扫描每一封发送或接收的电子邮件；每当检测到电子邮件中有病毒，都会立即将其删除并移到病毒库中。该组件还可过滤出特定类型的电子邮件附件，并为未感染病毒的邮件添加验证文本。***电子邮件保护*** 包括两个主要功能：

- E-mail Scanner
- Anti-Spam

6.3.1. E-mail Scanner

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 中没有自己插件的电子邮件客户端搭配使用，*但也可用于扫描 AVG 用特定插件进行支持的电子邮件客户端 即 Microsoft Outlook、The Bat 和 Mozilla Thunderbird*）的电子邮件。它主要与 Outlook Express、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 E-mail Scanner；E-mail Scanner 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*）。

E-mail Scanner 不适用于服务器平台！

6.3.2. Anti-Spam

Anti-Spam 的运行方式如何？

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为垃圾邮件。***Anti-Spam*** 可以通过添加特殊文本字符串修改电子邮件 *已被认定为垃圾邮件*）的主题。您可以在电子邮件客户端中轻松地过滤您的电子邮件。***Anti-Spam*** 组件用多种分析方法来处理每一封电子邮件，可最大程度地阻止不需要的电子邮件。***Anti-Spam*** 用定期更新的数据库检测垃

 2012 版权所有 AVG Technologies CZ, s.r.o. 保留所有权利。

垃圾邮件。也可使用 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（*从来都不会被标为垃圾邮件*）和黑名单（*始终都会被标为垃圾邮件*）手动添加电子邮件地址。

什么是垃圾邮件？

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。

6.3.3. 电子邮件保护界面

电子邮件保护 对话框中有描述该组件功能的简要文本、有关其当前状态的信息（*已激活*）。可用 ***在线查看 AVG 保护效果报告*** 链接在 AVG 网站 (http://www.avg.com/) 的专用网页上查看详细 **AVG Internet Security 2012** 活动统计信息和检测结果。

基本电子邮件保护设置

在 ***电子邮件保护*** 对话框中，可进一步编辑该组件的功能的某些基本特性：

- ***扫描传入的邮件***（*默认情况下已启用*）- 选中此框可指定对传送到您帐户的所有电子邮件都应进行病毒扫描。
- ***扫描传出的邮件***（*默认情况下已禁用*）- 选中此框可确认您的帐户外发的所有电

2012 版权所有 AVG Technologies CZ, s.r.o. 保留所有权利。

子邮件都应进行病毒扫描。

- ***扫描电子邮件时显示通知窗口*** *默认情况下已启用*)- 选中此选项可确认想要在扫描邮件的过程中，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。

- ***启用 Anti-Spam*** *默认情况下已启用*)- 选中该选项可指定是否要滤掉传入邮件中不请自来的电子邮件。

所有 AVG 组件均已由软件供应商为了提供最佳性能而设置好。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。

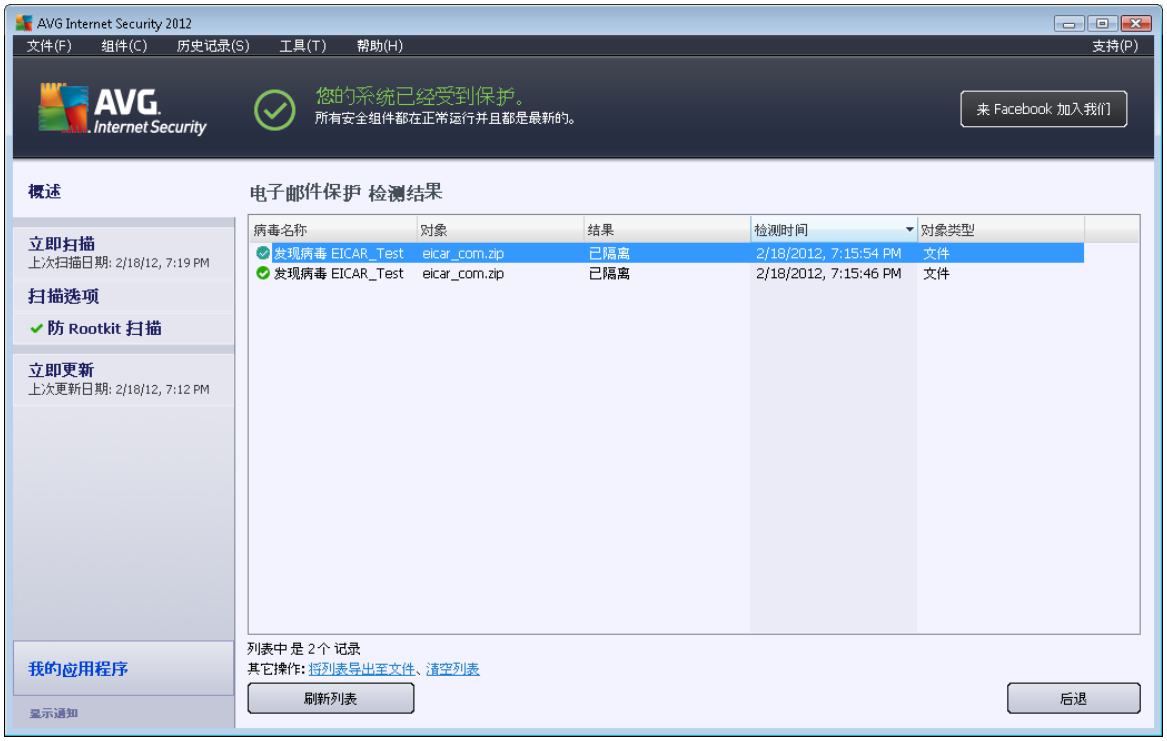
控制按钮

电子邮件保护 对话框中有如下控制按钮：

- ***保存更改*** - 按此按钮可保存并应用在此对话框中所作的所有更改

- ***取消*** - 按此按钮可返回默认的 AVG 主对话框(*组件概览*)

6.3.4. E-mail Scanner 检测结果



在 ***E-mail Scanner 检测结果***对话框 (*可通过系统菜单选项 历史记录 /“E-mail Scanner 检测结果 显示*)中，能看到电子邮件保护 组件检测到的所有结果的列表。对于检测到的每个对

2012 版权所有 AVG Technologies CZ, s.r.o. 保留所有权利。

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*** - 用于更新检测到的威胁的列表。
- ***后退*** - 用于切换回之前显示的对话框。

6.4. Firewall

防火墙是一个系统，用于通过阻止/允许网传信息在两个或更多网络之间强制执行访问控制策略。Firewall 中有一些用于防止内部网络受到外来攻击（*通常来自 Internet*）的规则，并控制着通过每个网络端口的所有通讯。会按指定的规则对这些通讯内容进行评估，然后会允许或禁止传输这些通讯内容。如果 ***Firewall*** 识别出入侵企图，则会 阻止 这种企图，不许入侵者访问计算机。

Firewall 经过配置后会允许或拒绝传输通过指定端口的或指定软件应用程序的内部/外部通讯内容（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。

Firewall 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其从您的计算机中发出。Firewall 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，***Firewall*** 还可防止每台计算机受到网络中其它计算机上的内部用户发起的攻击。

未得到 Firewall 保护的计算机，都会成为易受计算机黑客和数据窃贼攻击的目标。

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。*

6.4.1. Firewall 原理

在 **AVG Internet Security 2012** 中，***Firewall*** 控制着通过计算机的每个网络端口传输的所有网传信息。***Firewall*** 会根据指定的规则，对运行在您计算机中的*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。对于其中的每个应用程序，***Firewall*** 都会确定是否允许其通过这些网络端口进行通讯。默认情况下，如果应用程序不明 *即未指定相应的 Firewall 规则)*，则 ***Firewall*** 会询问是要允许还是阻止其通讯尝试。

AVG Firewall 不适用于服务器平台！

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

6.4.2. 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*** - 是制造商默认设置好的 Firewall 系统配置文件，始终都会显示出来。启用此配置文件后，会允许传输所有网络通讯内容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 - 要彻底禁用所有过滤功能，必须禁用 Firewall)。不能复制或删除此系统配置文件，也不能修改
- ***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。启用此配置文件后，所有网络通讯内容传输都将被阻止，计算机既不能从外部网络进行访问，也不能与外部进行通讯。不能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*** - 通过自定义配置文件，能利用自动切换配置文件功能，如果频繁连接各种不同的网络 *例如使用笔记本电脑时)*，此功能就特别有用。自定义配置文件在安装 **AVG Internet Security 2012** 之后自动生成，而且可以满足 Firewall 策略规则的每一项需要。可使用以下自定义配置文件：
    - ***直连到 Internet*** - 适用于直接连接到 Internet 并且没有任何额外保护措施的普通家用台式计算机或笔记本电脑。连接笔记本电脑和各种不明和可能不安全 (*例如，在网吧、酒店房间等场所上网*) 的网络时，也建议选中此选项。此配置文件的最严格的 Firewall 策略规则可确保此类计算机得到充分保护。
    - ***域中的计算机*** - 适用于本地网络 通常是在学校或工作场所) 中的计算机。

 2012 版权所有 AVG Technologies CZ, s.r.o. 保留所有权利。

这种情况下会假定网络有专业管理或受某些其它措施保护，因此安全级别比上述情况可以低一些，允许访问共享文件夹、磁盘设备等。

- ***小型家庭或办公网络*** - 适用于小型网络中的计算机，特别是家庭或小型企业中的计算机。此类网络通常没有 中央 管理员，只有几台计算机连在一起，经常共享一台打印机、扫描仪或类似设备，Firewall 规则必须反映这些情况。

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指定配置文件，则在下次连接到此区域时，Firewall 将显示一个对话框，要求指定配置文件。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。

6.4.3. Firewall 界面

名为 ***Firewall 组件*** 的主对话框中有关于该组件功能的一些基本信息，该组件的状态 *已激活*），以及简短的组件统计信息概览：

- ***Firewall 已启用*** - 自 Firewall 上次启动到目前所经过的时间

 2012 版权所有 AVG Technologies CZ, s.r.o. 保留所有权利。

- ***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

基本 Firewall 设置

- ***选择 Firewall 配置文件*** - 可从下拉菜单中选择某个指定的配置文件 *(对于各个配置文件及其推荐用途的详细说明，请查阅 Firewall 配置文件一章)*
- ***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。
- 此外，在此基本设置部分中，还可从三个用于指定 Firewall 组件当前状态的选项中进行选择：
  - ***已启用 Firewall*** *(默认情况下已启用)* - 选中此选项可允许与所选 Firewall 配置文件中指定的那套规则中指定为 "允许" 的那些应用程序通讯
  - ***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 通讯)*** - 选中此选项将阻止通过每个网络端口的所有网传信息；Firewall 仍在运行，但所有网传信息都会受阻。

请注意：*所有 AVG Internet Security 2012 组件均已由软件供应商为了提供最佳性能而设置好。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作的全部更改。
- ***取消*** - 按此按钮可返回到默认的 AVG 主对话框 *(组件概览)*。

6.5. Anti-Rootkit

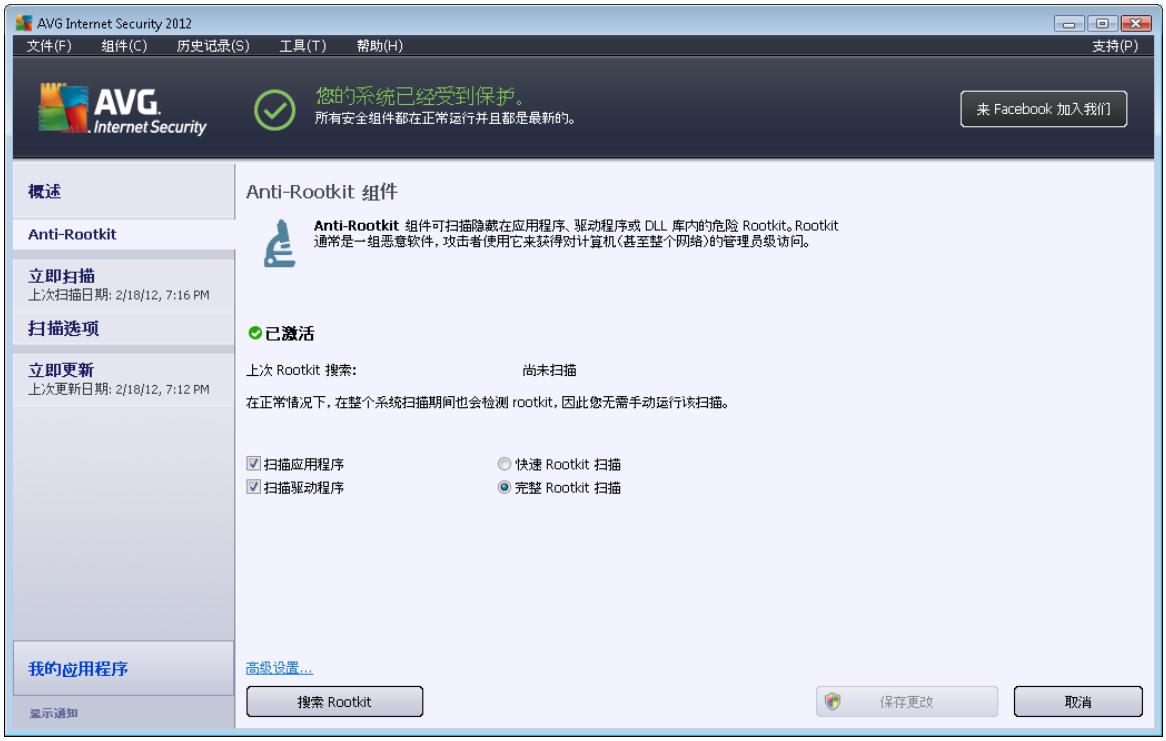
Anti-Rootkit 是一款专门用来检测和有效删除危险 Rootkit *(即可在您的计算机中掩饰恶意软件存在的程序和技术)*的工具。***Anti-Rootkit*** 能根据一组预先指定的规则检测 Rootkit。请注意，所有 Rootkit 都会被检测出来 *(不仅是已感染文件的 Rootkit)*。如果 ***Anti-Rootkit*** 发现一个 Rootkit，则未必意味着该 Rootkit 已感染文件。有时，Rootkit 会被用作驱动程序，或者是正当应用程序的组成部分。

 2012 版权所有 AVG Technologies CZ, s.r.o. 保留所有权利。

什么是 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。

6.5.1. Anti-Rootkit 界面



该 ***Anti-Rootkit*** 对话框简要说明了该组件的功能，并显示有关该组件的当前状态 *(活动)*，以及还提供有关上次启动 ***Anti-Rootkit*** 测试的信息 *(上次 Rootkit 搜索，rootkit 测试在扫描整个计算机*期间是默认运行的进程)。***"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。

所有 AVG 组件均已由软件供应商为了提供最佳性能而设置好。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。

基本 Anti-Rootkit 设置

在该对话框的底部，可设置一些基本的 Rootkit 扫描功能。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***

2012 版权所有 AVG Technologies CZ, s.r.o. 保留所有权利。

- ***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、已加载的驱动程序和系统文件夹 *(通常是 c:\Windows)*，以及所有本地磁盘 *(包括闪存驱动器，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，因此可以直接在 ***Anti-Rootkit*** 界面中通过此按钮执行 Rootkit 扫描。
- ***保存更改*** - 按此按钮可保存在此界面中所作的所有更改，并返回默认的 AVG 主对话框 *(组件概览)*。
- ***取消*** - 按此按钮可返回到默认的 AVG 主对话框 *(组件概览)*，但未保存所作的任何更改。

6.6. 系统工具

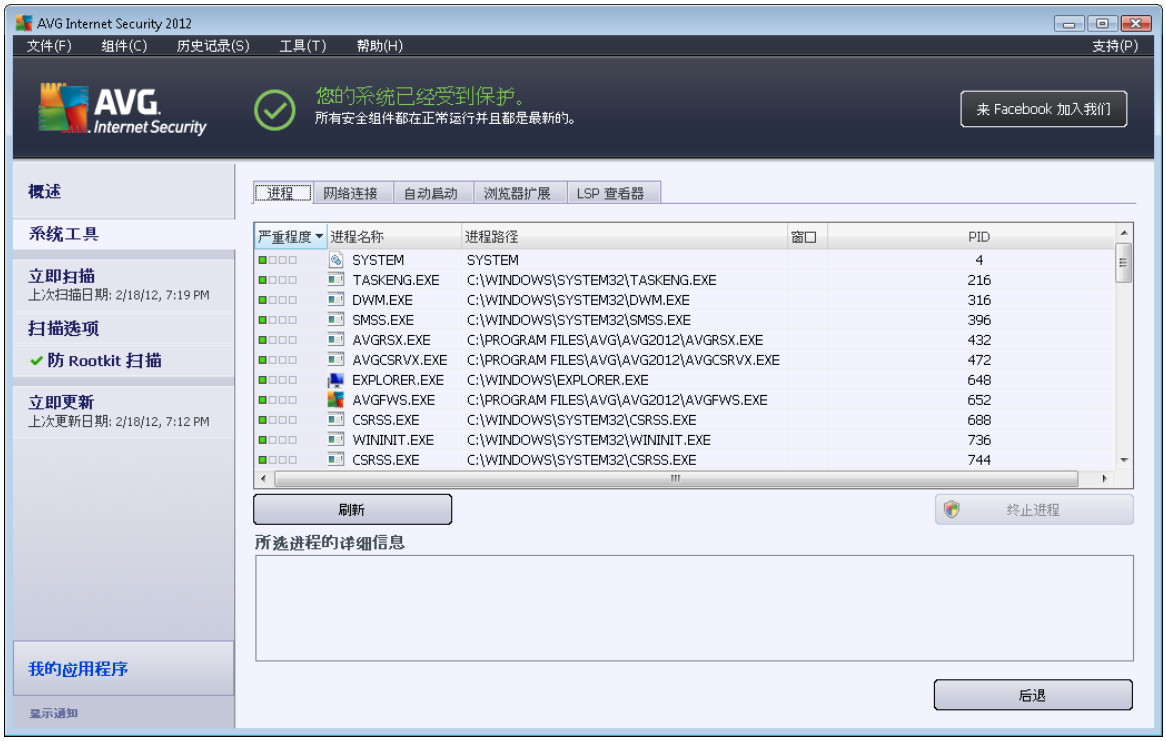
系统工具 是指可以显示 **AVG Internet Security 2012** 环境和操作系统详细摘要的工具。该组件显示了以下各项的概览：

- 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！

2012 版权所有 AVG Technologies CZ, s.r.o. 保留所有权利。

6.6.1. 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

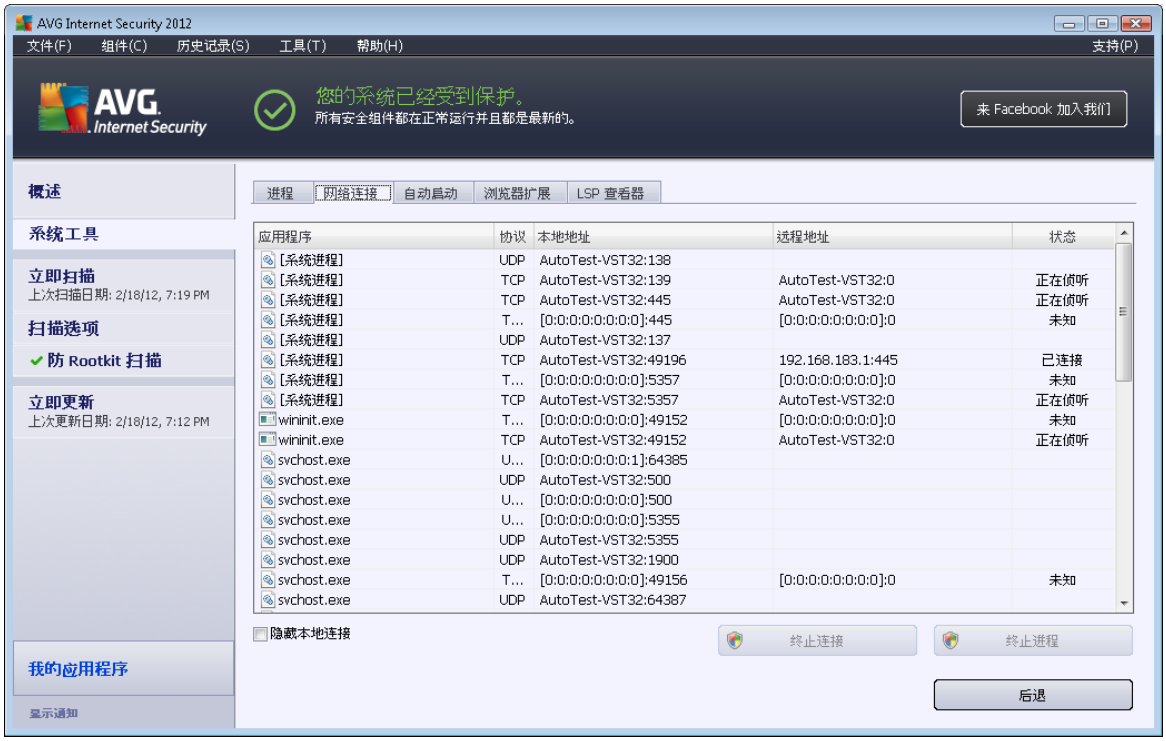
控制按钮

进程 选项卡中有如下控制按钮：

- ***'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！***
- ***后退*** - 用于切换回默认的 AVG 主对话框 *(组件概览)*

2012 版权所有 AVG Technologies CZ, s.r.o. 保留所有权利。

6.6.2. 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

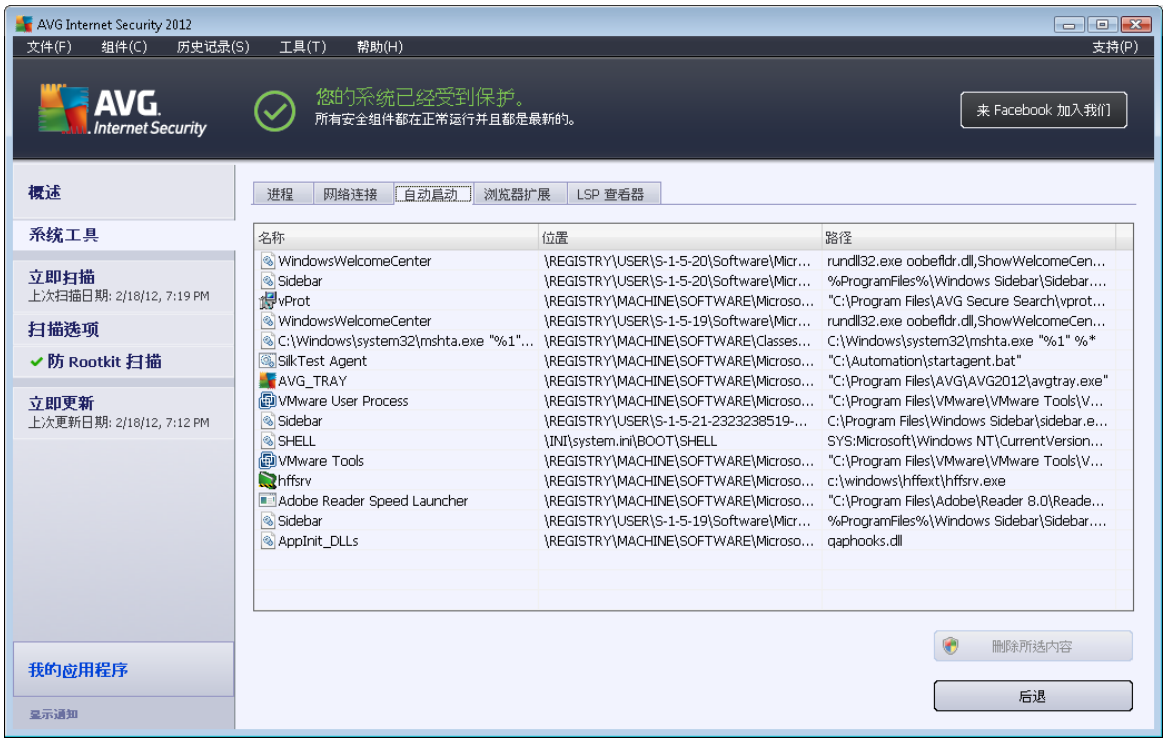
网络连接选项卡中有如下控制按钮：

 2012 版权所有 AVG Technologies CZ, s.r.o. 保留所有权利。

- ***'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*** - 用于切换回默认的 AVG 主对话框 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！

6.6.3. 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。有几种恶意应用程序通常会自动将自身添加到注册表启动项中。

控制按钮

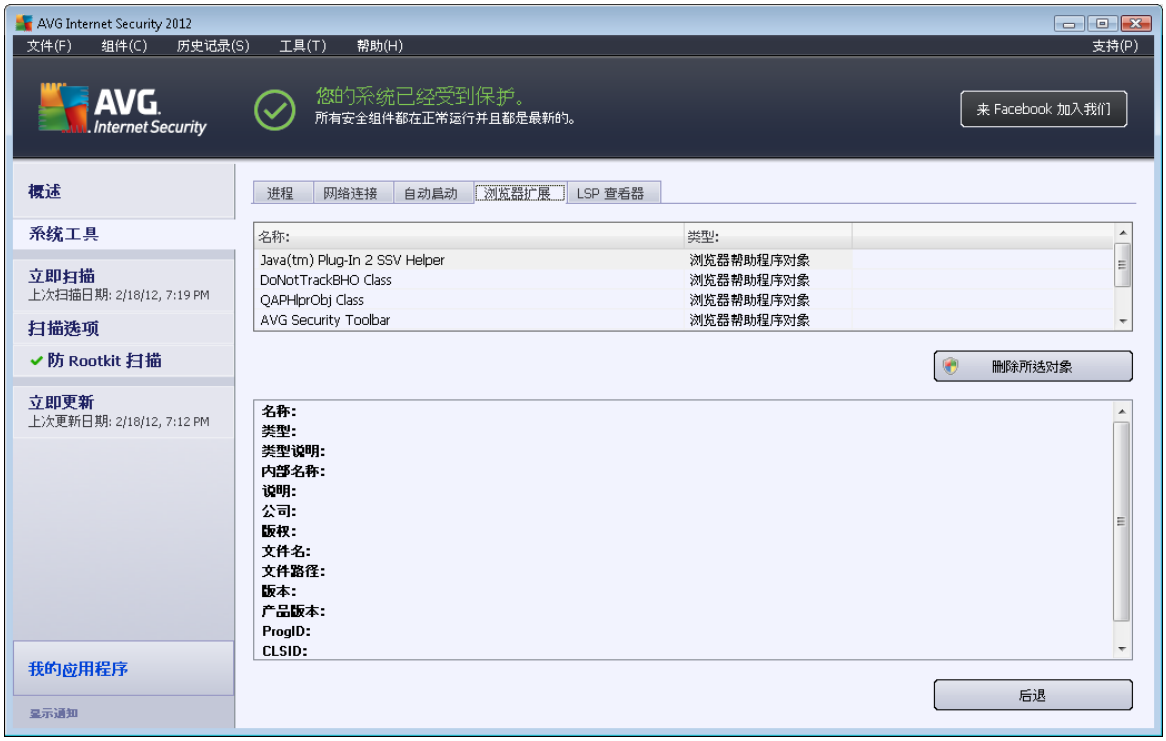
自动启动 选项卡中有如下控制按钮：

- ***删除所选内容*** - 按此按钮可删除一个或多个所选条目。
- ***后退*** - *用于切换回默认的* AVG 主对话框 组件概览）

强烈建议不要从此列表中删除任何应用程序，除非完全确定这些应用程序是真正的威胁！

2012 版权所有 AVG Technologies CZ, s.r.o. 保留所有权利。

6.6.4. 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。

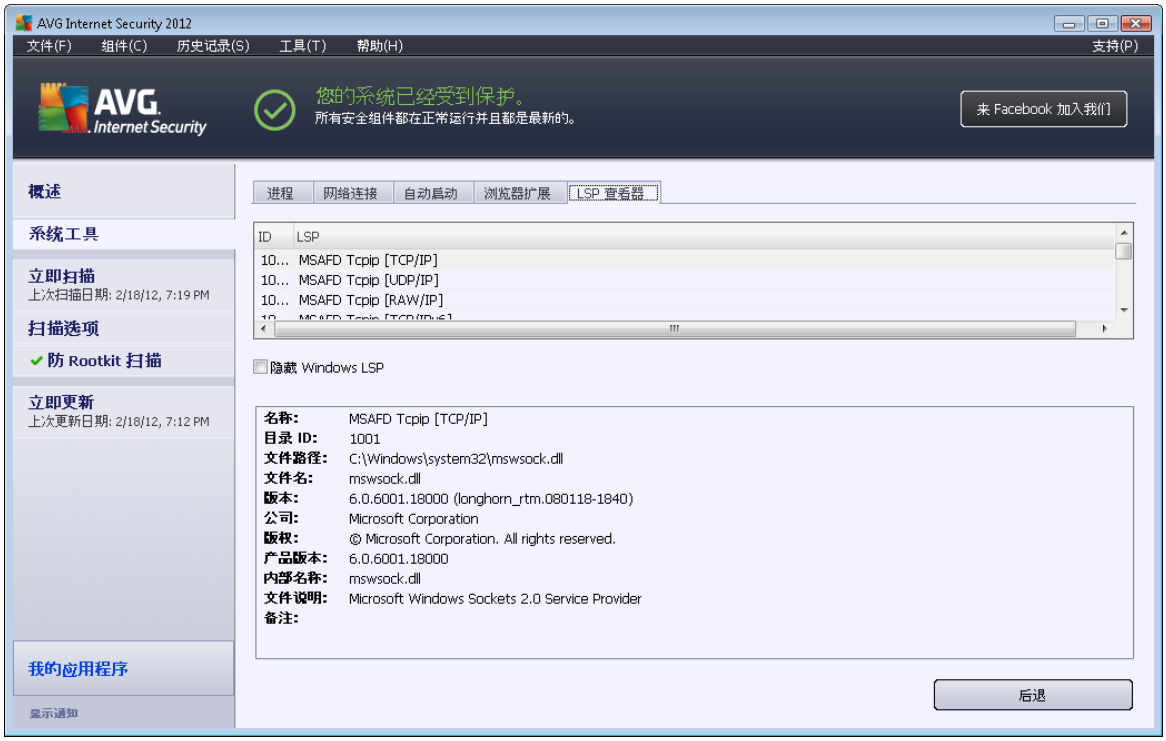
控制按钮

浏览器扩展 选项卡中有如下控制按钮：

- ***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*** - 用于切换回默认的 AVG 主对话框 *(组件概览)*。

2012 版权所有 AVG Technologies CZ, s.r.o. 保留所有权利。

6.6.5. 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。

控制按钮

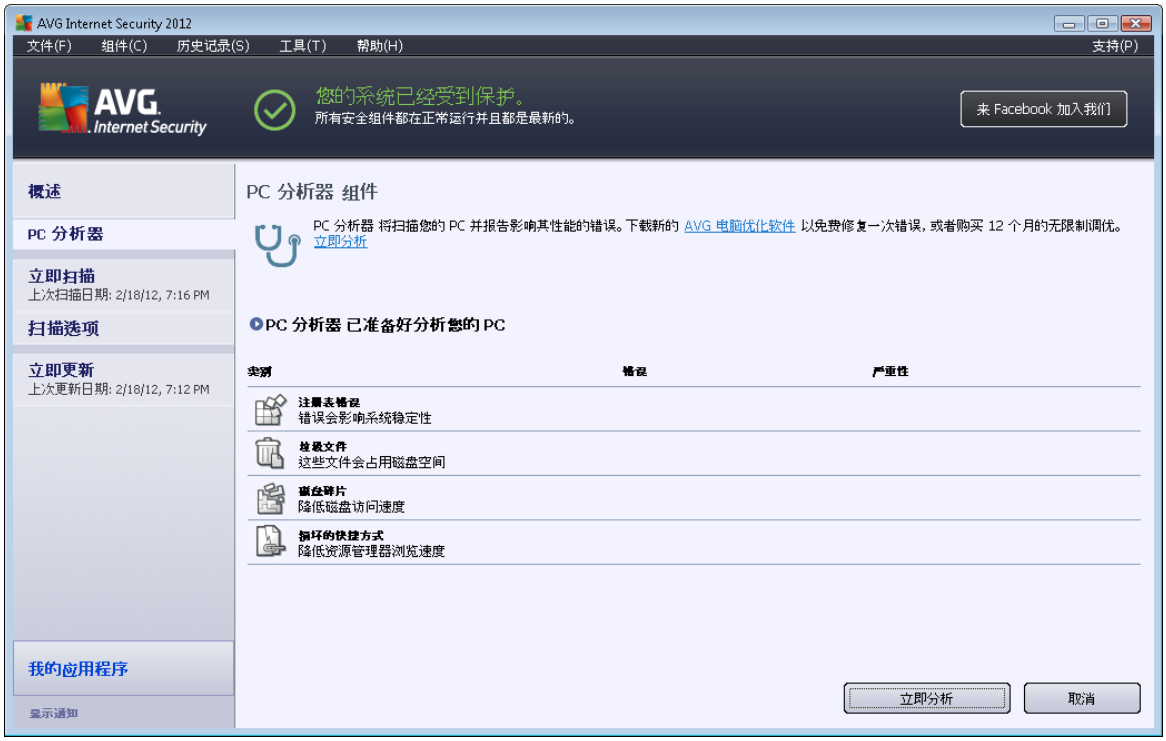
LSP 查看器 选项卡中有如下控制按钮：

- ***隐藏 Windows LSP*** - 要将 Windows LSP 添加到列表中，请取消选中此选项。
- ***后退*** - 用于切换回默认的 AVG 主对话框 (*组件概览*)。

6.7. 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：

2012 版权所有 AVG Technologies CZ, s.r.o. 保留所有权利。



- ***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*** - 可计算有碎片的硬盘空间 也就是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）的百分比。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：

2012 版权所有 AVG Technologies CZ, s.r.o. 保留所有权利。

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/) 上含有与 ***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 主对话框 (*组件概览*)

6.8. Identity Protection

Identity Protection 是一个防恶意软件组件，采用行为学技术为您抵御各种恶意软件 (*间谍软件、机器人、身份盗用等*)，并针对新的病毒提供零时差保护。***Identity Protection*** 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 或共享网络上运行的所有程序都正常运行。***Identity Protection*** 持续地识别和阻止可疑行为，并防止您的计算机受到所有新恶意软件侵害。

Identity Protection 可为您的计算机实时防范新威胁甚至不明威胁。Identity Protection 会监视所有进程 (*包括隐藏进程*) 以及超过 285 种不同的行为模式，并能够确定您的系统中是否已出现恶意行为。因此，Identity Protection 甚至可以发现尚未在病毒数据库中描述的威胁。有不明代码进入您的计算机时，Identity Protection 会立即监视其是否有恶意行为并对其进

行跟踪。如果发现是恶意文件，则 ***Identity Protection*** 会将此代码移入病毒库，并撤消对系统所作的任何更改 *（注入代码、更改注册表、打开端口等）*。无须启动扫描即可得到保护。该技术具有很强的前瞻性，很少需要更新，并且始终处于警戒状态。

Identity Protection 保护措施可以完善 Anti-Virus。强烈建议安装这两种组件以便对 PC 实施全面保护。

6.8.1. Identity Protection 界面

Identity Protection 对话框简要说明了该组件的基本功能、其状态 *（已激活）*以及某些统计数据：

- ***已删除威胁项目*** - 用于提供经检测而被认定为恶意软件并被删除的应用程序数量
- ***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。

基本 Identity Protection 设置

在该对话框的底部，可编辑该组件的功能的一些基本特性：

- ***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

2012 版权所有 AVG Technologies CZ, s.r.o. 保留所有权利。

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：

- ***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。*)
- ***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
- ***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

- ***高级设置...*** - 单击此链接可重定向到高级设置**AVG Internet Security 2012**中的相应对话框。从中可详细编辑该组件的配置。但请注意，已设置所有组件的默认配置以便**AVG Internet Security 2012**的性能和安全性达到最佳程度。除非确实有理由如此，否则建议保留默认配置！

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作的所有更改
- ***取消*** - 按此按钮可返回到默认的 AVG 主对话框（*组件概览*）

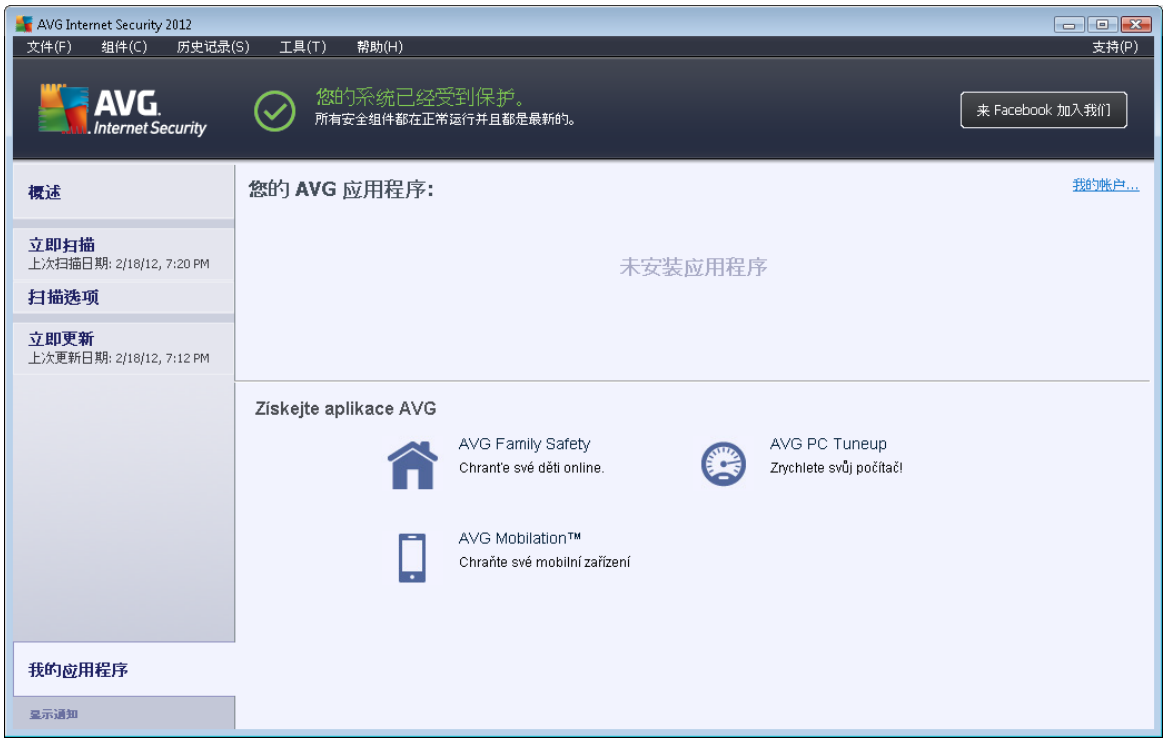
6.9. Remote Administration

如果已安装产品的 Business Edition，则 ***Remote Administration*** 组件仅会显示在 **AVG Internet Security 2012** 用户界面中 *有关用于安装的许可证的信息，请参见信息对话框的版本选项卡，您可以通过支持系统菜单项打开该对话框*）。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挡。该文档可在 AVG 网站 (http://www.avg.com/) 上的***支持中心/下载/文档*** 部分下载。

 2012 版权所有 AVG Technologies CZ, s.r.o. 保留所有权利。

7. 我的应用程序

我的应用程序对话框 *(可直接在 AVG 主对话框中通过 我的应用程序 按钮访问)*概述了已在计算机上安装或将要有选择性地准备安装的 AVG 独立应用程序：



此对话框分为两部分：

- ***您的 AVG 应用程序*** - 概述了已在计算机上安装的所有 AVG 独立应用程序；
- ***获取 AVG 应用程序*** - 概述了您可能会感兴趣的 AVG 的独立应用程序。这些程序已准备好安装。根据您的许可证、位置和其它标准提供动态更改。有关这些应用程序的详细信息，请参见 AVG 网站 (http://www.avg.com/)。

所有可用应程序的概述及其功能的简要说明如下：

7.1. AVG 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。***AVG Family Safety*** 使用击键技术监控您的孩子在聊天室和社交网络上的活动。如果它检测到用于在线欺骗儿童的词语、短语或语言，系统将立即通过短信或电子邮件通知您。该应用程序可对每个孩子设置相应的保护级别，通过不同的用户登录分别对其进行监控。

有关详细信息，请访问专用 AVG 网页，也可从中直接下载该组件。要访问该网页，可使用我的应用程序对话框中的 AVG Family Safety 链接。

2012 版权所有 AVG Technologies CZ, s.r.o. 保留所有权利。

7.2. AVG LiveKive

AVG LiveKive 专用于在受保护服务器中进行在线数据备份。***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。***AVG LiveKive*** 包括以下功能：

- 应对计算机和/或硬盘损坏的一项安全措施
- 通过连接到 Internet 的任何设备均可访问您的数据
- 易于整理
- 与经过您授权的每个人共享

对于详细信息，请访问专用 AVG 网页，也可从中直接下载该组件。要访问该网页，可使用我的应用程序对话框中的 AVG LiveKive 链接。

7.3. AVG Mobilation

AVG Mobilation 保护您的手机免受病毒和恶意软件的侵害，同时也在您想要隔断此类情况时提供远程跟踪智能手机的能力。***AVG Mobilation*** 功能包括：

- *File Scanner* 可对存储在不同的位置的文件启动安全扫描；
- *Task Killer* 可在设备变慢或卡住时停止应用程序；
- *App Locker* 可用密码锁定并保护一个或多个应用程序以防止滥用；
- *Tuneup* 可收集各种系统参数 *(电池容量、内存使用、应用程序安装大小和位置等)*。为单一中央视图以帮助您控制系统性能；
- *应用程序备份*可将应用程序备份到 SD 卡，以便以后恢复；
- *垃圾邮件和欺诈*功能让您将短信标记为垃圾邮件，以及将网站报告为欺诈网站；
- □□*删除个人数据*，以免您的电话被窃听；
- *安全网上冲浪*为您访问的网页提供实时监控。

有关详细信息，请访问专用 AVG 网页，也可从中直接下载该组件。要访问该网页，可使用我的应用程序对话框中的 AVG Mobilation 链接。

 2012 版权所有 AVG Technologies CZ, s.r.o. 保留所有权利。

7.4. AVG PC Tuneup

AVG PC Tuneup 应用程序是一种用于进行详细系统分析和更正（关于如何提高计算机速度和整体性能）的高级工具。***AVG PC Tuneup*** 包括以下功能：

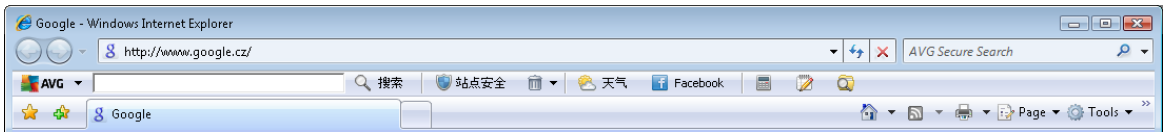
- Disk Cleaner - 用于删除致使计算机变慢的垃圾文件。
- Disk Defrag - 用于对磁盘驱动器进行碎片整理，以及优化系统文件位置。
- Registry Cleaner - 用于修复注册表错误以提高 PC 稳定性。
- Registry Defrag - 用于压缩注册表，从而消除耗费内存的空隙。
- Disk Doctor - 用于查找并修复坏扇区、丢失的簇和目录错误。
- Internet Optimizer - 用于定制特定 Internet 连接的不分大小的设置。
- Track Eraser - 用于删除计算机和 Internet 使用情况历史记录。
- Disk Wiper - 用于消除磁盘可用空间中的信息，以防恢复敏感数据。
- File Shredder - 用于清除磁盘或 U 盘中的所选文件，使其无法恢复。
- File Recovery - 用于从磁盘、U 盘或相机中恢复意外删除的文件。
- Duplicate File Finder - 用于查找和删除浪费磁盘空间的重复文件。
- Services Manager - 用于禁用已使计算机变慢的多余服务。
- Startup Manager - 用户用其可管理引导 Windows 时自动启动的程序。
- Uninstall Manager - 用于彻底卸载不再需要的软件程序。
- Tweak Manager - 用户用其可调整数百项隐藏 Windows 设置。
- Task Manager - 用于列出所有正在运行的进程、服务和已锁定文件。
- Disk Explorer - 用于显示那些所占计算机空间最大的文件。
- System Information - 用于提供有关已安装好的软硬件的详细信息。

有关详细信息，请访问专用 AVG 网页，也可从中直接下载该组件。要访问该网页，可使用[我的应用程序](#)对话框中的 AVG PC Tuneup 链接。

 2012 版权所有 AVG Technologies CZ, s.r.o. 保留所有权利。

8. AVG Security Toolbar

AVG Security Toolbar 是一种可与 LinkScanner 组件紧密协同运行的工具，还可在浏览 Internet 时最大程度地保护用户的安全。可有选择性地在 **AVG Internet Security 2012** 中安装 ***AVG Security Toolbar***；在安装过程中，会请用户决定是否要安装该组件。***AVG Security Toolbar*** 能直接在 Internet 浏览器中使用。目前，受支持的 Internet 浏览器包括 Internet Explorer（*6.0 和更高版本*）和/或 Mozilla Firefox（*3.0 和更高版本*）。其它浏览器都不受支持（*如果使用的是某种备选的 Internet 浏览器（如 Avant Browser），则可能会遇到意外情况*）。



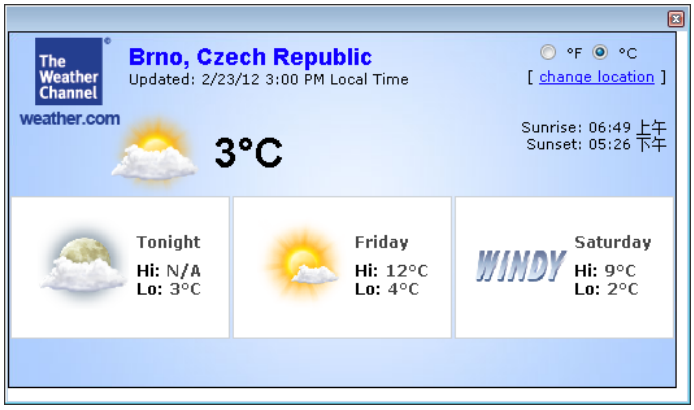
AVG Security Toolbar 由以下部分组成：

- ***带下拉菜单的 AVG 徽标***：
  - ***使用 AVG Secure Search*** - 用其可通过 ***AVG Secure Search*** 引擎直接在 ***AVG Security Toolbar*** 中进行搜索。所有搜索结果都会受到 Search-Shield 服务的持续检查，用户上网时可以高枕无忧。
  - ***当前威胁级别*** - 用于打开病毒实验室网页，其中以图形方式显示着网上的当前威胁级别。
  - ***AVG Threat Labs*** - 用于打开特定的 ***AVG Threat Lab*** 网站（*http://www.avgthreatlabs.com*），您可在这里找到有关各种网站安全和当前网上的威胁级别的信息。
  - ***Toolbar 帮助*** - 用于打开在线帮助，其中有全部 ***AVG Security Toolbar*** 功能的说明。
  - ***提交产品反馈*** - 用于打开其中有可以填写的表单的网页，然后请将您对 ***AVG Security Toolbar*** 的感觉告诉我们。
  - ***关于...*** - 用于打开一个新窗口，其中有关于目前已安装好的 ***AVG Security Toolbar*** 的版本的信息。
- ***搜索字段***- 用于通过 ***AVG Security Toolbar*** 搜索 Internet，以保证绝对安全舒适，因为显示出来的搜索结果百分百安全。请将关键字或短语填入搜索字段，然后按 ***Search*** 按钮（*或 Enter*）。所有搜索结果都会受到 Search-Shield 服务的持续检查（*在 LinkScanner 组件中*）。
- ***站点安全*** - 此按钮打开一个新对话框，上面提供有关您正访问的页面的当前威胁级别（*当前是安全的*）的信息。简短概述可展开，并在浏览器窗口显示与右边页面相关的所有安全活动的完整详细信息（*查看完整报告*）：

2012 版权所有 AVG Technologies CZ, s.r.o. 保留所有权利。

- ***删除*** - 垃圾箱 按钮提供下拉菜单，您可以在其中选择是否要删除有关浏览、下载、在线表单的信息，或一次删除所有搜索历史的信息。

- ***天气*** - 该按钮用于打开一个新对话框，显示有关用户本地目前的天气状况的信息，以及未来两天的天气预报。天气信息会定期更新，每 3-6 小时更新一次。在该对话框中，可手动更改所要查看的地点，还可以决定是要以摄氏度还是华氏度为单位查看气温信息。



- ***Facebook*** 用此按钮可直接在 AVG Security Toolbar 中连接到 ***Facebook*** 社交网络。

- 用于快速使用这些应用程序的快捷按钮包括：***计算器***、***记事本***、***Windows 资源管理器***.

 2012 版权所有 AVG Technologies CZ, s.r.o. 保留所有权利。

9. AVG Do Not Track

AVG Do Not Track 可帮助您识别收集有关您在线活动的数据的网站。浏览器中的某个图标可向您显示收集有关您活动的网站或广告商，并让您选择将其允许或禁止。

- ***AVG Do Not Track*** 为您提供有关每个相应服务的隐私政策及选择退出该服务的直接链接的更多信息（如果可用）。
- 此外，***AVG Do Not Track*** 支持使用 W3C DNT 协议自动通知您不想要被追踪的那些站点。默认情况下已启用该通知，但可随时进行更改。
- ***AVG Do Not Track*** 根据以下条款和条件提供。
- ***默认情况下已启用 AVG Do Not Track***，但可随时轻松将其禁用。可在常见问题解答的禁用 AVG Do Not Track 功能一章中找到说明。
- 有关 ***AVG Do Not Track*** 的更多信息，请访问我们的网站。

目前，***AVG Do Not Track*** 功能在 Mozilla Firefox、Chrome 和 Internet Explorer 浏览器中受支持。*（在 Internet Explorer 中，AVG Do Not Track 图标位于命令栏的右侧。如果在通过浏览器默认设置查看 AVG Do Not Track 图标时遇到一些问题，请确保您已激活命令栏。如果您仍看不到图标，请将命令栏拖动到左边以显示此工具栏中提供的所有图标和按钮）。*

9.1. AVG Do Not Track 界面

当在线时，只要一检测到任何类型的数据收集活动，***AVG Do Not Track*** 就会对您发出警告。您将会看到以下对话框：

 2012 版权所有 AVG Technologies CZ, s.r.o. 保留所有权利。

所有检测到的数据收集服务已按名称列在***本页的跟踪器***概览中。以下是 ***AVG Do Not Track*** 识别的三类数据收集活动：

- ***Web Analytics*** *（默认情况下已允许）*：用于改善相应网站的性能和体验的服务。在此类中，您可找到 Google Analytics、Omniture 或 Yahoo Analytics 之类的服务。我们建议您不要阻止 web analytics 服务，因为该网站可能不会像您想像那样工作。

- ***Social Buttons*** *（默认情况下已允许）*：专为提高社交网络体验而设计的组件。Social buttons 的服务范围从您的社交网站到您正访问的站点不等。它们可收集有关您登录时的在线活动。Social buttons 的例子包括 Facebook Social Plugins、Twitter Button、Google +1 等。

- ***Ad Networks*** *（默认情况下已阻止某些 Ad networks）*：用来直接或间接收集或者共享有关您在多个站点的在线活动的数据，为您提供不同于基于内容的 Ad 的个性化 Ad 的服务。根据其网站上的每个 Ad networks 提供的隐私政策来确定该服务。默认情况下，已阻止某些 Ad networks。

注意：*根据网站后台中运行的服务，以上三项描述部分的某一项可能不会出现在 AVG Do Not Track 对话框中。*

该对话框还包含两个超链接：

- ***什么是跟踪？*** - 单击该对话框上部的此链接，以重定向到提供有关跟踪原理的详细解释和特定跟踪类型的说明的专用网页。

- ***设置*** - 单击该对话框底部的此链接，以重定向到可在其中设置各种 ***AVG Do Not Track*** *参数特定配置的专用网页（有关详细信息，请参见 AVG Do Not Track 设置一章）*

9.2. 有关跟踪进程的信息

检测到的数据收集服务的列表仅提供特定服务的名称。要确切决定有关是否阻止或允许相应服务，您可能需要了解更多信息。在相应的列表项中移动鼠标。将会出现信息气球，上面提供了有关该服务的详细数据。您将会了解到该服务是收集个人数据还是其他可用数据；数据是否与其他第三方主体进行共享，所收集的数据是否进行存档以用于进一步的可能使用。

在信息气球的底部，您可以看到***隐私政策***超链接，可将您重定向到相应的检测服务的隐私政策专用网站。

 2012 版权所有 AVG Technologies CZ, s.r.o. 保留所有权利。

9.3. 阻止跟踪进程

通过列出所有 Ad Networks/Social Buttons/Web Analytics，现在您可以选择控制应阻止的服务。您可以选择以下两种方式：

- ***全部阻止*** - 单击位于该对话框底部的此按钮，以表明您不想要任何数据收集活动。*（但请记住，此操作可能会中断该服务正在该服务运行的相应网站中的运行！）*
- - 如果您不想一次阻止所有检测到的服务，则可以指定是否应分别允许或阻止该服务。允许运行某些检测到的系统 *（例如，Web Analytics）*.这些系统采用收集到的数据优化其自身网站，并通过此方法为所有用户改进常见的 Internet 环境。但同时，您可以阻止划分为 Ad Networks 的所有进程的数据收集活动。只需单击 相应服务旁的图标就可阻止数据收集 *（进程名将以划线的形式显示）*，或再次允许数据收集。

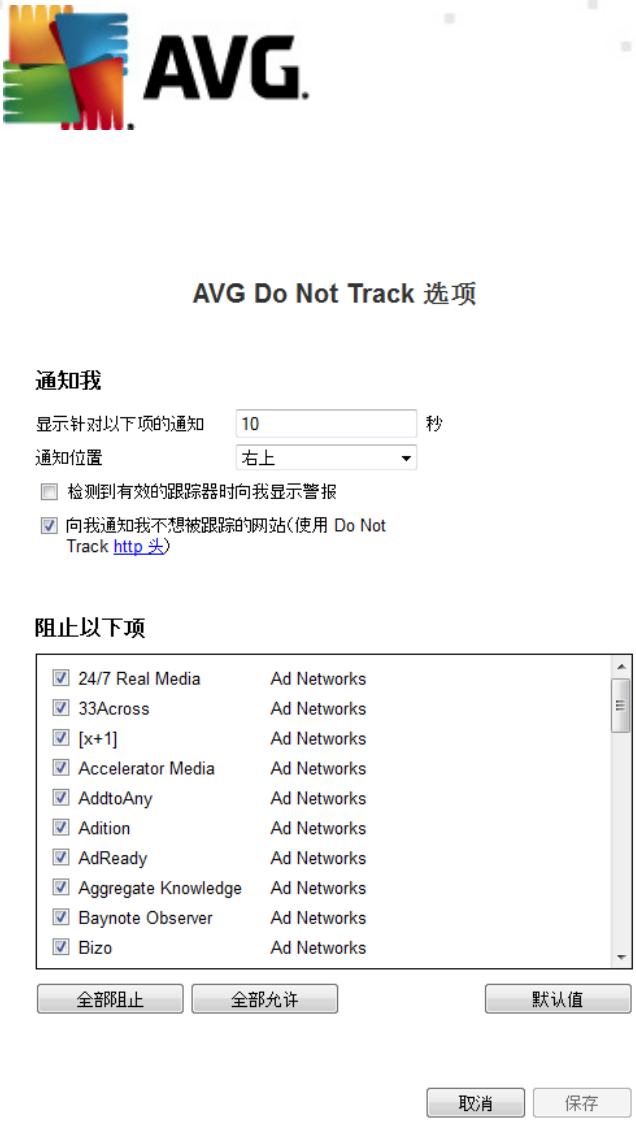
 2012 版权所有 AVG Technologies CZ, s.r.o. 保留所有权利。

9.4. AVG Do Not Track 设置

在 ***AVG Do Not Track*** 对话框中，只有一个配置选项：在该对话框的底部，您可以看到***检测到有效的跟踪器时向我显示警报***复选框。默认情况下，此项未选中。选中此复选框以确认，在您每次进入包含尚未受阻止的新数据收集服务的网页时都要通知您。选中之后，如果 ***AVG Do Not Track*** 在您当前访问的页面上检测到新数据收集服务，则屏幕上会出现通知对话框。否则，您只可以通过 ***AVG Do Not Track*** 图标 *位于浏览器的命令栏中*）从绿色变为黄色时通知您新检测到的服务。

但在 ***AVG Do Not Track*** 对话框底部，您可以找到***设置***链接。单击该链接以重定向到专用网页，您可以在此指定详细的 ***AVG Do Not Track 选项***：

 2012 版权所有 AVG Technologies CZ, s.r.o. 保留所有权利。



- ***通知位置*** *(默认情况下在右上方)* - 打开下拉菜单以指定您想要 ***AVG Do Not Track*** 对话框在您的监视器上出现的位置。
- ***显示通知的时间间隔*** *(默认情况下为 10)* - 在此字段中，您应决定您想要多长时间 *(以秒计)*在屏幕上看到 ***AVG Do Not Track*** 通知。您可以指定从 0 到 60 秒的数字范围 *(对于 0 秒，通知将不会出现在屏幕上)*。
- ***检测到有效的跟踪器时向我显示警报*** *(默认情况下已关闭)* - 选中此复选框以确认，在您每次进入包含尚未受阻止的新数据收集服务的网页时都要通知您。选中之后，如果 ***AVG Do Not Track*** 在您当前访问的页面上检测到新数据收集服务，则屏幕上会出现通知对话框。否则，您只可以通过 ***AVG Do Not Track*** 图标 *(位于浏览器的命令栏中)从绿色变为黄色时通知您新检测到的服务。*
- ***向我通知我不想被跟踪的网站*** *(默认情况下已启用)* - 选中此选项以确认您想要 ***AVG Do Not Track*** 通知检测到的数据收集服务提供商，您不想要被跟踪。
- ***阻止以下项*** *(默认情况下允许所有已列出的数据收集服务)* - 在此部分，您可以看到带有可划分为 Ad Networks 的已知数据收集服务列表的复选框。默认情况下，***AVG Do Not Track*** 会自动阻止某些 Ad 网络，它会让您决定是否也要阻止或允许其它 Ad 网络。要执行此操作，只需单击该列表下的***全部阻止***按钮。

控制按钮在 ***AVG Do Not Track 选项***页面中可用，如下所示：

 2012 版权所有 AVG Technologies CZ, s.r.o. 保留所有权利。

- ***全部阻止*** - 单击此按钮以一次阻止可划分为 Ad 网络的以上复选框中列出的所有服务。
- ***全部允许*** - 单击此按钮以一次取消阻止在以上复选框中列出且划分为 Ad 网络的所有以前阻止的服务；
- ***默认值*** - 单击此按钮以废弃您的所有自定义设置，并返回到默认配置；
- ***保存*** - 单击此按钮以应用并保存所有指定的配置；
- ***取消*** - 单击此按钮以取消先前指定的设置。

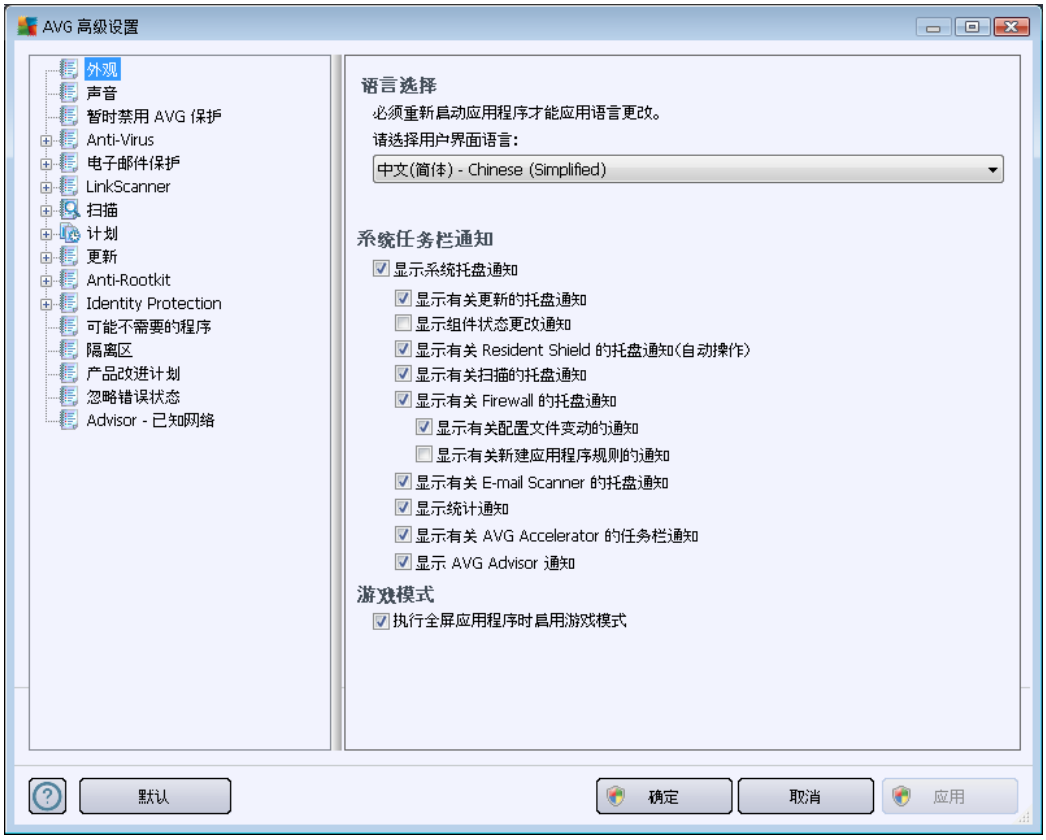
 2012 版权所有 AVG Technologies CZ, s.r.o. 保留所有权利。

10. AVG 高级设置

会在名为 ***"高级 AVG 设置"*** 的新窗口中打开 **AVG Internet Security 2012** 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。

10.1. 外观

导航树中的第一个选项 ***外观*** 有关 **AVG Internet Security 2012** 用户界面的常规设置，其中还有几个基本应用程序行为选项：



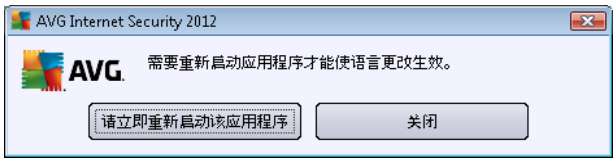
语言选择

在 ***语言选择*** 部分中，可从下拉菜单中选择所需语言。然后就会将所选语言应用于整个 **AVG Internet Security 2012** 用户界面。该下拉菜单中只有以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)* 和英语 *(默认情况下，始终都会自动安装英语)*。要完成 **AVG Internet Security 2012** 的语言切换，必须重新启动该应用程序。请按以下步骤操作：

- 在下拉菜单中，选择所需应用程序语言
- 通过按 ***应用*** 按钮 *(位于该对话框右下角)*

 2012 版权所有 AVG Technologies CZ, s.r.o. 保留所有权利。

- 按 ***确定*** 按钮确认
- 会弹出一个新对话框，告知必须重新启动 **AVG Internet Security 2012**
- 按 ***请立即重新启动该应用程序*** 按钮会同意重新启动该程序，然后等几秒钟，待语言更改生效：



系统任务栏通知

可在此部分中禁止显示有关 **AVG Internet Security 2012** 应用程序状态的系统任务栏通知。默认情况下允许显示系统通知。强烈建议保留此配置！例如，会就扫描或更新进程的启动，或者 **AVG Internet Security 2012** 组件的状态变动发出系统通知。应该一定注意这些通知！

但是，如果出于某种原因不想以这种方式得到通知，或者只想查看某些通知 *（与特定 AVG Internet Security 2012 组件有关）*，则可通过选中/取消选中以下选项定义并指定使用偏好：

- ***显示系统托盘通知*** *（默认情况下已启用）*- 默认情况下会显示所有通知。取消选中此项可彻底禁止显示所有系统通知。启用此项后，可进一步选择要显示什么特定通知：
  - ***显示有关更新的托盘通知*** *（默认情况下已启用）*- 用于决定是否要显示有关 **AVG Internet Security 2012** 更新过程的启动、进度和完成情况的信息。
  - ***显示组件状态更改通知*** *（默认情况下已禁用）*- 用于决定是否要显示有关组件的活动/不活动状态或其潜在问题的信息。报告组件的故障状态时，此选项相当于系统任务栏图标的通知功能，用于报告任何 **AVG Internet Security 2012** 组件的问题。
  - ***显示有关 Resident Shield 的托盘通知(自动操作)*** *（默认情况下已启用）*- 用于决定是要显示还是禁止显示有关文件保存、复制和打开过程的信息 *（仅当已启用 Resident Shield 自动修复选项时才会显示此配置）*。
  - ***显示有关扫描的托盘通知*** *（默认情况下已启用）*- 用于决定是否要显示有关计划内扫描的自动启动、进度和结果的信息。
  - ***显示有关 Firewall 的托盘通知*** *（默认情况下已启用）*- 用于决定是否要显示有关 Firewall 状态和进程的信息，如该组件的启用/停用警告、潜在网传信息受阻等信息。此选项多出了两个具体选项 *（对于其中每个选项的详细说明，请查阅本文档的 Firewall 一章）*：
    - ***显示有关配置文件变动的通知*** *（默认情况下已启用）*- 用于就 Firewall 配置文件的自动更改发出通知。

 2012 版权所有 AVG Technologies CZ, s.r.o. 保留所有权利。

- ***显示有关新建应用程序规则的通知*** *(默认情况下已启用)* - 对于新应用程序，用于根据安全列表就Firewall 规则的自动创建发出通知。

- ***显示有关 E-mail Scanner 的托盘通知*** *(默认情况下已启用)* - 用于决定是否要在扫描所有传入和传出电子邮件时显示信息。

- ***显示统计通知*** *(默认情况下已启用)* - 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。

- ***显示有关 AVG Accelerator 的托盘通知*** *(默认情况下已启用)* - 用于决定是否要在执行 ***AVG Accelerator*** 活动时显示信息。通过 ***AVG Accelerator*** 服务可使在线视频播放更加流畅，还可使后续下载更加容易。

- ***显示 AVG Advice 运行状况通知*** *(默认情况下已启用)* - ***AVG Advice*** 会监视受支持的 Internet 浏览器 *(Internet Explorer、Chrome、Firefox、Opera 和 Safari)* 的运行状况，如果浏览器所占用的内存量超过推荐量，还会发出通知。这种情况下，计算机速度可能会大幅减慢，建议重新启动 Internet 浏览器加快其进程的速度。保持***显示 AVG Advice 运行状况通知*** 选项的已启用状态，即可得到通知。

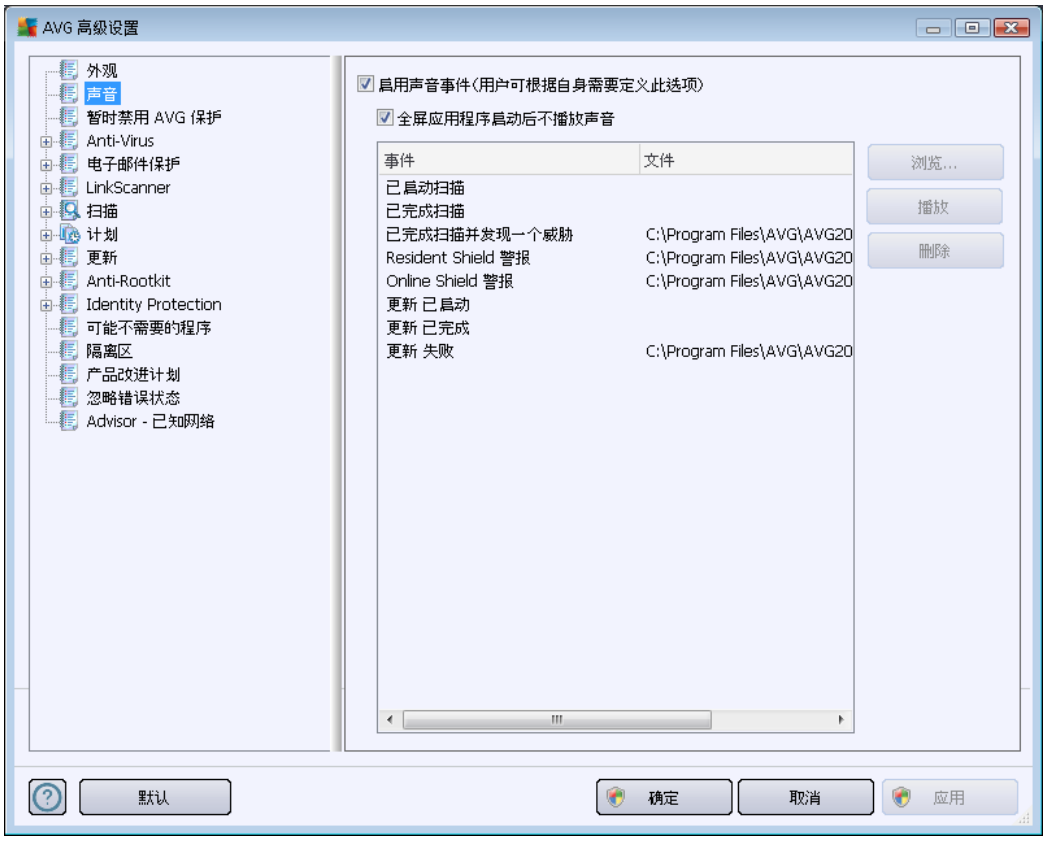
游戏模式

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)*。

2012 版权所有 AVG Technologies CZ, s.r.o. 保留所有权利。

10.2. 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 Internet Security 2012** 操作的情况：



这些设置仅对当前用户帐户有效，也就是说，计算机上的每个用户都可以拥有各自的声音设置。如果要允许发出声音通知，请保持***启用声音事件*** 选项 *(该选项默认情况下已启用)* 的选中状态，以启用所有相关操作的列表。此外，还可能需要选中***全屏应用程序启动后不播放声音*** 选项，才能在发出声音通知可能会打扰用户的情况下禁止发出这种通知 *(另请参见高级设置/外观一章的 游戏模式 一节)*。

控制按钮

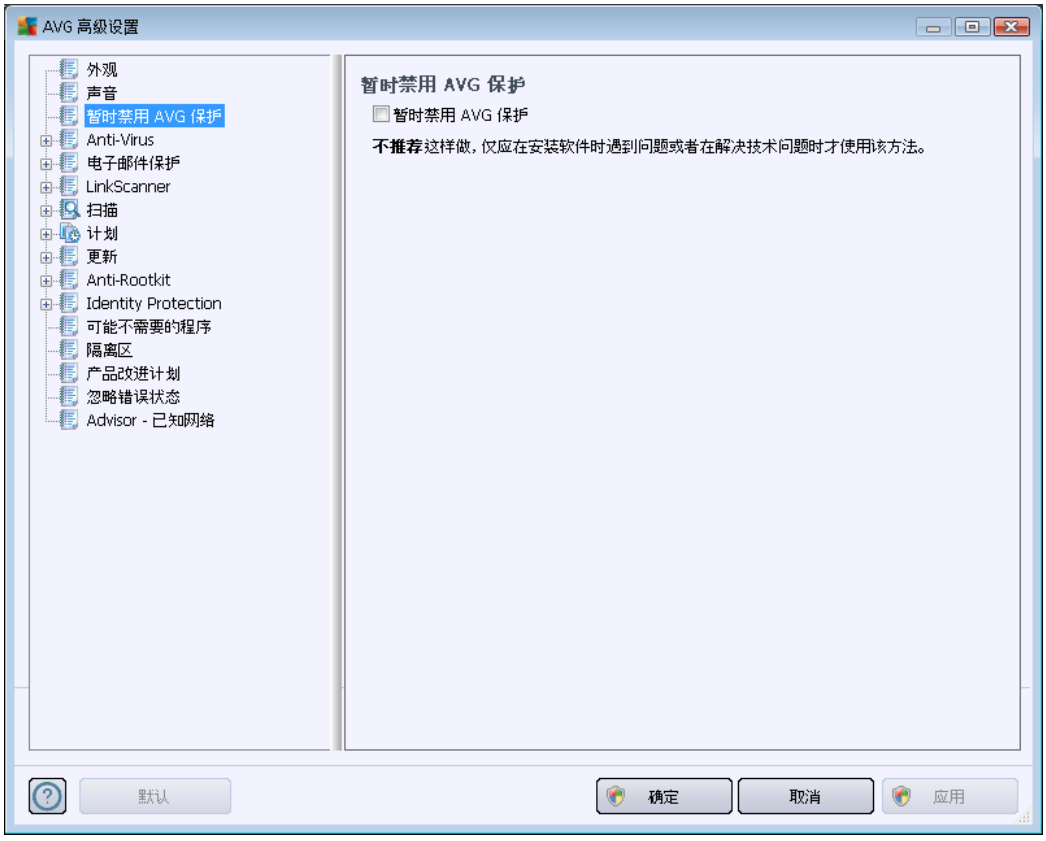
- ***浏览*** - 从列表中选择相应事件后，可用***浏览*** 按钮在磁盘中搜索要对其指定的所需声音文件。 *(请注意，目前仅支持 *.wav 声音文件！)*
- ***播放*** - 要听一下所选的声音，请突出显示此列表中的相应事件，然后按***播放*** 按钮。
- ***删除*** - 可用***删除*** 按钮删除为特定事件指定的声音。

2012 版权所有 AVG Technologies CZ, s.r.o. 保留所有权利。

10.3. 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 2012** 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 Internet Security 2012**，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，要尽量先停用常驻保护措施（*启用 Resident Shield*）。如果必须暂时禁用 **AVG Internet Security 2012**，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。

如何禁用 AVG 保护软件

- 请选中 ***暂时禁用 AVG 保护*** 复选框，然后通过按 ***应用*** 按钮确认所作的选择
- 在新打开的 ***暂时禁用 AVG 保护*** 对话框中，指定要禁用 **AVG Internet Security 2012** 多长时间。默认情况下会将该保护软件禁用 10 分钟，此段时间应足以完成任何常见任务，例如安装新软件等。请注意，可设置的初始时间限值是 15 分钟，不能出于安全原因而用自己的值替换该值。指定的禁用时段过后，会自动再次启动所有已停用的组件。

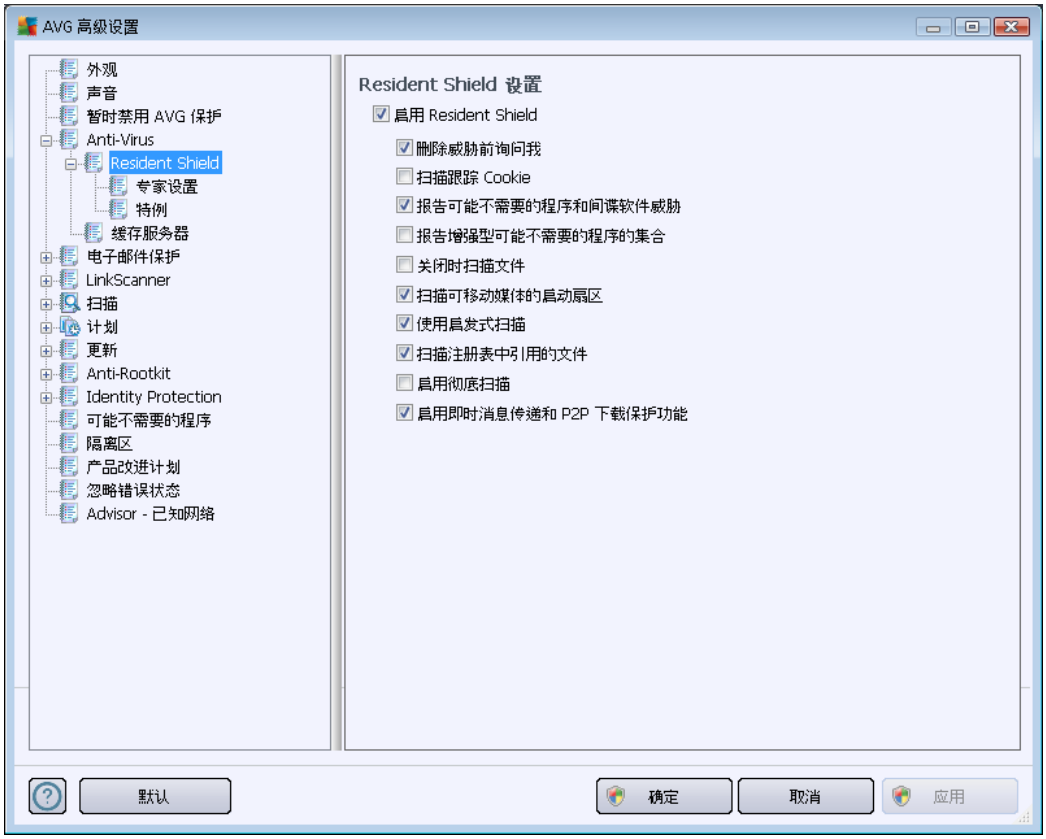
 2012 版权所有 AVG Technologies CZ, s.r.o. 保留所有权利。

10.4. Anti-Virus

Anti-Virus 组件用于持续保护您的计算机以免受到所有已知类型的病毒和间谍软件 *包括所谓的休眠和非活动恶意软件，即已下载但尚未激活的恶意软件）的侵害。*

10.4.1. Resident Shield

Resident Shield 用于实时防止文件和文件夹受到病毒、间谍软件及其它恶意软件的侵害。



 2012 版权所有 AVG Technologies CZ, s.r.o. 保留所有权利。

在 ***Resident Shield 设置*** 对话框中，您可以通过选中或取消选中***启用 Resident Shield*** 选项（*默认情况下此选项已启用*）来彻底激活或停用常驻保护措施。此外，还可选择应该激活常驻保护措施的哪些特性：

- ***删除威胁前询问我***（*默认情况下已启用*）- 选中此框以确保 Resident Shield 将不会自动执行任何操作；但将显示描述所检测威胁的对话框，让您决定应采取何种操作。如果将此框保留为未选中状态，**AVG Internet Security 2012**将自动修复感染；如果无法修复，则将该对象移动到病毒库。

- ***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：程序直接从制造商获得后极其安全而无害，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）被打开和关闭时对其进行扫描；此特性有助于防止计算机受到某些类型的复杂病毒的侵害

- ***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*）

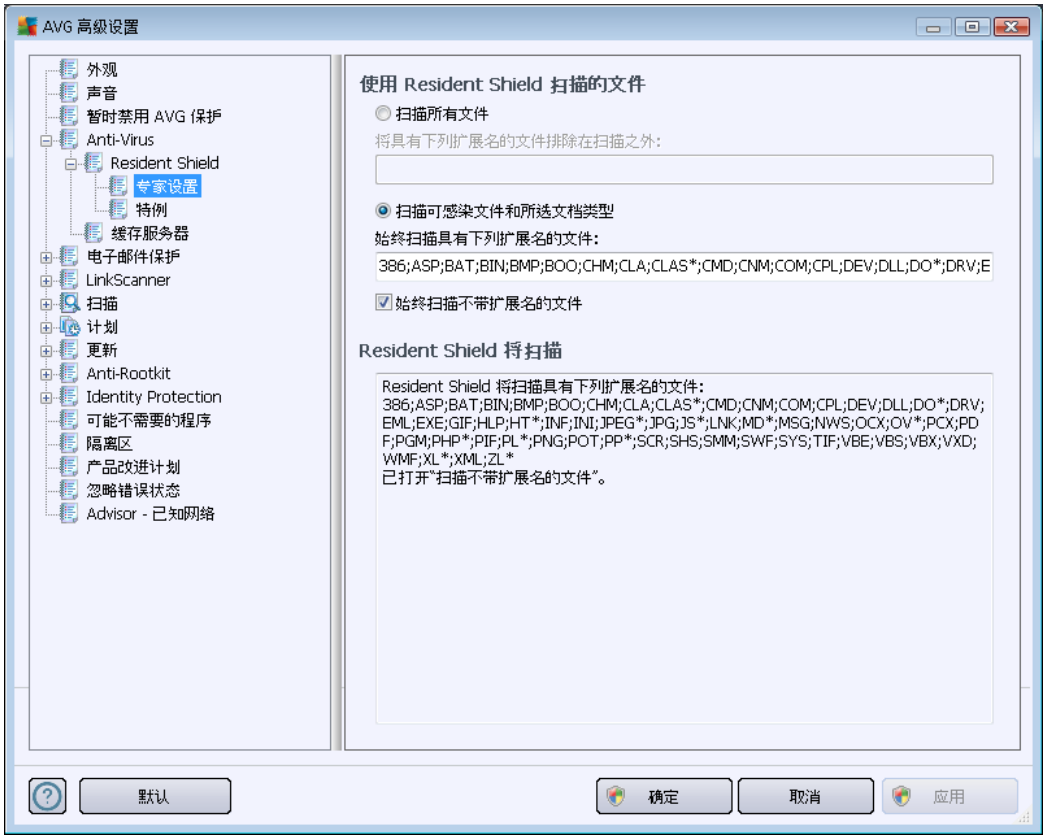
- ***扫描注册表中引用的文件***（*默认情况下已启用*）- 此参数定义 AVG 将扫描添加到 Startup 注册表项的所有可执行文件，以避免在计算机下次启动时执行已知的感染。

- ***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。但要记住，此方法相当耗时。

- ***启用即时消息传递和 P2P 下载保护功能***（*默认情况下已启用*）- 如果要验证即时消息传递通讯（*如 ICQ、MSN Messenger……*）和 P2P 下载是否没有病毒，请选中此选项。

2012 版权所有 AVG Technologies CZ, s.r.o. 保留所有权利。

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*）：

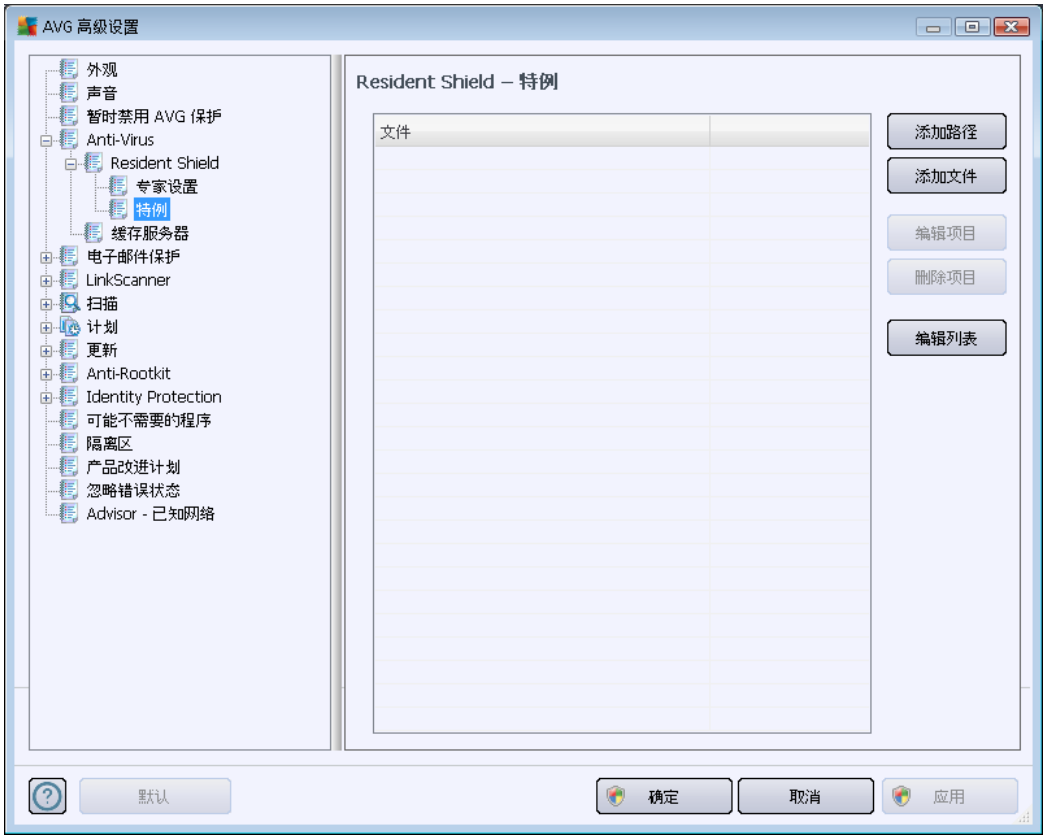


选中相应复选框可决定是要***扫描所有文件*** 还是要仅***扫描易受感染的文件和所选文档类型***。如果已决定使用第二个选项，则可以进一步指定一个扩展名列表，以指定要排除在扫描范围之外的文件，还可以指定另一个文件扩展名列表，以指定所有情况下都必须扫描的文件。

选中***始终扫描不带扩展名的文件***（*默认情况下已启用该选项*）以确保，即使文件没有扩展名且格式未知，Resident Shield 也应当对其进行扫描。建议始终打开此功能，因为没有扩展名的文件十分可疑。

下方名为 ***Resident Shield 将扫描*** 的部分用于对当前设置作进一步汇总，显示的是 ***Resident Shield*** 实际扫描内容的详细综览。

2012 版权所有 AVG Technologies CZ, s.r.o. 保留所有权利。



可通过 ***Resident Shield - 特例*** 对话框指定要排除在 ***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！

控制按钮

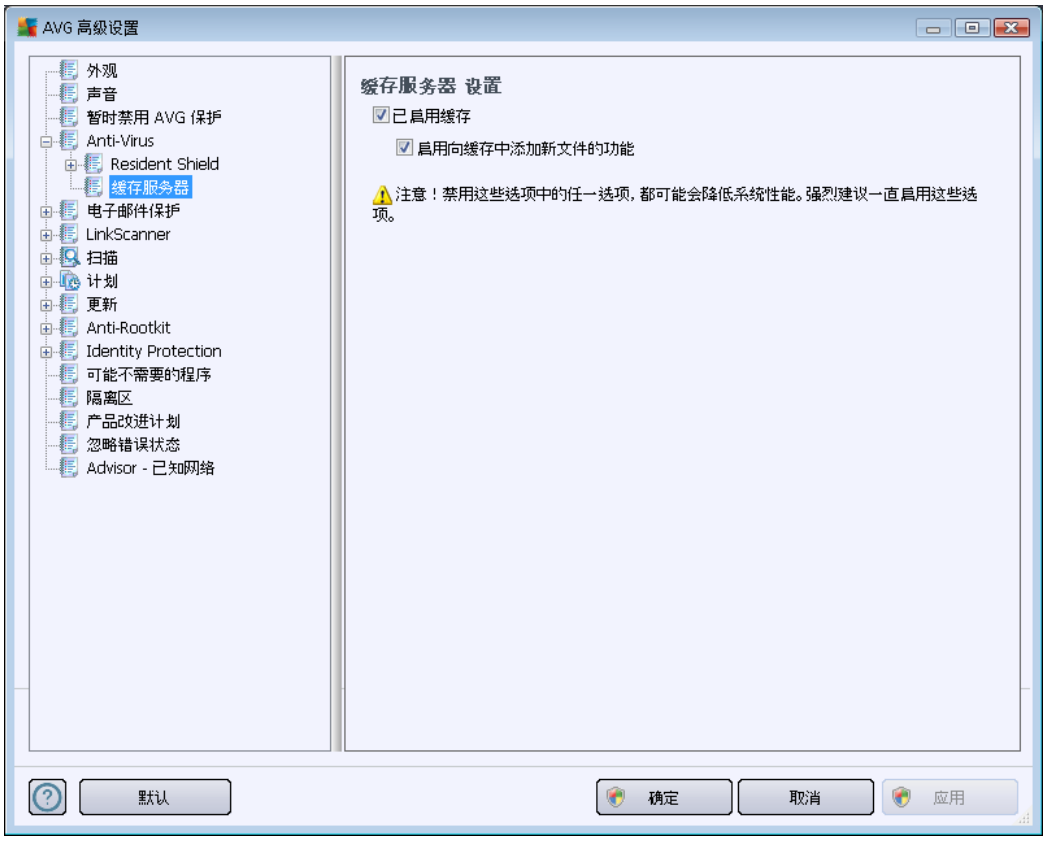
此对话框提供了以下控制按钮：

- ***"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
- ***编辑列表*** - 用其可在新对话框（作用类似于标准文本编辑器）中编辑整个指定特例的列表

 2012 版权所有 AVG Technologies CZ, s.r.o. 保留所有权利。

10.4.2. 缓存服务器

关于缓存服务器进程的***缓存服务器设置***对话框旨在提高各类 **AVG Internet Security 2012** 扫描速度：



缓存服务器收集并保存有关可靠文件的信息 *(如果已用来源可靠的数字签名签署文件，则会认为文件可靠)*。然后就会自动认为这些文件安全，无须重新扫描；因此会在扫描过程中略过这些文件。

缓存服务器设置 对话框中有如下配置选项：

- ***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。

除非有正当理由禁用缓存服务器，否则强烈建议保留默认设置，并保持这两个选项的已启用状态！否则可能会遇到系统速度和性能大幅下降的情况。

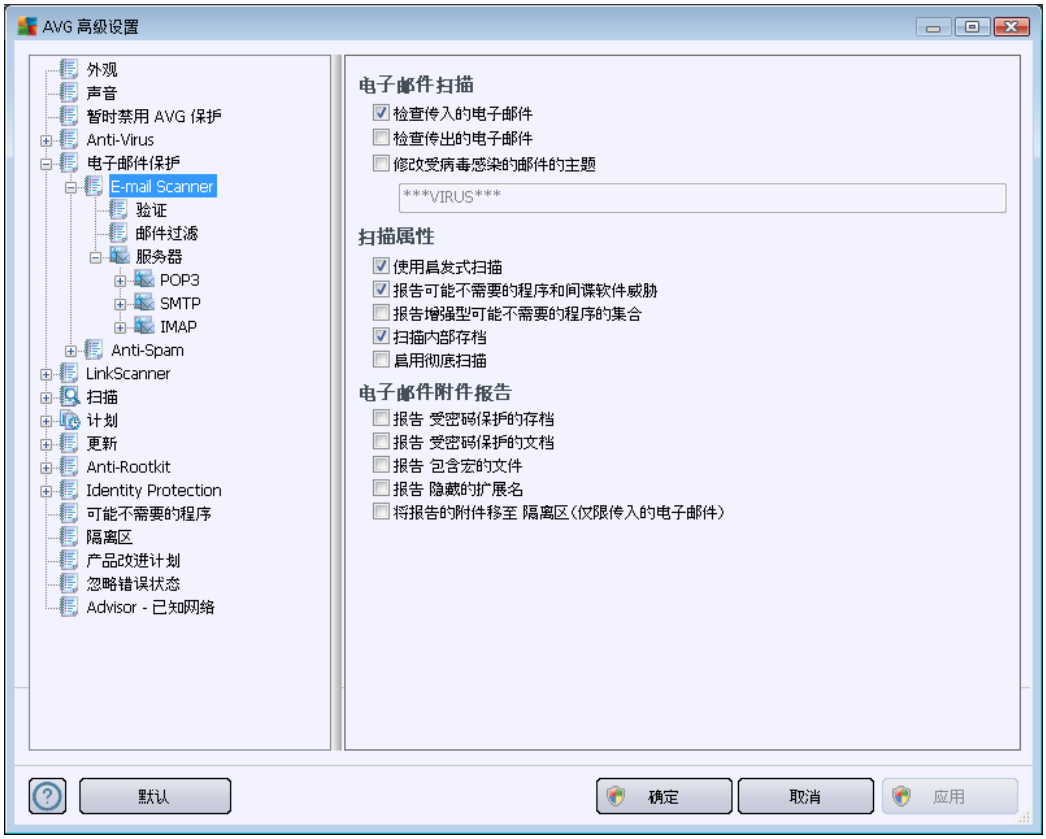
2012 版权所有 AVG Technologies CZ, s.r.o. 保留所有权利。

10.5. 电子邮件保护

在 ***电子邮件保护*** 部分中，可编辑 E-mail Scanner 和 Anti-Spam 的详细配置：

10.5.1. 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。

2012 版权所有 AVG Technologies CZ, s.r.o. 保留所有权利。

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

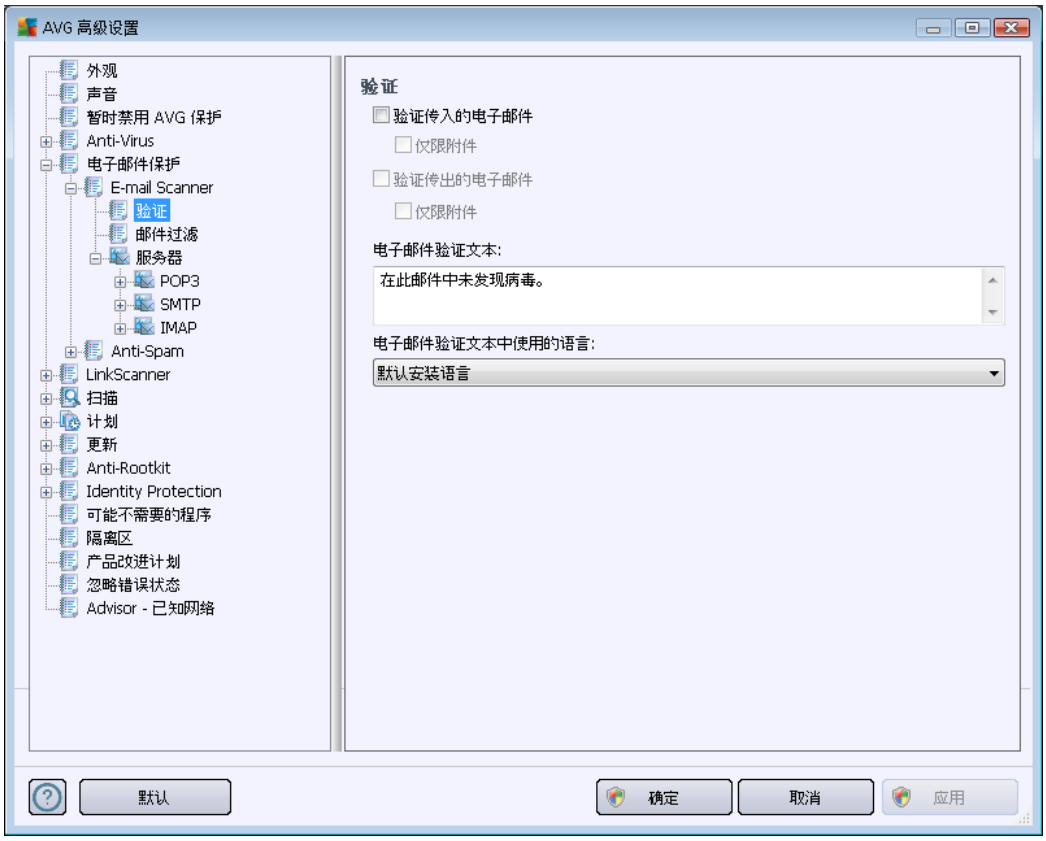
可在此部分中就有潜在危险或可疑的文件设置其它报告。请注意，不会显示警告对话框，而只是在电子邮件的末尾添加一段验证文本，所有此类报告都会列在"电子邮件扫描程序检测"对话框中：

- ***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（*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

 2012 版权所有 AVG Technologies CZ, s.r.o. 保留所有权利。

应将检测到的受感染对象移至病毒库。

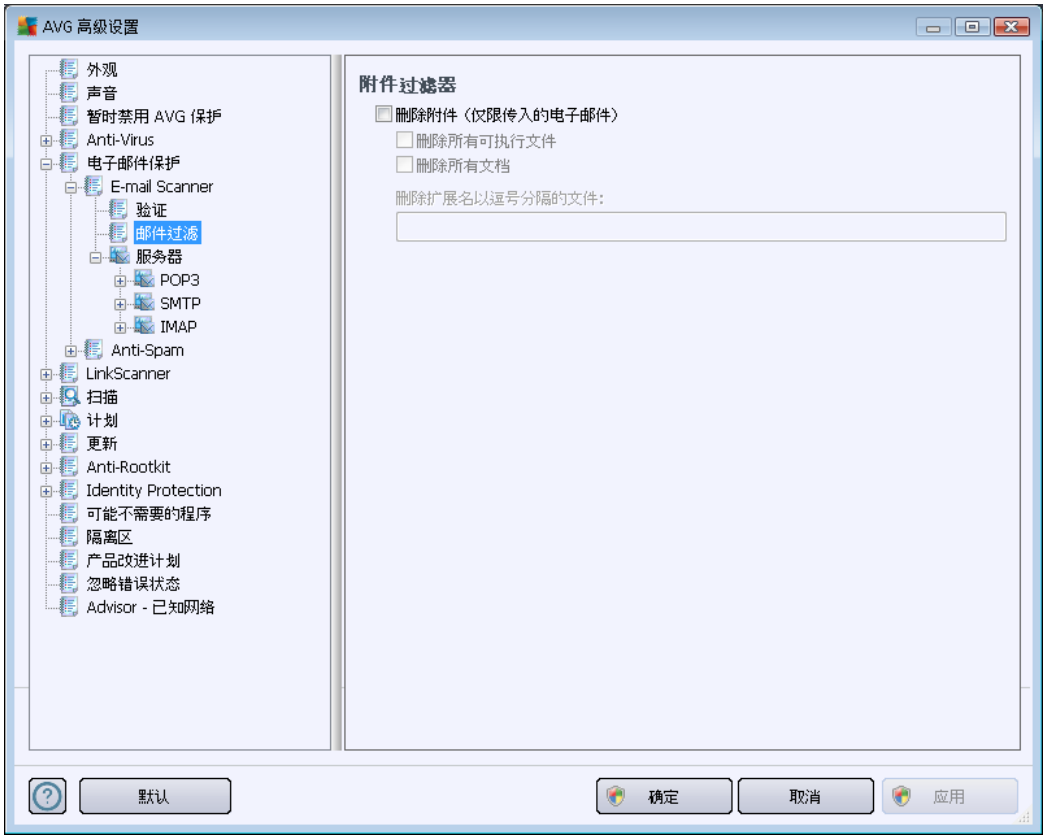
可在***验证*** 对话框中选中特定复选框，以决定是否要验证传入的邮件 ***(验证传入的电子邮件***)和/或传出的邮件 ***(验证传出的电子邮件***)。对于上述各个选项，均可进一步指定***仅限附件*** 参数，这样就仅会对有附件的邮件添加验证结果：



默认情况下，验证文本仅含基本信息（说明*在此邮件中未发现病毒。*）。但是，可按需加长或更改此信息：将中意的验证文本写入***电子邮件验证文本*** 字段。在***电子邮件验证文本中使用的语言*** 部分中，可进一步指定要用于显示验证结果自动生成的部分（*在此邮件中未发现病毒*）的语言。

注：*请注意，仅会以所请求的语言显示默认文本，不会自动翻译经过自定义的文本！*

2012 版权所有 AVG Technologies CZ, s.r.o. 保留所有权利。



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：

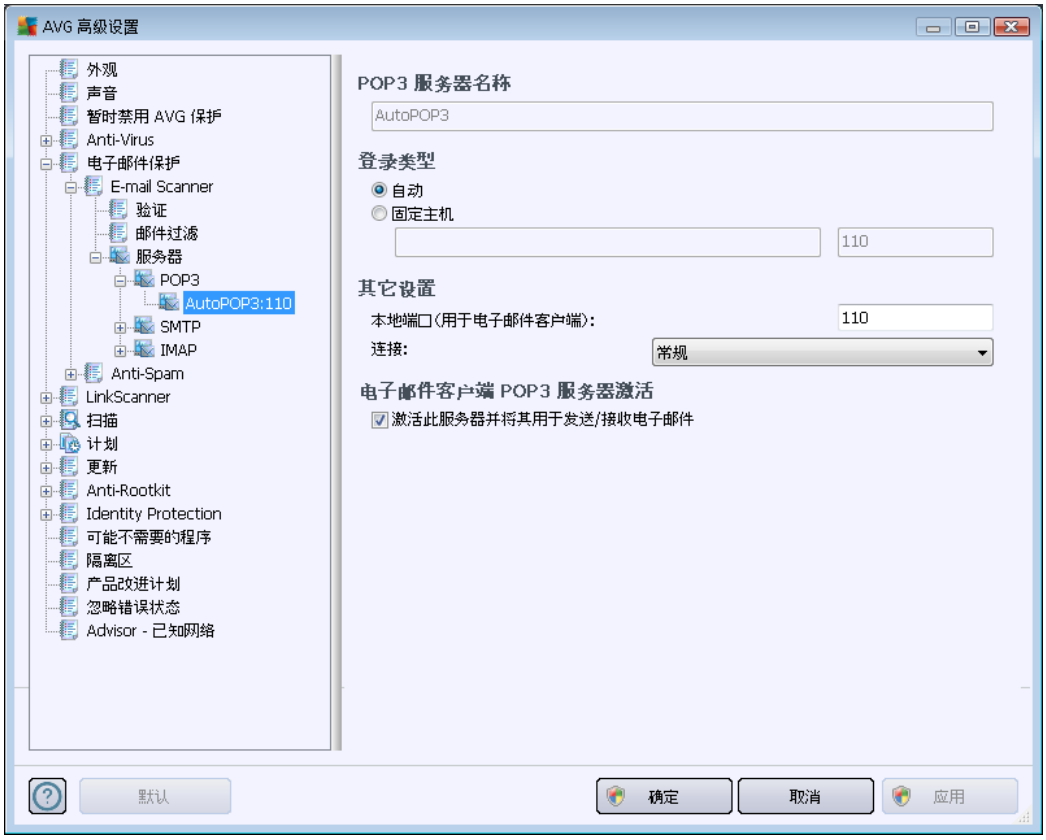
- ***移除所有可执行文件*** - 将删除所有 *.exe 文件
- ***移除所有文档*** - 将删除所有 *.doc、*.docx、*.xls、*.xlsx 文件
- ***移除带有以下扩展名（用逗号分隔）的文件*** - 将移除具有所定义扩展名的所有文件

可在 ***服务器*** 部分中编辑 E-mail Scanner 服务器参数：

- POP3 服务器
- SMTP 服务器
- IMAP 服务器

此外，还可通过 ***添加新服务器*** 按钮对传入或传出的邮件指定新服务器。

 2012 版权所有 AVG Technologies CZ, s.r.o. 保留所有权利。



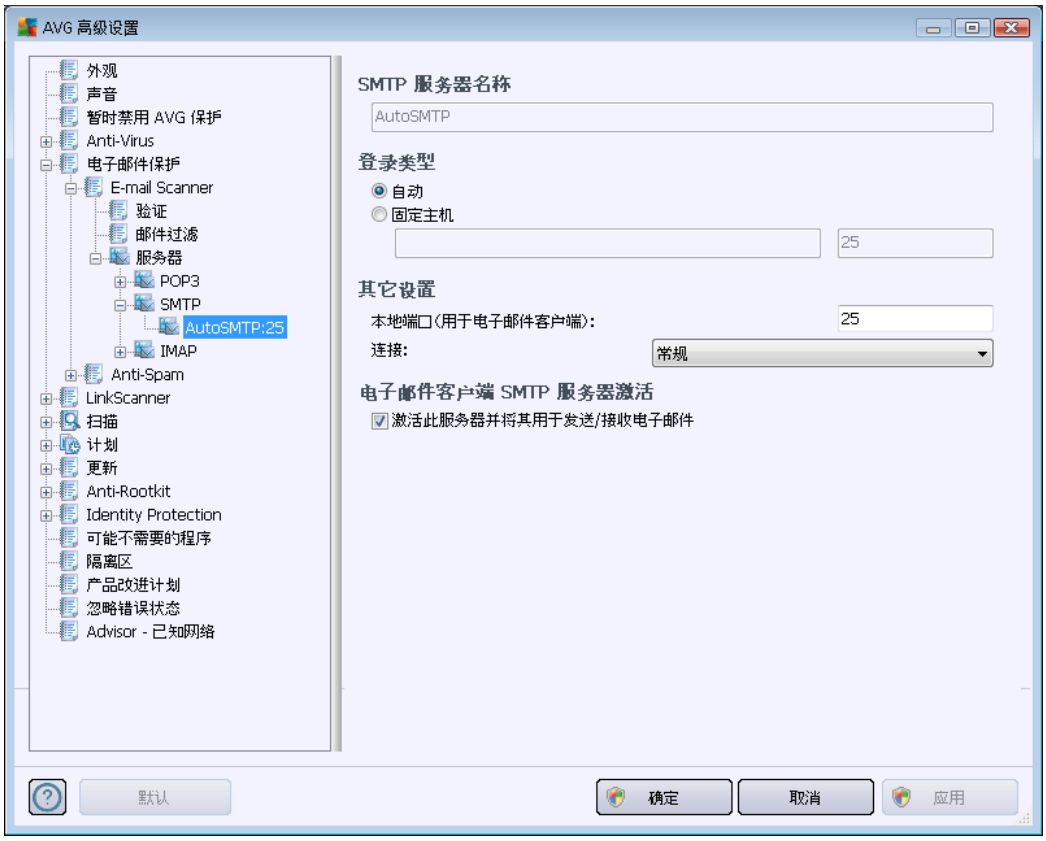
在此对话框 *通过**服务器/POP3*** 打开）中，您可以设置使用 POP3 协议接收邮件的新 电子邮件扫描程序 服务器：

- ***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）*。

2012 版权所有 AVG Technologies CZ, s.r.o. 保留所有权利。

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。

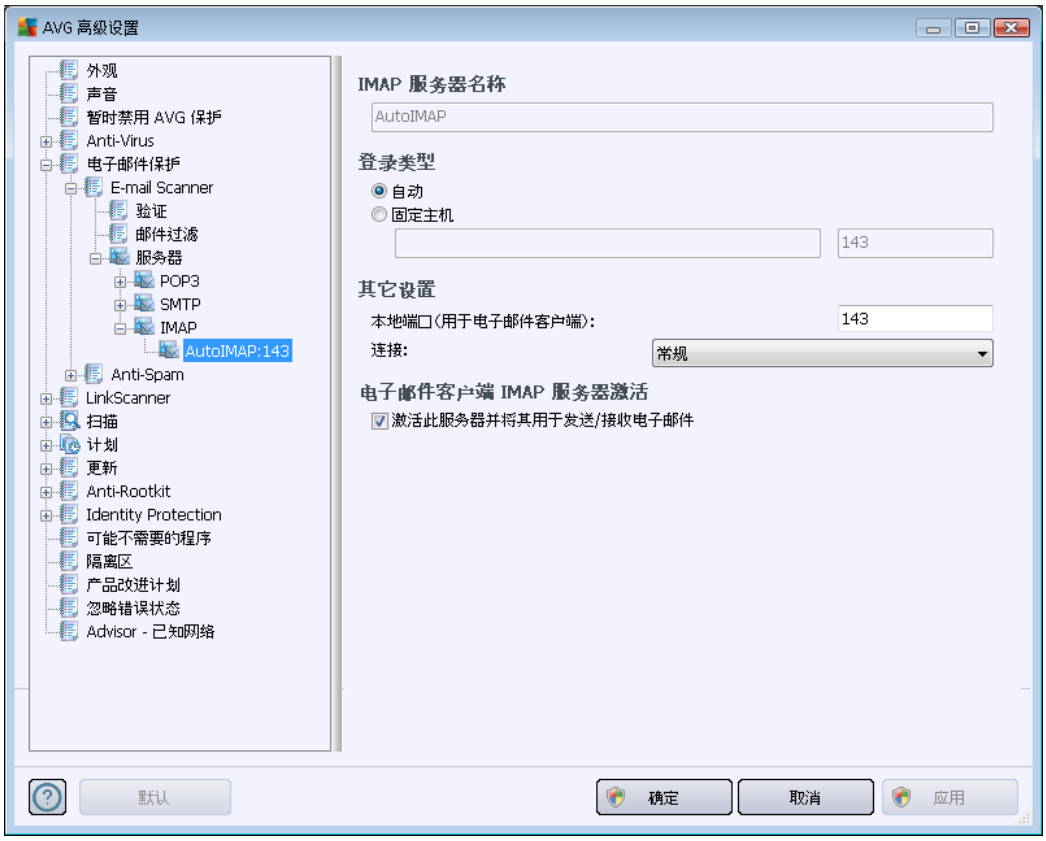
2012 版权所有 AVG Technologies CZ, s.r.o. 保留所有权利。

- ***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：

  - ***自动*** - 将自动根据您的电子邮件客户端设置进行登录

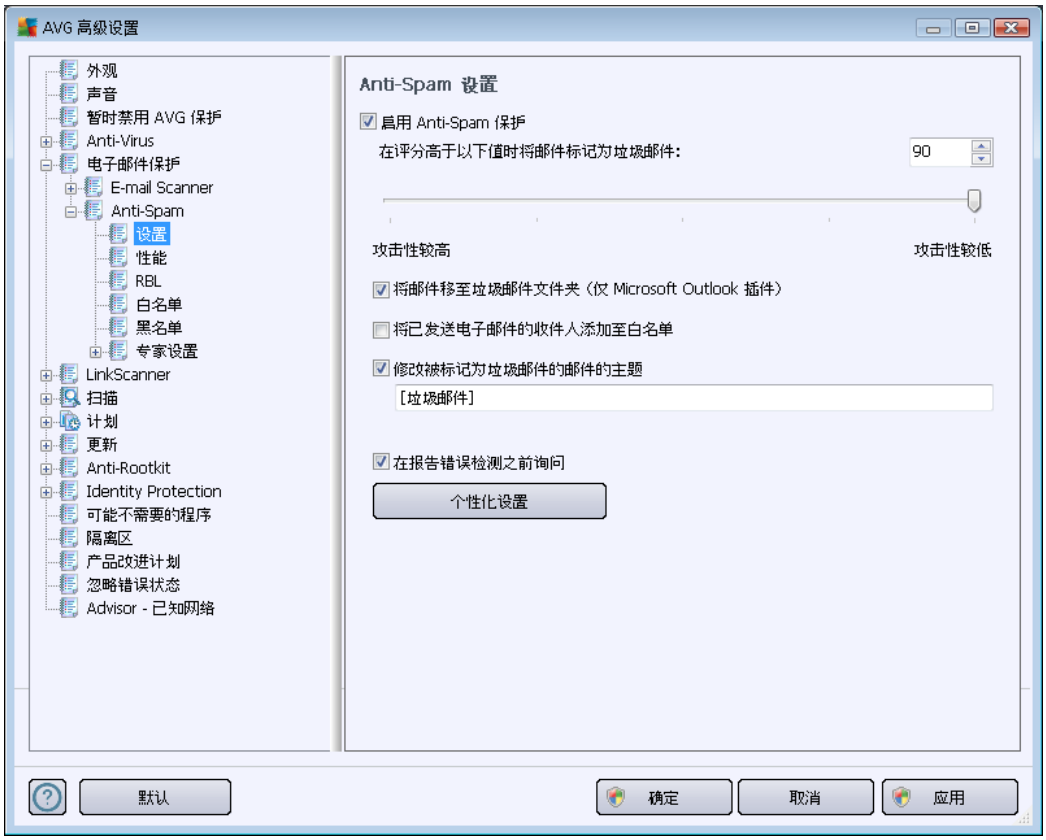
  - ***固定主机*** - 这种情况下，程序将始终使用此处指定的服务器。请指定邮件服

 2012 版权所有 AVG Technologies CZ, s.r.o. 保留所有权利。

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：
  - ***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。
  - ***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

10.5.2. Anti-Spam



在 ***Anti-Spam 设置*** 对话框中，可选中/取消选中***启用 Anti-Spam 保护***复选框，以允许/禁止对电子邮件通讯内容进行反垃圾邮件扫描。此选项在默认情况下已启用，同样建议，除非确有必要更改此配置，否则请予以保留。

2012 版权所有 AVG Technologies CZ, s.r.o. 保留所有权利。

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*** - 会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会被错误地过滤掉。
- ***介于 60 和 79 之间的值*** - 这些值被认为是相当严格的配置。会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会被捕获到。
- ***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。为了正常使用，不建议采用此阈值范围。

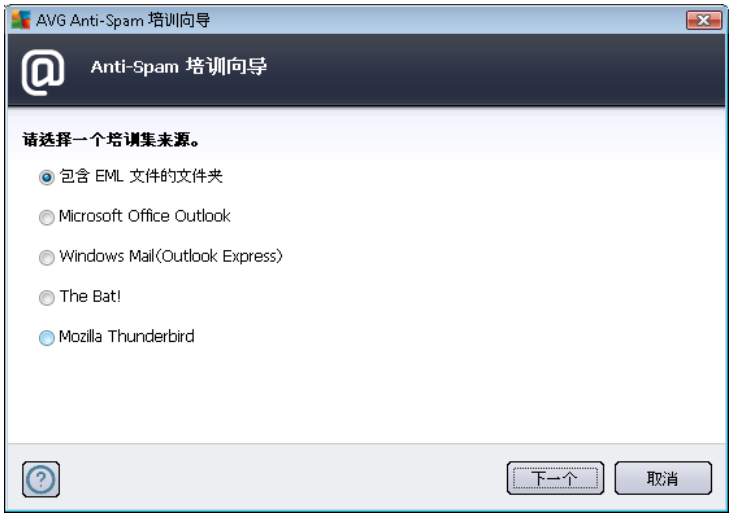
在 ***Anti-Spam 设置*** 对话框中，可进一步指定检测到的垃圾邮件的处理方式：

- ***将邮件移至垃圾邮件文件夹*** *(仅限于 Microsoft Outlook 插件)* - 选中此复选框可指定将检测到的每封垃圾邮件自动移至您 MS Outlook 中特定垃圾邮件文件夹中。此时，该功能在其它邮件客户端中不受支持。
- ***将已发送电子邮件的收件人添加至白名单*** - 选中此复选框可确认，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*** - 如果想在所有已检测到并标记为垃圾邮件的电子邮件主题字段中，用特定词语或字符进行标记，请选中此复选框；可以在已启用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*** - 如果已在安装过程中同意参与产品改进计划。如果是这样，则会允许向 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

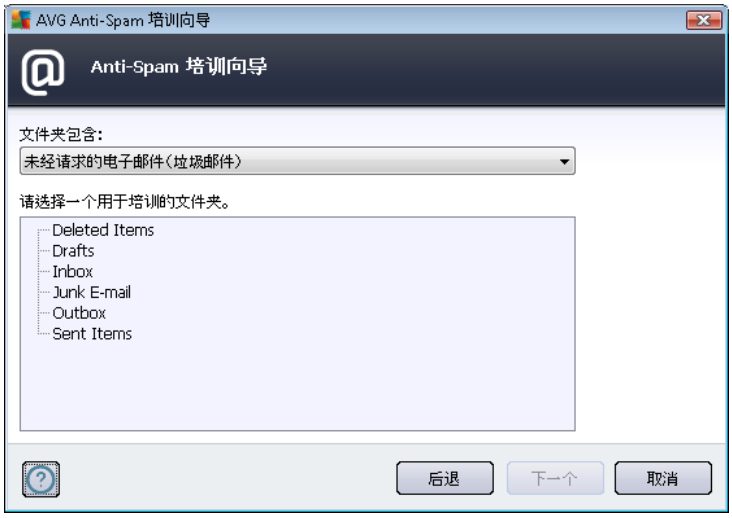
为加快并简化培训过程，最好事先对各文件夹中的电子邮件进行整理，以使您将用于培训的文件夹仅包含培训邮件（要么是需要的邮件，要么是不需要的邮件）。但并非必需进行整理，因为您可以稍后对这些电子邮件进行过滤。

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

2012 版权所有 AVG Technologies CZ, s.r.o. 保留所有权利。



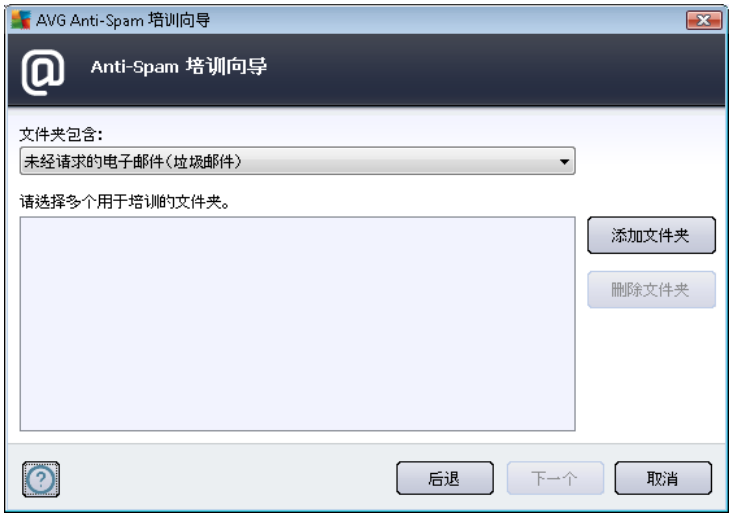
在此对话框中，请选择您要用于培训的邮件所在的文件夹。按 ***"添加文件夹"*** 按钮以找到包含 .eml 文件 *(已保存的电子邮件)* 的文件夹。所选的文件夹随后便会显示在此对话框中。

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。

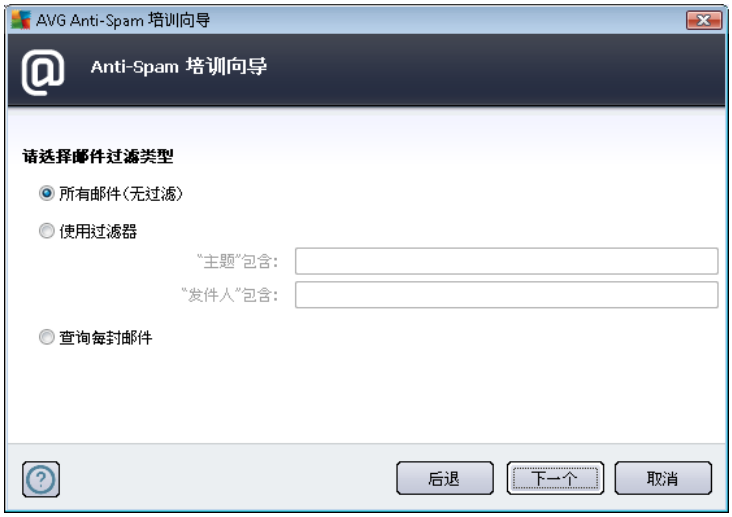


注：对于 Microsoft Office Outlook，系统会提示您先选择 MS Office Outlook 配置文件。

2012 版权所有 AVG Technologies CZ, s.r.o. 保留所有权利。

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。



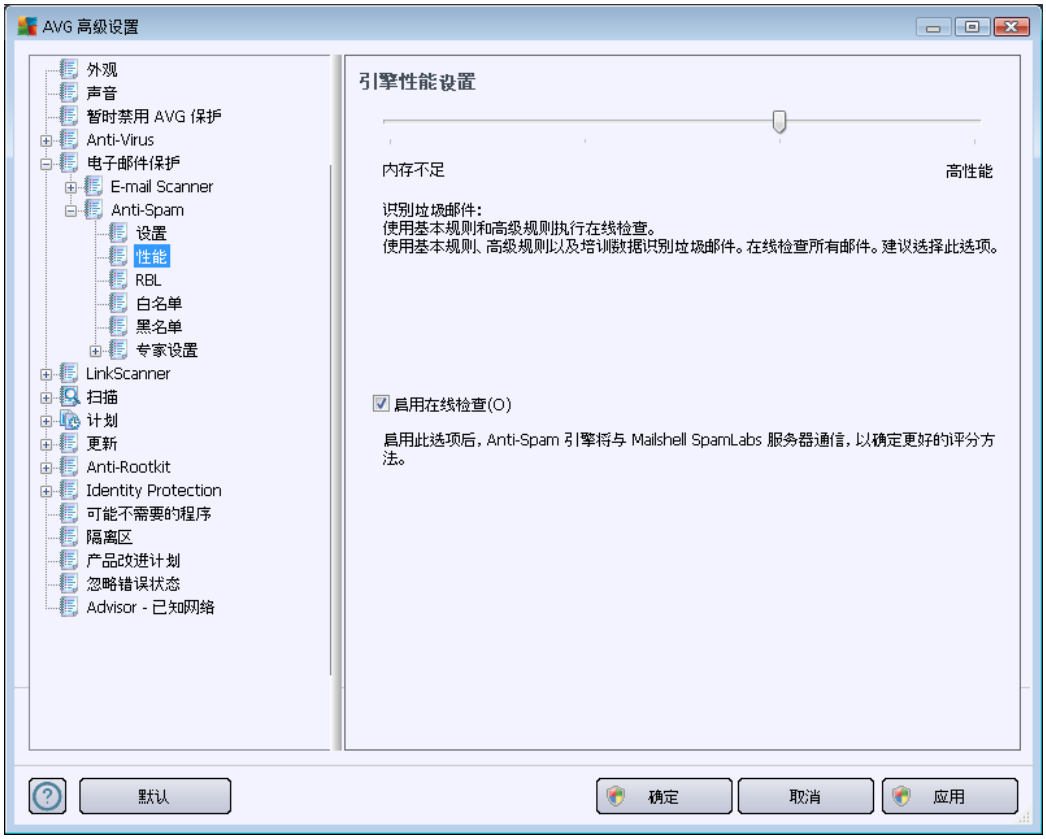
在此对话框中，您可以进行电子邮件过滤设置。

- ***所有邮件(无过滤)*** - 如果您确定所选文件夹仅包含您要用于培训的邮件，请选中 ***所有邮件(无过滤)*** 选项。
- ***使用过滤器*** - 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。如果在两个文本字段中都填入内容，则只与其中一个条件匹配的地址也将被用于培训！
- ***查询每封邮件*** - 如果无法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*），请选中 ***查询每封邮件*** 选项。

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。

2012 版权所有 AVG Technologies CZ, s.r.o. 保留所有权利。

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)*中有 ***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。

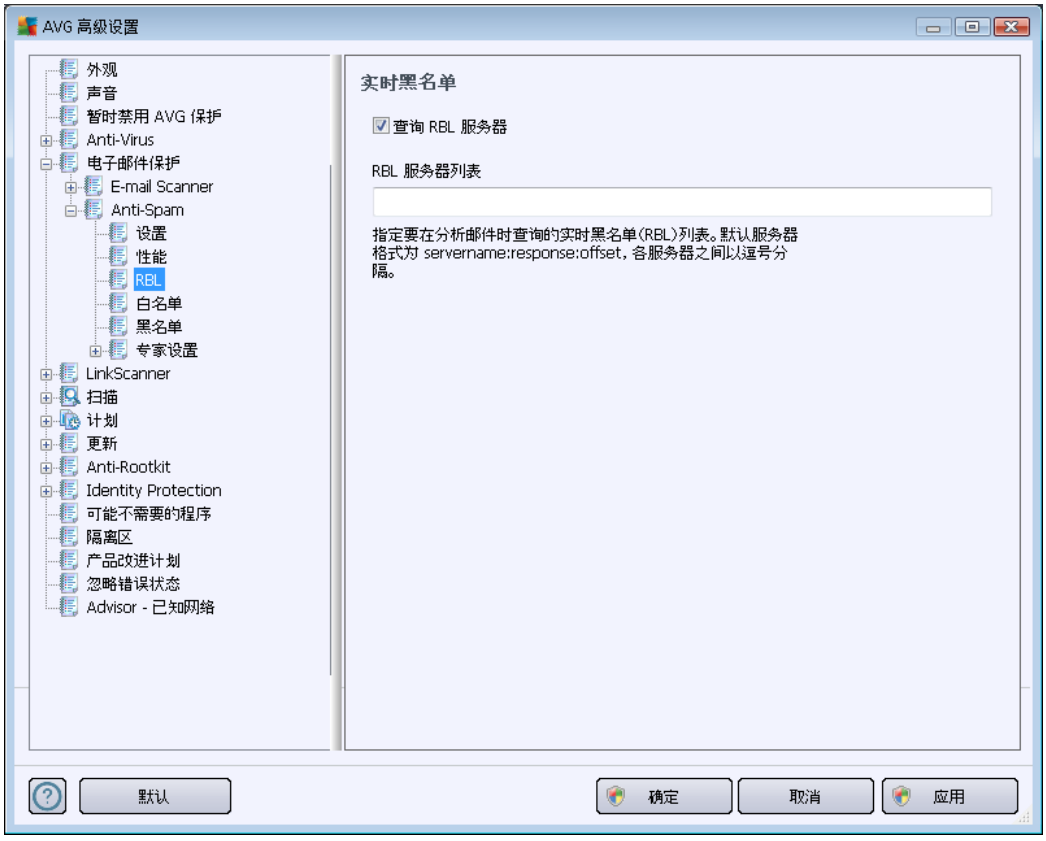
- ***低内存占用*** - 在扫描过程中识别垃圾邮件时，不使用任何规则。只使用培训数据进行识别。在一般使用情形中不建议采用此模式，除非计算机硬件配置非常低。
- ***高性能*** - 采用此模式时将占用大量内存。在扫描过程中，将使用以下功能来识别垃圾邮件：规则和垃圾邮件数据库缓存、基本规则和高级规则、垃圾邮件制造者的 IP 地址和垃圾邮件制造者数据库。

默认情况下，***启用在线检查*** 项已启用。这样可通过与 Mailshell 服务器进行通讯（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！

2012 版权所有 AVG Technologies CZ, s.r.o. 保留所有权利。

RBL 选项用于打开名为 ***实时黑名单*** 的编辑对话框，从中可启用/禁用 ***查询 RBL 服务器*** 功能：



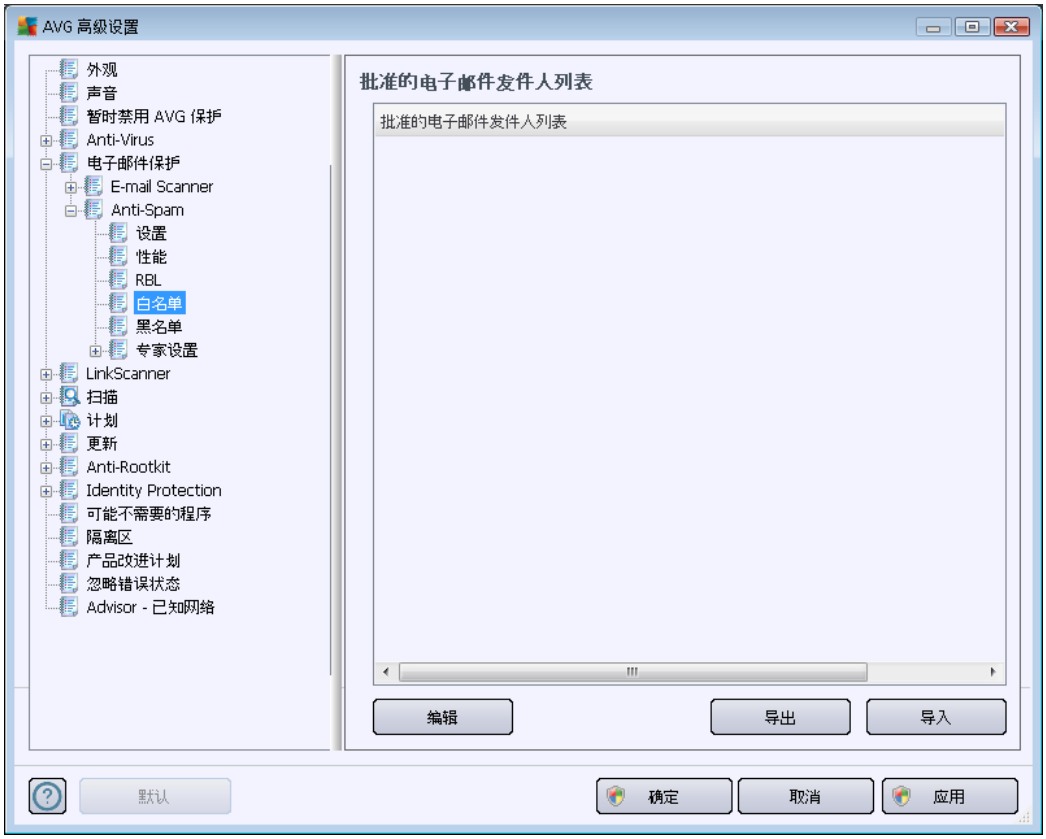
RBL（*实时黑名单*）服务器是一台承载着一个大型数据库的 DNS 服务器，该数据库中存储着已知的垃圾邮件发件人。启用此功能后，会根据 RBL 服务器数据库来验证所有电子邮件，如果有邮件与数据库中的任何条目相同，则会将该邮件标记为垃圾邮件。RBL 服务器数据库包含最新的垃圾邮件指纹，以便进行最佳、最准确的垃圾邮件检测。如果用户收到 Anti-Spam 引擎通常无法检测到的大量垃圾邮件，则此功能对他们来说尤为有用。

RBL 服务器列表可让您定义特定 RBL 服务器位置 *（请注意，在某些系统和配置中启用此性能可能会减缓电子邮件接收速度，其原因是每封邮件必须向 RBL 服务器数据库时进行验证）。*

不会将任何个人数据发送到此服务器！

2012 版权所有 AVG Technologies CZ, s.r.o. 保留所有权利。

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。这样的发件人和/或域名列表一准备好，就可以通过以下任一方法输入发件人和/或域名：直接输入每个电子邮件地址或一举导入整个地址列表。

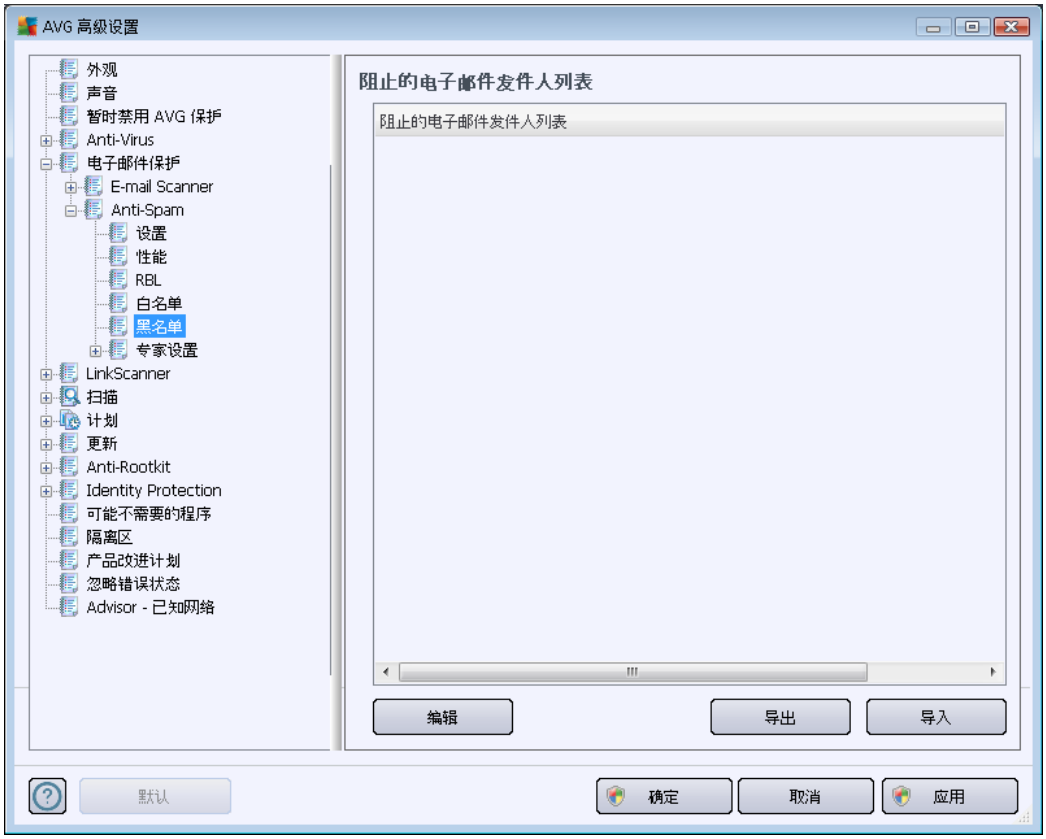
控制按钮

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*）。

2012 版权所有 AVG Technologies CZ, s.r.o. 保留所有权利。

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为垃圾邮件。



在该编辑界面中，可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。还可以整理一个您预期会发来垃圾邮件的所有域名 *(如 spammingcompany.com)* 的列表。来自所列出的地址/域的所有电子邮件都将被认定为垃圾邮件。这样的发件人和/或域名列表一准备好，就可以通过以下任一方法输入发件人和/或域名 :直接输入每个电子邮件地址或一举导入整个地址列表。

控制按钮

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。

2012 版权所有 AVG Technologies CZ, s.r.o. 保留所有权利。

对于 Anti-Spam 组件，'高级设置 '分支含有大量设置选项。这些设置仅面向经验丰富的用户，通常是需要对反垃圾邮件保护措施进行详尽配置，以便对电子邮件服务器实施最严密保护的网络管理员。因此，我们未对各个对话框提供其它帮助信息 ;但是，在用户界面中直接对每个选项作了简短说明。

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：

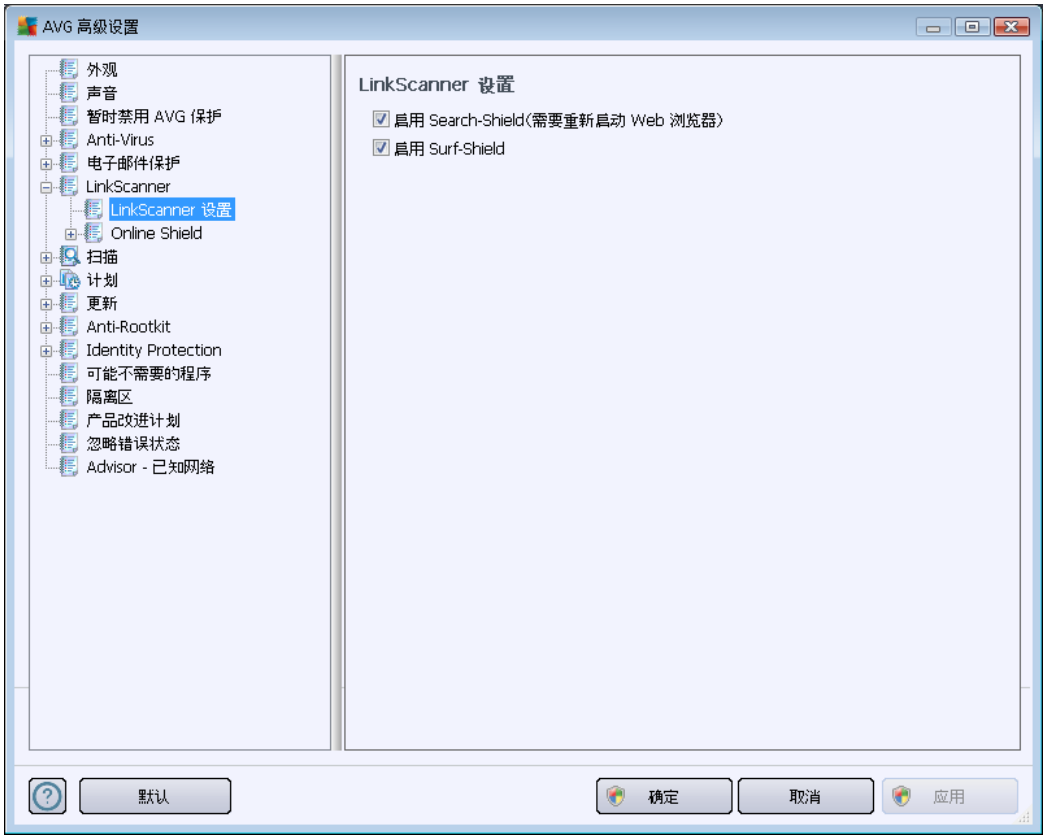
- ***缓存*** –指纹、域声誉、LegitRepute
- ***培训*** - 词语条目上限、自动培训阈值、权重
- ***过滤*** –语言列表、国家/地区列表、批准的 IP、阻止的 IP、阻止的国家/地区、阻止的字符集、冒牌发件人
- ***RBL*** –RBL 服务器、多重攻击、阈值、超时、最大 IP 数
- ***Internet 连接*** - 超时、代理服务器、代理服务器身份验证

10.6. LinkScanner

 2012 版权所有 AVG Technologies CZ, s.r.o. 保留所有权利。

10.6.1. LinkScanner 设置

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

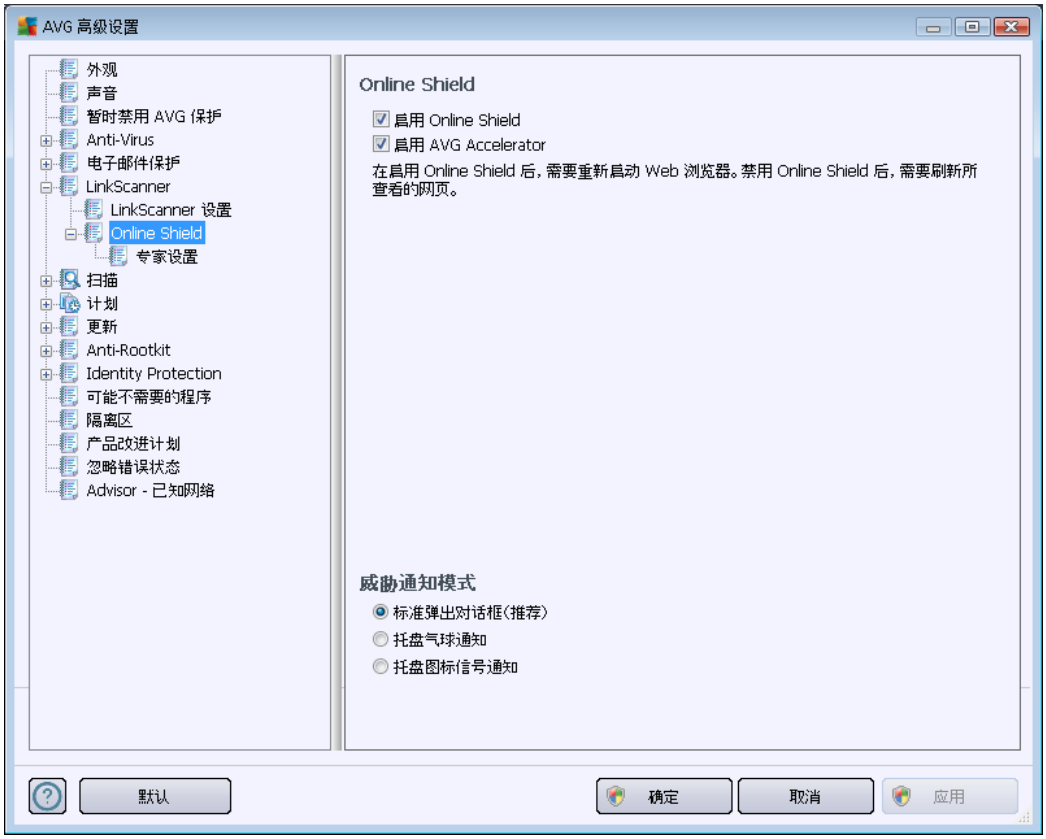


- ***启用 Search-Shield*** -(*默认情况下已启用*)：在对 Google, Yahoo! JP、WebHledani、Yandex、百度、Bing、AOL、AltaVista、EarthLink、Ask、Seznam、eBay、Twitter、Digg 或 SlashDot 等搜索引擎所返回的网站内容进行事先检查后，就所执行的搜索显示警告通知图标。

- ***"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。

2012 版权所有 AVG Technologies CZ, s.r.o. 保留所有权利。

10.6.2. Online Shield



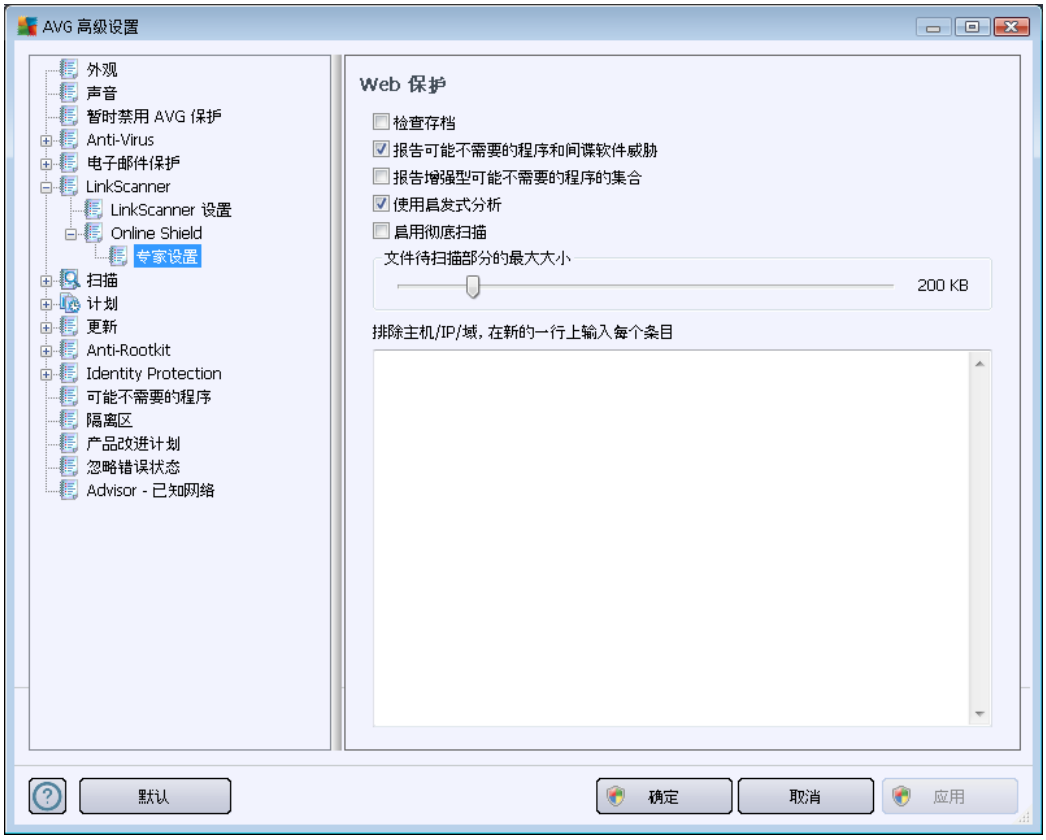
Online Shield 对话框中有以下选项：

- ***启用 Online Shield*** *（默认情况下已启用）*- 用于彻底启用/停用 ***Online Shield*** 服务。对于 ***Online Shield*** 的其它高级设置，请继续在名为 Web 保护的后续对话框中配置。
- ***启用 AVG Accelerator*** *（默认情况下已启用）*- 用于启用/停用 ***AVG Accelerator*** 服务，通过该服务可使在线视频播放更加流畅，还可使后续下载更加容易。

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。

2012 版权所有 AVG Technologies CZ, s.r.o. 保留所有权利。



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)*：选中此框可启用 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。

 2012 版权所有 AVG Technologies CZ, s.r.o. 保留所有权利。

- ***"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。

10.7. 扫描

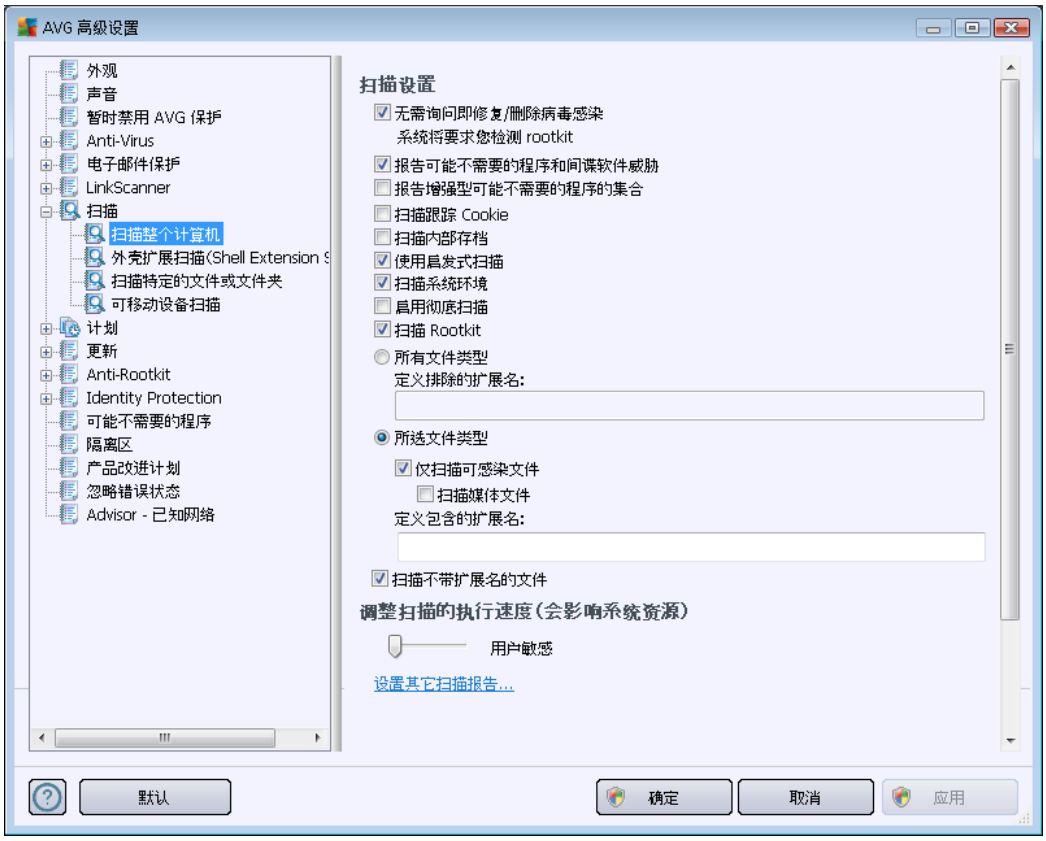
高级扫描设置分为四种类别，分别对应软件供应商定义的以下特定扫描类型：

- ***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

 2012 版权所有 AVG Technologies CZ, s.r.o. 保留所有权利。

10.7.1. 扫描整个计算机

通过***扫描整个计算机***选项，可编辑软件供应商预先指定的某项扫描（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：

- ***无需询问即修复/删除病毒感染***（*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。

2012 版权所有 AVG Technologies CZ, s.r.o. 保留所有权利。

- ***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。但要记住，此方法相当耗时。

- ***扫描 rootkit***(*默认情况下已启用*) - Anti-Rootkit 用于在您的计算机中搜索是否可能存在 rootkit（例如，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。

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。

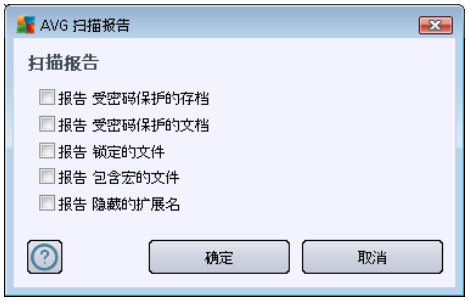
调整扫描的完成速度

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...

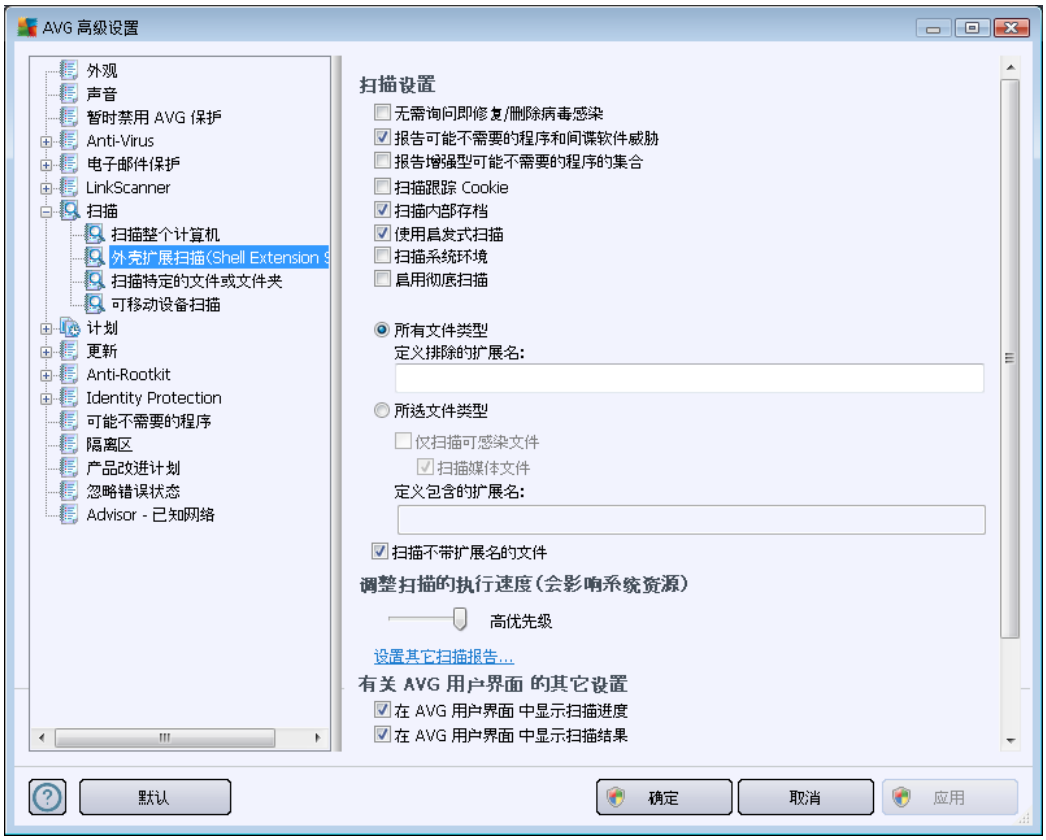
单击“***设置其它扫描报告...***”链接可打开一个名为“***扫描报告***”的独立对话框窗口，在此窗口中您可以通过勾选若干项来定义应报告哪些扫描结果：

 2012 版权所有 AVG Technologies CZ, s.r.o. 保留所有权利。



10.7.2. 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*** 的选项也有若干选项，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*）。

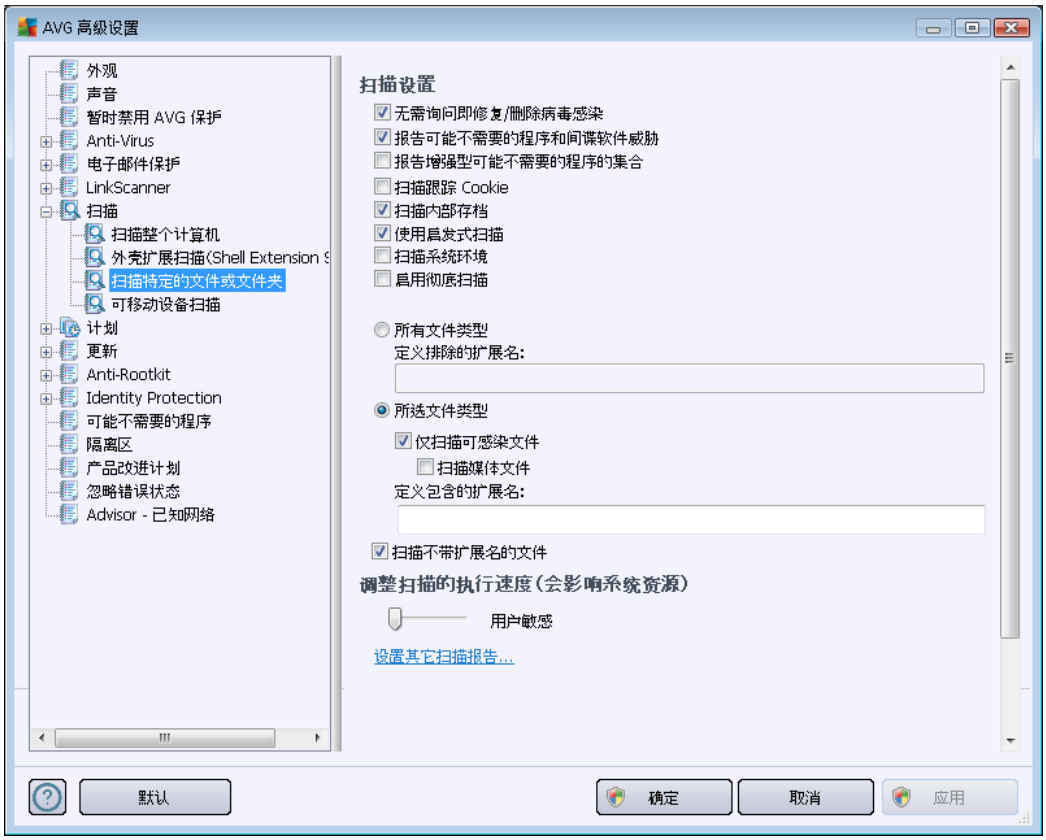
注意 :*有关特定参数的说明，请参阅 AVG 高级设置/扫描/扫描整个计算机 ”一章。*

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，从中可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。

10.7.3. 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：



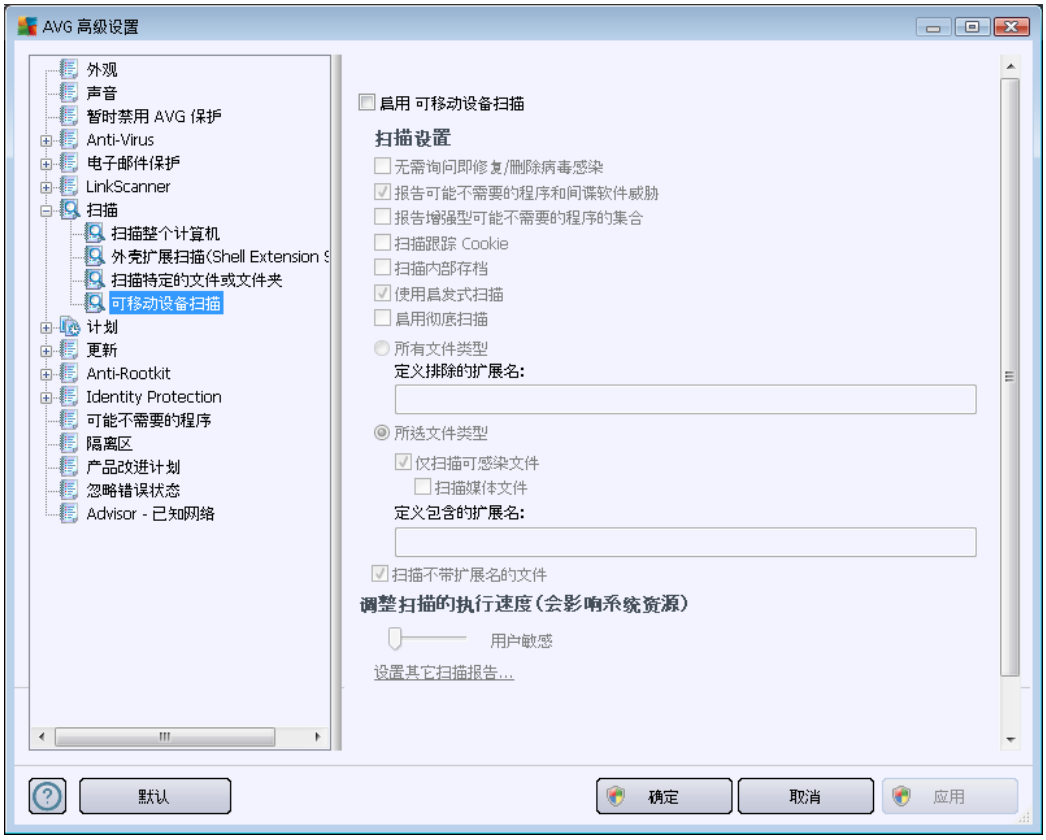
在此配置对话框中设置的所有参数都仅适用于选定使用"扫描特定的文件或文件夹"功能进行扫描的区域！

***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。*

2012 版权所有 AVG Technologies CZ, s.r.o. 保留所有权利。

10.7.4. 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。*

10.8. 计划

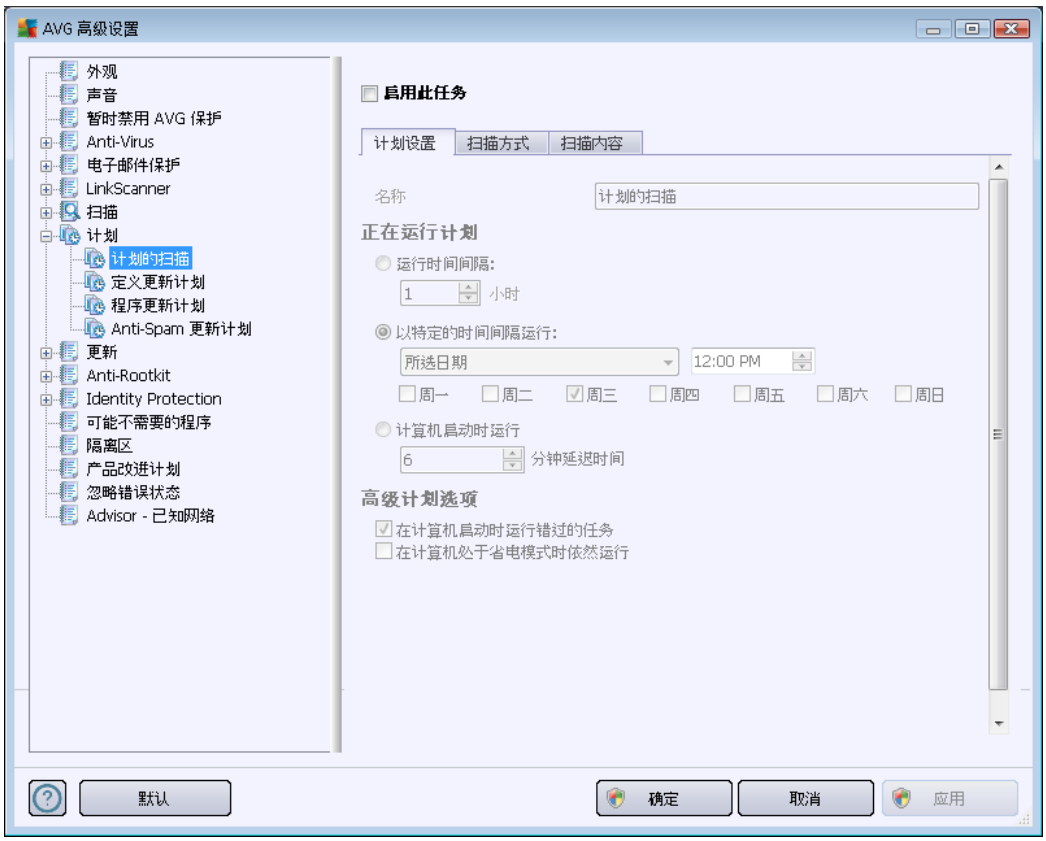
在*"计划"*区域中，您可以编辑以下各项的默认设置：

- [计划的扫描](#)
- [定义更新计划](#)
- [程序更新计划](#)
- [Anti-Spam 更新计划](#)

2012 版权所有 AVG Technologies CZ, s.r.o. 保留所有权利。

10.8.1. 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复启动扫描(***运行间隔...***)，或通过定义确切的日期和时间 ***以特定的***

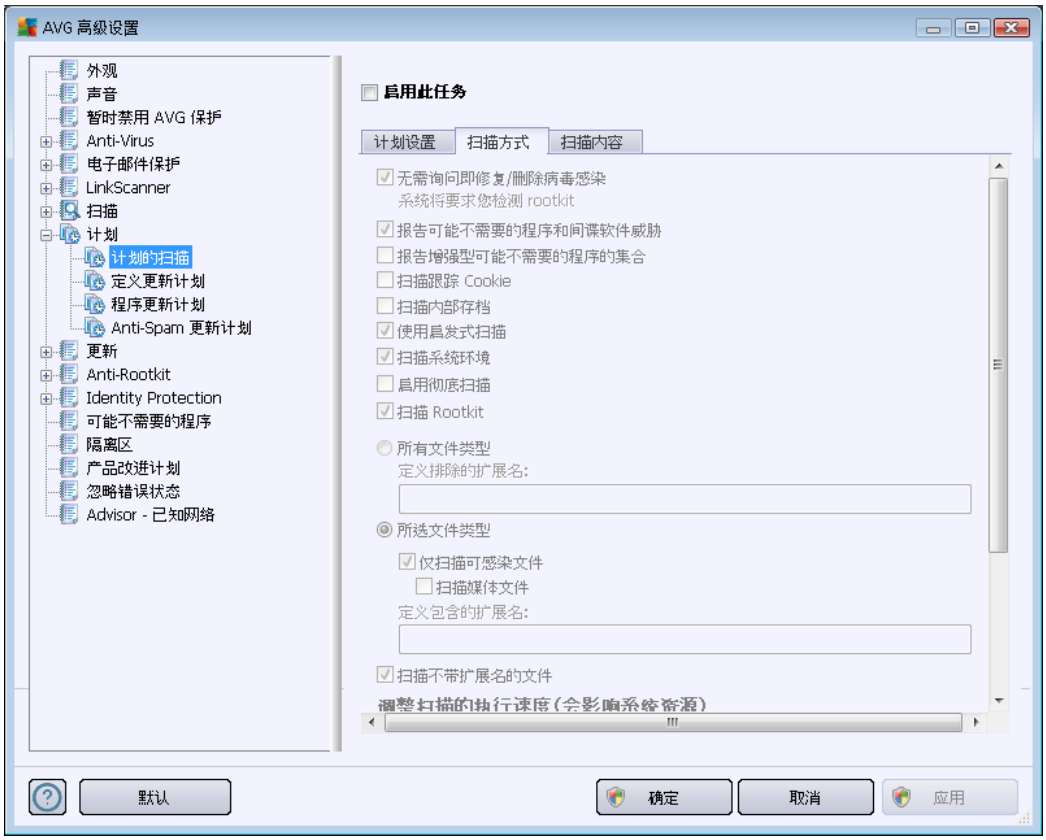
2012 版权所有 AVG Technologies CZ, s.r.o. 保留所有权利。

时间间隔运行...)，也可以定义扫描启动操作应关联的事件 (***计算机启动时运行***)。

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。计划的扫描一在指定的时间启动，就会通过在 AVG 系统任务栏图标上方打开一个弹出窗口就这种情况发出通知：

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。右键单击表示正在运行扫描的 AVG 图标，可打开一个上下文菜单。您可在此菜单中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先指定的配置***：

- ***无需询问即修复/删除病毒感染*** *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

 2012 版权所有 AVG Technologies CZ, s.r.o. 保留所有权利。

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。但要记住，此方法相当耗时。

- ***扫描 Rootkit***（*默认情况下已启用*）：Anti-Rootkit 用于在您的计算机中搜索是否可能存在 rootkit（例如，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。

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。

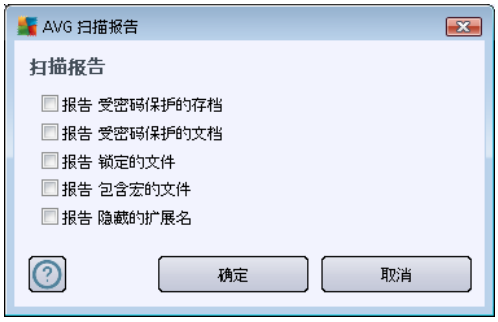
调整扫描的完成速度

 2012 版权所有 AVG Technologies CZ, s.r.o. 保留所有权利。

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

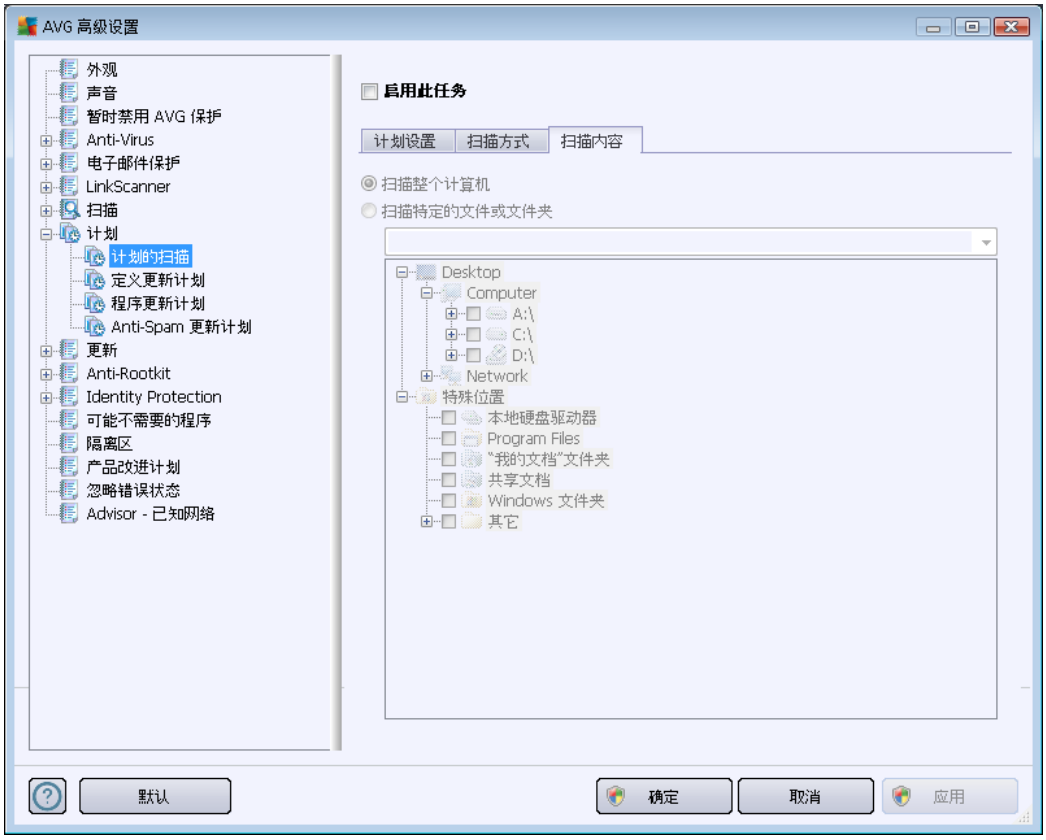
单击 ***"设置其它扫描报告..."*** 链接可打开一个名为 ***"扫描报告"*** 的独立对话框窗口，在此窗口中您可以通过勾选若干项来定义应报告哪些扫描结果：



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。

2012 版权所有 AVG Technologies CZ, s.r.o. 保留所有权利。

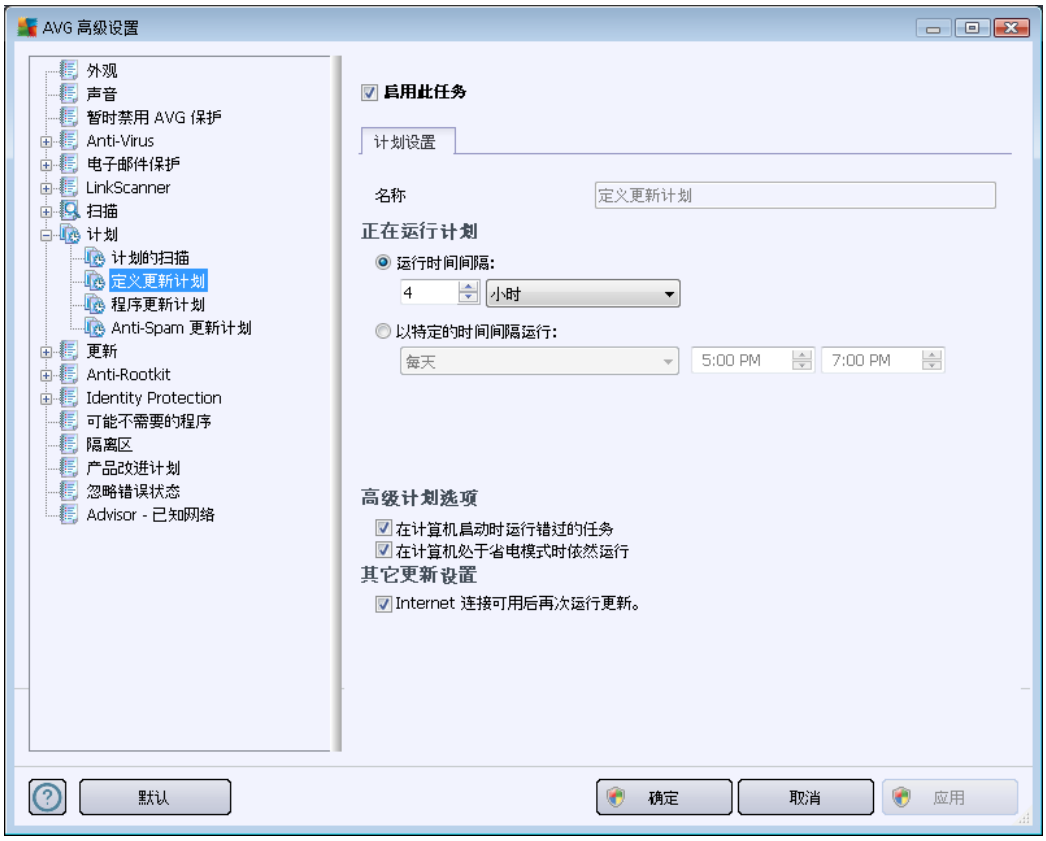


在 ***"扫描内容"*** 选项卡上，您可以定义您要计划的是[扫描整个计算机](#)还是[扫描特定的文件或文件夹](#)。如果您选择的是"扫描特定的文件或文件夹"，则在此对话框底部将激活如图所示的树结构，您可以利用它来指定要扫描的文件夹。

2012 版权所有 AVG Technologies CZ, s.r.o. 保留所有权利。

10.8.2. 指定更新计划

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定义更新，然后再将其启用：



可在此对话框中设置定义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，请指定新计划的定义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，可以指定当计算机处于省电模式或完全关闭时在哪些条件下定义更新应该/不应该启动。

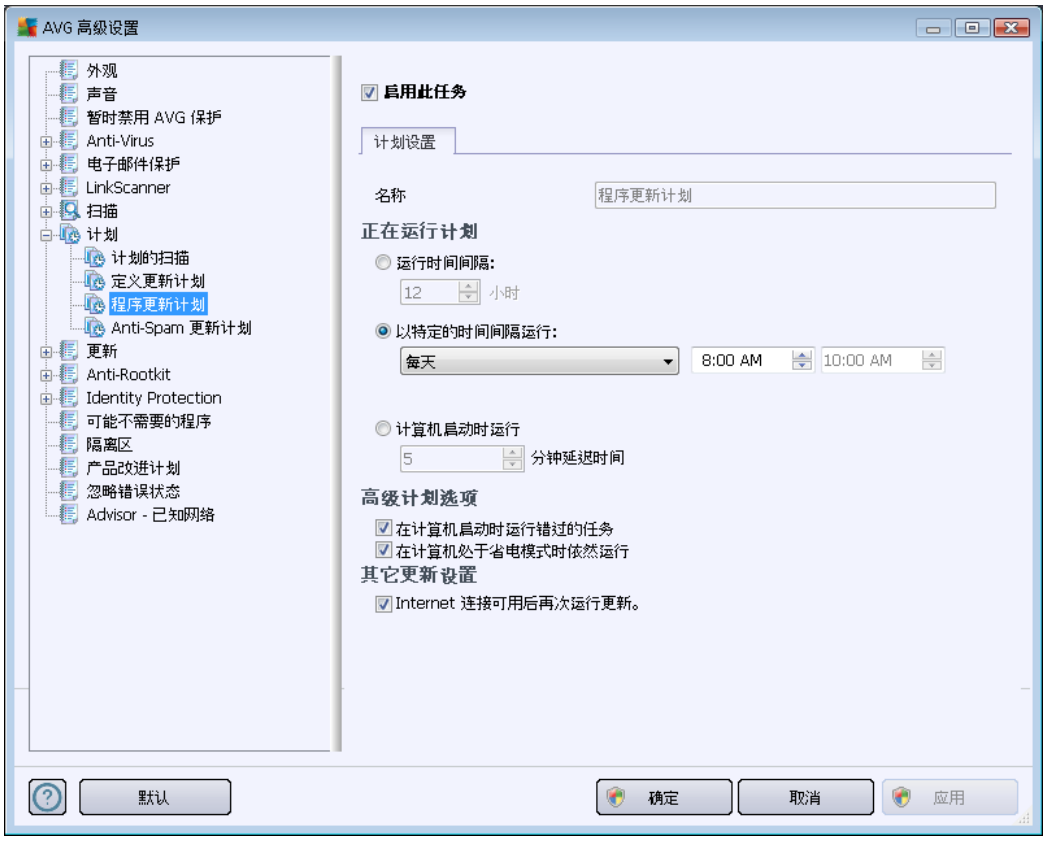
其它更新设置

2012 版权所有 AVG Technologies CZ, s.r.o. 保留所有权利。

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*）。

10.8.3. 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

 2012 版权所有 AVG Technologies CZ, s.r.o. 保留所有权利。

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。

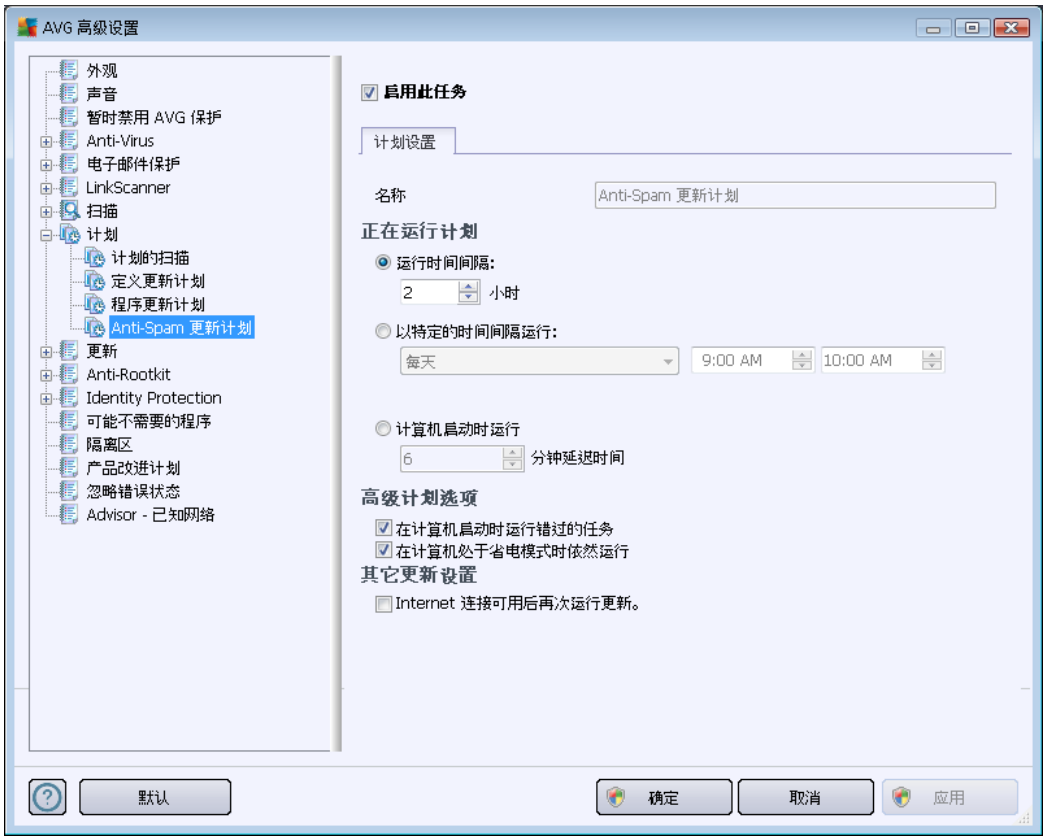
其它更新设置

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。

10.8.4. 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：



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

 2012 版权所有 AVG Technologies CZ, s.r.o. 保留所有权利。

请在此指定刚刚安排的 Anti-Spam更新启动任务的时间间隔。上述时间安排的指定方式有三种 :指定经过一段特定的时间后反复启动 Anti-Spam 更新(***运行时间间隔...***),指定确切的日期和时间 (***以特定的时间间隔运行***),也可以指定应该与更新启动操作相关联的事件(***计算机启动时的操作***)。

高级计划选项

通过此部分可指定计算机处于省电模式或已彻底关闭时,应该/不应该在哪些情况下启动 Anti-Spam 更新。

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 连接断开,因而 Anti-Spam 更新过程失败,则会在 Internet 连接恢复后立即重新启动更新过程。

计划内扫描一在所指定的时间启动,就会通过在 AVG 系统任务栏图标上方打开的一个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)。*

10.9. 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:

 2012 版权所有 AVG Technologies CZ, s.r.o. 保留所有权利。

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所需执行的操作
- ***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启启动计算机时才完成。请记住，此选项仅当确信计算机会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

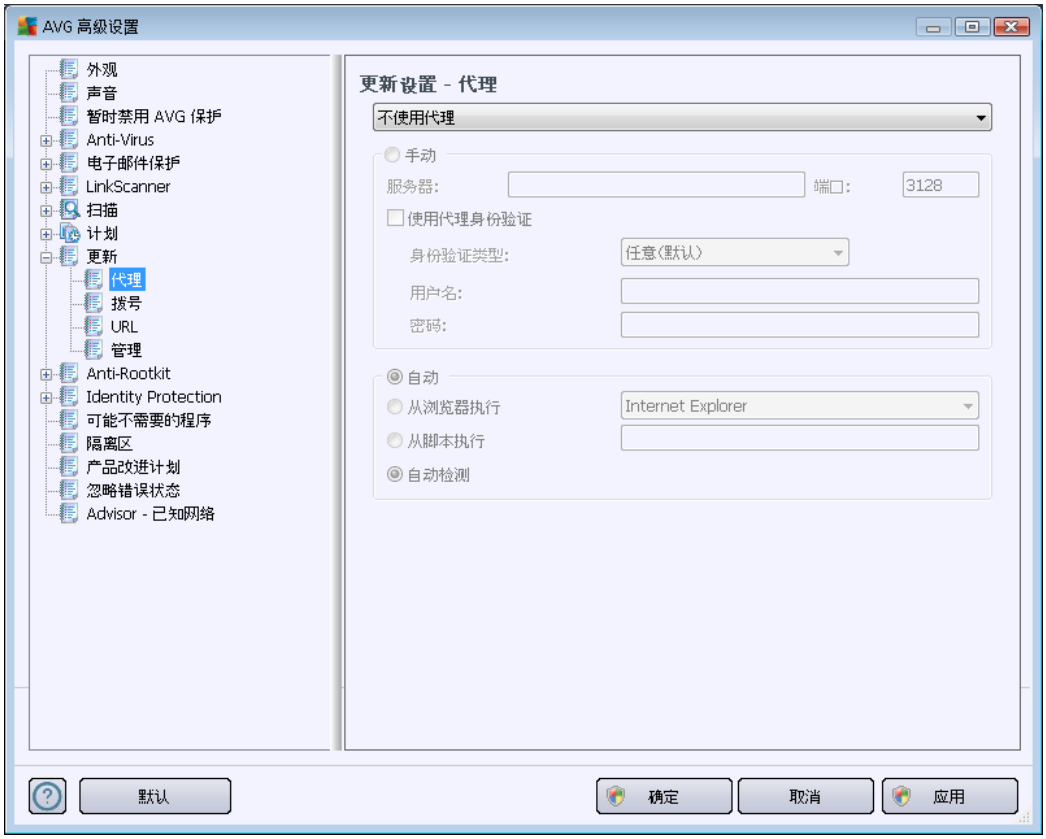
选中此复选框可指定，您希望在每次成功完成更新后启动新的内存扫描。最新下载的更新可能包含新的病毒定义，这些定义会被立即应用在扫描中。

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 2012** 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。

 2012 版权所有 AVG Technologies CZ, s.r.o. 保留所有权利。

10.9.1. 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*** - 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*

 2012 版权所有 AVG Technologies CZ, s.r.o. 保留所有权利。

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。

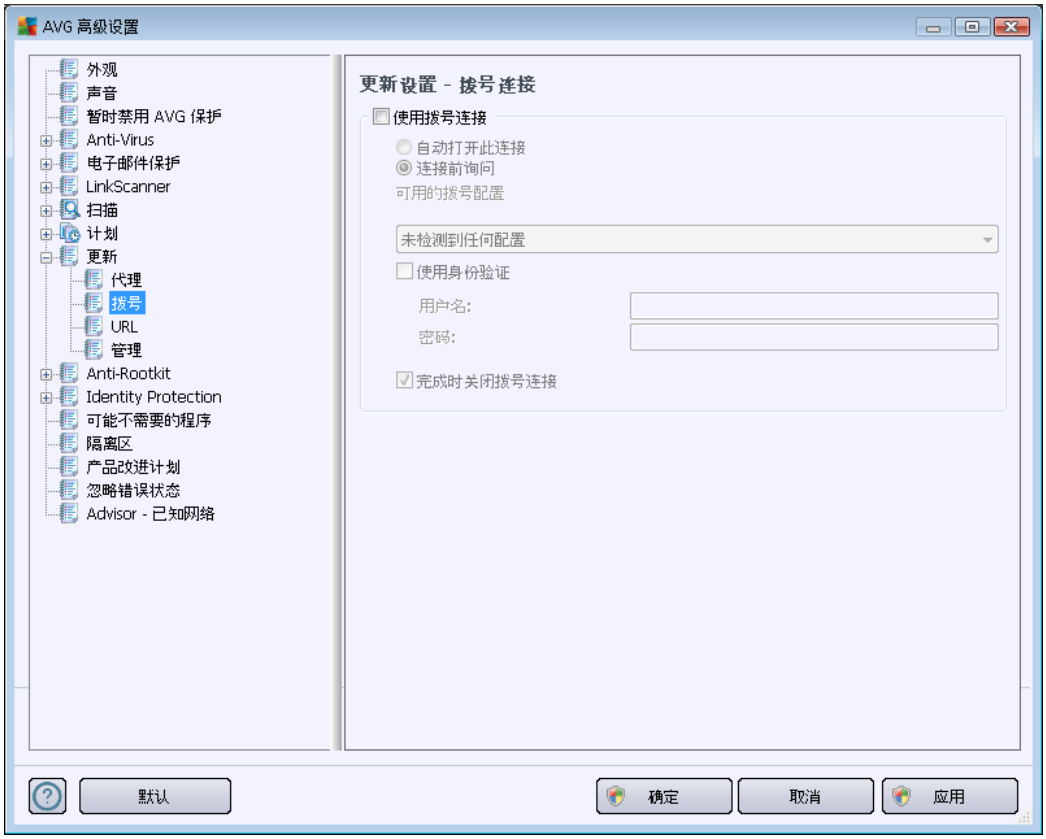
自动配置

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

10.9.2. 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处于已停用状态，直到选中 ***使用拨号连接*** 选项后，才会启用这些字段：



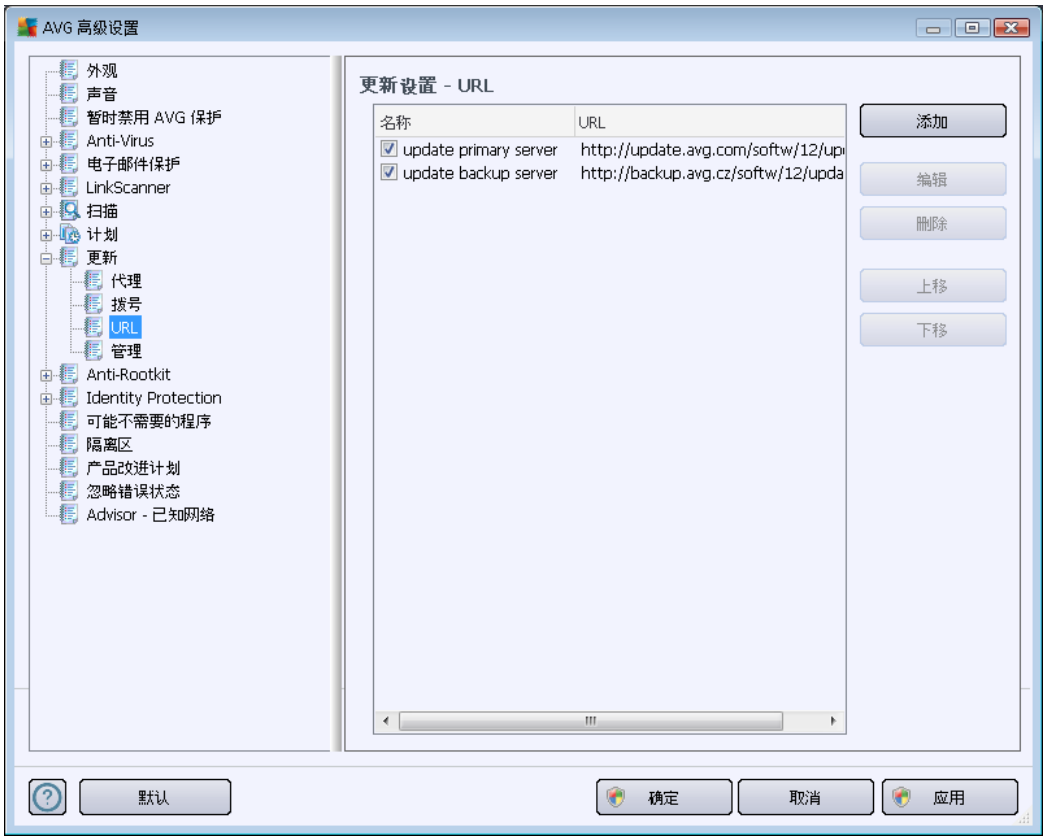
请指定您是希望自动连接到 Internet（***"自动打开此连接"*** 还是希望每次都手动确认连接（

 2012 版权所有 AVG Technologies CZ, s.r.o. 保留所有权利。

‘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’*。

10.9.3. URL

URL 对话框中有可用于下载更新文件的 Internet 地址列表：



控制按钮

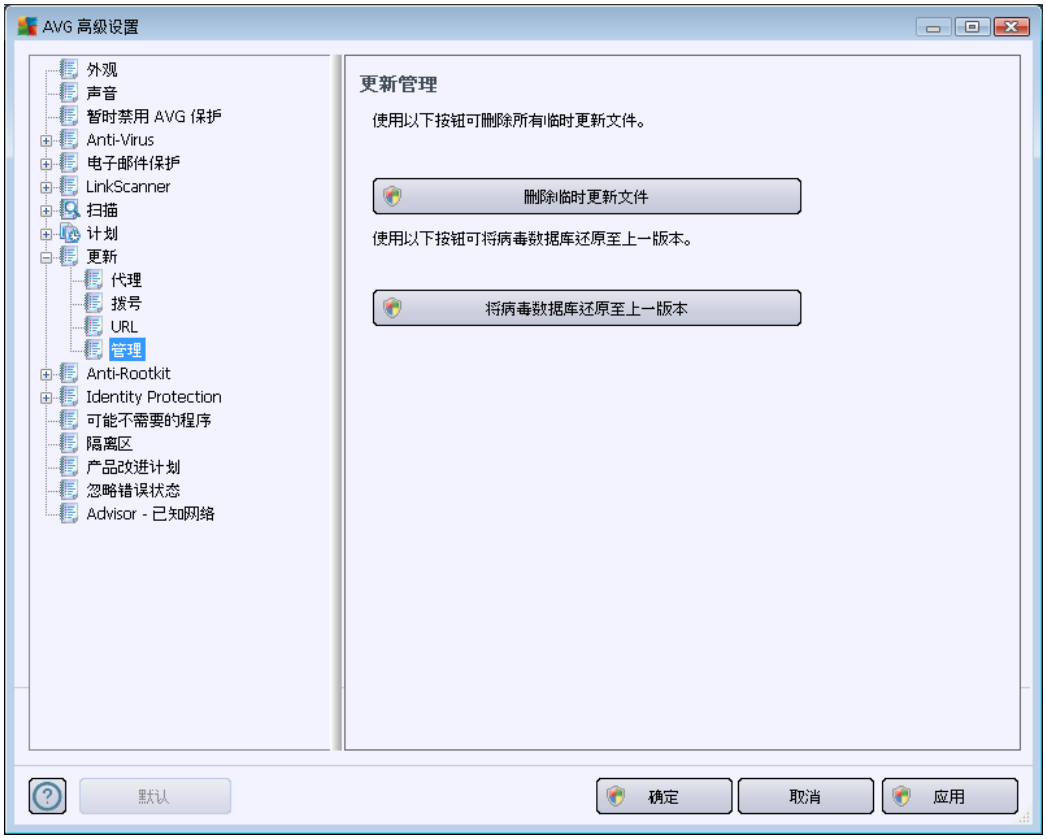
可以使用以下控制按钮修改此列表及其中的各项：

- ***‘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

2012 版权所有 AVG Technologies CZ, s.r.o. 保留所有权利。

10.9.4. 管理

更新管理 对话框中有两个选项，这两个选项分别可通过以下两个按钮显示出来：

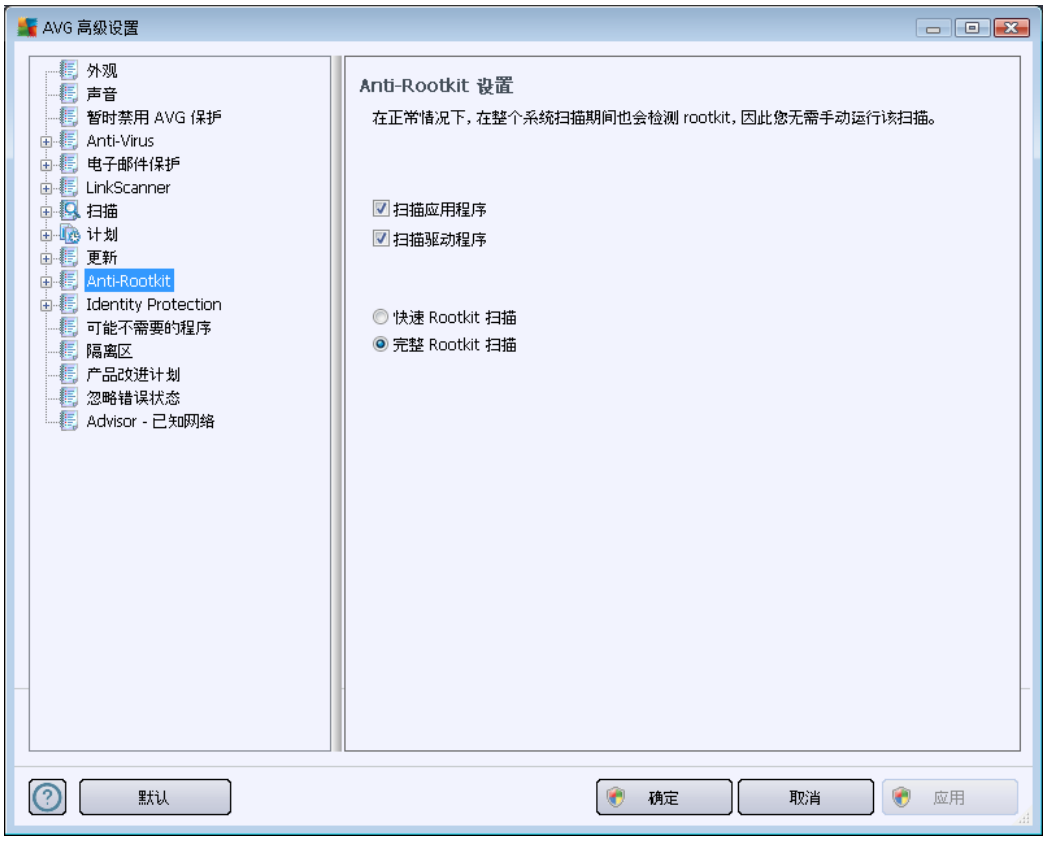


- ***'删除临时的更新文件'***–按此按钮可从硬盘上删除所有多余的更新文件 *默认情况下，这些文件的存储期限为 30 天*）
- ***'将病毒数据库恢复为上一版本'***–按此按钮可从硬盘上删除最新的病毒库版本，并恢复为以前保存的版本（*下次更新将包括新的病毒数据库版本*）

2012 版权所有 AVG Technologies CZ, s.r.o. 保留所有权利。

10.10. Anti-Rootkit

在 ***Anti-Rootkit 设置***对话框中，您可编辑 Anti-Rootkit 组件的配置和 anti-rootkit 扫描的特定参数。anti-rootkit 扫描即对整个计算机中包括的默认进程进行扫描：



此对话框中所有 Anti-Rootkit 组件功能的编辑操作，也都可以直接在 Anti-Rootkit 组件的界面中执行。

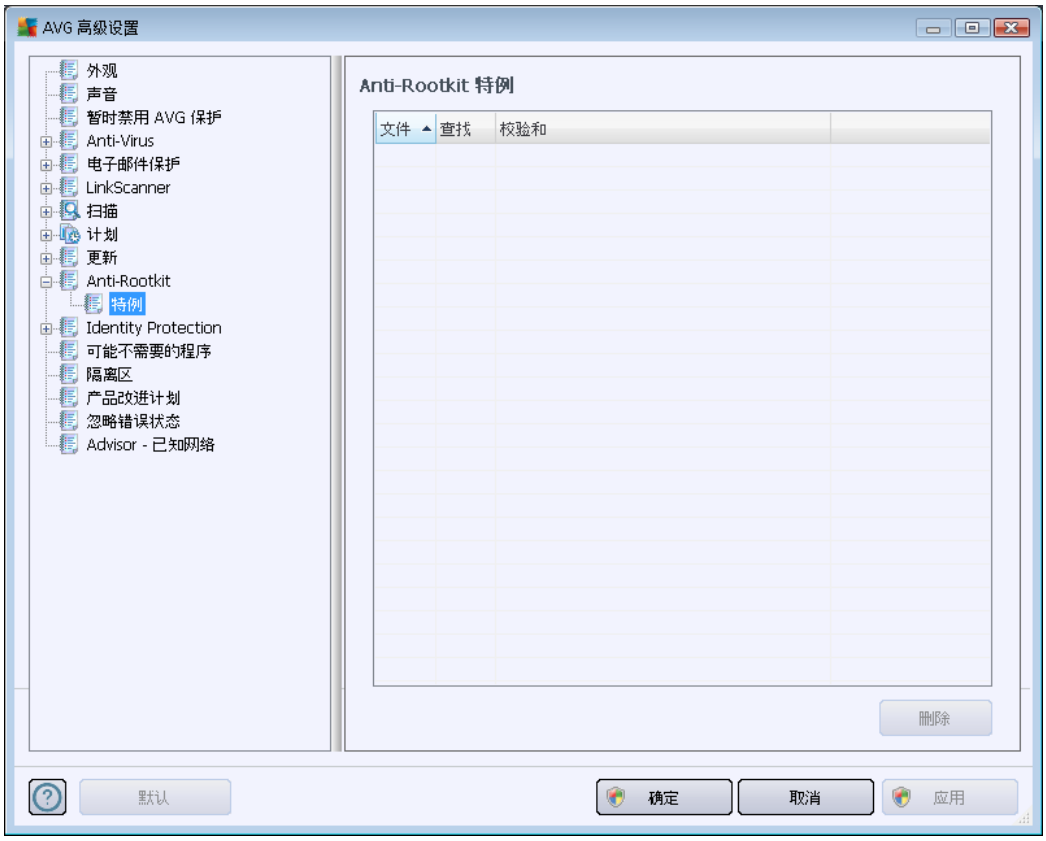
扫描应用程序和***扫描驱动程序***让您可以详细地指定 anti-rootkit 扫描应包含的内容。这些设置供高级用户使用；我们建议将所有选项都保持启用。此外，还可以选择 Rootkit 扫描模式：

- ***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、已加载的驱动程序和系统文件夹 *(通常是 c:\Windows)*，以及所有本地磁盘 *(包括闪存盘，但不包括软盘/CD 驱动器)*

2012 版权所有 AVG Technologies CZ, s.r.o. 保留所有权利。

10.10.1. 特例

在 ***Anti-Rootkit 特例*** 对话框中，可指定要排除在这种扫描的范围之外的特定文件 *如检测后可能会误报为 Rootkit 的某些驱动程序*）：



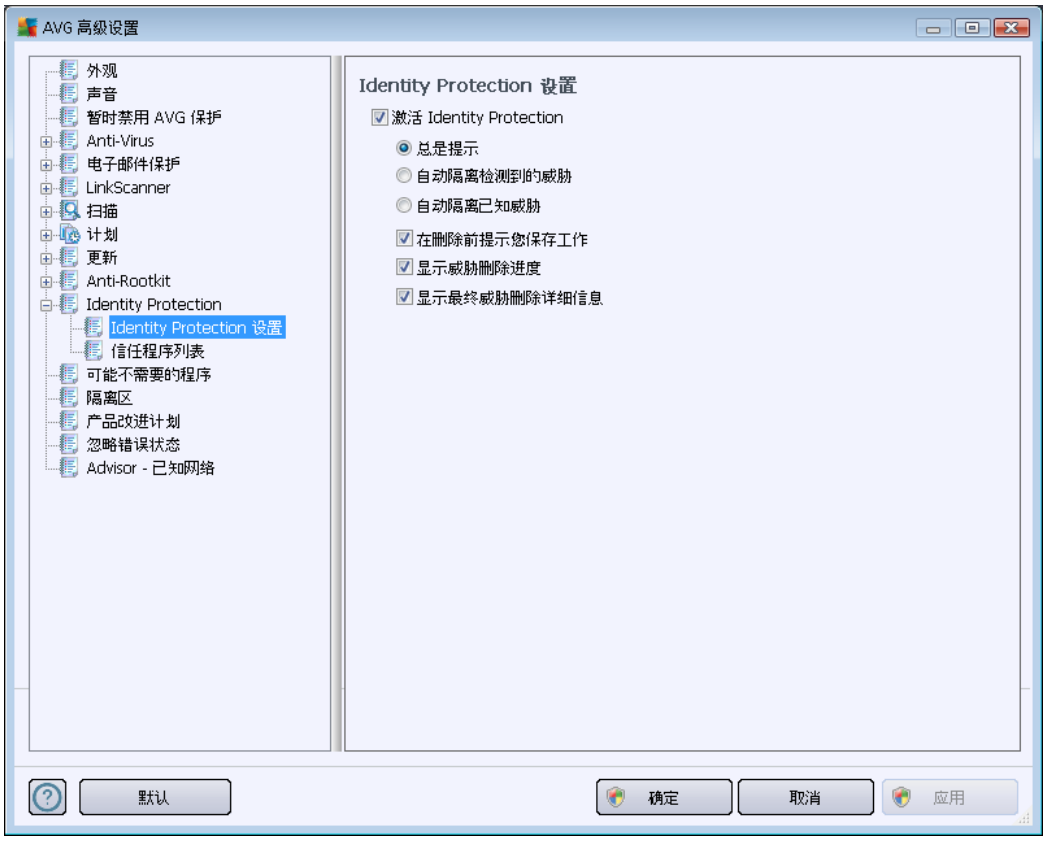
10.11. Identity Protection

Identity Protection 是一个防恶意软件组件，采用行为技术为您抵御各种恶意软件 *间谍软件、机器人、身份盗用等*）的侵害，并针对新的病毒提供零延时保护 *有关该组件功能说明的详细信息，请参阅 Identity Protection 一章*）。

2012 版权所有 AVG Technologies CZ, s.r.o. 保留所有权利。

10.11.1. 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 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应用程序。
- ***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 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

2012 版权所有 AVG Technologies CZ, s.r.o. 保留所有权利。

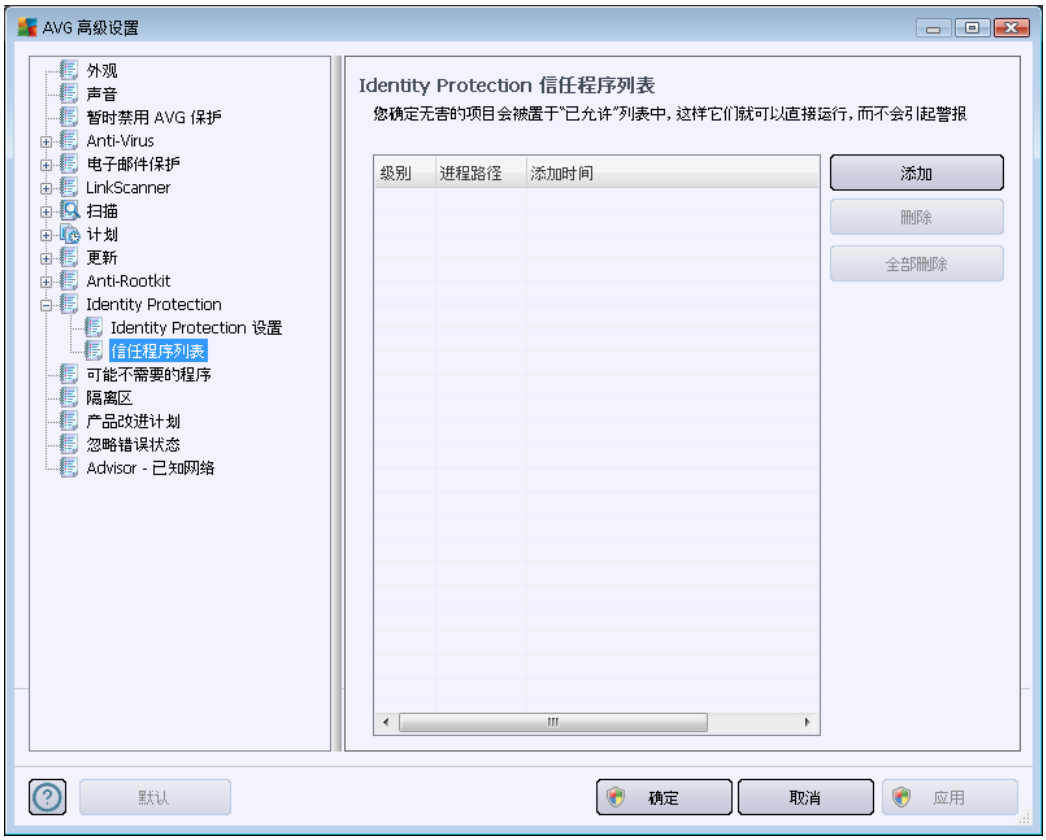
恶意软件的应用程序移到隔离区中之前收到警告，请保持此选项的选中状态。如果您正在使用该应用程序，您需要先保存项目以防丢失。默认情况下已启用此选项，强烈建议保持其已启用状态。

- ***显示威胁删除进度*** - *（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，以显示将恶意软件移到隔离区的进度。

- ***显示最终的威胁删除详细信息*** - *（默认情况下已启用）* - 启用此选项后，***Identity Protection*** 会显示有关移到隔离区中的各个对象的详细信息 *（严重程度、位置等）*。).

10.11.2. “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

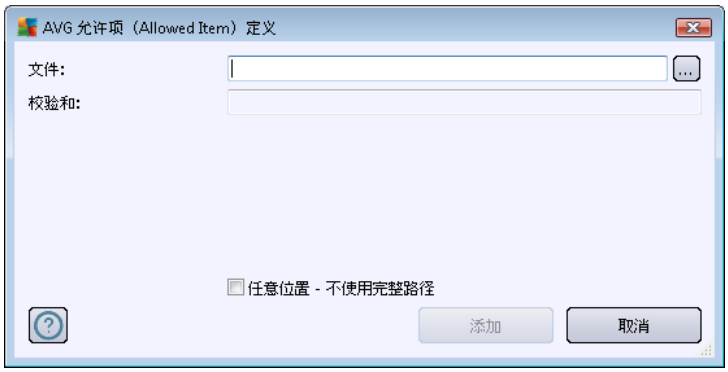
 2012 版权所有 AVG Technologies CZ, s.r.o. 保留所有权利。

- ***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：



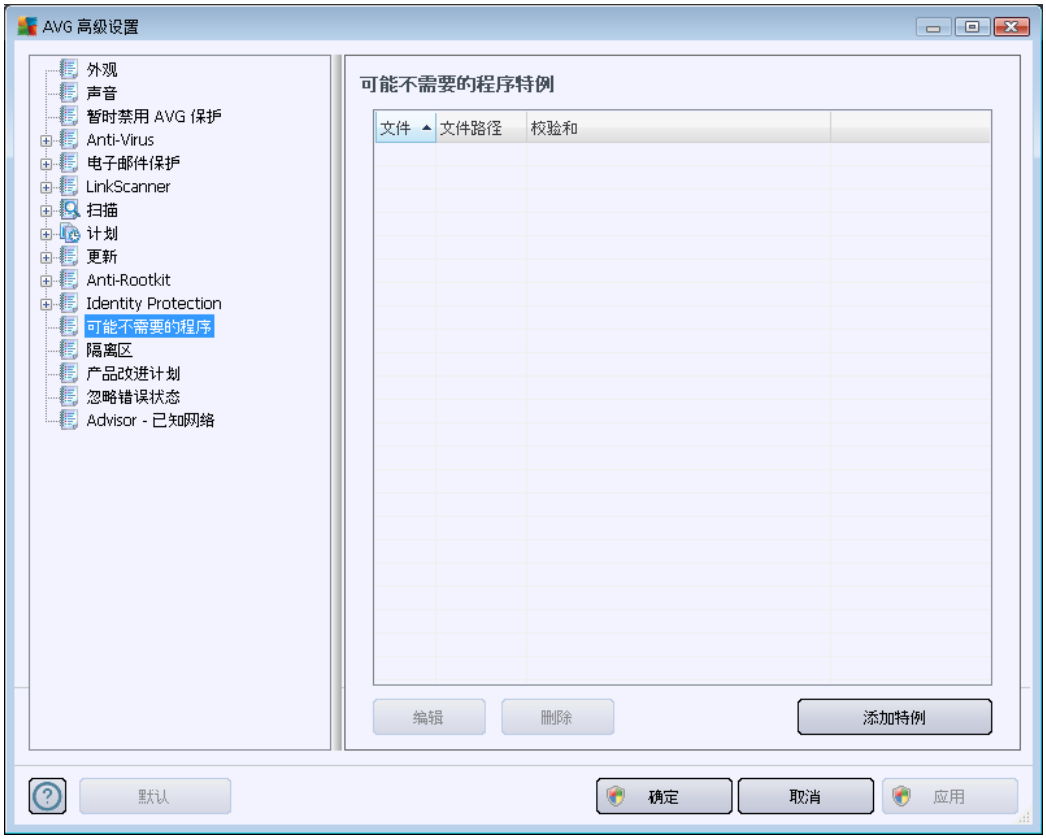
  - ***文件*** - 键入要标记为特例的文件（*应用程序*）的完整路径
  - ***校验和*** - 显示所选文件的唯一"签名"。此校验和是一个自动生成的字符串，AVG 通过它可明确地将所选文件与其它文件区分开来。此校验和在成功添加文件后生成并显示。
  - 任意位置 - 不使用完整路径 - 如果您希望将此文件仅定义为特定位置的特例，那么请将此复选框保留为未选中状态

- ***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

10.12. 可能不需要的程序

AVG Internet Security 2012 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 Internet Security 2012** 可能会检测到此类广告软件并将其报告为*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：

2012 版权所有 AVG Technologies CZ, s.r.o. 保留所有权利。



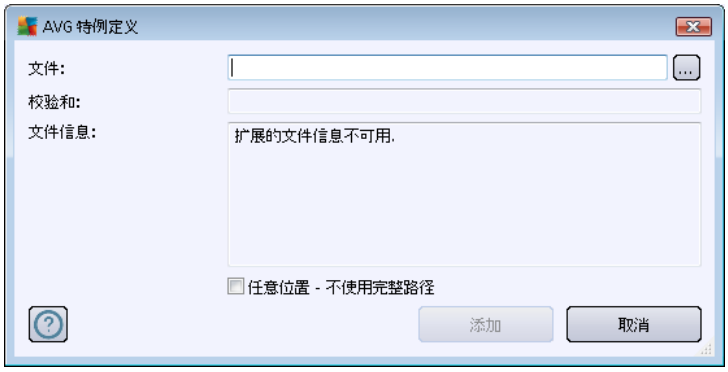
"可能不需要的程序特例" 对话框列出了已定义且当前有效的 可能不需要的程序 的特例。您可以对此列表进行编辑，删除现有项，或添加新特例。此列表中提供了有关每个特例的以下信息：

- ***文件*** - 用于提供相应应用程序的确切名称
- ***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，您可以在此对话框中定义要创建的新特例的参数：

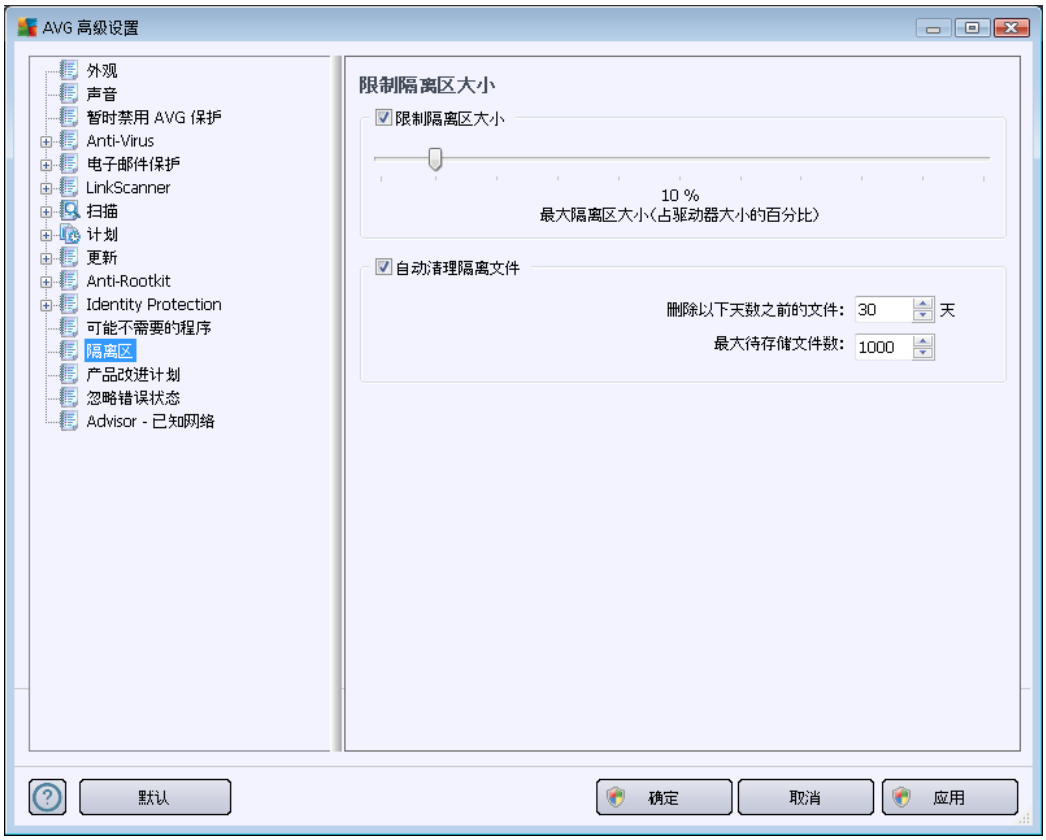
 2012 版权所有 AVG Technologies CZ, s.r.o. 保留所有权利。



- ***文件*** - 请键入您要标记为特例的文件的完整路径
- ***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。
- ***文件信息*** - 用于显示关于此文件的任何其它可用信息 *(许可证/版本信息等)*
- ***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，那么请保持此复选框的未选中状态。如果选中此复选框，指定的文件无论其位于*何处，都会被指定为特例 但是，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*)。

2012 版权所有 AVG Technologies CZ, s.r.o. 保留所有权利。

10.13. 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：

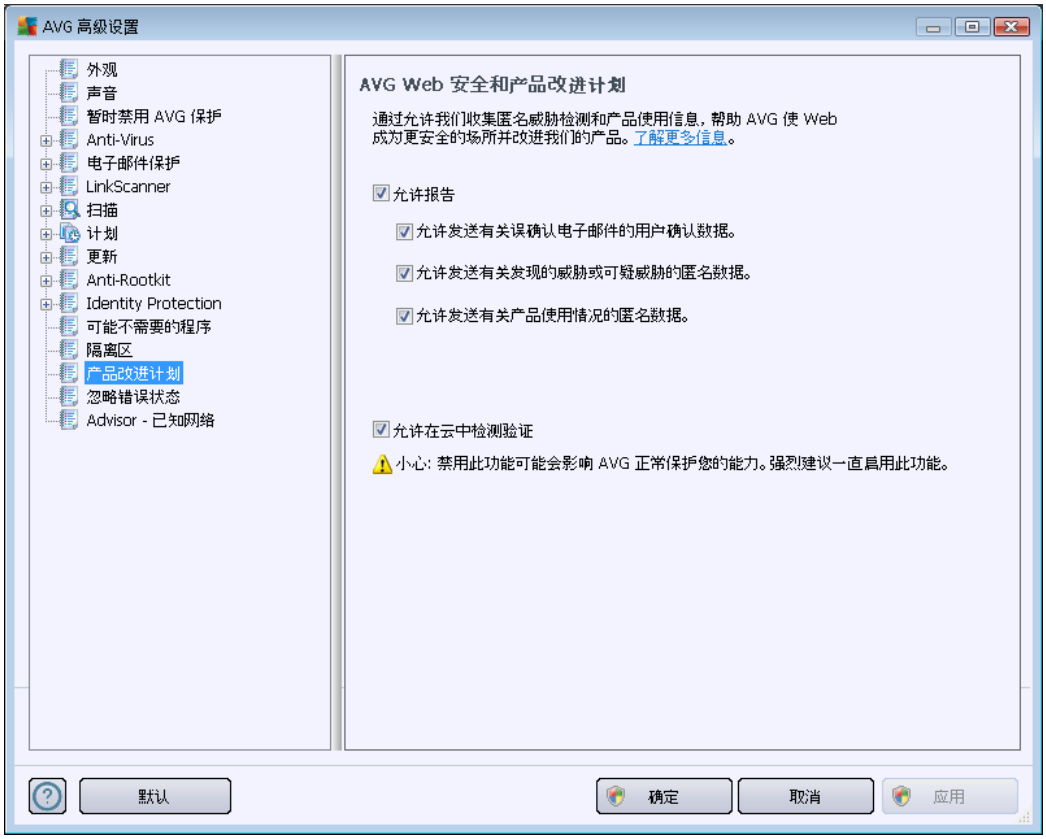
- ***限制病毒库大小*** - 可用滑块设置病毒库大小上限。此大小根据您本地磁盘的大小按比例指定。
- ***自动删除文件*** - 在此区域中，请定义对象应被存储在病毒库中的时间上限 (***删除存储时间超过 ... 天的文件***)，以及病毒库中的待存储文件数上限 (***要存储的最大文件数***)。

10.14. 产品改进计划

AVG Web 安全和产品改进计划 对话框用于邀请您参加 AVG 产品改进，并帮助我们提升 Internet 总体安全级别。保持 ***允许报告*** 选项的选中状态，即可向 AVG 实验室报告检测到的威胁。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，然后我们就会提升对所有用户的保护程度。

报告会自动进行，因此不会引起不便，也不会在报告中添加个人数据。 报告检测到的威胁是可选操作，但我们也确实请求您保持此选项的已启用状态。这有助于我们为您和其它 AVG 用户改善保护功能。

2012 版权所有 AVG Technologies CZ, s.r.o. 保留所有权利。



在该对话框中，提供了以下选项：

- ***允许报告*** *（默认情况下已启用）*- 如果想要帮助我们进一步改进**AVG Internet Security 2012**，请选择该复选框。它可向 AVG 报告所有遇到的威胁，这样我们将能够从世界各地的所有参与者处收集有关恶意软件的最新信息，然后就会提升对所有用户的保护程度。报告会自动进行，因此不会引起不便，也不会在报告中添加个人数据。
  - ***允许发送客户确认的关于未被正确识别的电子邮件的数据*** *（默认情况下已启用）*–发送有关被错误识别为垃圾邮件的电子邮件或有关 Anti-Spam 组件未检测到的垃圾邮件的信息。当发送此类信息时，系统将要求您确认。
  - ***允许发送有关识别身份的或可疑威胁的匿名数据*** *（默认情况下已启用）*–发送在计算机上检测到的有关任何可疑或确实危险的代码或行为模式 *（可能为病毒、间谍软件，或要访问的恶意网页）*的信息。
  - ***允许发送有关产品使用情况的匿名数据*** *（默认情况下已启用）*–发送有关应用程序使用情况的基本统计信息（例如，检测、已启动扫描、成功或不成功更新等项的数目）。
- ***允许在云中验证检测*** *（默认情况下已启用）*–对检测到的威胁进行检查以确认是否真的受到感染，以免出现误报。

2012 版权所有 AVG Technologies CZ, s.r.o. 保留所有权利。

最常见的威胁

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进行的。

- ***可能不需要的程序***是一类间谍软件，它们可能但不一定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***也可视为一类间谍软件，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***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是利用"愚弄邮件"来传播。

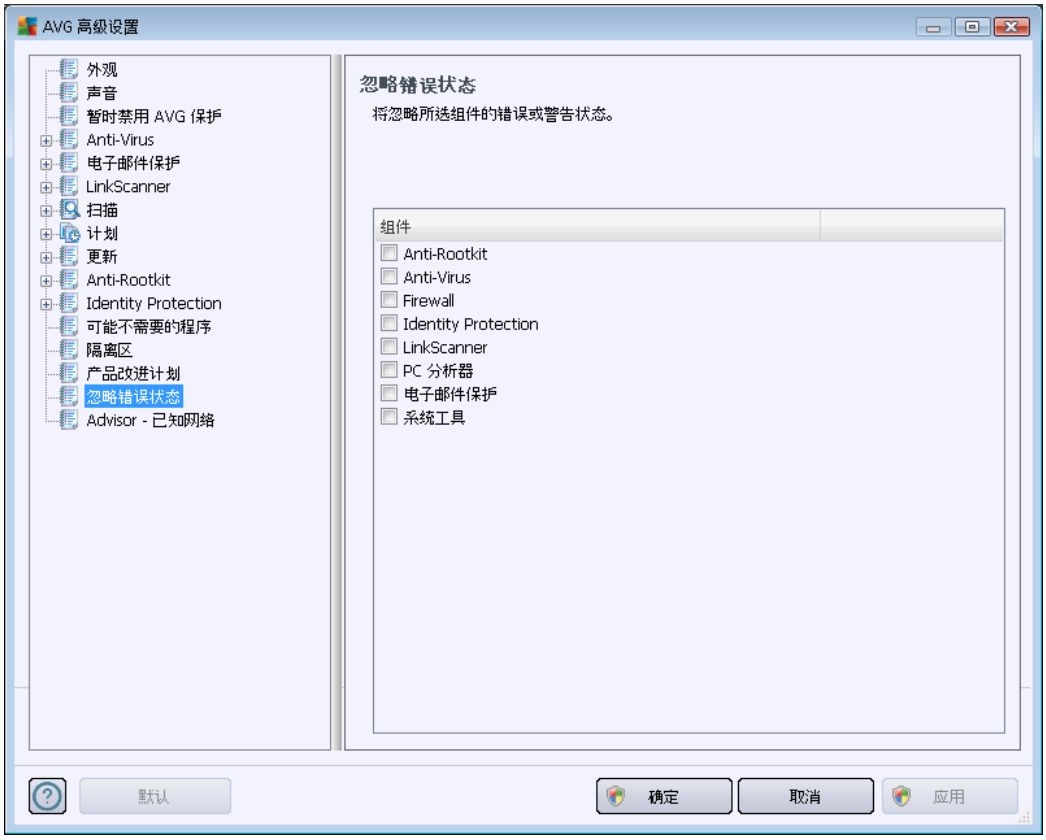
- ***恶意网站***会故意在访客的计算机中安装恶意软件，与一些已被病毒传染的站点一样，只是这些站点是已被传播威胁的访客侵入的合法网站。

为防止受到上述所有不同类型威胁的侵扰，AVG Internet Security 2012 包含一些专用组件。有关这些组件的简短说明，请查阅[组件概览](#)一章。

 2012 版权所有 AVG Technologies CZ, s.r.o. 保留所有权利。

10.15. 忽略错误状态

在 ***忽略错误状态*** 对话框中，可选中不想了解其情况的组件：



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 *(忽略组件状态)*。

2012 版权所有 AVG Technologies CZ, s.r.o. 保留所有权利。

10.16. Advisor - 已知网络

AVG Advisor 包含监控您所连接到的网络的功能。如果发现了新网络 *(带有已使用的网络名称，并让您感到困扰)*，则它将通知您并建议您检查网络的安全性。如果您确定新网络安全，可以连接，您也可将其保存到该列表 ;然后，AVG Advisor 将记住该网络的唯一属性 *(特别是 MAC 地址)*，且下次不会显示通知。

在该对话窗口中，您可检查已保存为已知的网络。您可通过按***删除***按钮删除各个条目 ;然后，相应的网络就再次被视为未知且可能不安全的网络。

 2012 版权所有 AVG Technologies CZ, s.r.o. 保留所有权利。

11. 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。

但是，所有 AVG Internet Security 2012 组件均已由软件供应商为了提供最佳性能而设置好。除非确实有理由更改默认配置，否则请勿如此操作。所有设置更改都应该仅由经验丰富的用户执行。

11.1. 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，会允许传输所有网传信息，但不会对其进行检查！
- ***紧急模式(阻止所有 Internet 通讯)*** - 选中此选项将阻止通过每个网络端口的所有网传信息；Firewall 仍在运行，但所有网传信息都会受阻。

2012 版权所有 AVG Technologies CZ, s.r.o. 保留所有权利。

- ***启用所有到 VPN 的通讯*** *(默认情况下已启用)*- 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*** 部分中，可***导出*** 或***导入*** Firewall 配置；也就是将指定的 Firewall 规则和设置导出到备份文件中，另一方面，也可导入整个备份文件。

11.2. 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*** - 用于指定获允更改 Firewall 配置的用户。
- ***为以下用户显示确认对话框*** - 用于指定要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)*。

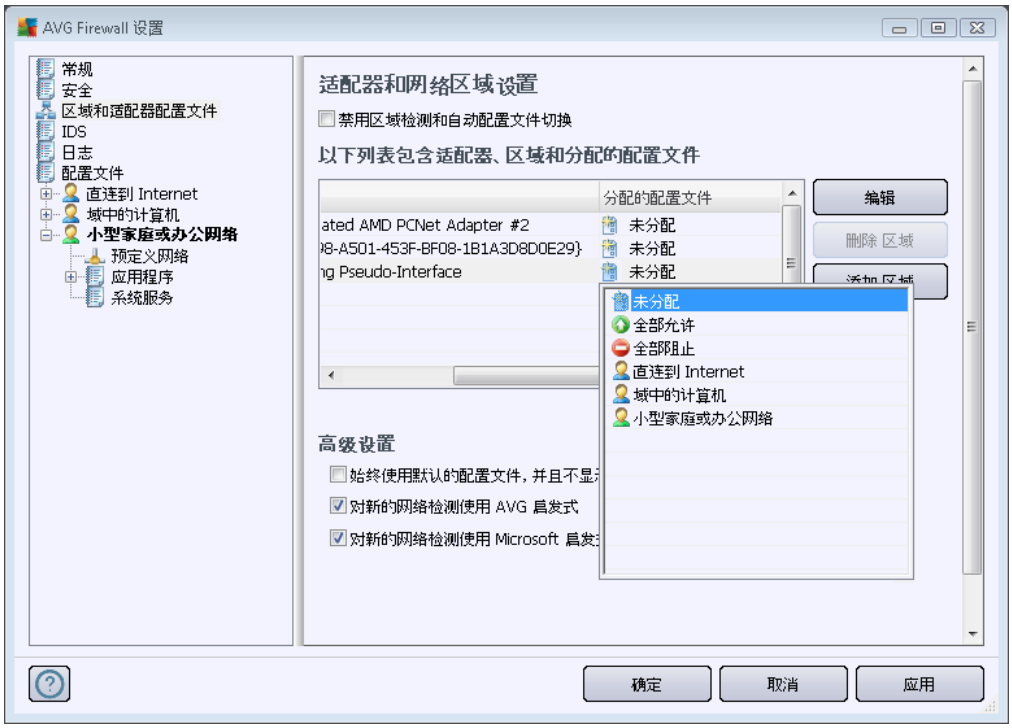
2012 版权所有 AVG Technologies CZ, s.r.o. 保留所有权利。

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它用户。

11.3. 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*** *(默认情况下已启用)* - 可分别针对每个区域，对每种网络接口类型指定其中一个指定的配置文件。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*** - 通过此列表可综览所检测到的适配器和区域。在指定的配置文件的菜单中，可为其中的每个适配器或区域指定特定配置文件。要打开此菜单，请 *在 分配的配置文件 列中)*用鼠标左键单击适配器列表中的相应适配器，然后从上下文菜单中选择配置文件。

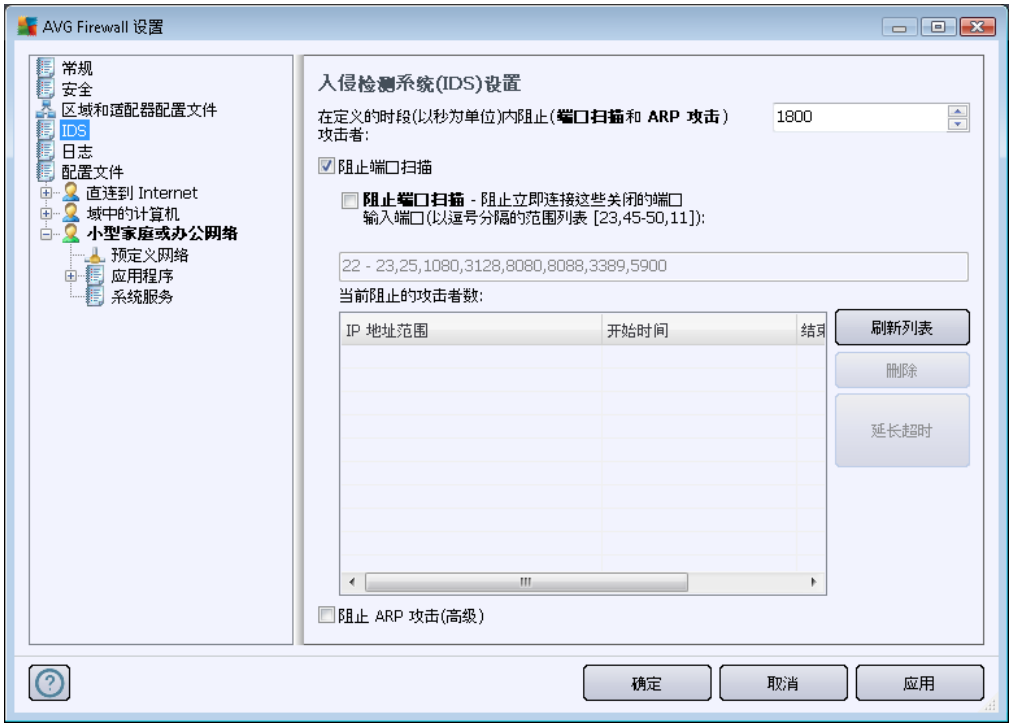
2012 版权所有 AVG Technologies CZ, s.r.o. 保留所有权利。

高级设置

- ***始终使用默认的配置文件，并且不显示新的网络检测对话框*** - 每当计算机连接到新网络时，Firewall 都会发出警报，并显示一个对话框，提示在其中选择网络连接类型并为其指定 Firewall 配置文件。如果不想显示该对话框，请选中此框。
- ***对新的网络检测使用 AVG 启发式*** - 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)*。
- ***对新的网络检测使用 Microsoft 启发式*** - 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 和更高版本中使用)*。

11.4. 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讯尝试。可在***入侵检测系统(IDS)设置*** 对话框中配置 IDS 参数：



入侵检测系统 (IDS) 设置 对话框中有以下配置选项：

- ***在定义的时段(以秒为单位)内阻止(端口扫描和 ARP 攻击)攻击者*** - 可在此处指定某个端口上检测到可疑通讯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*** *(默认情况下已启用)* - 选中该框可阻止从外部通过所有 TCP 和 UDP

2012 版权所有 AVG Technologies CZ, s.r.o. 保留所有权利。

端口向计算机进行的通讯尝试。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。该选项默认情况下会处于已启用状态，建议保留这种设置。如果保持***阻止端口扫描*** 选项的已启用状态，则可进行一些更详细的配置 *否则会禁用以下选项*）：

  - ***阻止端口扫描*** - 选中此框可立即阻止通过以下文本字段中指定的端口进行的任何通讯尝试。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。

  - 当前阻止的攻击者数 - 此部分中列有 Firewall 目前已阻止的任何通讯尝试。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。

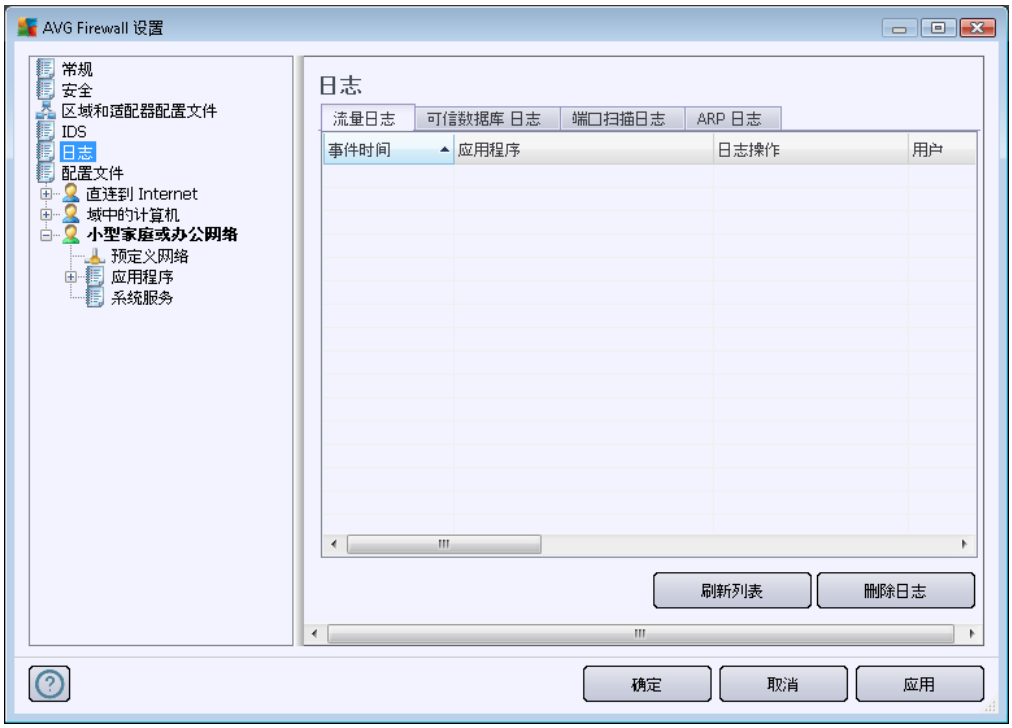
- ***阻止 ARP 攻击(高级)*** *默认情况下已禁用*）- 对于 ***IDS*** 检测到并认定为潜在危险网络的，本地网络中的特定类型的通讯内容，选中此选项可对其进行阻止。***"在定义的时段内阻止攻击者"*** 中设置的时间在此适用。我们建议仅由熟悉本地网络类型和风险级别的高级用户使用此功能。

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。

2012 版权所有 AVG Technologies CZ, s.r.o. 保留所有权利。

11.5. 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 "***–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*** - 用于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

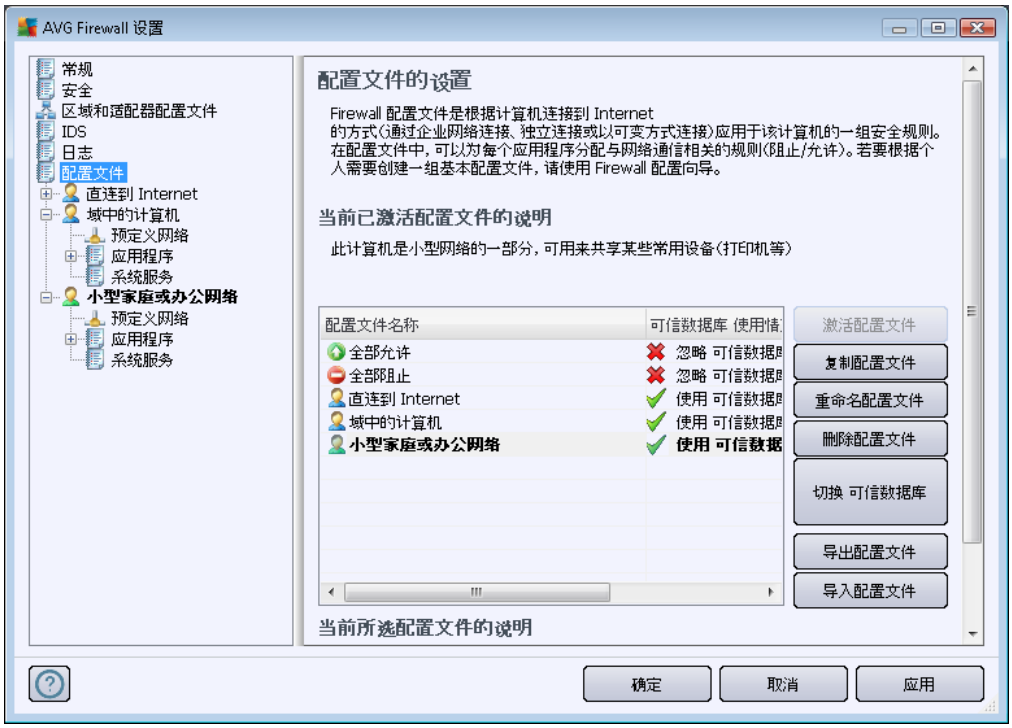
- ***刷新列表*** - 可以按照所选属性对所有已记录的参数进行排列 :按时间顺序排列（*日期*）或按字母顺序排列（*其它列*），只须单击相应列标题即可。使用 ***刷新列表*** 按钮可更新当前显示的信息。

2012 版权所有 AVG Technologies CZ, s.r.o. 保留所有权利。

- ***删除日志*** - 按此按钮可删除图表中的所有条目。

11.6. 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。



不能编辑系统配置文件 *(全部允许、全部阻止)*。但是，所有自定义配置文件 *(直连到 Internet、域中的计算机、小型家庭或办公网络)*都能直接在此对话框中用以下控制按钮编辑：

- ***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讯。
- ***复制配置文件*** - 用于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*** - 用其可为选定的配置文件指定新的名称。
- ***删除配置文件*** - 用于从列表中删除选定的配置文件。
- ***切换可信数据库*** - 对于所选配置文件，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讯。)*。
- ***导出配置文件*** - 用于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。

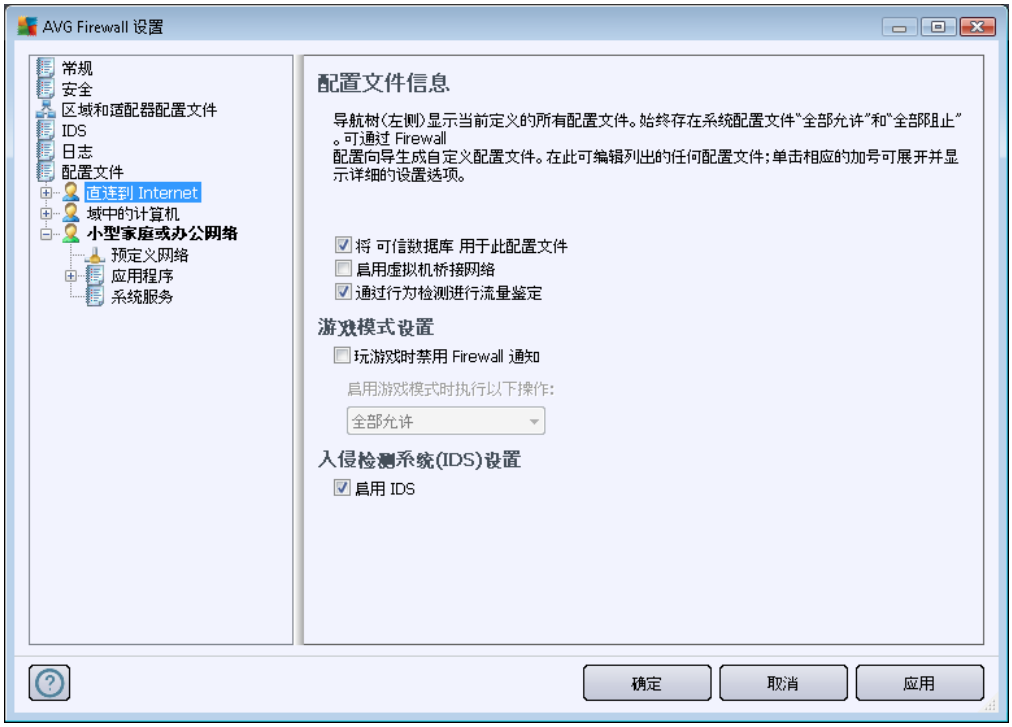
 2012 版权所有 AVG Technologies CZ, s.r.o. 保留所有权利。

- ***导入配置文件*** - 用于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：

11.6.1. 配置文件信息



'配置文件信息' 对话框是一个区域的首个对话框，在此区域中，您可以通过涉及配置文件特定参数的多个单独的对话框编辑每个配置文件的配置。

- ***将可信数据库用于此配置文件*** -*(默认情况下已启用)* 选中此选项可为相应配置文件激活*可信数据库(即收集进行在线通讯的可信、经认证应用程序的信息的 AVG 内部数据库)。如果尚未为对应的应用程序指定规则，则有必要确定是否可以向该应用程序授予网络访问权限。AVG 会先在可信数据库中进行搜索，如果发现其中列出了此应用程序，则会将它视作安全应用程序，从而允许它通过网络进行通信。否则，将会让您决定是否应允许此应用程序通过网络进行通信)*

- ***启用虚拟机桥接网络*** -*(默认情况下已禁用)* 选中此项可允许 WMware 中的虚拟机直接连接到网络。

- ***通过行为检测进行通讯鉴定*** -*(默认情况下已启用)* 选中此选项可允许 Firewall 在评估应用程序时使用 Identity Protection 功能，因为 Identity Protection 可以辨别此应用程序是否暴露出任何可疑行为，或者是否可以信任它进而允许它进行在线通

讯。

游戏模式设置

在***游戏模式设置***部分中，可通过选中相应项决定并确认是否希望即使在计算机上运行全屏应用程序（*通常为游戏，但适用于任何全屏应用程序，如 PPT 演示文稿*）时也要让Firewall提示消息显示，因为提示消息会产生一定的干扰。

如果您勾选***玩游戏时禁用 Firewall 通知***项，请在下拉菜单中选择在尚未指定规则的新应用程序（*通常会导致询问对话框显示的应用程序*）试图通过网络进行通信时要采取何种操作，对所有此类应用程序均可以执行允许或阻止操作。

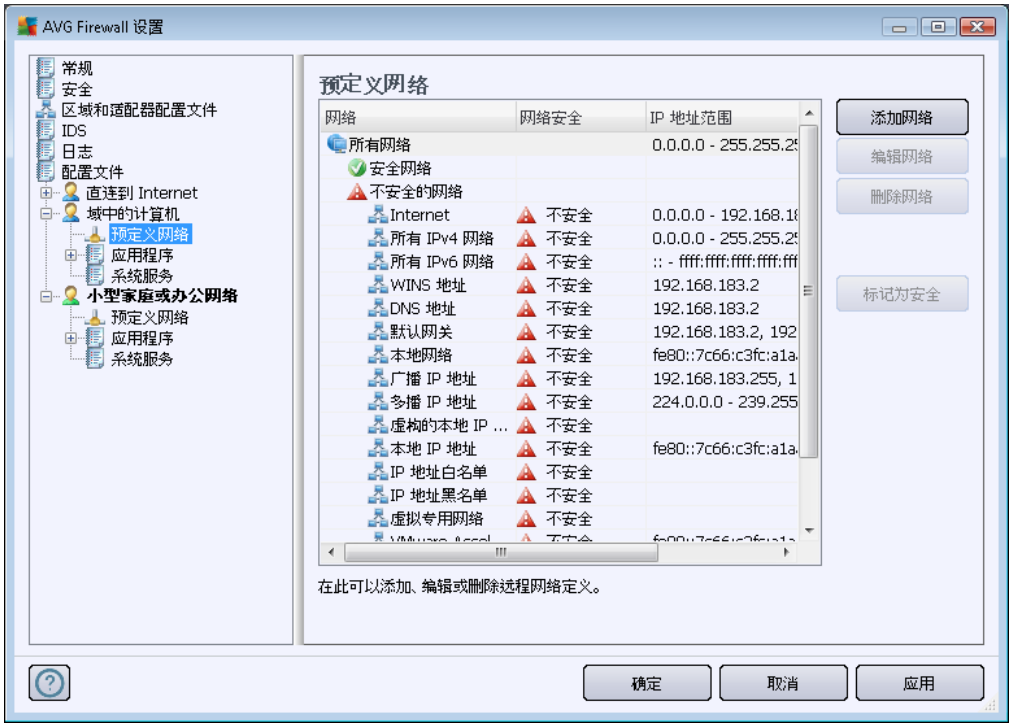
在启用了游戏模式的情况下，所有计划的任务（*扫描、更新*）都将推迟执行，直到全屏应用程序关闭为止。

入侵检测系统 (IDS) 设置

选中***启用 IDS***复选框可激活专门的行为分析功能，旨在发现和阻止计算机特定端口上的可疑通讯尝试（*有关此功能设置的详细信息，请参阅本文档的 IDS 一章*）。

11.6.2. 预定义网络

预定义网络对话框提供了您的计算机连接到的所有网络的列表。



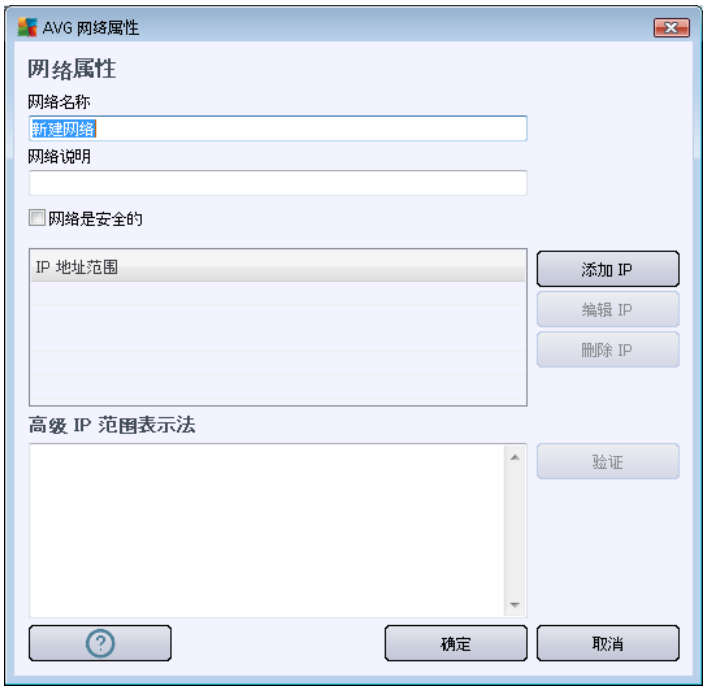
该列表中有关于检测到的各个网络的以下信息：

 2012 版权所有 AVG Technologies CZ, s.r.o. 保留所有权利。

- ***网络*** - 其中有与计算机相连的所有网络的名称列表。
- ***网络安全*** - 默认情况下会将所有网络都视为不安全网络，仅当确信相应网络是安全网络时，才能将其指定为安全网络 *(单击有关相应网络的列表项，然后从上下文菜单中选择 安全)*，所有安全网络都会划分到一组中，将应用程序规则设置为只允许与安全网络通讯后，应用程序就可以通过其中的网络进行通讯。
- ***IP 地址范围*** - 将自动检测每个网络，并以 IP 地址范围的形式加以指定。

控制按钮

- ***添加网络*** - 用于打开***网络属性*** 对话框窗口，从中可编辑新指定的网络的参数：



在此对话框中，可指定***网络名称***，提供***网络说明***，还可以将网络指定为安全网络。也可在一个独立对话框中手动指定新网络，此对话框可通过***添加 IP*** 按钮 *(*也可以通过***编辑 IP***/***删除 IP***) 打开，可在此对话框中通过提供网络的 IP 范围或掩码指定网络。如果有大量网络要被指定为新建网络的一部分，则可以使用***高级 IP 范围表示法*** 选项：请在相应文本字段中输入所有网络的列表 *(支持任何标准格式)*，然后按***验证*** 按钮以确保可以识别所用格式。然后按***确定*** 确认并保存数据。

- ***编辑网络*** - 用于打开***网络属性*** 对话框窗口 *(见上文)*，从中可编辑已指定的网络的参数 *(此对话框与用于添加新网络的对话框相同，请参见上一段中的说明)*。
- ***删除网络*** - 用于从网络列表中删除所选网络的名称。
- ***标记为安全*** - 默认情况下会将所有网络都视为不安全网络，仅当确信相应网络是安全网络时，才能用此按钮将其指定为安全网络 *(反之亦然，将网络指定为安全网*

 2012 版权所有 AVG Technologies CZ, s.r.o. 保留所有权利。

络后，按钮文本也会变成 '标记为不安全 '）。

11.6.3. 应用程序

'应用程序信息 '对话框用于列出可能需要进行网络通信的所有已安装应用程序，以及已指定的操作的图标：

应用程序列表中的应用程序是在计算机中检测到 *（并已指定相应的操作）*的应用程序。可使用以下操作类型：

- - 允许与所有网络通信
- - 只允许与定义为 '安全 '的网络通信
- - 阻止通信
- - 显示询问对话框 *（用户将能在应用程序尝试通过网络通信时决定是要允许还是阻止该通信）*
- - 已定义高级设置

请注意，只有已安装的应用程序才会被检测到，因此如果以后安装了新应用程序，就必须为其指定 Firewall 规则。默认情况下，当新的应用程序首次尝试通过网络进行连接时，Firewall 会根据可信数据库自动为它创建一项规则，或者询问您是允许还是阻止此通信。在后一种情况下，所作的回答能作为永久规则保存下来（然后会将其列在此对话框中）。

当然，也可以立即对新应用程序指定规则，方法是在此对话框中按***'添加 '***，然后填写应用

2012 版权所有 AVG Technologies CZ, s.r.o. 保留所有权利。

程序详细信息。

除了应用程序外，此列表还包含两个特殊项目：

- ***"优先应用程序规则"***（*位于列表顶部*）是优先规则，始终会先于任一应用程序的规则得到应用。
- ***"其它应用程序规则"***（*位于列表底部*）可在没有适用的具体应用程序规则的情况（例如，对于未知和不明应用程序）下用作"最后的措施"。选择在尝试网络通信时应触发的操作：
  - *阻止* - 始终阻止通信。
  - *允许* –允许通过任何网络进行通信。
  - *询问* –系统将会让您来决定是应允许还是应阻止此通信。

这些项目的设置选项不同于普通应用程序，仅供经验丰富的用户使用。强烈建议不要修改这些设置！

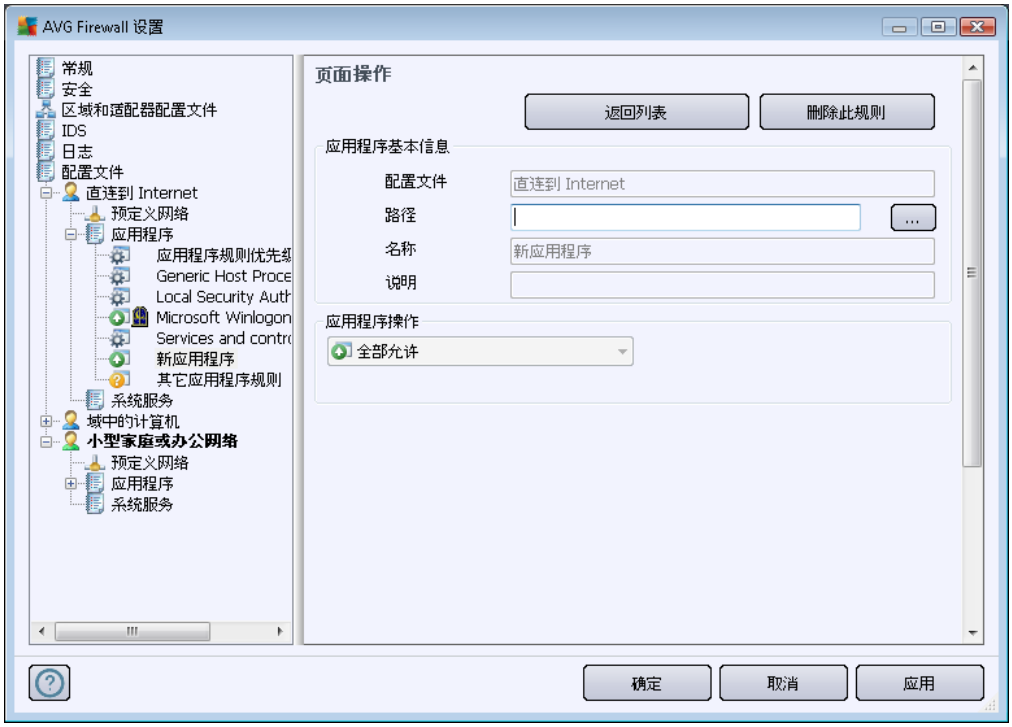
控制按钮

此列表可使用以下控制按钮进行编辑：

- ***添加*** - 用于打开一个空的页面操作对话框，用于指定新应用程序规则。
- ***编辑*** - 用于打开相同的页面操作对话框，其中的数据用于编辑一些现有的应用程序规则。
- ***删除*** - 用于从列表中删除所选应用程序。

 2012 版权所有 AVG Technologies CZ, s.r.o. 保留所有权利。

在 ***页面操作*** 对话框中，可以详细指定相应应用程序的设置：



控制按钮

该对话框顶部有两个控制按钮：

- ***返回列表*** - 按该按钮可综览已指定的所有应用程序规则。
- ***删除此规则*** - 按该按钮可清除目前已显示出来的应用程序规则。***请注意，此操作不能撤消！***

应用程序基本信息

在此部分中，请填写应用程序 ***"名称"***（也可以选填 ***"说明"***（*供您自己参考的简短注释*）。在 ***"路径"*** 字段中，输入应用程序（*可执行文件*）在磁盘上的完整路径；也可以按 *"..."* 按钮，然后方便地在树结构中找到该应用程序。

应用程序操作

在下拉菜单中，可以选择要应用于该应用程序的 Firewall 规则，即当该应用程序在尝试通过网络进行通信时，Firewall 应如何处理：

- ***允许与所有网络通讯*** - 用于允许该应用程序无限制地通过所有已指定的网络

 2012 版权所有 AVG Technologies CZ, s.r.o. 保留所有权利。

和适配器通讯。

- ***只允许与安全网络通讯*** - 用于允许该应用程序通过已指定为安全 *值得信任*）的网络通讯。
- ***阻止*** - 用于自动禁止通讯 ;将不许该应用程序连接到任何网络。
- ***询问*** - 用于显示一个对话框，这样当时就能决定是允许还是阻止该通讯尝试。
- ***高级设置*** - 用于显示其它详细设置选项，显示在对话框底部的***应用程序详细规则*** 部分中。将按照列表顺序应用这些详细规则，因此您可以根据需要在列表中***“上移”***或***“下移”***这些规则，以设置其优先顺序。单击列表中的特定规则后，会在对话框底部显示规则详细信息概况。在相应的设置对话框中单击任何带下划线的蓝色值，都可以对其进行更改。要删除突出显示的规则，只须按***“删除”***即可。要定义新规则，请用***“添加”***按钮打开***“更改规则详细信息”***对话框，这样就可以指定所有必需的详细信息。

11.6.4. 系统服务

只有经验丰富的用户才能在“系统服务和协议”对话框中进行编辑！

系统服务和协议 对话框中列有可能需要通过网络进行通讯的 Windows 标准系统服务及协议：

系统服务和协议的列表

图表中含有以下几列：

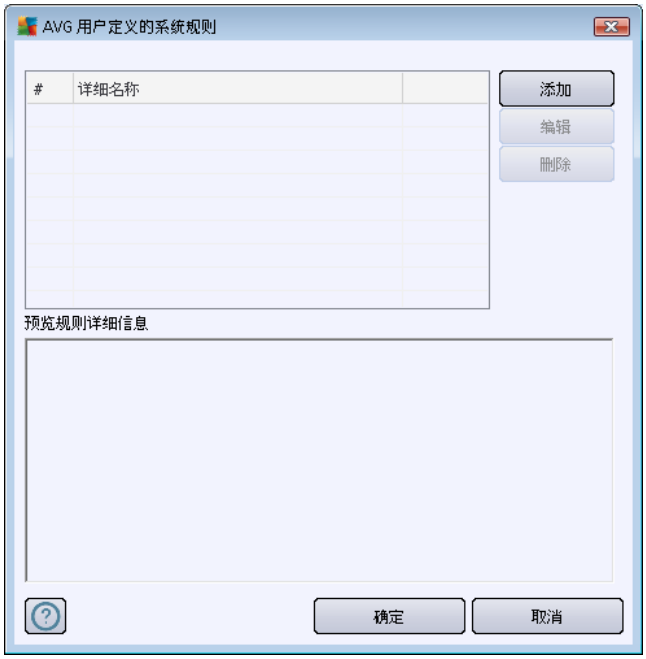
 2012 版权所有 AVG Technologies CZ, s.r.o. 保留所有权利。

- ***记录规则操作*** - 通过此框能启用将规则的每次应用情况记入日志的功能。
- ***系统服务和协议*** - 此列用于显示相应系统服务的名称。
- ***操作*** - 此列用于显示代表所分配操作的图标：
  - 允许与所有网络通信
  - 只允许与定义为 "安全" 的网络通信
  - 阻止通信
- ***网络*** - 此列用于说明此系统规则适用于哪个特定网络。

若要编辑此列表中任何一项的设置 *(包括所分配的操作)*，请右键单击该项，然后选择 ***"编辑"。不过，应当仅限高级用户执行系统规则编辑；强烈建议不要编辑系统规则！***

用户定义的系统规则

若要打开一个新对话框以定义您自己的系统服务规则 *(见下图)*，请按 ***"管理用户系统规则"*** 按钮。通过 ***"用户定义的系统规则"*** 对话框顶部，可大概了解目前已编辑过的系统规则的所有详细信息；对话框底部显示的则是所选详细信息。通过相应的按钮可编辑、添加或删除用户定义的规则详细信息；制造商定义的规则详细信息仅可编辑：



请注意，详细规则设置都是高级设置，主要供需要完全控制 Firewall 配置的网络管理员使用。如果不熟悉通信协议类型、网络端口号、IP 地址定义等，请勿修改这些设置！如果确实需要更改配置，请查阅相应对话框帮助文件中的特定详细信息。

2012 版权所有 AVG Technologies CZ, s.r.o. 保留所有权利。

记录未知通信

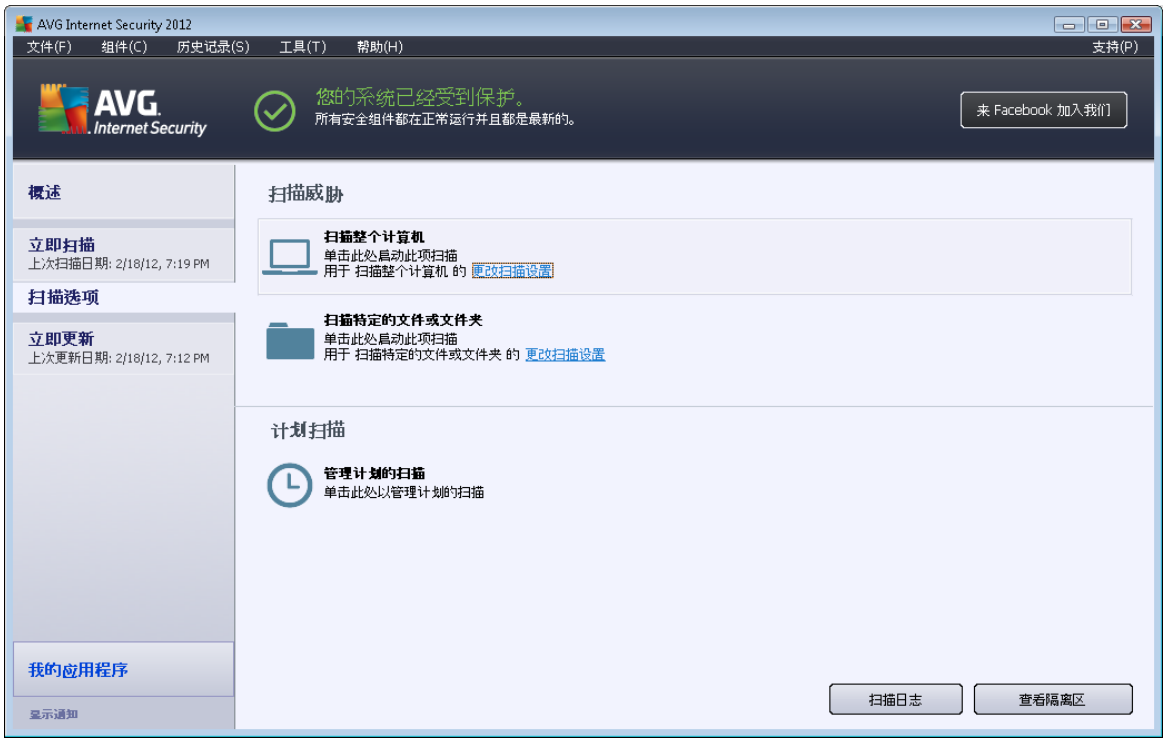
- ***记录未知的传入通讯*** *默认情况下已禁用)*- 选中此框可在每次外部有未知者企图连接到您的计算机时将这一情况记录在日志中。
- ***记录未知的传出通讯*** *默认情况下已启用)*- 选中此框可在每次您的计算机中有未知程序企图连接到外部位置时将这一情况记录在日志中。

2012 版权所有 AVG Technologies CZ, s.r.o. 保留所有权利。

12. AVG 扫描

默认情况下，**AVG Internet Security 2012** 不会执行扫描操作，因为第一次扫描执行完毕后，就应该会得到 **AVG Internet Security 2012** 常驻组件的严密保护，这些常驻组件始终处于警戒状态，根本不会让任何恶意代码进入计算机。当然，可以安排扫描，以便以固定时间间隔执行扫描，也随时均可按需手动发起扫描。

12.1. 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
- 计划扫描 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

2012 版权所有 AVG Technologies CZ, s.r.o. 保留所有权利。

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

12.2. 预定义扫描

按需扫描是 **AVG Internet Security 2012** 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。

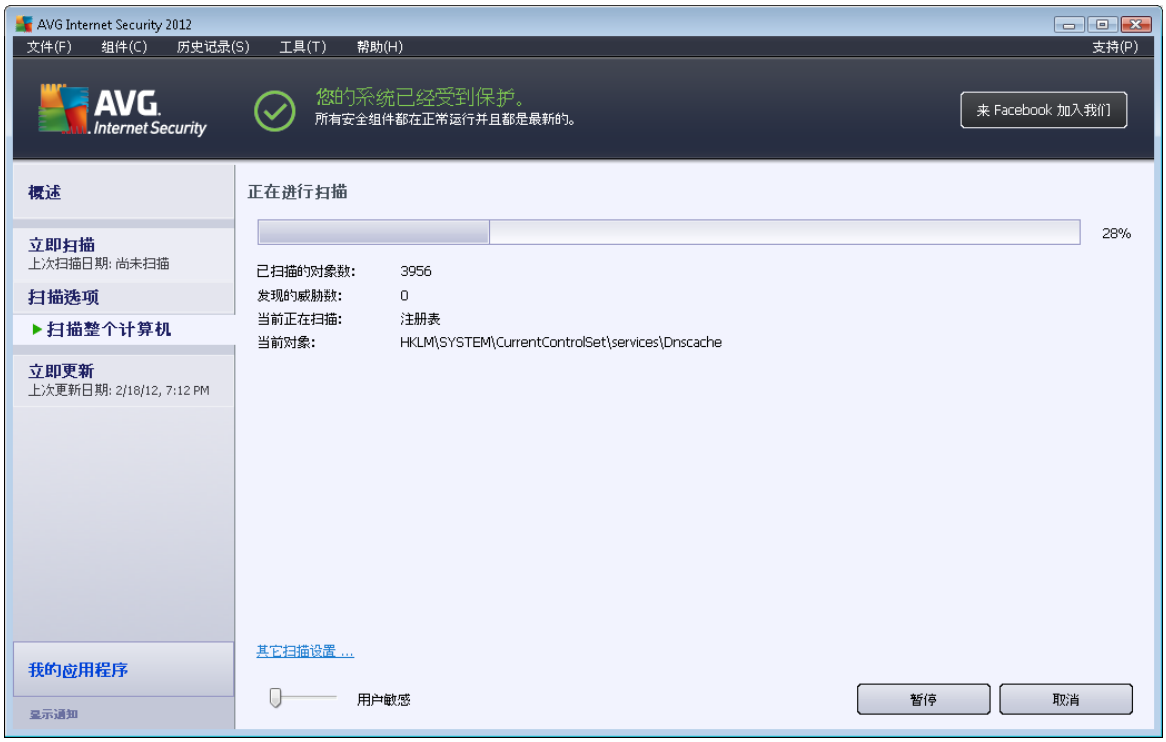
在 **AVG Internet Security 2012** 中提供了软件供应商预定义的以下扫描类型：

12.2.1. 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

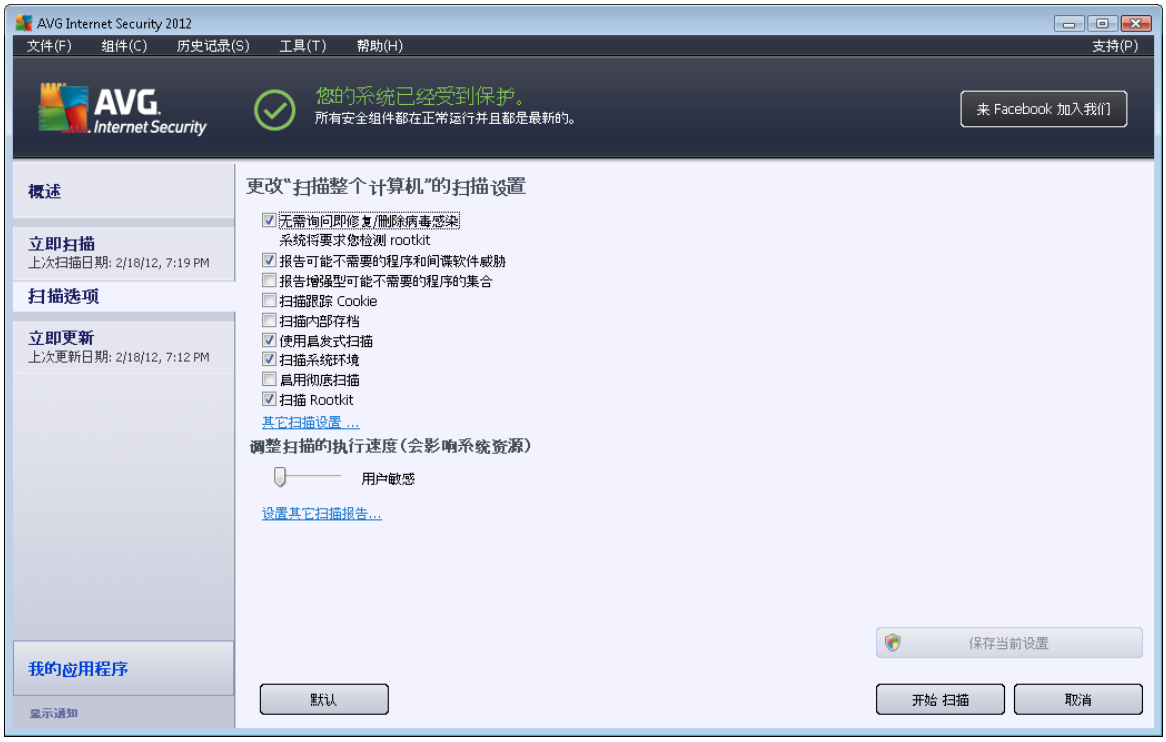
"扫描整个计算机" 可直接从扫描界面中通过单击扫描图标来启动。对于此类型的扫描，无须进一步配置任何特定设置，扫描将立即开始并显示 ***"正在进行扫描"*** 对话框 *(见截图)*。如果需要，可以暂时中断（***"暂停"***）或取消（***"停止"***）这种扫描。



 2012 版权所有 AVG Technologies CZ, s.r.o. 保留所有权利。

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：
    - ***无需询问即修复/删除病毒感染*** *(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：一些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的程序。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检测的 Cookie；*(HTTP cookies 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)*。

2012 版权所有 AVG Technologies CZ, s.r.o. 保留所有权利。

- o ***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

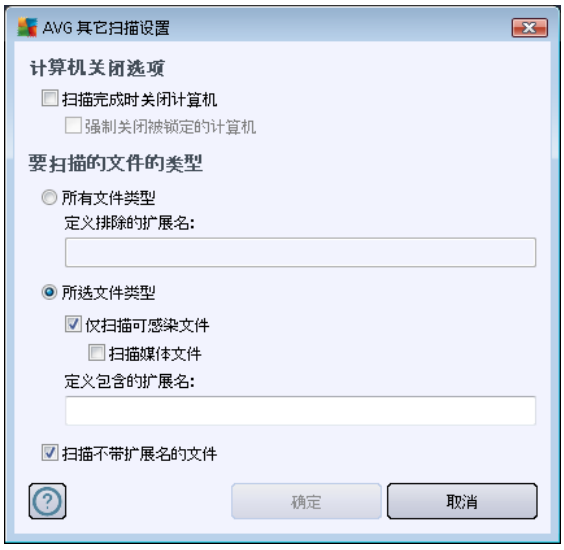
- o ***使用启发式扫描***(*默认情况下已启用*) - 启发式分析(*在虚拟的计算机环境中对已扫描对象的指令进行动态模拟*)将成为扫描期间用来进行病毒检测的方法之一。

- o ***扫描系统环境***(*默认情况下已启用*) - 扫描还将检查您计算机的系统区域。

- o ***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。但要记住,此方法相当耗时。

- o ***扫描 rootkit***(*默认情况下已启用*) - Anti-Rootkit 用于在您的计算机中搜索是否可能存在 rootkit(例如,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。

- ***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:



- o ***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。

- o ***要扫描的文件的类型*** - 应该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*

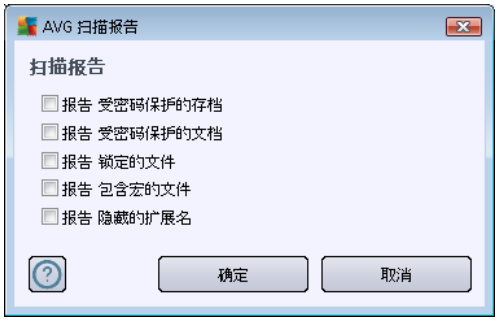
 2012 版权所有 AVG Technologies CZ, s.r.o. 保留所有权利。

)，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*** - 该链接用于打开新的***扫描报告***对话框，从中可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。*

12.2.2. 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。

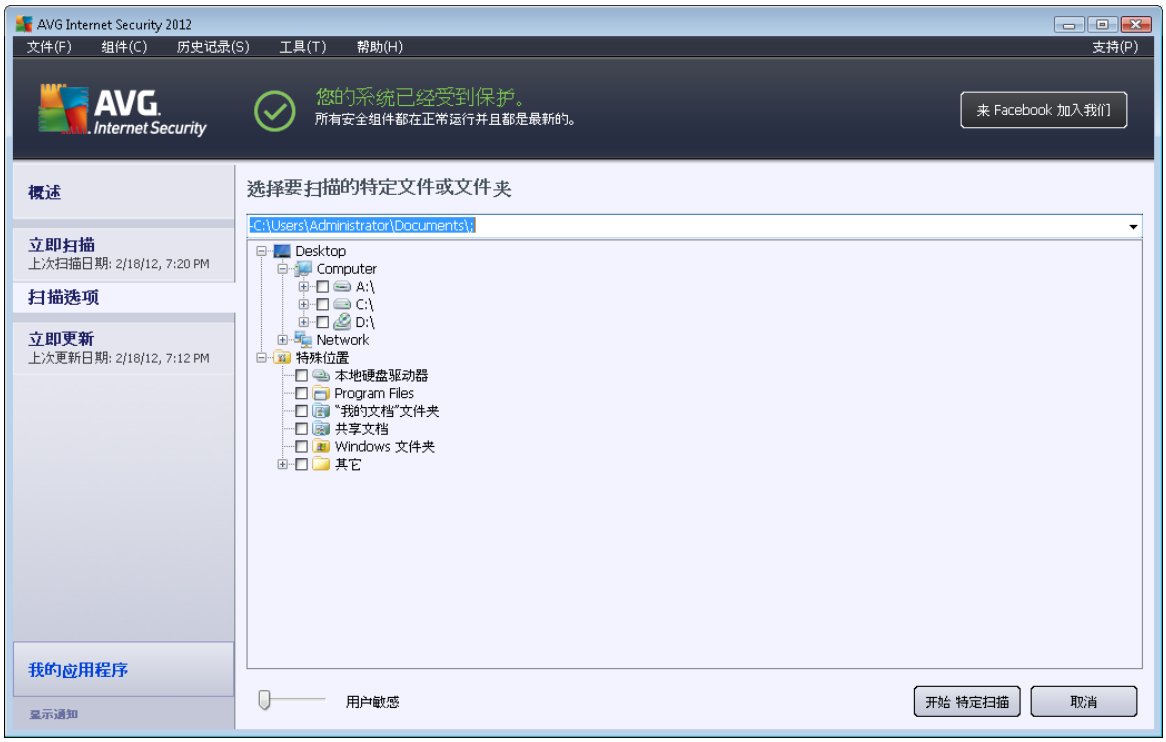
启动扫描

"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。

2012 版权所有 AVG Technologies CZ, s.r.o. 保留所有权利。

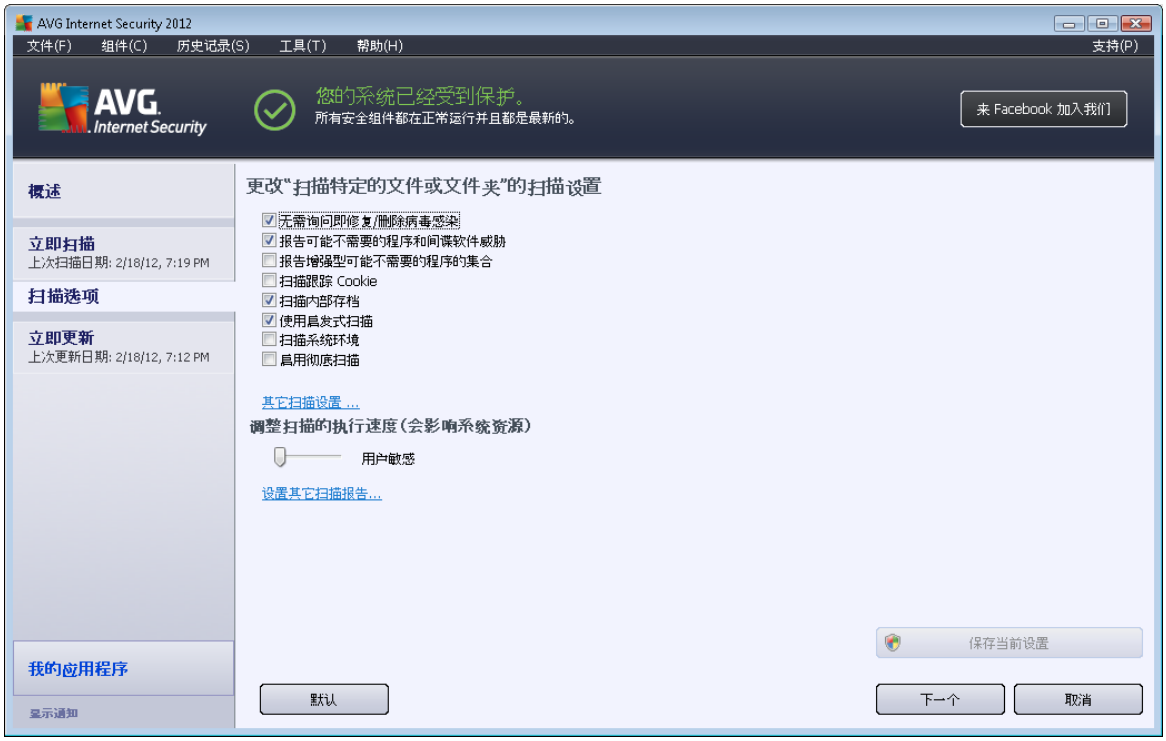
最后，若要启动扫描，请单击 ***'开始扫描'*** 按钮，扫描过程本身与 扫描整个计算机 基本上完全相同。



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！***

2012 版权所有 AVG Technologies CZ, s.r.o. 保留所有权利。



- ***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：

  - ***无需询问即修复/删除病毒感染***(*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。

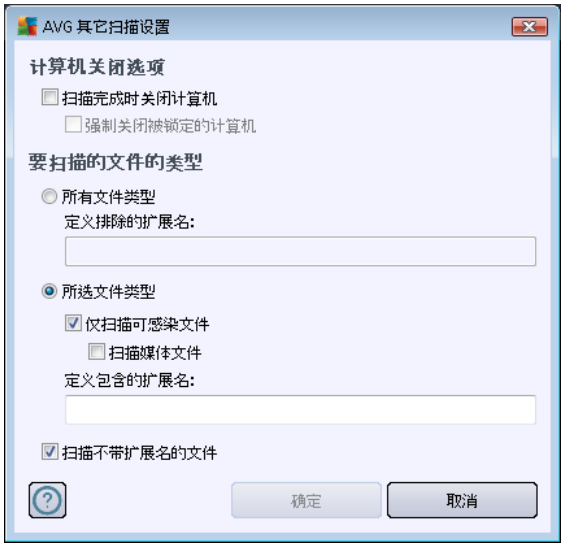
  - ***使用启发式扫描***(*默认情况下已启用*) - 启发式分析（*在虚拟的计算机环境中对已扫描对象的指令进行动态模拟*）将成为在扫描期间用来进行病毒检测的方法之一。

2012 版权所有 AVG Technologies CZ, s.r.o. 保留所有权利。

- ***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。

  - ***要扫描的文件的类型*** - 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；

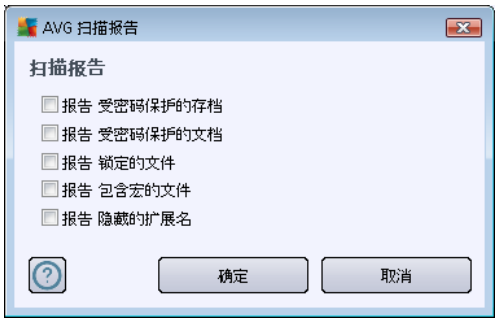
    - ***所选文件类型*** - 可以指定希望仅扫描可能受到感染的文件 *(将不扫描不可能遭到感染的文件，例如某些纯文本文件或某些其它的非可执行文件)*，其中包括媒体文件 *(视频、音频文件 - 如果将此框保留为未选中状态，则会进一步缩短扫描时间，因为这些文件通常很大，不太可能受到病毒感染)*。此外，您还可以通过扩展名指定哪些文件是始终应扫描的文件。

    - 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)*。

 2012 版权所有 AVG Technologies CZ, s.r.o. 保留所有权利。

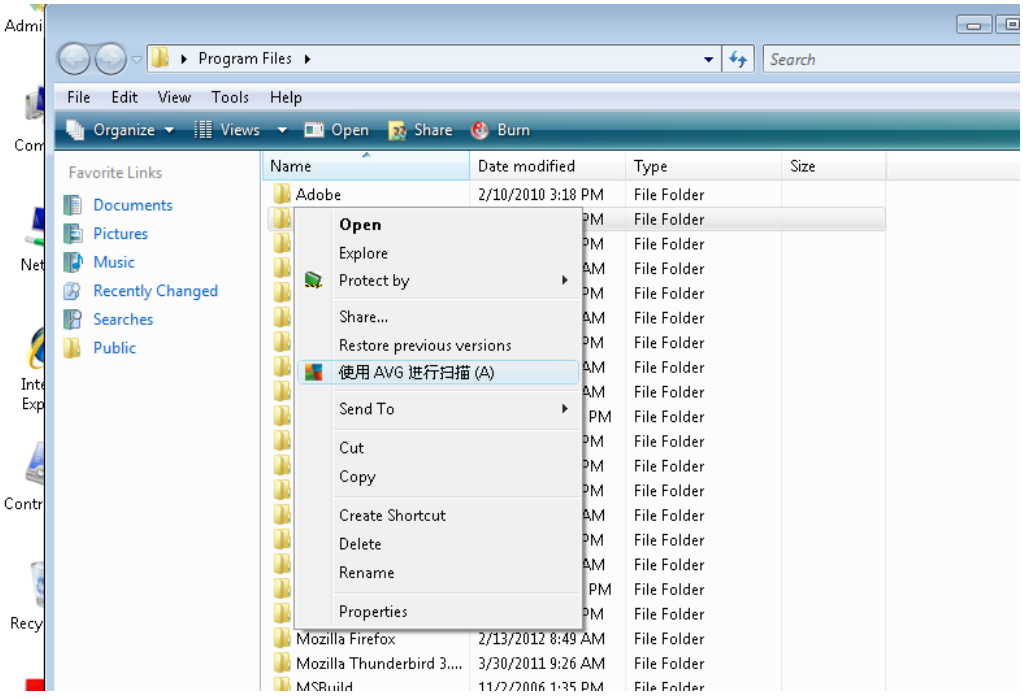
- ***设置其它扫描报告*** - 该链接将打开新的 ***"扫描报告"*** 对话框，在此对话框中您可以选择应报告可能发现的哪些类型的结果：



***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)。*

12.3. 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 2012** 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**AVG Internet Security 2012**

12.4. 命令行扫描

AVG Internet Security 2012 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。

12.4.1. CMD 扫描参数

下面列出了可用于命令行扫描的所有参数：

- ***/SCAN*** 用于扫描特定文件或文件夹 */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
- ***/LOG*** 生成扫描结果文件
- ***/MACROW*** 报告宏
- ***/PWDW*** 报告受密码保护的文件
- ***/ARCBOMBSW*** 报告存档炸弹 *反复压缩的存档*）
- ***/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
- ***/PUPEXT*** 报告更多可能不需要的程序

 2012 版权所有 AVG Technologies CZ, s.r.o. 保留所有权利。

- ***/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*** 用于设置扫描优先级 */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*** 用于扫描备用数据流 *(仅适用于 NTFS)*
- ***/HIDDEN*** 报告其扩展名已隐藏的文件
- ***/INFECTABLEONLY*** 仅扫描带可感染扩展名的文件
- ***/THOROUGHSCAN*** 启动彻底扫描
- ***/CLOUDCHECK*** 检查误报
- ***/ARCBOMBSW*** 用于报告重新压缩过的存档文件

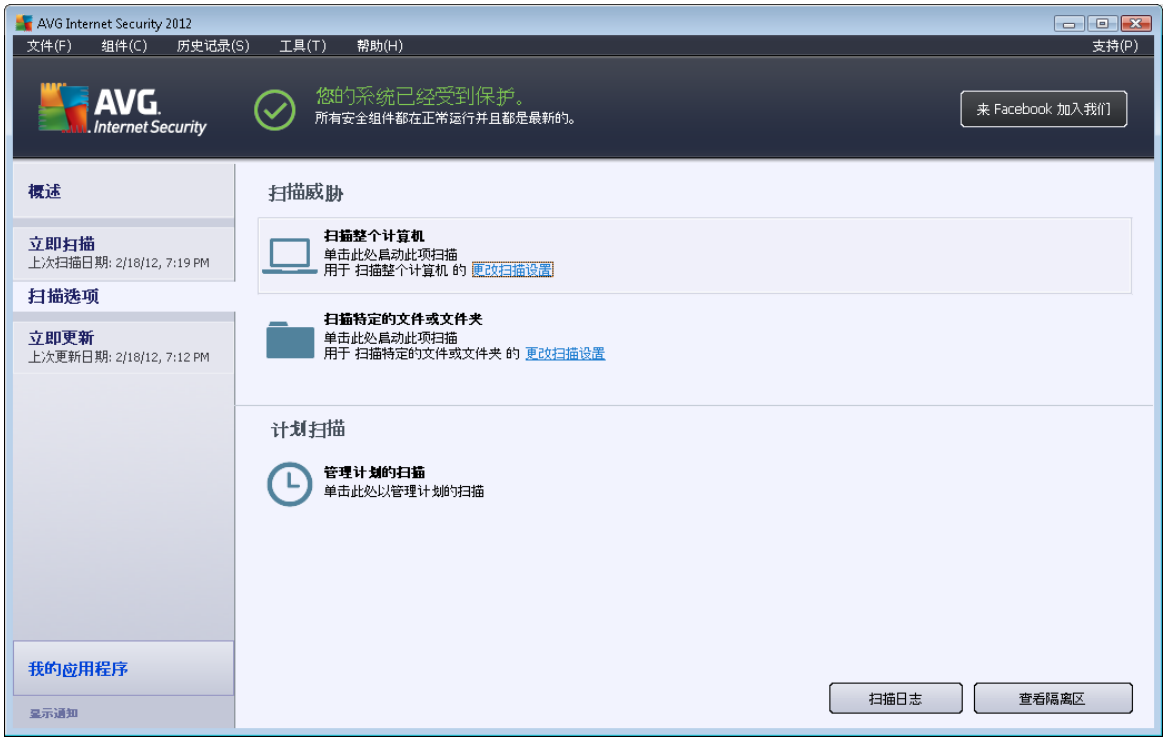
12.5. 扫描计划

通过 **AVG Internet Security 2012**，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非工作时间运行。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：

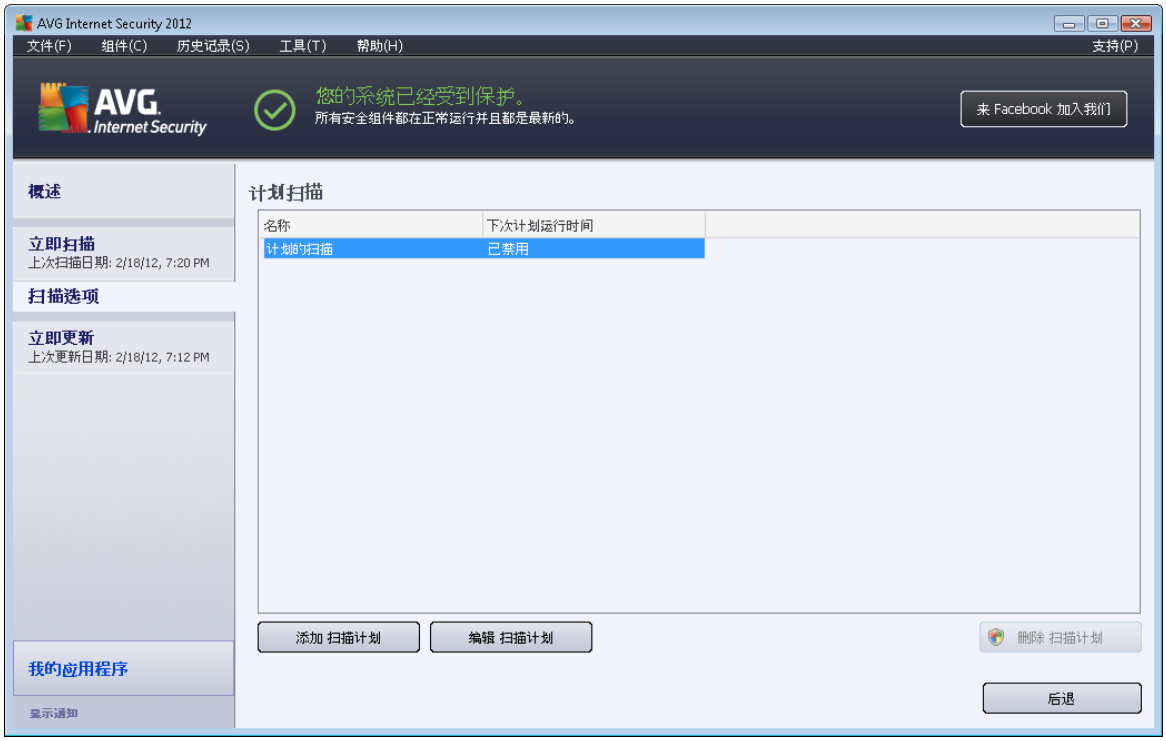
 2012 版权所有 AVG Technologies CZ, s.r.o. 保留所有权利。



计划扫描

单击 ***'计划扫描'*** 部分中的图形图标可打开一个新的 ***'计划扫描'*** 对话框，其中列出了当前计划的所有扫描：

 2012 版权所有 AVG Technologies CZ, s.r.o. 保留所有权利。



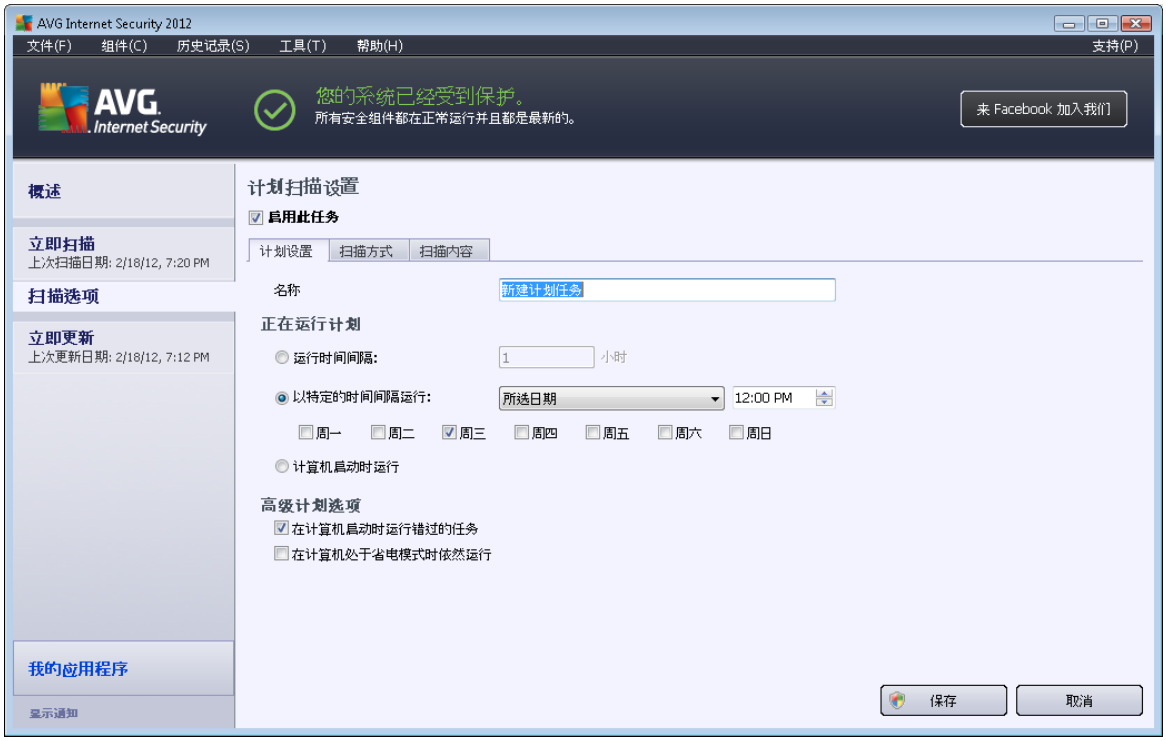
可以使用以下控制按钮来编辑/添加扫描：

- ***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

12.5.1. 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。

2012 版权所有 AVG Technologies CZ, s.r.o. 保留所有权利。



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：

2012 版权所有 AVG Technologies CZ, s.r.o. 保留所有权利。

- ***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。

12.5.2. 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：

- ***无需询问即修复/删除病毒感染***(*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*)：选中此框可启用 Anti-Spyware 引擎，还可对间谍软件和病毒进行扫描。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。

2012 版权所有 AVG Technologies CZ, s.r.o. 保留所有权利。

- ***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。

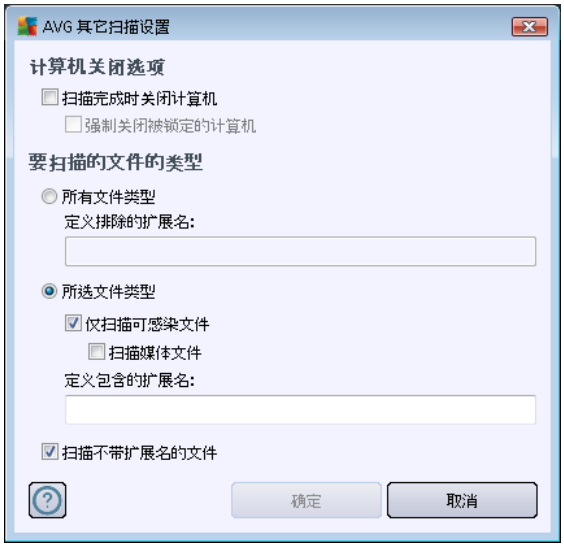
- ***扫描系统环境***(*默认情况下已启用*):扫描时还将检查您计算机的系统区域。

- ***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。

- ***扫描 Rootkit***(*默认情况下已启用*):Anti-Rootkit 用于在您的计算机中搜索是否可能存在 rootkit，例如，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。

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。

  - ***要扫描的文件的类型*** - 应该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

 2012 版权所有 AVG Technologies CZ, s.r.o. 保留所有权利。

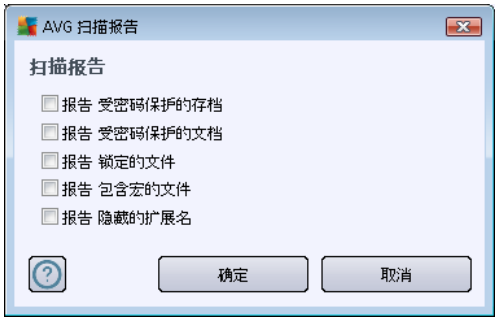
号分隔）指定特例，不对其进行扫描；

- ***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*** - 该链接用于打开新的***扫描报告*** 对话框，从中可选择应报告可能发现的哪些类型的结果：



控制按钮

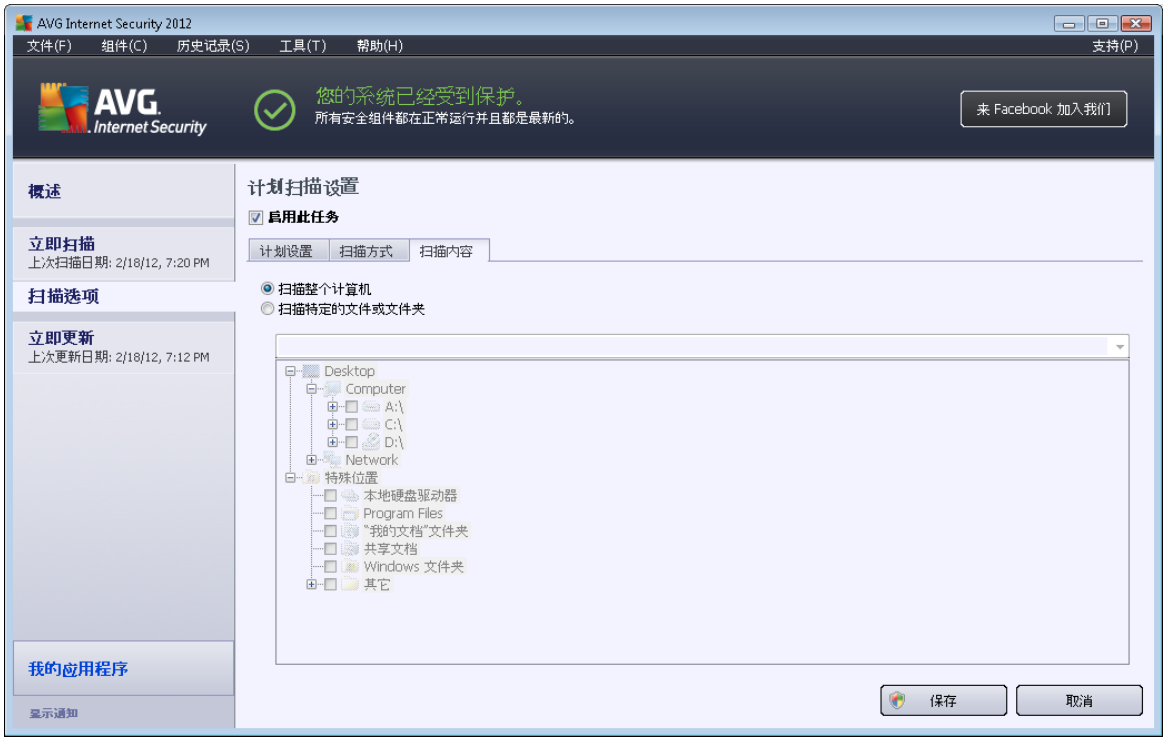
计划的扫描设置对话框的所有三个选项卡 *（计划设置、扫描方式和扫描内容）*中都有两个控制按钮，无论目前使用的是哪个选项卡，这两个按钮的功能都相同：

- ***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。

2012 版权所有 AVG Technologies CZ, s.r.o. 保留所有权利。

12.5.3. 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***
  - C:\Program Files\
  - *在 64 位版本中为* C:\Program Files (x86)
- ***'我的文档 '文件夹***
  - *对于 Win XP 为 :*C:\Documents and Settings\Default User\My Documents\

 2012 版权所有 AVG Technologies CZ, s.r.o. 保留所有权利。

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

- ***共享文档***
  - *对于 Win XP* 为：C:\Documents and Settings\All Users\Documents\
  - *对于 Windows Vista/7* 为：C:\Users\Public\Documents\
- ***Windows 文件夹*** - C:\Windows\
- ***其它***
  - *系统驱动器* - 装有操作系统的硬盘驱动器（通常是 C:）
  - *系统文件夹* - C:\Windows\System32\
  - *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*)
  - *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*)

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）*：

- ***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。

 2012 版权所有 AVG Technologies CZ, s.r.o. 保留所有权利。

12.6. 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

2012 版权所有 AVG Technologies CZ, s.r.o. 保留所有权利。

- ***'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

12.7. 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。

 2012 版权所有 AVG Technologies CZ, s.r.o. 保留所有权利。

12.7.1. “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

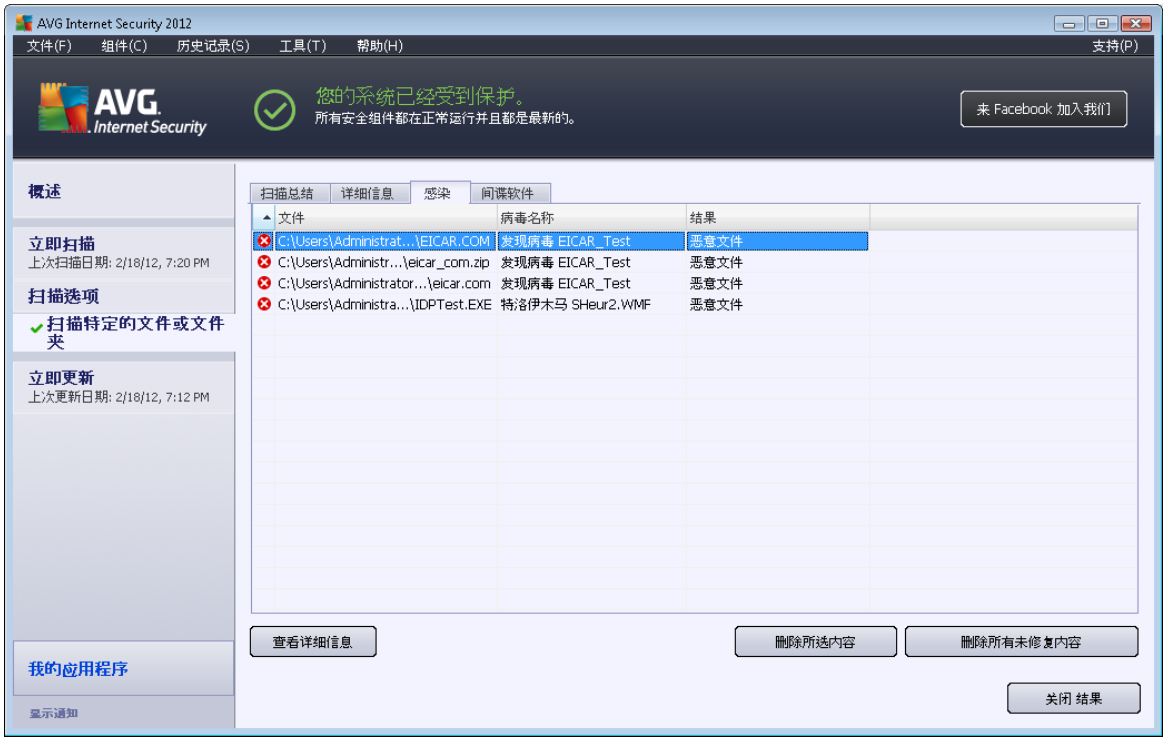
此外，您还将找到扫描启动的日期和确切时间、扫描的对象总数、扫描持续时间以及在扫描期间出现的错误数等信息。

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。

2012 版权所有 AVG Technologies CZ, s.r.o. 保留所有权利。

12.7.2. “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)*
  - ***“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*

2012 版权所有 AVG Technologies CZ, s.r.o. 保留所有权利。

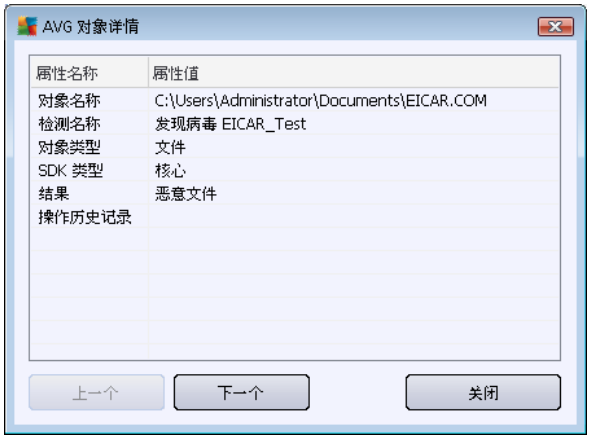
可能包含宏）;此信息仅仅是一则警告

- 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"*** 的新对话窗口：

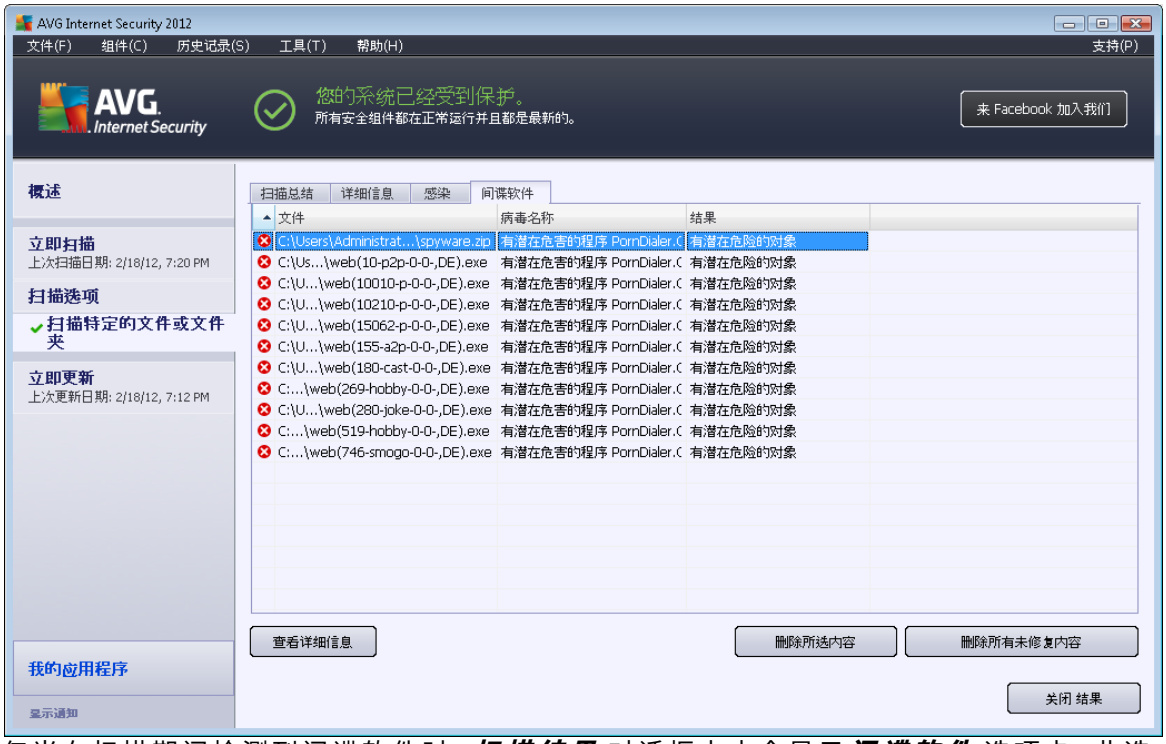


在此对话框中，可找到所检测到的受感染对象的详细信息 *例如，受感染对象的名称和位置、对象类型、SDK 类型、检测结果以及与检测到的对象相关的操作历史记录*）。用 ***"上一个"/"下一个"*** 按钮可查看特定检测结果的相关信息。使用 ***"关闭"*** 按钮可关闭此对话框。

- ***"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*** - 用于终止详细信息综览并返回到扫描结果概览对话框

2012 版权所有 AVG Technologies CZ, s.r.o. 保留所有权利。

12.7.3. “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*** - 用于指定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原位 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，并将其留在原位
    - ***已移至病毒库*** - 已将受感染的对象移入病毒库隔离区
    - ***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

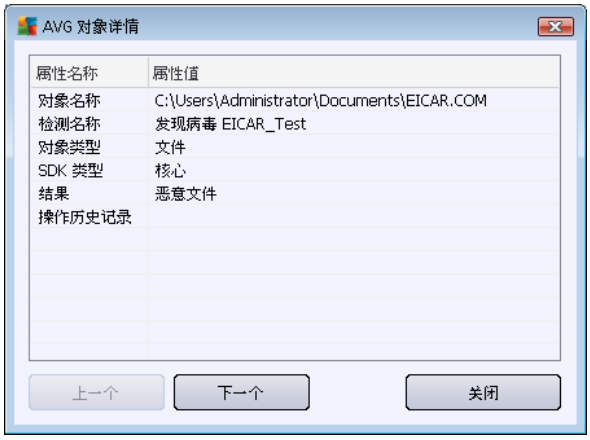
 2012 版权所有 AVG Technologies CZ, s.r.o. 保留所有权利。

- *“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”* 的新对话窗口：



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* - 用于终止详细信息综览并返回到扫描结果概览对话框

12.7.4. “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。如果测试结果中只有 **AVG Internet Security 2012** 检测到的警告，则不必执行任何操作。

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 **AVG Internet Security 2012** 报告了一个隐藏的文件并且您怀疑它有恶意，则您可以将它移到病毒库中。

 2012 版权所有 AVG Technologies CZ, s.r.o. 保留所有权利。

- ***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。

12.7.5. “Rootkit”选项卡

该 ***Rootkit*** 选项卡显示有关 anti-rootkit 扫描（包括在扫描整个计算机中）期间检测到的 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。

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。

12.7.6. “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。这些检测结果也不能肯定地标记为危险，但仍值得您注意。**AVG Internet Security 2012** 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 Internet Security 2012** 不能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*）。

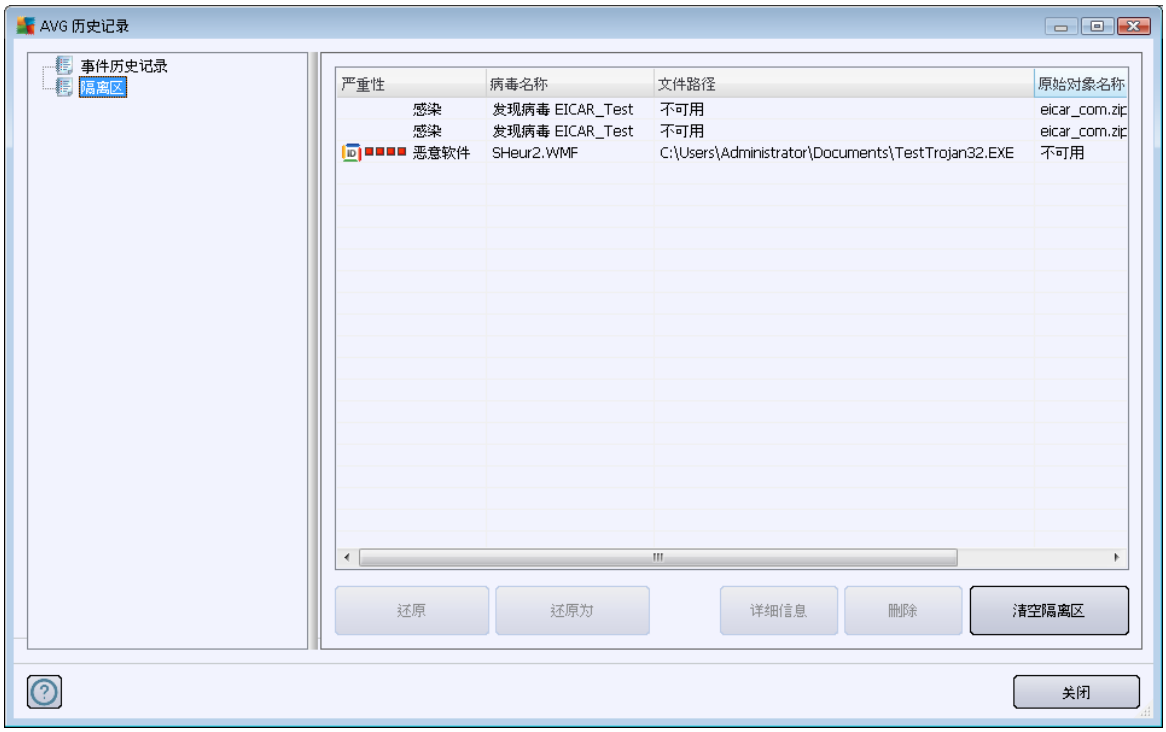
- ***包含宏的文档*** –所报告的文档包含可能有恶意的宏。

- ***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 Internet Security 2012** 会将此类文件报告出来以防止无意中将其打开。

- ***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*），则会将这种不一致情况报告出来。**AVG Internet Security 2012**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*** - 所报告的文件处于锁定状态，因而 **AVG Internet Security 2012** 不能对其进行扫描。这通常意味着系统正在持续使用某一文件（*例如交换文件*）。

12.8. 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：

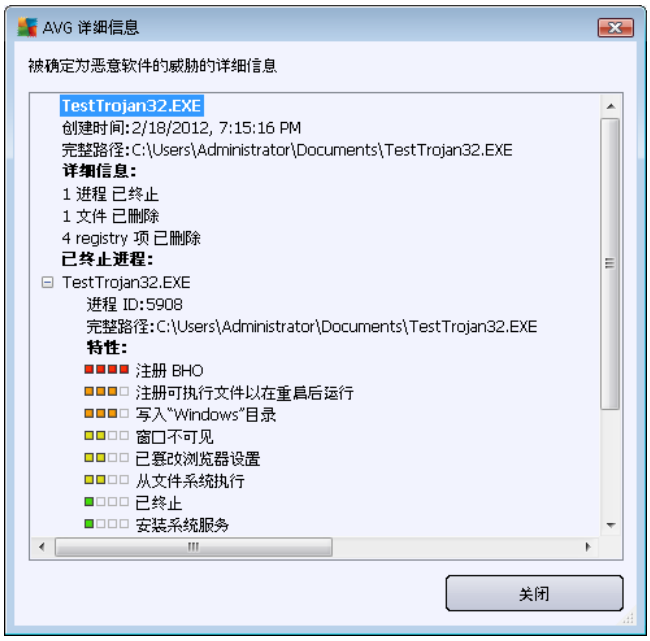
- ***严重程度*** - 如果决定安装 **AVG Internet Security 2012** 中的 Identity Protection 组件，则会在此部分中以图形方式显示所发现的各个受感染对象的严重程度，共分四级，从无可非议 (□□□□) 到非常危险 (■■■■)；还会显示有关感染类型的信息（*根据其感染程度分类，所有列出的对象要么肯定受到感染，要么可能受到感染*）
- ***病毒名称*** - 依据病毒百科全书 *在线）指定检测到的感染的名称*
- ***文件路径*** - 所检测到的受感染文件的原始位置的完整路径
- ***原始对象名称*** - 此图表中列出的所有检测到的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

2012 版权所有 AVG Technologies CZ, s.r.o. 保留所有权利。

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)*。

2012 版权所有 AVG Technologies CZ, s.r.o. 保留所有权利。

13. AVG 更新

除非得到定期更新，否则任何一款安全软件都不能保证真的可以防止受到各类威胁的侵害！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。

考虑到所有新涌现出来的计算机威胁，以及这些威胁的蔓延速度，定期更新 **AVG Internet Security 2012** 至关重要。继续使用程序默认设置（已在其中配置好自动更新），这是最佳解决方法。请注意，如果 **AVG Internet Security 2012** 的病毒数据库不是最新数据库，则程序不能检测到最新威胁！

定期更新 AVG 至关重要！如有可能，每天都应该更新基本病毒定义。不那么紧急的程序更新可以每周执行一次。

13.1. 更新启动

为了尽可能提高安全性，**AVG Internet Security 2012** 的默认更新计划是每四小时查找一次新更新。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，因此这种检查对于确保 AVG 病毒数据库始终处于最新状态很重要。

如果要减少更新启动次数，则可自行设置更新启动参数。但是，建议必须至少每天启动更新一次！可在高级设置/计划部分中编辑更新配置，具体而言，就是在以下对话框中编辑：

- 定义更新计划
- 程序更新计划
- Anti-Spam 更新计划

如果想要直接查看新更新文件，请使用主用户界面中的快速链接立即更新。任何用户界面对话框中都始终有此链接。

13.2. 更新进度

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 Internet Security 2012** 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，您将会重定向到***更新***界面，从中可查看以图形方式表示的过程进度，以及相关统计参数（*更新文件的大小、接收的数据、下载速度、经过时间等）概览*：

 2012 版权所有 AVG Technologies CZ, s.r.o. 保留所有权利。

***注 :**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 Windows 菜单 开始 /所有程序 /附件 /系统工具 /系统还原 使用此选项。建议仅限经验丰富的用户使用！*

13.3. 更新级别

AVG Internet Security 2012 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、反垃圾邮件和防恶意软件保护所需的更改。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。

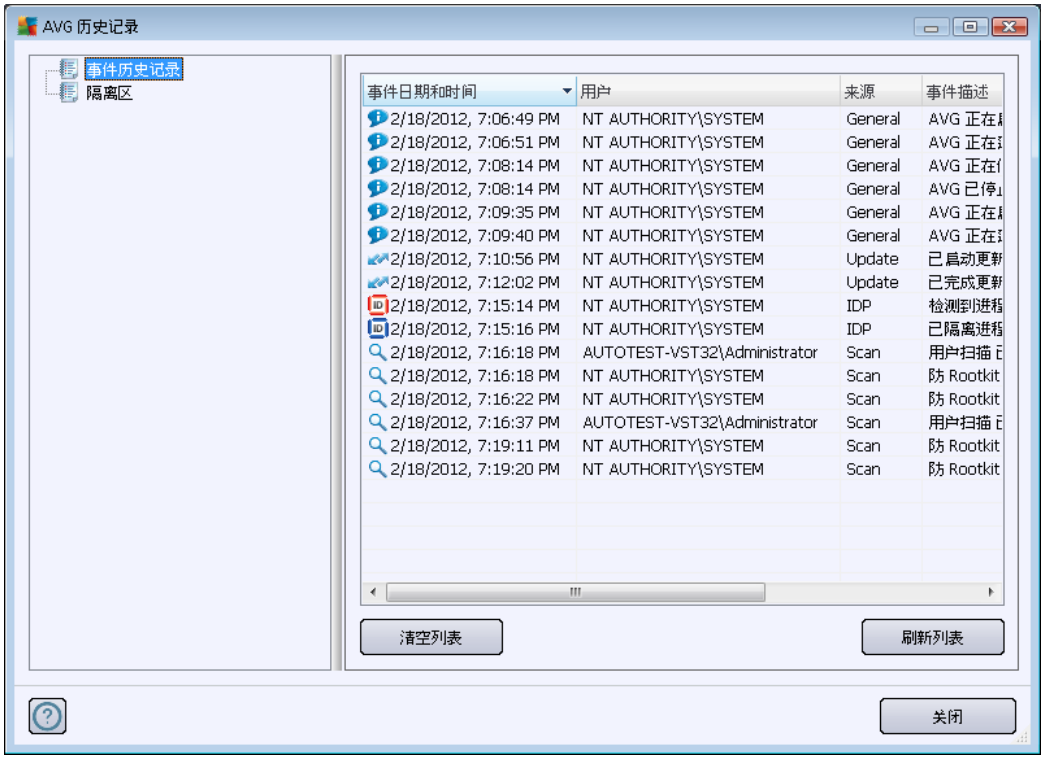
安排更新时，可同时对两个更新级别指定具体参数：

- 定义更新计划
- 程序更新计划

***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。*

2012 版权所有 AVG Technologies CZ, s.r.o. 保留所有权利。

14. 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 2012** 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
- 有关扫描开始、结束或停止的信息 *(包括自动执行的测试)*
- 有关病毒检测相关事件的信息 *(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***，用于说明事件发生的确切日期和时间
- ***用户***，用于说明目前已于发生事件时登录到系统中的用户的名称
- ***来源***，用于提供有关触发事件的源组件或 AVG 系统的其它部分的信息
- ***'事件说明'*** 提供实际情况的简短摘要

控制按钮

 2012 版权所有 AVG Technologies CZ, s.r.o. 保留所有权利。

- ***清空列表*** - 按该按钮可删除事件列表中的所有条目
- ***刷新列表*** - 按该按钮可刷新事件列表中的所有条目

2012 版权所有 AVG Technologies CZ, s.r.o. 保留所有权利。

15. 常见问题解答和技术支持

对于 **AVG Internet Security 2012** 应用程序，如果有销售或技术问题，可用多种方法寻求帮助。请从以下备选方法中进行选择：

- ***获取支持***：在 AVG 应用程序中就可以直接获取 AVG 网站的客户支持网页（http://www.avg.com/）。请选择***帮助/获取支持***主菜单项，通过可用支持途径重定向至 AVG 网站。要继续操作，请按该网页中的说明操作。

- ***支持（在菜单链接）***：AVG 应用程序菜单（*位于主用户界面顶部*）中有***支持***链接，用于打开一个新对话框，其中有尝试寻求帮助时可能需要了解的各类信息。该对话框中有关于所安装的 AVG 程序的基本资料（*程序/数据库版本*）、许可证详细信息，以及快速支持链接列表：

- ***帮助文件中的故障排除信息***：可在随 **AVG Internet Security 2012 附带的帮助文件中直接查看新的*故障排除***部分（*要打开该帮助文件，请按任何对话框中的 F1 键*）。此部分中列有用户想要寻求技术问题专业帮助时最常出现的情况。请选择最符合所遇到的问题的情况，然后单击该情况以打开详细说明，从而引导您解决问题。

- ***AVG 网站支持中心***：也可在 AVG 网站 (http://www.avg.com/) 中查找所遇到的问题的解决方法。在***支持中心***部分中，可综览结构化主题组（说明销售和支持问题）。

- ***常见问题解答***：在 AVG 网站 (http://www.avg.com/) 中，也可找到精心构成的独立的常见问题解答部分。可通过***支持中心/常见问题解答***菜单项查看此部分。其中的所有问题也已分门别类的划分，分为销售问题、技术问题和病毒问题这三类。

- ***关于病毒和威胁***：AVG 网站 (http://www.avg.com/) 的特定章节，专用于说明病毒问题（*可从主菜单中通过 帮助/关于病毒和威胁 选项访问该网页*）。在菜单中，依次选

2012 版权所有 AVG Technologies CZ, s.r.o. 保留所有权利。

择***支持中心/关于病毒和威胁***，即可进入一个页面，可在其中分门别类的概览在线威胁相关信息。其中也有关于删除病毒、间谍软件的说明，还有针对如何一直得到保护提出的建议。

- ***论坛***：也可使用 AVG 用户论坛 (http://forums.avg.com)。

2012 版权所有 AVG Technologies CZ, s.r.o. 保留所有权利。