AVG 9 Anti-Virus plus Firewall

用户手册

文档修订 90.21 (3.2.2010)

目录

1. 简介

本用户手册就是全面的 AVG 9 Anti-Virus plus Firewall 文档。

祝贺您购买 AVG 9 Anti-Virus plus Firewall！

AVG 9 Anti-Virus plus Firewall 是一系列屡获殊荣的 AVG 产品之一，旨在全面保护 PC，让用户高枕无忧。与所有其它 AVG 产品一样，AVG 9 Anti-Virus plus Firewall 经过了彻头彻尾的完全重新设计，以一种更具用户友好性、更高效的新方式提供 AVG 享有盛名、备受信赖的安全保护。

新 AVG 9 Anti-Virus plus Firewall 产品的界面经过优化，同时兼具更为严格、速度更快的扫描功能。为方便您使用，更多的安全功能实现了自动化；此外还引入了新的“智能型”用户选项，以便您可以根据自己的生活方式来调整我们的安全功能。不再为提升安全性而牺牲易用性！

AVG 旨在保护您的计算和网络活动。请尽享 AVG 的全面保护。

2. AVG 安装要求

2.1. 支持的操作系统

AVG 9 Anti-Virus plus Firewall 意在保护运行以下操作系统的工作站：

- Windows 2000 Professional SP4 + 更新汇总 1
- 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）

2.2. 最低和推荐硬件要求

对 AVG 9 Anti-Virus plus Firewall 的最低硬件要求：

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

对 AVG 9 Anti-Virus plus Firewall 的推荐硬件要求：

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

3. AVG 安装选项

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

在开始安装 AVG 之前，我们强烈建议您访问 AVG 网站 (http://www.avg.com/)，查看是否有新的安装文件。这样可确保安装的是最新版 AVG 9 Anti-Virus plus Firewall。

建议试用我们的新 AVG Download Manager 工具，这种工具将用所需语言帮助您设置安装文件！

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

4. AVG Download Manager

AVG Download Manager 是一种简单的工具，有助于为试用版 AVG 产品选择相应安装文件。根据您输入的数据，此管理器将选择特定的产品、许可证类型、所需的组件以及语言。最后，AVG Download Manager 会继续下载并启动相应的安装进程。

***警告：**请注意，AVG Download Manager 不适用于下载网络和 SBS 版本，仅支持以下操作系统：Windows 2000（SP4 + SRP 累积更新）、Windows XP、Windows Vista 和 Windows 7。*

AVG Download Manager 可从 AVG 网站 (http://www.avg.com/) 下载。随后请在 AVG Download Manager 中查看所需执行的每个步骤的简短说明：

4.1. 语言选择

这是 AVG Download Manager 的第一步，在此步骤中，请从下拉菜单中选择安装语言。请注意，您所选择的语言仅用于安装过程；安装之后，您可以直接从程序设置中更改语言。接下来请按 ***"下一步"*** 按钮以继续。

4.2. 连接检查

在下一步中，AVG Download Manager 会尝试建立 Internet 连接以便查找更新。AVG Download Manager 能完成连接测后才允许进入下载过程。

- 如果测试结果说明不存在连接，请确保您确实已连接到 Internet。然后单击 ***"重***

试”按钮

- 如果您是使用代理连接到 Internet 的，请单击 *“代理设置”*按钮以指定您的代理信息：
- 如果成功通过检查，请按 *“下一步”*按钮以继续。

4.3. 代理设置

如果 AVG Download Manager 无法识别您的代理设置，则您必须手动指定它们。请填写以下数据：

- ***"服务器"*** – 请输入有效的代理服务器名称或 IP 地址
- ***"端口"*** – 请提供相应的端口号
- ***"使用代理身份验证"*** – 如果您的代理服务器要求进行身份验证，请勾选此复选框。
- ***"选择身份验证类型"*** – 请从下拉菜单中选择身份验证类型。我们强烈建议您保留默认值（*代理服务器随后会自动将其要求告知您*）。不过，如果您是技能娴熟的用户，您也可以选择"基本"（*某些服务器需要*）或"NTLM"（*所有 ISA 服务器都需要*）选项。然后，请输入有效的 ***"用户名"*** 和 ***"密码"*** 可选）。

按 ***"应用"*** 按钮确认您的设置，以便接着执行 AVG Download Manager 的下一步操作。

4.4. 下载要安装的文件

现在已经提供 AVG Download Manager 开始下载安装软件包和启动安装进程所需的全部信息。然后要继续执行 AVG 安装过程。

5. AVG 安装过程

要将 AVG 9 Anti-Virus plus Firewall 安装到计算机中，需要获得最新的安装文件。您可以使用您的盒装版所含光盘中的安装文件，但此文件可能已过时。因此我们建议在线获取最新的安装文件。可以从 AVG 网站 (http://www.avg.com/) 上的 ***"支持中心"/"下载"*** 部分中下载该文件。也可使用我们的新 ***AVG Download Manager*** 工具，该工具有助于创建并下载所需的安装软件包，然后启动安装进程。

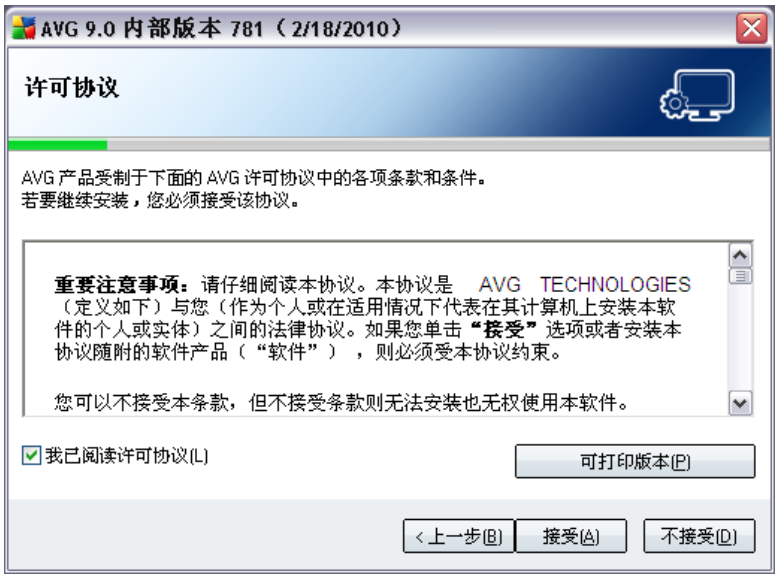
安装过程就是一系列对话框窗口，各个窗口中显示了有关每一步该如何操作的简短说明。下面，我们提供了对各个对话框窗口的说明：

5.1. 启动安装

安装过程开始时会显示 ***"欢迎使用 AVG 安装程序"*** 窗口。在此窗口中您需要选择要在此安装过程中使用的语言。在此对话框窗口的下部，可以找到 ***"选择您的安装语言"*** 项，请从相应的下拉菜单中选择所需的语言。接下来请按 ***"下一步"*** 按钮进行确认，然后接着按下一对话框的说明操作。

注意：*您在此处选择的语言仅用于此安装过程。您并不是在选择 AVG 应用程序的语言 – 稍后可以在安装过程中指定该应用程序的语言！*

5.2. 许可协议



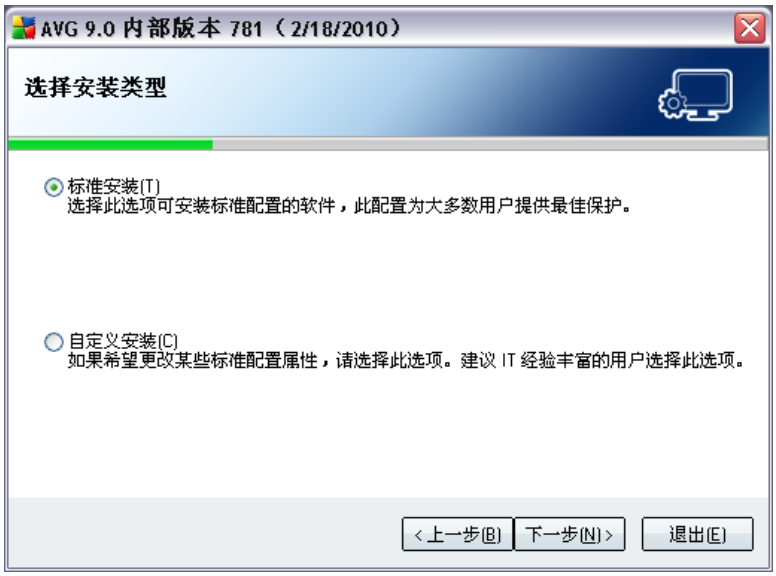
*“许可协议”*对话框提供了 AVG 许可协议的全文。请仔细阅读，然后选中 *“我已阅读许可协议”*复选框并按 *“接受”*按钮确认您已阅读、理解并接受此协议。

如果您不同意此许可协议，请按 *“不接受”*按钮，安装过程会立刻终止。

5.3. 正在检查系统状态

确认许可协议后，系统会将您重定向到 *“正在检查系统状态”*对话框。此对话框不需要任何干预；正在检查您的系统，检查完毕后才能开始安装 AVG。请等待此过程完成，完成后会自动显示下一对话框。

5.4. 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：***标准***安装和***自定义***安装。

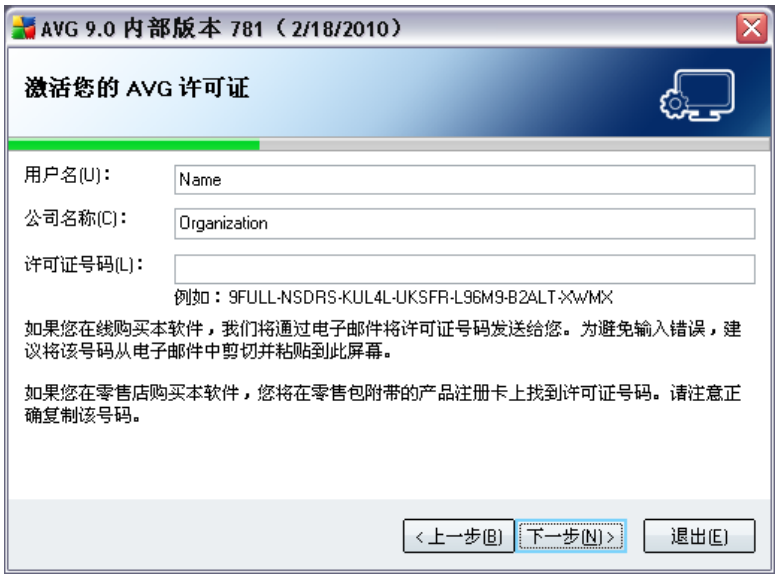
对于大多数用户而言，强烈建议保留默认的***标准安装***，选择这种安装方式时会采用程序供应商预定义的设置以完全自动的方式安装 AVG。这种配置可提供最佳的安全性，同时又会使资源得到最优利用。今后如果需要更改配置，您始终都可以直接在 AVG 应用程序中完成。

自定义安装只应由经验丰富的用户在确有必要不以标准设置安装 AVG 时使用；例如，为满足特定的系统要求，可使用此选项。

5.5. 激活您的 AVG 许可证

在***"激活您的 AVG 许可证"***对话框中，您需要填写您的注册数据。请键入您的名字（***"用户名"***字段）以及您所在组织的名称（***"公司名"***字段）。

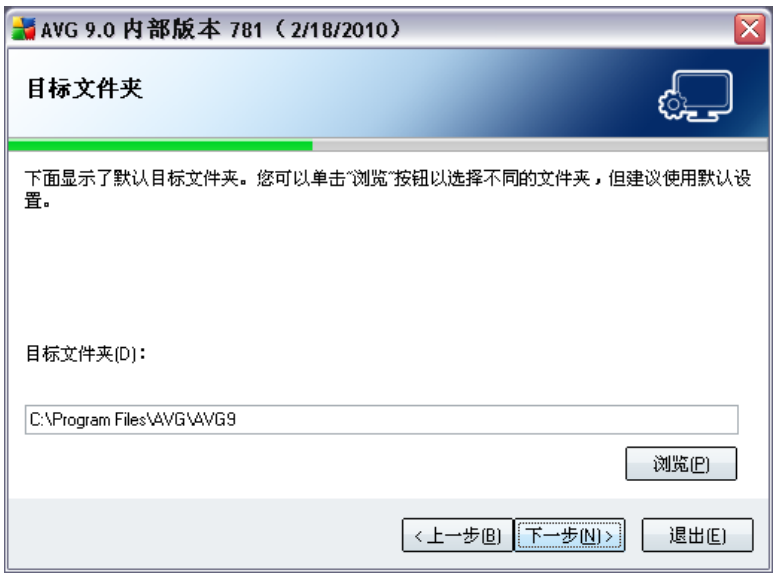
然后，在***"许可证号码"***文本字段中输入您的许可证/销售号码。销售号码可在 AVG 9 Anti-Virus plus Firewall 包装盒内的光盘包装上找到。许可证号码将在您在线购买 AVG 9 Anti-Virus plus Firewall 之后通过确认电子邮件发送给您。您必须完全按照如图所示键入号码。如果存在数字形式的许可证号码（*在电子邮件中*），建议使用复制和粘贴方法插入它。



按 ***"下一步"*** 按钮继续执行安装过程。

如果在上一步中您选择的是标准安装，则系统会直接将您重定向到 ***"AVG Security Toolbar"对话框。如果您选择的是自定义安装，则接下来显示的将是 ***"目标文件夹"*** 对话框。

5.6. 自定义安装 – 目标文件夹

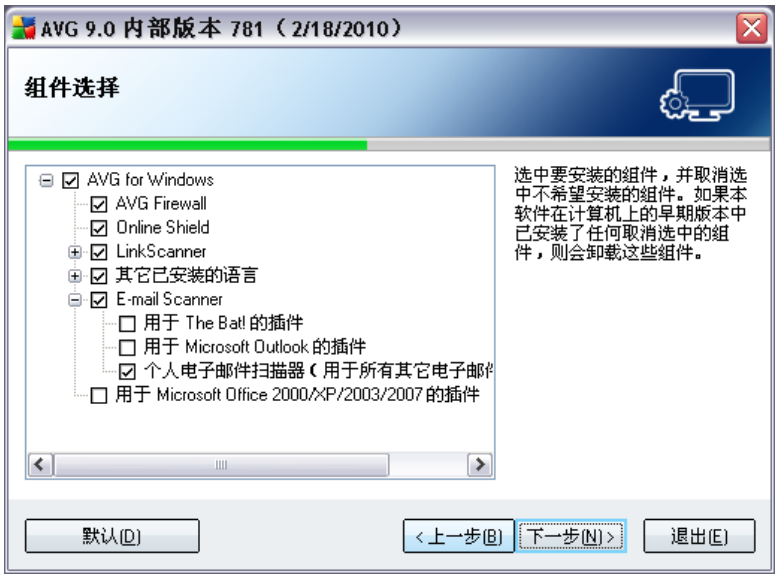


通过 ***"目标文件夹"***对话框，可指定要从中安装 AVG 9 Anti-Virus plus Firewall 的位置。默认情况下，AVG 会被安装到 C: 驱动器上的 "Program Files"文件夹中。如果此文件夹还不存在，将显示一个新的对话框，要求您确认同意 AVG 立即创建此文件夹。

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。

按 ***"下一步"***按钮以确认。

5.7. 自定义安装 –组件选择



通过 ***"组件选择"***对话框，可大概了解可以安装的所有 AVG 9 Anti-Virus plus Firewall 组件。如果默认设置不适合您，您可以删除/添加特定的组件。

不过，您只能从您购买的 AVG 版本所包含的组件中进行选择。"组件选择"对话框中将只提供这些组件供用户安装！

- ***语言选择***

  在待安装组件列表中，您可以定义安装 AVG 时应采用的语言。选中 ***"其它安装语言"***项，然后从相应的菜单中选择所需的语言。

- ***E-mail Scanner 插件***

  单击***"E-mail Scanner"***项以将其打开，然后决定要安装何种插件来保证电子邮件的安全。默认情况下，将安装 ***"Microsoft Outlook 插件"***。另一特定选项就是***"The Bat! 插件"***如果您使用的是任何其它电子邮件客户端（*MS Exchange*、*Qualcomm*

Eudora 等)，请使用 ***"个人电子邮件扫描器"***选项以自动保护您的电子邮件通信，而不管您运行何种电子邮件程序。

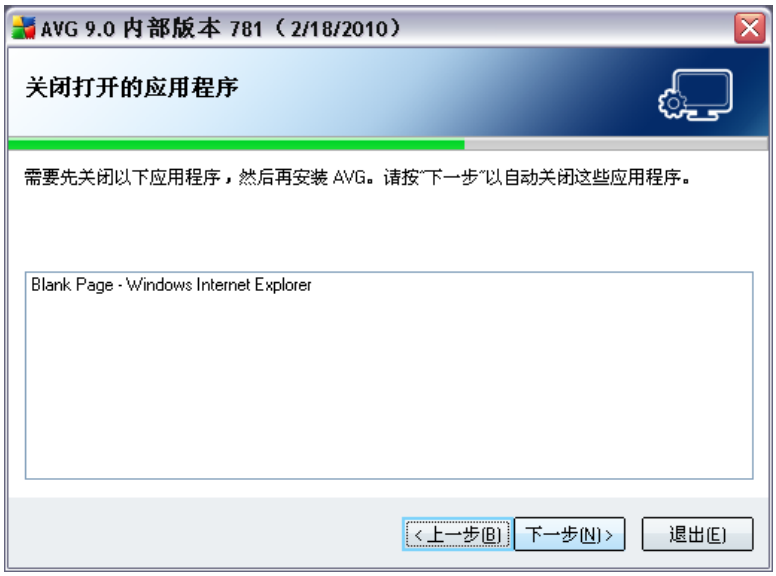
按 ***"下一步"***按钮以继续。

5.8. AVG Security Toolbar

在***"AVG Security Toolbar"***对话框中，要决定是否要安装 ***AVG Security Toolbar***(*用于验证受支持的 Internet 搜索引擎的搜索结果*)。如果不更改默认设置，则会将此组件自动安装到 Internet 浏览器 *(目前受支持的浏览器包括 Microsoft Internet Explorer v. 6.0 或更高版本，以及 Mozilla Firefox v. 2.0 或更高版本*)中，以便在上网冲浪时提供全面的在线保护。

同样，还可以决定是否要将 Yahoo! 选作默认搜索提供商。如果是这样，请选中相应的复选框。

5.9. 关闭打开的应用程序



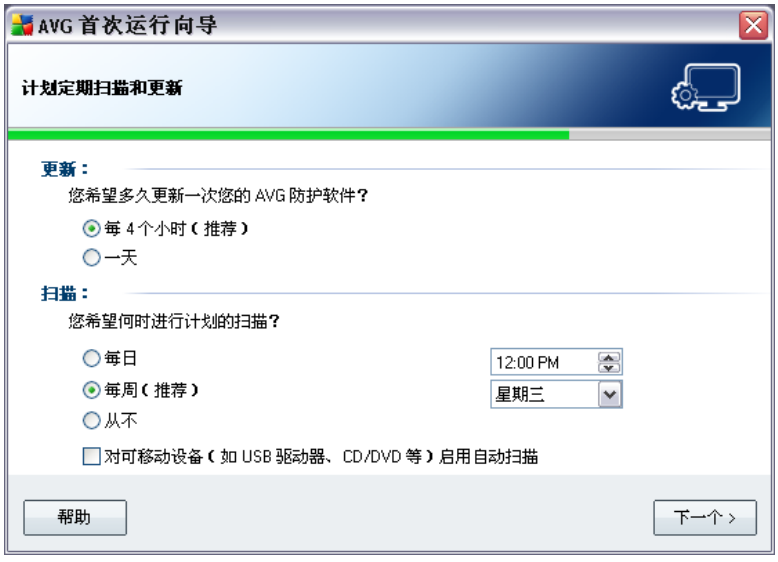
在安装过程中，仅当此时计算机中有一些有冲突的其它程序正在运行时，才会显示 ***"关闭打开的应用程序"*** 对话框。然后就会列出一些应用程序，必须将其关闭才能成功完成安装过程。按 ***"下一步"*** 按钮可确认同意关闭相应的应用程序，继续执行下一步。

5.10. 正在安装 AVG

*"正在安装 AVG"*对话框用于显示安装过程的进度，不需要进行任何干预：

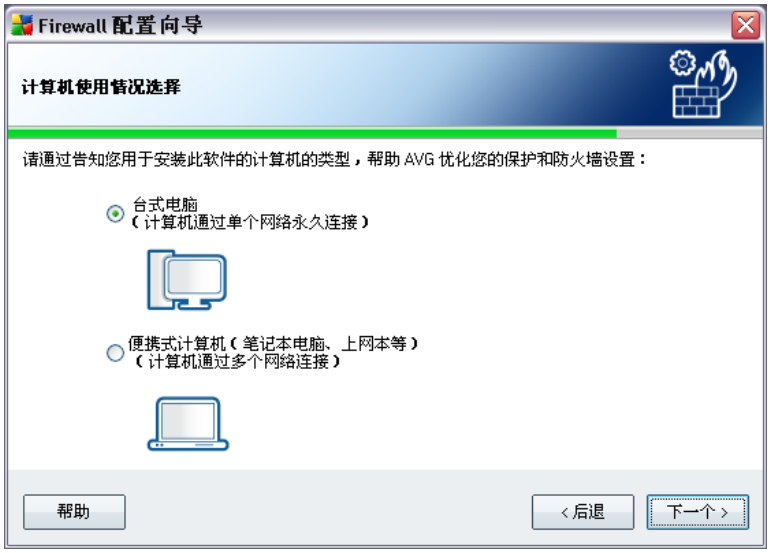
安装过程结束后，系统会自动将您重定向到下一对话框。

5.11. 计划定期扫描和更新



在 ***"计划定期扫描和更新"*** 对话框中，请设置检查是否有新的更新文件可用的时间间隔，并定义应启动计划的扫描的时间。建议保留默认值。按 ***"下一步"*** 按钮以继续。

5.12. 计算机使用情况选择



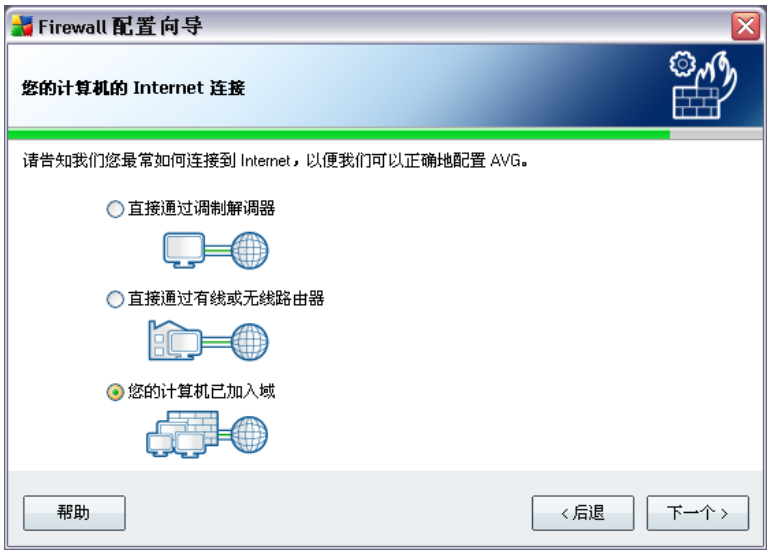
在此对话框中，***Firewall 配置向导*** 会询问您使用的是何种类型的计算机。例如，从许多不同位置（*机场、酒店房间等*）连接到 Internet 的笔记本电脑所需的安全规则要比域（*公司网络等*）。会对 ***Firewall*** 默认规则指定不同的安全级别，具体情况取决于所选计算机使用类型。

有两个备选选项可供您选择：

- ***台式计算机***
- ***便携式计算机***

按 ***"下一步"*** 按钮确认您所做的选择，然后接着按下一对话框的说明操作。

5.13. 您的计算机的 Internet 连接



在此对话框中，***Firewall 配置向导***会向您询问您的计算机连接到 Internet 的方式。会对 ***Firewall*** 默认规则指定不同的安全级别，具体情况取决于所选连接类型。

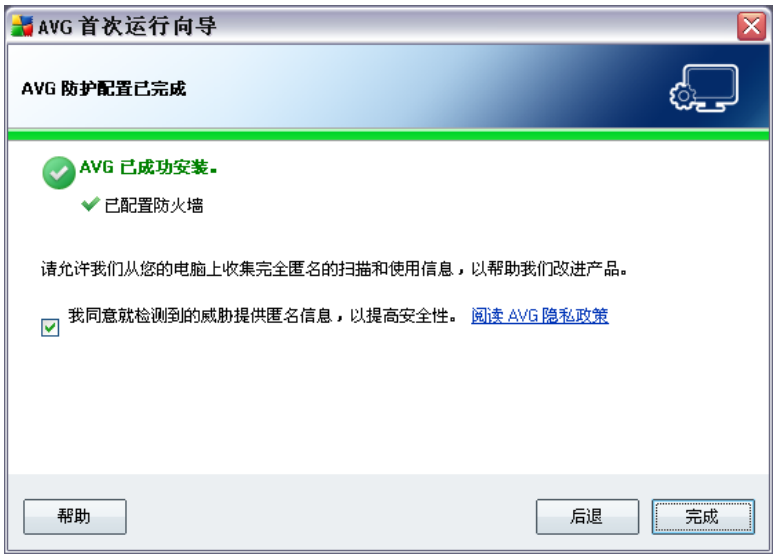
有三个备选选项可供您选择：

- ***直接通过调制解调器***
- ***直接通过有线或无线路由器***
- ***您的计算机已加入域***

请选择能够最恰当地描述您计算机的 Internet 连接的连接类型。

按 ***"下一步"*** 按钮确认您所做的选择，然后接着按下一对话框的说明操作。

5.14. AVG 防护配置已完成



现在 AVG 9 Anti-Virus plus Firewall 已配置完毕。

在此对话框中，要决定是否要激活向 AVG 病毒实验室匿名举报漏洞利用和恶意网站的选项。如果要举报，请选中 ***'我同意就检测到的威胁提供匿名信息，以提高安全性'*** 选项。

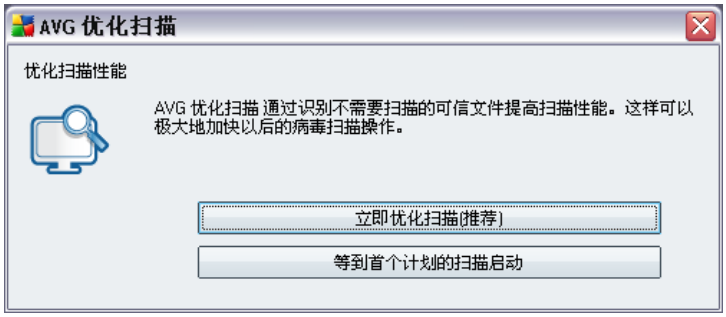
最后，请按 ***'完成'*** 按钮。可能需要重新启动您的计算机，然后您才能开始使用 AVG。

6. 安装后

6.1. 扫描优化

扫描优化功能用于搜索已从中检测到相应文件 *(目前包括 *.exe、*.dll 和 *.sys 文件)*的 *"Windows"*和 *"Program Files"*文件夹，以及保存有关这些文件的信息。下次访问时不会再对这些文件进行扫描，这样会大幅缩短扫描时间。

安装过程一结束，就会有一个新的对话窗口邀请您优化扫描：



建议使用此选项，并通过按 ***"立即优化扫描"***按钮来执行扫描优化过程。

6.2. 产品注册

安装完 AVG 9 Anti-Virus plus Firewall 之后，请在 AVG 网站 (http://www.avg.com/) 中的 ***"注册"***页面***上***在线注册您的产品 *(直接在该页面中按提供的说明操作)*。注册之后，您就可以完全访问您的 AVG 用户帐户、AVG 更新新闻稿，还以享受专为注册用户提供的其它服务。

6.3. 访问用户界面

AVG 用户界面可通过以下几种方式进行访问：

- 双击系统托盘中的 AVG 图标
- 双击桌面上的 AVG 图标
- 通过以下菜单进行访问：***"开始"*** / ***"所有程序"*** / ***"AVG 9.0"*** / ***"AVG 用户界面"***

6.4. 扫描整个计算机

存在一种潜在风险，即计算机病毒在 AVG 9 Anti-Virus plus Firewall 安装之前就已传播到您的计算机上。因此，您应运行 ***"扫描整个计算机"*** 这一功能以确保您的 PC 上不存在感染。

有关运行 ***扫描整个计算机*** 这一功能的说明，请参阅 ***AVG 扫描*** 一章。

6.5. Eicar 测试

要确保 AVG 9 Anti-Virus plus Firewall 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，不包含任何病毒代码段。大多数产品都会将它当成病毒而作出反应 *(尽管它们在报告它时通常使用一个清楚明白的名称，例如 "EICAR-AV-Test")*。您可以从 EICAR 网站 (www.eicar.com) 下载 EICAR 病毒，该网站上还提供了所有必要的 EICAR 测试信息。

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

也可从网站 http://www.eicar.com 中下载压缩版 EICAR "病毒" *(例如，以 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*** 就会检测到该 "病毒"。**如果 AVG 未能将 EICAR 测试文件当成病毒识别出来，则您应重新检查程序配置！**

6.6. AVG 默认配置

AVG 9 Anti-Virus plus Firewall 的默认配置（*即应用程序在刚安装完后的设置*）由软件供应商设置，这样所有组件和功能都会经过调整达到最佳性能。

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

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

7. AVG 用户界面

AVG 9 Anti-Virus plus Firewall 打开时会显示主窗口：

该主窗口分为若干区域：

- ***系统菜单*** *（窗口顶部的系统行）*提供了标准的导航方式，可用来访问所有 AVG 组件、服务和功能 – 详细信息 >>
- ***安全状态信息*** *（窗口上方区域）*提供了有关 AVG 程序当前状态的信息 – 详细信息 >>
- ***快速链接*** *（窗口左侧区域）*用于快速访问最重要和最常用的 AVG 任务 – 详细信息 >>

- ***组件概览*** *(窗口中央区域)*提供了已安装的所有 AVG 组件的概览 –详细信息 >>
- ***统计信息*** *(窗口左下方区域)*提供了有关程序运行情况的所有统计数据 –详细信息 >>
- ***系统托盘图标*** *(显示器右下角，系统托盘上)*指示 AVG 的当前状态 –详细信息 >>

7.1. 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 9 Anti-Virus plus Firewall 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：

7.1.1. 文件

- ***"退出"***– 关闭 AVG 9 Anti-Virus plus Firewall 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！

7.1.2. 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"*** – 打开 ***Anti-Virus*** 组件的默认页面
- ***"Anti-Rootkit"*** – 打开 ***Anti-Rootkit*** 组件的默认页面
- ***"Anti-Spyware"*** – 打开 ***Anti-Spyware*** 组件的默认页面
- ***"Firewall"*** – 打开 ***Firewall*** 组件的默认页面
- ***"Link Scanner"*** – 打开 ***Link Scanner*** 组件的默认页面
- ***"E-mail Scanner"*** – 打开 ***E-mail Scanner*** 组件的默认页面
- ***"许可证"***– 打开***许可证***组件的默认页面
- ***Online Shield*** - 用于打开 ***Online Shield*** 组件的默认页面

- ***"Resident Shield"*** – 打开 ***Resident Shield*** 组件的默认页面
- ***"更新管理器"*** – 打开***更新管理器***组件的默认页面

7.1.3. 历史记录

- ***"扫描结果"*** – 切换到 AVG 测试界面，具体而言，即切换到***"扫描结果概览"***对话框
- ***Resident Shield 检测*** - 用于打开一个对话框，从中大概了解 ***Resident Shield***
- ***E-mail Scanner 检测*** - 用于打开一个对话框，从中大概了解 ***E-mail Scanner*** 组件检测后断定有危险的邮件附件
- ***"通过Online Shield发现的威胁"*** - 用于打开一个对话框，从中大概了解 ***Online Shield***
- ***"病毒库"*** – 打开隔离区（***病毒库***）的界面，AVG 会将已检测到但出于某种原因而无法自动修复的所有感染移至此隔离区。在此隔离区内，受感染的文件会被隔离起来，因而您计算机的安全性会得到保证，同时受感染的文件也被存储了下来，以备日后修复。
- ***"事件历史记录日志"*** – 打开历史记录日志界面，其中包含了所有已记录的 AVG 9 Anti-Virus plus Firewall 操作的概览。
- ***"Firewall"*** – 打开 Firewall 设置界面中的***"日志"***选项卡，其中包含了所有 Firewall 操作的详细概览

7.1.4. 工具

- ***"扫描计算机"*** – 切换到 AVG 扫描界面并启动对整个计算机的扫描
- ***"扫描所选文件夹"*** – 切换到 AVG 扫描界面并允许您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"*** – 用于对从磁盘树结构中选择的单个文件执行按需测试
- ***"更新"*** – 自动启动 AVG 9 Anti-Virus plus Firewall
- ***"从目录更新"*** – 从位于您本地磁盘上指定文件夹中的更新文件执行更新过程。不过，建议仅将此选项用于应急情况，例如不存在 Internet 连接的情况 *例如，您的计算机受到感染且已从 Internet 断开；您的计算机连接到无权访问 Internet 的网络，等等*）。在新打开的窗口中，请选择您之前将更新文件放置到的文件夹，然后启动更新过程。

- ***"高级设置"***– 打开 ***"AVG 高级设置"***对话框，在此对话框中您可以对 AVG 9 Anti-Virus plus Firewall 配置进行编辑。一般而言，建议保留由软件供应商定义的应用程序默认设置。

- ***"Firewall 设置"***– 打开一个独立的对话框，其中显示了 ***Firewall*** 组件的高级配置

7.1.5. 帮助

- ***"目录"***– 打开 AVG 帮助文件

- ***"获取在线帮助"***– 打开 AVG 网站 (http://www.avg.com/) 中的客户支持中心页面

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

- ***"关于病毒和威胁"***– 打开在线***病毒百科全书***，您可以在其中查找关于所识别到的病毒的详细信息

- ***重新激活*** - 用于打开 ***"激活 AVG"***对话框，其中有安装过程中在 ***"对 AVG 进行个性化设置"***对话框中输入的数据。在此对话框中，您可以输入您的许可证号码来替换销售号码 *(您安装 AVG 时使用的号码)*或替换原来的许可证号码 *(例如在升级到新的 AVG 产品时)*。

- ***立即注册*** - 用于连接到 AVG 网站 (http://www.avg.com/) 的注册页面。请填写您的注册数据；只有注册了自己的 AVG 产品的客户才能享受到免费的技术支持。

注：*如果使用的是试用版 AVG 9 Anti-Virus plus Firewall，后两个选项会显示为* ***"立即购买"****和* ***"激活"****；这样就可以立即购买该程序的完整版。对于通过销售号码安装的 AVG 9 Anti-Virus plus Firewall，这两个选项显示为* ***"注册"****和* ***"激活"****。有关更多信息，请见本文档的许可证一节。*

- ***"关于 AVG"***– 打开 ***"信息"***对话框，此对话框包含五个选项卡，提供了有关程序名称、程序和病毒数据库版本、系统信息、许可协议以及 ***AVG Technologies CZ*** 联系信息的数据。

7.2. 安全状态信息

"安全状态信息"区域位于 AVG 主窗口的上部。在此区域中，始终可以找到 AVG 9 Anti-Virus plus Firewall 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 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。


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

如果您出于某种原因决定忽略组件的错误状态（*可通过在 AVG 主窗口的组件概览中右键单击相应组件的图标打开上下文菜单，从中即可选择"忽略组件状态"选项*），此图标也会显示。在特定情况下您可能需要使用此选项，但极力建议尽快禁用***"忽略组件状态"***选项。


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

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

注：*AVG 状态信息也可以随时通过系统任务栏图标获得。*

7.3. 快速链接

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

- ***"概览"***– 使用此链接可从当前打开的任何 AVG 界面切换到包含已安装的所有组件概览的默认界面 – 请参见此章：***"组件概览"***>>
- ***计算机扫描器*** - 使用此链接可打开 AVG 扫描界面，在此界面中您可以直接运行测试，对扫描进行计划，或编辑其参数 - 请参见此章：***AVG 扫描*** >>
- ***"立即更新"***– 此链接用于打开更新界面并立即启动 AVG 更新过程 – 请参见此章：***"AVG 更新"***>>

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

7.4. 组件概览

"组件概览"区域位于 AVG 用户界面的中央位置。该区域分为两个部分：

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

在 **AVG 9 Anti-Virus plus Firewall 中，*"组件概览"***部分中含有关于以下组件的信息：

- ***Anti-Virus***，可确保您的计算机免遭企图进入您计算机的病毒侵害 – 详细信息 >>
- ***Anti-Spyware***，在您运行应用程序时在后台对它们进行扫描 – 详细信息 >>
- ***Firewall***，控制您的计算机与 Internet 或本地网络上的其它计算机交换数据的方式 – 详细信息 >>
- ***Link Scanner***，检查在您的 Internet 浏览器中显示的搜索结果 – 详细信息 >>
- ***Anti-Rootkit***，检测企图掩饰恶意软件的程序和技术 – 详细信息 >>
- ***E-mail Scanner***，检查所有传入和传出的邮件是否携带病毒 – 详细信息 >>
- ***许可证***，用于显示许可证号、类型和到期日期 - 详细信息 >>
- ***Online Shield***，用于扫描正在通过 Web 浏览器下载的所有数据 - 详细信息 >>
- ***Resident Shield***，在后台运行并在文件被复制、打开或保存时扫描它们 – 详细信息 >>
- ***更新管理器***，控制所有 AVG 更新 – 详细信息 >>

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

在组件图标的上方右键单击鼠标可展开一个上下文菜单；除了打开该组件的图形界面之外，您还可以选择 ***"忽略组件状态"***。选择此选项可表明已经知道该组件的错误状态，但出

于某种原因想要保持 AVG 的这种状态，而且不想通过系统任务栏图标收到警告。

7.5. 统计信息

"统计信息"区域位于 AVG 用户界面的左下部。它提供了关于此程序运行情况的一列信息：

- ***"上次扫描"***– 提供了上次扫描的执行日期
- ***"上次更新"***– 提供了上次更新的启动日期
- ***"病毒数据库"***– 告知您当前安装的病毒数据库版本情况
- ***"AVG 版本"***– 告知您所安装的 AVG 版本情况 *版本号采用的格式为 9.0.xx，其中 9.0 是产品系列版本，xx 代表内部版本号）*
- ***"许可证到期日期"***– 提供了您的 AVG 许可证的到期日期

7.6. 系统托盘图标

系统任务栏图标（*在 Windows 任务栏中*）用于指示 **AVG 9 Anti-Virus plus Firewall** 的当前状态。不论 AVG 主窗口是处于打开状态还是关闭状态，此图标在系统托盘中始终都是可见的。

如果图标是彩色的，则***系统任务栏图标***表示所有 AVG 组件均已激活且完全正常运行。此外，如果 AVG 处于错误状态，但您完全清楚这种情况并有意决定***忽略组件状态***，也会显示彩色的 AVG 系统任务栏图标。

带感叹号的图标表示有问题 *（组件已停用，处于错误状态等）*。双击***系统托盘图标***可打开主窗口并对组件进行编辑。

系统任务栏图标还会通过从 AVG 系统任务栏图标打开的弹出窗口，通知当前的 AVG 活动情况以及此程序中可能发生的状态变化情况 *（例如，计划的扫描或更新自动启动，Firewall 配置文件切换，组件状态变化，出现错误状态……）*：

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

- ***"打开 AVG 用户界面"***– 单击此选项可打开 AVG 用户界面
- ***"更新"***– 用于立即启动更新

8. AVG 组件

8.1. Anti-Virus

8.1.1. Anti-Virus 原理

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

防病毒保护软件的一项重要功能就是不让任何已知病毒在计算机上运行！

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

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

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

8.1.2. Anti-Virus 界面

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

- ***"感染定义"***– 此数字提供了在最新版病毒数据库中定义的病毒计数
- ***"最新的数据库更新"***– 指定病毒数据库的上次更新日期和时间
- ***"数据库版本"***– 定义最新的病毒数据库版本号；此版本号将随病毒库的每次更新而递增

此组件的界面中仅有一个操作按钮（***"后退"***）– 按该按钮可恢复默认 AVG 用户界面 组件概览）。

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

8.2. Anti-Spyware

8.2.1. Anti-Spyware 原理

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

目前，最常见的感染来源是包含具有潜在危险的内容的网站。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。

还有一种潜在风险，即恶意软件已在安装 AVG 之前传播到您的计算机中，或者由于疏忽大意，您未将 AVG 9 Anti-Virus plus Firewall 与最新的数据库和程序更新保持同步。因此，AVG 允许您使用扫描功能对计算机进行全面扫描，以检查是否存在恶意软件/间谍软件。它还能够检测休眠和非活动的恶意软件 即已经下载但尚未激活的恶意软件）。

8.2.2. Anti-Spyware 界面

Anti-Spyware 组件的界面简要概述了该组件的功能，提供了有关该组件当前状态的信息

（*"Anti-Spyware 组件已激活。"*），以及一些 ***Anti-Spyware*** 统计信息：

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

此组件的界面中仅有一个操作按钮（***"后退"***）– 按该按钮可恢复默认 AVG 用户界面 组件概览）。

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

8.3. Anti-Rootkit

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

8.4. Firewall

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

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

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

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

8.4.1. Firewall 原理

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

注：*AVG Firewall 不可用于服务器平台！*

AVG Firewall 的功能包括：

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

8.4.2. Firewall 配置文件

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

可用配置文件

- ***全部允许*** - 是制造商预先设置好的 ***Firewall*** 系统配置文件，始终都会显示出来。激活此配置文件后，将允许所有网络通信而不应用任何安全策略规则，就如同关闭 ***Firewall*** 保护一样 *即允许所有应用程序，但仍检查数据包 –若要完全禁用所有过滤功能，您需要禁用 Firewall)*。您不得复制或删除此系统配置文件，也不得修改其设置。
- ***全部阻止*** - 是制造商预先设置好的 ***Firewall*** 系统配置文件，始终都会显示出来。激活此配置文件后，所有网络通信都将被阻止，计算机既不能从外部网络进行访问，也不能与外部进行通信。您不得复制或删除此系统配置文件，也不得修改其设置。

- ***自定义配置文件***:

  - ***直连到 Internet*** - 适用于直接连接到 Internet 的普通家用台式计算机，或在安全的公司网络以外连接到 Internet 的笔记本电脑。如果您是在家中进行连接的或者是在没有中央控制措施的小型公司网络中，请选择此选项。此外，在旅行中或从多种未知且可能有危险的场所 *网吧、酒店房间等*）将笔记本电脑联网时，也请选择此选项。在这种情况下将创建更具限制性的规则，因为会假定这些计算机未采取额外的保护措施，因此需要得到最大程度的保护。

  - ***域中的计算机*** –适用于本地网络 如学校或公司网络）中的计算机。假定网络受某些其它措施保护，因此其安全级别可低于独立计算机。

  - ***小型家庭或办公网络*** –适用于小型网络 如家庭或小型企业）中的计算机，这种网络通常只有几台计算机连在一起，没有 '中央 '管理员。

配置文件切换

借助于配置文件切换功能，***Firewall*** 可在使用特定网络适配器或在连接到特定类型的网络时自动切换到预定义的配置文件。如果尚未为某一网络区域分配配置文件，则在下次连接到此区域时，***Firewall*** 将显示一个对话框，要求您分配配置文件。

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

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

8.4.3. Firewall 界面

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

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

基本组件配置

- ***"选择 Firewall 配置文件"*** – 请从下拉菜单中选择预定义的配置文件之一（有两个配置文件始终都提供，名为 ***"全部允许"*** 和 ***"全部阻止"*** 的默认配置文件），其它配置文件是您在 ***"Firewall 设置"*** 中的 ***"配置文件"*** 对话框中通过编辑配置文件手动添加的。
- ***启用游戏模式*** - 选中此选项可确保在运行全屏应用程序（游戏、PowerPoint 演示文稿等）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。

- ***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***，会允许所有网络流量通行，但不会对其进行检查！
  - ***“紧急模式（阻止所有 Internet 通信）”*** - 选中此选项将阻止通过每个网络端口的所有通信；***Firewall*** 仍在运行，但所有网络通信都会被停止

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

控制按钮

- ***“配置向导”*** - 按此按钮可切换到名为 ***“计算机使用情况选择”*** 的相应对话框（*在安装过程中使用*），在此对话框中可以指定 ***Firewall*** 组件的配置
- ***“保存更改”*** - 按此按钮可保存并应用在此对话框中所做的任何更改
- ***“取消”*** - 按此按钮可返回默认的 AVG 用户界面（*组件概览*）

8.5. E-mail Scanner

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。

8.5.1. E-mail Scanner 原理

E-mail Scanner 组件会自动扫描传入/传出的电子邮件。可将其用于 AVG 中没有专用插件的电子邮件客户端（*如 Outlook Express、Mozilla、Incredimail 等*）。

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。

E-mail Scanner 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，***E-mail Scanner*** 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（*默认情况下已禁用用于扫描传出邮件的功能，可以手动加以设置*）。

注：*AVG E-mail Scanner 不可用于服务器平台！*

8.5.2. E-mail Scanner 界面

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

- ***已扫描的电子邮件总数*** - 自 ***E-mail Scanner*** 上次启动以来扫描了多少封电子

邮件 *如果需要则可重置此值;例如,可出于统计目的重置此值,单击'重置值'即可*)

- ***"发现并阻止的威胁数"***– 提供自 ***E-mail Scanner*** 上次启动以来在电子邮件中检测到的感染数目
- ***"已安装的电子邮件保护插件"***– 有关特定电子邮件保护插件(指您默认安装的电子邮件客户端)的信息

基本组件配置

此对话框的底部有一个名为 ***"E-mail Scanner 设置"*** 的区域,在此区域中您可以编辑该组件功能的一些基本设置:

- ***"扫描传入的邮件"***– 选中此项可指定应对被传递到您帐户的所有电子邮件进行病毒扫描。默认情况下已启用此项,建议不要更改此设置!
- ***"扫描传出的邮件"***– 选中此项可确认应对从您的帐户发出的所有电子邮件进行病毒扫描。默认情况下,此项已禁用。
- ***扫描电子邮件时显示通知图标*** - 选中此选项可确认自己想要在通过 ***E-mail Scanner*** 组件扫描邮件的过程中,通过显示在系统任务栏中的 AVG 图标上的通知对话框得到通知。默认情况下已启用此项,建议不要更改此设置!

E-mail Scanner 组件的高级配置可通过系统菜单的 ***"工具"*** | ***"高级设置"*** 项进行访问;但建议仅限经验丰富的用户使用高级配置!

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

控制按钮

E-mail Scanner 界面中提供的控制按钮如下:

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

8.5.3. E-mail Scanner 检测

在 ***"E-mail Scanner 检测"*** 对话框（*可通过系统菜单选项'历史记录'/'E-mail Scanner 检测'显示*）中，可以看到其中列有 ***E-mail Scanner*** 组件的所有检测结果。对于检测到的每个对象，提供了以下信息：

- ***"感染"*** – 对检测到的对象的描述（甚至可能就是其名称）
- ***"对象"*** – 对象的位置
- ***"结果"*** – 对检测到的对象执行的操作
- ***"检测时间"*** – 检测到此可疑对象的日期和时间
- ***"对象类型"*** – 检测到的对象的类型

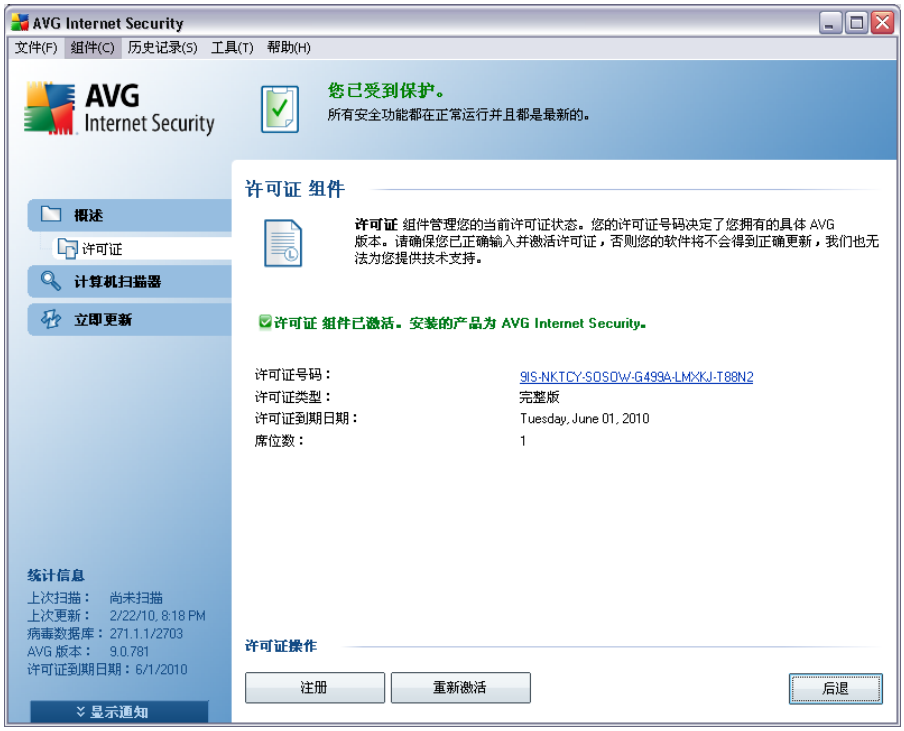
在此对话框底部的列表下方，显示了上面列出的检测到的对象总数信息。此外，还可以将列出的所有检测到的对象都导出到文件中（***"将列表导出至文件"***），也可删除检测到的对象的所有相关条目（***"清空列表"***）。

控制按钮

*"E-mail Scanner 检测"*界面中提供的控制按钮如下：

- *"刷新列表"*– 更新检测到的威胁列表
- *"后退"*– 切换回默认的 *AVG 用户界面* 组件概览）

8.6. 许可证



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

- *"许可证号码"*– 提供您的许可证号码的精确形式。当输入您的许可证号码时，您必须确保其绝对精确并完全按照如图所示键入它。因此，我们强烈建议在对许可证号码进行任何操作时始终使用"复制和粘贴"方法。
- *"许可证类型"*– 指定所安装产品的类型。

- ***许可证到期日期*** –此日期决定了您的许可证的有效期。如果您希望在此日期后继续使用 AVG 9 Anti-Virus plus Firewall，您必须续订您的许可证。在 AVG 网站 (http://www.avg.com/) 上可在线进行许可证续订。

- ***席位数*** –您有权在多少个工作站上安装您的 AVG 9 Anti-Virus plus Firewall。

控制按钮

- ***注册*** - 用于连接到 AVG 网站 (http://www.avg.com/) 的注册页面。请填写您的注册数据；只有注册了自己的 AVG 产品的客户才能享受到免费的技术支持。

- ***重新激活*** - 用于打开 ***"激活 AVG"*** 对话框，其中有安装过程中在 ***对 AVG 进行个性化设置*** 对话框中输入的数据。在此对话框中，您可以输入您的许可证号码来替换销售号码 *(您安装 AVG 时使用的号码)* 或替换原来的许可证号码 *(例如在升级到新的 AVG 产品时)*。

***注**：如果使用的是试用版 AVG 9 Anti-Virus plus Firewall，这两个按钮会显示为 **"立即购买"** 和 **"激活"**，这样就可以立即购买该程序的完整版。对于通过销售号码安装的 AVG 9 Anti-Virus plus Firewall，这两个按钮显示为 **"注册"** 和 **"激活"**。*

- ***"后退"*** – 按此按钮可返回默认的 AVG 用户界面 组件概览)。

8.7. Link Scanner

8.7.1. Link Scanner 原理

LinkScanner 组件用于防范旨在通过 Web 浏览器或其插件将恶意软件安装到用户计算机中的网站。***LinkScanner*** 技术由 ***AVG Search-Shield*** 和 ***AVG Active Surf-Shield*** 这两项功能组成：

- ***AVG Search Shield*** 包含了已知存在危险的网站 *(URL 地址)* 的列表。通过 Google、Yahoo!、Bing、百度、Altavista 或 Yandex 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)*。此外，如果您直接在浏览器中键入某一地址，单击任何网站或电子邮件等包含的链接，都会自动对其进行检查并在必要时予以阻止。

- ***AVG Active 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 ***AVG Search Shield*** 未检测到某一网站 *(例如在创建了新的恶意网站时，或在以前未受感染的网站现在包含了某种恶意软件时)*，用户尝试访问它时 ***AVG Active Surf-Shield*** 也会对它进行检测和阻止。

注 :*AVG Link Scanner 不可用于服务器平台！*

8.7.2. Link Scanner 界面

LinkScanner 组件由两部分组成，您可以在 ***LinkScanner 组件***的界面中启用/禁用它们。

LinkScanner组件的界面简要说明了该组件的功能，并提供了有关该组件当前状态的信息（*"LinkScanner 组件已激活。"*）。此外，此界面中还有关于最新 ***LinkScanner*** 数据库版本号的信息（*"LinkScanner 版本"*）。

在此对话框的底部，您可以对若干选项进行编辑：

- ***启用 AVG Search-Shield*** -（*默认情况下已启用*）：在对 Google、Yahoo!、Bing、百度、Yandex 或 Altavista 等搜索引擎所返回网站的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 AVG Active 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。

- ***"允许向 AVG 报告检测到的威胁"***– 选中此项后，用户可通过 ***Safe Surf*** 或 ***Safe Search*** 以反馈的方式报告自己所发现的漏洞利用和恶意网站，以提供给在 Web 上收集恶意活动信息的数据库。

8.7.3. AVG Search-Shield

如果启用 ***AVG Search-Shield*** 后在 Internet 上进行搜索，则 Yahoo!、Google、Bing、Altavista、Yandex 等最常用的搜索引擎返回的所有搜索结果将被评估是否存在危险或可疑链接。通过检查这些链接并标记恶意链接，***AVG Link Scanner*** 在您点击危险或可疑链接前就发出警告，从而可以确保您只访问安全网站。

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

所链接的页面是安全的（使用 *Yahoo! 搜索引擎在 AVG Security Toolbar 中时，将不显示此图标！*）。

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。信息包括威胁（如果有）的其它详细信息、链接的 IP 地址，以及 AVG 扫描该页面的时间：

8.7.4. AVG Active Surf-Shield

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

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

进入此类网站会带来很大的风险，建议不要进入！

8.8. Online Shield

8.8.1. Online Shield 原理

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

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

注：*AVG Online Shield 不适用于服务器平台！*

8.8.2. Online Shield 界面

Online Shield 组件的界面描述了这种保护的行为。此外，您还可以找到*有关组件当前状态的信息*（Online Shield 已激活并且运行完全正常。"）。接着，在此对话框的底部，您可以找到该组件功能的基本编辑选项。

基本组件配置

首先，您可以通过选中/取消选中 ***"启用 Online Shield"*** 项来直接启用/禁用 ***Online Shield*** 。默认情况下此选项已启用，因而 ***Online Shield*** 组件已激活。不过，若非必要，请勿更改此设置，建议将此组件保留为激活状态。如果此项已选中且 ***Online Shield*** 正在运行，则以下两个选项卡上会有更多配置选项可供选用和编辑：

- ***"Web"*** – 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：

o ***Web 保护*** - 此选项用于确认 ***Online Shield*** 应对万维网页面内容进行扫描。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"*** – 扫描要显示的 www 页面中可能包含的存档的内容
  - ***报告可能不需要的程序和间谍软件威胁*** -*(默认情况下已启用)*：选中此框可激活 ***Anti-Spyware*** 引擎，进行间谍软件和病毒扫描。间谍软件属于疑似恶意软件类软件：即使间谍软件通常是一种安全风险，也可故意安装其中的某些程序。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*** - 如果已激活上一选项，也可选中此框，以

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，但之后却能以不正当的方式使用以达到恶毒的目的。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*** - 使用启发式分析方法（也就是在虚拟的计算机环境中对已扫描对象的指令进行模拟和评估）扫描要显示的页面的内容。因此，它甚至可以检测病毒数据库中尚未描述的恶意代码（*请见 [Anti-Virus 原理](#)*）。

- ***"特扫描文件的最大大小"*** – 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。

- ***"即时通讯"*** – 用于编辑涉及即时通讯（*如 ICQ、MSN、Yahoo 等*）扫描的组件设置。

o 即时通讯保护 - 如果想用 Online Shield 验证在线通信内容是否无毒，请选中此项。如果此选项已启用，您可以进一步指定您要控制哪个即时通讯应用

程序 –目前 AVG 9 Anti-Virus plus Firewall 支持 ICQ、MSN 和 Yahoo 应用程序。

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

控制按钮

Online Shield 界面中有下列控制按钮：

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

8.8.3. Online Shield 检测

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

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

对于检测到的每个对象，提供了以下信息：

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

在此对话框底部的列表下方，显示了上面列出的检测到的对象总数信息。此外，您还可以

将检测到的对象的整个列表导出到一个文件中（***"将列表导出至文件"***），以及删除所有检测到的对象条目（***"清空列表"***）。单击 ***"刷新列表"*** 按钮将更新 ***Online Shield*** 检测结果列表。按 ***"后退"*** 按钮可恢复默认 ***AVG 用户界面*** 组件概览）。

8.9. Resident Shield

8.9.1. Resident Shield 原理

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

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

8.9.2. Resident Shield 界面

除最重要的统计数据概览以及有关组件当前状态的信息（*Resident Shield 已激活并且运*

*行完全正常"之外，**Resident Shield** 界面还提供了一些基本的组件设置选项。统计信息如下：*

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

基本组件配置

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

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

- *自动删除 (***"自动删除所有威胁"**)*
- *或在用户同意后方可删除 (***"删除威胁前询问我"**)*

此选项对安全级别无影响，只是体现了您的使用偏好而已。

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

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

控制按钮

***Resident Shield** 界面中提供的控制按钮如下：*

- ***管理特例** - 用于打开 **Resident Shield - 排除目录**对话框，在此对话框中您可以定义 **Resident Shield** 在扫描时应忽略的文件夹*

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

8.9.3. Resident Shield 检测

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

此对话框提供了有关所检测到的威胁的信息，并请您决定当前应采取何种操作：

- ***"修复"***– 如果存在修复方案，AVG 将自动修复受感染的文件；此选项是建议采取的操作
- ***"移至库"***– 将病毒移至 AVG ***病毒库***
- ***"转至文件"***– 此选项用于将您重定向到可疑对象的确切位置（*打开一个新的 Windows 资源管理器窗口*）
- ***"忽略"***– 我们极力建议，若非绝对必要，请勿使用此选项！

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 发现结果***访问此对话框：

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

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

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

8.10. 更新管理器

8.10.1. 更新管理器原理

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

定期更新 AVG 至关重要！

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

注：*请留意 "AVG 更新"一章，了解有关更新类型和更新级别的更多信息！*

8.10.2. 更新管理器界面

更新管理器的界面显示了有关该组件功能及其当前状态（*更新管理器已激活。*）的信息，

并提供了相关的统计数据：

- ***"最新更新"***– 指定数据库的更新日期和时间
- ***"病毒数据库版本"***– 定义最新的病毒数据库版本号 ;此版本号将随病毒库的每次更新而递增
- ***"下次计划更新"***– 指定计划下次更新此数据库的日期和时间

基本组件配置

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

此外，您还可以定义应在何时启动更新：

- ***"定期"***– 定义时间间隔
- ***"在特定时间"***– 定义确切的日期和时间。

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

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

控制按钮

更新管理器界面中提供的控制按钮如下：

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

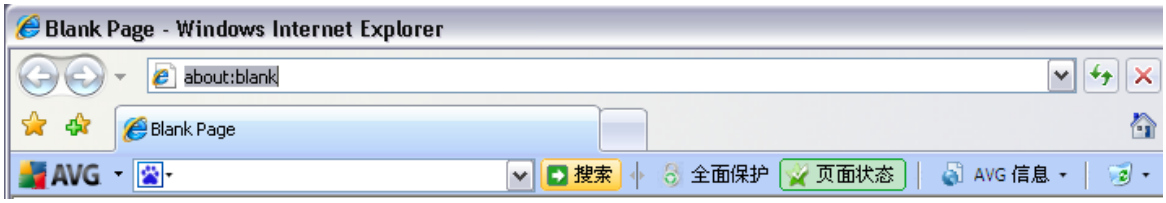
9. AVG Security Toolbar

AVG Security Toolbar 是一种新工具，可与 ***AVG Link Scanner*** 组件一同使用，用于检查受支持的 Internet 搜索引擎（*Yahoo!*、*Google*、*Bing*、*Altavista*、*百度*）的搜索结果。可用 ***AVG Security Toolbar*** 控制 ***AVG Link Scanner*** 功能，以及调整其行为。

如果在 AVG 9 Anti-Virus plus Firewall 安装过程中选择安装此工具栏，则会自动将其添加到 Web 浏览器中。如果使用的是某种备选 Internet 浏览器（*例如 Avant Browser*），则可能会遇到意外情况。

9.1. AVG Security Toolbar 界面

AVG Security Toolbar 旨在与 ***MS Internet Explorer***（*6.0 版或更高版本*）和 ***Mozilla Firefox***（*2.0 版或更高版本*）配合使用。在您决定要安装 ***AVG Security Toolbar***（*在 AVG 安装过程中，系统会询问您是否要安装该组件*）后，该组件将位于您的 Web 浏览器中地址栏的紧下方：



注：*AVG Security Toolbar 不可用于服务器平台！*

AVG Security Toolbar 由以下部分组成：

- ***AVG 徽标*** - 提供对一般工具栏项目的访问。单击此徽标按钮可重定向到 AVG 网站（http://www.avg.com/）。单击 AVG 图标旁边的指针可打开以下内容：
  - ***"Toolbar 信息"***– 指向 ***AVG Security Toolbar*** 主页的链接，该主页详细介绍了此工具栏提供的保护情况
  - ***启动 AVG 9 Anti-Virus plus Firewall*** - 打开 AVG 9 Anti-Virus plus Firewall 用户界面
  - ***"选项"***– 打开一个配置对话框，您可以在此对话框中调整 ***AVG Security Toolbar*** 设置以满足您的需要 –请参见后面的章节：***"AVG Security Toolbar 选项"***
  - ***"删除历史记录"***– 用于 *"删除整个历史记录"*（AVG Security Toolbar），或者 *"删除搜索历史记录"*、*"删除浏览器历史记录"*、*"删除下载历史记录"* 以及 *"删除 Cookie"*。

- ***"更新"*** – 将检查 ***AVG Security Toolbar 的最新更新***

- ***帮助*** - 其中的选项用于打开帮助文件、提交产品反馈意见或查看目前所使用的 Toolbar 版本的详细信息。

- ***搜索框*** - 可将词语或短语输入搜索框。无论目前显示的是什么网页，均可按 ***"搜索"*** 开始通过指定的搜索引擎进行搜索 *(可在 AVG Security Toolbar 高级选项中指定所要使用的搜索引擎，也可选用 Yahoo!、Wikipedia、百度、WebHledani 或 Yandex)*。搜索框还会列出您的搜索历史记录。通过搜索框执行的搜索会被使用 AVG Search-Shield ***保护功能来进行分析。***

- ***全面保护*** - 此按钮会随用户所作的选择显示为 ***"全面保护"*** / ***"有限保护"*** / ***"没有保护"***，具体情况取决于AVG 9 Anti-Virus plus Firewall配置

- ***页面状态*** - 此按钮用于直接在工具栏中显示根据 ***AVG Search-Shield*** 组件的标准得出的正在上载的网页的评估结果 *(页面安全 / 可疑 / 确定有风险 / 包含威胁 / 无法扫描)*。单击该按钮可打开一个信息面板，其中有关于特定网页的详细数据。

- ***AVG 信息*** - 提供指向 AVG 网站 (http://www.avg.com/) 上的重要安全信息的链接。

  - ***"Toolbar 信息"*** – 指向 ***AVG Security Toolbar*** 主页的链接，该主页详细介绍了此工具栏提供的保护情况

  - ***关于威胁*** - 用于打开 AVG 网页，其中有关于 Internet 上当前病毒和威胁的信息

  - ***AVG 新闻*** - 用于打开网页，其中有关于 AVG 的最新新闻

  - ***当前威胁级别*** - 用于打开相应的病毒实验室网页，其中以图形方式显示了网上的当前威胁级别

  - ***病毒百科全书*** - 用于打开 "病毒百科全书" 页面，在此页面中您可以按名称搜索特定的病毒，获得每个病毒的详细信息

9.2. AVG Security Toolbar 选项

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

9.2.1. ‘常规 ’选项卡

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

- ***‘AVG 新闻 ’按钮*** - 该按钮用于打开网页，其中有关于 AVG 的最新新闻
- ***‘新闻 ’按钮*** - 通过该按钮可分门别类地大概了解媒体每天发布的最新新闻
- ***‘AVG 信息 ’按钮*** - 通过该按钮可了解有关 AVG 工具栏、最新威胁和 Internet 威胁严重程度的信息，可打开病毒百科全书，还可查看更多 AVG 产品相关新闻
- ***‘删除历史记录 ’按钮*** – 通过此按钮可以直接从 ‘AVG Security Toolbar ’面板中 ‘删除整个历史记录 ’、‘删除搜索历史记录 ’、‘删除浏览器历史记录 ’、‘删除下载历史记录 ’或 ‘删除 Cookie ’。

9.2.2. ‘有用的按钮 ’选项卡

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

9.2.3. '安全 '选项卡

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

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

请选中相应的选项以确认您希望获得关于此特定威胁级别的通知。不过，无法禁止

显示为包含活动威胁和危险威胁的页面分配的红色标记。***再次说明，对于程序供应商设置的默认配置，除非确有必要更改，否则建议保留。***

9.2.4. '高级选项'选项卡

首先要在 ***"高级选项"***选项卡中选择要在默认情况下使用的搜索引擎，可从 *Yahoo!*、*百度*、*WebHledani* 和 *Yandex* 中进行选择。更改默认搜索引擎后，请重新启动 Internet 浏览器，以使所作的更改生效。

此外，还可激活或关闭其它特定 ***AVG Security Toolbar*** 设置：

- ***"将 Yahoo! 设置并保留为地址栏搜索引擎"***–(*默认情况下已启用*) –如果选中此选项，则您可以直接在 Internet 浏览器的地址栏中键入搜索关键字，将自动利用 Yahoo! 服务来搜索相关网站。
- ***让 AVG 就浏览器导航错误(404/ DNS)提出建议*** -(*默认情况下已启用*)- 如果在网上搜索时进入不存在的页面或无法显示的页面（404 错误），则会自动重定向到一个网页，用其可从相关主题的备选页面中进行选择。
- ***"将 Yahoo! 设置并保留为浏览器搜索引擎"***–(*默认情况下已禁用*) –Yahoo! 是 AVG Security Toolbar 中用来进行网上搜索的默认搜索引擎，如果激活此选项，则它也会成为您的 Web 浏览器的默认搜索引擎。
- ***"重新显示隐藏的 AVG Security Toolbar（每周）"***–(*默认情况下已启用*) –此选

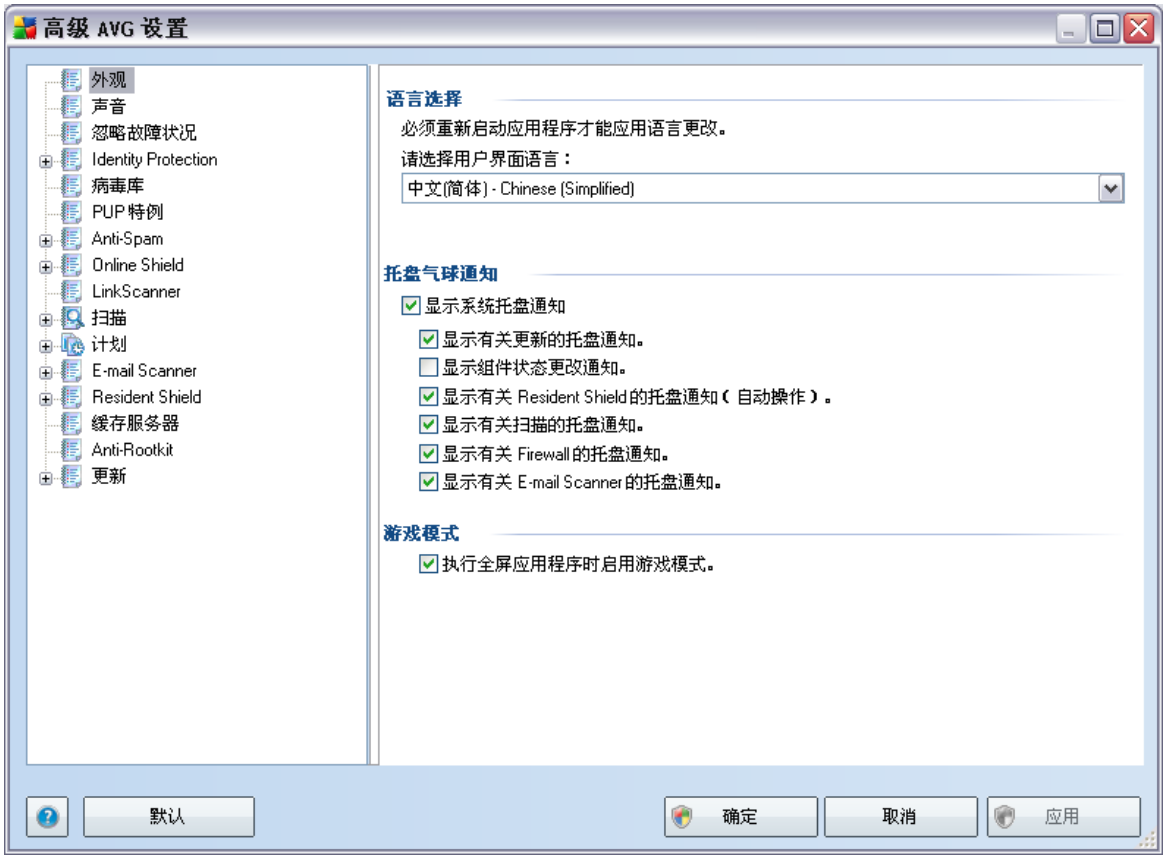
项在默认情况下已激活，当您的 ***AVG Security Toolbar*** 被意外隐藏起来时，此选项会在一周内重新显示它。

10. AVG 高级设置

会在名为 ***"高级 AVG 设置"***的新窗口中打开 AVG 9 Anti-Virus plus Firewall 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

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

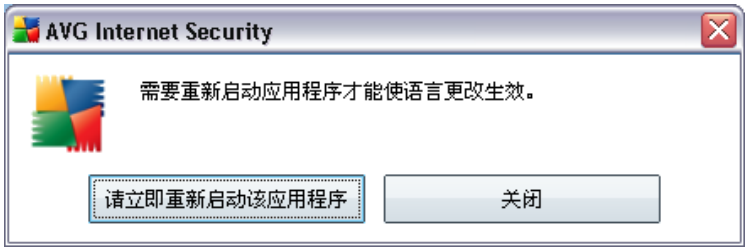


语言选择

在 ***"语言选择"***区域中，可以从其中的下拉菜单中选择所需的语言；然后整个 AVG 用户界面都将使用该语言。此下拉菜单仅提供您之前在安装过程中选择安装的那些语言 (请参见

"自定义安装 – 组件选择"一章)。不过,您必须重新启动用户界面才能完成将应用程序切换到其它语言的过程;请按以下步骤操作:

- 选择所需的应用程序语言,然后按 ***"应用"*** 按钮 (位于右下角)确认您所做的选择
- 按 ***"确定"*** 按钮进行确认
- 随即会弹出一个新的对话框窗口,告知您更改 AVG 用户界面语言后需要重新启动应用程序:



托盘气球通知

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

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

- ***"显示系统托盘通知"*** – 默认情况下此项已选中 (*启用*),因而通知会显示。取消选中此项可完全禁止显示所有气球通知。启用此项后,您可以进一步选择应显示哪些特定通知:
  - ***"显示有关更新的托盘通知"*** – 决定是否应显示有关 AVG 更新过程的启动、进度及完成情况的信息;
  - ***"显示组件状态变更通知"*** – 决定是否应显示有关组件的活动/不活动状态或其可能存在的问题的信息。在报告组件的故障状态时,此选项相当于系统托盘图标 (颜色变化)的通知功能,该功能用来报告任何 AVG 组件中存在的问题;
  - ***显示有关 Resident Shield 的任务栏通知*** - 用于决定是否会显示有关文件保存、复制和进程打开的信息 (*此配置仅可显示是否已启用 Resident Shield "自动修复"选项*);

- ***"显示有关扫描的托盘通知"***– 决定是否应显示有关计划的扫描的自动启动、进度及结果的信息；

- ***"显示有关 Firewall 的托盘通知"***– 决定是否应显示有关 Firewall 状态和进程的信息，例如该组件的启用/停用警告、可能的通信阻止等情况；

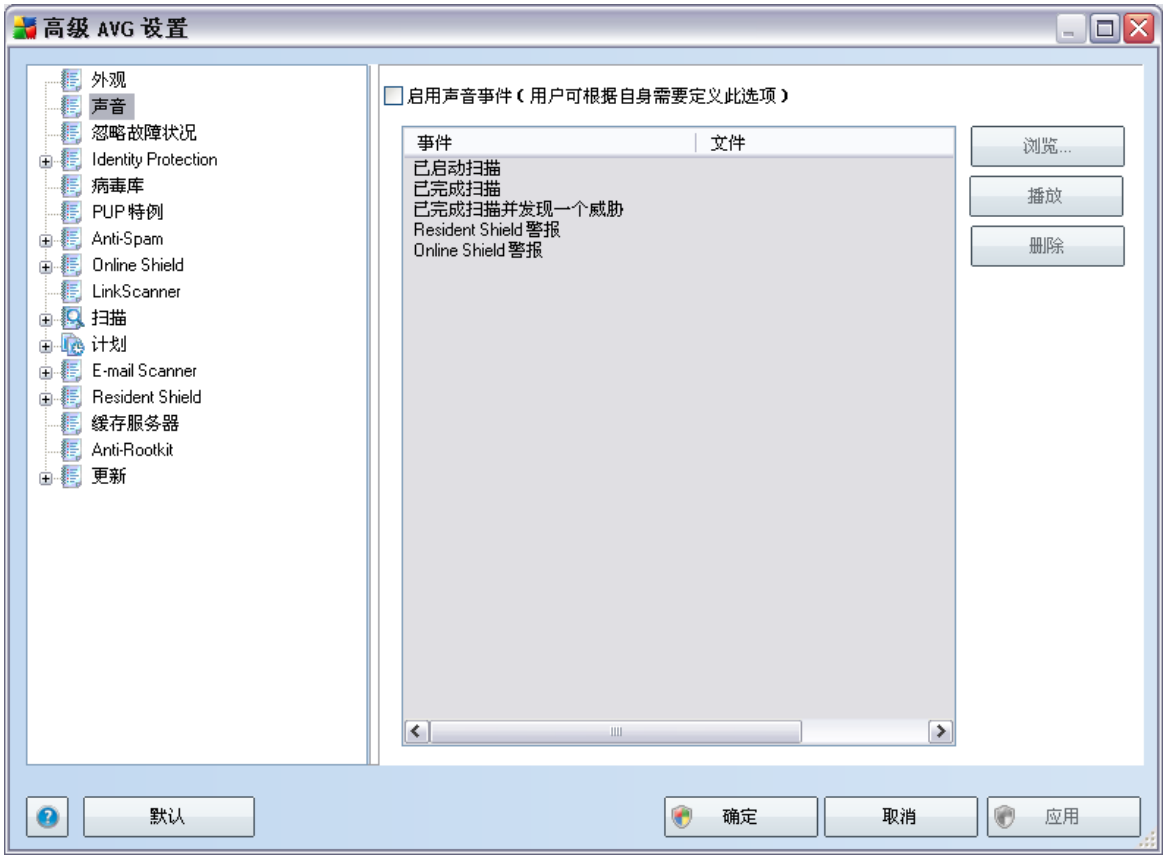
- ***"显示有关 E-mail Scanner 的托盘通知"***– 决定是否应显示有关所有传入和传出电子邮件的扫描的信息。

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)*。

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 操作的情况。如果是，请选中 ***"启用声音事件"*** 选项 *(默认情况下已禁用)* 以激活 AVG 操作的列表：

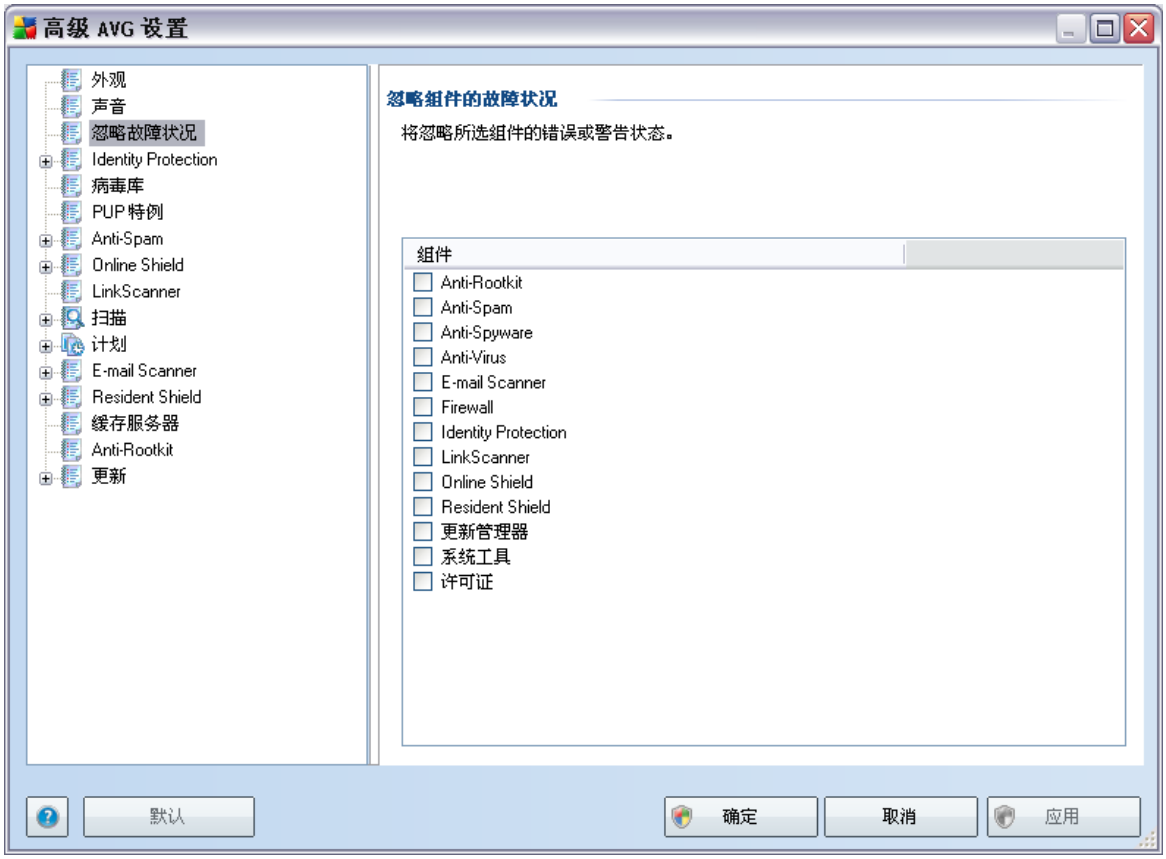


接着，请从此列表中选择相应的事件，然后在磁盘中通过浏览 (***"浏览"***) 查找要为此事件分配的合适声音。若要听一下所选的声音，请突出显示此列表中的相应事件，然后按 ***"播放"*** 按钮。使用 ***"删除"*** 按钮可删除为特定事件分配的声音。

注：*仅支持 *.wav 格式的声音！*

10.3. 忽略故障状况

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



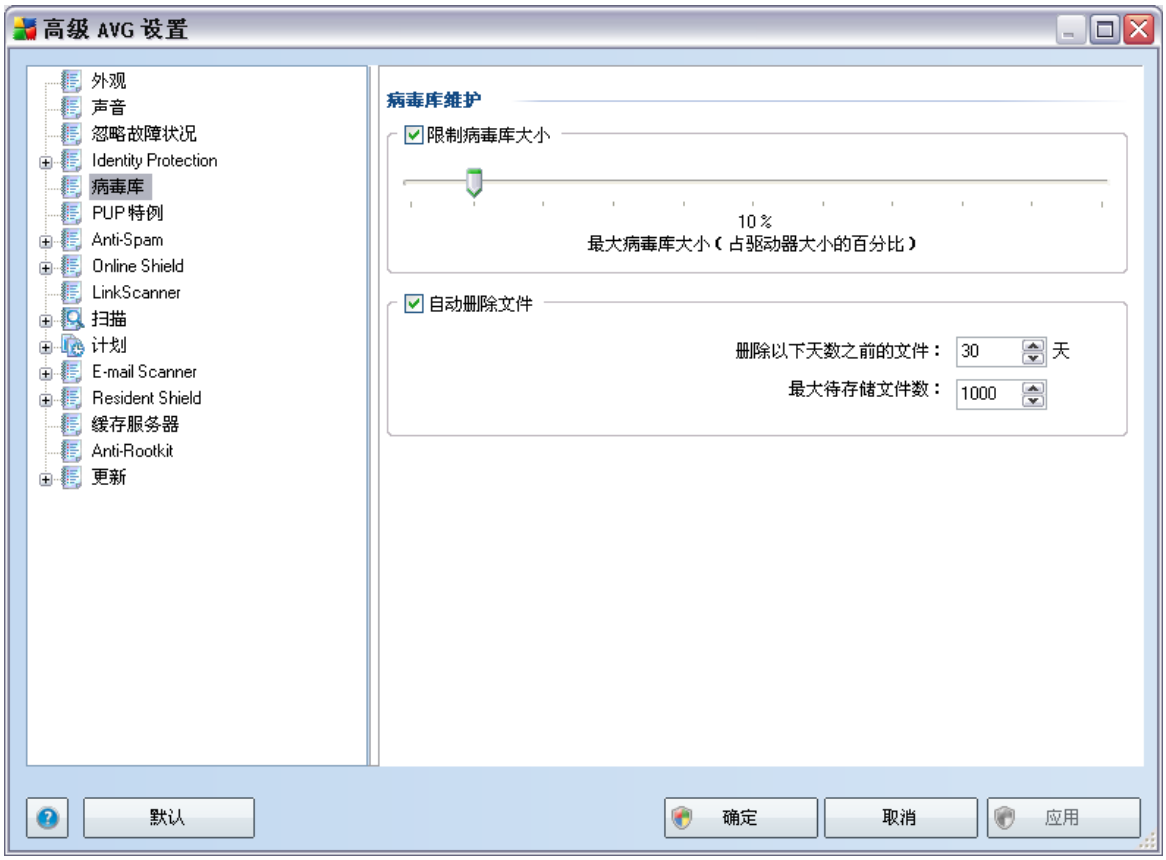
默认情况下，此列表中未选定任何组件。这意味着，如果有任何组件出现错误状态，系统会立即通过以下方式将此情况告知您：

- ***系统托盘图标*** – 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，系统托盘图标会自动报告该组件的错误状态。但对于这种特殊的情况，我们不能将其算作真正的错误，因为这是您自己故意引起的，并且您也知道这带来的潜在危险。同时，一旦此图标以灰色显示，它实际上就无法报告可能出现的任何其它错误。

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

10.4. 病毒库

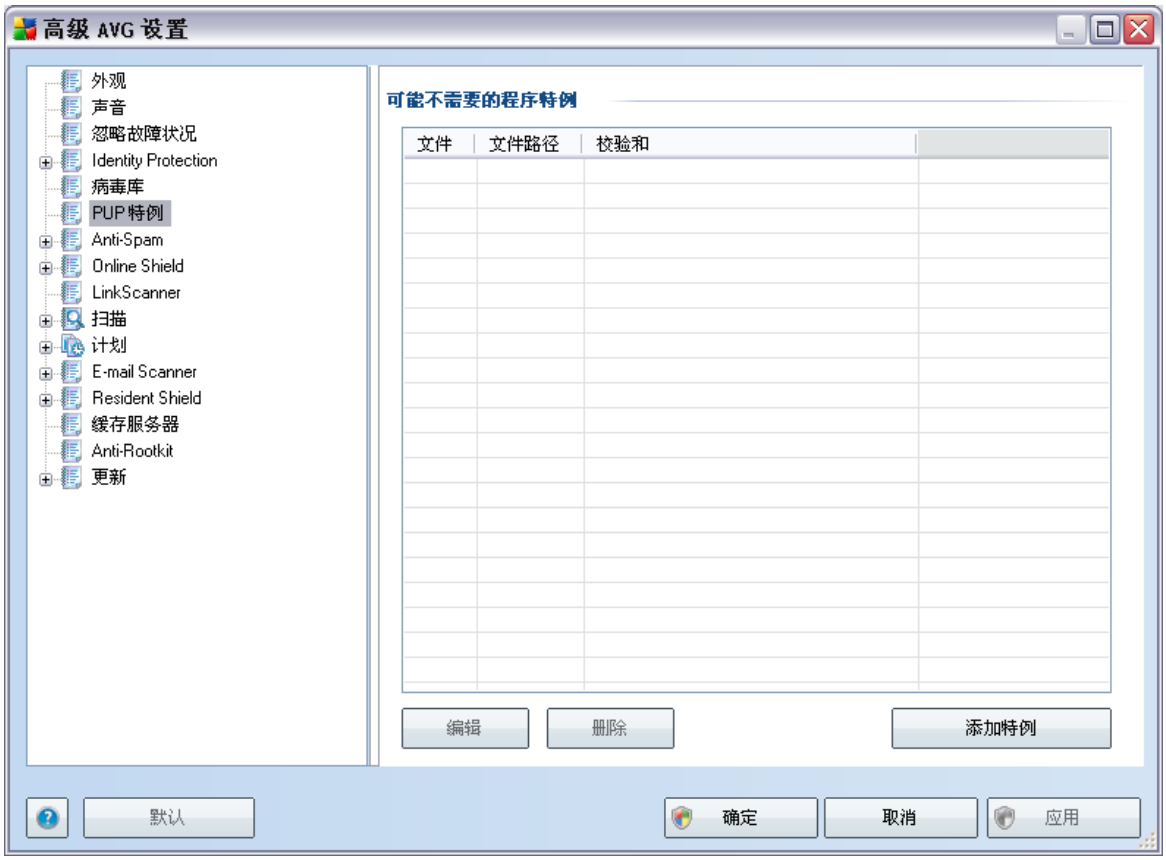


通过 ***"病毒库维护"*** 对话框，可定义关于管理 ***病毒库*** 中存储的对象的若干参数：

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

10.5. PUP 特例

AVG 9 Anti-Virus plus Firewall 能够分析和检测系统中可能不需要的可执行应用程序或 DLL 库。在某些情况下，用户可能希望让某些不需要的程序留在计算机上（*这些程序是有意安装的*）。有些程序（特别是免费程序）包含广告软件。AVG 可能会检测到此类广告软件并将它们报告为***可能不需要的程序***。如果您希望将这样的程序保留在您的计算机上，则可以将它定义为可能不需要的程序特例：



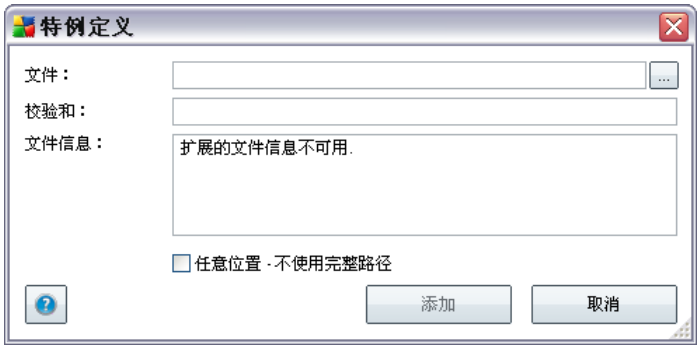
"可能不需要的程序特例"对话框列出了已定义且当前有效的"可能不需要的程序"的特例。您可以对此列表进行编辑，删除现有项，或添加新特例。此列表中提供了有关每个特例的以下信息：

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

成并显示。

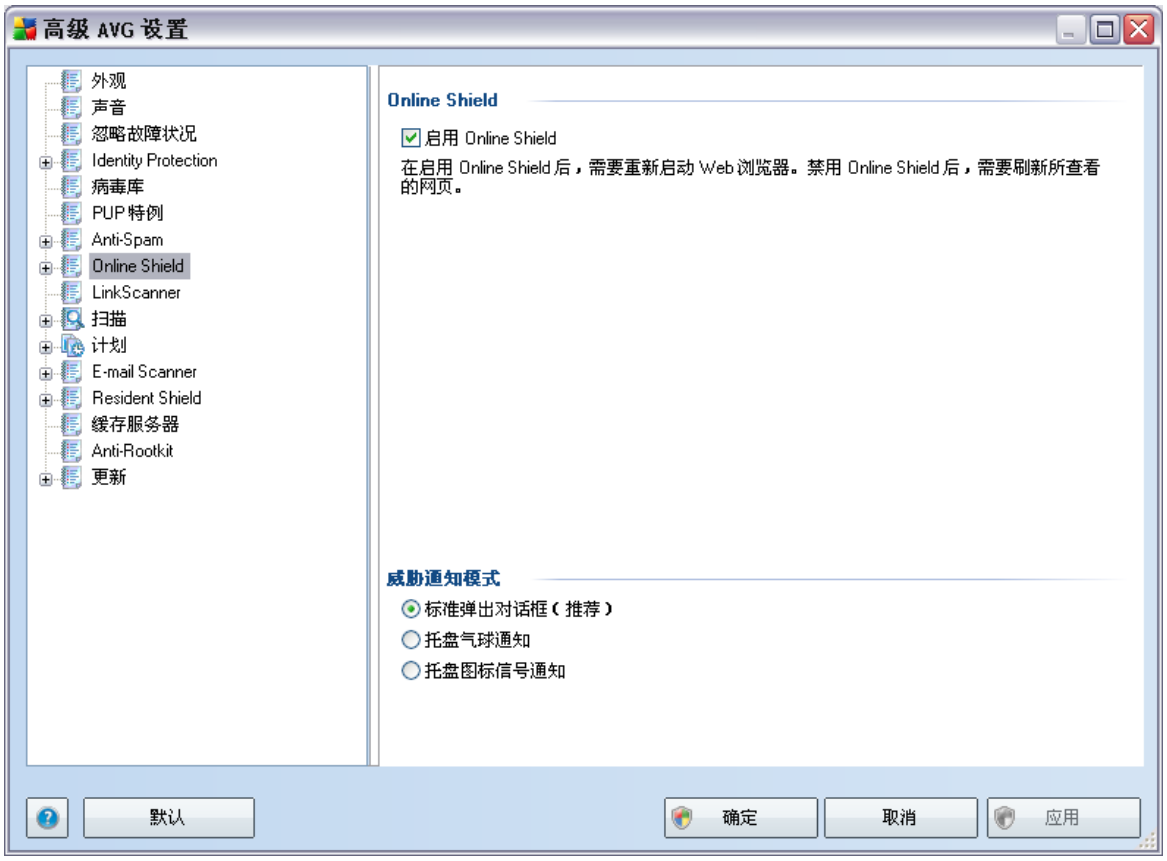
控制按钮

- ***"编辑"***– 打开已定义的特例的编辑对话框 *(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：



- ***"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"***– 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，那么请将此复选框保留为未选中状态

10.6. Online Shield



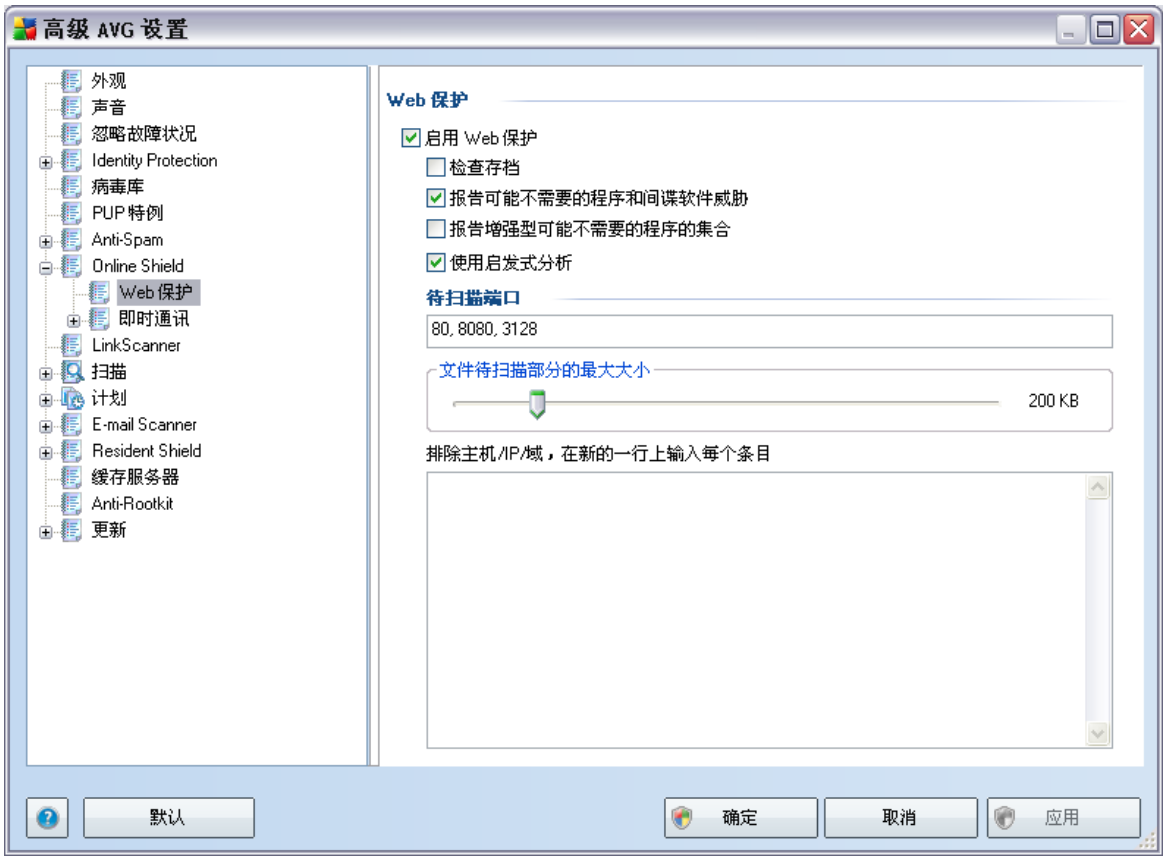
通过 ***"Web 保护"***对话框，可由 ***"启用 Online Shield"***选项 *(默认情况下已激活)* 来激活/停用整个 ***Online Shield*** 组件。有关此组件的进一步高级设置，请继续访问树导航结构中列出的后续对话框：

- ***Web 保护***
- ***即时通讯***

威胁通知模式

在此对话框的底部区域，请选择您希望通过哪种方式获知可能检测到威胁的情况：通过标准的弹出对话框，通过托盘气球状通知，还是通过托盘图标信息。

10.6.1. Web 保护



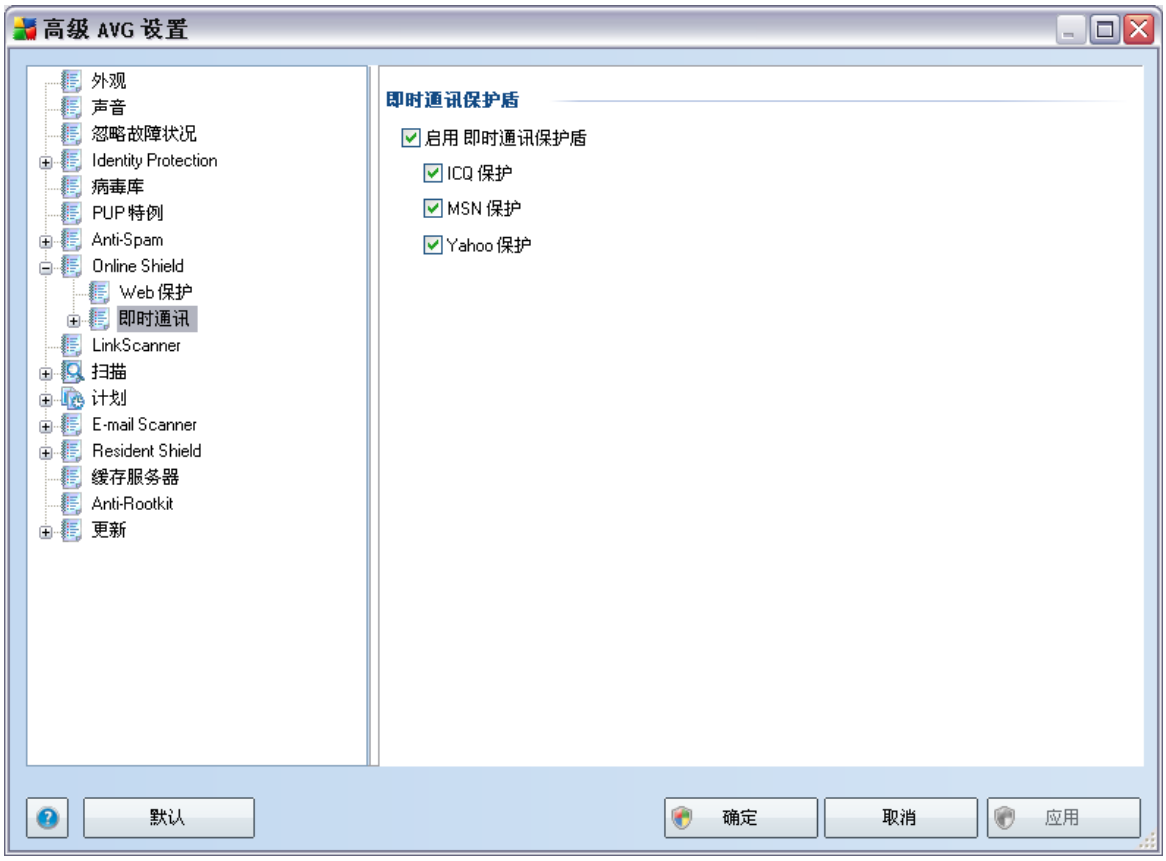
在 ***"Web 保护"*** 对话框中，您可以编辑该组件的与网站内容扫描有关的配置。在编辑界面中，可以配置下列基本选项：

- ***启用 Web 保护*** - 此选项用于确认 ***Online Shield*** 应对万维网页面内容进行扫描。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*** - 扫描要显示的万维网页面中可能包含的存档的内容。
    - ***报告可能不需要的程序和间谍软件威胁*** -*(默认情况下已启用)*：选中此框可激活 ***Anti-Spyware*** 引擎，进行间谍软件和病毒扫描。间谍软件属于疑似恶意软件类软件：即使间谍软件通常是一种安全风险，也可故意安装其中的某些程序。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*** - 如果已激活上一选项，也可选中此框，以检测更多间谍软件：程序直接从制造商获得后极其安全而无害，但之后却能以

不正当的方式使用以达到恶毒的目的。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*** - 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。
- ***"待扫描端口"*** – 此字段列出了标准的 http 通信端口号。如果您的计算机配置与此不同，则您可以根据需要更改这些端口号。
- ***"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 地址码或 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。

10.6.2. 即时通讯

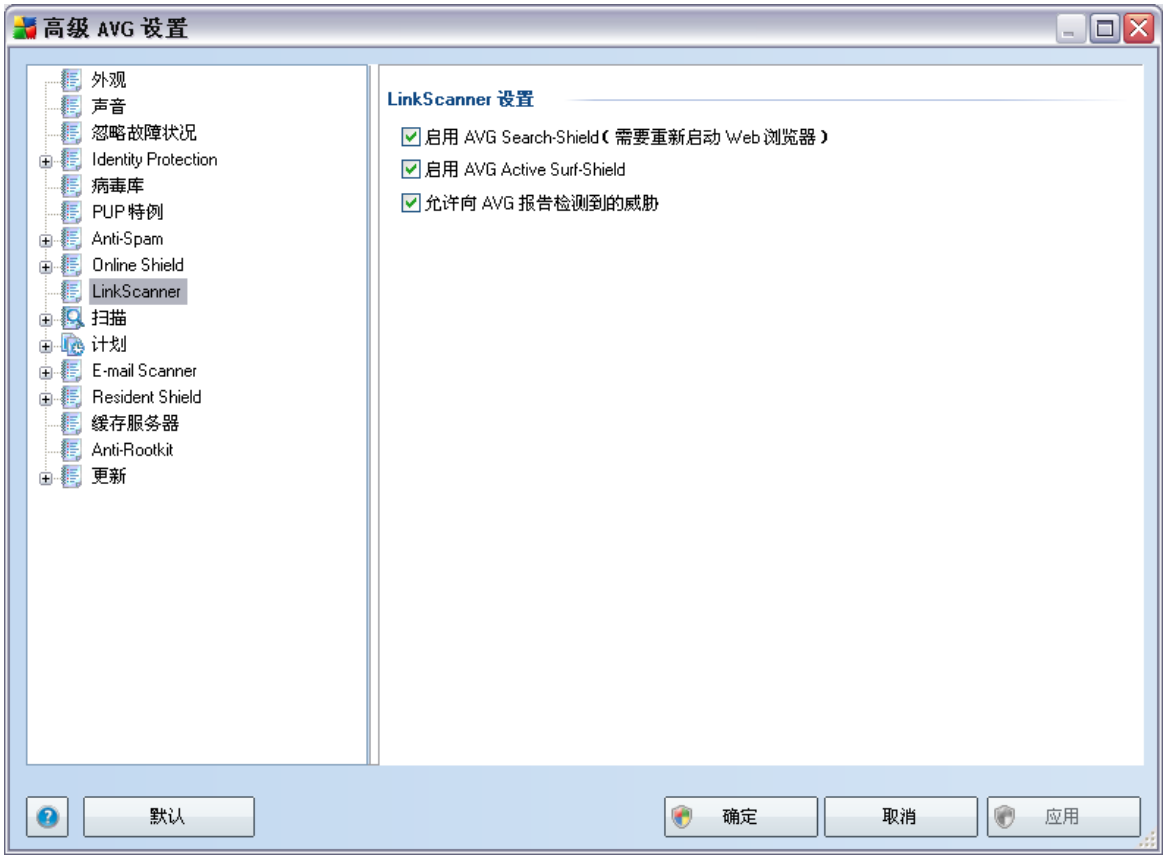


在 ***"即时通讯保护盾"*** 对话框中，可编辑涉及即时通讯扫描的 ***Online Shield*** 组件设置。目前支持以下三种即时消息传递程序：***ICQ***、***MSN*** 和 ***Yahoo*** - 如果要让 ***Online Shield*** 验证在线通信内容是否无病毒，请勾选上述每种程序的相应选项。

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

10.7. Link Scanner

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



- ***启用 AVG Search-Shield*** -（*默认情况下已启用*）：在对 Google、Yahoo、Bing、Yandex、Altavista 或百度等搜索引擎所返回网站的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 AVG Active 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。
- ***“允许向 AVG 报告检测到的威胁”***-（*默认情况下已启用*）：选中此项后，用户可通过 ***AVG Active Surf-Shield*** 或 ***AVG Search-Shield*** 以反馈的方式报告自己所发现的漏洞利用和恶意网站，以提供给在 Web 上收集恶意活动信息的数据库。

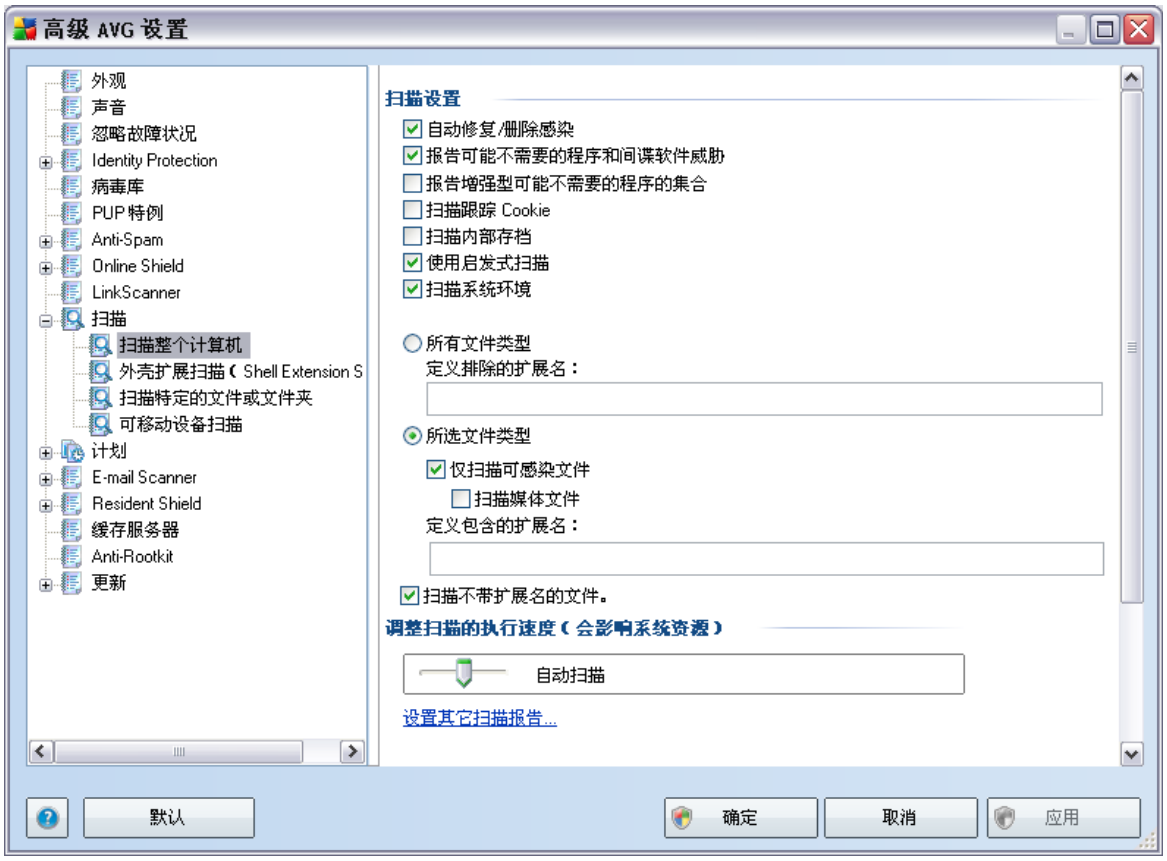
10.8. 扫描

高级扫描设置分为三种类别，分别对应于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

10.8.1. 扫描整个计算机

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



扫描设置

"扫描设置"区域提供了可以选择启用/禁用的扫描参数的列表：

- ***"自动修复/删除感染"***– 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，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：即使间谍软件通常是一种安全风险，也可故意安装其中的某些程序。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*** - 如果已激活上一选项，也可选中此框，以检测更多间谍软件：程序直接从制造商获得后极其安全而无害，但之后却能以不正当的方式使用以达到恶毒的目的。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"***– Anti-Spyware 组件的此参数用于定义应检测的 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"***– 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、RAR 等）内也不例外
- ***"使用启发式扫描"***– 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"***– 扫描时还将检查您计算机的系统区域。

此外，您还应决定要扫描的文件类型：

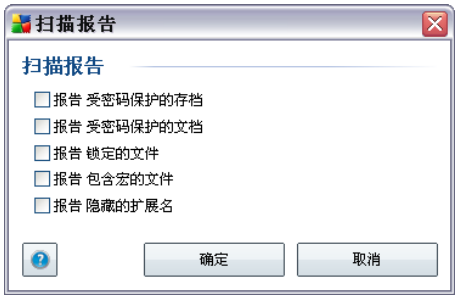
- ***所有文件类型***，选择此选项可以通过提供一列由逗号分隔（*保存后逗号会变成分号*）、不应扫描的文件扩展名来定义一些排除在扫描范围之外的特例；
- ***"所选文件类型"***– 可以指定希望仅扫描可能受到感染的文件（*将不扫描不可能遭到感染的文件，例如某些纯文本文件或某些其它的不可执行文件*），其中包括媒体文件（*视频、音频文件 – 如果将此框保留为未选中状态，则会进一步缩短扫描时间，因为这些文件通常很大，不太可能受到病毒感染*）。此外，您还可以通过扩展名指定哪些文件是始终应扫描的文件。
- 您也可以选择指定要 ***"扫描不带扩展名的文件"***– 默认情况下此选项已启用：我们建议，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

在 ***"扫描进程优先级"*** 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，此选项值设置为中级，即自动确定资源使用。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。

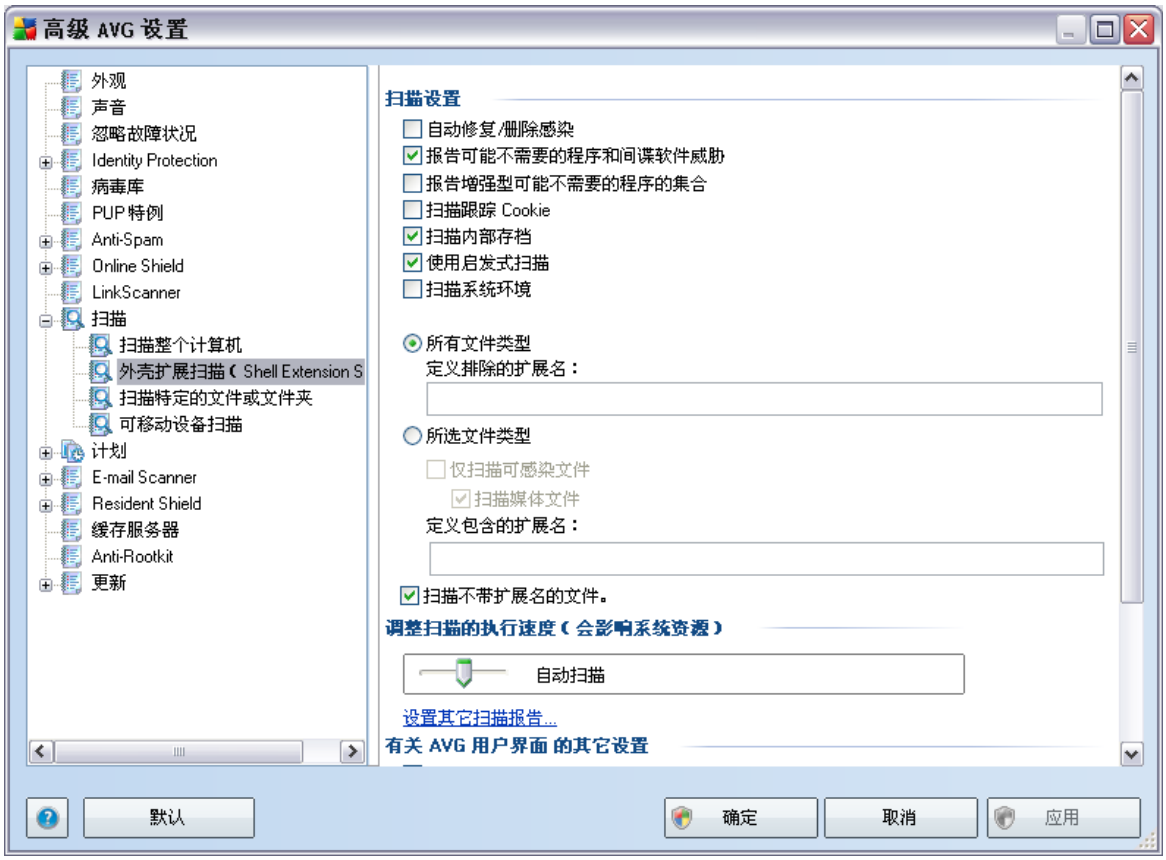
设置其它扫描报告...

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：



10.8.2. 外壳扩展扫描

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

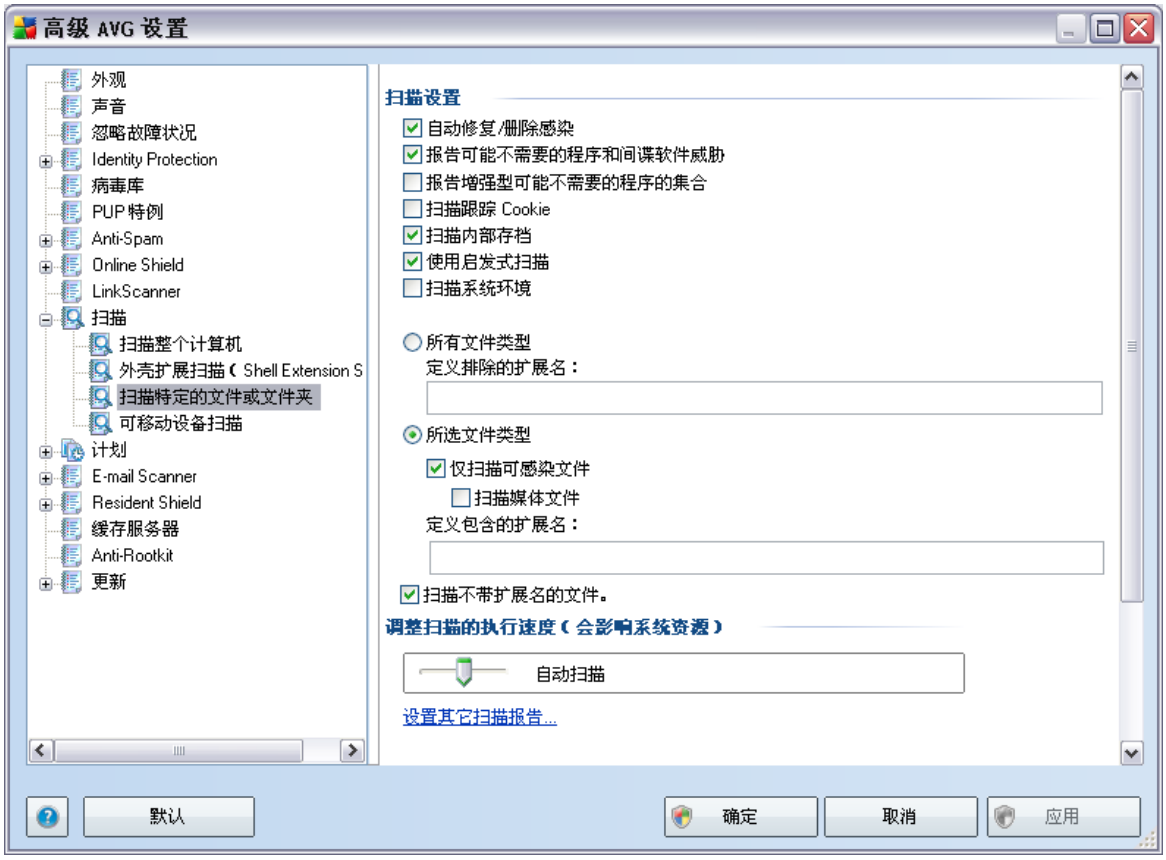


相应的参数列表与可用于 ***"扫描整个计算机"*** 的参数列表相同。但是，二者的默认设置是不同的：对于 ***"扫描整个计算机"***，大多数参数均已选定；而对于 ***"外壳扩展扫描"***（***在 Windows 资源管理器中扫描***），只有相关参数已启用。

***注：**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。*

10.8.3. 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：**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。*

10.8.4. 可移动设备扫描

*"可移动设备扫描"*的编辑界面与*"扫描整个计算机"*编辑对话框也非常相似：

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：**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。*

10.9. 计划

在*"计划"*区域中，您可以编辑以下各项的默认设置：

- 整个计算机扫描计划
- 病毒数据库更新计划

- 程序更新计划

10.9.1. 计划的扫描

可以在以下三个选项卡上编辑计划的扫描的参数 *(或设置新的计划)*:

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。

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

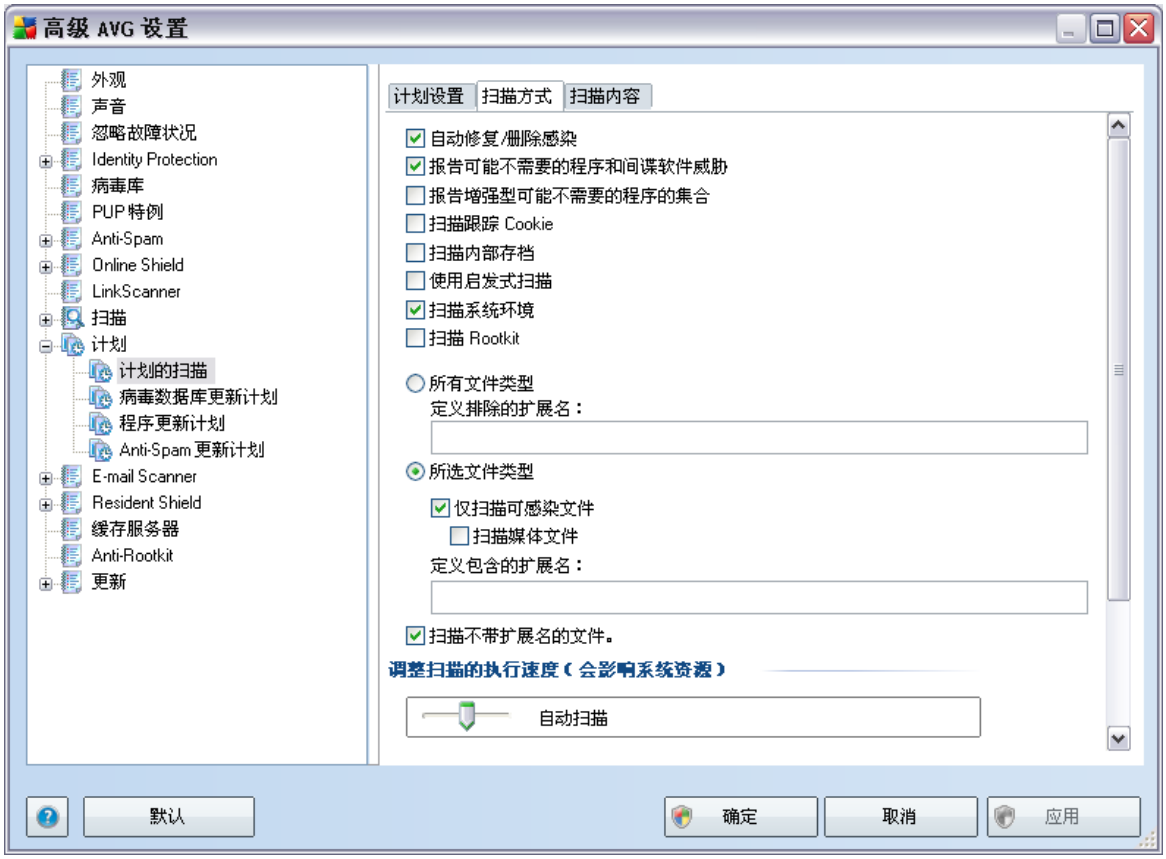
可在此指定新计划的扫描启动任务的时间间隔。此时间间隔的定义方式有三种：指定经过一段特定的时间后重复启动扫描（***"每隔...运行一次"***），或通过定义确切的日期和时间（***"以特定的时间间隔运行..."***），也可以定义扫描启动操作应关联的事件（***"计算机启动时的操作"***）。

高级计划选项

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

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

随即便会出现一个新的 AVG 系统托盘图标（*以全部颜色显示并带有一个白色箭头 –见上图*），告诉您计划的扫描正在运行。右键单击这个表示正在运行扫描的 AVG 图标可打开一个上下文菜单，在此菜单中您可以决定暂停甚至停止正在运行的扫描：



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

- ***"自动修复/删除感染"***– 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，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 :即使间谍软件通常是一种安全风险，也可故意安装其中的某些程序。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*** - 如果已激活上一选项，也可选中此框，以检测更多间谍软件 :程序直接从制造商获得后极其安全而无害，但之后却能以不正当的方式使用以达到恶毒的目的。这项附加措施可以进一步提高计算机的安全性，但也可能会阻止合法程序，因此默认情况下已将其禁用。

- ***扫描跟踪 Cookie*** -(*默认情况下已启用*):***Anti-Spyware*** 组件的此参数用于定义在扫描期间应检测的 Cookie;(*HTTP Cookie 用于验证用户身份、跟踪和维护有关用户的特定信息,如站点首选项或其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所有文件,即使这些文件被存储在压缩包 (如 ZIP、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;

- ***"扫描 Rootkit"***-如果您要将 Rootkit 检测纳入对整个计算机的扫描,请勾选此项。在 ***Anti-Rootkit*** 组件中,Rootkit 检测功能也单独作为一项功能供用户使用;

此外,您还应决定要扫描的文件类型:

- ***所有文件类型***,选择此选项可以通过提供一列由逗号分隔 (*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;

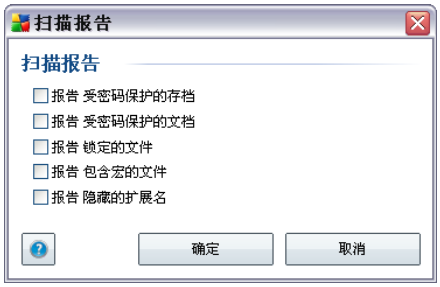
- ***"所选文件类型"***-可以指定希望仅扫描可能受到感染的文件 (*将不扫描不可能遭到感染的文件,例如某些纯文本文件或某些其它的不可执行文件*),其中包括媒体文件 (*视频、音频文件 -如果将此框保留为未选中状态,则会进一步缩短扫描时间,因为这些文件通常很大,不太可能受到病毒感染*)。此外,您还可以通过扩展名指定哪些文件是始终应扫描的文件。

- 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。

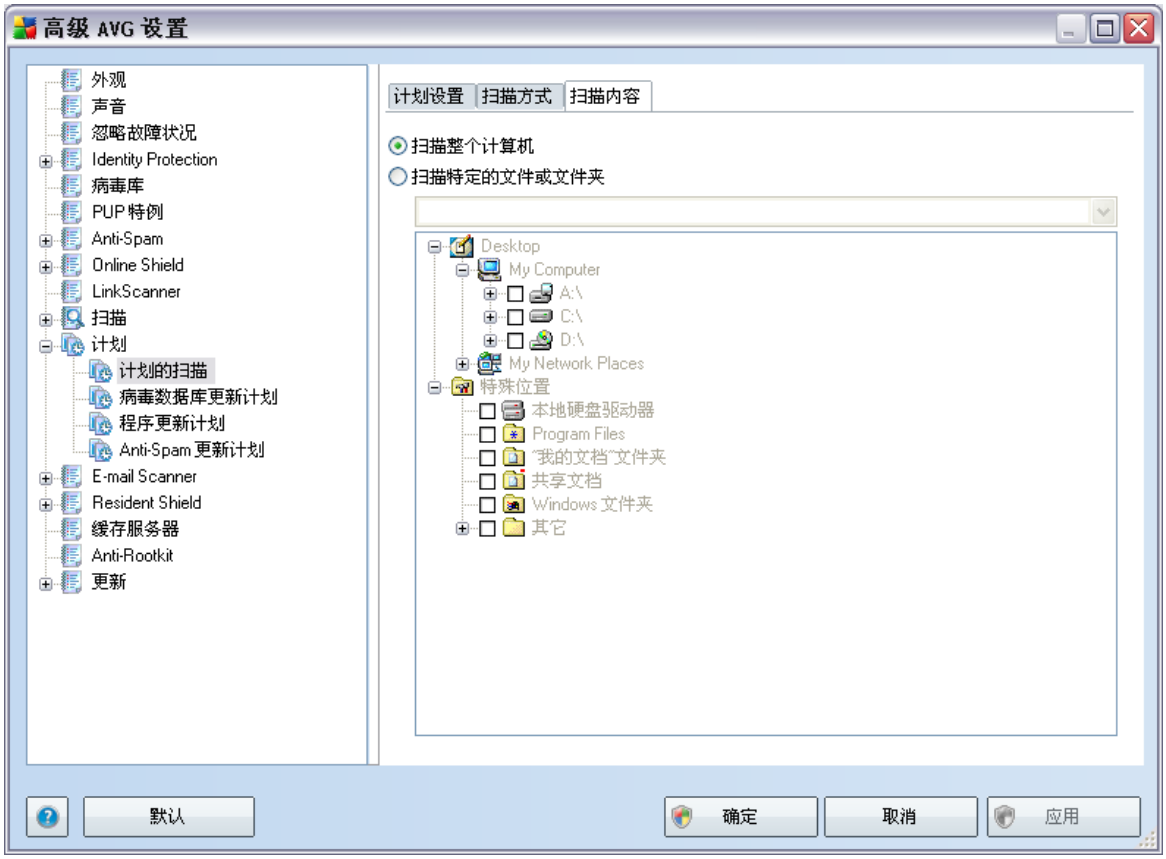
扫描进程优先级

在 ***"扫描进程优先级"***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,此选项设置为中级,即自动确定资源使用。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。

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:

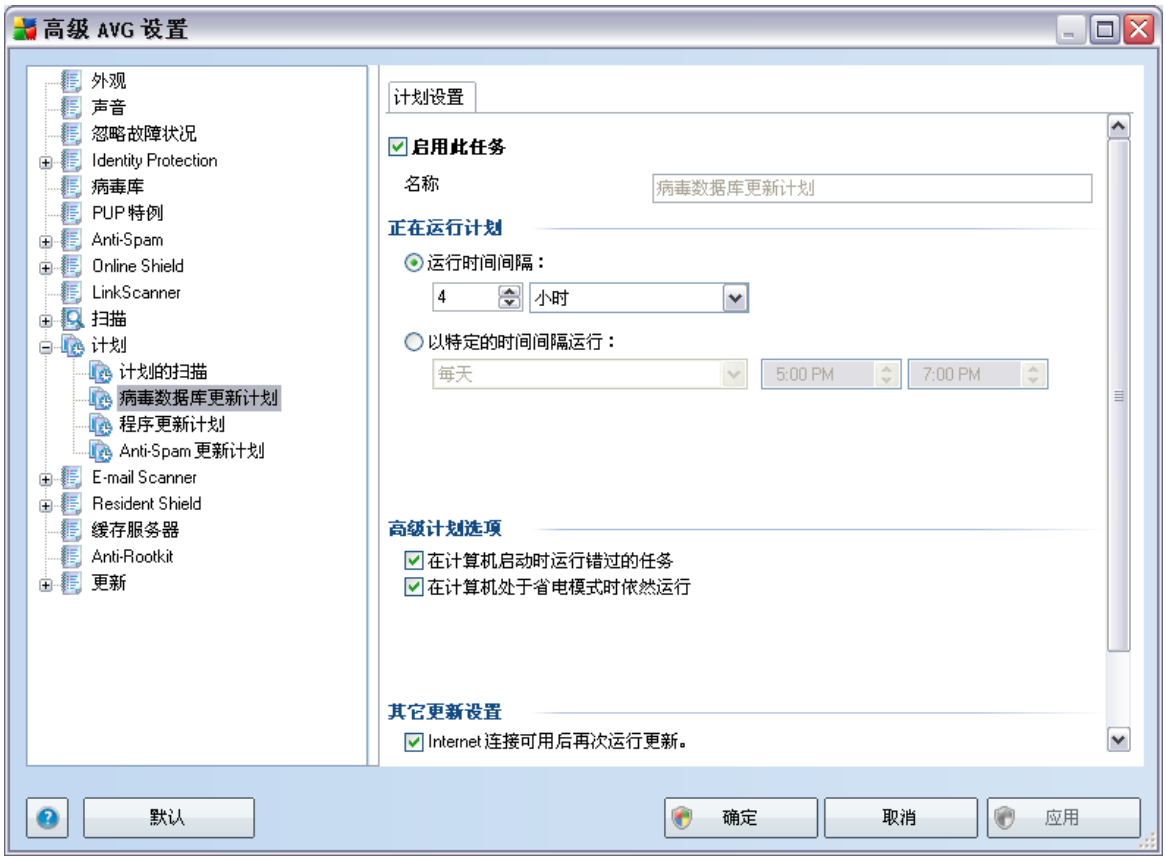


单击 ***"其它扫描设置..."*** 句打开新的 ***"计算机关闭选项"*** 对话框，在此可以决定当扫描进程运行结束后，是否应自动关闭计算机。在确认此选项（***"扫描完成时关闭计算机"***）后，将激活一个新选项（***"强制关闭锁定的计算机"***），通过该选项，即使目前已锁定计算机也可关机。



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

10.9.2. 病毒数据库更新计划



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病毒数据库更新，在实际需要时再启用它。***更新管理器*** 组件中包含了基本的病毒数据库更新计划功能。在此对话框中，您可以设置病毒数据库更新计划的某些详细参数。在名为 ***"名称"*** 的文本字段 *(已对所有默认计划停用此字段)* 中，有程序供应商对此计划指定的名称。

计划执行

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

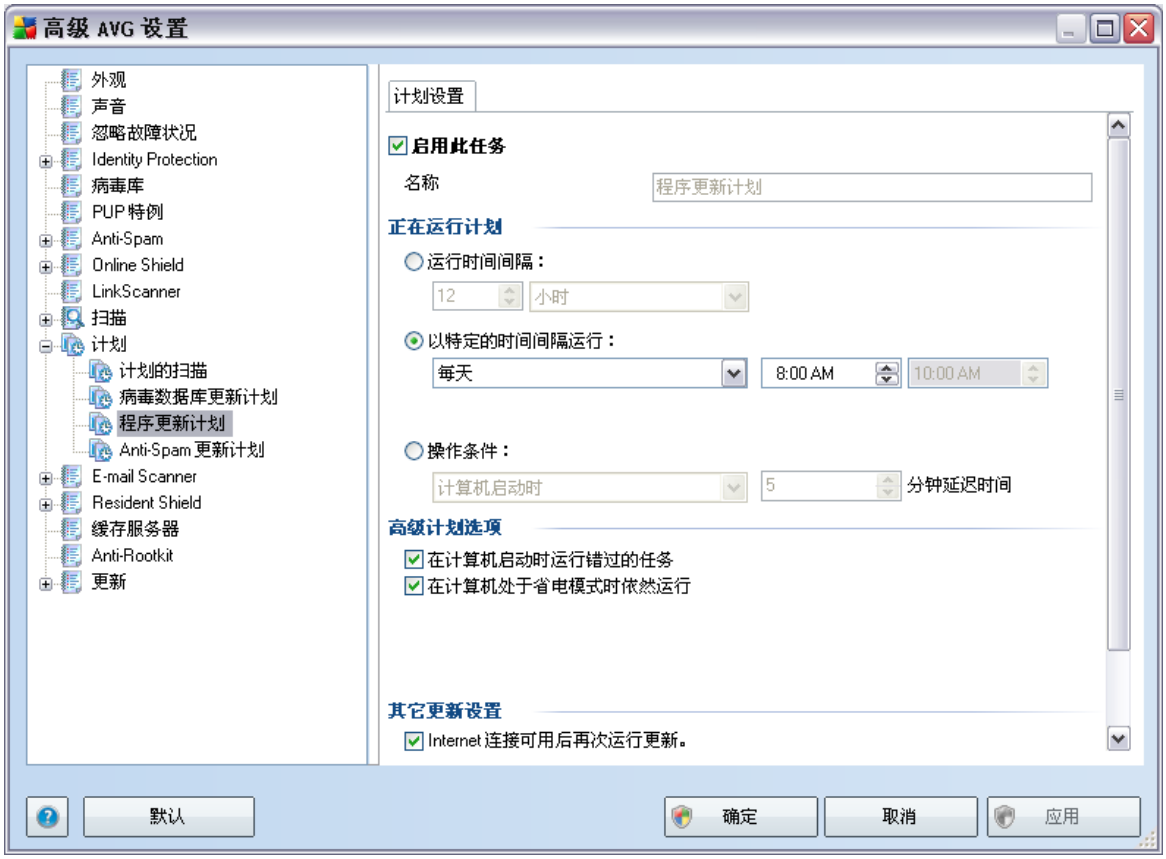
高级计划选项

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

其它更新设置

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

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



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程序更新，在实际需要时再启用它。在名为 ***"名称"*** 的文本字段 *（已对所有默认计划停用此字段）*中，有程序供应商对此计划指定的名称。

计划执行

请在此指定新计划的程序更新启动任务的时间间隔。此时间间隔的定义方式有三种：指定经过一段特定的时间后重复启动更新（***"每隔...运行一次"***），定义确切的日期和时间（***"在特定的时间运行..."***），也可以定义更新启动操作应关联的事件（***"计算机启动时的操作"***）。

高级计划选项

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

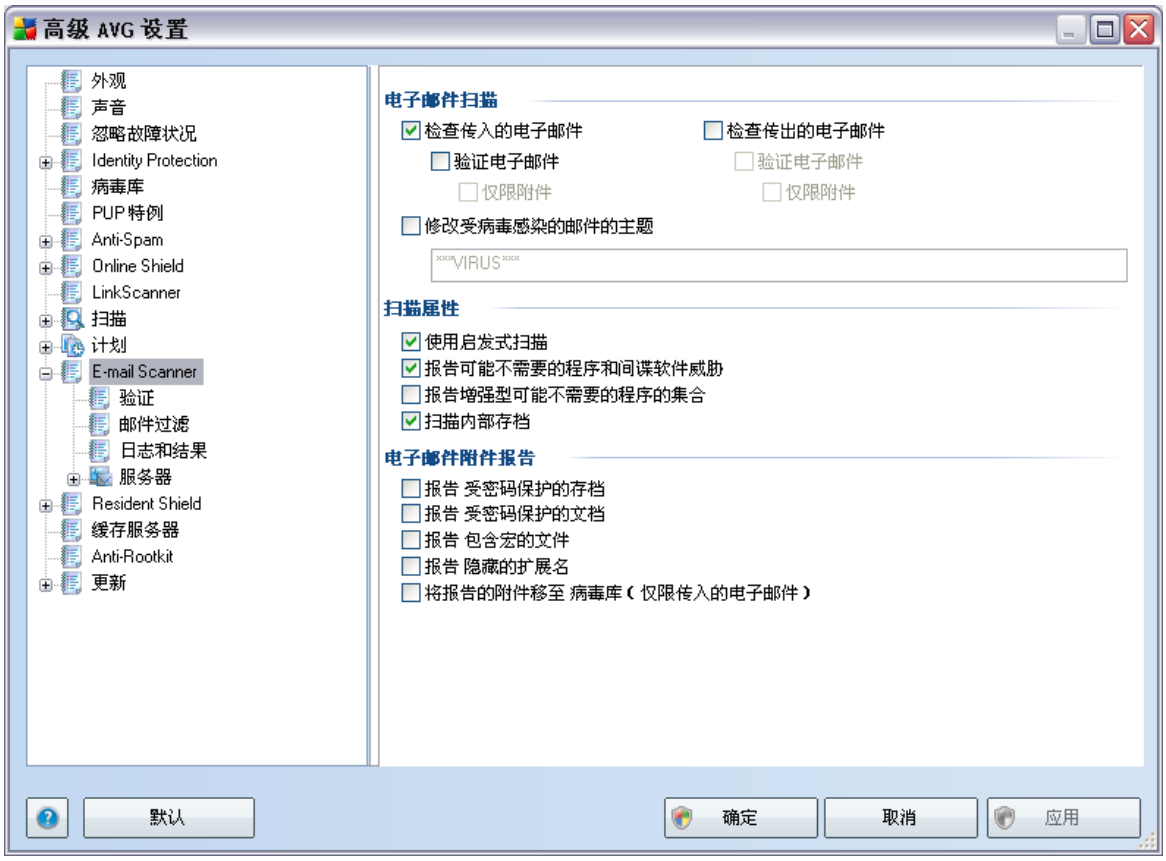
其它更新设置

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

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

注：*如果计划程序更新和计划扫描同时执行，则更新进程优先，扫描会中断。*

10.10. E-mail Scanner



*"E-mail Scanner"*对话框分为三个区域：

- ***电子邮件扫描*** - 可在此部分中对传入和/或传出的电子邮件作以下基本设置：
    - o 是否应当对电子邮件进行病毒扫描。
    - o 是否应向每封邮件的末尾添加验证文本，证明邮件不含病毒。可在验证对话框中调整验证文本。
    - o 是否只向带有附件的邮件添加验证文本。

若要修改受病毒感染的邮件的主题，请选中 ***'修改受病毒感染的邮件的主题'***框，并在文本字段中键入所需的值。该值随后将被添加到每封受感染的电子邮件的主题字段中，以便于识别和过滤。默认值为 :* * * VIRUS* * * 。建议保留此值。

- ***扫描属性*** - 可在此部分中指定电子邮件扫描方式：

  - ***使用启发式扫描*** - 选中此框可在扫描电子邮件时采用启发式检测方法。启用此选项时，不仅会按扩展名过滤电子邮件附件，还会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*）：选中此框可激活 ***Anti-Spyware*** 引擎，进行间谍软件和病毒扫描。间谍软件属于疑似恶意软件类软件：即使间谍软件通常是一种安全风险，也可故意安装其中的某些程序。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*** - 如果已激活上一选项，也可选中此框，以检测更多间谍软件：程序直接从制造商获得后极其安全而无害，但之后却能以不正当的方式使用以达到恶毒的目的。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。

  - ***“扫描内部存档”*** – 选中此框可扫描电子邮件所附存档的内容。

- ***电子邮件附件报告*** - 可在此部分设置有关潜在危险或可疑文件的其它报告。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：

  - ***“报告受密码保护的存档”*** – 受密码保护的存档（ZIP、RAR 等）不能进行病毒扫描；选中此框可将这类存档报告为有潜在危险。

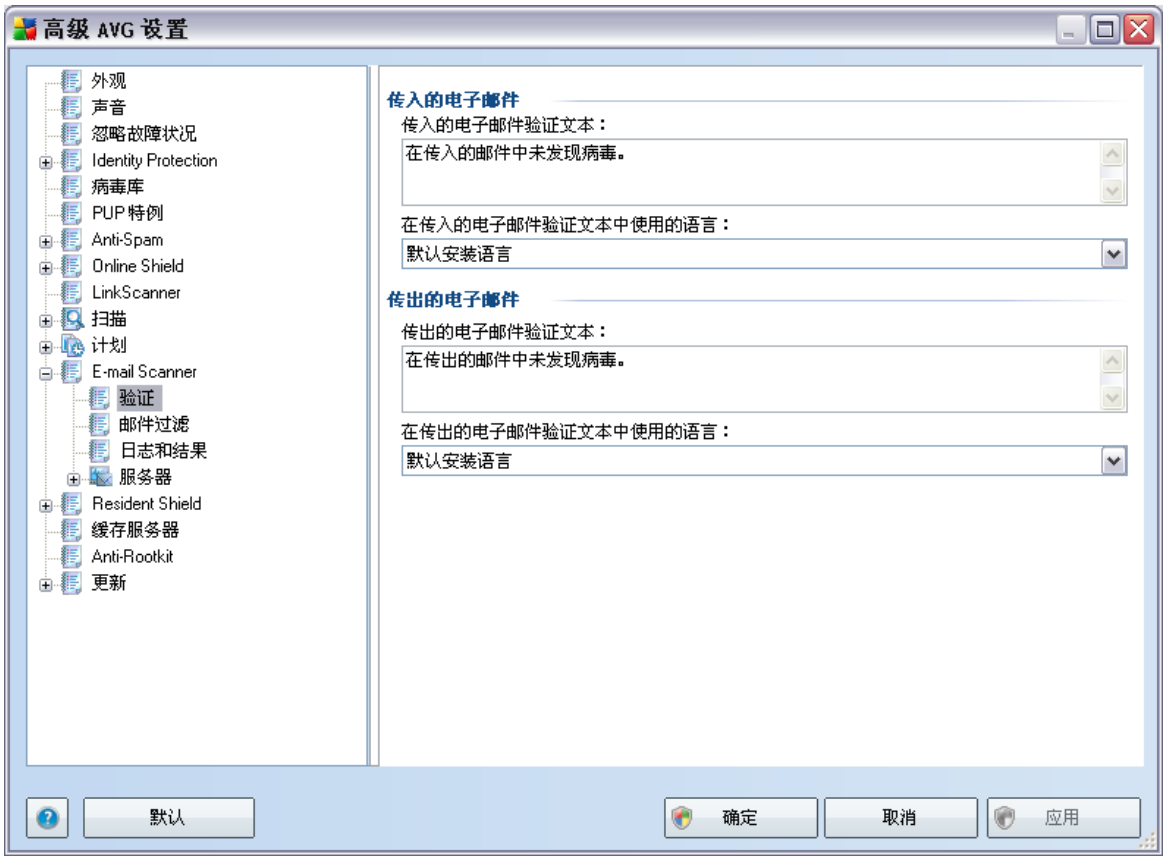
  - ***“报告受密码保护的文档”*** – 受密码保护的文档不能进行病毒扫描；选中此框可将这类文档报告为有潜在危险。

  - ***“报告包含宏的文件”*** – 宏是一个预定义的操作序列，旨在为用户简化某些任务的执行过程（MS Word 宏已为大家所熟悉）。因此，宏可能包含有潜在危险的指令，您可能需要选中此框，以确保将包含宏的文件报告为可疑。

  - ***“报告隐藏的扩展名”*** – 隐藏的扩展名能使可疑的可执行文件看起来像没有危险的纯文本文件（如“something.txt.exe”伪装成“something.txt”）；选中此框可将这类文件报告为有潜在危险。

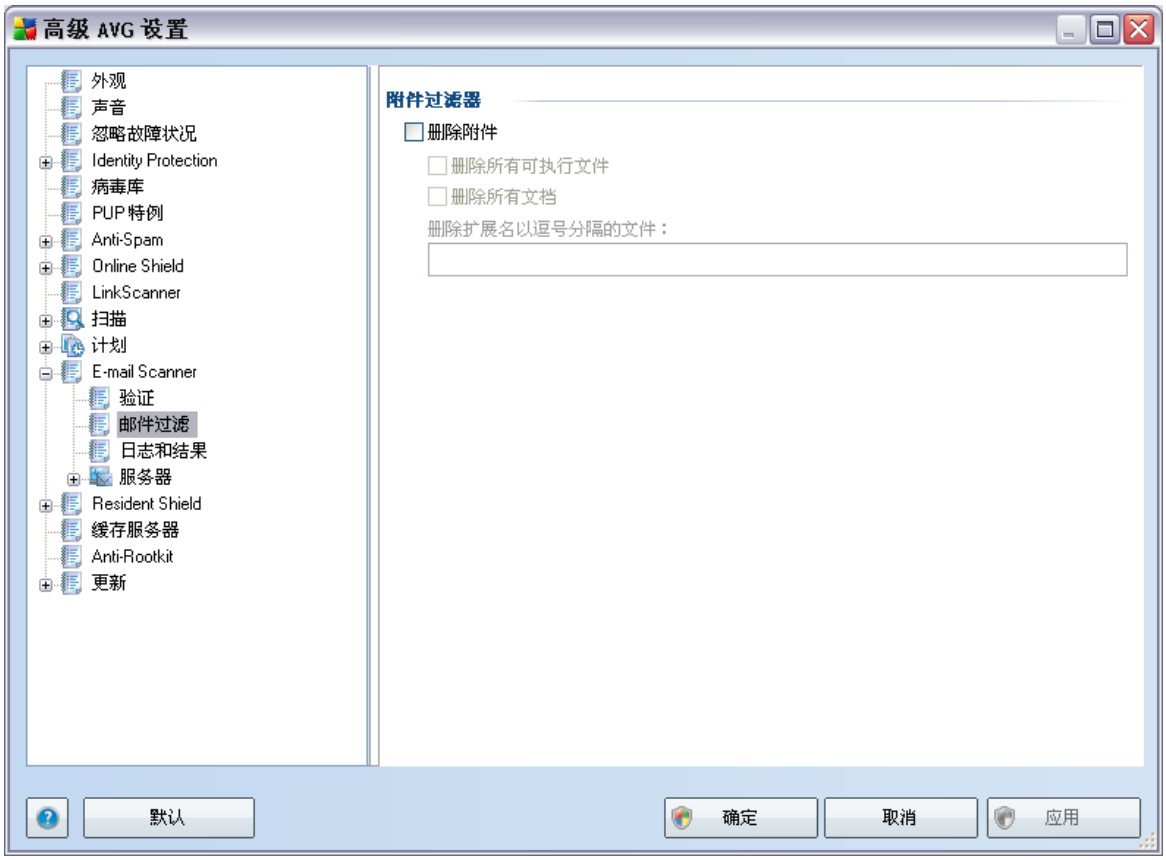
  - ***将报告的附件移至病毒库*** - 指定电子邮件经过扫描后发现其附件是受密码保护的存档、受密码保护的文档、含有文件的宏和/或隐藏了扩展名的文件时是否要通过电子邮件就相关情况发出通知。如果在扫描期间识别到此类邮件，请指定是否应将检测到的受感染对象移至***病毒库***。

10.10.1. 验证



在 ***"验证"*** 对话框中，您可以指定验证说明应包含的确切文本及所采用的语言。对于 ***传入的邮件*** 和 ***传出的邮件***，应分别指定这些内容。

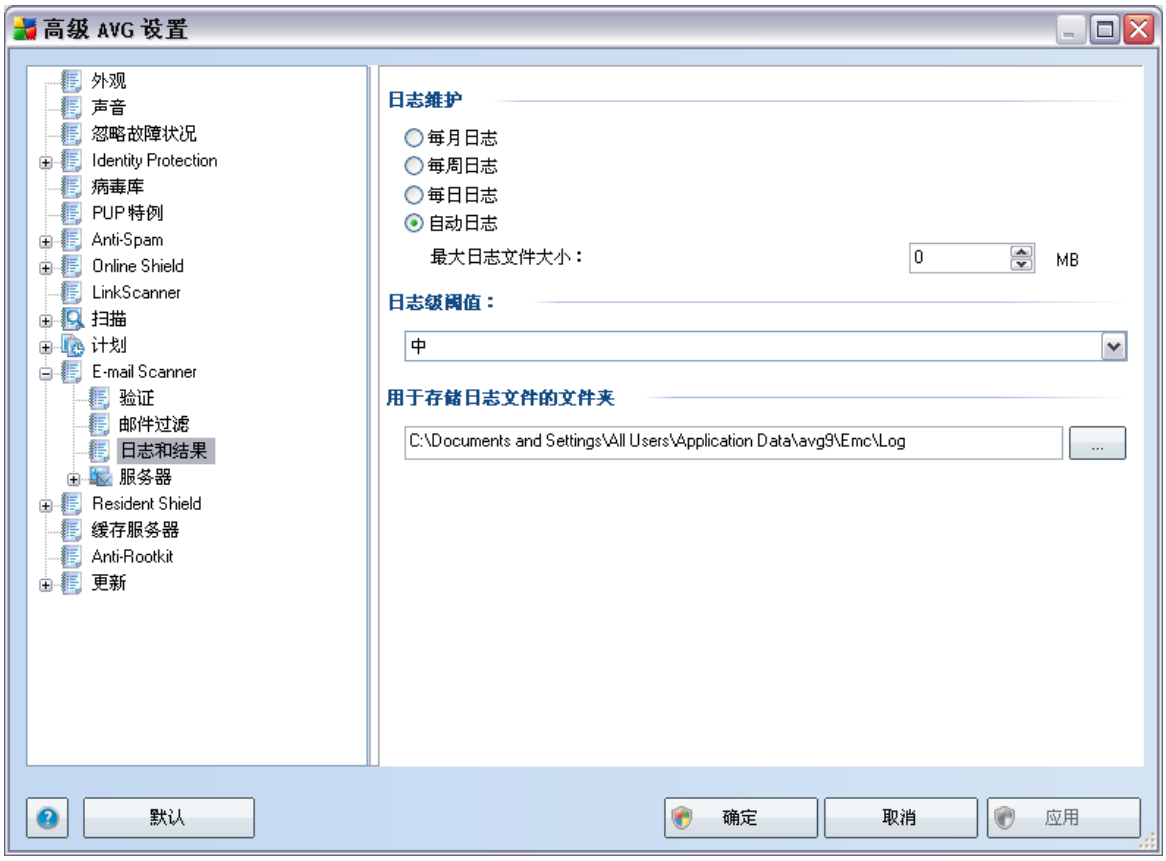
10.10.2. 邮件过滤



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

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

10.10.3. 日志和结果

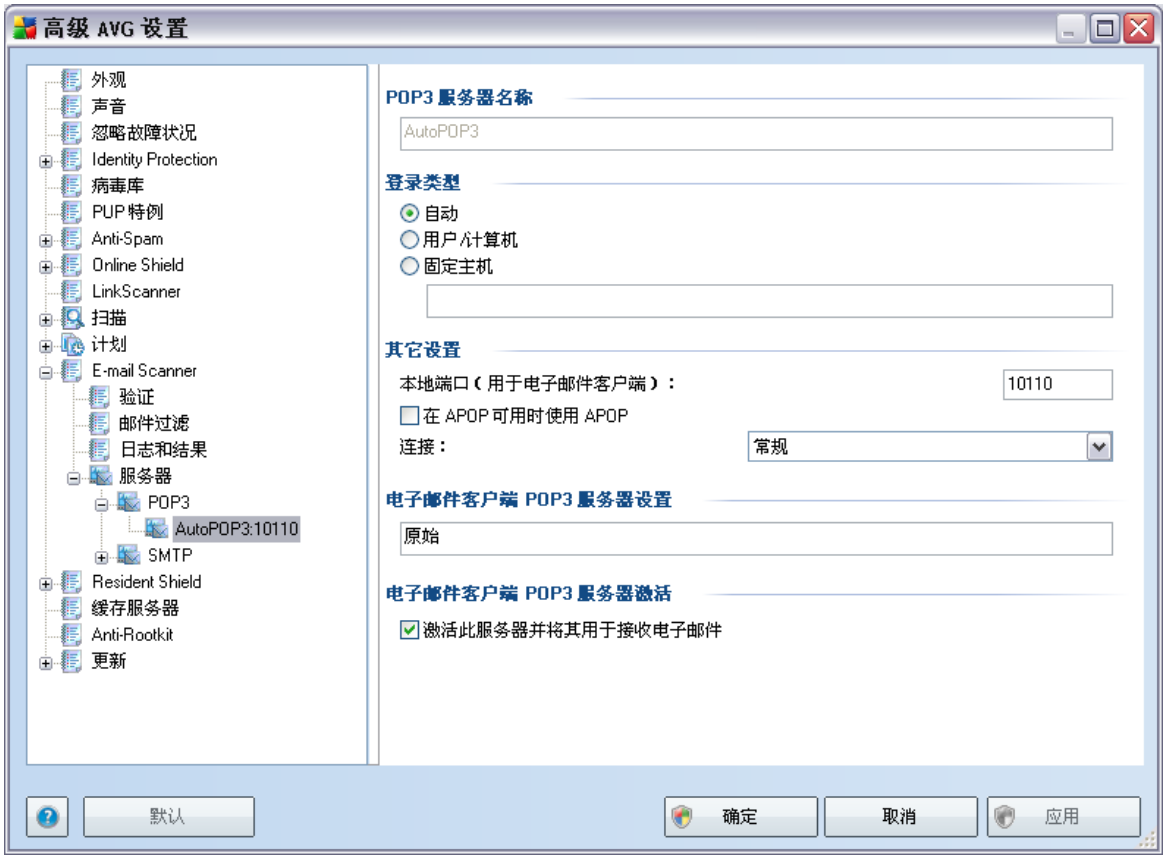


在通过 ***"日志和结果"*** 导航项打开的对话框中，您可以指定用于维护电子邮件扫描结果的参数。此对话框分为若干区域：

- ***"日志维护"*** – 用于定义您希望记录电子邮件扫描信息的频率（每天、每周、每月...），此外还可以通过此区域指定日志文件的最大大小（*以 MB 为单位*）
- ***"日志级别阈值"*** – 默认情况下设置为中级 – 您可以选择较低级别（*记录基本的连接信息*）或较高级别（*记录所有通信*）
- ***"用于存储日志文件的文件夹"*** – 定义应将日志文件存放于何处

10.10.4. 服务器

在 ***"服务器"*** 区域中，您可以编辑 ***E-mail Scanner*** 组件服务器的参数，或使用 ***"添加新服务器"*** 按钮设置新服务器。

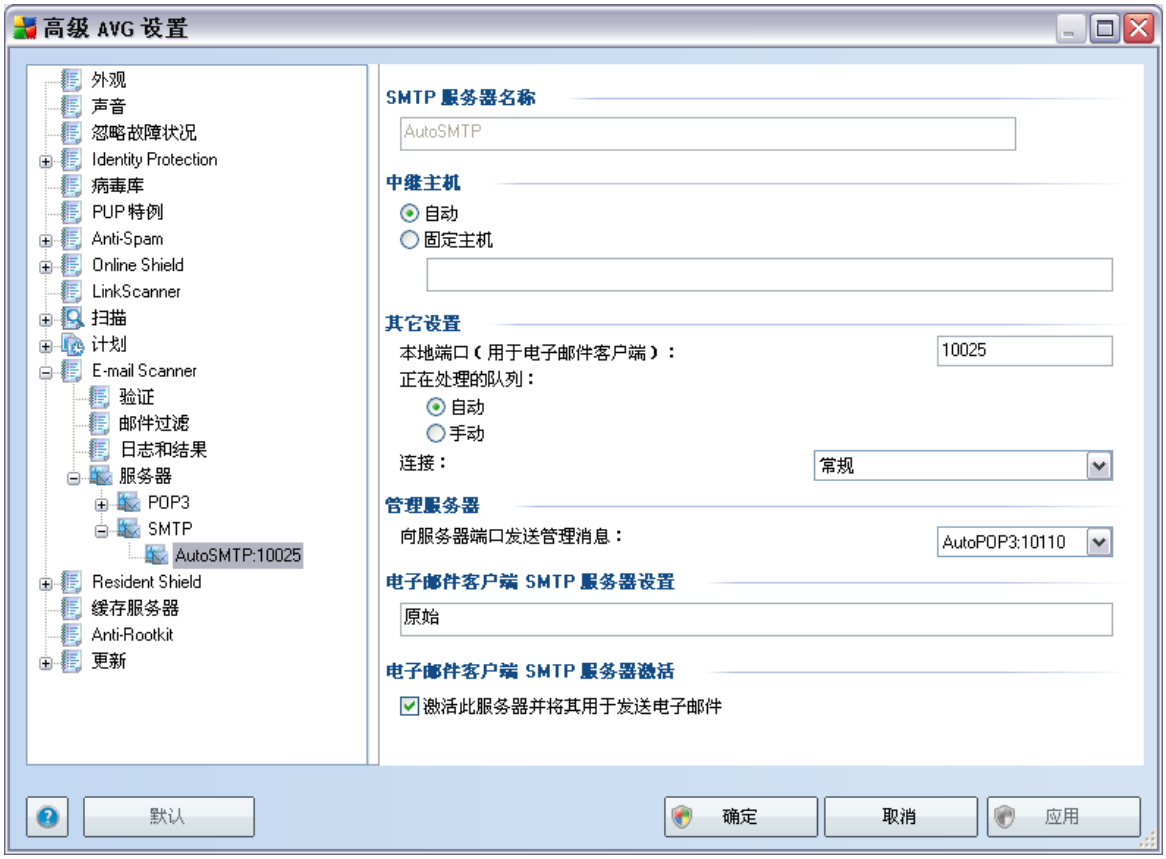


在此对话框 通过 ***"服务器"*** / ***"POP3"*** 打开）中，您可以设置使用 POP3 协议接收邮件的新 ***E-mail Scanner*** 服务器：

- ***"POP3 服务器名称"*** – 请键入相应服务器的名称或保留默认名称 AutoPOP3
- ***"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。
  - ***"用户/计算机"*** – 确定目标邮件服务器的最简单且最常用的方法就是代理方法。若要使用此方法，请在指定给定邮件服务器的登录用户名时将代理名称或地址也包含在内（或者将端口也包含在内），并用 *"/"* 字符将其与用户名隔开。例如，对于通过服务器 pop.acme.com 和端口 8200 登录的 user1 帐户，可使用 user1/pop.acme.com:8200 作为登录名。
  - ***"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）。用于 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。
  - ***"在 APOP 可用时使用 APOP"***– 此选项可实现更为安全的邮件服务器登录。这样可确保 ***E-mail Scanner*** 使用一种替代方法来转发用户帐户的登录密码，从而借助从服务器收到的可变链，不以公开方式而是以加密格式将该密码发送到服务器。当然，只有在目标邮件服务器支持此功能时，此功能才可用。
  - ***"连接"***– 在此下拉菜单中，您可以指定要使用何种连接（常规/SSL/SSL 默认）。如果选择 SSL 连接，则数据以加密方式发送，因而没有被第三方跟踪或监视的风险。此功能也是只有在目标邮件服务器支持它时才可用。
- ***"电子邮件客户端 POP3 服务器设置"***– 简要说明了正确配置您的电子邮件客户端（以使 ***E-mail Scanner*** 检查所有传入邮件）所需的配置设置。这是根据在此对话框及其它相关对话框中指定的对应参数概括出来的摘要。
- ***"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 ***E-mail Scanner*** 服务器：

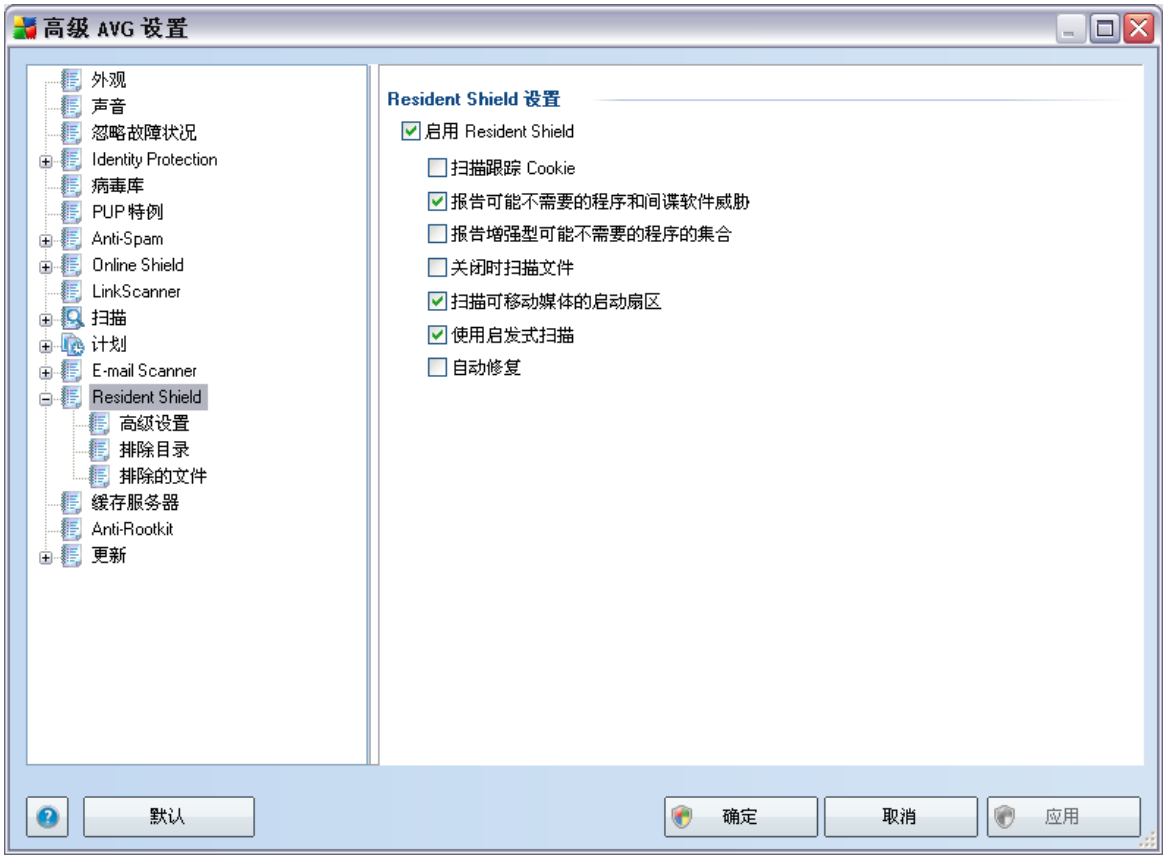
- ***"SMTP 服务器名称 "***– 请键入相应服务器的名称或保留默认名称 AutoSMTP
- ***"中继主机 "***– 定义应采用何种方法来决定用于传出邮件的邮件服务器：
  - ***"自动 "***– 将自动根据您的电子邮件客户端设置进行登录
  - ***"固定主机 "***– 这种情况下，程序将始终使用此处指定的服务器。请指定邮件服务器的地址或名称。可以使用域名 例如，smtp.acme.com）以及 IP 地址 例如，123.45.67.89）来表示名称。如果此邮件服务器使用非标准端口，则您可以在服务器名称后面键入此端口，二者之间用冒号隔开 例如，smtp.acme.com:8200）。用于 SMTP 通信的标准端口为 25。
- ***"其它设置 "***– 用于指定更为详细的参数：

- ***"本地端口"*** – 指定应在哪个端口允许来自邮件应用程序的通信。然后必须在对应的邮件应用程序中指定此端口作为用于 SMTP 通信的端口。
- ***"队列处理"*** – 决定 ***E-mail Scanner*** 在处理邮件发送请求时的行为：
  - "自动" – 立即将传出的邮件送达（发送到）目标邮件服务器
  - "手动" – 将邮件插入到传出邮件队列中，稍后再发送
- ***"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。

- ***"管理服务器"*** – 显示了将用于回传管理报告的服务器端口号。在目标邮件服务器拒绝所传出的邮件或该邮件服务器不可用等情况下，会生成这种回传邮件。
- ***"电子邮件客户端 SMTP 服务器设置"*** – 提供了一些信息，用以说明如何配置客户端邮件应用程序，以便使用在当前修改后用来检查传出邮件的服务器来检查传出邮件。这是根据在此对话框及其它相关对话框中指定的对应参数概括出来的摘要。
- ***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

10.11. Resident Shield

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



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

- ***"扫描跟踪 Cookie"***–此参数用于定义在扫描期间应对 Cookie 进行检测。*(HTTP Cookie 用于验证、跟踪和维护有关用户的特定信息，例如网站首选项或电子购物车中的内容)*
- ***报告可能不需要的程序和间谍软件威胁*** -*(默认情况下已启用)*:选中此框可激活 ***Anti-Spyware*** 引擎，进行间谍软件和病毒扫描。间谍软件属于疑似恶意软件类软件:即使间谍软件通常是一种安全风险，也可故意安装其中的某些程序。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*** - 如果已激活上一选项，也可选中此框，以检测更多间谍软件 :程序直接从制造商获得后极其安全而无害，但之后却能以不正当的方式使用以达到恶毒的目的。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"*** – 关闭时执行的扫描可确保 AVG 在活动的对象（如应用程序、文档等）被打开和关闭时对它们进行扫描 ;此功能可帮助您保护您的计算机免遭某些类型的复杂病毒侵害

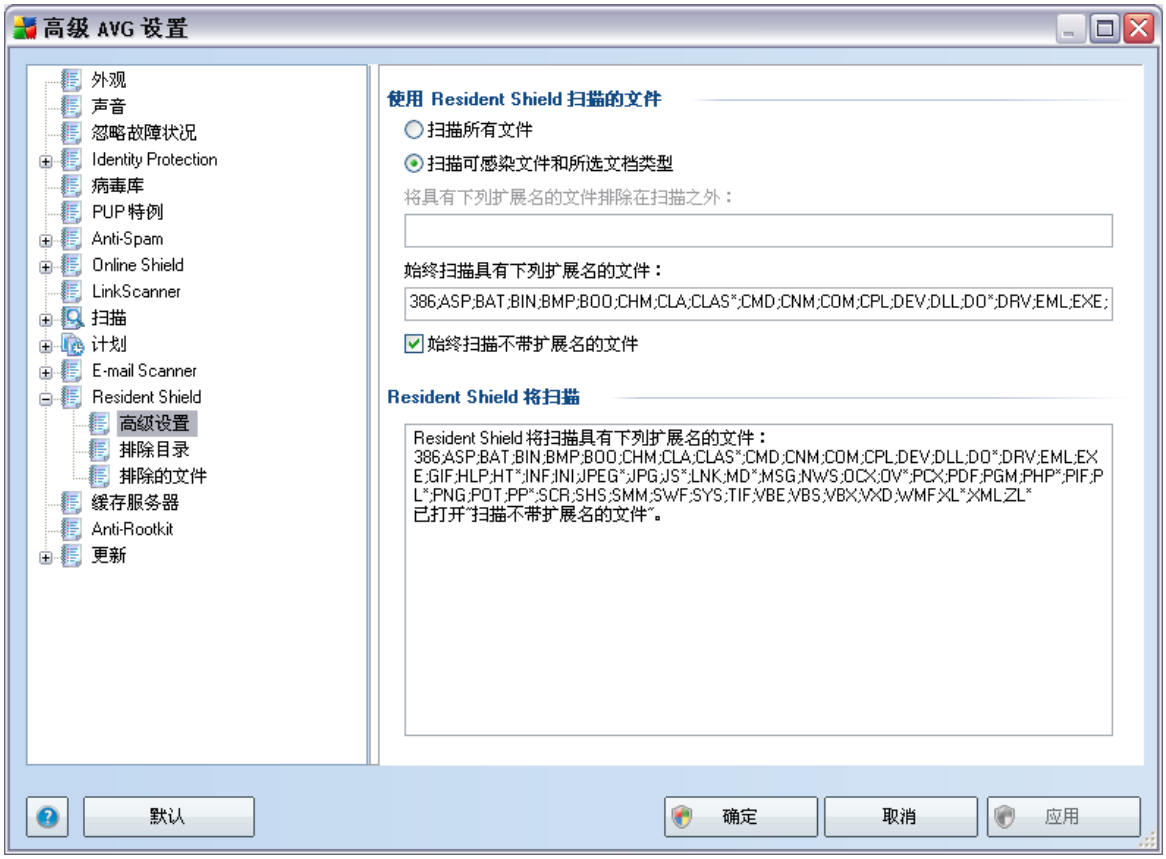
- ***"扫描可移动介质的启动扇区"*** –（*默认情况下已启用*）

- ***"使用启发式扫描"*** –（*默认情况下已启用*）将使用启发式分析方法进行检测（*在虚拟的计算机环境中对已扫描对象的指令进行动态模拟*）

- ***"自动修复"*** – 对于检测到的任何感染，如果存在修复方案，则会自动对其进行修复

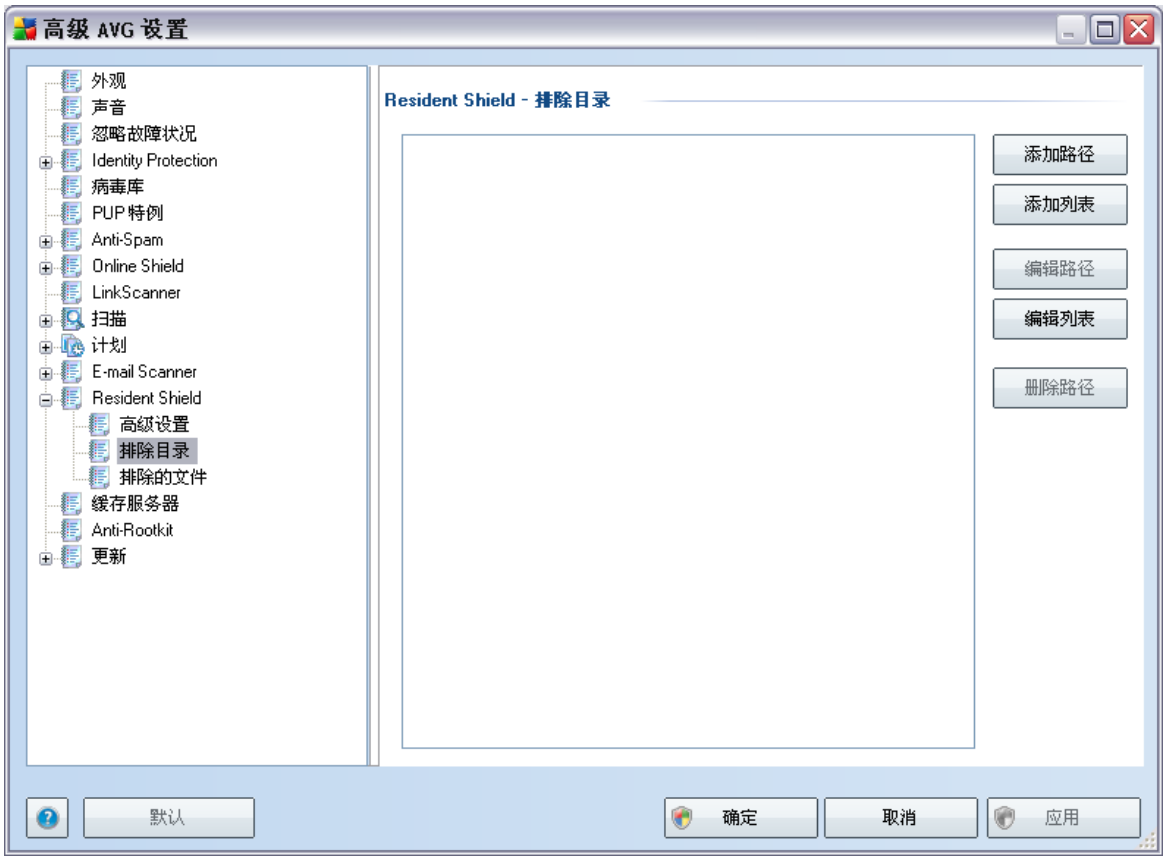
10.11.1. 高级设置

在 ***"常驻保护盾扫描的文件"***对话框中，可以配置所要扫描的文件（*通过特定扩展名*）：



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

10.11.2. 排除目录



*"Resident Shield –排除目录"*对话框可用于定义应排除在 ***Resident Shield*** 扫描范围之外的文件夹。

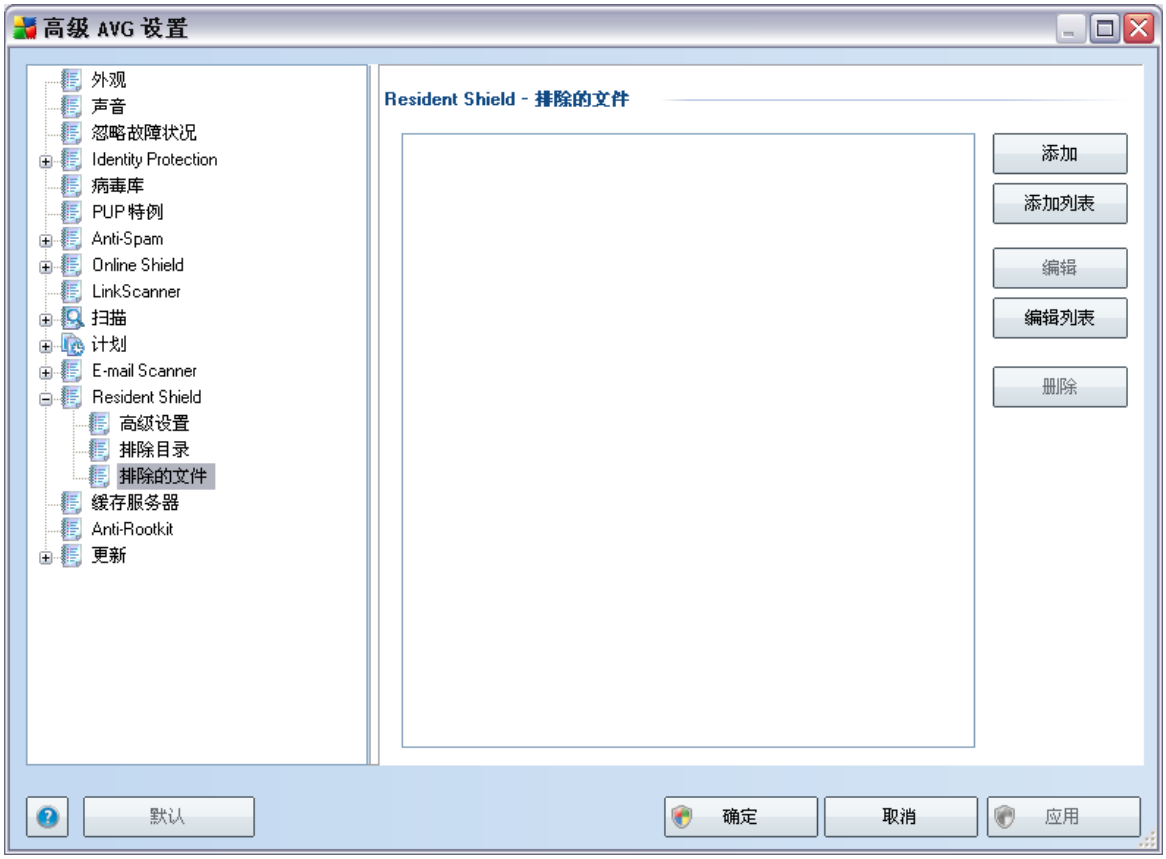
若非必要，否则我们强烈建议不要排除任何目录！

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
- ***"添加列表"***– 用于输入要排除在 ***Resident Shield*** 扫描范围之外的整个目录列表
- ***"编辑路径"***– 用于编辑选定文件夹的指定路径
- ***"编辑列表"***– 用于编辑文件夹列表

- ***"删除路径"***– 用于从列表中删除选定文件夹的路径

10.11.3. 排除的文件



"Resident Shield –排除的文件"对话框在行为方面与前述***"Resident Shield –排除目录"***相似，只不过在此对话框中要排除的不是文件夹，您可以定义应排除在***Resident Shield***扫描范围之外的特定文件。

我们强烈建议，若非必要，不要排除任何文件！

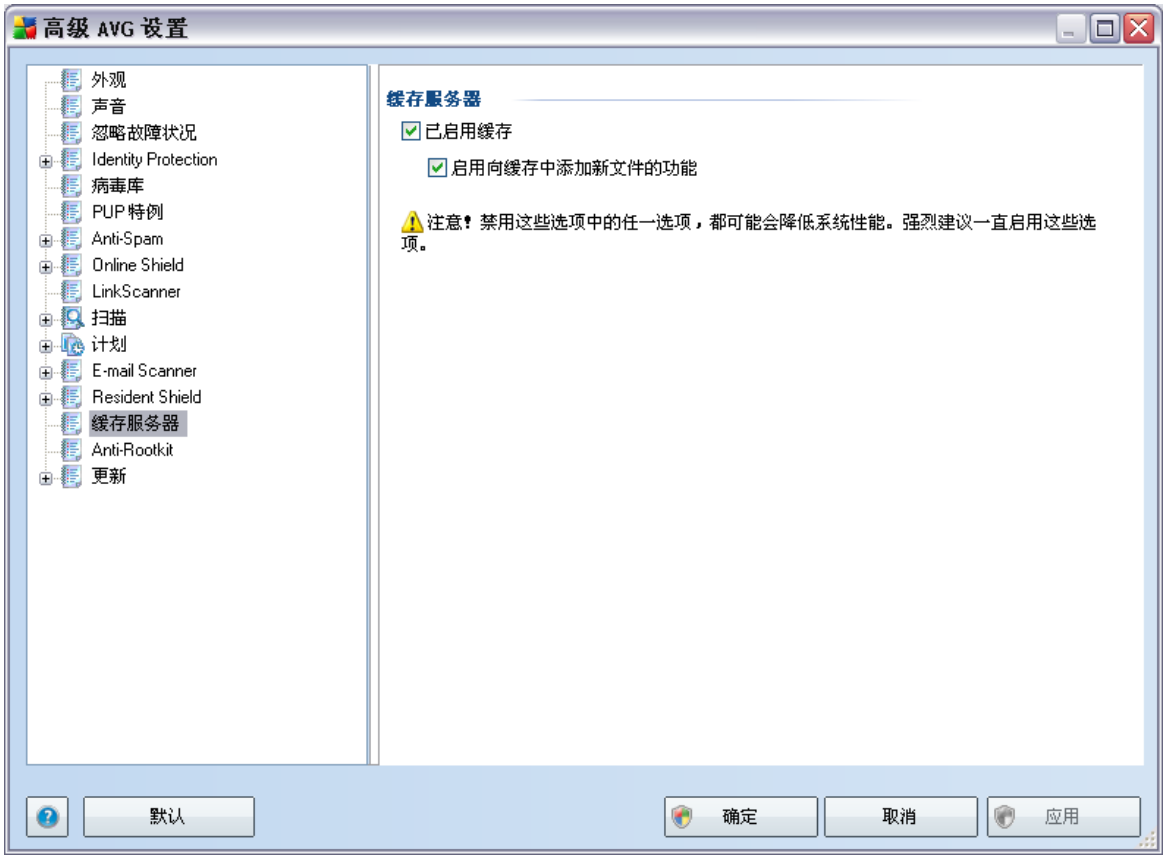
此对话框提供了以下控制按钮：

- ***"添加"***– 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
- ***"添加列表"***– 用于输入要排除在***Resident Shield***扫描范围之外的整个文件列表

- ***"编辑"***– 用于编辑选定文件的指定路径
- ***"编辑列表"***– 用于编辑文件列表
- ***"删除"***– 用于从列表中删除选定文件的路径

10.12. 缓存服务器

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



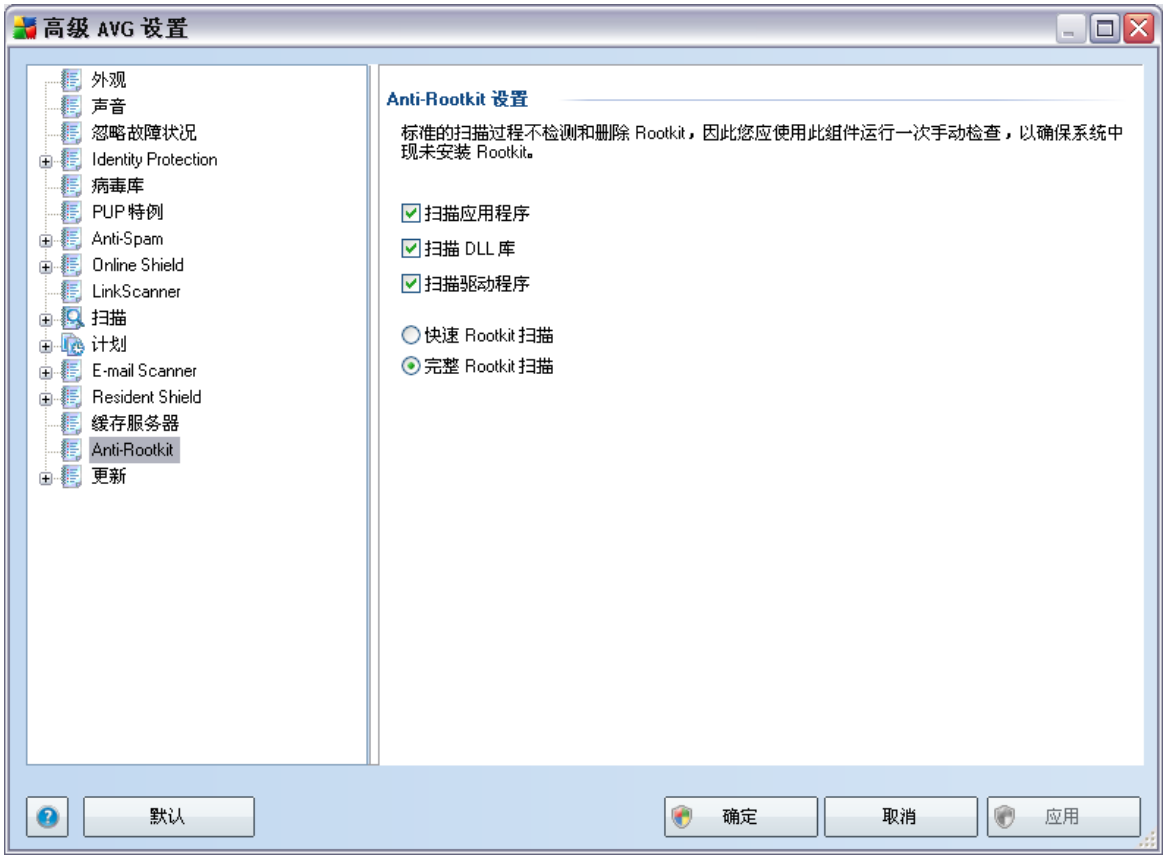
设置对话框中有两个选项：

- ***已启用缓存***(*默认情况下已启用*)- 取消选中该框可禁用***缓存服务器***，清空缓存。请注意，扫描速度可能会减慢，计算机的总体性能会降低，因为会先对每个正在使用的文件进行病毒和间谍软件扫描。

- ***启用向缓存中添加新文件的功能***(*默认情况下已启用*)- 取消选中该框可停止向缓存中添加更多文件。会保留并使用所有已存入缓存的文件，直到彻底禁用缓存功能为止，或直到下次更新病毒数据库为止。

10.13. Anti-Rootkit

在此对话框中，可以编辑 ***Anti-Rootkit*** 组件的配置：



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

选中相应的复选框可指定应扫描的对象：

- ***扫描应用程序***
- ***扫描 DLL 库***

- ***扫描驱动程序***

此外，还可以选择 Rootkit 扫描模式：

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

10.14. 更新

"更新"导航选项用于打开一个新对话框，从中可指定与 AVG 更新有关的常规参数：

文件更新时间

在此区域中您可以在以下两个备选选项中进行选择：可以计划在 PC 下次重新启动时进行更新，也可以立即启动更新。默认情况下选择的是立即启动选项，因为这样 AVG 可确保实现最佳的安全级别。只有在您确定计算机会以至少每天一次的频率定期重新启动时，才建议计划在 PC 下次重新启动时进行更新。

如果您决定保留默认配置并立即启动更新过程，则您可以指定在哪些情况下应执行可能需要的重新启动操作：

- ***"需要用户确认"***– 对于是否重新启动 PC，需征得您同意，重新启动后才能完成更新过程
- ***"立即重新启动"***– 更新过程结束后计算机将立即自动重新启动，不需要事先征得您同意
- ***"在下次计算机重新启动时完成"***– 更新过程将推迟到下次计算机重新启动时完成 –再次说明，请谨记只有在您确定计算机会以至少每天一次的频率定期重新启动时，才建议使用此选项

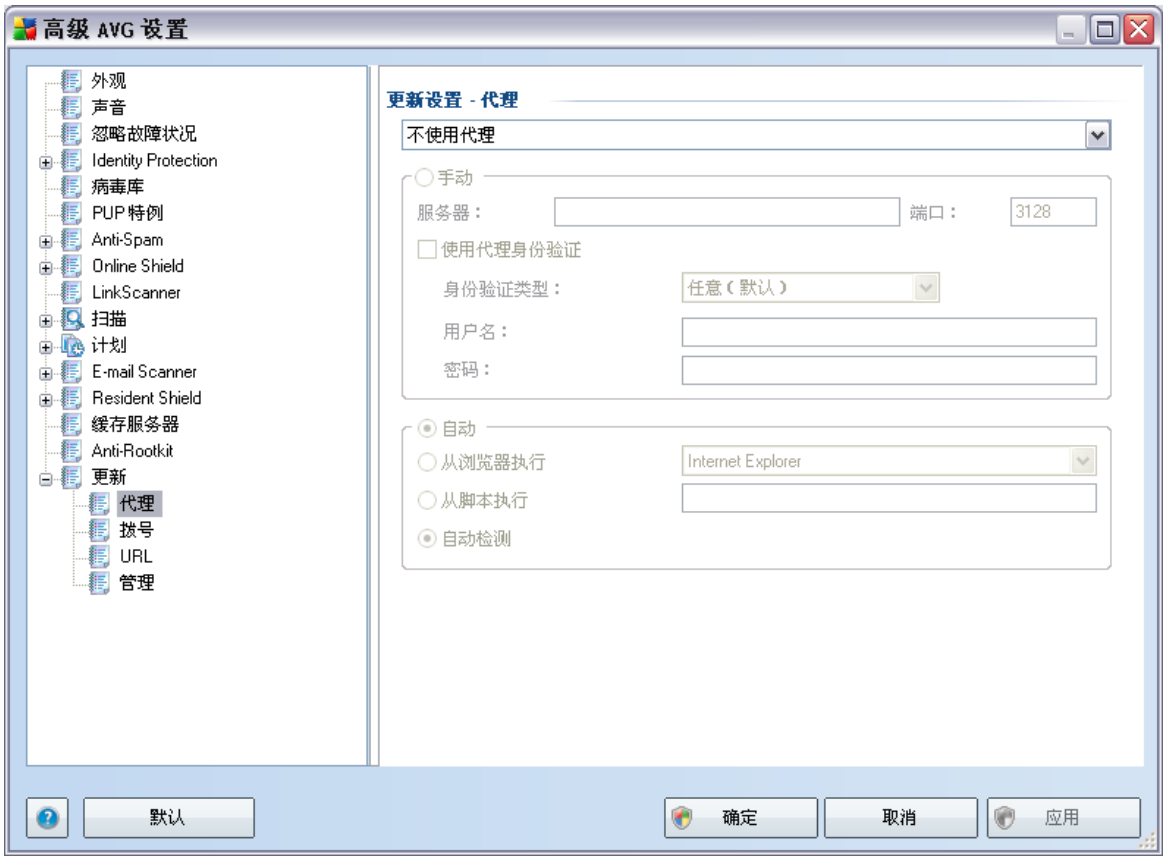
更新后进行内存扫描

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

- ***"在每次更新程序后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"***– 选中此复选框可确认，您要使用无需在更新服务器与 AVG 客户端之间传输数据的更新文件检测方法；
- ***"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。

10.14.1. 代理



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

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

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

手动配置

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

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

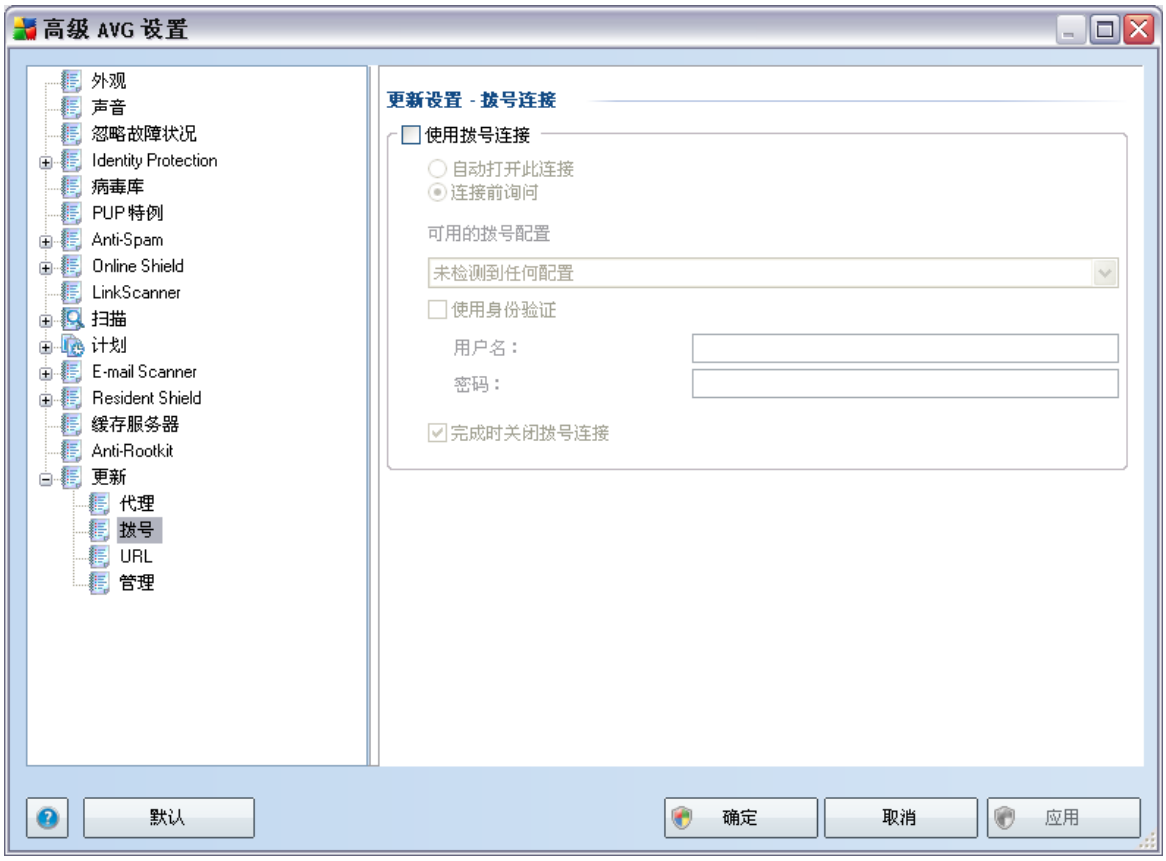
代理服务器也可以针对每个用户配置特定的规则。如果您的代理服务器是这样设置的，请选中 ***"使用代理身份验证"***选项以验证您的用户名和密码是否有效，即能否通过代理服务器连接到 Internet。

自动配置

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

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

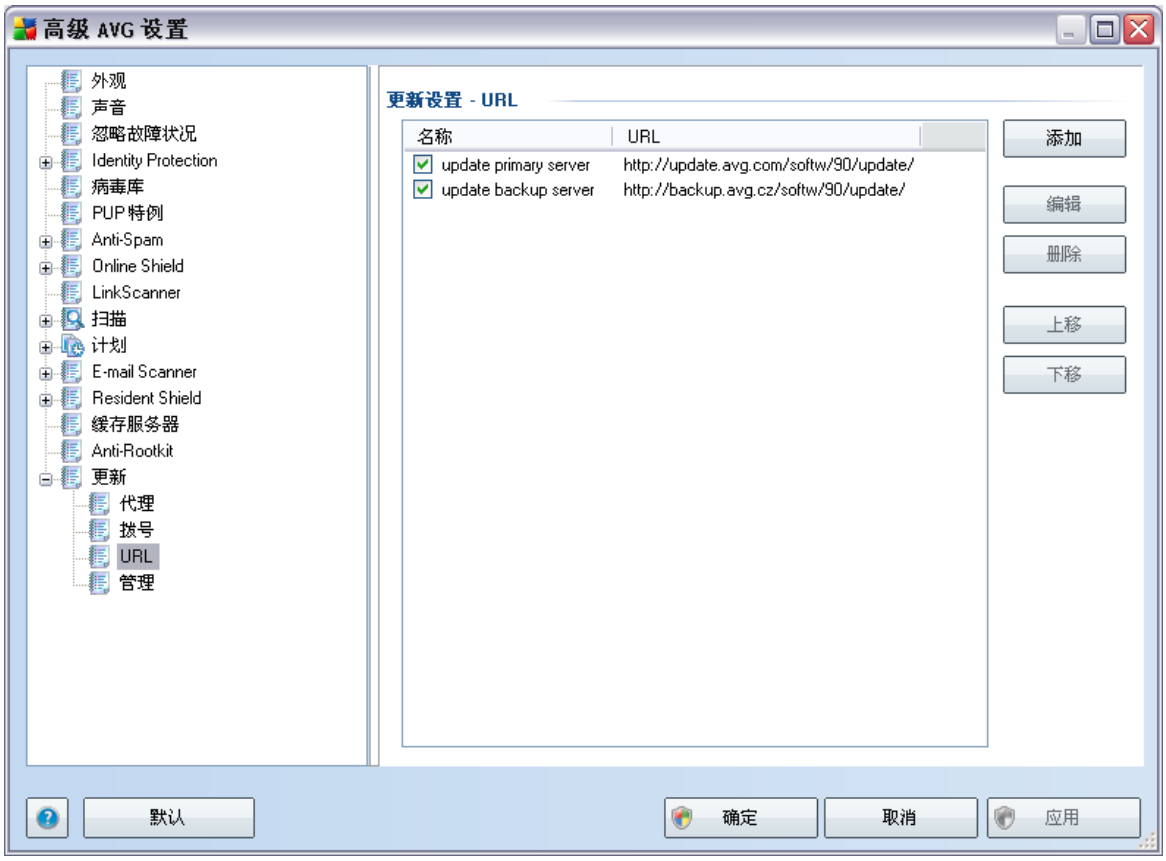
10.14.2. 拨号



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

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

10.14.3. URL

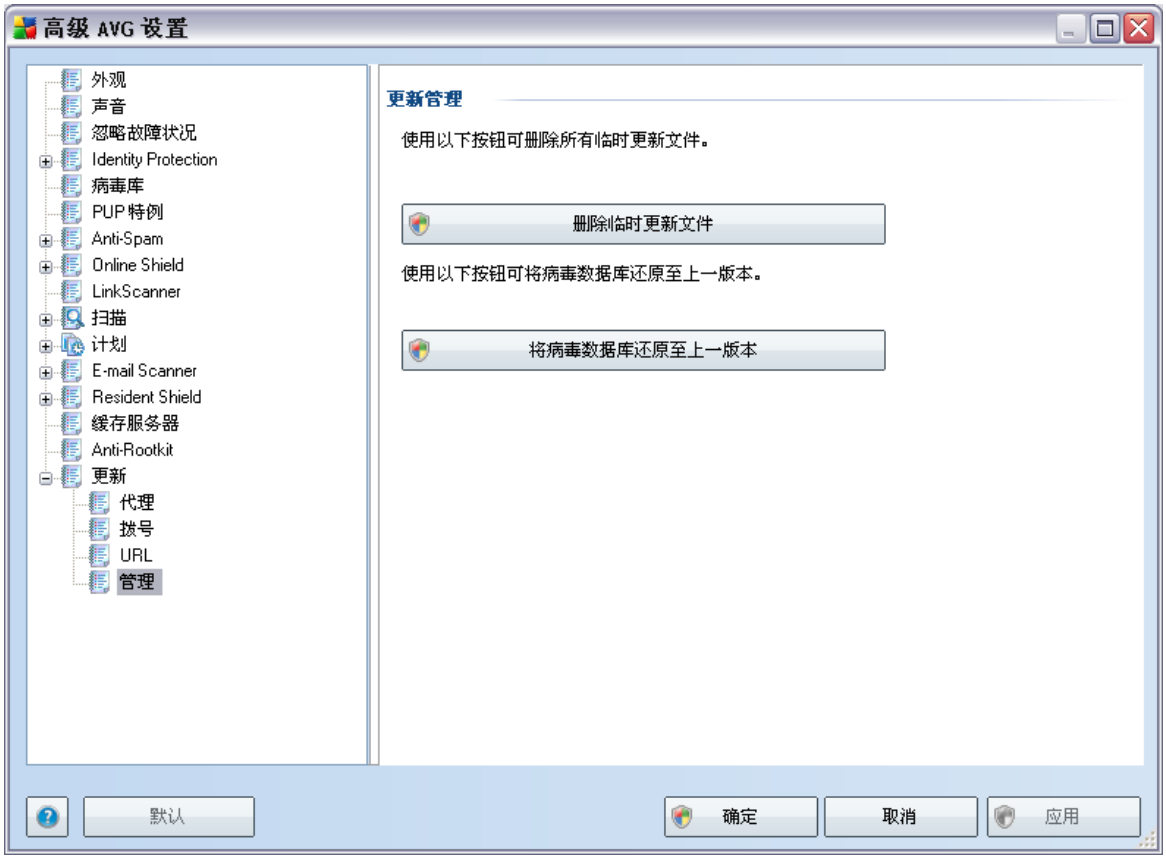


"URL"对话框提供了可从中下载更新文件的 Internet 地址列表。可以使用以下控制按钮修改此列表及其中的各项：

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

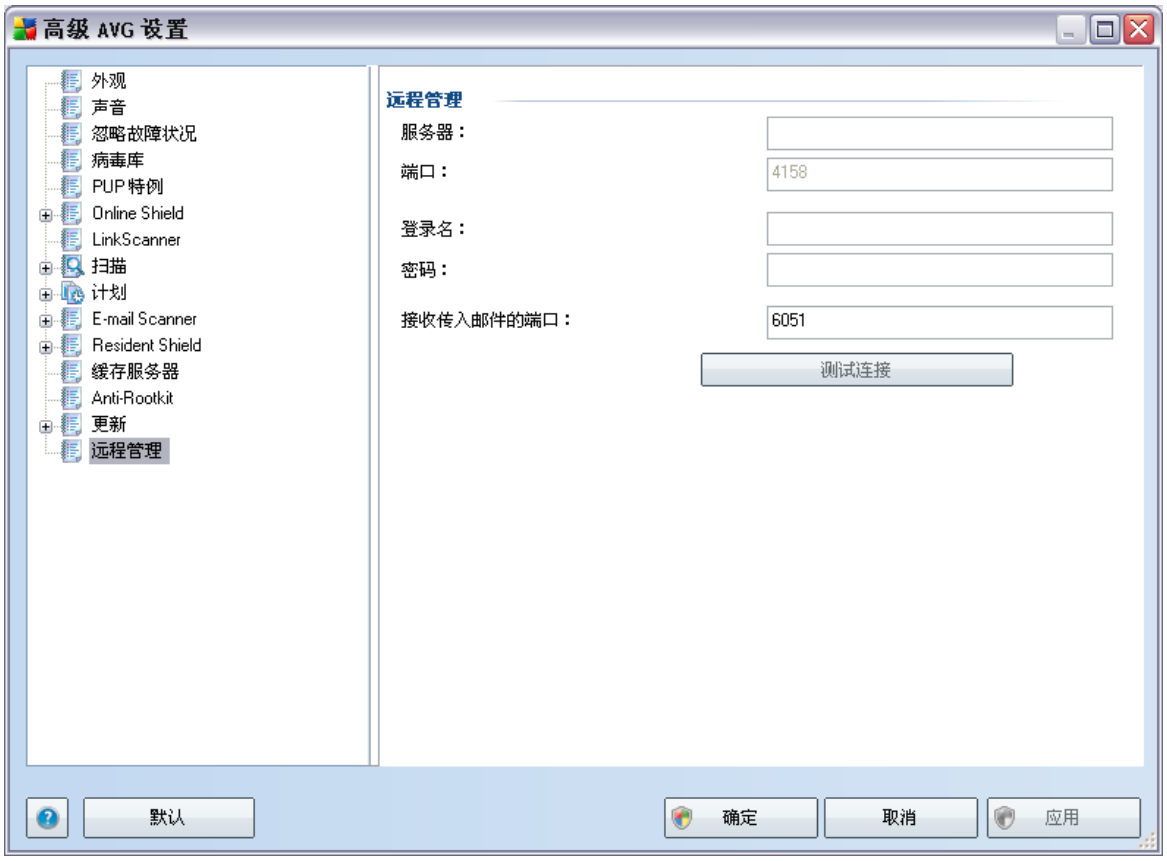
10.14.4. 管理

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



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

10.15. 远程管理



远程管理设置涉及将 AVG 客户端站连接到远程管理系统。如果您打算将相应的站连接到远程管理系统，请指定以下参数：

- ***"服务器"***– 安装 AVG Admin Server 的服务器的名称 或服务器的 IP 地址）
- ***"端口"***– 请提供 AVG 客户端用来与 AVG Admin Server 进行通信的端口号（*端口号 4158 被视为默认端口 –如果您使用此端口号，则无需明确指定*）
- ***"登录名"***– 如果 AVG 客户端与 AVG Admin Server 之间的通信被定义为保密通信，请提供您的用户名 ...
- ***"密码"***– ... 及您的密码
- ***"接收传入消息的端口"***– AVG 客户端用来从 AVG Admin Server 接收传入消息的端口号

*"测试连接"*按钮可帮助您验证所有上述数据是否有效以及能否用来成功连接到 DataCenter。

***注：**有关远程管理的详细说明，请参阅 AVG Network Edition 文档。*

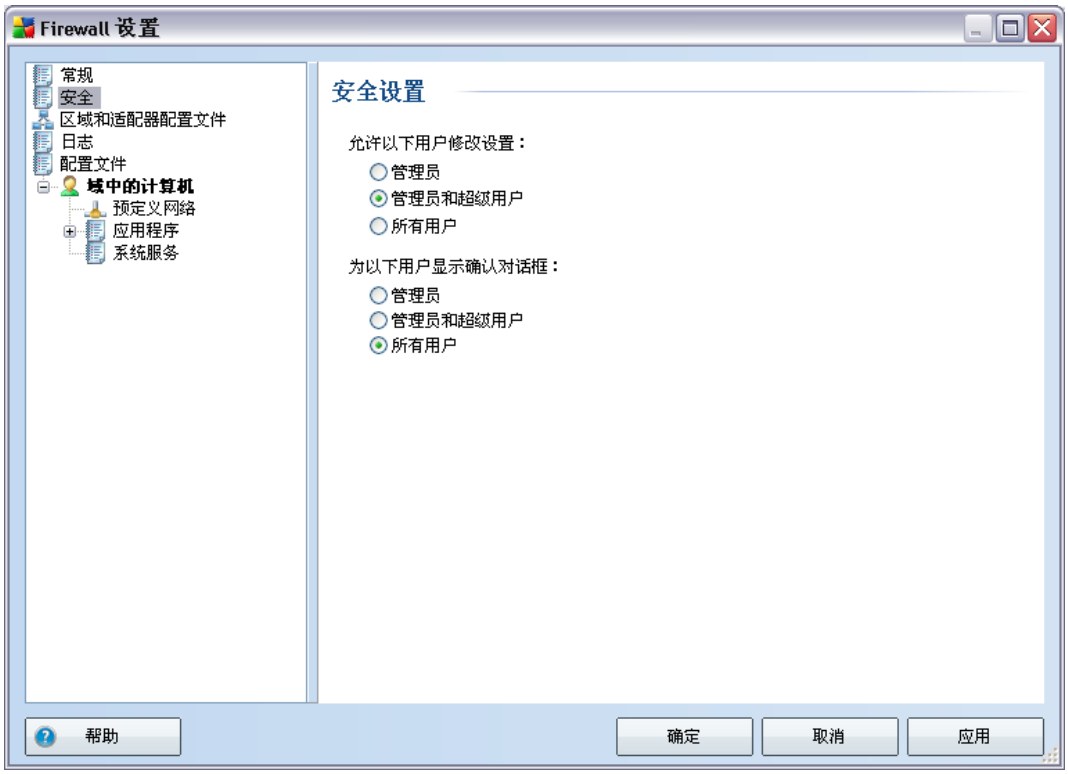
11. Firewall 设置

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。***不过，高级配置只能由专家及经验丰富的用户进行编辑。***

11.1. 常规

可在 ***"常规信息"*** 中 ***导出/导入*** ***Firewall*** 配置；也就是将已定义的 ***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



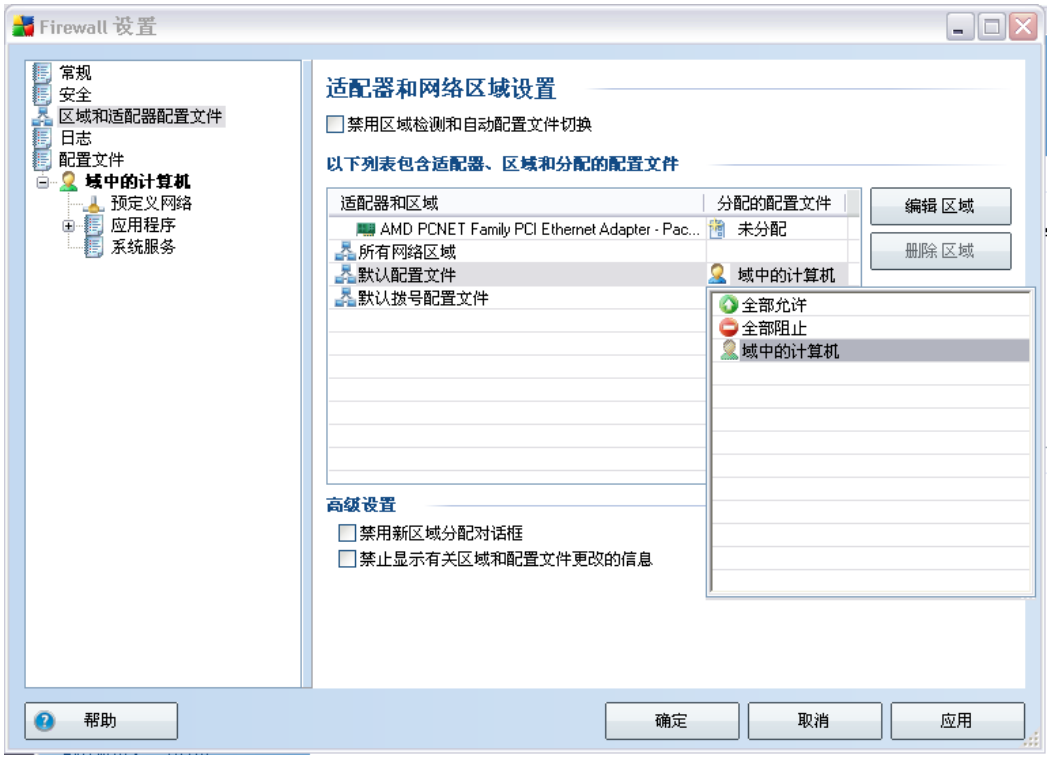
在 ***"安全设置"***对话框中，您可以定义 ***Firewall*** 行为的通用规则（不管选定的配置文件如何，这些规则都适用）：

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

在这两种情况下，您都可以将相应的特定权限分配给以下用户组之一：

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

11.3. 区域和适配器配置文件



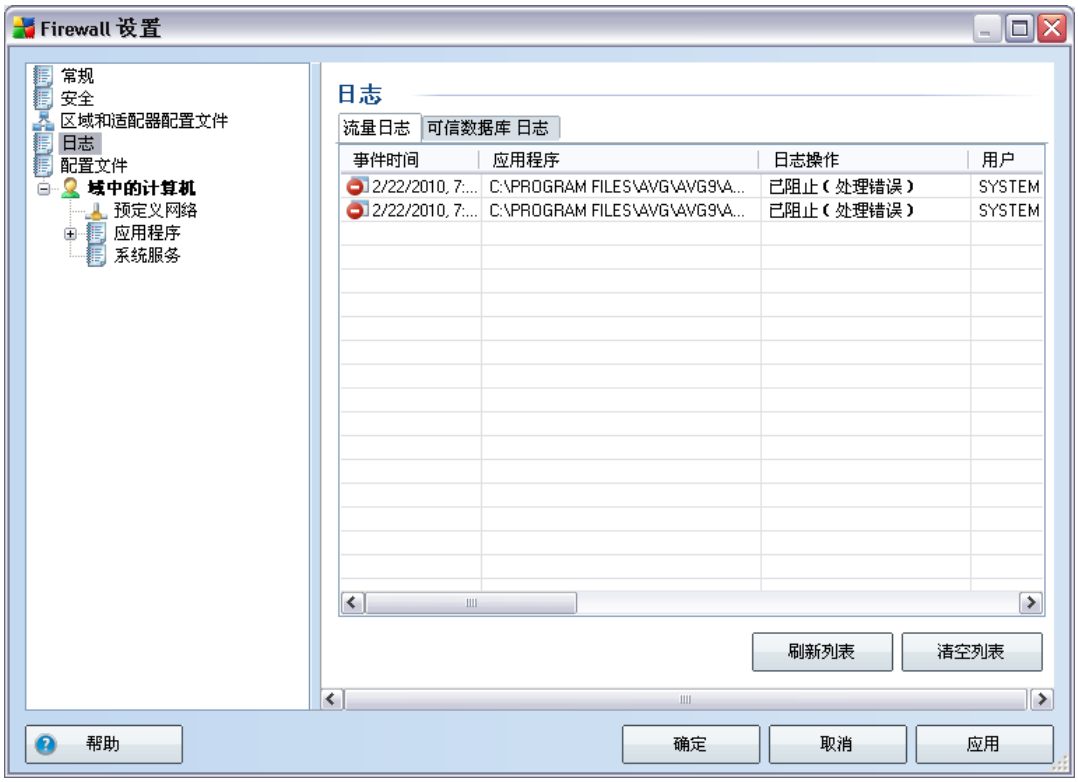
在 ***"适配器和网络区域设置"*** 对话框中，您可以编辑与向特定适配器及相应网络分配定义的配置文件相关的设置：

- ***禁用区域检测和自动配置文件切换*** - 对于每个区域，可分别对每种网络接口类型指定某个所指定的配置文件。如果您不想定义特定的配置文件，将使用根据您在***安装过程***中选择的计算机使用情况和计算机联网设计所定义的一个通用配置文件。不过，如果您决定区分配置文件，将它们分配给特定的适配器和区域，之后由于某种原因，您希望暂时改变这种安排，那么请勾选 ***"禁用区域检测和自动配置文件切换"*** 选项。

- ***适配器、区域及分配的配置文件列表*** - 通过此列表可大概了解所检测到的适配器和区域。您可以为其中的每一项分配预定义配置文件菜单中的一个特定配置文件。若要打开此菜单，请单击适配器列表中的对应项，然后选择配置文件。

- ***高级设置*** - 勾选相应的选项会停用显示提示消息的功能。

11.4. 日志



通过 ***"日志"***对话框，可查看已记入日志的所有 ***Firewall*** 操作和事件的列表，以及相关参数 *(事件时间、应用程序名称、相应的日志操作、用户名、PID、流量方向、协议类型、远程及本地端口号等)*的详细说明，分别显示在以下两个选项卡中：

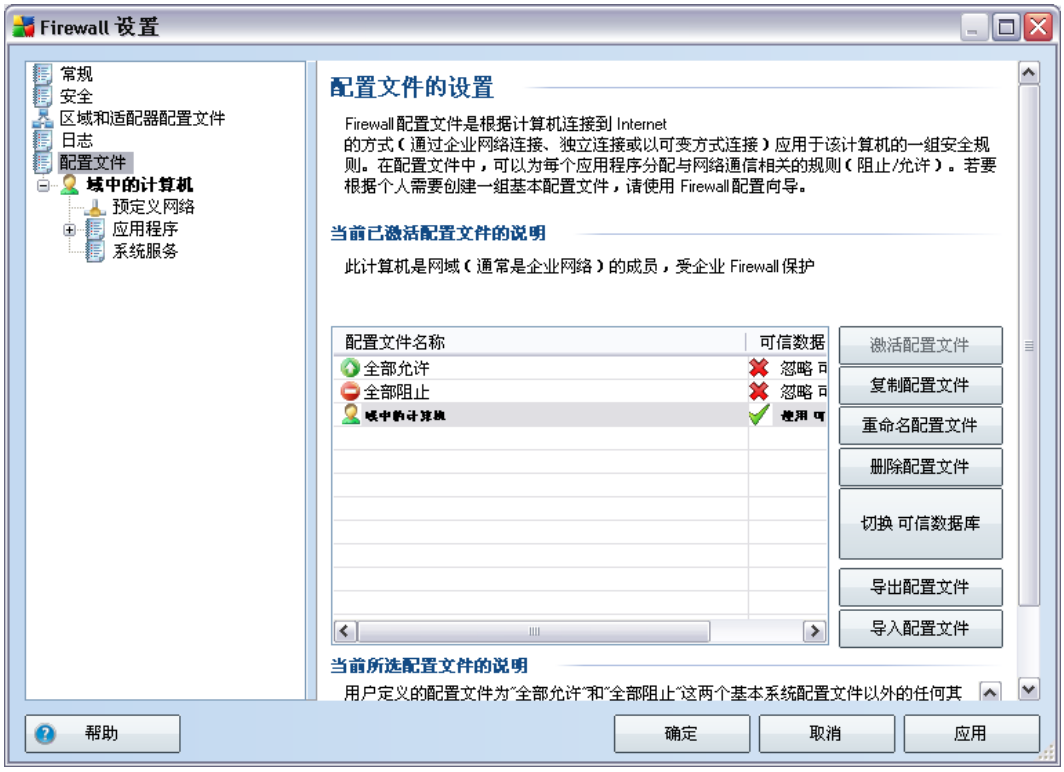
- ***"通信日志"*** – 提供了所有尝试连接到网络的应用程序的活动信息。
- ***"可信数据库日志"*** – *可信数据库*是指收集有关经过验证的可信应用程序的信息的 AVG 内部数据库，始终都可以允许此类应用程序在线进行通信。新的应用程序首次尝试连接到网络时(*即尚未为此应用程序指定防火墙规则时*)，有必要确定是否应允许相应应用程序进行网络通信。首先，AVG 会在 *可信数据库*中进行搜索，如果其中列出了此应用程序，则会自动授予它网络访问权限。只有在经过搜索之后发现数据库中没有关于此应用程序的信息时，才会通过一个独立的对话框询问您是否要允许此应用程序访问网络。

控制按钮

- ***'帮助 "***– 打开与对话框相关的帮助文件
- ***'刷新列表 "***– 可以按照所选属性对所有已记录的参数进行排列 :按时间顺序排列（*日期*）或按字母顺序排列（*其它列*）– 只需单击相应列标题即可。使用 ***'刷新列表 "*** 按钮可更新当前显示的信息。
- ***'清空列表 "***– 删除图表中的所有条目。

11.5. 配置文件

'配置文件的设置 "对话框中列有全部可用配置文件。



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

- ***"激活配置文件"***– 此按钮用于将选定的配置文件设置为活动配置文件，这意味着 ***Firewall*** 将使用选定配置文件的配置来控制网络通信。

- ***"复制配置文件"***– 创建一份与选定配置文件完全相同的副本，随后您就可以对该副本进行编辑和重命名，以创建基于所复制的原始配置文件的新配置文件

- ***"重命名配置文件"***– 用于为选定的配置文件定义新名称

- ***"删除配置文件"***– 从列表中删除选定的配置文件

- ***"切换可信数据库"***– 对于所选的配置文件，您可以决定使用*可信数据库*信息（*可信数据库是指收集有关经过验证的可信应用程序的数据的 AVG 内部数据库，始终都可以允许此类应用程序在线进行通信。*）

- ***"导出配置文件"***– 将选定配置文件的配置记录到一个文件中，该文件将被保存下来以供以后可能使用

- ***"导入配置文件"***– 根据从备份配置文件中导出的数据来配置选定配置文件的设置

- ***"帮助"***– 打开与对话框相关的帮助文件

在此对话框的底部区域中，请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：

11.5.1. 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的配置文件激活*可信数据库*（*即，收集进行在线通信的可信、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*）

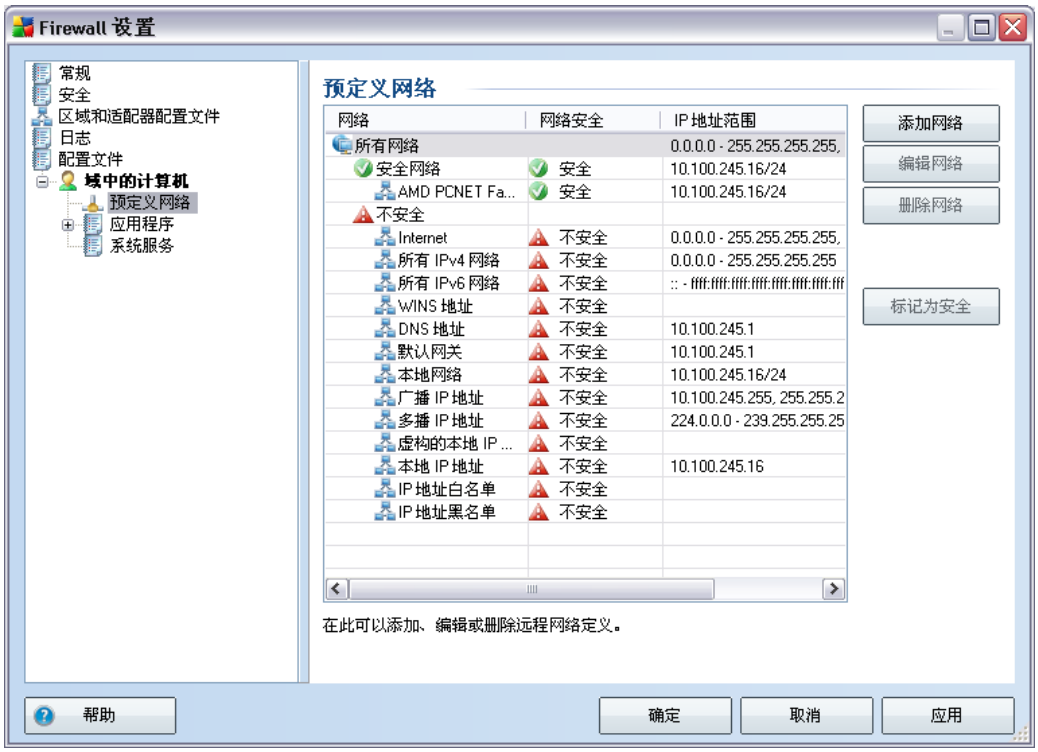
- ***启用虚拟机桥接网络*** -（*默认情况下已禁用*）勾选此项可允许 WMware 中的虚拟机直接连接到网络

游戏模式设置

在 ***"游戏模式设置"*** 区域中，您可以通过勾选相应的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。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。

11.5.2. 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。对于检测到每个网络，将提供以下信息：

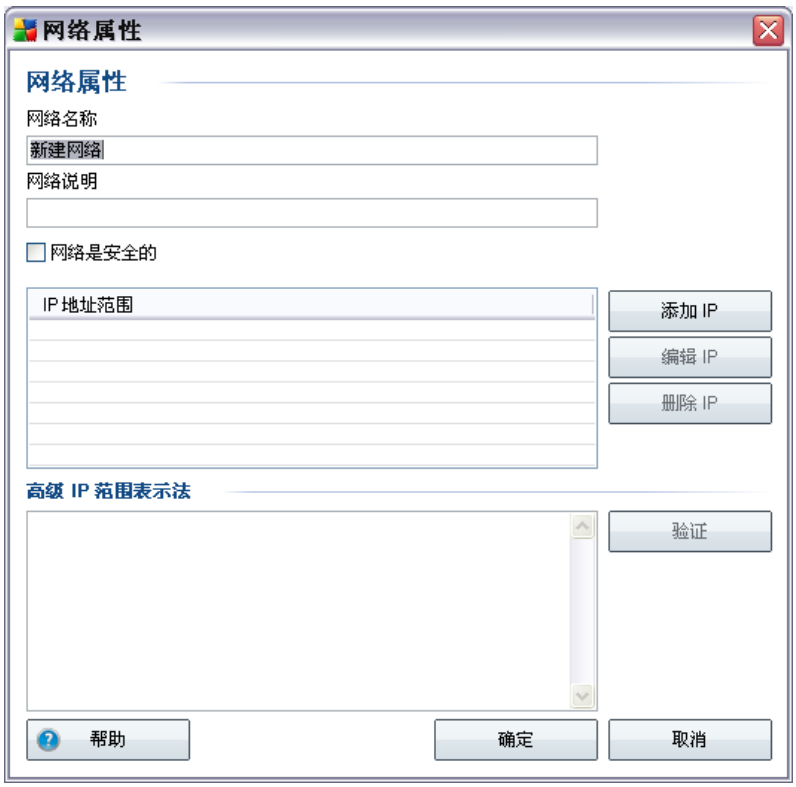
- ***"网络"*** – 计算机连接到的所有网络的名称列表
- ***网络安全*** - 默认情况下会将所有网络都视为不安全网络，仅当确信相应网络是安全网络时，才能将其指定为安全网络 *(单击表示相应网络的列表项，然后从上下文*

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信"后，应用程序就可以通过其中的网络进行通信。

- ***"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"***– 打开 ***"网络属性"***对话框窗口，您可以在此窗口中编辑新定义的网络的参数：



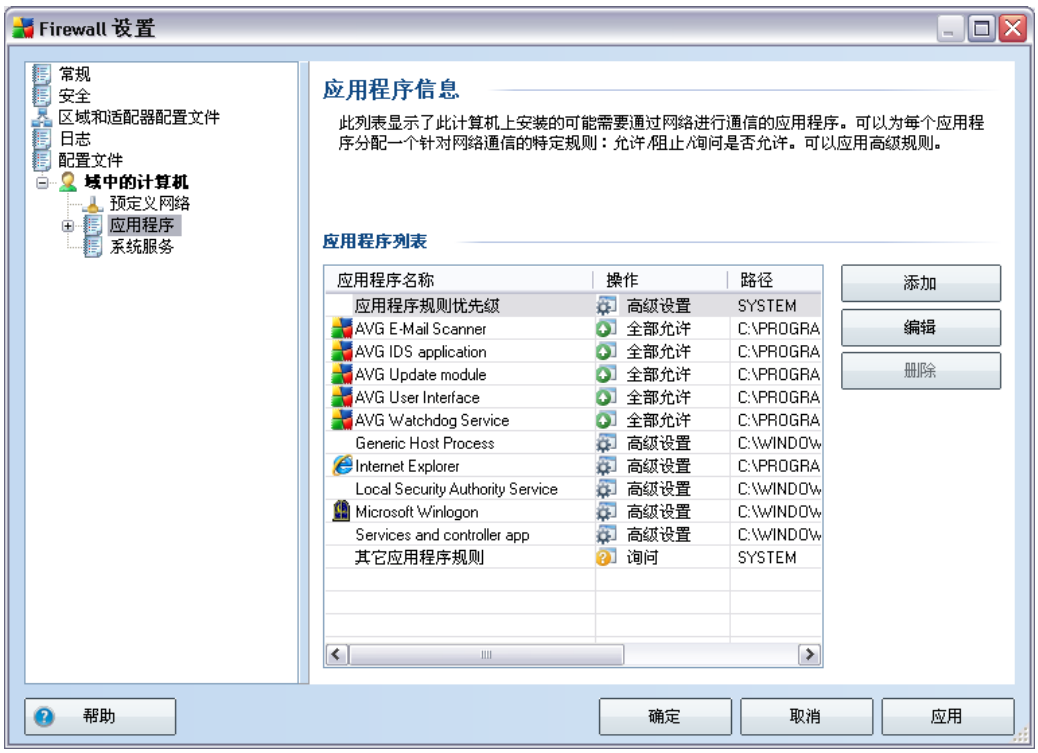
在此对话框中，您可以指定***网络名称***，提供***网络说明***，或许还可以为网络分配安全标记。也可在一个独立对话框中手动定义新网络，此对话框可通过 ***"添加 IP"***按钮 也可以通过 ***"编辑 IP"*** ***"删除 IP"***打开，可在此对话框中通过提供网络的 IP 范围或掩码指定网络。

如果有大量网络应被定义为新建网络的组成部分，则可以使用 ***"高级 IP 范围表示法"***选项 :请在对应的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"***– 打开 ***"网络属性"***对话框窗口(*见上文*),在此对话框中,您可以编辑已定义的网络的参数 *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"***– 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络后,按钮文本也会变成'标记为不安全'*。
- ***"帮助"***– 打开与对话框相关的帮助文件

11.5.3. 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:

- 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 *(用户此时能决定是要允许还是禁止进行通信)*
- 已定义高级设置

列表中的应用程序是 ***Firewall 配置向导***执行搜索时在计算机中检测到的 *(已指定相应的操作)*;如果是不明或新安装的应用程序,则在以后进行检测。

注:请注意,只有已安装的应用程序才能检测到,因此如果以后安装新应用程序,则必须对其指定 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:

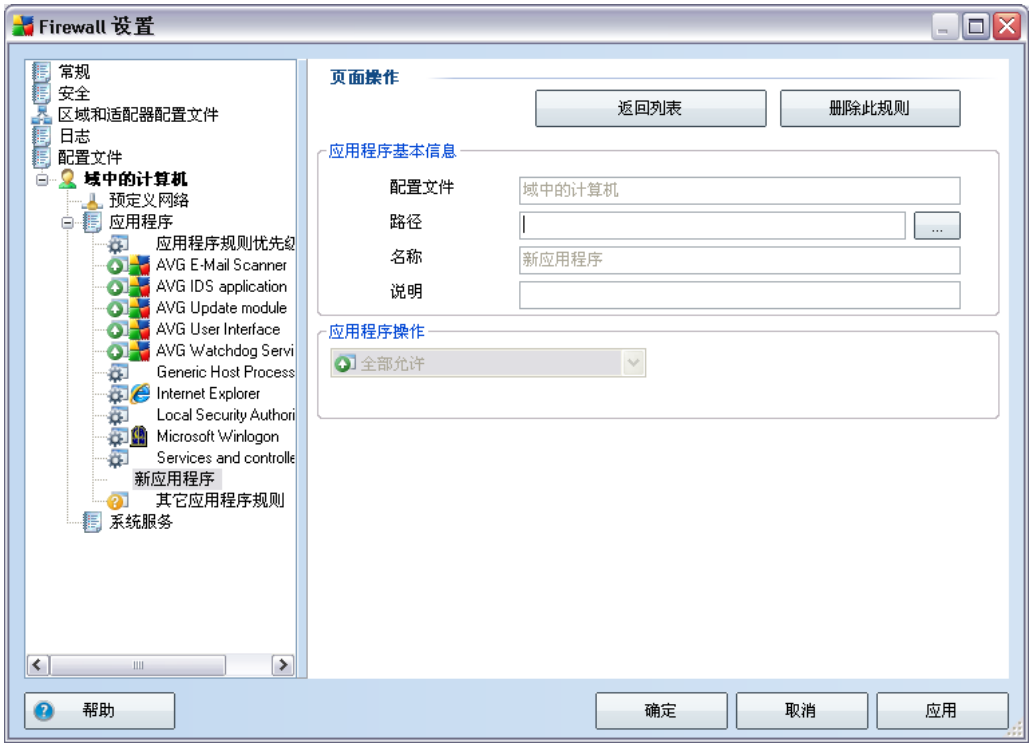
- ***"优先应用程序规则"*** *(位于列表顶部)*是优先规则,始终会先于任一应用程序的规则得到应用。
- ***"其它应用程序规则"*** *(位于列表底部)*可在没有适用的具体应用程序规则的情况(例如,对于未知和不明应用程序)下用作 '最后的措施 "。

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*** - 用于打开空的 ***"页面操作"***对话框,以便指定新应用程序规则
- ***编辑*** - 用于打开同一***页面操作***对话框,其中的数据用于编辑原有的一套应用程序规则
- ***"删除"***–从列表中删除选定的应用程序
- ***"帮助"***–打开与对话框相关的帮助文件



在此对话框中，可以详细定义相应应用程序的设置。

页面操作

- □□ ***"返回列表"*** 按钮，可大概了解已定义的所有应用程序规则。
- ***"删除此规则"*** 按钮用于清除当前显示的应用程序规则。请注意，此操作无法撤销！

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防火墙规则，即当该应用程序在尝试通过网络进行通信时，防火墙应如何处理：

- ***"允许与所有网络通信"*** 将允许该应用程序毫无限制地通过所有已定义的网络和适配器进行通信。
- ***"只允许与安全网络通信"*** 将只允许该应用程序通过已定义为 "安全"（值得信任）的网络进行通信。
- ***"阻止"*** 将自动禁止通信；将不允许该应用程序连接到任何网络。
- ***"询问"*** 将显示一个对话框，使您可以即时决定是允许还是阻止该通信尝试。
- ***"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。将按照列出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。要指定新规则，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。

11.5.4. 系统服务

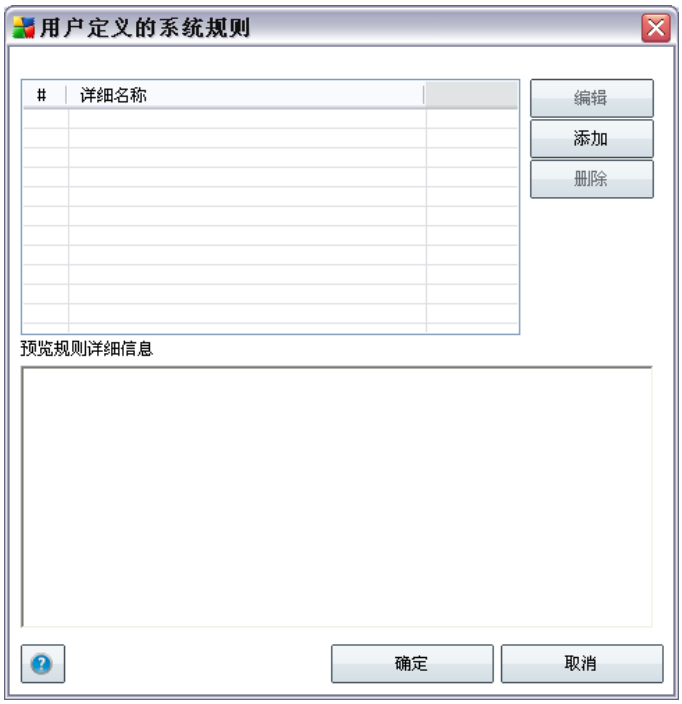
'系统服务和协议'对话框中的任何编辑都仅限经验丰富的用户执行！

系统服务和协议对话框列出了可能需要通过网络进行通信的 Windows 标准系统服务及协议。图表中含有以下几列：

- ***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*** - 此列显示了相应系统服务的名称。
- ***操作*** - 此列显示了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*** - 此列指出此系统规则适用于哪个特定网络。

可以使用以下按钮编辑此列表 *(包括指定的操作)*:

- 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"***。
- 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，底部显示的则是所选详细信息。通过相应的按钮可编辑、添加或删除用户指定的规则详细信息，制造商指定的规则详细信息仅可编辑：



警告：*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。*

记录未知通信

- ***记录未知的传入通信*** - 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。
- ***记录未知的传出通信*** - 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。

12. AVG 扫描

扫描是 AVG 9 Anti-Virus plus Firewall 功能的关键组成部分。您可以运行按需测试或安排它们定期运行（在方便的时间运行）。

12.1. 扫描界面

可通过 ***"计算机扫描器"***快速链接访问 AVG 扫描界面。单击此链接可切换到 ***"扫描威胁"*** 对话框。在此对话框中，您将找到以下内容：

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

控制按钮

此测试界面内提供的控制按钮如下：

- ***"扫描历史记录"***– 显示"扫描结果概览"对话框，该对话框中包含了完整的扫描历史记录
- ***"查看病毒库"*** – 在一个新窗口中打开病毒库 –即用于隔离检测到的感染的区域

12.2. 预定义扫描

按需扫描是 AVG 9 Anti-Virus plus Firewall 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。

AVG 9 Anti-Virus plus Firewall 中有软件供应商预先指定的两种扫描操作：

12.2.1. 扫描整个计算机

"扫描整个计算机"– 扫描您的整台计算机是否可能存在感染和/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"功能可以直接从扫描界面中通过单击此扫描功能的图标来启动。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 *(见屏幕快照)*。如果需要，可以暂时中断（***"暂停"***）或取消（***"停止"***）这种扫描。

编辑扫描配置

您可以选择编辑 ***"扫描整个计算机"*** 的预定义默认设置。按 ***"更改扫描设置"*** 链接可转到 ***"更改 扫描整个计算机 的扫描设置"*** 对话框。***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。默认情况下，大多数参数均已启用，在扫描期间将自动使用这些参数。
- ***"其它扫描设置"***– 该链接将打开新的 ***"其它扫描设置"***对话框，在此对话框中可以指定以下参数：

- ***"计算机关闭选项"***– 决定在扫描过程完成时是否应自动关闭计算机。在确认此选项（***"扫描完成时关闭计算机"***）后，将激活一个新选项（***"强制关闭锁定的计算机"***），通过该选项，即使目前已锁定计算机也可关机。

- ***"定义要扫描的文件类型"***– 应进一步决定要扫描的文件类型：

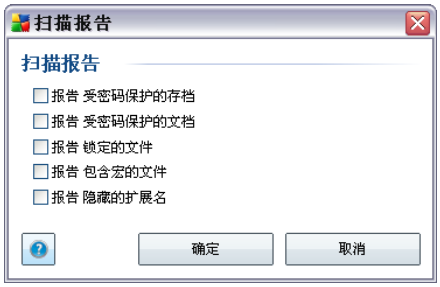
  - ***所有文件类型***，选择此选项可以通过列出不应扫描的文件扩展名（由逗号分隔）指定特例，不对其进行扫描；

  - ***"所选文件类型"***– 可以指定希望仅扫描可能受到感染的文件（*将不扫描不可能遭到感染的文件，例如某些纯文本文件或某些其它的不可执行文件*），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，此优先级设置为中级（*自动扫描*），中级可优化扫描进程的速度和对系统资源的占用。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，在计算机暂时无人值守时*）。

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



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

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展与采用 '扫描整个计算机 '这一功能处理此情况时相同 :修复所发现的任何病毒或将其移至***病毒库***。可以利用 '扫描特定的文件或文件夹 '这一功能来根据您的需要设置您自己的测试并计划这些测试的运行时间。

启动扫描

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

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

最后,若要启动扫描,请按 ***'开始扫描 '***按钮 ;扫描过程本身与扫描整个计算机基本相同。

编辑扫描配置

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

- ***"扫描参数"***– 在扫描参数列表中，您可以根据需要启用/禁用特定参数（*有关此设置的详细说明，请参阅"AVG 高级设置" "扫描" "扫描特定的文件或文件夹"* 章节）。
- ***"其它扫描设置"***– 该链接将打开新的 "其它扫描设置 "对话框，在此对话框中可以指定以下参数：

- ***"计算机关闭选项"***– 决定在扫描过程完成时是否应自动关闭计算机。在确认此选项（***"扫描完成时关闭计算机"***）后，将激活一个新选项（***"强制关闭锁定的计算机"***），通过该选项，即使目前已锁定计算机也可关机。

- ***"定义要扫描的文件类型"*** – 应进一步决定要扫描的文件类型：

  - ***所有文件类型***，选择此选项可以通过列出不应扫描的文件扩展名（由逗号分隔）指定特例，不对其进行扫描；

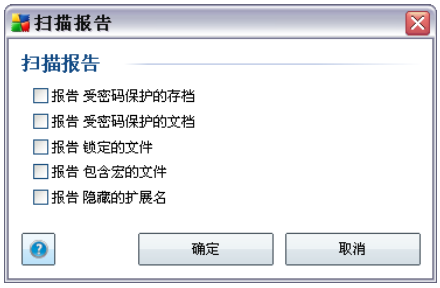
  - ***"所选文件类型"***– 可以指定希望仅扫描可能受到感染的文件（*将不扫描不可能遭到感染的文件，例如某些纯文本文件或某些其它的不可执行文件*），其中包括媒体文件（*视频、音频文件 – 如果将此框保留为未选中状态，则会进一步缩短扫描时间，因为这些文件通常很大，不太可能受到病毒感染*）。此外，您还可以通过扩展名指定哪些文件是始终应扫描的文件。

  - 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，此优先级设置为中级（*自动扫描*），中级可优化扫描进程的速度和对系统资源的占用。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，在计算机暂时无人值守时*）。

- ***"设置其它扫描报告"***– 该链接将打开新的***"扫描报告"***对话框，在此对话框中您

可以选择应报告可能发现的哪些类型的结果：



***警告：**这些扫描设置与新定义的扫描的参数相同 – 有关说明请参见 **"AVG 扫描"**、**"扫描计划"**、**"扫描方式"**章节。如果您决定更改 **"扫描特定的文件或文件夹"**功能的默认配置，则您可以将您的新设置保存为默认配置，以用于今后对特定文件或文件夹进行的所有扫描。此外，此配置将被用来作为您新计划的所有扫描的模板（所有自定义的扫描都基于用于扫描选定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 9 Anti-Virus plus Firewall 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 **"用 AVG 扫描"**选项以使用 AVG 扫描此文件

12.4. 命令行扫描

AVG 9 Anti-Virus plus Firewall 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 图形用户界面中给出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*** 扫描特定的文件或文件夹 /SCAN=路径;路径 （例如 /SCAN=C:\;D:\）
- ***/COMP*** 扫描整个计算机
- ***/HEUR*** 使用启发式分析
- ***/EXCLUDE*** 将路径或文件排除在扫描范围之外
- ***/@*** 命令文件 /文件名/
- ***/EXT*** 扫描这些扩展名 /例如 EXT=EXE,DLL/
- ***/NOEXT*** 不扫描这些扩展名 /例如 NOEXT=JPG/
- ***/ARC*** 扫描压缩包
- ***/CLEAN*** 自动清理
- ***/TRASH*** 将受感染的文件移至病毒库
- ***/QT*** 快速测试
- ***/MACROW*** 报告宏
- ***/PWDW*** 报告受密码保护的文件
- ***/IGNLOCKED*** 忽略被锁定的文件
- ***/REPORT*** 将报告输出至文件 /文件名/
- ***/REPAPPEND*** 附加到报告文件
- ***/REPOK*** 将未受感染的文件报告为“正常”
- ***/NOBREAK*** 不允许使用 Ctrl-Break 中止操作
- ***/BOOT*** 启用 MBR/BOOT 检查

- ***/PROC*** 扫描活动的进程
- ***/PUP*** 报告“可能不需要的程序”
- ***/REG*** 扫描注册表
- ***/COO*** 扫描 Cookie
- ***/?*** 显示有关此主题的帮助
- ***/HELP*** 显示有关此主题的帮助
- ***/PRIORITY*** 设置扫描优先级 /低、自动、高/ (请参见“高级设置”/“扫描”)
- ***/SHUTDOWN*** 扫描完成时关闭计算机
- ***/FORCESHUTDOWN*** 扫描完成时强制关闭计算机
- ***/ADS*** 扫描备用数据流 (仅限 NTFS)

12.5. 扫描计划

通过 AVG 9 Anti-Virus plus Firewall，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：

计划扫描

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

可以使用以下控制按钮来编辑/添加扫描：

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

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***。

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"***），定义确切的日期和时间（***"在特定的时间运行..."***），也可以定义扫描启动操作应关联的事件（***"操作条件：计算机启动时"***）。
- ***"高级计划选项"*** – 在此区域中，可以定义当计算机处于省电模式或完全关闭时，应该/不应启动扫描的条件。

“计划的扫描设置”对话框中的控制按钮

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

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

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：

- ***“自动修复/删除感染”***–（*默认情况下已启用*）：如果在扫描期间发现病毒并且有修复方案，则可以自动对其进行修复。如果受感染的文件无法自动修复，或者您决定禁

用此选项，则会在检测到病毒时通知您，此时您必须决定要对检测到的感染作何处理。建议操作是将受感染的文件删除至***病毒库***。

- ***报告可能不需要的程序和间谍软件威胁*** -(*默认情况下已启用*)：选中此框可激活 ***Anti-Spyware*** 引擎，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：即使间谍软件通常是一种安全风险，也可故意安装其中的某些程序。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*** - 如果已激活上一选项，也可选中此框，以检测更多间谍软件：程序直接从制造商获得后极其安全而无害，但之后却能以不正当的方式使用以达到恶毒的目的。这项附加措施可以进一步提高计算机的安全性，但也可能会阻止合法程序，因此默认情况下已将其禁用。

- ***"扫描跟踪 Cookie"***-(*默认情况下已启用*)：***Anti-Spyware*** 组件的此参数用于定义在扫描期间应检测的 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所有文件，即使这些文件已被打包到某种压缩包（如 ZIP、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；

接下来，您可以更改扫描配置，说明如下：

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

- ***"计算机关闭选项"***– 决定在扫描过程完成时是否应自动关闭计算机。在确认此选项（***"扫描完成时关闭计算机"***）后，将激活一个新选项（***"强制关闭锁定的计算机"***），通过该选项，即使目前已锁定计算机也可关机。

- ***"定义要扫描的文件类型"*** – 应进一步决定要扫描的文件类型：

  - ***所有文件类型***，选择此选项可以通过列出不应扫描的文件扩展名（由逗号分隔）指定特例，不对其进行扫描；

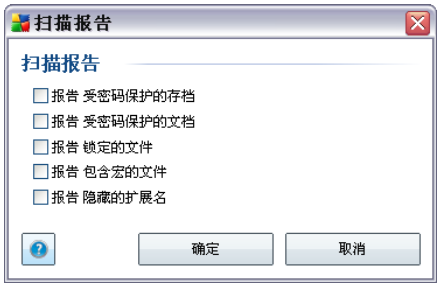
  - ***"所选文件类型"***– 可以指定希望仅扫描可能受到感染的文件（*将不扫描不可能遭到感染的文件，例如某些纯文本文件或某些其它的不可执行文件*），其中包括媒体文件（*视频、音频文件 – 如果将此框保留为未选中状态，则会进一步缩短扫描时间，因为这些文件通常很大，不太可能受到病毒感染*）。此外，您还可以通过扩展名指定哪些文件是始终应扫描的文件。

  - 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，此优先级设置为中级（*自动扫描*），中级可优化扫描进程的速度和对系统资源的占用。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，在计算机暂时无人值守时*）。

- ***"设置其它扫描报告"***– 该链接将打开新的***"扫描报告"***对话框，在此对话框中您

可以选择应报告可能发现的哪些类型的结果：



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

控制按钮

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

- ***"保存"***– 保存您在此选项卡或此对话框的任何其它选项卡中所执行的所有更改并返回 AVG 扫描界面的默认对话框。因此，如果您希望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。

12.5.3. 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
- ***Program Files*** – C:\Program Files\
- ***"My Documents"文件夹*** - C:\Documents and Settings\User\My Documents\

- ***共享文档*** – C:\Documents and Settings\All Users\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* – Windows/System32
    - *临时文件文件夹* – Documents and Settings/用户/Local Settings/Temp
    - *Internet 临时文件* – Documents and Settings/用户/Local Settings/Temporary Internet Files

"计划的扫描设置"对话框中的控制按钮

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

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

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
- ***"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况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
- ***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。

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。

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：

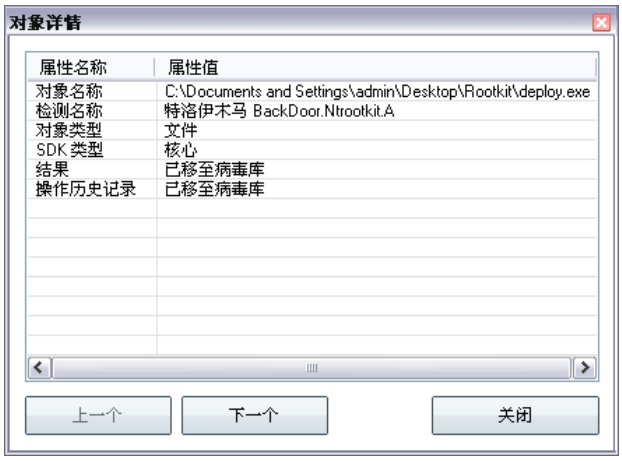
- ***“文件 ”***– 受感染对象原始位置的完整路径
- ***“感染 ”***– 检测到的病毒的名称 *（有关特定病毒的详细信息，请参阅在线病毒百科全书）*
- ***“结果 ”***– 定义在扫描期间检测到的受感染对象的当前状态：
  - ***“已感染 ”***– 已检测到受感染的对象并将其留在其原始位置 *（例如，如果您已在特定扫描设置中关闭自动修复选项）*
  - ***“已修复 ”***– 已自动修复受感染的对象，并将其留在其原始位置
  - ***“已移至病毒库 ”***– 已将受感染的对象移至***病毒库***隔离区
  - ***“已删除 ”***– 已删除受感染的对象

- ***"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)* 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
- ***"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 ***"扫描结果详细信息"*** 的新对话框窗口：



在此对话框中，可找到所检测到的受感染对象的位置信息 (***"属性名称"***)。用 ***"上一个"*** / ***"下一个"*** 按钮可查看特定检测结果的信息。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"***– 使用此按钮可删除所有这样的发现结果 :无法修复或无法移至 ***病毒库***
- ***"关闭结果"***– 终止详细信息概览并返回 ***"扫描结果概览"*** 对话框

12.7.3. '间谍软件'选项卡

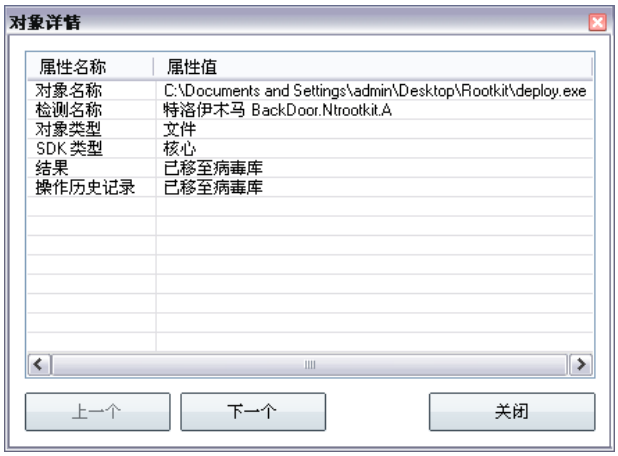
仅当在扫描期间检测到间谍软件时，***'扫描结果'***对话框中才会显示***'间谍软件'***选项卡。此选项卡分为三个部分，分别提供下列信息：

- ***'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'***– 定义在扫描期间检测到的对象的当前状态：
  - ***'已感染'***– 已检测到受感染的对象并将其留在其原始位置 例如，如果您已在特定扫描设置中关闭自动修复选项)
  - ***'已修复'***– 已自动修复受感染的对象，并将其留在其原始位置
  - ***'已移至病毒库'***– 已将受感染的对象移至***病毒库隔离区***
  - ***'已删除'***– 已删除受感染的对象
  - ***'已添加至 PUP 特例'***– 已将发现结果评估为特例并已将其添加至 PUP 特例列表(*在高级设置的**'PUP 特例'**对话框中配置*)中
  - ***'锁定的文件 –未测试'***– 相应对象已被锁定，因而 AVG 无法对它进行扫描
  - ***'有潜在危险的对象'***– 已检测到该对象有潜在危险，但未受感染 例如，它可能包含宏）;此信息仅仅是一则警告
  - ***'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***'扫描结果详细信息'***的新对话框窗口：



在此对话框中，可找到所检测到的受感染对象的位置信息（***"属性名称"***）。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"***– 使用此按钮可删除所有这样的发现结果：无法修复或无法移至***病毒库***
- ***"关闭结果"***– 终止详细信息概览并返回***"扫描结果概览"***对话框

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存档等。此类文件对您的计算机或安全不会构成任何直接威胁。如果在您的计算机上检测到了广告软件或间谍软件，则有关这些文件的信息通常会有用。如果 AVG 测试仅检测到严重程度为"警告"的内容，则不必采取任何操作。

下面简要说明了此类对象最常见的一些例子：

- ***隐藏的文件*** – 默认情况下隐藏的文件在 Windows 中是不可见的，因此有些病毒或其它威胁可能会在存储自己的文件时为它们设置隐藏属性，以此方式企图逃避检测。如果您的 AVG 报告了一个隐藏的文件并且您怀疑它有恶意，则您可以将它移至 ***AVG 病毒库***。

- ***Cookie*** – Cookie 是一些纯文本文件，网站使用它们来存储特定于用户的信息，之后会利用这些信息来加载具有定制特点的网站布局、预先填写用户名，等等。

- ***可疑的注册表项*** – 有些恶意软件会将其信息存储到 Windows 注册表中，以确保在启动时加载它，或扩大其在操作系统上的影响。

12.7.5. ‘Rootkit ’选项卡

如果您启动了 ***Anti-Rootkit 扫描***或手动将防 Rootkit 扫描选项添加到***扫描整个计算机***中 *默认情况下已禁用此选项*），则***"Rootkit"***选项卡会显示有关扫描期间检测到的 Rootkit 的信息。

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。它们不能被肯定地标记为危险，但仍值得您注意。AVG 扫描功能可以检测到可能并未受感染但可疑的文件。会以 ***"警告"*** 或 ***"信息"*** 的形式报告这些文件。

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

- ***运行时间压缩*** – 该文件是使用不太常见的某一运行时间压缩器（Run-time Packer）压缩的，这可能表示有防止扫描此类文件的企图。不过，并非每次报告此类文件时都表示存在病毒。
- ***运行时间递归压缩*** – 与上一项相似，不过在常用软件中不太常见。此类文件可疑，应考虑删除它们或提交它们以进行分析。
- ***受密码保护的压缩包或文档*** – AVG 无法扫描受密码保护的文件（*一般而言，任何其它防恶意软件程序也都无法扫描*）。
- ***包含宏的文档*** – 所报告的文档包含可能有恶意的宏。
- ***隐藏的扩展名*** – 隐藏了扩展名的文件可能似乎是图片等内容，但事实上它们是可执行文件（*如 picture.jpg.exe*）。默认情况下第二个扩展名在 Windows 中不可见，AVG 会将此类文件报告出来以防止无意中打开它们。
- ***文件路径不正确*** – 如果某一重要的系统文件是从非默认路径运行的（*例如 winlogon.exe 从"Windows"文件夹以外的位置运行*），AVG 会将这种不一致情况报告出来。有些情况下，病毒会使用标准系统进程的名称以使自己在系统中不太显眼。
- ***锁定的文件*** – 所报告的文件已被锁定，因而 AVG 无法对它进行扫描。这通常意味着某一文件正在不断地被系统使用（*例如交换文件*）。

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，这样就能确保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，或将其放回原始位置。

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*** - 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***病毒库的日期和时间***

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"***– 如果您决定将检测到的受感染对象从***病毒库***移至选定的文件夹，请使用此按钮。检测到的可疑对象将被使用其原始名称进行保存。如果不知道原始名称，将使用标准名称。
- ***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 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***中彻底删除
- ***清空库*** - 彻底删除***病毒库***中的所有内容。通过将文件从病毒库中删除，可将这些文件从磁盘中删除（不可还原，不是移到回收站中）。

13. AVG 更新

让您的 AVG 保持最新对于确保尽快检测到所有新发现的病毒至关重要。

AVG 安装过程中会邀请用户指定 AVG 的更新频率。可供选择的选项包括 ***"每 4 小时"*** 和 ***"每天"*** 请见对话框 ***计划定期扫描和更新***)。由于 AVG 更新并不按任何固定时间安排发布，而是要视新威胁的数量和严重程度而定，因此建议至少每天都核实一次是否有新更新。每 4 个小时检查一次可保证 AVG 9 Anti-Virus plus Firewall 在一天当中也会保持最新状态。

13.1. 更新级别

AVG 提供了两种更新级别供选用：

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

在计划更新时，可以选择应下载并应用哪种优先级别。

注：*如果计划程序更新和计划扫描同时执行，则更新进程优先，扫描会中断。*

13.2. 更新类型

您可以将以下两种类型的更新区分开来：

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

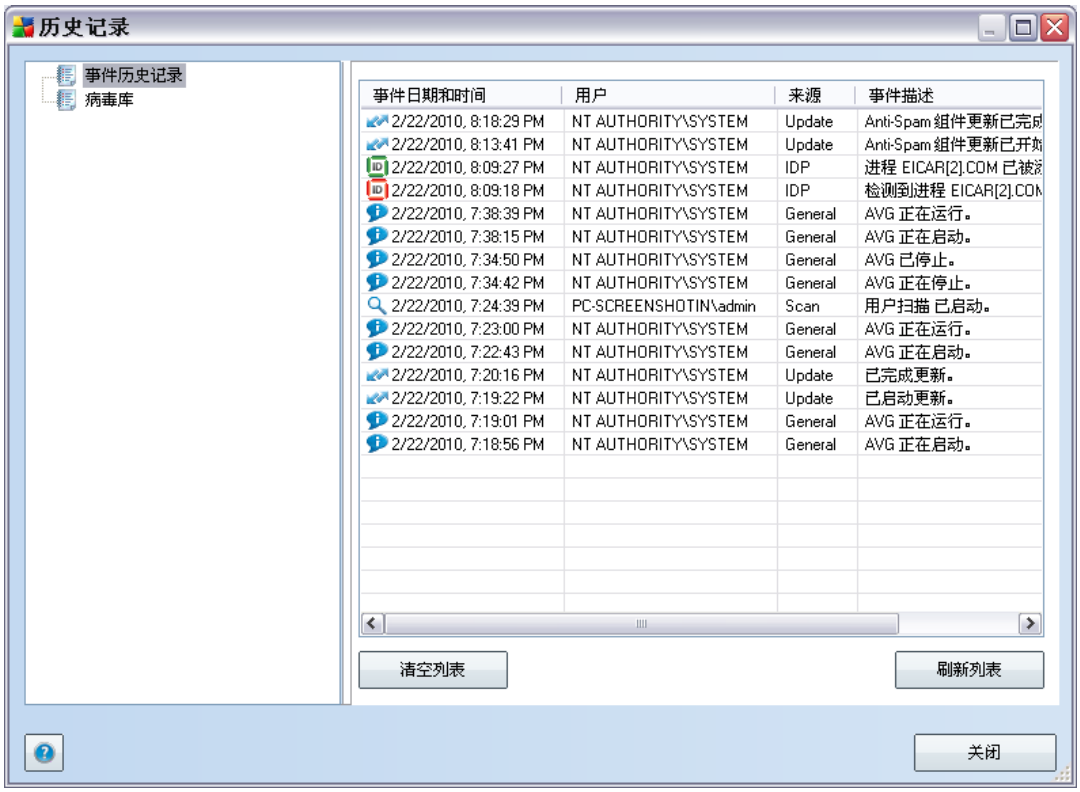
13.3. 更新过程

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

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

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

14. 事件历史记录



"事件历史记录"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 9 Anti-Virus plus Firewall 运行期间发生的重大事件的摘要。***"事件历史记录"***记录了以下类型的事件：

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

控制按钮

- ***"清空列表"***– 删除事件列表中的所有条目

- ***'刷新列表'***– 更新事件列表中的所有条目

15. 常见问题解答和技术支持

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

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

