AVG File Server 2011

用户手册

文档修订 2011.01 (20. 9. 2010)

目录

1. 简介

本用户手册提供全面的 AVG File Server 2011 文档。

祝贺您购买 AVG File Server 2011！

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

AVG 旨在保护您的计算和网络活动。请尽享 AVG 的全面保护。

所有 AVG 产品均可提供

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

2. AVG 安装要求

2.1. 支持的操作系统

AVG File Server 2011 旨在保护使用以下操作系统的工作站 /服务器：

- Windows 2003 Server 和 Windows 2003 Server x64 Edition
- Windows 2008 Server 和 Windows 2008 Server x64 Edition

（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 File Server 2011 的最低硬件要求：

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

对 AVG File Server 2011 的推荐硬件要求：

- Intel Pentium CPU 1,8 GHz
- 512 MB RAM 内存
- 600 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 File Server 2011。

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

4. AVG 安装过程

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

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

4.1. 欢迎使用

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

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

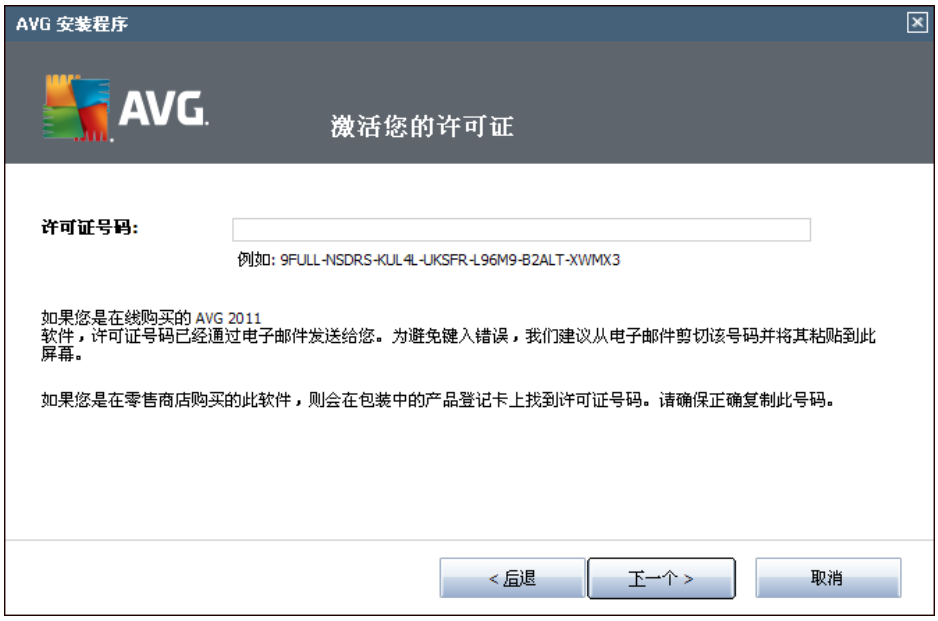
另外，此对话框还提供了 AVG 许可协议的完整文本。请仔细阅读该协议。若要确认您已阅读、了解并接受该协议，请单击 ***"接受"***按钮。如果您不同意该许可协议，请单击 ***"拒绝"***按钮，安装过程会立即终止。

4.2. 激活您的 AVG 许可证

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

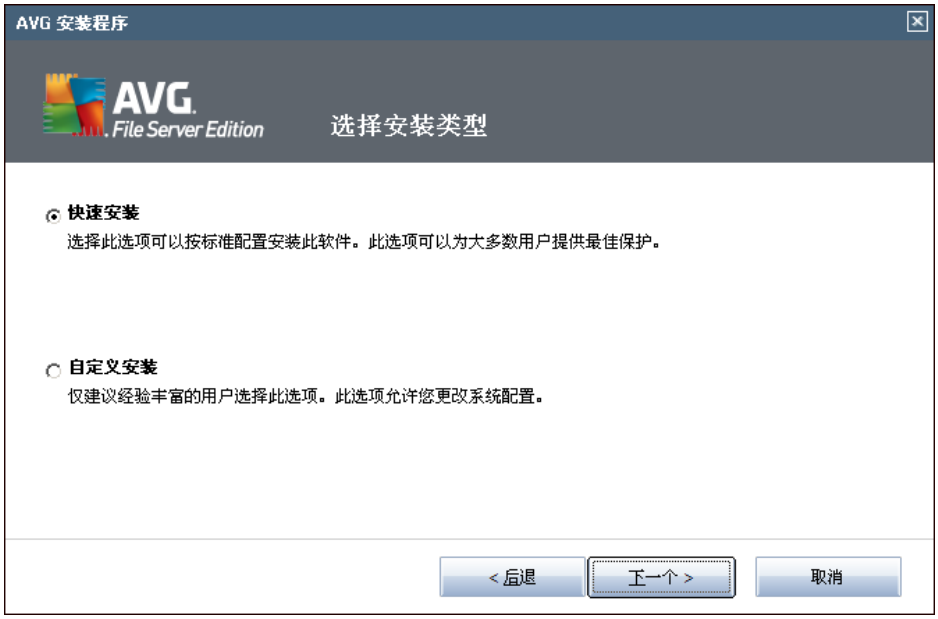
销售号码可在 AVG File Server 2011 包装盒内的光盘包装上找到。许可证号码将在您在线购买 AVG File Server 2011 之后通过确认电子邮件发送给您。您必须完全按照如图所示键入号码。如果存在数字形式的许可证号码（ *在电子邮件中* ），建议使用复制和粘

贴方法插入它。



按 ***“下一步”***按钮继续执行安装过程。

4.3. 选择安装类型



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

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

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

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

4.4. 自定义选项

“自定义选项” 对话框允许您设置两个安装参数：

目标文件夹

在该对话框的 ***“目标文件夹”*** 部分，您应该指定要安装 AVG File Server 2011 的位置。默认情况下， AVG 会被安装到 C: 驱动器上的“ Program Files ”文件夹中。如果此文件夹尚不存在，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。

组件选择

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

不过，您只能从您购买的 AVG 版本所包含的组件中进行选择！

突出显示 ***“组件选择”*** 列表中的任何项，此区域右侧将会显示对应组件的简要说明。

- ***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。

- ***服务器加载项 - Document Scanner for MS SharePoint***

此组件可扫描存储在 MS SharePoint 中的文档文件并抵御各种可能的威胁。此组件是整个 AVG File Server 2011 的关键组成部分，因此我们强烈建议安装它。

- ***AVG Remote Admin 客户端***

如果您打算将您的计算机连接至 AVG Remote Administration，请将与之对应的项选中以便同时安装它。

- ***设置管理器***

AVG Settings Manager 是一个小型应用程序，可以使用它简单快捷地配置本地 AVG 安装（甚至包括那些不是运行在 Remote Administration 下的安装）。可在安装了 AVG 应用程序的每台计算机上使用 AVG 设置管理器轻松创建它所使用的（ .pck 格式）配置文件。然后，您可以将这些文件复制到任何可移动设备，并且可在每台计算机上使用这些文件。当然，这些文件同样适用于 AVG Settings Manager 本身。有关此应用程序的更多信息，请单击 **此处** 。

按 ***“下一步”***按钮以继续。

4.5. 安装进度

“安装进度” 对话框显示安装过程的进度，不需要任何人工干预：

安装过程结束后，将会自动更新病毒数据库和程序。然后会进入下一个对话框。

4.6. 安装已成功

“安装已成功” 对话框确认 AVG File Server 2011 已经完整安装并配置完成。

如果以前选择了要安装的 AVG Remote Admin 客户端项目（请参见 “客户端选项”），则显示的对话框使用以下界面：

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

我同意参加 AVG 2011 Web 安全和产品改进计划 ... - 选中此复选框即确认您希望参加产品改进计划（ *有关详细信息，请参阅 "AVG 高级设置 / 产品改进计划"* 一章），该计划将收集关于检测到的威胁的匿名信息，以便提高总体 Internet 安全级别。

5. 安装后

5.1. 产品注册

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

5.2. 访问用户界面

AVG 用户界面 可通过以下几种方式进行访问：

- 双击 ***AVG 系统任务栏图标***
- 双击桌面上的 AVG 图标
- 从菜单 ***“开始”/“程序”/“AVG 2011”/“AVG 用户界面”***

5.3. 扫描整个计算机

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

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

5.4. AVG 默认配置

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

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

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

6. AVG 用户界面

AVG File Server 2011 打开时会显示主窗口：

该主窗口分为若干区域：

- ***系统菜单*** *（窗口顶部的系统行）* 提供了标准的导航方式，可用来访问所有 AVG 组件、服务和功能 – 详细信息 >>
- ***安全状态信息*** *（窗口上方区域）* 提供了有关 AVG 程序当前状态的信息 – 详细信息 >>
- ***快速链接*** *（窗口左侧区域）* 用于快速访问最重要和最常用的 AVG 任务 – 详细信息 >>
- ***组件概览*** *（窗口中央区域）* 提供了已安装的所有 AVG 组件的概览 – 详细信息 >>
- ***统计信息*** *（窗口左下方区域）* 提供了有关程序运行情况的所有统计数据 – 详细信息 >>
- ***系统托盘图标*** *（显示器右下角，系统托盘上）* 指示 AVG 的当前状态 – 详细信息 >>

6.1. 系统菜单

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

系统菜单分为五个主要部分：

6.1.1. 文件

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

6.1.2. 组件

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

- ***系统概览*** - 切换到默认的用户界面对话框，其中提供了 已安装的所有组件及其状态的概览
- ***服务器组件*** - 显示可用的安全组件及其状态的概览 - 详细信息 >>
- ***Anti-Virus***，可确保您的计算机免受企图进入您计算机的病毒侵害 - 详细信息 >>
- ***Anti-Spyware***，可确保您的计算机免受间谍软件和广告软件侵害 - 详细信息 >>
- ***Resident Shield***，在后台运行并 在文件被复制、打开或保存时扫描它们 - 详细信息 >>
- ***更新管理器*** ，控制所有 AVG 更新 - 详细信息 >>
- ***许可证*** ，用于显示许可证号、类型和到期日期 - 详细信息 >>
- ***Remote Administration*** 仅当您在 安装过程 中指定了要安装此组件的情况下，才会显示。
- ***Anti-Rootkit*** 检测企图掩饰恶意软件的程序和技术 - 详细信息 >>

6.1.3. 历史记录

- ***"扫描结果"*** – 切换到 AVG 测试界面 ，具体而言，即切换到 ***"扫描结果概览"*** 对话框
- ***Resident Shield 检测*** - 用于打开一个对话框，从中大概了解 ***Resident Shield***
- ***"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

File Server 2011 操作的概览。

6.1.4. 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 File Server 2011
- ***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 File Server 2011 配置进行编辑。一般而言，建议保留由软件供应商定义的应用程序默认设置。

6.1.5. 帮助

- ***目录*** - 打开 AVG 帮助文件
- ***获取在线帮助*** - 打开 AVG 网站（http://www.avg.com）中的客户支持中心页面
- ***您的 AVG Web*** - 打开 AVG 网站（http://www.avg.com）
- ***关于病毒和威胁*** - 打开在线 ***病毒百科全书***，您可以在其中查找关于所识别到的病毒的详细信息
- ***下载 AVG Rescue CD*** - 打开 Web 浏览器，指向 AVG Rescue CD 下载页面。
- ***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 File Server 2011，后两个选项会显示为* ***"立即购买"****和* ***"激活"****，这样就可以立即购买该程序的完整版。对于通过销售号码安装的 AVG File Server 2011，这两个选项显示为* ***"注册"****和* ***"激活"****。有关更多信息，请见本文档的 许可证 一节。*

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

6.2. 安全状态信息

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

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

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

如果您出于某种原因决定 忽略一组件的错误状态 （*可通过在 AVG 主窗口的组件概览中右键单击相应组件的图标打开上下文菜单，从中即可选择“忽略组件状态”选项*），此图标也会显示。在特定情况下您可能需要使用此选项，但极力建议尽快禁用 ***“忽略组件状态”*** 选项。

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

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

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

注： *AVG 状态信息也可以随时通过 系统任务栏图标 获得。*

6.3. 快速链接

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

- ***概览*** - 使用此链接可从当前打开的任何 AVG 界面切换到包含已安装的所有组件概览的默认界面 - 请参见此章： ***"组件概览"*** >>

- ***"立即扫描"*** - 默认情况下，此按钮提供上次启动的扫描的信息（ *扫描类型*、*上次启动的日期* ）可以执行 ***"立即扫描"*** 命令以再次启动相同的扫描，也可以单击 ***"计算机扫描程序"*** 链接打开 AVG 扫描界面，您可以在其中运行扫描、对扫描进行计划或编辑其参数 - 请参阅 ***"AVG 扫描"*** 一章 >>

- ***"立即更新"*** - 此链接提供上次启动更新过程的日期。按此按钮可打开更新界面并立即启动 AVG 更新过程 - 请参阅 ***"AVG 更新"*** 一章 >>

- ***服务器组件*** - 此链接将您带到 ***"服务器组件概述"*** 。

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

6.4. 组件概览

"组件概览" 区域位于 AVG 用户界面 的中央位置。该区域分为两个部分：

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

- 所选组件的说明

在 **AVG File Server 2011 中，** ***"组件概览"*** 部分中含有关于以下组件的信息：

- ***Anti-Virus***，可确保您的计算机免遭企图进入您计算机的病毒侵害 - 详细信息 >>

- ***Anti-Spyware***，可确保您的计算机免受间谍软件和广告软件侵害 - 详细信息 >>

6.5. 服务器组件

"服务器组件" 区域位于 AVG 用户界面 的中心位置。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 File Server 2011 中，***"服务器组件"*** 部分包含了以下组件信息：

- ***SharePoint*** 会扫描存储在 MS SharePoint 中的文档文件，并防止受到潜在威胁的侵害 - 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。

在组件图标的上方单击鼠标右键可展开一个上下文菜单：除了可以打开该组件的图形界面以外，还可以选择 ***"忽略组件状态"*** 。选择此选项表明您已意识到 组件的错误状态 ，但出于某种原因想要保持 AVG 的这种状态，并且不希望通过 系统任务栏图标 变化发出警告。

6.6. 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：

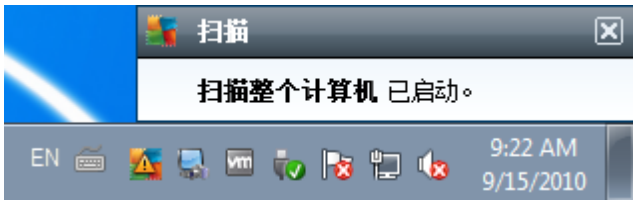
- ***“病毒数据库”*** – 告知您当前安装的病毒数据库版本情况
- ***“AVG 版本”*** - 告知您所安装的 AVG 版本情况 *（版本号采用的格式为 10.0.xxxx，其中 10.0 是产品系列版本， xx 代表内部版本号）*
- ***“许可证到期日期”*** – 提供了您的 AVG 许可证的到期日期

6.7. 系统任务栏图标

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

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

系统托盘图标还会通过从 AVG 系统托盘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、组件状态变化、出现错误状态等* ）：



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

- ***“打开 AVG 用户界面”*** – 单击此选项可打开 AVG 用户界面
- ***“扫描”*** - 单击可以打开 预定义扫描 的上下文菜单（ *“扫描整个计算机”*、*“扫描特定的文件或文件夹”* 和 *“Anti-Rootkit 扫描”*），然后选择所需的扫描，该扫描会立即启动
- ***“运行扫描”*** - 仅当计算机上当前有扫描正在运行时才会显示此项。对于该扫描，然后您可以设置其优先级，或者停止或暂停正在运行的扫描。此外，可以使用以下操作： *“设置所有扫描的优先级”*、*“暂停所有扫描”* 或 *“停止所有扫描”*。

- ***“立即更新”*** - 用于立即启动 更新
- ***“帮助”*** - 可在起始页上打开帮助文件

7. AVG 组件

7.1. Anti-Virus

7.1.1. Anti-Virus 原理

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

7.1.2. Anti-Virus 界面

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

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

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

7.2. Anti-Spyware

7.2.1. Anti-Spyware 原理

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

目前，最常见的感染来源是包含具有潜在危险的内容的网站。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 File Server 2011 与最新的 数据库和程序更新 保持同步。因此， AVG 允许您使用扫描功能对计算机进行全面扫描，以检查是否存在恶意软件 /间谍软件。它还能够检测休眠和非活动的恶意软件，即已经下载但尚未激活的恶意软件。

7.2.2. Anti-Spyware 界面

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

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

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

7.3. Resident Shield

7.3.1. Resident Shield 原理

Resident Shield 组件可对计算机进行持续的保护。它会扫描正在被打开、保存或复制的每一个文件，并守护计算机系统区域。当 ***Resident Shield*** 在被访问的文件中发现病毒时，它会停止当前正在执行的操作，不允许病毒激活自身。一般情况下，您甚至觉察不

到这一过程，因为它“在后台”运行，只会在发现威胁时通知您；同时，***Resident Shield*** 还会阻止威胁激活并将其删除。***Resident Shield*** 是在系统启动期间被加载到计算机内存中的。

Resident Shield 的功能包括：

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

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

7.3.2. Resident Shield 界面

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

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

Resident Shield 设置

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

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

- 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"****，然后在新打开的 "AVG 高级设置"对话框中编辑 AVG 配置。*

控制按钮

Resident Shield 界面中提供的控制按钮如下：

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

7.3.3. Resident Shield 检测

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

在此警告对话框中，您将找到关于经检测被认定为受感染的文件的数据（ *“文件名”*、识别到的感染的名称（ *“威胁名称”*），以及指向 ***病毒百科全书*** 的链接，如果所检测到感染是已知的，您可以在病毒百科全书中找到关于该感染的详细信息（ *“更多信息”*）。

另外，您必须决定应立即采取什么操作 - 可用选项如下：

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

- ***“以超级用户身份删除威胁”*** – 如果您认为您作为普通用户可能没有足够的权限来删除此威胁，请选中此框。超级用户拥有很高的访问权限，如果威胁位于某个系统文件夹中，那么您可能需要选中此复选框才能成功删除它。
- ***“修复”*** – 仅当检测到的感染可修复时才会显示此按钮。然后会将感染从文件中删除，并将文件恢复原始状态。如果文件本身是病毒，使用此功能可将其删除（即 *转移到* ***病毒库***）
- ***“移至库”*** – 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！

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

Resident Shield 检测到的所有威胁的完整概览可在 ***‘Resident Shield 检测”*** 对话框中找

到，可通过系统菜单选项 ***“历史记录”/ “Resident Shield 检测”***访问该对话框：

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

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

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

7.4. 更新管理器

7.4.1. 更新管理器原理

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

定期更新　AVG 至关重要！

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

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

7.4.2. 更新管理器界面

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

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

更新管理器设置

在此对话框的底部，可以找到　***"更新管理器设置"*** 区域，在此区域中，您可以对更新过程

启动规则进行一些更改。您可以定义是希望自动下载更新文件（ ***“启动自动更新”*** ）还是希望仅在需要时下载。默认情况下， ***“启动自动更新”*** 选项已启用，我们建议将其保留此状态！定期下载最新的更新文件对于任何安全软件的正常运行都是至关重要的！

此外，您还可以定义应在何时启动更新：

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

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

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

控制按钮

更新管理器 界面中提供的控制按钮如下：

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

7.5. 许可证

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

- ***许可证号码*** - 提供您的许可证号码的截短形式（ *出于安全考虑，不显示最后四个符号* ）。当输入您的许可证号码时，您必须确保其绝对精确并完全按照如图所示键入它。因此，我们强烈建议在对许可证号码进行任何操作时始终使用“ 复制和粘贴 ”方法。
- ***许可证类型*** - 指定所安装产品的类型。
- ***许可证到期日期*** - 此日期决定了您的许可证的有效期。如果您希望在此日期后继续使用 AVG File Server 2011，您必须更新您的许可证。许可证更新可在 AVG 网站 上在线进行。
- ***席位数*** - 您有权在多少个工作站上安装您的 AVG File Server 2011。

控制按钮

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

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

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

7.6. 远程管理

仅当您安装了产品的网络版的情况下，***远程管理*** 组件才会显示在 AVG File Server 2011 的用户界面中（*请参见组件的* ***许可证***）。在 ***“远程管理”*** 对话框中，您可以找到关于该组件是否处于活动状态并连接到服务器的信息。***远程管理*** 组件的所有设置都将在 ***“高级设置”/“远程管理”*** 中进行。

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

控制按钮

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

7.7. Anti-Rootkit

Rootkit 是一种程序，旨在在未经计算机系统所有者及合法管理员授权的情况下获得对计算机系统的基本控制。Rootkit 基本上不需要访问硬件，因为它的目的就是要控制硬件上运行的操作系统。通常情况下，Rootkit 通过破坏或避开标准操作系统安全机制来掩饰它们存在于系统中。它们往往又是特洛伊木马，因而会骗取用户的信任，使其认为在系统

中运行它们是安全的。用来实现此目的的方法可能包括隐藏正在运行的进程以使监测程序无法发现它们，或者隐藏文件或系统数据以使操作系统无法发现它们。

7.7.1. Anti-Rootkit 原理

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

7.7.2. Anti-Rootkit 界面

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

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

Anti-Rootkit 设置

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

- ***扫描应用程序***
- ***扫描 DLL 库***

- ***扫描驱动程序***

此外，还可以选择 Rootkit 扫描模式：

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

控制按钮

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

8. AVG Settings Manager

AVG Settings Manager 是一种主要适用于较小网络的工具，用其可复制、编辑和发布 AVG 配置。可将配置保存到便携设备（ USB 闪存驱动器等）中，然后手动应用于所选工作站。

该工具包括在 AVG 安装内容中，能通过 Windows “ 开始 ” 菜单使用：

“所有程序” / “AVG 2011 ” “AVG Settings Manager ”

- ***编辑本计算机的 AVG 配置***

  可用此按钮打开含有本地 AVG 高级设置的对话框。在此作的所有更改也都会反映在本地 AVG 安装内容中。

- ***加载并编辑 AVG 配置文件***

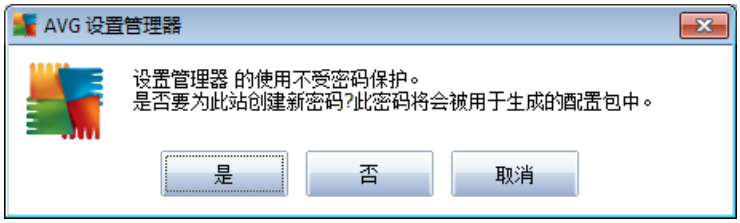
  如果已有 AVG 配置文件 (.pck)，则可用此按钮打开该文件进行编辑。一通过 ***“确定”***或 ***“应用”***按钮确认所作的更改，就会用新设置替换该文件！

- ***将文件上的配置应用到此计算机上的 AVG***

  可用此按钮打开 AVG 配置文件 (.pck)，将其应用于本地 AVG 安装内容。

- ***将本地 AVG 配置存储到文件中***

  可用此按钮保存本地 AVG 安装内容的 AVG 配置文件 (.pck)。如果未对允许执行的操作设置密码，则可能会显示以下对话框：



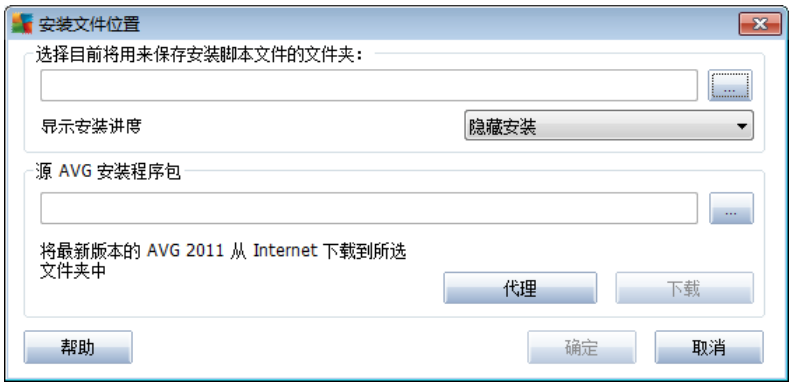
如果想要立即对允许访问的项目的访问操作设置密码，请选择 ***“是”***，然后填入所需信息并确认所作的选择。选择 ***“否”***可略过密码创建过程，继续将本地 AVG 配置保存到文件中。

- ***克隆 AVG 安装***

用此选项可通过创建有自定义选项的安装程序包复制本地 AVG 安装内容。除了以下设置，克隆时包括大多 AVG 设置：

- 语言设置
- 声音设置
- Firewall 配置
- “已允许”列表和 Identity Protection 组件的可能不需要的程序特例。

要继续操作，请先选择要从中保存安装脚本的文件夹。



然后从下拉菜单中选择以下某个选项：

- ***隐藏安装*** - 不会在安装过程中显示信息。
- ***仅显示安装进度*** - 安装过程中不需要用户予以注意，但安装进度一目了然。
- ***显示安装向导*** - 能看到安装过程，用户必须手动确认所有步骤。

可用 ***“下载”***按钮直接将最新可用 AVG 安装程序包从 AVG 网站下载到所选文件夹中，也可将 AVG 安装程序包手动放入该文件夹。

如果必须设置代理服务器用自己的网络才能连接成功，则可用 ***“代理”***按钮定义代理服务器设置。

通过单击 ***“确定”***可开始进行克隆，克隆过程不久就应该结束。也可能会显示一个对话框，询问是否要对允许的项目设置密码（请见上文）。完成后所选文件夹中会有 ***AvgSetup.bat*** 和其它文件。如果运行 ***AvgSetup.bat*** 文件，则会按上面所选的参数安装 AVG。

9. AVG 服务器组件

9.1. Documents Scanner for MS SharePoint

9.1.1. Document Scanner 原理

Document Scanner for MS SharePoint 服务器组件用于扫描存储在 MS SharePoint 中的文档。如果检测到病毒，则会将其移到 病毒库 中或完全删除。

Microsoft SharePoint 由一系列产品和软件元素组成，其组件选择越来越丰富，其中包括基于 Internet Explorer 的协作功能、进程管理模块、搜索模块和文档管理平台。 SharePoint 可被用于托管访问共享工作区、信息存储和文档的网站。

9.1.2. Document Scanner 界面

除了最重要的统计数据的概览和该组件当前状态（ *组件处于活动状态* ）的相关信息，***Documents Scanner for MS SharePoint*** 界面中还有一些统计信息 组件统计信息概览：

- ***检查过的文档*** - 自某日期起已经过检查的文档的数量
- ***检测到的威胁*** - 自某日期起已检测到的感染例数

您可以单击 ***“刷新统计值”*** 链接来随时更新这些统计数据。几乎会立即显示新数据。如果希望将所有统计值设置为零，请单击 ***“重置统计值”*** 链接。最后，单击 ***“扫描结果”*** 链接将会触发包含扫描结果列表的新对话框。使用单选按钮和 / 或选项卡对列表中的数据进行排序。

控制按钮

Documents Scanner for MS SharePoint 界面中有如下控制按钮：

- ***设置*** - 用于再打开一个对话框，从中　　可调整有关　***Document Scanner for MS SharePoint*** 文档病毒扫描性能的若干参数　　（有关此对话框的更多信息，请阅读 ***Document Scanner for MS SharePoint 高级设置*** 一章和 / 或 ***检测操作*** 一章）。
- ***后退*** - 按此按钮可恢复默认　***服务器组件界面***。

10. AVG for SharePoint Portal Server

本章说明的是在 ***MS SharePoint Portal Server***（可将其视为特殊类型的文件服务器）中维护 AVG 的方法。

10.1. 程序维护

AVG for SharePoint Portal Server 使用 Microsoft SP VSAPI 1.4 病毒扫描界面防止服务器受到潜在病毒的感染。当用户通过服务器下载和 / 或上载对象后，会检测服务器上的对象是否存在恶意软件。您可以使用 SharePoint Portal Server 的 ***管理中心*** 界面来设置防病毒保护配置。在 ***管理中心*** 中，还可以查看并管理 AVG for SharePoint Portal Server 日志文件。

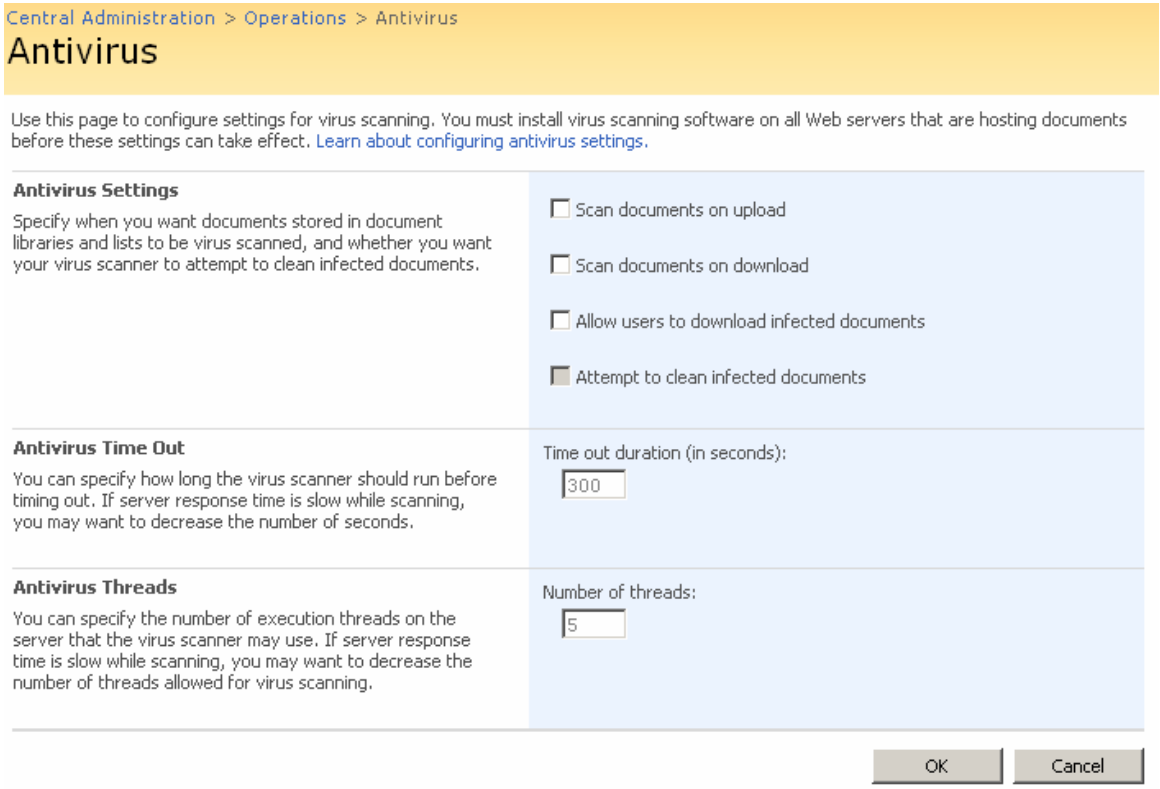
当您登录到服务器所运行的计算机上时，可以启动 ***SharePoint Portal Server 管理中心***。管理界面是基于 Web 的界面（以及 *SharePoint Portal Server 的用户界面* ），您可以使用 Windows ***“开始”菜单的“程序”/ “Microsoft Office Server”***文件夹（还取决于 ***SharePoint Portal Server 的版本）中的“ SharePoint 管理中心”*** 选项，或者通过导航至 ***“管理工具”*** 并选择 ***“Sharepoint 中心管理”*** 。

您还可以使用正确的访问权限和 URL 远程访问 ***“SharePoint Portal Server 管理中心”*** 网页。

10.2. AVG for SPPS 配置 - SharePoint 2007

在 ***SharePoint 3.0 管理中心*** 界面中，可轻松配置性能参数和 AVG for SharePoint Portal Server 扫描程序的操作。在 ***“管理中心”*** 部分中选择 ***“操作”***选项。随即将显示一个新的对话框。在 ***“安全性配置”*** 部分中选择 ***“防病毒”***项。

然后就会显示以下窗口：

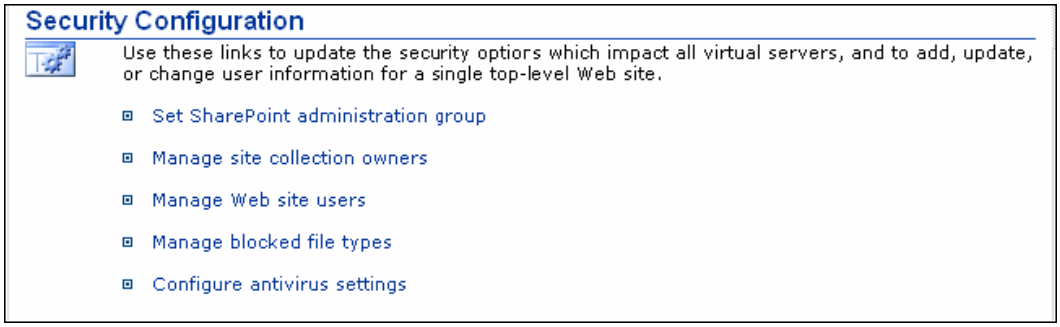


可在此配置各种 AVG for SharePoint Portal Server 防病毒扫描操作和性能特性：

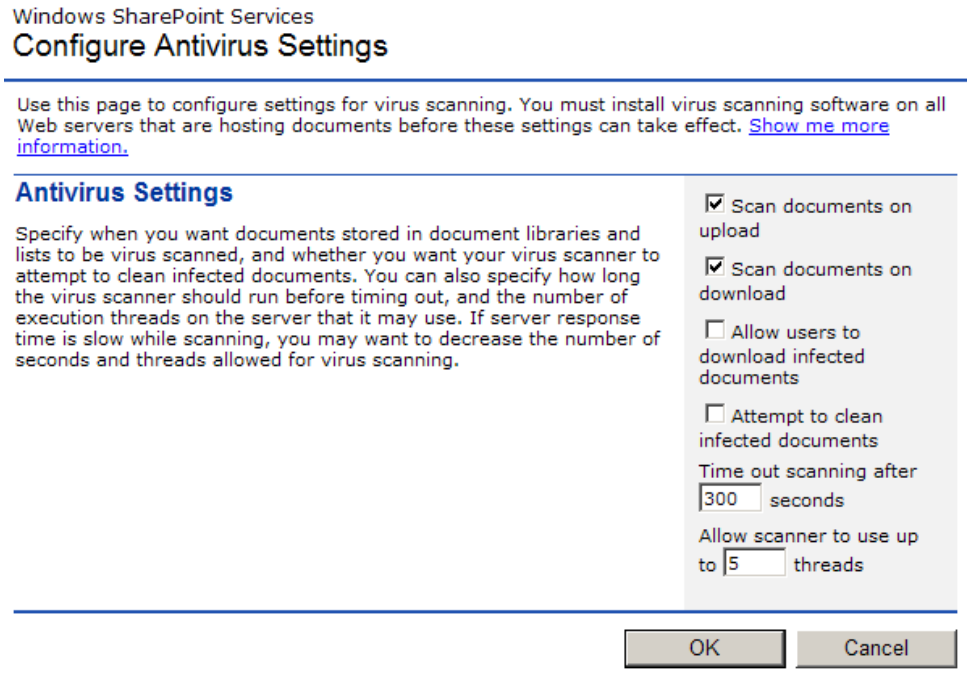
- ***在上载时扫描文档*** - 用于启用 / 禁用扫描正在上载的文档的功能
- ***在下载时扫描文档*** - 用于启用 / 禁用扫描正在下载的文档的功能
- ***允许用户下载受感染文档*** - 用于允许 / 禁止用户下载受感染文档
- ***尝试清除受感染文档*** - 启用 / 禁用自动修复受感染文档的功能（如果可能）
- ***超时持续时间*** （*秒*）- 单次启动后运行病毒扫描进程之前等待的最大秒数（如果扫描文档时服务器响应似乎很慢，则减小该值）
- ***线程数*** - 可以指定可同时运行的病毒扫描线程数；增大该数就能加快扫描速度，因为并行度更高，但另一方面，这样却会延长服务器的响应时间

10.3. AVG for SPPS 配置 - SharePoint 2003

在 ***SharePoint Portal Server 管理中心*** 界面中，可轻松配置性能参数和 AVG for SharePoint Portal Server 扫描程序的操作。在 ***“安全性配置”*** 部分中选择 ***“防病毒操作配置”*** 选项：



然后就会显示以下窗口：



可在此配置各种 AVG for SharePoint Portal Server 防病毒扫描操作和性能特性：

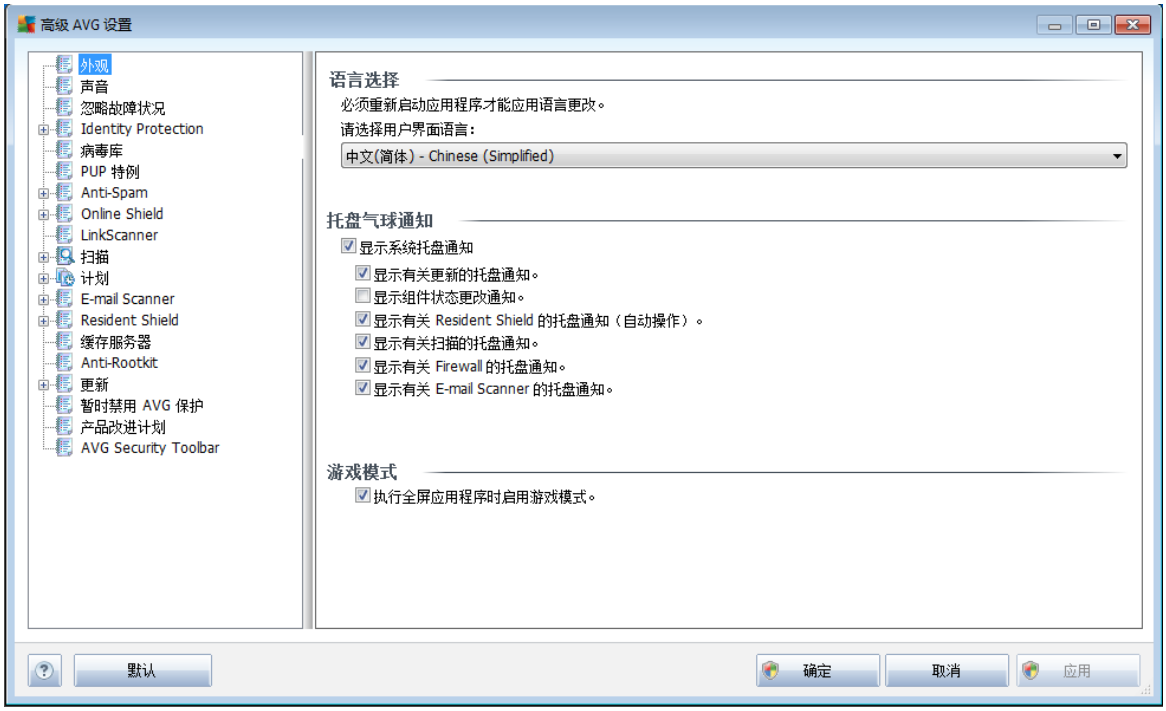
- ***在上载时扫描文档*** - 用于启用 / 禁用扫描正在上载的文档的功能
- ***在下载时扫描文档*** - 用于启用 / 禁用扫描正在下载的文档的功能
- ***允许用户下载受感染文档*** - 用于允许 / 禁止用户下载受感染文档
- ***尝试清除受感染文档*** - 启用 / 禁用自动修复受感染文档的功能（如果可能）
- ***扫描时间限制*** - 单次启动后运行病毒扫描进程之前等待的最大秒数（*如果扫描文档时服务器响应似乎很慢，则减小该值*）
- ***扫描文档时最多使用 X 个子进程*** - X 用于指定可同时运行的病毒扫描线程数；增大该数就能加快扫描速度，因为并行度更高，但另一方面却会延长服务器的响应时间

11. AVG 高级设置

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

11.1. 外观

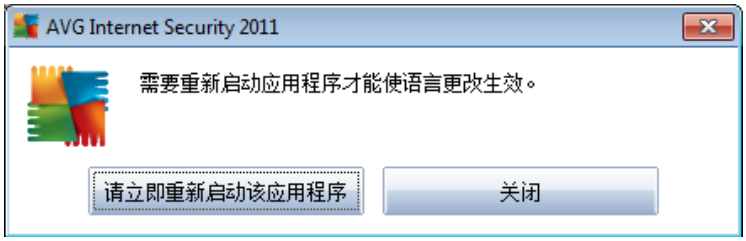
导航树的第一项内容（ *“外观”*）是指 AVG 用户界面 的常规设置，以及有关应用程序行为的几个基本选项：



语言选择

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

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



任务栏气球通知

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

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

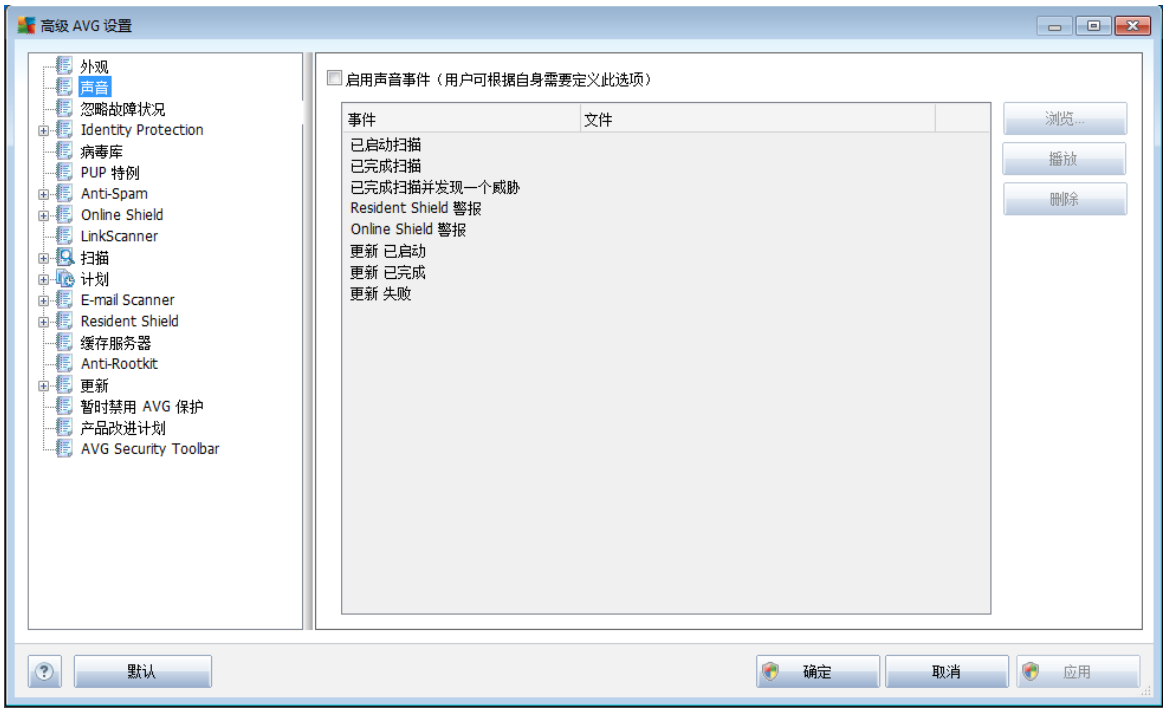
- ***显示系统任务栏通知*** - 默认情况下此项已选中（ *启用* ），因而通知会显示。取消选中此项可完全禁止显示所有气球通知。启用此项后，您可以进一步选择应显示哪些特定通知：
  - ***显示有关 更新的任务栏通知*** - 决定是否应显示有关 AVG 更新过程的启动、进度及完成情况的信息；
  - ***显示组件状态变更通知*** - 决定是否应显示有关组件的活动 / 不活动状态 或其可能存在的问题的信息。在报告组件的故障状态时，此选项相当于 系统任务栏图标 （颜色变化）的通知功能，该功能用来报告任何 AVG 组件中存在的问题；
  - ***“显示有关 Resident Shield 的任务栏通知（自动操作）”*** - 用于决定是应显示还是禁止有关文件保存、复制和 打开进程的信息（ *仅当已启用 Resident Shield “自动修复”选项时才会显示此配置* ）；
  - ***显示有关 扫描的任务栏通知*** - 决定是否应显示有关计划的扫描的自动启动、进度及结果的信息；

游戏模式

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

11.2. 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：

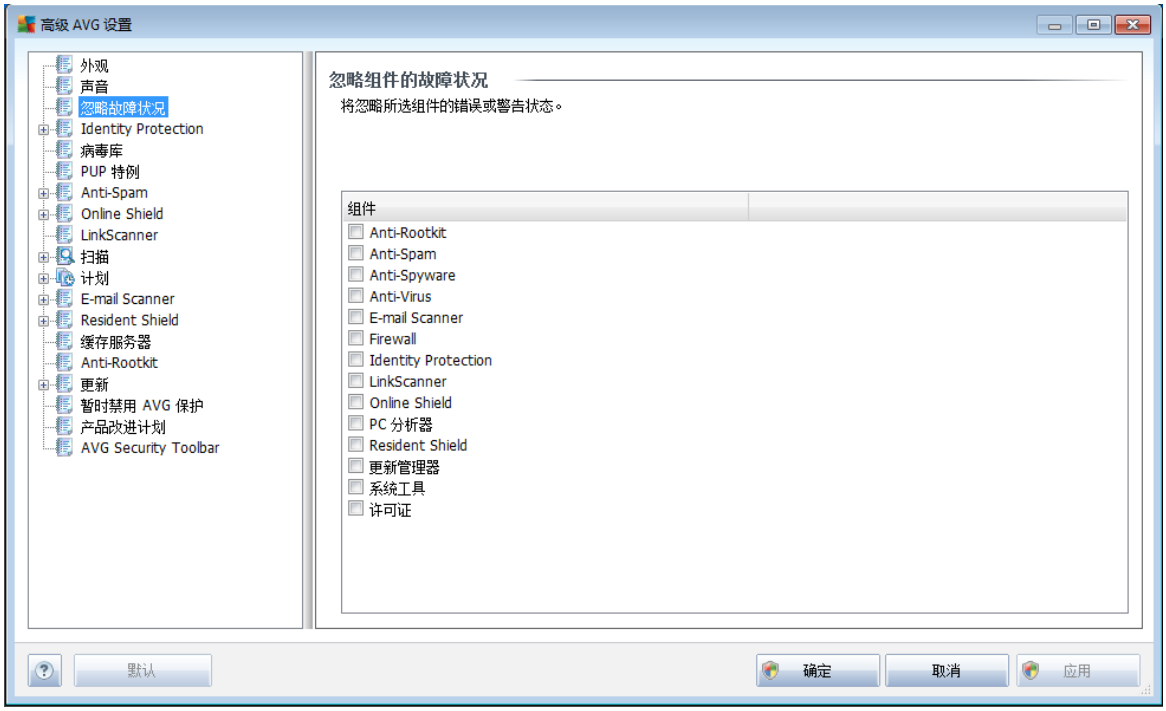


接着，请从此列表中选择相应的事件，然后在磁盘中通过浏览（ ***“浏览”***）查找要为此事件分配的合适声音。若要听一下所选的声音，请突出显示此列表中的相应事件，然后按 ***“播放”***按钮。使用 ***“删除”***按钮可删除为特定事件分配的声音。

注： *仅支持 *.wav 格式的声音！*

11.3. 忽略故障状况

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



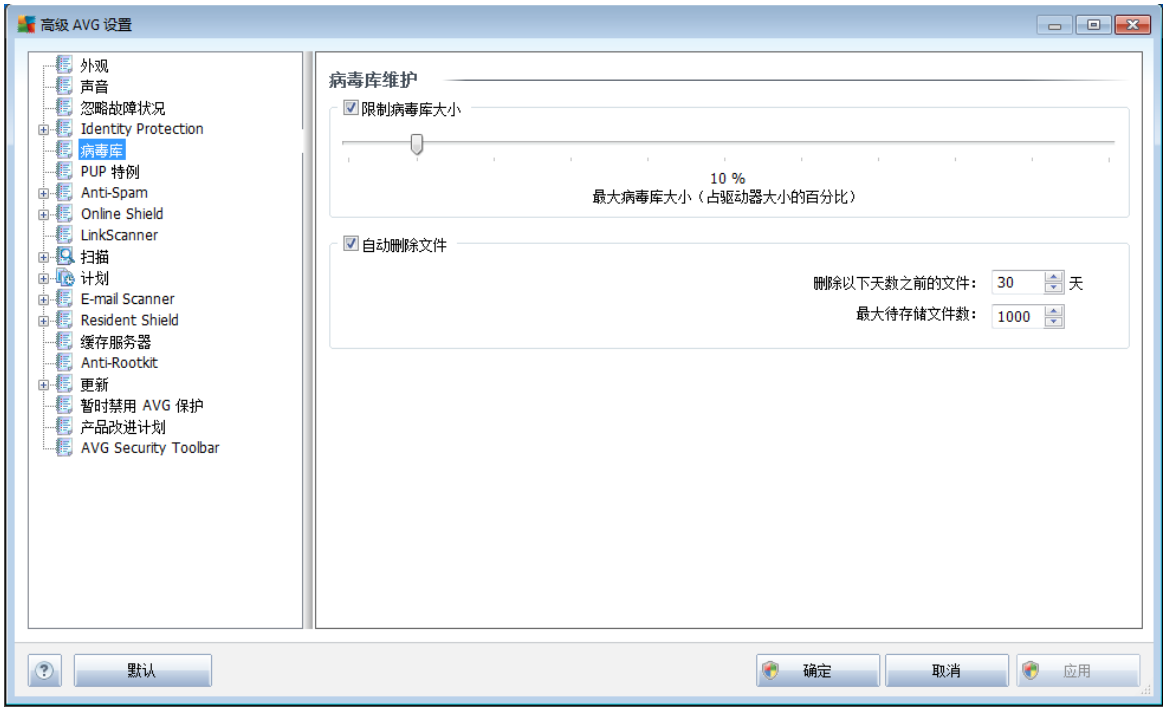
默认情况下，此列表中未选定任何组件。这意味着，如果有任何组件出现错误状态，系统会立即通过以下方式将此情况告知您：

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

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

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

11.4. 病毒库

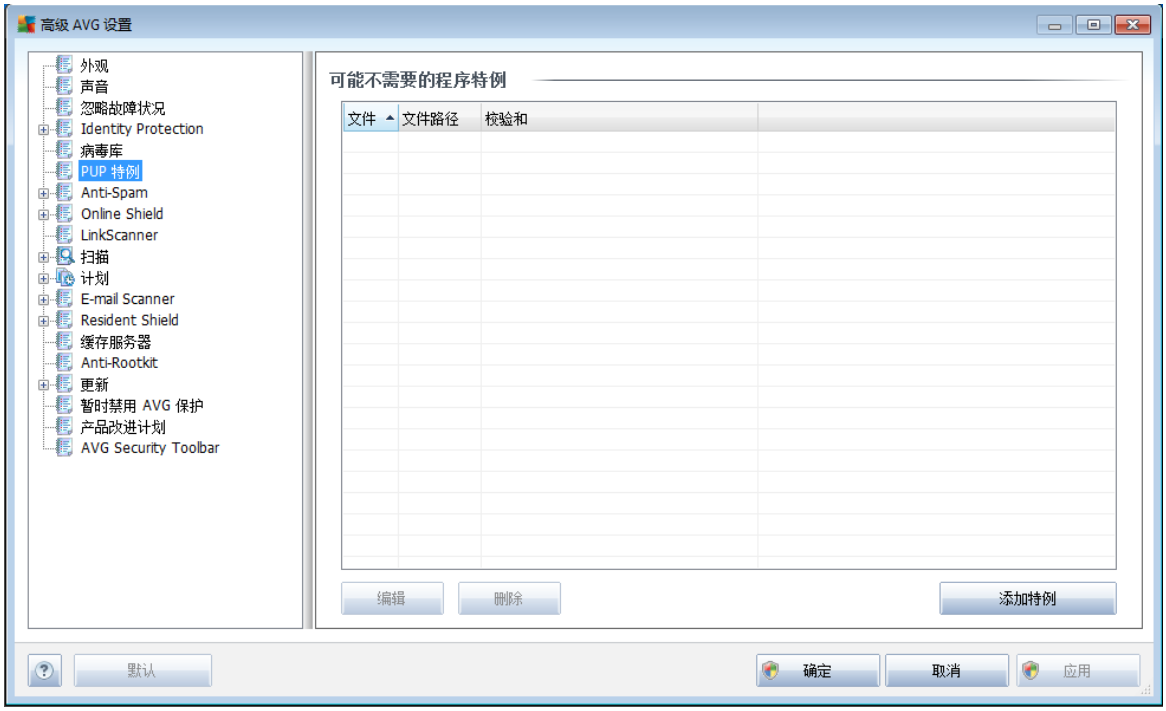


通过 ***“病毒库维护”*** 对话框，可定义关于管理 ***病毒库*** 中存储的对象的若干参数：

- ***“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”*** ）

11.5. PUP 特例

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

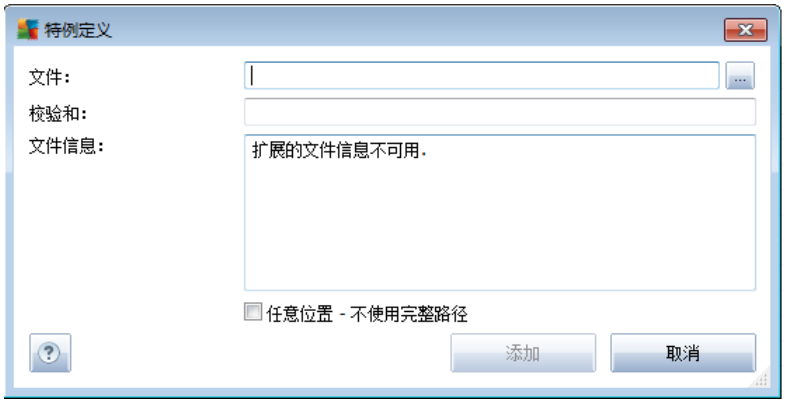


“可能不需要的程序特例” 对话框列出了已定义且当前有效的“可能 不需要的程序”的特例。您可以对此列表进行编辑，删除现有项，或添加新特例。此列表中提供了有关每个特例的以下信息：

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

控制按钮

- ***编辑*** - 打开已定义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。 如果选中此复选框，指定的文件无论其位置在何处，都会被定义为特例（ *不过，您无论如何都必须填写特定文件的完整路径；然后倘若您的系统中出现两个具有相同名称的文件，该文件将用作唯一示例* ）。

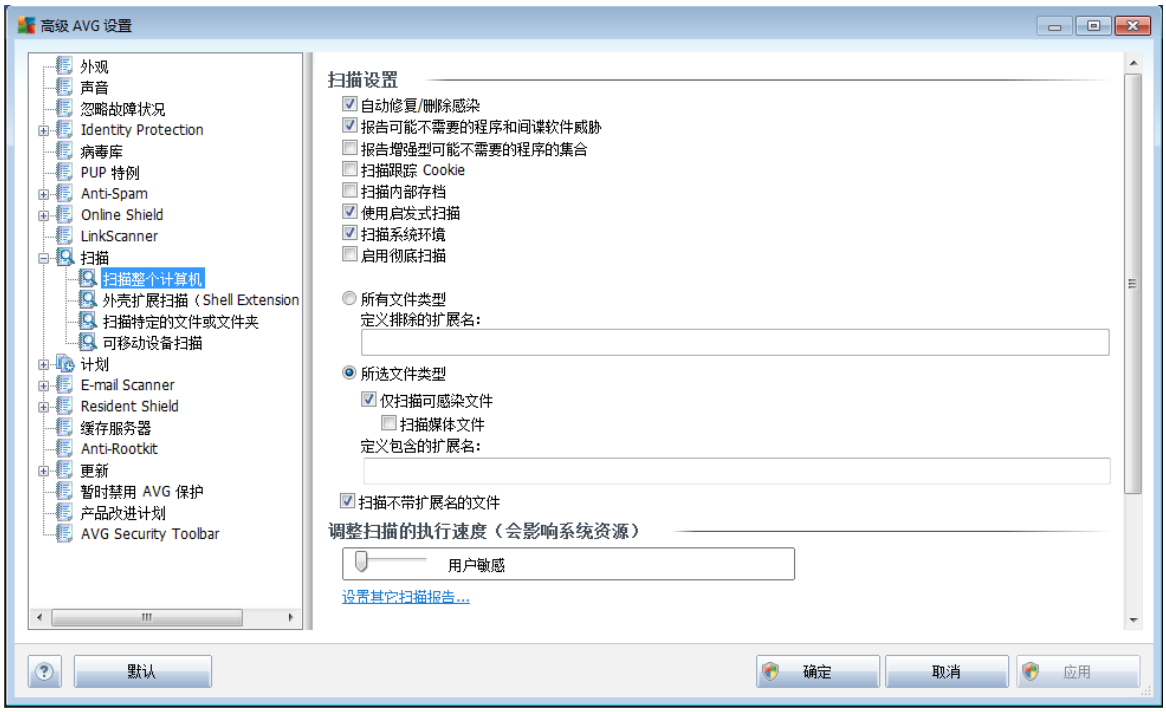
11.6. 扫描

高级扫描设置分为四种类别，分别对应软件供应商定义的以下特定扫描类型：

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

11.6.1. 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”***（*默认情况下已启用*）- 如果在扫描期间发现病毒并且有修复方案，则可以自动对其进行修复。如果不能自动修复受感染文件，则会将受感染对象移到 ***病毒库*** 中。
- ***“报告可能不需要的程序和间谍软件威胁”***（*默认情况下已启用*）- 选中此框可激活 ***Anti-Spyware*** 引擎以及针对间谍软件和病毒的扫描。间谍软件属于疑似恶意软件类软件：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”***（*默认情况下已禁用*）- 选中此框可检测更多间谍软件：程序直接从制造商处获得时极其安全而无害，但之后却可能被滥用以达到恶意目的。这项附加措施可以进一步提高计算机的安全性，但也可能会阻止合法程序，因此默认情况下已将其禁用。
- ***“扫描跟踪 Cookie”***（*默认情况下已启用*）- Anti-Spyware 组件的此参数用于定义在扫描期间应检测 Cookie（*HTTP Cookie 用于验证、跟踪和维护有关用户的特定信息，例如网站首选项或电子购物车中的内容*）

- ***“扫描压缩包”***（*默认情况下已禁用*）- 此参数定义扫描时应检查存储在压缩包（如 ZIP 和 RAR 等）中的所有文件。
- ***“使用启发式扫描”***（*默认情况下已启用*）- 启发式分析（*在虚拟的计算机环境中对已扫描对象的指令进行动态模拟*）将成为在扫描期间用来进行病毒检测的方法之一；
- ***“扫描系统环境”***（*默认情况下已启用*）- 扫描时还将检查您计算机的系统区域。
- ***“启动彻底扫描”***（*默认情况下已禁用*）- 在特定情况下（*怀疑计算机受到感染*），您可以选中此选项以激活最全面的扫描算法，该算法甚至会对计算机上极难被感染的区域进行扫描以确保绝对安全。不过要记住，此方法相当耗时。

此外，您还应决定要扫描的文件类型：

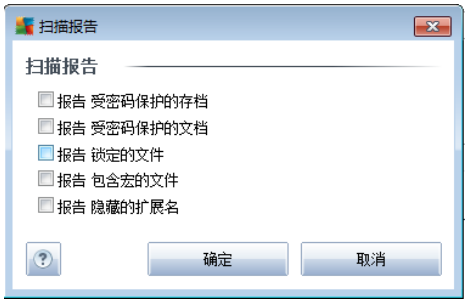
- ***“所有文件类型”***，选择此选项可以通过提供一列由逗号分隔（*保存后逗号会变成分号*）、不应扫描的文件扩展名来定义一些排除在扫描范围之外的特例；
- ***所选文件类型*** - 可以指定希望仅扫描可能受到感染的文件（*将不扫描不可能遭到感染的文件，例如某些纯文本文件或某些其它的非可执行文件*），其中包括媒体文件（*视频、音频文件 - 如果将此框保留为未选中状态，则会进一步缩短扫描时间，因为这些文件通常很大，不太可能受到病毒感染*）。此外，您还可以通过扩展名指定哪些文件是始终应扫描的文件。
- 您也可以选择指定要 ***“扫描不带扩展名的文件”*** - 默认情况下此选项已启用；我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

调整扫描的完成速度

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

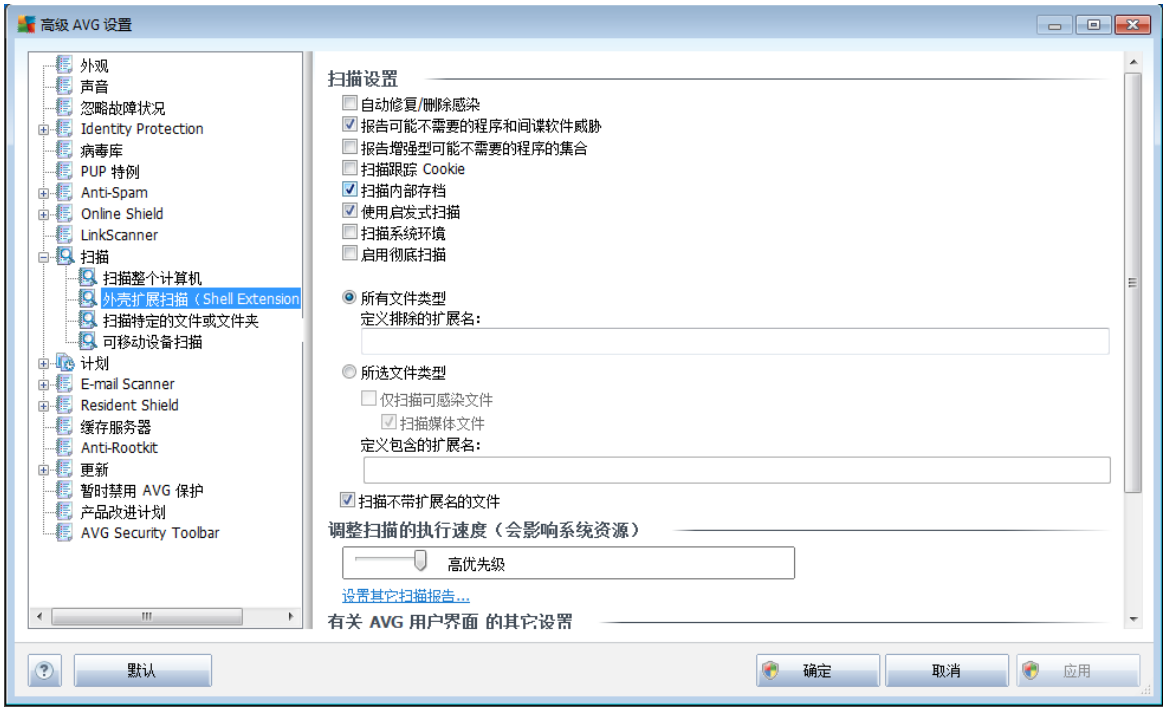
设置其它扫描报告 ...

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



11.6.2. 外壳扩展扫描

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



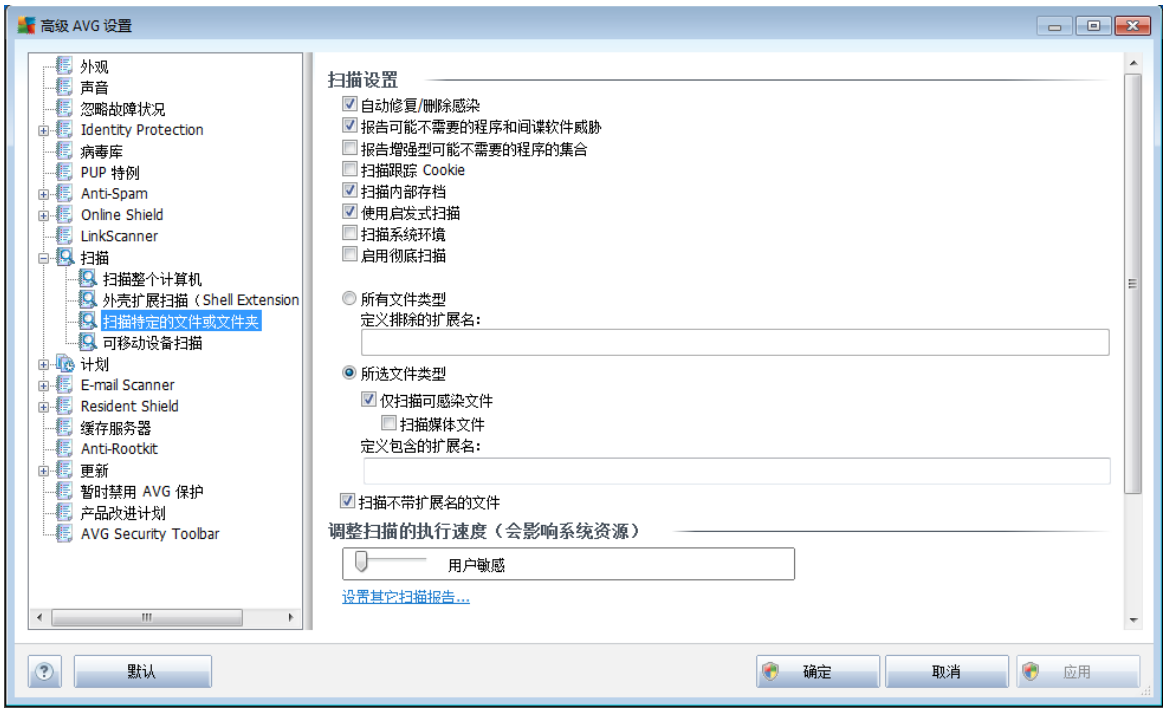
相应的参数列表与可用于 ***“扫描整个计算机”*** 的参数列表相同。不过，二者的默认设置是不同的（ *例如，“扫描整个计算机”默认情况下不检查压缩包，但是会扫描系统环境，而“外壳扩展扫描”则相反* ）。

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

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

11.6.3. 扫描特定的文件或文件夹

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



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

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

11.6.4. 可移动设备扫描

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

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

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

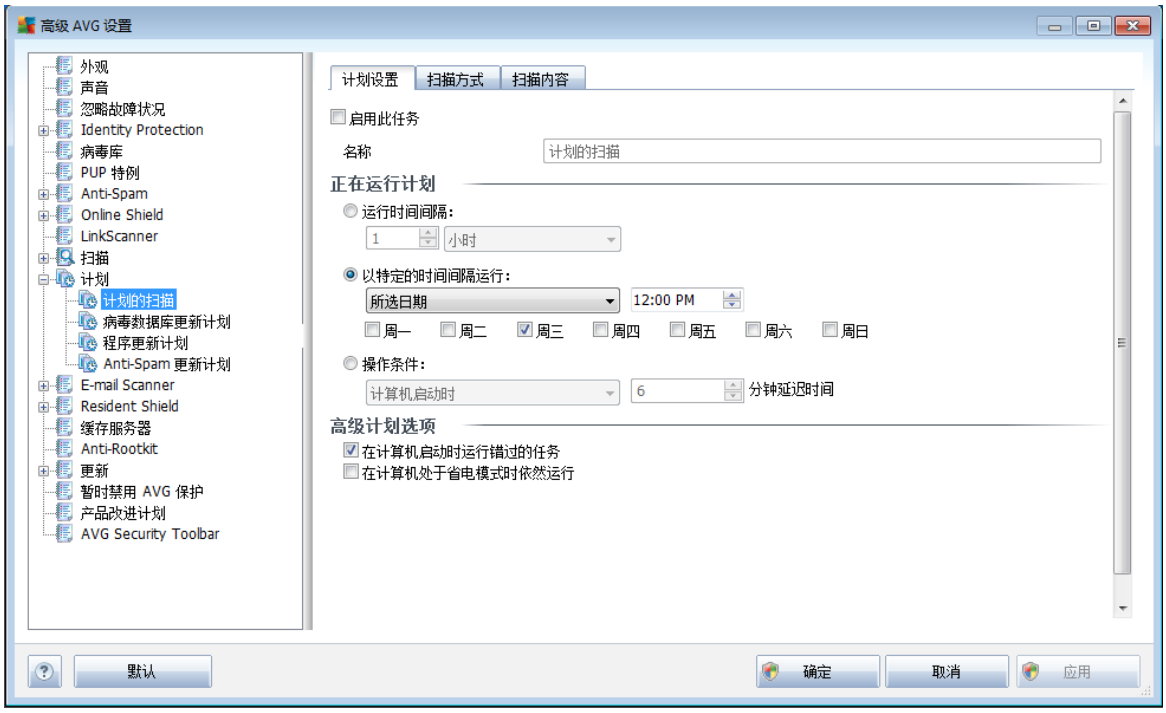
11.7. 计划

在 *“计划”* 区域中，您可以编辑以下各项的默认设置：

- 计划的扫描
- 病毒数据库更新计划
- 程序更新计划

11.7.1. 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：

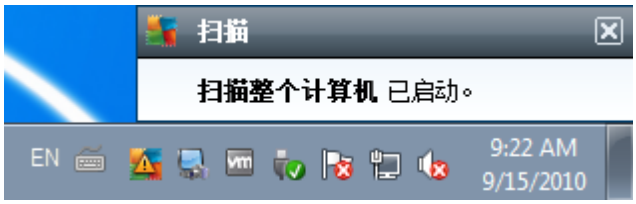
计划执行

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新启动扫描（ ***“每隔...运行一次”*** ）；或定义确切的日期和时间（ ***“以特定的时间间隔运行 ...”*** ）；也可以定义扫描启动操作应关联的事件（ ***“操作条件：计算机启动时”*** ）。

高级计划选项

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

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



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

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

- ***“自动修复 / 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。如果不能自动修复受感染文件，则会将受感染对象移到 ***病毒库*** 中。
- ***“报告可能不需要的程序和间谍软件威胁”***（*默认情况下已启用*）：选中此框可激活 ***Anti-Spyware*** 引擎以及针对间谍软件和病毒的扫描。间谍软件属于疑似恶意软件类软件：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”***（*默认情况下已禁用*）：选中此框可检测更多间谍软件：程序直接从制造商处获得时极其安全而无害，但之后却可能被滥用以达到恶意目的。这项附加措施可以进一步提高计算机的安全性，但也可能会阻止合法程序，因此默认情况下已将其禁用。
- ***“扫描跟踪 Cookie”***（*默认情况下已禁用*）：***Anti-Spyware*** 组件的此参数用于定义在扫描期间应检测 Cookie（*HTTP Cookie 用于验证、跟踪和维护有关用户的特定信息，例如网站首选项或电子购物车中的内容*）
- ***“扫描压缩包”***（*默认情况下已禁用*）：此参数定义扫描时应检查所有文件，即使这些文件被存储在压缩包（如 ZIP 和 RAR 等）内也不例外
- ***“使用启发式扫描”***（*默认情况下已启用*）：启发式分析（*在虚拟的计算机环境中对已扫描对象的指令进行动态模拟*）将成为在扫描期间用来进行病毒检测的方法

之一；

- ***“扫描系统环境”***（*默认情况下已启用*）：扫描时还将检查您计算机的系统区域；
- ***“启动彻底扫描”***（*默认情况下已禁用*）- 在特定情况下（*怀疑计算机受到感染*），您可以选中此选项以激活最全面的扫描算法，该算法甚至会对计算机上极难被感染的区域进行扫描以确保绝对安全。不过要记住，此方法相当耗时。
- ***“扫描 Rootkit”***（*默认情况下已禁用*）：如果您要将 Rootkit 检测纳入对整个计算机的扫描，请勾选此项。在 ***Anti-Rootkit*** 组件中，Rootkit 检测功能也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：

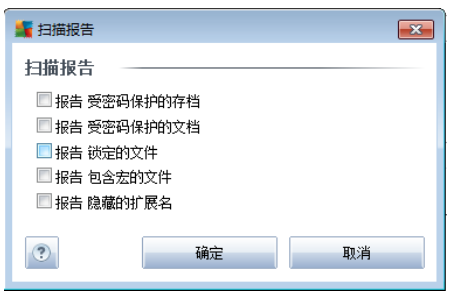
- ***“所有文件类型”***，选择此选项可以通过提供一列由逗号分隔（*保存后逗号会变成分号*）、不应扫描的文件扩展名来定义一些排除在扫描范围之外的特例；
- ***所选文件类型*** - 可以指定希望仅扫描可能受到感染的文件（*将不扫描不可能遭到感染的文件，例如某些纯文本文件或某些其它的非可执行文件*），其中包括媒体文件（*视频、音频文件 - 如果将此框保留为未选中状态，则会进一步缩短扫描时间，因为这些文件通常很大，不太可能受到病毒感染*）。此外，您还可以通过扩展名指定哪些文件是始终应扫描的文件。
- 您也可以选择指定要 ***“扫描不带扩展名的文件”*** - 默认情况下此选项已启用；我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

调整扫描的完成速度

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

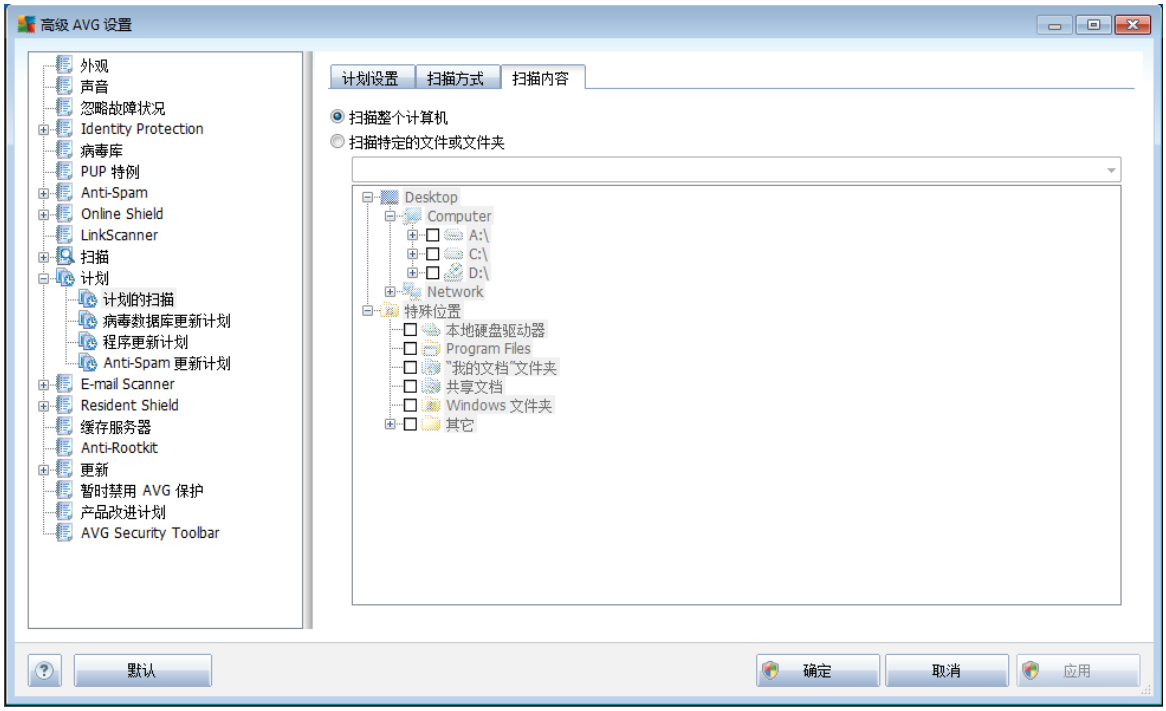
设置其它扫描报告

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



其它扫描设置

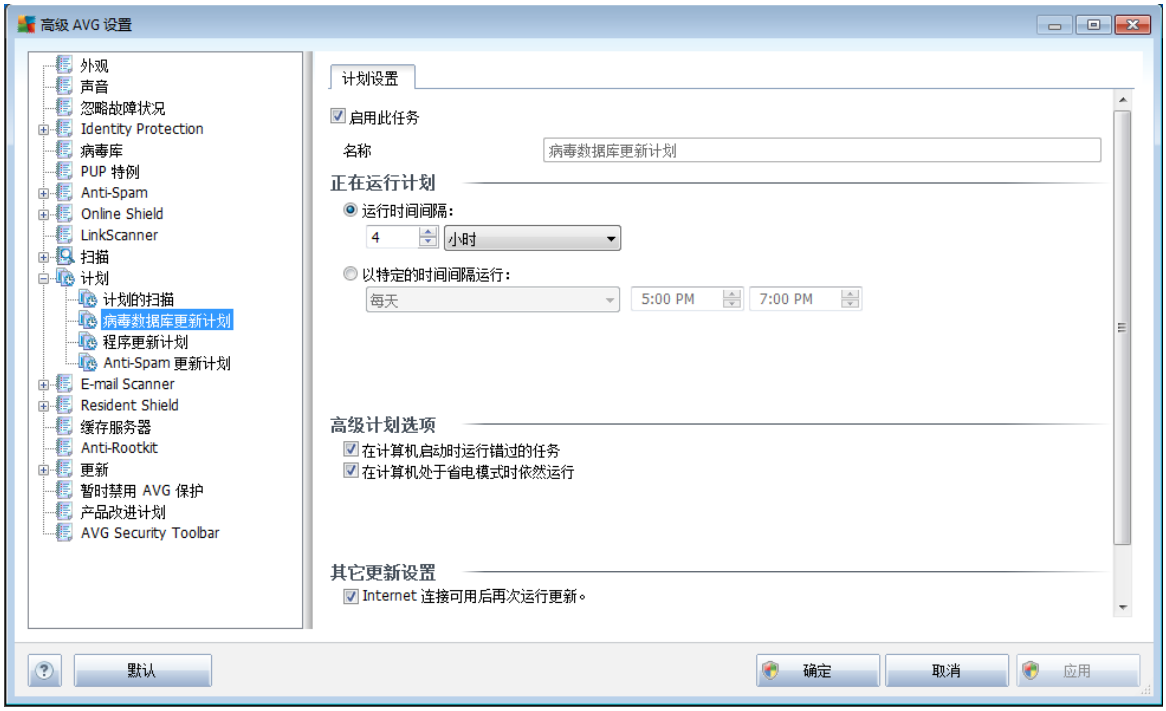
单击 ***“其它扫描设置 ...”***可打开 新的 ***“计算机关闭选项”*** 对话框，在此可以决定当扫描进程运行结束后，是否应自动关闭计算机。在确认此选项（ ***“扫描完成时关闭计算机”*** ）后，将激活一个新选项（ ***“强制关闭锁定的计算机”*** ），通过该选项，即使目前已锁定计算机也可关机。



在 ***“扫描内容”*** 选项卡上，您可以定义您要计划的是 “扫描整个计算机”还是“扫描特定的文件或文件夹”。如果您选择的是“扫描特定的文件或文件夹”，则在此对话框底部将激活如

图所示的树结构，您可以利用它来指定要扫描的文件夹。

11.7.2. 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。

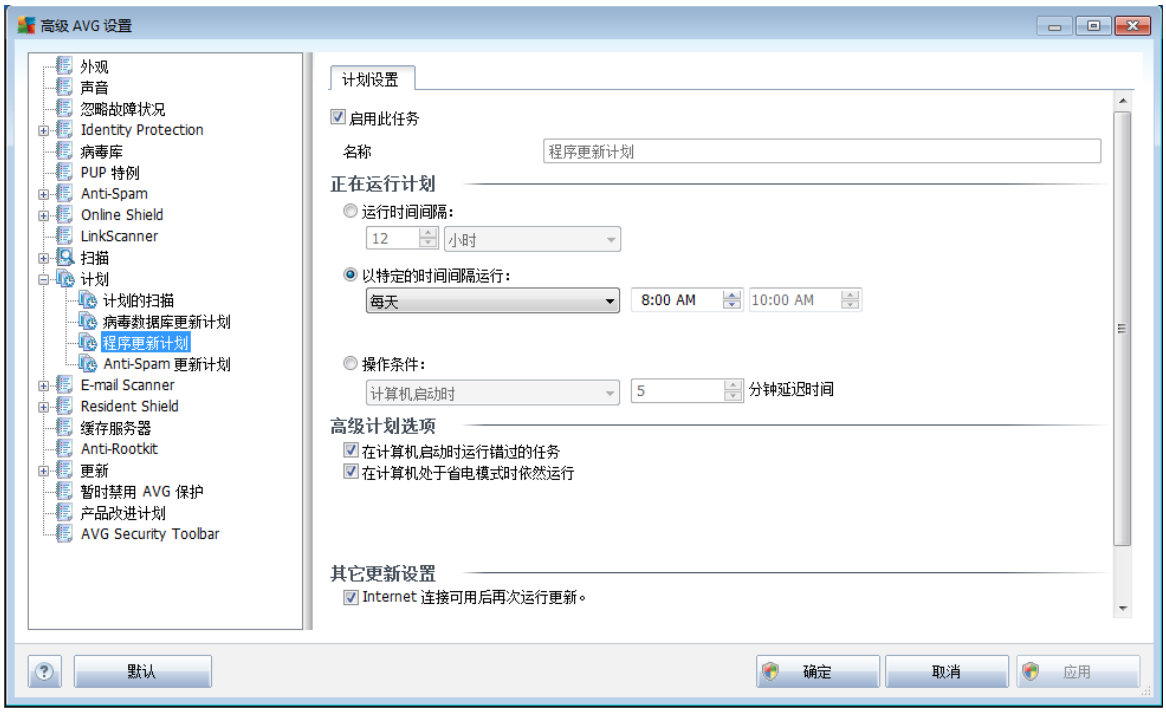
其它更新设置

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*） 。

11.7.3. 程序更新计划



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

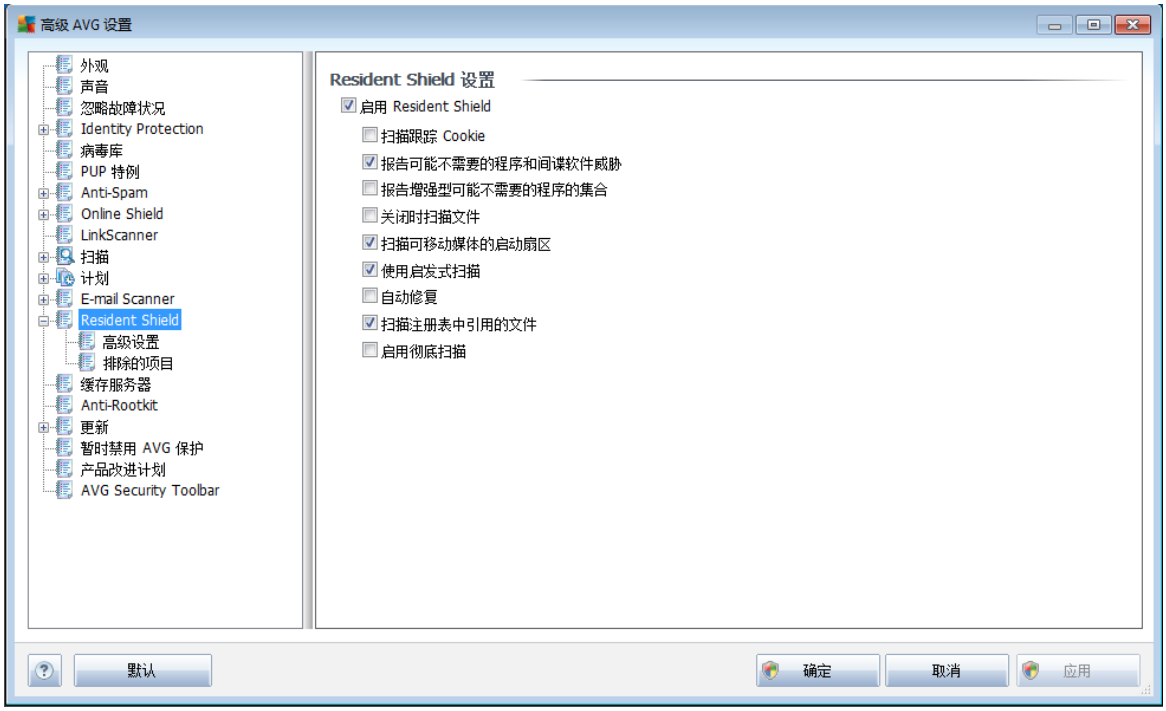
选中 ***“一旦 Internet 连接可用就再次运行更新”*** 选项可确保：如果 Internet 连接断开，导致更新过程失败，则在 Internet 连接恢复后更新过程会立即重新启动。

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。*

11.8. Resident Shield

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



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

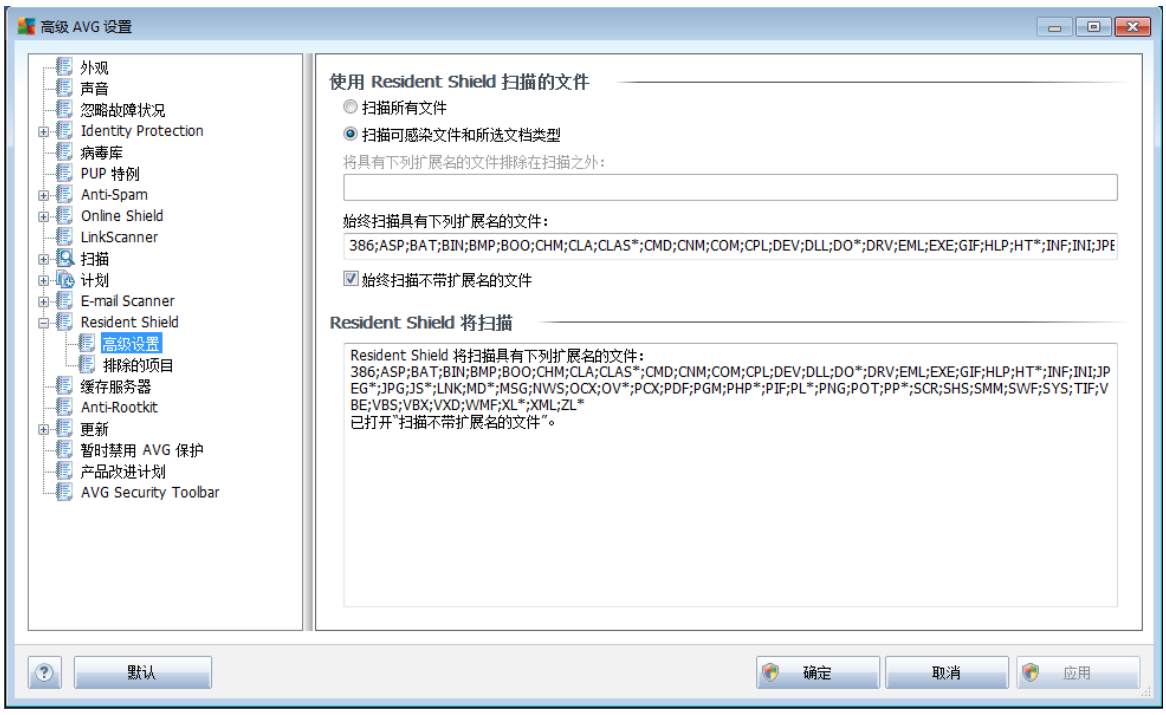
- ***“扫描跟踪 Cookie”***（*默认情况下已禁用* ）- 此参数用于指定在扫描期间应对 Cookie 进行检测。 （*HTTP Cookie 用于验证、跟踪和维护有关用户的特定信息，例如网站首选项或电子购物车中的内容* ）
- ***“报告可能不需要的程序和间谍软件威胁”*** -（*默认情况下已启用* ）：选中此框可激活 ***Anti-Spyware*** 引擎，进行间谍软件和病毒扫描。 间谍软件 属于疑似恶意软件类软件：即使间谍软件通常是一种安全风险，也可故意安装其中的某些程序。建议保持此功能的激活状态，因为此功能会使计算机更加安全。
- ***“报告更多可能不需要的程序”*** （*默认情况下已禁用* ）- 选中 此框可检测更多 间谍软件 ：程序直接从制造商处获得时极其安全而无害，但之后却可能被滥用以达

到恶意目的。这项附加措施可以进一步提高计算机的安全性，但也可能会阻止合法程序，因此默认情况下已将其禁用。

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

11.8.1. 高级设置

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

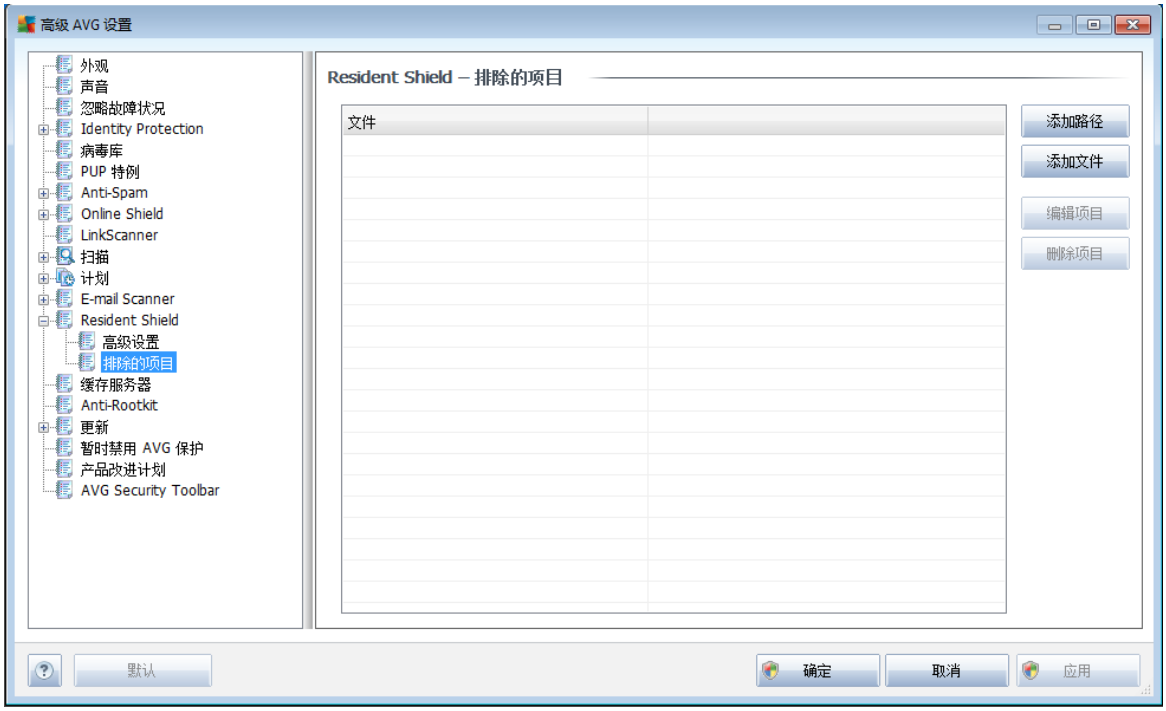


决定是要扫描所有文件还是仅扫描可感染文件 – 如果选择后者，则可以进一步指定一个

扩展名列表以定义应排除在扫描范围之外的文件，还可以指定另一个文件扩展名列表以定义在所有情况下都必须扫描的文件。

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

11.8.2. 排除的项目



可通过 ***"Resident Shield - 排除项目"*** 对话框定义应排除在 ***Resident Shield*** 扫描范围之外的文件和 / 或文件夹。

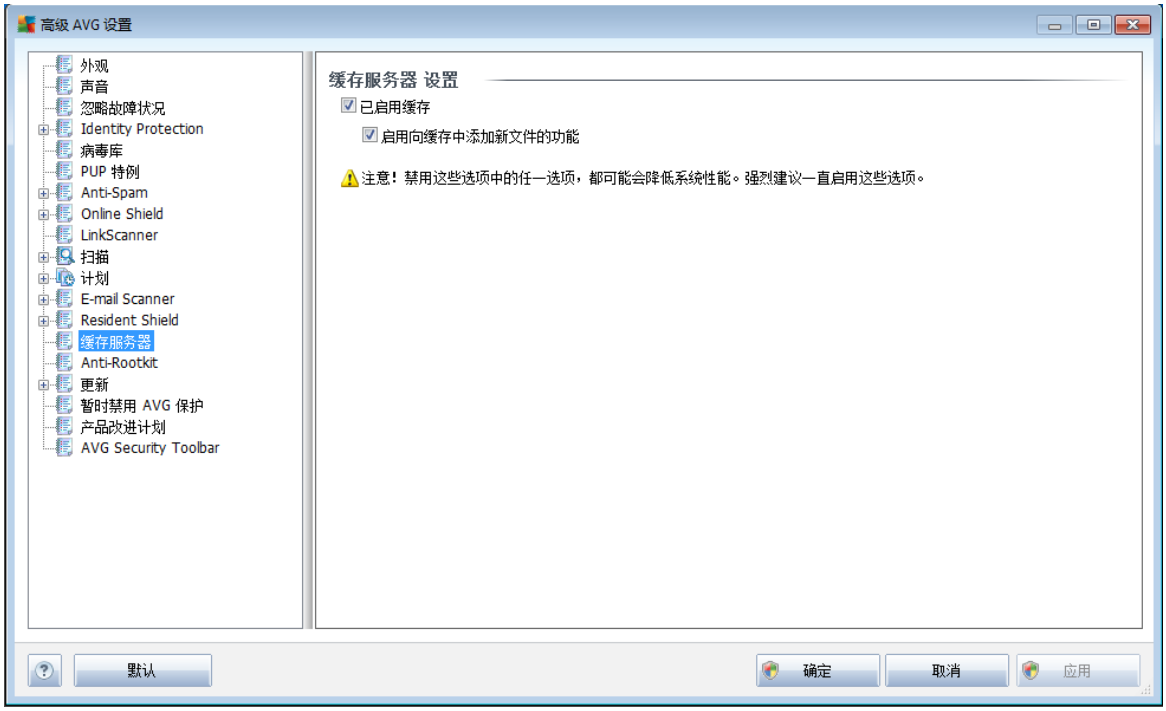
我们强烈建议，若非必要，不要排除任何项目！

此对话框提供了以下控制按钮：

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

11.9. 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。

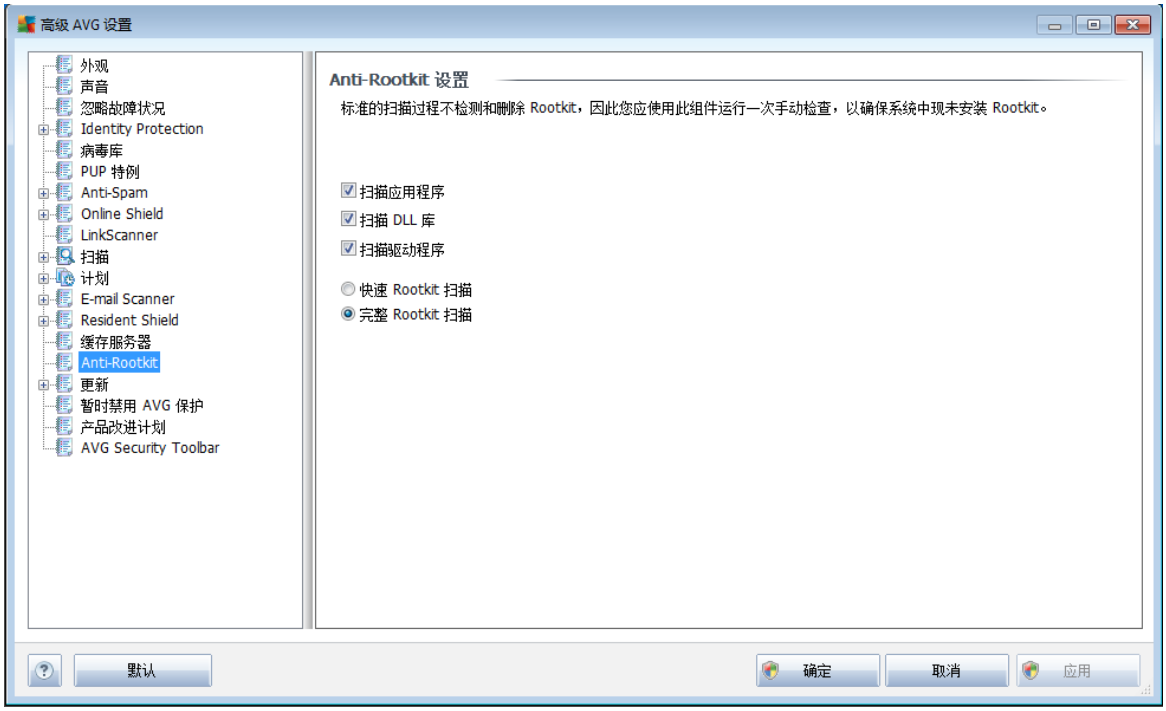


设置对话框中有两个选项：

- ***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。

11.10. 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。

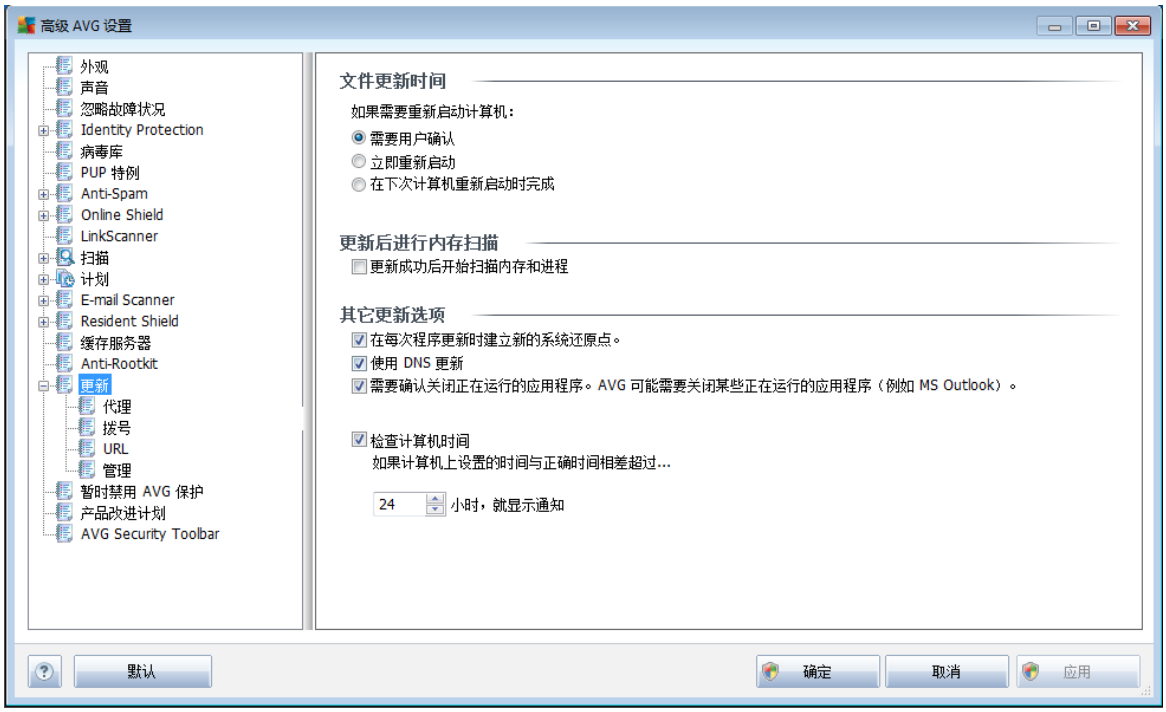
选中相应的复选框可指定应扫描的对象：

- ***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*）

11.11. 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

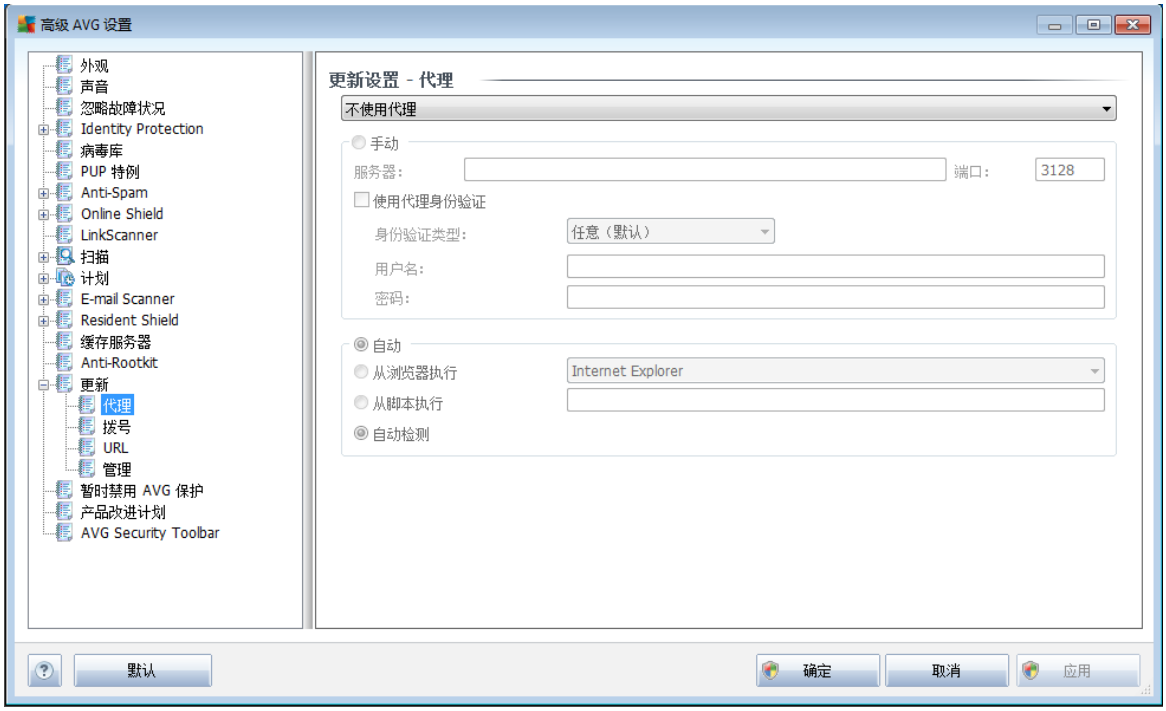
更新后进行内存扫描

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

- ***“在每次程序更新时建立新的系统还原点”*** – 在每次启动 AVG 程序更新前，都会创建一个系统还原点。万一更新过程失败并且您的操作系统崩溃，那么您始终都可以利用此还原点将您的操作系统还原成其原始配置。可通过“开始”/“所有程序”/“附件”/“系统工具”/“系统还原”访问此选项，但建议仅限经验丰富的用户进行任何更改！如果您要利用此功能，请将此复选框保持选中状态。
- ***“使用 DNS 更新”*** – 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。

11.11.1. 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*）

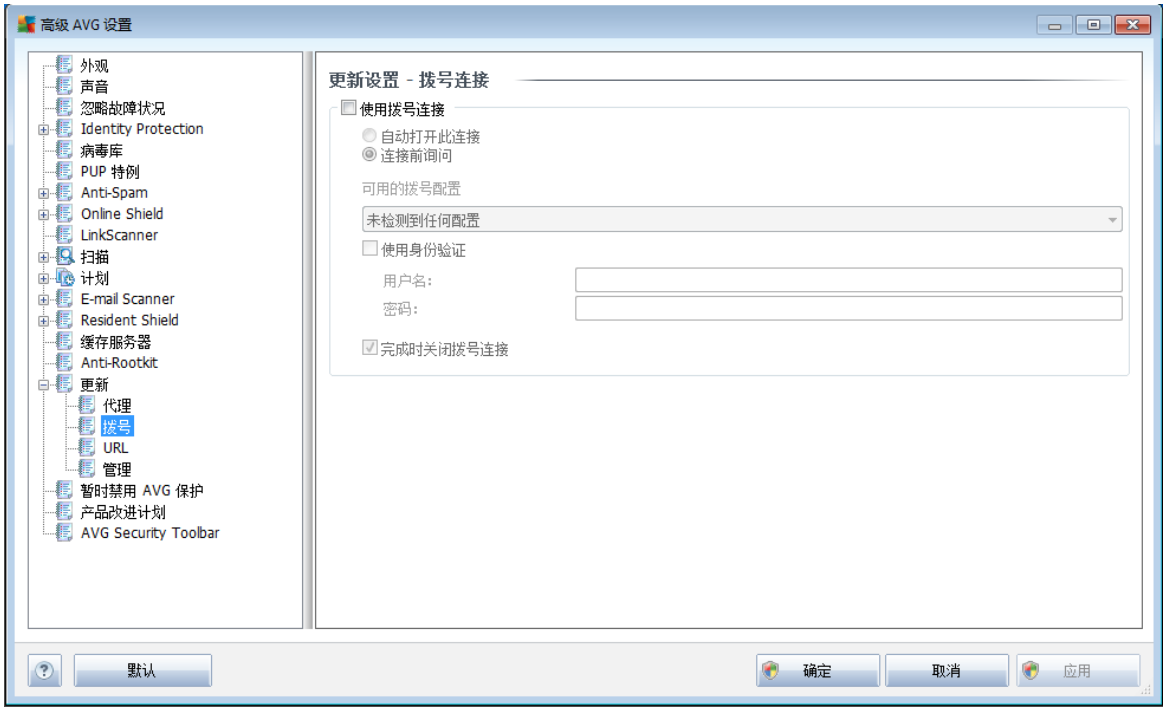
代理服务器也可以针对每个用户配置特定的规则。如果您的代理服务器是这样设置的，请选中 ***“使用代理身份验证”*** 选项以验证您的用户名和密码是否有效，即能否通过代理服务器连接到 Internet。

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

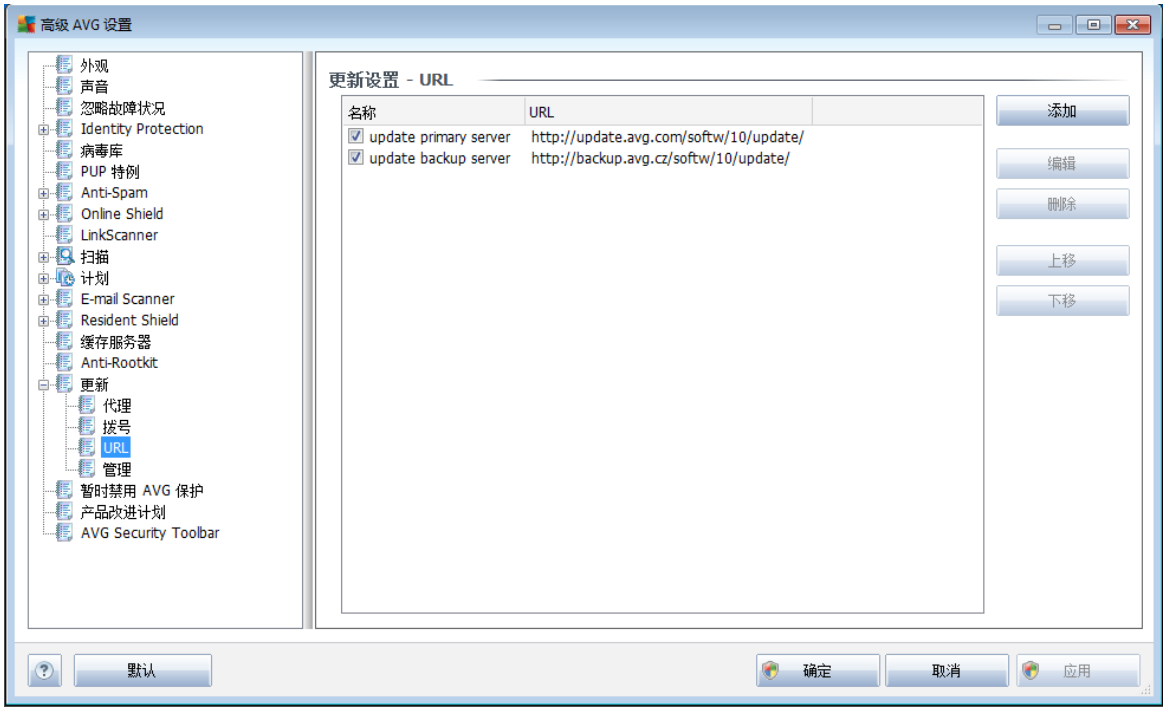
11.11.2. 拨号



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”***）。

11.11.3. URL

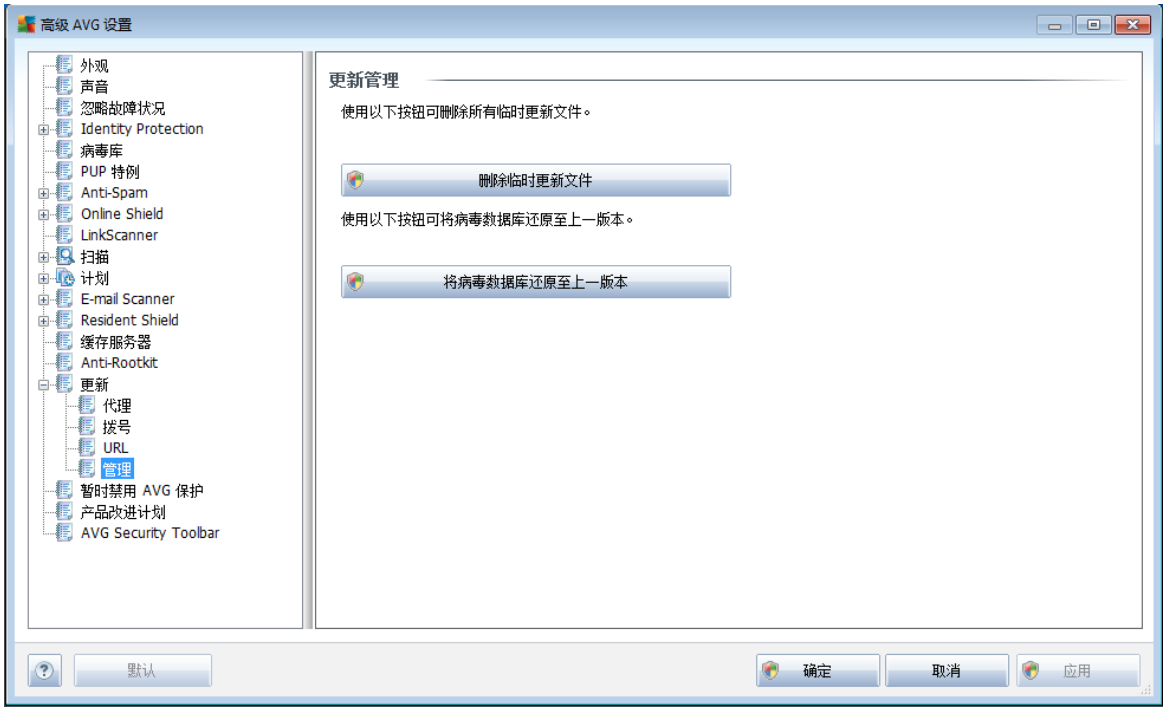


"URL"对话框提供了可从中下载更新文件的 Internet 地址列表。可以使用以下控制按钮修改此列表及其中的各项：

- ***"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

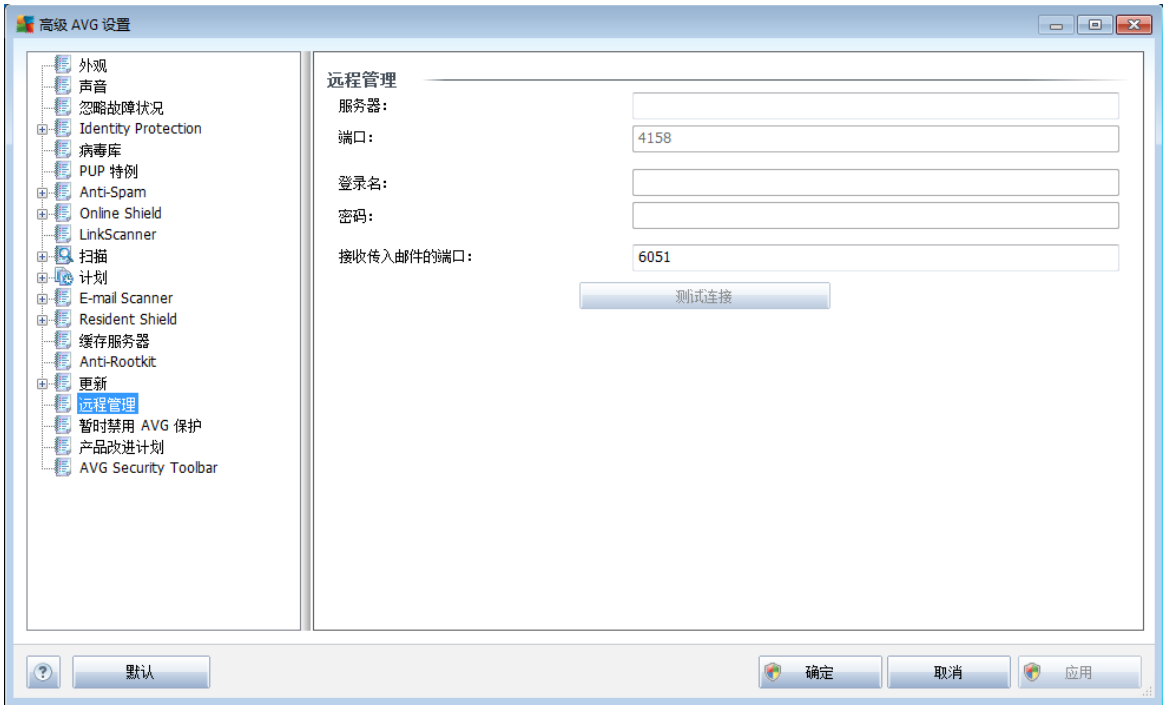
11.11.4. 管理

*“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* ）

11.12. 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

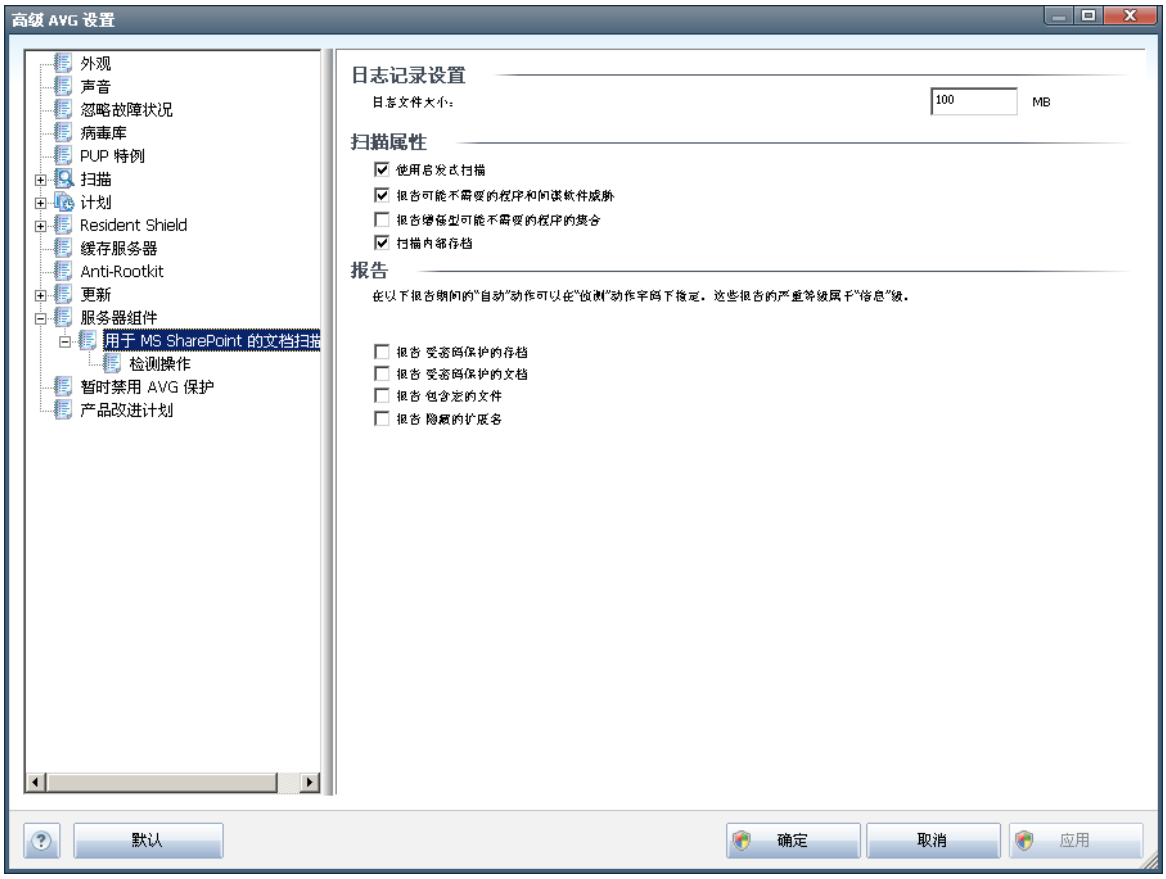
“测试连接” 按钮可帮助您验证所有上述数据是否有效以及能否用来成功连接到 DataCenter。

注意： *有关远程管理的详细说明，请参阅 AVG Business 版文档。*

11.13. 服务器组件

11.13.1. Document Scanner for MS SharePoint

在此对话框中，您将发现与 ***Document Scanner for MS SharePoint*** 文档病毒扫描性能相关的多个预设选项。此对话框分为若干区域：



日志记录设置

“日志文件大小”字段 - 日志文件中有各种 ***Document Scanner for MS SharePoint*** 相关事件的记录，如程序库加载说明、发现病毒事件、故障排除警告等记录。此文本字段用于设置该文件的最大大小。

扫描属性

- ***使用启发式扫描*** - 选中此框可在扫描文档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文档，还会检测文档的实际内容。
- ***报告可能不需要的程序和间谍软件威胁*** - 选中此框可使用 Anti-Spyware 引擎，即在扫描文档时检测和报告可疑和可能不需要的程序。
- ***报告更多可能不需要的程序*** - 选中此框可检测更多间谍软件：程序直接从制造商获得后极其安全而无害，但之后却能以不正当的方式使用以达到恶毒的目的，

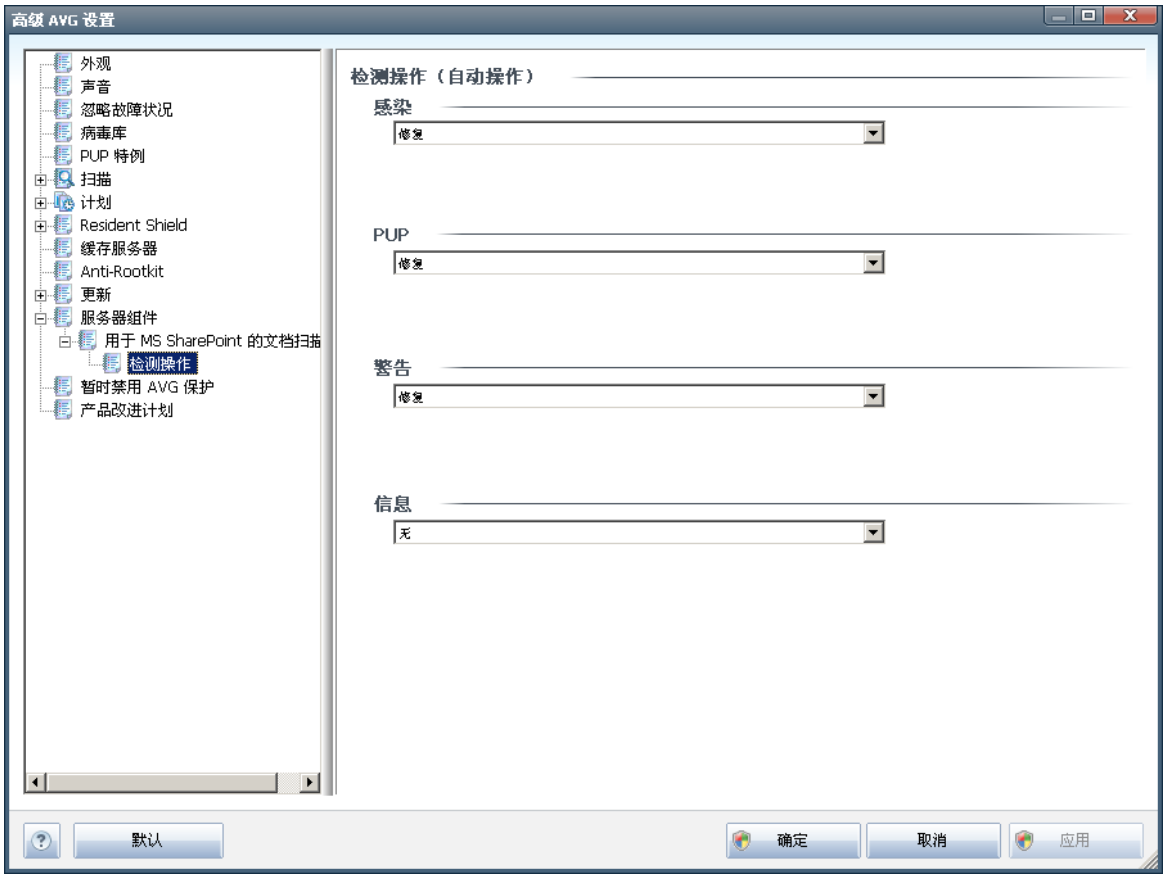
或者程序始终是无害的，但可能并不需要（各种工具栏等）。这项附加措施可以进一步提高计算机的安全性，但也可能会阻止合法程序，因此默认情况下已将其禁用。注意：该检测功能是以前选项中没有的，因此，如果要抵御基本类型的间谍软件，请始终选中以前的框。

- ***扫描内部存档*** - 选中此框可扫描存档的内容。

报告

- ***报告受密码保护的压缩包*** - 受密码保护的压缩包（ ZIP、RAR 等）不能进行病毒扫描；选中此框可将这类压缩包报告为有潜在危险。
- ***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。

11.13.2. 检测操作



在此对话框中，可以配置 ***Document Scanner for MS SharePoint*** 组件在检测到威胁时应有的行为方式。威胁分为多个类别：

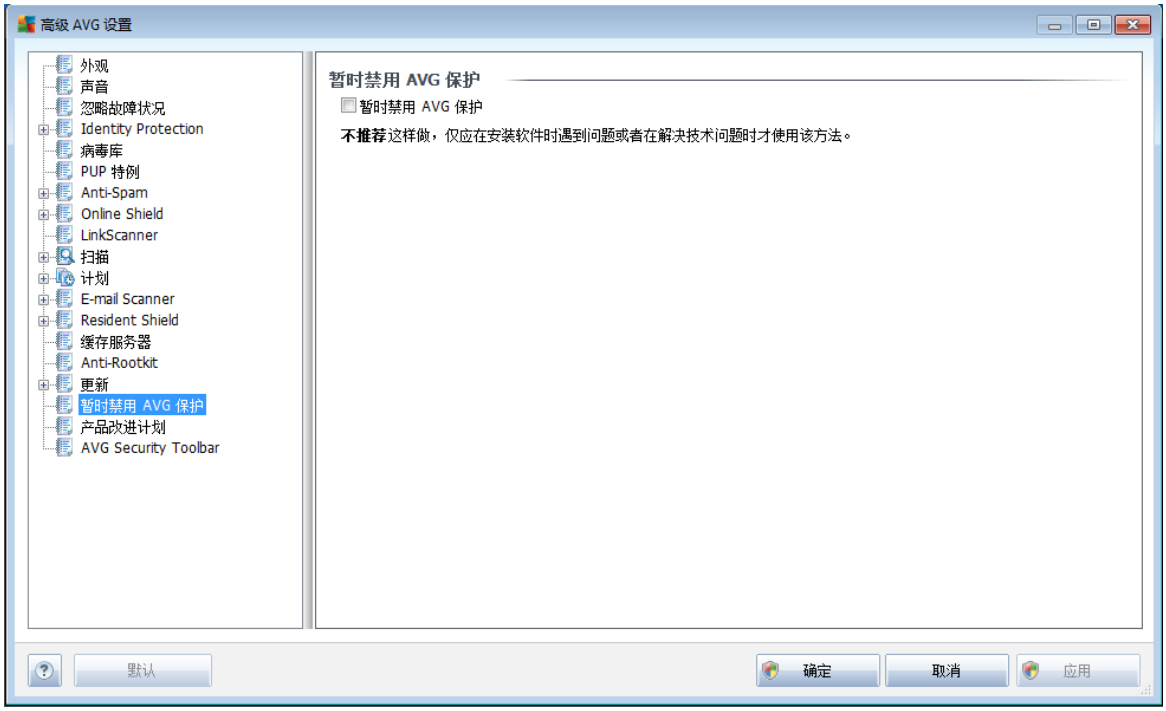
- ***感染*** - 自我复制和传播的恶意代码，通常直到造成破坏时才会被发觉。
- ***PUP（可能不需要的程序）*** - 一般而言，既包括确实威胁严重的程序也包括对您的隐私存在潜在威胁的程序。
- ***警告*** - 检测到无法扫描的对象。
- ***信息*** - 包括所有检测到但不能归入上述任何类别的潜在威胁。

请使用下拉菜单为每个类别选择自动操作：

- ***无*** - 将保留包含此类威胁的文档。
- ***修复*** - 尝试修复受感染的文件 / 文档。
- ***移至库*** *** - 将每个受感染的文档都移动到病毒库隔离环境中。

- ***删除*** - 将删除检测到病毒的文档。

11.14. 暂时禁用 AVG 保护



在***“暂时禁用 AVG 保护”***对话框中，您可以选择一次性关闭由 AVG File Server 2011 实施的整个保护。

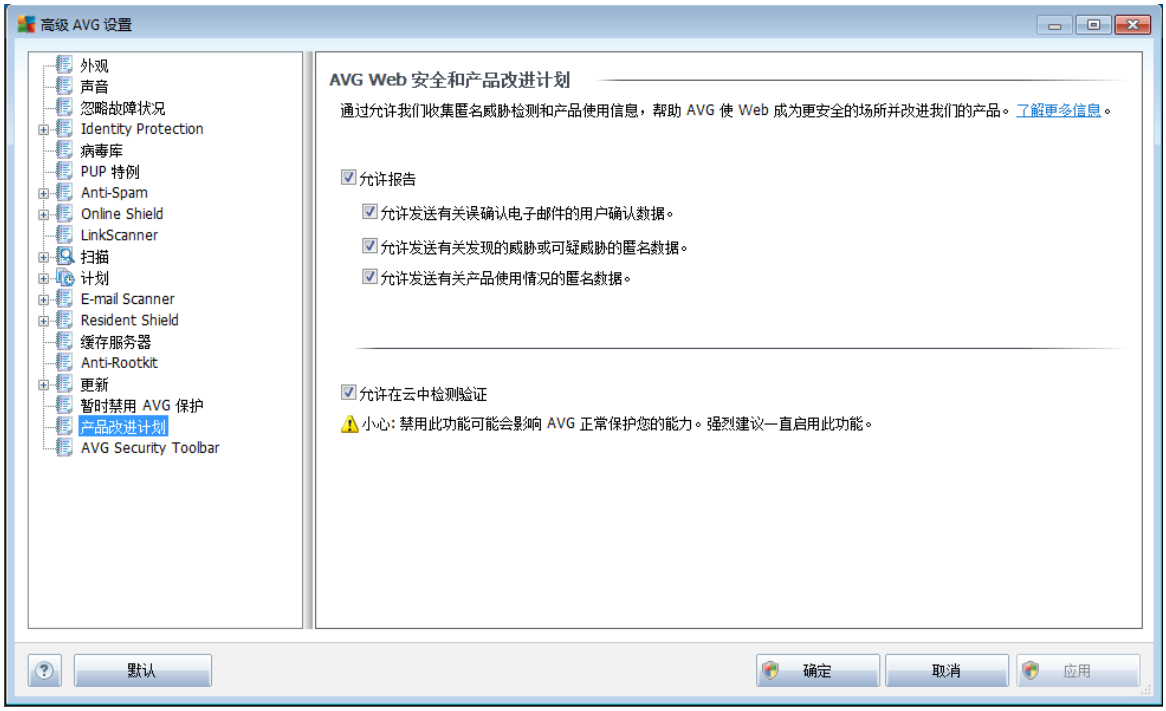
请记住，只有在绝对必要的情况下才使用此选项！

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

11.15. 产品改进计划

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

报告会自动进行，因此不会引起不便，也不会向报告中添加个人数据。 报告检测到的威胁是可选操作，但我们也确实希望您启用此功能，因为这有助于我们为所有 AVG 用户改善保护功能。



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

- ***病毒*** 是一种自我复制和传播的恶意代码，通常直到造成破坏时才会被发觉。有些病毒是严重的威胁，它们在传播途中会删除或有意更改文件；而有些病毒则会执行一些看似无害的操作，例如播放一段音乐。但所有病毒都有危险性，因为它们都有基本的繁殖能力。即使是一个简单的病毒也能很快耗尽所有计算机内存，从而造成崩溃。

- ***蠕虫*** 是病毒的一个子类别，与普通病毒不同的是，它不需要依附于一个“载体”对象；它将自身作为一个独立的对象发送到其它计算机（通常通过电子邮件发送），因此往往会造成电子邮件服务器和网络系统过载。

- ***间谍软件*** 通常被定义为一类包含程序（通常是特洛伊木马），旨在窃取个人信息、密码、信用卡号码或潜入计算机以使攻击者得以对其进行远程控制的恶意软件（*意软件 = 任何有恶意的软件，包括病毒*）；当然，所有这些行径都是在计算机所有者不知情或未同意的情况下实施的。

- ***可能不需要的程序*** 是一类间谍软件，它们可能但不一定会对您的计算机产生危险。广告软件就是 PUP 的一个具体例子，这种软件用于分发广告，分发途径通常是显示弹出广告；虽然惹人讨厌，但其实是无害的。

- _|∑□***跟踪 Cookie*** 视为一类间谍软件，因为这些小型文件（存储在 Web 浏览器中并在您再次访问其“父”网站时会自动发送至该网站）可能会包含诸如您的浏览历史记录等数据以及其它一些类似信息。

- ***漏洞利用*** 是一种恶意代码，它利用操作系统、Internet 浏览器或其它基本程序中的缺陷或漏洞进行攻击。

- ***网络钓鱼*** 试图通过假冒可靠的知名组织骗取敏感的个人数据。潜在受害者往往被大量的电子邮件诱入圈套，这些电子邮件要求他们执行银行帐户详细信息更新之类的操作。为执行这类操作，潜在受害者会受邀单击所提供的链接，然后就会被诱拐到假银行网站。

- ***愚弄邮件*** 通过大量含有危险、恐吓或只有骚扰和无用信息的电子邮件实施。以上所列的许多威胁都用“ 愚弄邮件 ”来传播。

- ***恶意网站*** 会故意在访客的计算机中安装恶意软件，已被攻陷的站点的行径完全一样，只是这些站点是已被传播威胁的访客侵入的合法网站。

为保护您免遭上述所有不同类型威胁的侵扰，AVG 包含了以下这些专用组件：

- ***Anti-Virus***，用来保护您的计算机免遭病毒入侵；

- ***Anti-Spyware***，用来防范计算机中的间谍软件。

12. AVG 扫描

扫描是 AVG File Server 2011 功能的关键组成部分。您可以运行按需测试或 安排它们 定期运行 （在方便的时间运行）。

12.1. 扫描界面

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

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

12.2.1. 扫描整个计算机

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

编辑扫描配置

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

- ***扫描参数*** - 在扫描参数列表中，您可以根据需要启用 / 禁用特定参数：

  - ***"自动修复 / 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。如果不能自动修复受感染文件，则会将受感染对象移到 ***病毒库*** 中。

  - ***"报告可能不需要的程序和间谍软件威胁"*** （*默认情况下已启用* ）- 选中此框可激活 ***Anti-Spyware*** 引擎以及针对间谍软件和病毒的扫描。 间谍软件属于疑似恶意软件类软件：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"*** （*默认情况下已禁用* ）- 选中此框可检测更多 间谍软件 ：程序直接从制造商处获得时极其安全而无害，但之后却可能被滥用以达到恶意目的。这项附加措施可以进一步提高计算机的安全性，但也可能会阻止合法程序，因此默认情况下已将其禁用。

  - ***"扫描跟踪 Cookie"***（*默认情况下已禁用* ）- ***Anti-Spyware*** 组件的此参数用于定义在扫描期间应检测 Cookie（*HTTP Cookie 用于验证、跟踪和维护有关用户的特定信息，例如网站首选项或电子购物车中的内容* ）。

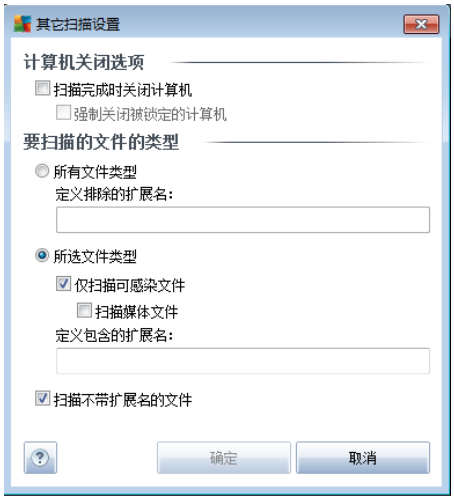
  - ***"扫描压缩包"*** （*默认情况下已禁用* ）- 此参数定义扫描时应检查存储在压缩包（如 ZIP 和 RAR 等）中的所有文件。

  - ***"使用启发式扫描"*** （*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。

- o ***“启动彻底扫描”*** *（默认情况下已禁用）* - 在特定情况下（*怀疑计算机受到感染*），您可以选中此选项以激活最全面的扫描算法，该算法甚至会对计算机上极难被感染的区域进行扫描以确保绝对安全。不过要记住，此方法相当耗时。

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



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

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

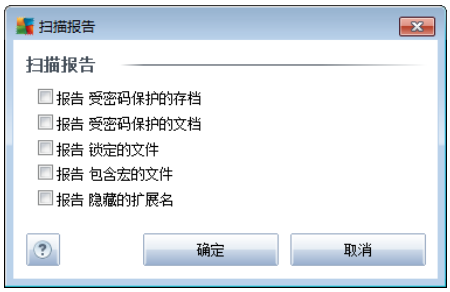
    - ➢ ***“所有文件类型”***，选择此选项可以通过列出不应扫描的文件扩展名（由逗号分隔）指定特例，不对其进行扫描；

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

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

- ***“调整扫描的完成速度”*** - 您可以使用滑块更改扫描进程的优先级。默认情况下，此优先级设置为 *“用户敏感信息”*优先级，该优先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，请单击 ***“开始扫描”***按钮，扫描过程本身与 “ 扫描整个计算机 ”基本上完全相同。

编辑扫描配置

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

- ***扫描参数*** - 在扫描参数列表中，您可以根据需要启用 / 禁用特定参数：

- ***“自动修复 / 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。如果不能自动修复受感染文件，则会将受感染对象移到 ***病毒库*** 中。

- ***“报告可能不需要的程序和间谍软件威胁”*** *（默认情况下已启用）* - 选中此框可激活 ***Anti-Spyware*** 引擎以及针对间谍软件和病毒的扫描。 间谍软件属于疑似恶意软件类软件：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”*** *（默认情况下已禁用）* - 选中此框可检测更多间谍软件：程序直接从制造商处获得时极其安全而无害，但之后却可能被滥用以达到恶意目的。这项附加措施可以进一步提高计算机的安全性，但也可能会阻止合法程序，因此默认情况下已将其禁用。

- ***“扫描跟踪 Cookie”*** *（默认情况下已禁用）* - ***Anti-Spyware*** 组件的此参数用于定义在扫描期间应检测 Cookie（*HTTP Cookie 用于验证、跟踪和维护有关用户的特定信息，例如网站首选项或电子购物车中的内容*）。

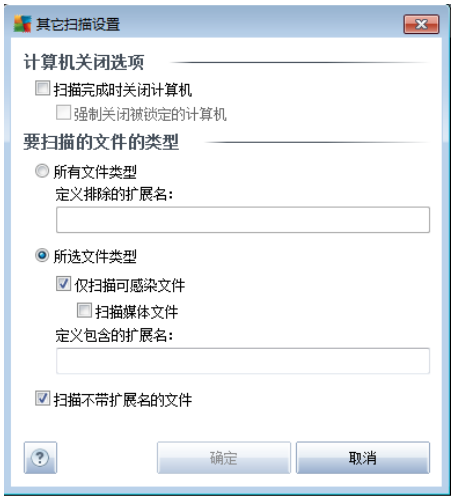
- ***“扫描压缩包”*** *（默认情况下已启用）* - 此参数定义扫描时应检查存储在压缩包（如 ZIP 和 RAR 等）中的所有文件。

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

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

- ***“启动彻底扫描”*** *（默认情况下已禁用）* - 在特定情况下（*怀疑计算机受到感染*），您可以选中此选项以激活最全面的扫描算法，该算法甚至会对计算机上极难被感染的区域进行扫描以确保绝对安全。不过要记住，此方法相当耗时。

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



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

- ***定义要扫描的文件类型*** - 应进一步决定要扫描的文件类型：

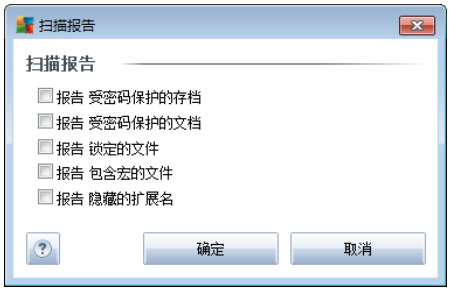
  - ***"所有文件类型"***，选择此选项可以通过列出不应扫描的文件扩展名（由逗号分隔）指定特例，不对其进行扫描；

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

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

- ***扫描进程优先级*** - 您可以使用滑块更改扫描进程的优先级。默认情况下，此优先级设置为 *"用户敏感信息"*级别，该级别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）。*

12.2.3. Anti-Rootkit 扫描

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

启动扫描

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

编辑扫描配置

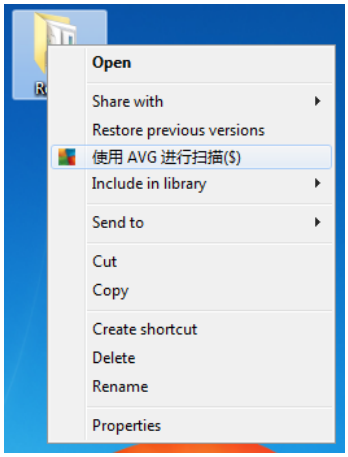
Anti-Rootkit 扫描 始终以默认设置启动，只能在 ***"AVG 高级设置 / Anti-Rootkit"*** 对话框中编辑相应的扫描参数。在扫描界面中，仅当正在扫描时才提供以下配置：

- ***自动扫描*** - 您可以使用滑块更改扫描进程的优先级。默认情况下，此优先级设置为中级（*"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*）。

- ***其它扫描设置*** - 该链接将打开新的 ***"其它扫描设置"*** 对话框，在此对话框中，您可以定义可能与 ***Anti-Rootkit 扫描*** 相关的计算机关机条件（***"扫描完成时关闭计算机"，或"强制关闭锁定的计算机"***）：

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 File Server 2011 还提供了直接在 Windows 资源管理器环境中快速扫描特定对象的选项。如果您要打开一个未知文件并且无法确定其内容，则您可能想在需要时对它进行检查。请按照以下步骤操作：



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

12.4. 命令行扫描

AVG File Server 2011 中有从命令行执行扫描的选项。例如，可以在服务器上使用此选项，或者在创建要在计算机启动后自动启动的批处理脚本时使用此选项。您可以使用 AVG 图形用户界面中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）
- ***/ARCBOMBSW*** 报告重新压缩的存档文件

12.5. 扫描计划

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

您应定期 ***扫描整个计算机***，至少每周一次。不过，如果可能，对整个计算机的扫描应每日进行一次 - 扫描计划的默认配置中便是这样设置的。 如果计算机“始终处于开机状态”，那么您可以将扫描安排在非工作时间运行 。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”*** ）；或定义确切的日期和时间（ ***“在特定的时间运行 ...”*** ）；也可以定义扫描启动操作应关联的事件（ ***“操作条件：计算机启动时”*** ）。

- ***“高级计划选项”*** – 在此区域中，可以定义当计算机处于省电模式或完全关闭时，应该 / 不应启动扫描的条件。

“计划的扫描设置”对话框中的控制按钮

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

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

- ***“取消”***– 取消您在此选项卡或此对话框的任何其它选项卡中所执行的任何更改并返回 AVG 扫描界面的默认对话框 。

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*** 引擎以及针对间谍软件和病毒的扫描。间谍软件属于疑似恶意软件类软件：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”***（*默认情况下已禁用*）：选中此框可检测更多间谍软件：程序直接从制造商处获得时极其安全而无害，但之后却可能被滥用以达到恶意目的。这项附加措施可以进一步提高计算机的安全性，但也可能会阻止合法程序，因此默认情况下已将其禁用。

- ***“扫描跟踪 Cookie”***（*默认情况下已禁用*）：***Anti-Spyware*** 组件的此参数用于定义应在扫描期间检测 Cookie（*HTTP Cookie 用于验证、跟踪和维护有关用户的特定信息，例如网站首选项或电子购物车中的内容*）。

- ***“扫描压缩包”***（*默认情况下已禁用*）：此参数定义扫描时应检查所有文件，即使这些文件被存储在某种压缩包（如 ZIP 和 RAR 等）内也不例外。

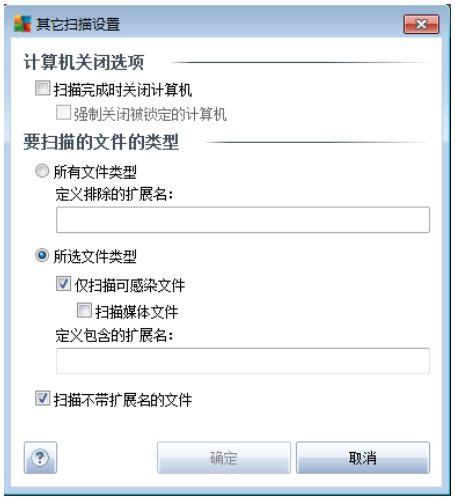
- ***“使用启发式扫描”***（*默认情况下已启用*）：启发式分析（*在虚拟的计算机环境中对已扫描对象的指令进行动态模拟*）将成为在扫描期间用来进行病毒检测的方法之一。

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

- ***“启动彻底扫描”***（*默认情况下已禁用*）- 在特定情况下（*怀疑计算机受到感染*），您可以选中此选项以激活最全面的扫描算法，该算法甚至会对计算机上极难被感染的区域进行扫描以确保绝对安全。不过要记住，此方法相当耗时。

接下来，您可以更改扫描配置，说明如下：

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



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

- ***定义要扫描的文件类型*** - 应进一步决定要扫描的文件类型：

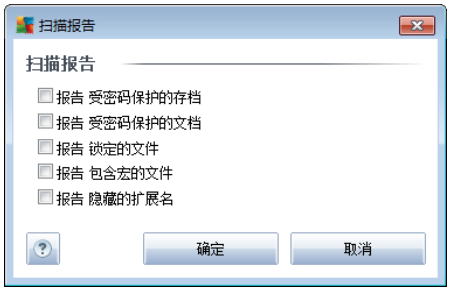
  - ***"所有文件类型"***，选择此选项可以通过列出不应扫描的文件扩展名（由逗号分隔）指定特例，不对其进行扫描；

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

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

- ***"调整扫描的完成速度"*** - 您可以使用滑块更改扫描进程的优先级。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
- ***程序文件***
    - C:\Program Files\
    - *在 64 位版本中为* C:\Program Files (x86)
- ***“我的文档”文件夹***
    - *对于 Win XP 为：* C:\Documents and Settings\Default User\My Documents\
    - *对于 Windows Vista/7 为：* C:\Users\user\Documents\
- ***共享文档***
    - *对于 Win XP* 为：C:\Documents and Settings\All Users\Documents\
    - *对于 Windows Vista/7* 为：C:\Users\Public\Documents\
- ***“Windows”文件夹*** - C:\Windows\
- ***其它***
    - *系统驱动器* - 装有操作系统的硬盘驱动器（通常是 C:）
    - *系统文件夹* - C:\Windows\System32\
    - *临时文件文件夹* - C:\Documents and Settings\User\Local\ (*Windows XP*)；或 C:\Users\user\AppData\Local\Temp\ (*Windows Vista/7*)
    - *Internet 临时文件* - C:\Documents and Settings\User\Local Settings\Temporary Internet Files\ (*Windows XP*)；或 C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files (*Windows Vista/7*)

“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
- __“Rootkit”__ – 仅当扫描期间检测到 Rootkit 的情况下，此选项卡才会显示

- ***信息*** **-** 仅当检测到某些潜在威胁但这些威胁不能划归为上述任何类别时，此选项卡才会显示；此时此选项卡会就检测结果提供一则警告消息。此外，此选项卡中也有关于无法对其进行扫描的对象（如受密码保护的存档）的信息。

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：

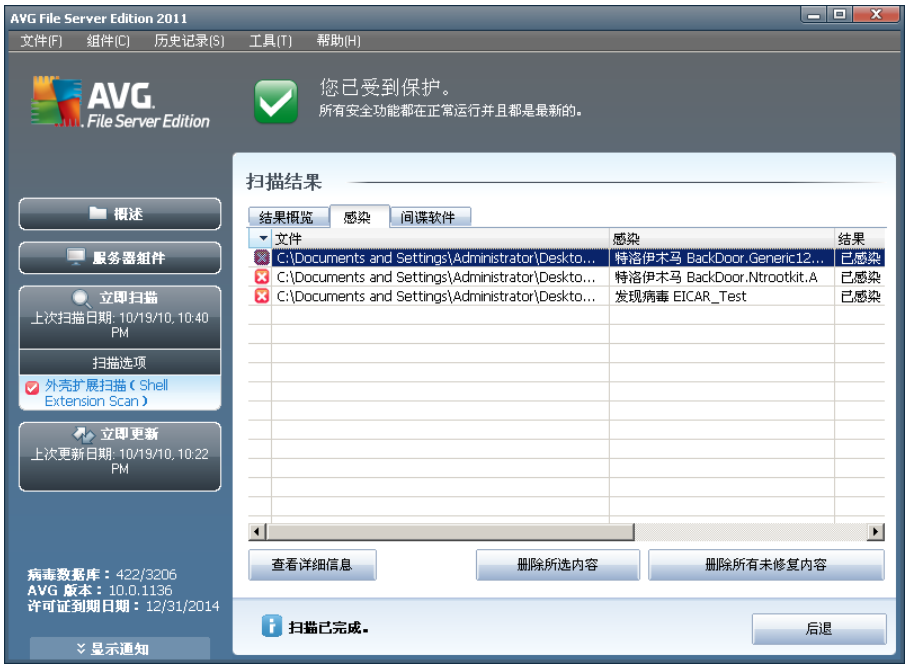
- 检测到的 病毒感染 /间谍软件
- 已删除的 病毒感染 /间谍软件
- 无法删除或修复的 病毒感染 /间谍软件 的数量

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：

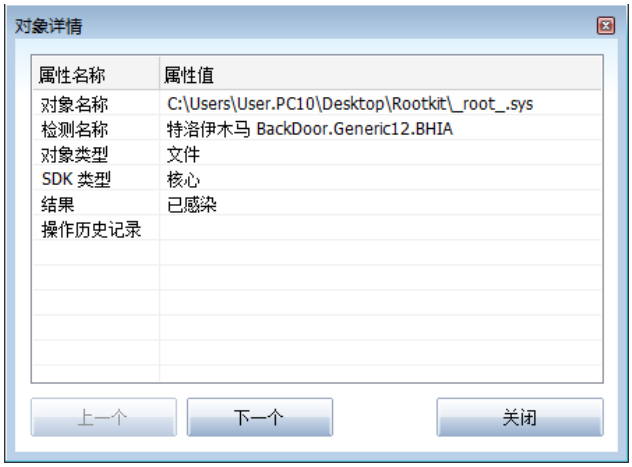
- ***“文件”***– 受感染对象原始位置的完整路径
- ***“感染”***– 检测到的 病毒 的名称（ *有关特定病毒的详细信息，请参阅在线 病毒百科全书*）
- ***“结果”***– 定义在扫描期间检测到的受感染对象的当前状态：
  - ***“已感染”*** – 已检测到受感染的对象并将其留在其原始位置（ *例如，如果您已在特定扫描设置中 关闭自动修复选项* ）
  - ***“已修复”*** – 已自动修复受感染的对象，并将其留在其原始位置
  - ***“已移至病毒库”*** – 已将受感染的对象移至 ***病毒库*** 隔离区
  - ***“已删除”*** – 已删除受感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

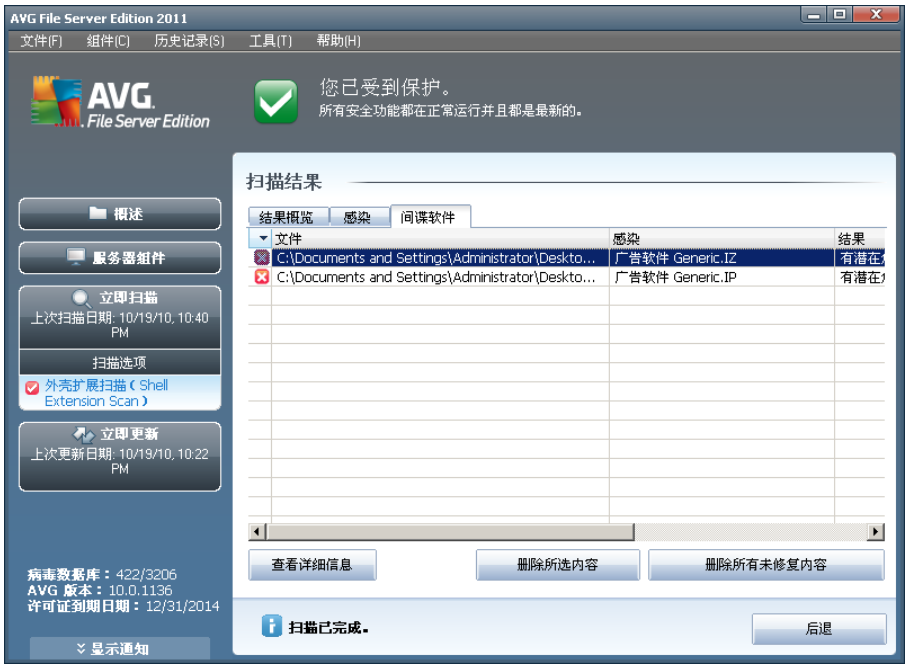
- ***“查看详细信息”*** - 此按钮用于打开一个名为 ***“详细对象信息”*** 的新对话窗口：



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

- ***“删除选定的感染对象”*** - 使用此按钮可将选定的发现结果移至 ***病毒库***
- ***“删除所有未修复的感染对象”*** - 此按钮会删除无法修复的所有发现结果，或将其移至 ***病毒库***
- ***“关闭结果”*** – 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：

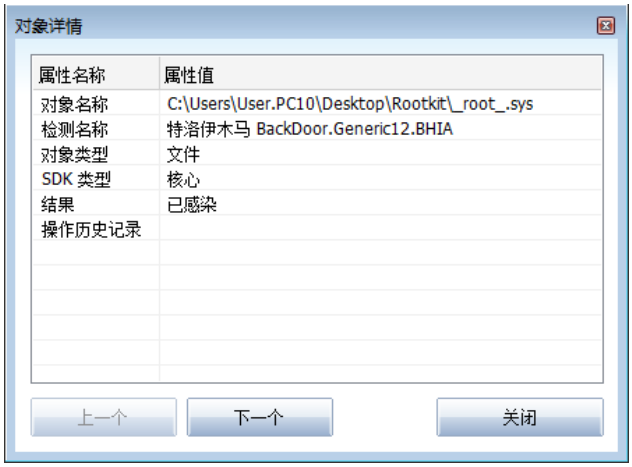
- ***“文件”***– 受感染对象原始位置的完整路径
- ***“感染”***– 检测到的 间谍软件 的名称（ *有关特定病毒的详细信息，请参阅在线* ***病毒百科全书*** ）
- ***“结果”***– 定义在扫描期间检测到的对象的当前状态：
  - ***“已感染”***– 已检测到受感染的对象并将其留在其原始位置（例如，如果您已在特定扫描设置中 关闭自动修复选项 ）
  - ***“已修复”***– 已自动修复受感染的对象，并将其留在其原始位置
  - ***“已移至病毒库”*** – 已将受感染的对象移至 ***病毒库 隔离区***
  - ***“已删除”***– 已删除受感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

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

控制按钮

此对话框中有三个控制按钮：

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



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

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

12.7.4. “警告”选项卡

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

Rootkit 是一种程序，旨在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

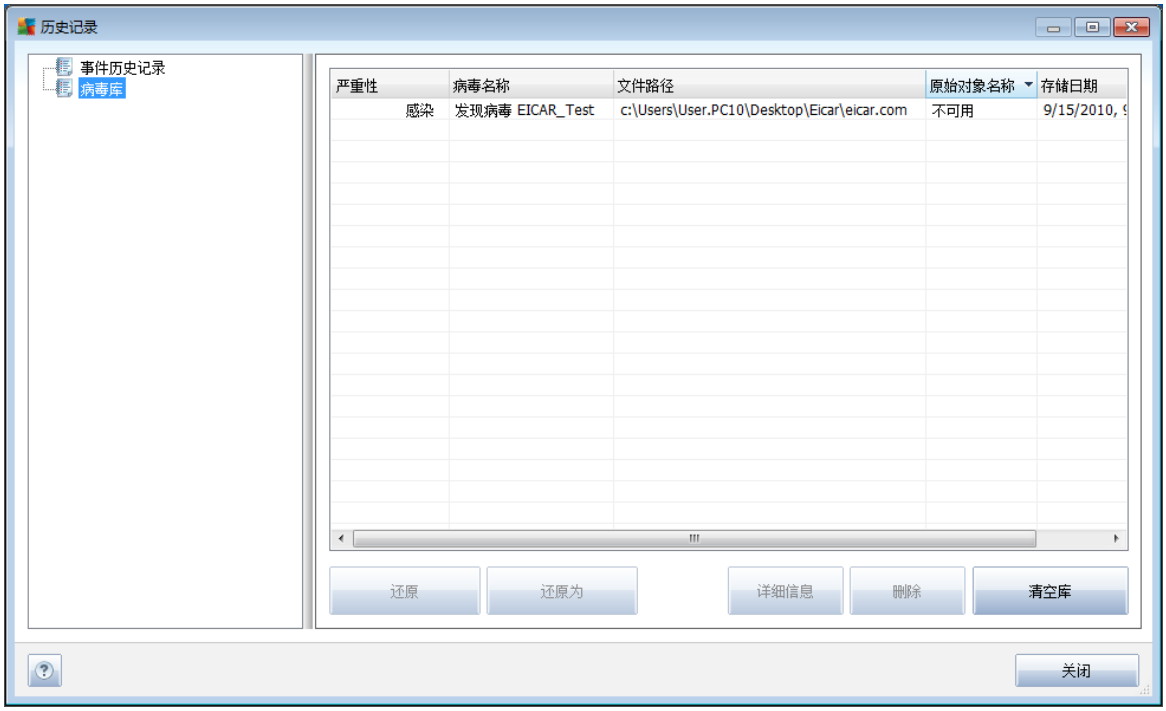
"信息"选项卡包含有关那些不能被归为感染、间谍软件等类别的 "发现结果" 的数据。它们不能被肯定地标记为危险，但仍值得您注意。 AVG 扫描功能可以检测到可能并未受感染但可疑的文件。会以 ***"警告"***或 ***"信息"***的形式报告这些文件。

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，以便您能确定不再需要将已删除的文件保留在其原始位置。如果发现该文件缺失会引起问题，则可发送受感染文件进行分析，或将其还原至原始位置。

病毒库 界面在一个单独的窗口中打开，概述了有关被隔离的受感染对象的信息：

- ***严重性*** - 指定 感染类型 （*基于其感染程度 - 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。
- ***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。通过从 ***病毒库*** 中删除文件，将会以不可还原的方式从磁盘中删除这些文件（*不是移动到回收站*）。

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。

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

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"*** 是可随时在需要时立即执行的一种 AVG 更新。
- ***计划更新*** - 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。

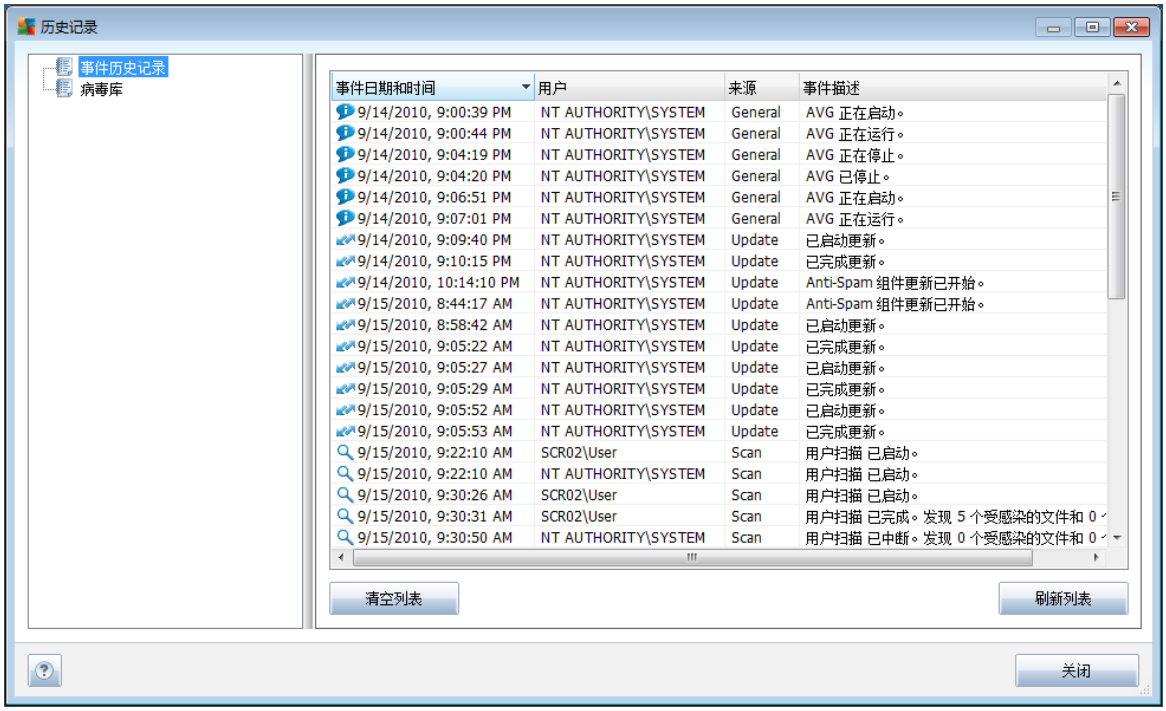
13.3. 更新过程

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



"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 File Server 2011 运行期间发生的重大事件的摘要。 ***"历史记录"*** 可记录以下类型的事件：

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

对于每个事件，将列出以下信息：

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

控制按钮

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

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。