AVG Protection

用户手册

文档修订 AVG.04 （2016/2/9）

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

目录

1. 简介 **4**

1.1 硬件要求 4

1.2 软件要求 4

2. AVG Zen **6**

2.1 Zen 安装过程 7

2.2 Zen 用户界面 8

2.2.1 类别拼贴图 *8*

2.2.2 设备区域 *8*

2.2.3 “消息”按钮 *8*

2.2.4 “状态”按钮 *8*

2.2.5 “升级/续订”按钮 *8*

2.2.6 “刷新”按钮 *8*

2.2.7 “设置”按钮 *8*

2.3 逐步指南 18

2.3.1 如何接受邀请 *18*

2.3.2 如何添加设备至您的网络 *18*

2.3.3 如何更改设备名称和类型 *18*

2.3.4 如何连接至现有 Zen 网络 *18*

2.3.5 如何新建 Zen 网络 *18*

2.3.6 如何安装 AVG 产品 *18*

2.3.7 如何离开网络 *18*

2.3.8 如何将设备从您的网络中移除 *18*

2.3.9 如何查看和/或管理 AVG 产品 *18*

2.4 常见问题解答和支持 31

3. AVG Internet Security **32**

3.1 AVG 安装过程 33

3.1.1 欢迎 *33*

3.1.2 安装 AVG *33*

3.2 安装后 34

3.2.1 病毒库更新 *34*

3.2.2 产品注册 *34*

3.2.3 访问用户界面 *34*

3.2.4 扫描整个计算机 *34*

3.2.5 Eicar 测试 *34*

3.2.6 AVG 默认配置 *34*

3.3 AVG 用户界面 36

3.3.1 上条导航 *36*

3.3.2 安全状态信息 *36*

3.3.3 组件概览 *36*

3.3.4 扫描/更新快速链接 *36*

3.3.5 系统托盘图标 36
3.3.6 AVG Advisor 36
3.3.7 AVG Accelerator 36
3.4 AVG 组件 44
3.4.1 计算机保护 44
3.4.2 Web 浏览保护 44
3.4.3 Identity Protection 44
3.4.4 电子邮件保护 44
3.4.5 Firewall 44
3.4.6 PC 分析器 44
3.5 AVG 高级设置 54
3.5.1 外观 54
3.5.2 声音 54
3.5.3 暂时禁用 AVG 保护 54
3.5.4 计算机保护 54
3.5.5 Email Scanner 54
3.5.6 Web 浏览保护 54
3.5.7 Identity Protection 54
3.5.8 扫描 54
3.5.9 计划 54
3.5.10 更新 54
3.5.11 特例 54
3.5.12 隔离区管理 54
3.5.13 AVG 自我防护 54
3.5.14 隐私首选项 54
3.5.15 忽略错误状态 54
3.5.16 Advisor - 已知网络 54
3.6 Firewall 设置 96
3.6.1 常规 96
3.6.2 应用程序 96
3.6.3 文件和打印机共享 96
3.6.4 高级设置 96
3.6.5 预定义网络 96
3.6.6 系统服务 96
3.6.7 日志 96
3.7 AVG 扫描 105
3.7.1 预定义扫描 105
3.7.2 扫描 Windows 资源管理器 105
3.7.3 命令行扫描 105
3.7.4 扫描计划 105
3.7.5 扫描结果 105
3.7.6 扫描结果详细信息 105
3.8 AVG File Shredder 126

3.9 隔离区管理 127
3.10 历史记录 128
3.10.1 扫描结果 *128*
3.10.2 Resident Shield 结果 *128*
3.10.3 Identity Protection 结果 *128*
3.10.4 电子邮件保护结果 *128*
3.10.5 Online Shield 结果 *128*
3.10.6 事件历史记录 *128*
3.10.7 Firewall 日志 *128*
3.11 AVG 更新 137
3.12 常见问题解答和技术支持 137

1. 简介

祝贺您购买了 AVG Protection 套装！使用此套装，您可享受 **AVG Internet Security** 的所有功能，现在还用 **AVG Zen** 进行了增强。

AVG Zen

这一价值非凡的管理工具可让您照管您及所有家人的设备。您的所有设备将整齐地列在一个地方，以便您可轻松地密切关注每个设备上的保护、性能和隐私状态。有了 **AVG Zen** 后，逐个对设备进行检查的日子终于可以结束了；您甚至可以远程运行扫描和维护任务并修复最紧急的安全问题。**AVG Zen** 直接内置在套装中，所以一开始就会自动运行。

单击此处以了解 AVG Zen

AVG Internet Security

这款安全应用程序屡获殊荣，为您在线所做的一切事情提供了多重保护，这也就意味着您无需再担心身份盗用、病毒或访问危险网站。其中包括 AVG 云保护技术和 AVG Community Protection Network，这意味着我们收集最新威胁信息并将其分享给我们的社区，以确保用户得到最严密的保护：您可安全地网上购物和办理银行业务，在社交网络上享受生活或使用具有实时保护的冲浪和搜索。

单击此处以了解 AVG Internet Security

1.1. 硬件要求

AVG Internet Security 的最低硬件要求：

- Intel Pentium 1.5 GHz 或更快
- 512 MB （Windows XP） /1024MB （Windows Vista、7和 8） RAM 内存
- 1.3 GB 可用硬盘空间 *（用于安装）*

AVG Internet Security 的推荐硬件要求：

- Intel Pentium CPU 1.8 GHz 或更快
- 512 MB （Windows XP） /1024MB （Windows Vista、7和 8） RAM 内存
- 1.6 GB 可用硬盘空间 *（用于安装）*

1.2. 软件要求

AVG Internet Security 用于保护运行以下操作系统的工作站：

- Windows XP Home Edition SP2

- Windows XP Professional SP2
- Windows XP Professional x64 Edition SP1
- Windows Vista（x86 和 x64，所有版本）
- Windows 7（x86 和 x64，所有版本）
- Windows 8 （x32 和 x64）
- Windows 10 （x32 和 x64）

（应用了更高 Service Pack 版本的特定操作系统可能也适用）

Windows XP x64 中不支持 Identity 组件。 在此操作系统上，您只能安装不带 ID Protection 组件的 AVG Internet Security。

2. AVG Zen

用户手册的本部分提供了 AVG Zen 的全面文档。请注意，此手册仅描述了本产品的 PC 版本。

AVG 为全球知名的安全软件开发商，现在仍继续朝着消费者的需求大步迈进，努力满足消费者的全部安全需要。新版 AVG Zen 在一个简单的软件包中，高效地从台式机连接至移动设备、数据和使用这些设备的人们，旨在让我们复杂的数字生活变得更简单。通过一个应用程序，AVG Zen 可让用户更轻松地在一个地点，即可查看所有设备的安全和隐私设置。

AVG Zen 背后的理念就是，让个人重新掌控其所有设备的数据和安全性。因为我们相信，只有掌控，才能带来更多选择。事实上，AVG 并不是要在这告知您共享或跟踪完全是坏事；相反，我们想要为客户提供信息，让他们能够掌控所分享的内容，并且在被跟踪时能够自己做出知情的决定。这个选择可以让他们自由选择所要的生活方式，并且在提及家庭或申请工作时无需担心隐私被侵犯。

AVG Zen 的另一个优点在于，它让客户在所有设备上均享有始终如一的用户体验。因此，即便是新手，也能快速了解如何轻松管理并保证其多个设备安全。至少，在如今这个复杂的世界，那是正在变得越来越简单的一件事。但是，最后也是最重要的是，AVG Zen 设计用于让客户在实际日常生活中安全无虞。Internet 已成为我们这个互连世界的中心，而 AVG Zen 则将这些点连接起来。

文档的此部分包含 AVG Zen 特定功能的描述。如果您需要了解有关 AVG 其他产品的信息，请查阅此文档的其他部分或其它的用户指南。可从 AVG 网站下载这些指南。

2.1. Zen 安装过程

使用下面的网页以购买和下载您的 AVG Protection 套件。 运行 AVG Internet Security安装程序；只需几个步骤，就可以轻松完成（点击此处查看更多相关信息）。 AVG Zen 作为该过程的一部分，也将被安装。 安装完成后，会立即出现 Zen 用户界面。 您也将被建议来创建新的 Zen 网络，或者加入现有的网络。 但是，并不强制您执行建议 -您可以跳过此建议，并在未来随时利用 Zen 网络连接。

您可能想要查看以下相关主题：

- 在 AVG Zen 中的三个用户模式是什么 ？
- 如何接受邀请？
- 如何连接至现有 Zen 网络？
- 如何新建 Zen 网络？

2.2. Zen 用户界面



这是您 AVG Zen 用户界面的主对话框。在每个其他对话框，始终显示有一个按钮 -单击即可返回至主屏幕（在一些后续对话框中，此按钮仅会退回至上一步，即退回至该系列对话框中的前一个）。

此对话框由几个不同的部分组成：

- 类别拼贴图
- 设备区域
- 消息按钮
- 状态按钮
- 升级/续订按钮
- 刷新按钮
- 设置按钮

2.2.1. 类别拼贴图



类别拼贴图让您可以安装 AVG 软件产品、查看其状态并轻松打开其用户界面。 Zen 网络管理员也可使用它们来查看和管理安装在远程设备上的 AVG 产品。 使用设备区域以浏览 Zen 网络中可用的远程设备。

在每个拼贴图中均会有一个圆圈，其颜色指示了此类别中产品的状态，您应该努力保持其显示为绿色。 对于某些类别，您可能只看到半圆，这表示您已安装该类别中的一个产品，但还有另一个要安装的产品。

尽管无论您查看的是何种设备，都会看到同一组拼贴图，但拼贴图的内容可能有所不同，具体取决于所监控设备的类型（PC、Android 或 Mac 设备）。

2.2.1.1. PC

保护

AVG Internet Security –此安全软件为您在线所做的一切事情提供多重保护，这就意味着您无需再担心身份盗用、病毒或访问危险网站。 其中包括 AVG 云保护技术和 AVG Community Protection Network，这意味着我们收集最新威胁信息并将其分享给我们的社区，以确保用户得到最严密的保护：您可安全地网上购物和办理银行业务，在社交网络上享受生活或使用具有实时保护的冲浪和搜索。

状态概况

- 如果未安装 AVG Internet Security，此拼贴图将一直显示为灰色，且下方文本显示为 "未受到保护"，但您只需一点即可安装此 AVG 应用程序。
- 如果需要注意的问题太多（如，当整个 AVG Internet Security 已禁用时），拼贴图中的圆圈会显示为红色且下方文本显示为 "未受到保护"。 如果只存在一些小问题，则拼贴图会显示为绿色，但下方文本显示为 "已部分受到保护"。 在这两种情况下，您都将会看到以橙色圆圈圈住的数字（在拼贴图的右上角），显示了您需要注意的问题数。 使用消息按钮以查看问题列表并尽可能解决它们。
- 如果 AVG Internet Security 未存在任何问题，则此拼贴图将显示为绿色且下方文本显示为 "已受到保护"。

单击此拼贴图后会发生什么：

- 如果尚未安装 AVG Internet Security –将会打开一个新对话框，可让您安装 AVG Internet Security。 阅读更多有关安装 AVG 产品的信息。
- 如果要查看安装有 AVG Internet Security 的自有设备 – 将打开 AVG Internet Security 用户界面。
- 如果您（作为管理员）要查看安装有 AVG Internet Security 的远程设备 –将打开一个对话框，显示远程设备上的 AVG Internet Security 的状态概况。 此对话框可让您执行多个远程操作，如运行扫描（**立即扫描**按钮）或进行更新（**更新**按钮）。 对于其它的远

程操作，如开启先前禁用的防护组件等，可通过单击**显示详细信息**按钮（这会打开当前所选设备的消息对话框）进行访问。 阅读有关查看和管理远程设备的更多信息。

性能

AVG PC TuneUp –使用此应用程序，您可恢复操作系统、游戏和程序的完整性能功能。 AVG PC TuneUp 也可自动运行重要的维护任务，如清理硬盘和注册表，或您也可手动运行这些任务。 AVG PC TuneUp 将快速识别您的系统中是否存在问题，并提供简单的解决方案。 您也可使用 AVG PC TuneUp 自定义您的 Windows 系统外观以满足您的个人需求。

状态概况

- 如果未安装 AVG PC TuneUp，此拼贴图将显示为灰色，且下方文本显示为 "未优化"，但您只需一点即可安装此 AVG 应用程序。
- 如果需要注意的问题太多（如，当整个 AVG PC TuneUp 已禁用），拼贴图中的圆圈会显示为红色且下方文本显示为 "未优化"。 如果只存在一些小问题，则拼贴图会显示为绿色，但下方文本显示为 "部分优化"。 在这两种情况下，您都将会看到以橙色圆圈圈住的数字（在拼贴图的右上角），显示了您需要注意的问题数。 使用消息按钮以查看问题列表并尽可能解决它们。
- 如果 AVG PC TuneUp 未存在任何问题，此拼贴图内的圆圈将显示为绿色且下方文本显示为 "已优化"。

单击此拼贴图后会发生什么：

- 如果尚未安装 AVG PC TuneUp –将会打开一个新对话框，可让您安装 AVG PC TuneUp。 阅读更多有关安装 AVG 产品的信息。
- 如果您要查看安装有 AVG PC TuneUp 的自有设备 – 将打开 AVG PC TuneUp 用户界面。
- 如果您（作为管理员）要查看安装有 AVG PC TuneUp 的远程设备 –将打开一个对话框，显示远程设备上安装的 AVG PC TuneUp 的状态概况。 此对话框可让您执行多个远程操作，如执行维护（**运行维护**按钮）或进行更新（**更新**按钮）。 其它的远程操作可通过单击**显示详细信息**按钮（这会打开当前所选设备的消息对话框）进行访问。 阅读有关查看和管理远程设备的更多信息。

隐私和身份

此类别由两个不同的部分组成 –AVG PrivacyFix（安全浏览器加载项）和 Identity Protection（AVG Internet Security 应用程序的一个组件）。 为了在此拼贴图中看到完整的（尽可能为绿色）圆圈，您需要安装这两个应用程序。

AVG PrivacyFix –此浏览器加载项可让您了解并控制数据收集。 只需点击一下，它即可检查您在 Facebook、Google 和 LinkedIn 上的隐私漏洞，并将您带到可进行修复的设置处。 阻拦了超过 1,200个跟踪者追踪您的在线动向。 您还可查看那些网站保留了售卖您个人数据的权利，并可轻松地要求其删除其保留的有关您的数据。 最后，当您访问网站时向您警告隐私风险，且当政策变更时会告知您。

AVG Internet Security –Identity Protection 组件 –此组件（AVG Internet Security 应用程序的一部分）可让您的计算机获得实时保护，抵御最新甚至未知的威胁。 它可监控所有进程（包括隐藏的进程）和数百种行为模式，并可确定您的系统中是否出现了恶意项。 因此，它甚至可以发现尚未在病毒数据库中描述的威胁。

状态概况

- 如果尚未安装上述任一应用程序，则此拼贴图会显示为灰色，且下方文本显示为"未安装"，但您只需一点即可安装这些 AVG 应用程序。
- 如果仅安装了这两个应用程序中的一个，则拼贴图中会显示为半圆。圆圈的颜色取决于所安装应用程序的状态 –可能为绿色（表示"激活"/"受保护"）或红色（表示"已禁用"/"未受保护"）。
- 如果两个应用程序均已安装，其中一个已激活，一个为禁用，则拼贴图中的圆圈会显示为红色，且显示文本"部分受保护"。
- 如果两个应用程序均已安装且激活，您将会在拼贴图中看到完整的绿色圆圈，文本显示为"受保护"。祝贺您！您的隐私和身份已完全安全！

单击此拼贴图后，将打开一个由两个额外拼贴图组成的新对话框 –一个为 AVG Identity Protection，另一个为 AVG PrivacyFix。这些拼贴图是 AVG Zen 应用程序主用户界面上的主拼贴图，属交互式且可点击项。

- 如果两个应用程序中有一个尚未安装，则您可单击**免费获取**按钮以进行修复。阅读更多有关安装 AVG 产品的信息。
- 如果至少有一个应用程序已安装，您单击其拼贴图以打开其用户界面。
- 如果您（作为管理员）要查看安装有这些应用程序的远程设备 –将打开一个对话框，其中包含了远程设备上这些应用程序的状态概况。但是，此对话框仅用作参考，您无法对其作出任何更改。阅读有关查看和管理远程设备的更多信息。

WEB TUNEUP

AVG Web TuneUp –此功能强大的浏览器插件完全免费，且可在 Chrome、Firefox 和 Internet Explorer 浏览器上运行。它会提醒您危险的站点并允许您阻止入侵式 web 跟踪器（通过向您显示哪些 Web 站点正在收集有关您在线活动的数据）。它还可快速轻松地清理您的在线跟踪，其中包括浏览和下载历史记录及 Cookie。

状态概况

- 如果未安装 AVG Web TuneUp，此拼贴图将显示为灰色，且下方文本显示为"未安装"，但您只需一点即可安装此 AVG 应用程序。*请注意，某些浏览器需要重新启动才能完成安装进程；有时您可能还必须允许直接在您的浏览器中进行安装。*
- 如果整个 AVG Web TuneUp 已禁用，则此拼贴图中的圆圈将显示为黄色且下方文本显示为"已禁用"。在这种情况下，您可点击此拼贴图并使用"在浏览器中打开"链接（或使用消息按钮）；然后您的浏览器会打开并且您将通读有关如何在您的浏览器中启用 AVG Web TuneUp 的说明。
- 如果 AVG Web TuneUp 浏览器插件已激活且未存在任何问题，则此拼贴图中的圆圈将显示为绿色且下方文本显示为"已启用"。

单击此拼贴图后会发生什么：

- 如果尚未安装 AVG Web TuneUp –将会打开一个新对话框，可让您安装 AVG Web TuneUp。阅读更多有关安装 AVG 产品的信息。
- 如果您在查看安装有 AVG Web TuneUp 的自有设备 –将打开 AVG Web TuneUp 概览，允许您查看个人隐私功能部件列表（***Site Safety***、***Do Not Track***、***Browser Cleaner*** 和 ***AVG Secure Search***），且它们是否已激活以及是否正在运行。您还可使用***在浏览器中打开***链接在您的当前默认 Web 浏览器中打开 AVG Web TuneUp 界面。
- 如果您（作为管理员）在查看安装有 AVG Web TuneUp 的远程设备 –将打开一个对话框，显示远程设备上安装的 AVG Web TuneUp 的状态概况。此对话框仅用作参考，您无法对其作出任何更改。如果有任何需要注意的问题，可使用**显示详细信息**按钮；

点击该按钮可打开当前所选设备的消息对话框。 阅读有关查看和管理远程设备的更多信息。

您可能想要查看以下相关主题：

- 如何安装 AVG 产品？
- 如何查看和 *或*管理 AVG 产品？

2.2.1.2. Android 设备

本手册仅针对 AVG Zen 的 PC 相关问题；但是，作为管理员，您可能看到网络中也会包含 Android？设备。此类情况下，当您看到这些设备中 类别拼贴图的内容有所变化时，请不要惊讶。

当前可用的 AVG 移动应用程序：

- ***AVG AntiVirus***（免费或付费版） –此应用程序可让您免遭有害病毒、间谍软件、恶意软件和文本消息的骚扰，并保证您的个人数据安全。使用此应用程序，您可以受到有效而易用的病毒和恶意软件保护，还有实时应用程序扫描程序、手机定位器、终止进程、应用程序锁定器和本地设备擦除，以帮助您免受隐私和在线身份方面的威胁。实时安全扫描软件可保护您免受下载的应用程序和游戏的威胁。
- ***AVG Cleaner***（免费版） –此应用程序可让您快速擦除并清理您的浏览器、通话记录和文本历史记录，还可在设备的内部存储器和 SD 卡中识别并移除不想要的应用程序缓存数据。它可显著地优化存储空间，以帮助您的 Android？设备实现更优的性能并运行更顺畅。
- ***AVG PrivacyFix***（免费版） –此应用程序为您提供了一种简单方式，可通过移动设备管理您的在线隐私设置。它可让您访问一个主仪表盘，快速而轻松地显示您在 Facebook、Google 和 LinkedIn 上分享的内容和分享的人。如果您想更改设置，则只需一点即可转至更改设置的位置。新的 WiFi 跟踪保护让您可以预先设置您所知道的 WiFi 网络，同意或停止您的设备在其它网络上被跟踪。

各类别如下：

保护

单击此拼贴图将显示与 **AVG AntiVirus** 相关的信息 –扫描和其结果及病毒定义更新等。作为网络管理员，您也可在远程 Android 设备上执行扫描（**立即扫描**按钮）或进行更新（**更新**按钮）。

性能

单击此拼贴图将显示与性能相关的数据，即，所激活的 **AVG AntiVirus** 性能功能（***终止进程***、***电池状态***、***数据计划***（仅限付费版）和***内存使用情况***，以及 **AVG Cleaner** 是否已安装且正在运行（包括相关的一些统计信息）。

隐私

单击此拼贴图将显示与隐私相关的数据，即，所激活的 **AVG AntiVirus** 隐私功能（***应用程序锁定***、***应用程序备份***和***电话和消息阻止程序***以及 **AVG PrivacyFix** 应用程序是否已安装且正在运行。

ANTI-THEFT

单击此拼贴图将显示与 **AVG AntiVirus** 的 ***防盗*** 功能相关的信息，可让您使用 Google Maps 来定位被盗的手机。如果在连接的设备上安装了 **AVG AntiVirus** 付费版 （**Pro**），则您还可以看到 ***相机陷阱*** 功能（可秘密拍下尝试解开手机锁定的人的照片）、***设备锁定*** 功能（一旦更换 SIM 卡，则用户可以锁定该移动设备）。

您可能想要查看以下相关主题：

- 如何将您的 Android 移动设备连接至现有 Zen 网络？
- 如何查看和/或管理 AVG 产品？

2.2.1.3. Mac 设备

本手册仅针对 AVG Zen 的 PC 相关问题；但是，作为管理员，您很有可能看到网络中也会包含 Mac 设备。此类情况下，当您看到这些设备中 类别拼贴图的内容有所变化时，请不要惊讶。

当前可用的 AVG Mac 应用程序（仅提供英文版）：

- ***AVG AntiVirus***（免费） –这款功能强大的应用程序让您可以扫描特定的文件或文件夹以查看是否存在病毒或其他威胁，甚至只需一点即可对您整个 Mac 运行彻底扫描。同时也可提供实时保护，在后台静默运行。将会自动扫描您所打开、复制或保存的每个文件，而不会拖慢您的 Mac 速度。
- ***AVG Cleaner***（免费） –此应用程序让您可清理所有不必要的垃圾，如缓存和垃圾文件、下载文件历史记录和垃圾内容等，从而可释放空间。同时还可在硬盘上查找重复文件并快速删除不必要的副本。

各类别如下：

保护

单击此拼贴图将显示与 **AVG AntiVirus** 相关的信息 –扫描和其结果及病毒定义更新等。您还可查看实时保护是否已激活或已关闭。作为网络管理员，您也可更新远程设备上的 AVG AntiVirus（**更新** 按钮），或开启先前禁用的实时防护（可通过消息对话框进行操作，该对话框通过单击 **显示详细信息** 按钮进行访问）。阅读更多有关查看和管理远程设备的信息。

性能

单击此拼贴图会显示性能相关数据，即有关 **AVG Cleaner** 两个组件 –***Disk Cleaner*** 和 ***Duplicate Finder*** –的数据。您可查看上次测试这些性能功能的时间及结果。

您可能想要查看以下相关主题：

- 如何将您的 Mac 连接至现有 Zen 网络？
- 如何查看和/或管理 AVG 产品？

2.2.2. 设备区域



AVG Zen 用户界面的此部分显示了您 Zen 网络中所有可用的设备。 如果您是单个用户或仅连接至某人的 Zen 网络，则您只能看到一个设备，即您当前所用的设备。 但是，如果作为管理员连接，则可查看的设备可能会很多，需要使用箭头按钮进行浏览。

单击其拼贴图以选择要查看的设备。 您将会看到类别部分发生相应变化，显示了所选设备上的 AVG 产品状态。 您可能也会注意到在一些拼贴图的右上角显示了很多以橙色圆圈圈住的数字。 这表示此设备上的 AVG 产品中出现了问题，需要引起您的注意： 单击消息按钮以获取更多信息。

作为 Zen 网络管理员，您还可能想要添加新设备至您的网络。 为此，请单击设备区域右边的  按钮。 受邀设备会立即显示在设备区域中；但保留为未激活（处于等待中状态）等待其用户接受邀请。

您可能想要查看以下相关主题：

- 如何添加设备至您的网络？
- 如何将设备从您的网络中移除？
- 如何接受 Zen 网络邀请？

2.2.3. “消息”按钮



此按钮位于设备区域的上方，状态按钮的左侧。但是，仅当您当前设备上的 AVG 产品出现问题时，此按钮才会显示。橙色圆圈中的数字表示您可能需要注意的问题数（此橙色圆圈可能会包含感叹号，警告一些 AVG 应用程序已完全被禁用）。

作为网络管理员，您还可通过单击**显示详细信息**按钮（在类别拼贴图视图中）访问远程设备上的***消息对话框***。请注意，此按钮仅在出现需要您注意的紧急事项时才可用。单击此处以阅读此操作和其它远程管理操作的相关信息。

单击此按钮后，将显示一个新对话框：



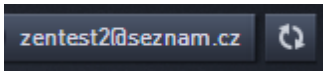
此对话框显示了按产品类别分类的问题列表。将用不同的颜色（红色、黄色或绿色）显示问题，从而区分紧急问题与相对不紧急的问题。

如果您是具有多个设备的网络的管理员，则此对话框的外观会稍有不同。左边有一个设备概况，让您可查看仅与此特定设备相关的消息。但是，如果您想在一个有序列表中查看所有设备的消息，您可选择***所有设备***选项（该选项位于概况的最上方）。

也可直接从此对话框中处理一些问题 –这些问题旁会显示一个特别操作按钮（大部分为**立即修复**）。作为网络管理员，您可远程直接从您的 AVG Zen 修复这些问题。作为单个用户或已连接用户，您只能管理您自己设备上的 AVG 产品，但仍无需打开各个应用程序的界面 – 这更便于同时查看所有的问题。

例如，如果您看到 ***"需要重新启动 Firewall - 要激活 Firewall，请重启您的计算机"*** 文本，则可以单击**立即重新启动**按钮。您的电脑将会立即重启以激活 Firewall 组件。

2.2.4. "状态"按钮



此按钮显示当前的用户模式。作为 Zen 网络管理员，通常您将看到您用于连接至网络的 MyAccount 电子邮件。

单击此按钮后，将显示一列其它操作。可用的操作取决于您当前所用的用户模式：

作为单个用户：

- **连接** - 让您连接至 Zen 现有网络（或新建一个）。

- **访问 AVG MyAccount** - 将启动您的浏览器并打开 https://myaccount.avg.com/ 网站，让您登录至 AVG MyAccount。

作为已连接的用户：

- **以管理员身份登录** - 单击以获得管理员权限，让您可查看并管理此 Zen 网络（要求进行登录）。
- **离开此网络** - 单击以离开此 Zen 网络（要求进行确认）。
- **了解更多信息** - 显示一个参考对话框，显示关于您当前所连接 Zen 网络及其管理员的信息。
- **访问 AVG MyAccount** - 将启动您的浏览器并打开 https://myaccount.avg.com/ 网站，让您登录至 AVG MyAccount。

作为管理员：

- **以管理员身份登出** - 单击以放弃您的管理员权限并成为该 Zen 网络内的已连接用户。
- **访问 AVG MyAccount** - 将启动您的浏览器并打开 https://myaccount.avg.com/ 网站，让您登录至 AVG MyAccount。

AVG MyAccount 是什么？

AVG MyAccount 是来自 AVG 的免费网络（云）服务，让您可以：

- 查看您已注册的产品和许可证信息
- 轻松续订您的订购并下载产品
- 检查过去的订单和发票
- 管理您的个人信息和密码
- 使用 AVG Zen

AVG MyAccount 可直接在 https://myaccount.avg.com/ 网站上进行访问。

2.2.4.1. 三个用户模式

在 AVG Zen中，一般有三个用户模式。**状态按钮**中显示的文本取决于您使用的用户模式：

- **单个用户**（状态按钮显示***连接***）- 您刚刚安装了 AVG Zen。您并非 AVG MyAccount 管理员，也未连接至任何网络，因此您只可查看和管理此设备上安装的 AVG 产品。
- **已连接用户**（状态按钮显示***已连接***）- 您已使用配对代码，因此接受邀请以连接至某人的网络。现在，此网络的管理员可查看和管理您设备上所有的 AVG 产品。对于您自己来说，您仍可查看并管理此设备上的 AVG 产品（就如单个用户一样）。如果您不想再停留在某一网络中，您可轻松地离开此网络。
- **管理员**（状态按钮显示 ***AVG MyAccount 名称***）- 您已使用您的 MyAccount 登录（可能您先前已新建一个）。这意味着您可以访问所有的 AVG Zen 功能。您可添加设备至您的网络、远程查看上面安装的 AVG 产品，并在需要时可从您的网络移除它们。您甚至可在连接的设备上执行各种远程操作。

您可能想要查看以下相关主题：

- 如何接受邀请？

- 如何连接至现有 Zen 网络？
- 如何新建 Zen 网络？
- 如何离开某一网络？
- 如何查看和/或管理 AVG 产品？

2.2.5. “升级/续订”按钮



单击此小按钮（位于状态按钮的右边）在您 Web 浏览器中打开 AVG 在线商店：

- 如果您当前使用的是免费 AVG 软件，但希望尝试其他功能以及仅在付费版本上可用的功能，您可使用该商店为您购买一年或两年订阅。
- 如果您当前使用的是付费 AVG 软件，但您的订阅即将到期（或已到期），您可使用该商店进行续订。

请注意，为了激活您新购买的（或续订的）订阅，必须登录到您的 AVG MyAccount。

2.2.6. “刷新”按钮



单击此小按钮（位于升级/续订按钮的右边），将立即刷新所有设备和类别的所有数据。例如，如果某些新添加的设备未显示在设备区域中，但您知道它已连接且想要查看其详细信息时，此按钮可能会有用。

2.2.7. “设置”按钮



单击此小按钮（位于刷新按钮的右边），将会弹出一个小对话框：

- 您可单击 ***设备设置***选项以打开设备设置对话框，让您可针对您的设备（及Zen网络中的其它设备，如果存在且您是此网络管理员）更改名称和类型。此对话框让您从您的网络中移除设备。



- 点击 ***在线支持*** 选项，在网页浏览器中打开 AVG 支持中心；如果您需要有关 AVG 产品的任何帮助，请在此包含广泛信息的 Web 站点查找即可。
- 点击 ***帮助*** 选项为您提供访问该程序的帮助（您也可以随时通过按 **F1** 键打开帮助窗口）。
- 最后，您也可点击 ***关于 AVG Internet Security*** 选项以查看关于您软件产品的信息，或甚至阅读许可协议。

您可能想要查看以下相关主题：

- 如何更改设备名称和类型？
- 如何将设备从您的网络中移除？

2.3. 逐步指南

本章节包含了一些描述 Zen 环境中最常见操作的逐步指南。

2.3.1. 如何接受邀请？

如果您在多个设备上使用 AVG 产品，或可能不是很熟练而希望其他人可以帮助您监控您的 AVG 产品并修复任何问题，您可能需要将您的 PC 或 Android？移动设备连接至一些现有的 Zen 网络。但是，首先，您需要收到来自所加入网络的管理员的邀请。因此，请联系管理员以向您发送邀请电子邮件。收到邮件后，打开后将会发现其中包含的**邀请代码**。

接下来要执行的步骤取决于您要添加的是 PC 还是 Android？移动设备：

PC 设备：

1. 安装 AVG Zen（如果未曾执行此步骤）。

2. 单击状态按钮（显示有***连接***文本）并通过在弹出的小窗口中单击***继续***按钮以确认。

3. 选择新打开的子对话框中左边的***使用邀请代码连接***窗格。



4. 使用复制粘贴法从电子邮件中复制邀请代码并粘贴至 Zen 子对话框中相应的文本字段中（或者手动输入）。

复制粘贴法是一个常见过程，可让您将任何可复制项（文本、图片等）输入至 Windows 剪贴板，然后再将其粘贴到其它位置。其工作方式如下：
i. 突出显示一段文本（此种情况下，为电子邮件中的邀请代码）。这一步可通过按着鼠标左键或按住 Shift 键选择实现。
ii. 在键盘上按下 ***Ctrl+C***（注意：在此阶段，不会有任何提示告知您已成功复制该文本）。
iii. 转至所需要的地点（此种情况下，为 **Zen 加入网络**对话框），然后单击一下要粘贴该文本的文本框。
iv. 按 ***Ctrl+V***。
v. 这样，将显示已粘贴的文本（此种情况下，为电子邮件中的邀请代码）。一切搞定。

5. 单击**连接**按钮。一会儿后，您将会成为Zen所选网络的成员了。对您个人来说，实际上没有什么发生改变（只有您状态按钮将会更改为***已连接***）。但是，您的设备从此将会受网络管理员监控，从而让他识别可能的问题并帮助您进行修复。但是，如果您想要离开此网络，您可随时轻松离开。

Android 移动设备：

与在 PC 设备上不同，Android 移动设备上的网络连接将会直接在应用程序中执行：

1. 首先，您需要安装一个 AVG 移动应用程序，从而连接至一些 Zen 网络（单击此处以了解关于您 Android？移动设备连接至现有 Zen 网络的更多信息）。事实上，在移动设备上接受一个邀请即意味着您离开当前的 Zen 网络并转换至一个新网络。

2. 打开您的应用程序，点击主屏幕左上角的***菜单图标***（即应用程序的徽标）。

3. 显示了菜单后，点击**管理设备**选项。

4. 点击屏幕底端的**加入另一 Zen 网络**选项，然后输入此网络管理员之前发送给您的邀请代码并点击**加入**。

5. 祝贺您！您现在已成为 Zen 网络的成员。但是，如果您改变了想法，也可随时轻松离开此网络。

Mac 设备：

与在 PC 设备上不同，Mac 设备上的网络连接将会直接在应用程序中执行：

1. 首先，您需要安装一个 AVG Mac 应用程序，甚至可能已连接至一些 Zen 网络（单击此处以了解关于您 Mac 设备连接至现有 Zen 网络的更多信息）。如果已连接，请单击应用程序屏幕右上角的按钮（当前显示"已连接"）并从下拉菜单中选择**离开此网络**。

2. 应用程序屏幕右上角的按钮当前显示"未连接"。单击该按钮并从下拉菜单那中选择**连接**选项。

3. 在新打开的对话框中，单击最右边的选项**使用邀请代码**。

4. 此时将会显示一个文本框，您可在其中输入本网络管理员先前发送给您的邀请代码。输入该代码后，单击**连接**按钮。

5. 祝贺您！您现在已成为 Zen 网络的成员。但是，如果您改变了想法，也可随时轻松离开此网络。

2.3.2. 如何添加设备至您的网络？

1. 要添加新设备至您的 Zen 网络，您首先需要邀请该设备。为此，请单击设备区域右边的  按钮。

请注意，只有管理员才能够发送邀请并将设备添加至其网络。因此，如果当前未连接至任何 Zen 网络，请执行此操作，或为您自身创建一个新网络。

2. 将显示一个新对话框。通过突出显示对应的拼贴图来选择要添加的设备类型（即 PC 或 Android？移动设备），然后单击**继续**按钮。



3. 将显示另一对话框。输入新设备上使用的电子邮件地址，然后单击**继续**按钮。



4. 邀请电子邮件已发送。现在该设备已在设备区域中显示为“等待中”。这表示您的邀请正在等待接受。



如果您的邀请一直处于等待中状态，您可以选择**重新发送邀请链接**，或完全**取消邀请**。

5. 在您的邀请被接受时，您可立即更改新添加设备的名称和类型（当然，您也可在将来任何时间进行更改）。现在，该设备已是您 Zen 网络的成员，且您可以远程查看上面安装的 AVG 产品。恭喜您！您已成为真正的 Zen 管理员！

2.3.3. 如何更改设备名称和类型？

1. 单击设置按钮，然后在弹出的对话框中选择***设备设置***。



2. 您所看到的设置将应用于您当前所选择的设备。您网络中的当前可用设备（即已接受邀请的设备）列表将显示在 *设备设置* 对话框左边的一列拼贴图中。只需单击各个拼贴图，即可在其间进行切换。

3. ***设备名称***文本框显示您当前所选设备的名称。您可删除现有名称并将其替换为任何您喜欢的名称。

4. 在下面，您可选择当前所选设备的***类型***（手机、平板电脑、笔记本电脑或台式机）。只需单击相应的拼贴图即可。

5. 单击**保存**按钮以确认更改。

2.3.4. 如何连接至现有 Zen 网络？

PC 设备：

1. 如果您当前未登录任何 AVG MyAccount，请单击状态按钮（显示有***连接***文本）并在弹出的小对话框中按**继续**按钮以确认。

> 如果您已连接至一些 AVG MyAccount，则您需要先登出，以便连接至其它帐户。单击状态按钮（上面有您当前 AVG MyAccount 名称）并在弹出的小对话框中单击**登出**按钮以确认。

2. 选择新打开的子对话框中左边的***连接至现有 Zen 网络***窗格。



3. 输入您的 AVG MyAccount 用户名和密码。如果还没有自己的 AVG MyAccount，只需为您自身创建一个新帐户即可。如果您要以管理员身份登录，从而能够查看此 Zen 网络中远程设备上的 AVG 产品，请保持选中***以管理员身份连接***复选框。否则，您只能以连接的用户身份进行操作。

如果您忘记了密码，请单击***忘记密码？***链接（在密码文本框下方）。这会将您重定向至一个网页，可以找回丢失的密码。

4. 单击**连接**按钮。连接过程几秒内便可完成。成功连接后，您应该可以看到您的 MyAccount 名显示在状态按钮上。

Android 移动设备：

与在 PC 设备上不同，Android 移动设备上的网络连接将会直接在应用程序中执行：

1. 如果您想将 Android 移动设备连接至 Zen 网络，您需要下载一个 AVG 移动应用程序（即 AVG AntiVirus、AVG Cleaner 和 或 AVG PrivacyFix）。可在 Google Play 轻松下载，上面所有的应用程序均可免费下载和安装。为使该连接正常运行，请确保您所使用的是当前可用的最新版本。

2. 安装 AVG 应用程序后，请打开并点击主屏幕左上角的***菜单图标***（即应用程序的徽标）。

3. 显示了菜单后，点击**管理设备**选项。

4. 在这里，点击**登录**选项卡并输入相应的 AVG MyAccount 凭据（即您的***用户名***和***密码***）。

5. 祝贺您！您现在已成为 Zen 网络的成员。单击菜单图标后，您现在应该能看到***已连接***

为：文本，且当前 AVG MyAccount 名称显示在菜单最上方。但是，如果您改变了想法，也可随时轻松离开此网络。

Mac 设备：

与在 PC 设备上不同，Mac 设备上的网络连接将会直接在应用程序中执行：

1. 如果想将 Mac 设备连接至 Zen 网络，您需要下载一个 AVG Mac 应用程序（即 AVG AntiVirus 和 或 AVG PrivacyFix）。这非常容易，例如，可在 AVG 下载中心或 Mac App Store 等许多地方免费下载和安装。为使该连接正常运行，请确保您所使用的是当前可用的最新版本。

2. 安装完 AVG 应用程序后，再打开它。应用程序屏幕的右上角将会显示一个椭圆形按钮（当前显示 "未连接"）。单击该按钮并从下拉菜单那中选择**连接**选项。

3. 在新打开的对话框中，单击中间的选项**登录至 AVG MyAccount**（默认情况下应已选择）。

4. 输入相应的 AVG MyAccount 凭证，即您的***用户名***（MyAccount 电子邮件）和***密码***。

5. 祝贺您！您现在已成为 Zen 网络的成员。右上角的按钮现在显示 "已连接"。如果您单击该按钮，则会看到您当前所连接的网络。如果您改变了想法，也可随时轻松离开此网络。

2.3.5. 如何新建 Zen 网络？

要创建（并管理）新的 Zen 网络，您首先需要创建您自己的 AVG MyAccount。基本上有两种方式进行创建 -使用您的 Web 浏览器，或直接从 AVG Zen 应用程序中创建。

从浏览器：

1. 使用浏览器打开 https://myaccount.avg.com/ 网站。

2. 单击**创建 AVG MyAccount** 按钮。

3. 输入您的登录电子邮箱、设置密码并再次输入，然后单击**创建帐户**按钮。

4. 将会向您发送用于激活 AVG MyAccount 的链接（该链接将发送至您在步骤 3中所使用的电子邮件地址）。您需要单击此链接，才能完成 MyAccount 创建过程。如果您在收件箱中未发现此邮件，则可能在垃圾文件夹中。

从 AVG Zen：

1. 如果您当前未登录至任何 AVG MyAccount，请单击状态按钮（显示有***连接***文本）并通过在弹出的小窗口中单击**继续**按钮以确认。

如果您已连接至一些 AVG MyAccount，则您需要先登出，以便连接至其它帐户。单击状态按钮（上面有您当前 AVG MyAccount 名称）并在弹出的小对话框中单击**登出**按钮以确认。

2. 请确保已选择在新打开子对话框左侧的***新建 Zen 网络***窗格。



3. 输入您的登录电子邮箱并设置密码（如果要查看隐藏的字符，请勾选下方的***显示密码***复选框），然后单击**连接**按钮。

4. 几秒钟后，您将连接到新建的网络，并拥有管理员权限。这也就是说，您可以添加设备至您的网络，远程查看安装在这些设备上的 AVG 产品，且在必要时将它们从您的网络中移除。

2.3.6. 如何安装 AVG 产品？

1. 可以通过 Zen 轻松安装 AVG 产品。为此，单击选择的类别拼贴图（拼贴图将为灰色，表示您尚未安装此类别的产品；或为半绿色，表示您已安装此类别的一个产品，但还有一个产品未安装）。



2. 如果您想立即开始产品安装，您所要做的只是单击**免费获取**按钮。该产品将会自动使用默认设置进行安装。

   如果您想控制安装过程，请单击**免费获取**按钮右边的小箭头按钮，然后单击**自定义安装**。这样，安装过程可看作一系列对话框，让您可以更改目标文件夹和已安装组件等。

有关各种 AVG 产品安装过程在此文档的其他部分或其它的用户指南中进行了详细描述。这些指南可从 AVG 网站轻松下载。

3. 随着安装的进行，您将会看到在所选类别拼贴图中显示绿色的圆圈。成功安装后，拼贴图中的圆圈会全部变为绿色（在某些类别中，也可能会只显示半圆，表示该类别中还有其它可安装的产品）。请注意，安装完成后，绿色圆圈（或半圆）还可能会立即变为另一种颜色（黄色或红色），这表示该产品中出现了一些问题，需要引起注意。

4. 您将会收到确认消息（该消息显示在类别拼贴图的正下方），告知您安装已成功完成。

2.3.7. 如何离开网络？

PC 设备：

1. 您如果您是一些 Zen 网络的成员，但是想要离开，操作非常简单。首先，单击状态按钮（显示有***已连接***文本），然后在弹出的小对话框中单击**离开此网络**按钮以继续。

2. 接下来您将需要确认是否确实要离开该 Zen 网络。要离开，请单击**离开**按钮。

3. 几秒后，您将永久性地断开连接。先前网络的管理员将无法再管理您 PC 上的 AVG 产品。状态按钮上的文本将会变为***连接***（即恢复到其最初的状态）。

Android 移动设备：

与在 PC 设备上不同，Android 移动设备上的网络连接将会直接在应用程序中执行：

1. 打开您的 AVG 应用程序，然后点击主屏幕右上角的***菜单图标***（即该应用程序的徽标）。

2. 在该菜单的最上方，您将会看到***已连接为：***文本，还可看到您当前 AVG MyAccount 名。旁边有一个门状小图标，上有一个箭头指向右边。单击该图标。

3. 单击**确定**按钮以确定确实要离开 Zen 网络。

4. 几秒后，您将永久性地断开连接。先前网络的管理员将无法再管理您 Android？移动设备上的 AVG 产品。但是，您可再次轻松连接至该 Zen 网络或任何其它网络 -直接或通过接受邀请进行连接。

Mac 设备：

与在 PC 设备上不同，Mac 设备上的网络连接将会直接在应用程序中执行：

1. 打开 AVG 应用程序并单击应用程序屏幕右上角的椭圆形按钮（现在显示"已连接"）。

2. 在下拉菜单的最上方，您将会看到***已连接至以下的 Zen 网络：***文字，还可看到您当前 AVG MyAccount 名。

3. 在Zen网络信息的正下方提供有**离开此网络**选项。单击该选项。

4. 几秒后，您将永久性地断开连接。先前网络的管理员将无法再管理您 Mac 设备上的 AVG 产品。但是，您可再次轻松连接至该 Zen 网络或任何其它网络 -直接或通过接受邀请进行连接。

2.3.8. 如何将设备从您的网络中移除？

1. 如果您不想让某些设备继续作为您 Zen 网络的成员，您可轻轻松将其移除。单击设置按钮，然后在弹出的对话框中选择***设备设置***。

2. 在"设备设置"对话框左边的一列拼贴图列中，显示有您设备中的当前可用设备列表。单击上面有要移除设备名称的拼贴图以转至该设备。

3. 在该对话框最底边，您将会看到***从网络移除***链接。单击该图标。

> 请注意，在您当前正使用的设备的设置中，不会有此类链接。此设备被视为您网络的核心，因此不能被移除。

4. 接下来，您需要确定是否确实要将此设备从您的 Zen 网络中移除。要移除，请单击**移除**按钮。

5. 几秒钟后，将会永久性地移除该设备。您将无法再管理该设备上的 AVG 产品；该设备也将从您的用户界面中的设备区域中消失。

2.3.9. 如何查看和 成管理 AVG 产品？

如果您想要查看并管理您自己的设备

实际上，您只需勾选相应的类别拼贴图。这会打开 AVG 产品的用户界面，让您可以随意查看并进行配置。例如，勾选***保护***拼贴图将打开 AVG Internet Security 用户界面等。如果一个类别中包含多个产品，您将需要单击其拼贴图，然后选择相应的子拼贴图，如，在***隐私和身份***类别下选择 AVG PrivacyFix。

可通过 Zen 查看并管理的 AVG 产品在此文档的其它部分或其它的用户指南中进行了详细描述。可从 AVG 网站上随意下载这些手册。

如果有任何需要您注意的紧急问题，还可单击消息按钮。新打开的对话框中包含一列问题和困难，其中的一些甚至可直接在此对话框中处理 -此类事项旁边显示有特别的操作按钮。

如果您想要查看和管理远程设备（仅限管理员）

这也相当容易。在设备区域中选择您想要查看的设备，然后单击相应的类别拼贴图。然后，将会打开一个新对话框，其中包含了此类别中 AVG 产品的简要概况。



作为管理员，您可使用多个按钮对 Zen 网络中的 AVG 产品执行各种远程操作。可用操作取决于设备类型（PC、Android 或 Mac）以及您当前所查看的类别拼贴图。请注意，如果近期有执行过某些操作（如扫描或更新），则此类操作可能不可用。以下列示了 AVG 产品所有可用的远程操作：

设备类型	类别拼贴图	可用远程操作
PC	***保护 （AVG Internet Security）***	• **立即扫描**按钮 –按下此按钮可立即开始扫描，检查远程设备以查看是否存在病毒和其它有害软件。扫描完成后，您可立即获得结果通知。单击此处以了解有关 AVG Internet Security 扫描的更多信息。 • **更新**按钮 –单击该按钮以开始远程设备上 AVG Internet Security 的更新过程。所有防病毒软件必须均为最新版本以确保最高级别的防护。单击此处以了解有关 AVG Internet Security 更新重要性的更多信息。 • **显示详细信息**按钮 –此按钮仅在出现需要您注意的紧急事项时才可用。单击该按钮以打开当前所选设备的消息对话框。此对话框显示了按产品类别分类的问题列表。其中一些问题可通过单击**立即修复**按钮直接解决。例如，在 AVG Internet Security 中，您可打开先前禁用的保护组件。
PC	***性能 （AVG PC TuneUp）***	• **运行维护**按钮 –单击该按钮以启动系统维护 –即执行一系列的各种任务，用于清理远程设备上的系统，加快其运行速度并优化其性能。 • **更新**按钮 –单击该按钮以开始远程设备上 AVG PC TuneUp 的更新过程。AVG PC TuneUp 务必始终为最新版本，因为其各个功能均会不断扩展或进行调整，以适应最新技术及修复错误。 • **显示详细信息**按钮 –此按钮仅在出现需要您注意的紧急事项时才可用。单击该按钮以打开当前所选设备的消息对话框。此对话框显示了按产品类别分类的问题列表。其中一些问题可通过单击**立即修复**按钮直接解决。
Android	***保护 （AVG AntiVirus）***	• **立即扫描**按钮 –按下此按钮可立即开始扫描，检查远程 Android 设备以查看是否存在病毒和其它有害内容。扫描完成后，您可立即获得结果通知。 • **更新**按钮 –单击该按钮以开始远程 Android 设备上 AVG AntiVirus 的更新过程。所有防病毒软件必须均为最新版本以确保最高级别的防护。 • **显示详细信息**按钮 –此按钮仅在出现需要您注意的紧急事项时才可用。单击该按钮以打开当前所选设备的消息对话框。此对话框显示了按产品类别分类的问题列表。但是，对于 AVG AntiVirus Android 版，此对话框仅用作参考，您无法对其作出任何更改。
Mac	***保护 （AVG AntiVirus）***	• **更新**按钮 –单击该按钮以开始远程 Mac 设备上 AVG AntiVirus 的更新过程。所有防病毒软件必须均为最新版

设备类型	类别拼贴图	可用远程操作
		本以确保最高级别的防护。 • **显示详细信息**按钮 –此按钮仅在出现需要您注意的紧急事项时才可用。单击该按钮以打开当前所选设备的消息对话框。此对话框显示了按产品类别分类的问题列表。对于 AVG AntiVirus Mac 版，您可使用**立即修复**以开启先前禁用的实时防护。

2.4. 常见问题解答和支持

随时均可通过点击设置按钮并选择***支持***选项轻松访问 AVG Zen 的用户支持。

在您的浏览器中，AVG 支持中心将会打开。此页面让您可访问专业 AVG 用户支持。您可询问有关许可证、安装、病毒和特定产品功能的问题。如果您需要有关 AVG 产品的任何帮助，请在此处查找即可。

您可能还想获取有关 AVG Zen 的完整信息 –在这种情况下，请访问 www.avg.com/zh/avg-zen 站点。

如果您处于离线状态且无法重新连接到 Internet，请联系您的 Internet 提供商以获取帮助。没有 Internet 连接，AVG Zen 将无法正常工作，其支持选项也将不可用。

3. AVG Internet Security

用户手册的本部分提供了 **AVG Internet Security** 的全面用户文档。

但是，您还可能需要使用其它来源的信息：

- ***帮助文件***：可在随 **AVG Internet Security** *附带的帮助文件中直接查看故障排除*部分（要打开该帮助文件，请在应用程序的任意对话框中按 F1 键）。此部分中列有用户想要寻求技术问题专业帮助时最常出现的情况。请选择最符合所遇到的问题的情况，然后单击该情况以打开详细说明，从而引导您解决问题。
- ***AVG 网站支持中心***：也可在 AVG 网站（http://www.avg.com/）中查找所遇到的问题的解决方法。在***支持中心***部分中，可综览结构化主题组（说明销售和支持问题）。
- ***常见问题解答***：在 AVG 网站（http://www.avg.com/）中，也可找到精心构成的独立的常见问题解答部分。可通过***支持中心 常见问题解答和教程***菜单项查看此部分。其中的所有问题也已分门别类的划分，分为销售问题、技术问题和病毒问题这三类。
- ***AVG ThreatLabs***：特定的 AVG 相关网站（http://www.avgthreatlabs.com/website-safety-reports/），是有关病毒问题的专业站点，提供有关在线威胁相关的结构化概览。其中也有关于删除病毒、间谍软件的说明，还有针对如何一直得到保护提出的建议。
- ***论坛***：也可使用 AVG 用户论坛（http://forums.avg.com）。

3.1. AVG 安装过程

要将 **AVG Internet Security** 安装到计算机中，需要获得最新的安装文件。为了确保要安装的是最新版 **AVG Internet Security**，建议从 AVG 网站（http://www.avg.com/）下载安装文件。通过 ***支持*** 部分可分类综览各个 AVG 版本的安装文件。将安装文件下载并保存到您的硬盘上之后，您就可以启动安装过程。安装过程中会显示一系列简单易懂的对话框。每个对话框都会简短说明执行安装过程的每个步骤时所要执行的操作。下面，我们会详细说明各个对话窗口。

3.1.1. 欢迎！

安装过程开始时会显示 ***欢迎使用 AVG Internet Security*** 对话框：



语言选择

可在此对话框中选择要在安装过程中使用的语言。单击 ***语言*** 旁边的组合框可下拉语言菜单。选择所需语言，然后就会以所选语言继续执行安装过程。同时，该应用程序将用所选语言显示安装过程，并带有选项可切换至默认情况下始终安装的英语。

最终用户许可协议和隐私政策

在您继续安装过程前，我们建议您开始熟悉 ***最终用户许可协议*** 和 ***隐私政策*** 文件。可通过对话框底部的活动链接访问这两个文件。单击任一超链接将打开新对话框 新浏览器窗口，上面显示相应的全文。请仔细阅读这些有法律约束力的文件。单击 ***继续*** 按钮即表明您确认同意这些文件。

继续安装

要继续安装过程，只需单击 ***继续*** 按钮。系统将要求您输入许可证号码，然后安装过程将以完全自动模式进行运行。建议大多数用户使用此标准选项来安装 **AVG Internet Security**，上面有程序供应商预定义的所有设置。此配置可提供最大程度的安全性，同时又会使资源得

到最优利用。 今后如果需要更改配置，您始终可以直接在应用程序中完成此操作。

此处，有一个***自定义安装***，以***继续***按钮下的超链接形式提供。 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来安装该应用程序时使用，例如，为满足特定的系统要求。 如果您决定这样做，在输入许可证号码后，您将重定向至***自定义安装***对话框，您可在这里指定您的设置。

3.1.2. 安装 AVG

已确认之前的对话框中的安装启动，安装过程在全自动模式下运行，不需要进行任何干预：



完成安装过程后，您将被邀请创建网络帐户 -有关详细信息，请参见 ***'如何创建一个新的 Zen 网络？'章节***。

3.2. 安装后

3.2.1. 病毒库更新

请注意，安装时*（或者如有需要，计算机重新启动后）*，**AVG Internet Security** 会自动更新其病毒库和所有组件，并使其完全正常运行，这可能会耗费几分钟的时间。 正在执行更新进程时，主对话框中显示的信息将会告知您情况。 请稍候，等待完成更新进程，完全更新您的 **AVG Internet Security** 并准备就绪为您提供保护！

3.2.2. 产品注册

安装完 **AVG Internet Security** 后，请在 AVG 网站 （http://www.avg.com/） 上在线注册您的产品。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。最简单的注册方法是直接在 **AVG Internet Security** 用户界面中注册。

请选择上条导航选项立即注册项。您将被重定向到 AVG 网站（http://www.avg.com/）上的***注册***页面。请按照页面上的说明操作。

3.2.3. 访问用户界面

AVG 主对话框可通过以下几种方式进行访问：

- 双击 AVG Internet Security 系统托盘图标
- 双击桌面上的 AVG 图标
- 通过以下菜单：*开始/所有程序/AVG/AVG Protection*

3.2.4. 扫描整个计算机

存在一种潜在风险，即计算机病毒在 **AVG Internet Security** 安装之前就已传播到您的计算机上。因此，您应运行扫描整个计算机这一功能以确保您的 PC 上不存在感染。第一次扫描可能需要相当长的时间（*大约一小时*），但建议您启动第一次扫描，以确保您的计算机未受威胁而导致性能损耗。有关运行扫描整个计算机的说明，请参阅 AVG 扫描一章。

3.2.5. Eicar 测试

若要确认 **AVG Internet Security** 是否已正确安装，您可以执行 EICAR 测试。

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

请尝试下载 *eicar.com* 文件并将其保存到您的本地磁盘上。在您确认下载此测试文件后 **AVG Internet Security** 会立即对它作出反应，即显示一则警告。这则通知表明 AVG 已在计算机中安装妥当。



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

3.2.6. AVG 默认配置

AVG Internet Security 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。***如果您想要更改 AVG 配置以更好地满足自己的需要，请转至 AVG 高级设置：选择主菜单项*选项 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。

3.3. AVG 用户界面

AVG Internet Security 打开时会显示主窗口：



该主窗口分为若干区域：

- ***上部条导航***包括主窗口的上部区域对准的四个活动链接（*如 AVG、报告、支持、选项一样*）。 详细信息 >>
- ***安全状态信息***提供有关 **AVG Internet Security** 当前状态的信息。 详细信息 >>
- ***转至 Zen 按钮***将会打开 ZEN 应用程序的主用户界面，您可在其中集中管理您所用的全部电子设备的保护、性能和隐私。
- ***安装组件概述***可在主窗口中心区域的水平条板块中找到。此组件会显示为由相应组件图标标记的淡绿板块，并提供有关组件状态的信息。 详细信息 >>
- ***扫描 更新快速链接***位于主窗口的板块条的下方。使用这些按钮可直接访问最重要且最常用的 AVG 功能。 详细信息 >>

在 **AVG Internet Security** 主窗口之外，有另外一个用于访问应用程序的控制元素：

- ***系统托盘图标***位于控制程序的右下角（*在系统托盘中*），说明 **AVG Internet Security** 的当前状态。 详细信息 >>

3.3.1. 上条导航

上条导航包含排列在主窗口上部中的多个活动的链接。此导航包括以下按钮：

3.3.1.1. 在 Facebook 上加入我们

单击此链接加入 AVG Facebook 社区，一起分享 AVG 最新信息、新闻、提示和技巧，一切皆可获得最大的 Internet 安全保护。

3.3.1.2. 报告

打开一个新***报告***对话框，其中有关于以前启动的扫描和更新进程的所有相关报告的概述。如果当前正在运行扫描或更新，则会在主用户界面的上条导航的***报告***文本旁显示旋转圆形。单击此圆形获取描述正运行进程的进度对话框：



3.3.1.3. 支持

打开一个由四个选项卡构成的对话框，其中有关于 **AVG Internet Security** 的所有相关信息：



- ***支持*** - 该选项卡提供了清楚地安排给客户支持的所有可用联系人的概述。
- ***产品*** - 此选项提供了有关 **AVG Internet Security** AV 的产品信息、已安装组件、已安装电子邮件保护的最重要技术数据的概述：
- ***计划*** - 在此选项卡上，您可以找到有关安装的 **AVG Internet Security** 的详细技术信息，例如主要产品版本号，以及所有相应产品版本号的列表 *（如 Zen、PC TuneUp...）*。是事实接下来，该选项卡提供所有已安装组件的概述，以及特定安全信息 *（病毒库、 LinkScanner 和 Anti-Spam 的版本号）*。
- ***许可协议*** - 此选项卡会提供您和 AVG Technologies 之间的许可协议全文。

3.3.1.4. 选项

AVG Internet Security 的维护可通过 ***选项*** 项进行访问。单击箭头打开下拉菜单：

- ***扫描计算机*** 可启动扫描整个计算机。
- ***扫描所选文件夹 ...***- 可切换到 AVG 扫描界面，还可以在计算机的树结构中定义应扫描的文件和文件夹。
- ***扫描文件 ...***- 可以对单个文件执行按需测试。单击此选项可打开带有硬盘树结构的新窗口。选择所需的文件，然后确认启动扫描。
- ***更新*** - 自动启动 **AVG Internet Security** 的更新过程。
- ***从目录更新 ...***- 从位于您本地硬盘上指定的文件夹中的更新文件执行更新过程。不过，建议仅将此选项用于应急情况，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。

- ***隔离区管理*** - 打开隔离区的界面，即“隔离区管理”，AVG 可将所有检测到的受感染文件均移至其中。 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，以后可能会对其进行修复。
- ***历史记录*** - 用于进一步提供特定子菜单选项：
    - *扫描结果* - 用于打开提供扫描结果概述的对话框。
    - *Resident Shield 结果* - 用于打开一个对话框，从中可综览 Resident Shield 检测到的威胁。
    - *Identity Protection 结果* - 这将打开一个对话框，从中可综览 Identity Protection 组件检测到的威胁。
    - *电子邮件保护结果* - 用于打开一个对话框，从中可综览电子邮件保护组件检测后断定有危险的邮件附件。
    - *Online Shield 结果* - 用于打开一个对话框，从中可综览 Online Shield 检测到的威胁。
    - *事件历史记录日志* - 用于打开历史记录日志界面，其中有全部已记录的 **AVG Internet Security** 操作的概述。
    - *Firewall 日志* - 用于打开一个对话框，其中详细概述了所有 Firewall 操作。
- ***高级设置 ...*** - 打开“AVG 高级设置”对话框，您可以在此对话框中对 **AVG Internet Security** 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。
- ***防火墙设置 ...*** - 用于打开一个独立的对话框，以便对 Firewall 组件进行高级配置。
- ***帮助目录*** - 打开 AVG 帮助文件。
- ***获取支持*** - 打开支持对话框，其中提供了所有可访问的联系和支持信息。
- ***您的 AVG Web*** - 用于打开 AVG 网站 (*http://www.avg.com/*)。
- ***关于病毒和威胁*** - 用于打开AVG 网站 (*http://www.avg.com/*) 上的在线病毒百科全书，从中可查找关于已识别出的病毒的详细信息。
- ***MyAccount*** - 连接至 ***AVG MyAccount*** 网站 (*http://www.avg.com/*) 的注册页面。 创建您的 AVG 帐号，以便您可轻松维护您已注册的 AVG 产品和许可证、下载新产品、查看您的订单状态或为您的个人数据设定密码。 请填写您的注册数据；只有已注册各自 AVG 产品的客户才能享受免费技术支持。
- ***关于 AVG*** - 打开一个包含四个选项卡的新对话框，分别提供有关已购买的许可证、访问支持、产品和程序信息以及完整许可协议的相关信息。 *（也可通过主导航的支持链接打开此对话框。）*

3.3.2. 安全状态信息

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

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

- 黄色图标警告***一个或多个组件配置不当***，您应对其属性设置加以注意。**AVG Internet Security** 中未出现严重问题，您可能出于某些原因已决定将某些组件关闭。用户仍处于受保护状态！不过，请对问题组件的设置加以注意！错误配置的组件将通过主用户界面中的橙色条警告显示。

  如果出于某种原因决定忽略组件的错误状态，也会显示黄色图标。可通过高级设置 *忽略错误状态*分支查看忽略***错误状态***选项。在此您可选择表明已经知道该组件的错误状态，但出于某种原因想要保持 **AVG Internet Security** 的这种状态，而且不想收到有关它的警告。在特定情况下您可能需要使用此选项，但极力建议您尽快禁用***忽略组件状态***选项！

  此外，如果您的 **AVG Internet Security** 需要重新启动计算机（***需要重新启动***），则也会显示黄色图标。请特别注意此选项并重新启动 PC。

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

如果 AVG Internet Security 未设置为达到最佳性能，则安全状态信息旁边会显示一个名为“点击进行修复”（或在问题涉及多个组件的情况下为“点击进行修复”）的新按钮。按此按钮可启动检查和配置程序的自动进程。这是将 AVG Internet Security 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***，如果所报告的内容出现任何问题，请立即设法予以解决。否则您的计算机将面临风险！

注意： *AVG Internet Security 状态信息也可以随时通过系统托盘图标获得。*

3.3.3. 组件概览

安装组件概述可在主窗口中心区域的水平条板块中找到。此组件以由相应组件图标标记的谈绿色板块形式显示。每个板块提供有关当前保护状态的信息。如果已正确配置组件并完全正常运行，则会以绿色字母显示信息。如果组件已停止、其功能受到限制或组件处于错误状态，则会以橙色文本字段显示警告文本向您发出通知。***强烈建议您注意相应的组件设置！***

在组件上移动鼠标以在主窗口底部显示简短文本。此文本提供了组件功能的基本简介。它还会显示组件的当前状态并指定未正确配置的组件服务。

已安装组件的列表

在 **AVG Internet Security** 中，***“组件概览”***区域包含有关以下组件的信息：

- ***计算机*** - 此组件包含两种服务：***AntiVirus Shield*** 用于检测病毒、间谍软件、蠕虫、特洛伊木马、不需要的可执行文件或系统中的库，并保护您免遭恶意广告软件的入侵；***Anti-Rootkit*** 用于扫描隐藏在应用程序、驱动程序或库中的危险 Rootkit。 详细信息 >>
- ***网页浏览*** - 在您于 Internet 上搜索和上网时保护您免遭基于 Web 的攻击。 详细信息 >>
- ***Identity*** - 该组件运行 ***Identity Shield*** 服务，用来持续保护您的数字资产免遭 Internet 上的新威胁和未知威胁的侵害。 详细信息 >>
- ***电子邮件*** - 用于检查传入的电子邮件中的垃圾邮件，以及阻止病毒、仿冒攻击或其它威胁。 详细信息 >>
- ***Firewall*** - 用于控制通过每个网络端口传输的所有通讯内容，从而防止受到恶意攻击，并阻止所有入侵企图。 详细信息 >>

能执行的操作

- ***将鼠标光标移到任一组件的图标上*** 即可在组件概览中突出显示该组件。同时，该组件的基本功能说明也会显示在用户界面的底部。
- ***单击组件图标*** 可打开带有有关组件当前状态信息的组件自身界面，并可访问其配置和统计数据。

3.3.4. 扫描 更新快速链接

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

- ***立即扫描*** - 此按钮以图形方式划分成两个部分。单击 ***立即扫描*** 链接可立即启动扫描整个计算机，并在自动打开的报告窗口中查看其进度和结果。***选项*** 按钮可打开 ***扫描选项*** 对话框，您可在其中管理计划的扫描以及编辑扫描整个计算机/扫描特定文件或文件夹的参数。 *（对于详细信息，请参见 AVG 扫描一章）*
- ***修复性能*** - 单击此按钮将会转至 ***PC 分析器*** 服务，这是一种用于进行详细系统分析和更正（有关如何提高计算机速度和整体性能）的高级工具。
- ***立即更新*** - 按此按钮可立即启动产品更新。系统将在 AVG 系统托盘图标上的滚动对话框显示更新结果的信息。 *（有关详细信息，请参见 AVG 更新一章）*

3.3.5. 系统托盘图标

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

AVG 系统托盘的显示方式

- 该图标处于全彩状态，而且没有附加元素，表明所有 **AVG Internet Security** 组件都已激活，都运行完全正常。但是，如果某个组件的运行不完全正常，但用户已决定忽略组件状态，则也会这样显示该图标。 *（确认忽略组件状态选项，就表示知道组*

件的错误状态，但出于某种原因想要保持这种状态，不想看到有关这种情况的警告。）

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

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

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

AVG 系统托盘信息

AVG 系统托盘图标还会通过从系统托盘图标打开的弹出窗口显示 **AVG Internet Security** 中的当前活动，以及该程序内可能的状态变化*（例如，计划的扫描或更新的自动启动、防火墙配置文件切换、组件的状态变化以及错误状态的出现等 ..）*。

可通过 AVG 系统托盘图标执行的操作

也可将 ***AVG 系统托盘图标***用作快速链接，以访问 **AVG Internet Security** 用户界面，仅需双击 AVG 系统托盘图标即可。通过用右键单击此图标，可以打开一个简短的上下文菜单，其中有以下选项：

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

- ***暂时禁用 AVG 保护*** - 使用该选项可以一次性关闭由 **AVG Internet Security** 提供的整个保护。请记住，只有在绝对必要的情况下才使用此选项！在大多数情况下，不必在安装新软件或驱动程序之前禁用 **AVG Internet Security**，即使安装程序或软件安装向导建议先关闭正在运行的程序和应用程序，以确保在安装过程中不发生意外中断。如果必须暂时禁用 **AVG Internet Security**，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。

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

- ***Firewall*** - 单击此项以打开上下文菜单，可快速访问所有可用的 Firewall 模式。从概述中选择并单击以确认您想要更改当前设定的 Firewall 模式。

- ***正在运行扫描 ...*** - 仅当计算机上当前有扫描正在运行时才会显示此项。对于该扫描，您可以设置其优先级，或者停止或暂停正在运行的扫描。也可执行以下操作：*设置所有扫描的优先级*、*暂停所有扫描*或*停止所有扫描*。

- ***登录到 AVG MyAccount*** - 打开 MyAccount 网页，可在其中管理您的订阅产品、购买其它保护、下载安装文件、检查过去的订单和发票以及管理您的个人信息。

- ***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。

3.3.6. AVG Advisor

AVG Advisor 用来检测问题，这些问题可能会减缓计算机速度或将其置于危险的境地，因此建议您采取措施解决该问题。 如果您遇到过计算机速度突然减慢的情况 *（Internet 浏览、整体性能）*，您通常不是很清楚真正的罪魁祸首是什么，以及如何去解决该问题。 这样 ***AVG Advisor*** 就有了用武之地：它将会在系统托盘中显示通知，通知您问题可能是什么，以及如何修复的建议。 ***AVG Advisor*** 可保持监控您 PC 中所有运行的进程以找到潜在的问题，并提示如何避免此问题发生。

AVG Advisor 在系统托盘以滑动的弹出窗口形式出现。



具体来说，***AVG Advisor*** 监控以下项：

- ***任何当前所打开的 Web 浏览器的状态***。 Web 浏览器可能会重载内存，特别是当一段时间内打开多个选项卡或窗口时，会消耗太多的系统资源（例如减缓您的计算机速度）。 在此类情况下，重新启动 web 浏览器通常很有用。
- ***正在运行点对点连接***。 使用 P2P 协议共享文件之后，该连接有时会处于激活状态，从而消耗一些带宽。 因此，您就会在网页浏览时速度减慢。
- ***带熟悉名称的未知网络***。 通常只有那些连接到不同网络且通常是使用便携式计算机的用户才会遇到这种情况：如果新的未知网络与您熟知的常用网络 *（例如，Home 或 MyWifi）* 同名，则会感到困扰，这样您可能会意外地连接到完全未知且可能不安全的网络。 ***AVG Advisor*** 可通过警告您已知的网络实际上是新网络，来防止此类事件发生。 当然，如果您确定未知网络安全，则可将其保存到 ***AVG Advisor*** 已知网络列表以便将来不再报告。

在上述任何情况中，***AVG Advisor*** 会警告您可能发生的潜在问题，并提供冲突进程或应用程序的名称和图标。 另外，***AVG Advisor*** 会建议采取何种措施来避免潜在的问题。

支持的 Web 浏览器

该功能可在以下 web 浏览器上使用：Internet Explorer、Chrome、Firefox、Opera 和 Safari。

3.3.7. AVG Accelerator

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



3.4. AVG 组件

3.4.1. 计算机保护

计算机 组件包含两项主安全服务： ***AntiVirus*** 和 ***Data Safe***：

- ***AntiVirus*** 包含保护所有文件、计算机的系统区域和可移动介质 *（闪存盘等）*，并可扫描已知病毒。 对于检测到的任何病毒，系统都会阻止其执行任何操作，然后在隔离区管理中将其清除或隔离。 用户甚至不会注意到此过程，因为这也称为常驻保护"在后台"运行。 AntiVirus 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。 这意味着，如果新病毒包含现有病毒的一些典型特征，则 AntiVirus 程序便可以检测到新的未知病毒。 **AVG Internet Security** 也能够分析和检测系统中可能不需要的可执行应用程序或 DLL 库 *（各种间谍软件、广告软件等）*。 此外，AntiVirus 会扫描系统注册表是否含有可疑条目，扫描 Internet 临时文件，并允许您像处理任何其它感染一样处理所有可能不需要的内容。

- ***数据保险箱*** 可让您创建安全的虚拟保险箱以储存珍贵或敏感数据。数据保险箱的内容使用您所选的密码来加密和保护，以确保在未经许可的情况下，任何人都无法访问它。



对话框控制项

要在对话框的两个区域之间切换，您仅需单击相应服务面板的任意一处。 然后此面板会以浅蓝色突出显示。 在对话框的两个区域中，您可找到以下控制项。 不管它们属于一个安全服务或其它安全服务（*AntiVirus 或数据安全*），它们的功能均相同：

已启用 已禁用 - 无论是在外观和功能上，此按钮均可使用通信灯提醒您。 单击一次即可在两个位置之间切换。 绿色代表***已启用***，意味着 AntiVirus 安全服务已激活，可以完全正常工作。 红色代表***已禁用***状态，即此服务已停用。 若非必要，请勿停用此服务，强烈建议保持所有安全配置的默认设置。 默认设置可保证应用程序的最优性能以及最高安全。 如果出于某些原因您要停用服务，则系统会通过红色***警告***符号立即对您发出可能的风险的警告，并通知您此时未受到完全保护。 ***请注意，您必须马上再次激活此服务！***

设置 - 单击此按钮可重新定向到高级设置界面。 相应的对话框会打开，您将可以配置所选的服务，即 AntiVirus。 在高级设置界面中，您可编辑 **AVG Internet Security** 中的每个安全服务的所有配置，但建议仅限经验丰富的用户编辑任何配置！

箭头 - 使用此对话框左上区域的绿色箭头返回到包含组件概述的主用户界面。

如何创建数据保险箱

在***计算机保护***对话框的***数据保险箱***部分，您可以找到***创建保险箱***按钮。 单击该按钮以打开同名的新对话框，您可以在其中指定所计划保险箱的参数。 请填写所有必要信息，然后按应用程序中的说明进行操作：



首先，您必须指定保险箱的名称，然后创建强密码：

- ***保险箱名*** - 要创建新数据保险箱，必须首先选择适合的保险箱名进行识别。 如果要与家庭其它成员共享计算机，可能需要包括您名称及保险箱内容指示，例如，*Dad's emails（爸爸的电子邮箱）*。

- ***创建密码 重新输入密码*** - 为数据保险箱创建密码，然后在各自的文本字段中输入密码。 右侧的图形指示器将指出您的密码是弱 *（比较容易使用特殊软件工具来破解）* 还是强。 我们建议选择至少为中等强度的密码。 您可在密码中包含大写字母、数字或其他字符，如点号和破折号等，以提升密码强度。如果想要确保键入的密码无误，可选中***显示密码***框 *（当然，不要泄漏给他人）*。

- ***密码提示*** - 我们强烈建议您同时创建有用的密码提示，在忘记时提醒您的密码是什么。 请记住，数据保险箱只允许通过密码访问，从而保护文件安全；没有其他变通方法，因此，如果您忘记了密码，您将无法访问您的数据保险箱！

在通过在文本字段中指定所有必需的数据后，单击***下一步***按钮以继续前一步骤：



此对话框提供以下配置选项：

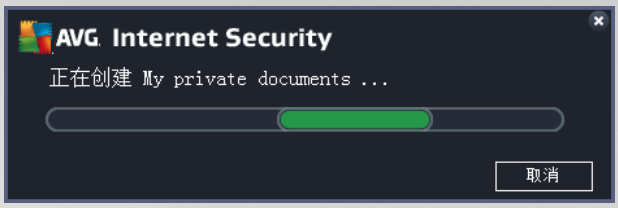
- ***位置***指出数据保险箱实际所处的位置。 浏览以查找硬盘上的适合目标，或您可以保留预定义的位置，它是您的*文档*文件夹。 请注意，创建数据保险箱之后，就不可再更改其位置。

- ***大小*** - 您可以预定义数据保险箱的大小，该操作会在磁盘上分配必要的空间。 该值不应设置得太小 *（无法满足需要）*，也不应设置得太大 *（不必要地占用太多磁盘空间）*。 如果您已知道要在数据保险箱中存放什么内容，则可将所有文件放在一个文件夹中，然后使用***选择文件夹***链接以自动计算总大小。 但是，以后您也可以根据需求更改这个大小。

- ***访问*** - 此部分的该复选框让您为数据保险箱创建便捷的快捷方式。

如何使用数据保险箱

完成所有设置之后，单击***创建保险箱***按钮。 将弹出新对话框***您的数据保险箱已就绪***，提示您可使用保险箱存储文件了。这样，保险箱已打开，可立即访问保险箱。 此后每次尝试访问保险箱时，都将要求您使用已定义的密码来解锁保险箱：



要使用新的数据保险箱,您必须先将其打开 -单击***立即打开***按钮。 打开之后，数据保险箱将在电脑上显示为新的虚拟磁盘。 请从下拉菜单中分配您所选择的盘符（*您将只能从当前可用磁盘中进行选择*）。 通常，不允许选择 C 盘（*通常已分配给硬盘*）、A 盘（*软盘驱动器*）或 D 盘（*DVD 驱动器*）。 请注意，每次解锁数据保险箱时，您可选择另一个可用的驱动器盘符。

如何解锁数据保险箱

下次尝试访问保险箱时，将要求您使用已定义的密码来解锁保险箱：



在文本字段中，请输入密码对您自己进行验证，然后单击***解锁***按钮。 如果您需要密码提示，请单击***提示***以显示您在创建数据保险箱时定义的密码提示。 新的数据保险箱将在数据保险箱概览中显示为已解锁，您可根据需要添加 删除文件。

3.4.2. Web 浏览保护

网页浏览保护 包含两种服务： ***LinkScanner Surf-Shield*** 和 ***Online Shield***：

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

- ***Online Shield*** 是一种实时常驻保护功能；它甚至可以在所访问的网页（以及其中可能包含的文件）在您的 Web 浏览器中显示或下载到您的计算机前便扫描它们的内容。 Online Shield 可以检测到您即将访问的页面包含一些危险的 javascript，并阻止该页面显示。 另外，它还会识别页面中包含的恶意软件，发现它们后会立即停止下载，使其绝无可能进入您的计算机。 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。 ***Online Shield 保护措施不可用于服务器平台！***



对话框控制项

要在对话框的两个区域之间切换，您仅需单击相应服务面板的任意一处。然后此面板会以浅蓝色突出显示。在对话框的两个区域中，您可找到以下控制项。不管它们属于一个安全服务或其他安全服务（*LinkScanner Surf-Shield 或 Online Shield*），它们的功能均相同：

已启用 已禁用 - 无论是在外观和功能上，此按钮均可使用通信灯提醒您。单击一次即可在两个位置之间切换。绿色代表 ***已启用***，意味着 LinkScanner Surf-Shield/Online Shield 安全服务已激活，可以完全正常工作。红色代表 ***已禁用*** 状态，即此服务已停用。若非必要，请勿停用此服务，强烈建议保持所有安全配置的默认设置。默认设置可保证应用程序的最优性能以及最高安全。如果出于某些原因您要停用服务，则系统会通过红色 ***警告*** 符号立即对您发出可能的风险的警告，并通知您此时未受到完全保护。 ***请注意，您必须马上再次激活此服务！***

设置 - 单击此按钮可重新定向到高级设置界面。相应的对话框会打开，您将配置所选的服务，即 LinkScanner Surf-Shield 或 Online Shield。在高级设置界面中，您可编辑 **AVG Internet Security** 中的每个安全服务的所有配置，但建议仅限经验丰富的用户编辑任何配置！

箭头 - 使用此对话框左上区域的绿色箭头返回到包含组件概述的主用户界面'。

3.4.3. Identity Protection

Identity Protection 组件运行 ***Identity Shield*** 服务，用来持续保护您的数字资产免遭 Internet 上的新威胁和未知威胁的侵害：

- ***Identity Protection*** 是一款防恶意软件的服务，采用行为学技术为您抵御各种恶意软件（*间谍软件、僵尸程序、身份盗用等*），并针对新的病毒提供零时差保护。Identity Protection 旨在阻止身份盗用者通过针对您的 PC 的各种恶意软件（*恶意软件*）窃取您的密码、银行帐户详细信息、信用卡号码和其它个人数字财富。它确保在您的 PC

或共享网络上运行的所有程序都正常运行。 Identity Protection 持续地识别和阻止可疑行为，并防止您的计算机受到所有新恶意软件侵害。 Identity Protection 可为您的计算机实时防范新威胁甚至不明威胁。 Identity Protection 会监视所有进程 *（包括隐藏进程）*以及超过 285种不同的行为模式，并能够确定您的系统中是否已出现恶意行为。 因此，它甚至可以发现尚未在病毒数据库中描述的威胁。 有不明代码进入您的计算机时，Identity Protection 会立即监视其是否有恶意行为并对其进行跟踪。 如果发现是恶意文件，那么 Identity Protection 会将此代码移入隔离区管理，并撤消对系统所作的任何更改 *（注入代码、更改注册表、打开端口等）*。 无须启动扫描即可得到保护。 该技术非常主动，很少需要更新，并且始终保持警惕。



对话框控制项

在对话框中，您可找到以下控制项：

已启用 已禁用 - 无论是在外观和功能上，此按钮均可使用通信灯提醒您。 单击一次即可在两个位置之间切换。 绿色代表***已启用***，意味着 Identity Protection 安全服务已激活，可以完全正常工作。 红色代表***已禁用***状态，即此服务已停用。 若非必要，请勿停用此服务，强烈建议保持所有安全配置的默认设置。 默认设置可保证应用程序的最优性能以及最高安全。 如果出于某些原因您要停用服务，则系统会通过红色***警告***符号立即对您发出可能的风险的警告，并通知您此时未受到完全保护。 ***请注意，您必须马上再次激活此服务！***

设置 - 单击此按钮可重新定向到高级设置界面。 相应的对话框会打开，您将可以配置所选的服务，即 Identity Protection。 在高级设置界面中，您可编辑 **AVG Internet Security** 中的每个安全服务的所有配置，但建议仅限经验丰富的用户编辑任何配置！

箭头 - 使用此对话框左上区域的绿色箭头返回到包含组件概述的主用户界面。

很遗憾，**AVG Internet Security** 不包括 Identity Alert 服务。 如果您想使用此类保护，请遵循***升级以激活***按钮以重新定向到您可在其中购买 Identity Alert 许可证的专用网页。

请注意，即使安装有 AVG Premium Security 版本，Identity Alert 服务也只在所选的地区有提供：美国、英国、加拿大和爱尔兰。

3.4.4. 电子邮件保护

电子邮件保护 组件包含以下两种安全服务：***Email Scanner*** 和 ***Anti-Spam*** *（Anti-Spam 服务仅在 Internet / Premium Security 版本中才可用）*。

- ***Email 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。电子邮件保护组件用于扫描每一封发送或接收的电子邮件；每当检测到电子邮件中有病毒，都会立即将其删除并移到 隔离区管理 中。该组件还可过滤出特定类型的电子邮件附件，并为未感染病毒的邮件添加验证文本。***Email Scanner 不适用于服务器平台！***

- ***Anti-Spam*** 可检查所有传入的电子邮件并将不需要的电子邮件标记为垃圾邮件 *（垃圾邮件是指未经请求的电子邮件，大多以宣传产品或服务为目的，采取群发方式，每次同时寄给大量的电子邮件地址，充斥收件人的邮箱。垃圾邮件并不包括那些已征得消费者同意而发送的合法的商业电子邮件）*。Anti-Spam 可以通过添加特殊文本字符串修改电子邮件 *（已被认定为垃圾邮件）* 的主题。您可以在电子邮件客户端中轻松地过滤您的电子邮件。Anti-Spam 组件用多种分析方法来处理每一封电子邮件，可最大程度地阻止不需要的电子邮件。Anti-Spam 用定期更新的数据库检测垃圾邮件。也可使用 RBL 服务器 *（存储着 "已知的垃圾邮件发送者 "电子邮件地址的公共数据库）*，以及向白名单 *（从来都不会被标为垃圾邮件）* 和黑名单 *(始终都会被标为垃圾邮件* 手动添加电子邮件地址。



对话框控制项

要在对话框的两个区域之间切换，您仅需单击相应服务面板的任意一处。然后此面板会以浅蓝色突出显示。在对话框的两个区域中，您可找到以下控制项。不管它们属于一个安全服务或其他安全服务 *（Email Scanner 或 Anti-Spam），它们的功能均相同*：

已启用 已禁用 - 无论是在外观和功能上，此按钮均可使用通信灯提醒您。单击

一次即可在两个位置之间切换。绿色代表***已启用***，意味着安全服务已激活，可以完全正常工作。红色代表***已禁用***状态，即此服务已停用。若非必要，请勿停用此服务，强烈建议保持所有安全配置的默认设置。默认设置可保证应用程序的最优性能以及最高安全。如果出于某些原因您要停用服务，则系统会通过红色***警告***符号立即对您发出可能的风险的警告，并通知您此时未受到完全保护。***请注意，您必须马上再次激活此服务！***

设置 - 单击此按钮可重新定向到高级设置界面。相应的对话框会打开，您将可以配置所选的服务，即 Email Scanner 或 Anti-Spam。在高级设置界面中，您可编辑 **AVG Internet Security** 中的每个安全服务的所有配置，但建议仅限经验丰富的用户编辑任何配置！

箭头 - 使用此对话框左上区域的绿色箭头返回到包含组件概述的主用户界面。

3.4.5. Firewall

防火墙是一个系统，用于通过阻止*允许*网传信息在两个或更多网络之间强制执行访问控制策略。Firewall 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。会按指定的规则对这些通讯内容进行评估，然后会允许或禁止传输这些通讯内容。如果 Firewall 识别出入侵企图，则会阻止这种企图，不许入侵者访问计算机。Firewall 经过配置后会允许或拒绝传输通过指定端口的或指定软件应用程序的内部*外部通信（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。它会保护可据以识别您个人身份的信息，以免在未经您同意的情况下将其从您的计算机中发出。Firewall 控制着您的计算机与 Internet 或本地网络上的其它计算机交换数据的方式。在组织中，Firewall 还可防止每台计算机受到网络中其它计算机上的内部用户发起的攻击。

在 **AVG Internet Security** 中，***Firewall*** 控制着通过计算机的每个网络端口传输的所有通信。Firewall 会根据指定的规则，对运行在您计算机中的*要连接至 Internet/本地网络*的应用程序，以及尝试从计算机外部连接至您的 PC 的应用程序进行评估。对于每个应用程序，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。

AVG Firewall 不可用于服务器平台保护！

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。*



***注意：** 安装完您的 AVG Internet Security 之后，Firewall 组件可能要求重启电脑。 在这种情况下，将显示提示您需要重启的组件对话框。 您将直接在对话框中看到**立即重启**按钮。 直到重启之后，Firewall 组件才能完全激活。 同时，对话框中的所有编辑选项将被禁用。 请注意警告信息，并尽快重启电脑！*

可用的 Firewall 模式

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，具体级别可在相应的模式中查看。 简言之，Firewall 模式就是 Firewall 组件的一项特定配置，您可以使用多项此类预定义配置。

- ***自动*** - 在此模式中，Firewall 会自动处理所有网络通信。 您将不能做任何决定。 Firewall 将允许每个已知应用程序的连接，同时会为应用程序创建一个规则，指定应用程序可在以后始终连接。 对于其它应用程序，Firewall 将根据应用程序的行为决定允许还是阻止连接。 但在此类情况下，系统将不会创建规则，当应用程序再次尝试连接时，系统会再次检查应用程序。 建议大多数用户使用此不显眼的自动模式。

- ***交互*** - 如果您想要完全控制进入或来自您计算机的所有网络通信，则推荐使用此模式。 Firewall 会将其控制且系统会在每次尝试通信或转移数据时通知您，让您任意允许或阻止这些尝试。 仅建议高级用户使用。

- ***阻止 Internet 访问*** - Internet 连接已被完全阻止，您无法访问 Internet 且其他人也无法访问您的计算机。 仅建议在特殊情况下短时间使用。

- ***禁用 Firewall 防护*** - 禁用此项将支持进入到或来自您计算机的所有网络通信。 因此，这将使计算机很容易受到黑客攻击。 请仔细考虑此选项。

请注意，特定的自动模式也可在 Firewall 中使用。 当 计算机 或 Identity protection 组件被关闭，会使您的计算机会更容易受到攻击时，会静默激活此模式。 在此类情况下，Firewall 仅会自动允许已知和绝对安全的应用程序。 对于所有其他模式，将会询问您的决定。 这就补偿了停用保护组件并保持您的计算机安全。

我们强烈建议您不要关闭 Firewall！但如果有必要，必须要禁用 Firewall 组件，您可从以上的可用 Firewall 模式列表中选择‘禁用 Firewall 保护’模式。

对话框控制项

此对话框提供有关 Firewall 组件状态基本信息的概述：

- ***Firewall 模式*** - 提供有关当前所选 Firewall 模式的信息。如果您想将当前模式更改为其他模式，请使用位于所提供信息旁的 ***更改*** 按钮，以切换到 Firewall 设置 界面 *（有关使用 Firewall 配置文件的描述和建议，请参见以上段落）*。
- ***文件和打印机共享*** - 通知您是否在此时允许文件和打印机共享 *（双向通信）*。文件和打印机共享实际上意味着共享您在 Windows 中标记为 "已共享 "的任何文件或文件夹、常用磁盘设备、打印机、扫描仪和所有类似设备。仅在认为安全的网络 *（例如在家、在办公室或在学校）*中共享此类项目。但是，如果您连接到公共网络 *（例如机场 Wi-Fi 或 Internet café）*，则您可能不想要共享。
- ***已连接至*** - 提供有关您当前连接至的网络名称的信息。使用 Window XP，网络名称对应您在第一次连接时为特定网络指定的名称。使用 Windows Vista 及更高版本，会自动从网络和共享中心获取网络名称。
- ***重置为默认值*** - 按此按钮将覆盖当前 Firewall 配置，并恢复到基于自动检测的默认配置。

此对话框包含以下图形控制项：

设置 - 单击此按钮可重新定向到高级设置界面。

- ***高级设置*** - 单击此按钮重新定向到 Firewall settings 设置界面，您可在其上编辑所有 Firewall 配置。但是，请记住任何配置都仅应由经验丰富的用户执行！
- ***删除 Firewall 保护*** - 选择此选项后，您将要卸载 Firewall 组件，这样做可能会削弱您的安全保护。如果您仍然要删除 Firewall 组件，确认您的决定，将完全卸载该组件。

箭头 - 使用此对话框左上区域的绿色箭头返回到包含组件概述的 主用户界面 '。

3.4.6. PC 分析器

PC 分析器 组件是一种用于进行详细系统分析和更正（有关如何提高计算机速度和整体性能）的高级工具。可通过 ***修复性能*** 按钮（位于主用户界面对话框）或系统托盘 AVG 图标上下文菜单中的修复性能选项打开。可以直接在该图表中观察分析进度及其结果：



可分析以下几类问题：注册表错误、垃圾文件、磁盘碎片和损坏的快捷方式：

- 通过***注册表错误***可了解 Windows 注册表中的错误数量，这些错误可能会减慢计算机速度，或者导致显示错误消息。
- 通过***垃圾文件***可了解耗尽磁盘空间文件（但很可能被全部删除）的数量。垃圾文件通常包括许多种临时文件以及回收站中的文件。
- ***磁盘碎片***可计算有磁盘碎片的硬盘空间（也就是使用很长一段时间后，大部分文件会分散在物理磁盘的各个位置）的百分比。
- 通过***'脱节的快捷方式'***可找到已不起作用或指向不存在的位置的快捷方式。

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

控制按钮

- ***停止分析***（*在分析运行时显示*）- 按此按钮可中断对计算机的分析。
- ***安装以修复***（*分析完成即会显示*）-很遗憾，**AVG Internet Security** 中 PC 分析器的功能仅限于分析您 PC 的目前状态。但是，AVG 可提供用于进行详细系统分析和更正（有关如何提高计算机速度和整体性能）的高级工具。单击该按钮可重定向至专用网站，以了解更多信息。

3.5. AVG 高级设置

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

3.5.1. 外观

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



语言选择

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

- 在下拉菜单中，选择所需应用程序语言
- 通过按*应用*按钮（*位于该对话框右下角*）*确认所作的选择*
- 按*确认*按钮确认
- 会弹出一个新对话框，告知必须重新启动 AVG Internet Security **才能更改应用程序语言**
- 按*立即重新启动 AVG* 按钮会同意重新启动该程序，等待几秒钟后语言更改即会生效：



系统托盘通知

可在此部分中禁止显示有关 **AVG Internet Security** 应用程序状态的系统托盘通知。 默认情况下允许显示系统通知。 强烈建议保留此配置！ 例如，系统通知会提供扫描或更新进程的启动，或者 **AVG Internet Security** 组件的状态变动的信息。 请务必关注这些通知！

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

- ***显示系统托盘通知*** *（默认情况下已启用）* - 默认情况下会显示所有通知。 取消选中此项可彻底禁止显示所有系统通知。 启用此项后，您可以进一步选择应显示哪些特定通知：
    - ***更新通知*** *（默认情况下已启用）* - 用于决定是否要显示有关 **AVG Internet Security** 更新过程的启动、进度和完成情况的信息。
    - ***Resident Shield 威胁自动删除通知*** *（默认情况下已启用）* - 用于决定是要显示还是禁止显示有关文件保存、复制和打开过程的信息（*仅当已启用 Resident Shield 自动修复选项时才会显示此配置*）。
    - ***扫描通知*** *（默认情况下已启用）* - 用于决定是否要显示有关计划的扫描的自动启动、进度和结果的信息。
    - ***Firewall 通知*** *（默认情况下已启用）* - 用于决定是否要显示有关 Firewall 状态和进程的信息，如该组件的启用/停用警告、潜在网传信息受阻等。 此选项多出了两个具体选项 *（对于其中每个选项的详细说明，请查阅本文档的 Firewall 一章）*：
        - ***网络连接点*** *（默认情况下已禁用）* - 连接到网络时，Firewall 会通知您它是否能够识别此网络以及如何设置文件和打印机共享。
        - ***阻止的应用程序*** *（默认情况下已启用）* - 当未知或可疑的应用程序尝试连接到网络时，Firewall 会阻止此尝试并显示通知。 保持收到通知很有用，但我们建议始终将此功能保持为开启状态。
    - ***Email Scanner 通知*** *（默认情况下已启用）* - 用于决定是否要显示有关扫描所有传入和传出电子邮件的信息。
    - ***统计通知*** *（默认情况下已启用）* - 保持此选项的选中状态可允许在系统托盘中定期显示统计复查通知。
    - ***AVG Accelerator 通知*** *（默认情况下已启用）* - 用于决定是否显示有关执行 ***AVG Accelerator*** 活动的信息。 通过 ***AVG Accelerator*** 服务可使在线视频播放更加流畅，还可使后续下载更加容易。
    - ***启动时间提高通知*** *（默认情况下已禁用）* - 决定您是否希望得到有关计算机启动时间加速的通知。
    - ***AVG Advisor 通知*** *（默认情况下已启用）* - 决定是否在系统托盘的滑动面板中显示有关 AVG Advisor 活动的信息。

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*）。

3.5.2. 声音

在***声音设置***对话框中，您可以指定是否要通过声音通知来获知特定 **AVG Internet Security** 操作的情况：



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

控制按钮

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

3.5.3. 暂时禁用 AVG 保护

在 ***"暂时禁用 AVG 保护"*** 对话框中，您可以选择一次性关闭由 **AVG Internet Security** 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**AVG Internet Security**安装新软件或驱动程序之前禁用，即使安装程序或软件安装向导建议先关闭正在运行的程序和应用程序，以确保在安装过程中不发生意外中断。如果您在安装过程中确实遇到了问题，请先尝试禁用 Resident Shield *（在链接的对话框中，首先取消选中**启用 Resident Shield** 项）*。如果必须暂时禁用 **AVG Internet Security**，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时连接到 Internet 或网络，计算机很容易受到攻击。

如何禁用 AVG 保护软件

请选中 ***暂时禁用 AVG 保护*** 复选框，然后通过按 ***应用*** 按钮确认所作的选择。 在新打开 ***的暂时禁用 AVG 保护*** 对话框中，指定要禁用 **AVG Internet Security** 多长时间。 默认情况下会将该保护软件禁用 10分钟，此段时间应足以完成任何常见任务，例如安装新软件等。 您可以考虑更长的时间，但如果非必要情况，不推荐此选项。 然后，所有停用的组件将会自动再次激活。 您最多可禁用 AVG 保护到下次计算机重新启动的时候。 关闭 ***Firewall*** 组件的独立选项会在暂时禁用 ***AVG 保护*** 对话框中出现。 选中 ***禁用 Firewall 保护*** 执行此操作。



3.5.4. 计算机保护

3.5.4.1. AntiVirus

AntiVirus 和 ***Resident Shield*** 通常可保护您的计算机以免受到所有已知类型的病毒、间谍软件和恶意软件 *（包括所谓的休眠和非活动恶意软件，即已下载但尚未激活的恶意软件）的侵害。*



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

- ***删除威胁前询问我***（*默认情况下已启用*） -选中此框以确保 Resident Shield 将不会自动执行任何操作；而将显示描述检测到的威胁的对话框，让您决定应采取何种操作。如果将此框保留为未选中状态，**AVG Internet Security** 将自动修复感染；如果无法修复，则将该对象移动到隔离区管理。
- ***报告可能不需要的程序和间谍软件威胁***（*默认情况下已启用*） -选中此框以激活对间谍软件和病毒的扫描。间谍软件属于疑似恶意软件类软件：虽然它通常代表了安全风险，但有些程序也可能是被特意安装的。建议保持此功能的激活状态，因为此功能会使计算机更加安全。
- ***详细报告可能不需要的程序的集合***（*默认情况下已禁用*） - 选择此框可检测更多间谍软件：这类程序是指直接从制造商获得后极其安全而无害，但之后却可能被滥用以达到恶意目的的程序。这项附加措施可以进一步提高计算机的安全性，但也可能会阻止合法程序，因此默认情况下已将其禁用。
- ***关闭时扫描文件***（*默认情况下已禁用*） - 关闭时执行的扫描可确保 AVG 在活动的对象（如应用程序、文档等）被打开和关闭时对其进行扫描；此特性有助于防止计算机受到某些类型的复杂病毒的侵害。
- ***扫描可移动介质的启动扇区***（*默认情况下已启用*） -如果选中此框，则扫描所有插入的 USB 闪存盘、外部磁盘驱动器和其它可移动介质的启动扇区有无威胁存在。
- ***使用启发式扫描***（*默认情况下已启用*） -将使用启发式分析方法进行检测（*在虚拟的计算机环境中对已扫描对象的指令进行动态模拟*）。
- ***扫描注册表中引用的文件***（*默认情况下已启用*） -此参数定义 AVG 将扫描添加到

Startup 注册表项的所有可执行文件，以避免在计算机下次启动时执行已知的感染。

- ***启用彻底扫描***（*默认情况下已禁用*）- 特定情况下（*在极其紧急的状态下*），您可以选中此选项以激活最彻底的算法，该算法将深度检查所有可能的威胁对象。但要记住，此方法相当耗时。

- ***启用即时消息传递和 P2P 下载保护功能***（*默认情况下已启用*）-如果要验证即时消息传递通讯（*如 AIM、Yahoo!、ICQ、Skype、MSN Messenger 等*）在点对点网络（*该网络可让多个客户端在无服务器的情况下直接连接，这种情况存在潜在的危险；通常用于共享音乐文件*）中下载的数据是否没有病毒，则选择此项。

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



选中相应复选框可决定是要***扫描所有文件***还是要仅***扫描易受感染的文件和所选文档类型***。要同时加速扫描并提供最高级别的保护，我们建议您保留默认设置。此方法仅可用于扫描可感染文件。在此对话框的相应区域中，您还可找到定义包括在扫描中文件的扩展名的可编辑列表。

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

3.5.4.2. Anti-Rootkit

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



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

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

3.5.4.3. 缓存服务器

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



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

缓存服务器设置对话框中有如下配置选项：

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

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

3.5.5. Email Scanner

在此部分中，可编辑 Email Scanner 和 Anti-Spam 的详细配置：

3.5.5.1. Email Scanner

Email Scanner 对话框分成三个区域：



电子邮件扫描

在此部分中，您可以进行有关传入和/或传出电子邮件的以下基本设置：

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

扫描属性

在此部分，您可以指定扫描电子邮件的方式：

- ***使用启发式扫描***（*默认情况下已启用*） -选中此框将在扫描电子邮件时使用启发式检测方法。启用此选项时，不仅可以按扩展名过滤电子邮件附件，还可以检测附件的实际内容。过滤设置可在邮件过滤对话框中完成。
- ***报告可能不需要的程序和间谍软件威胁***（*默认情况下已启用*） -选中此框以激活对间谍软件和病毒的扫描。间谍软件属于疑似恶意软件类软件：虽然它通常代表了安全风险，但有些程序也可能是被特意安装的。建议保持此功能的激活状态，因为

此功能会使计算机更加安全。

- ***详细报告可能不需要的程序的集合***（*默认情况下已禁用*） -选择此框可检测更多间谍软件：这类程序是指直接从制造商获得后极其安全而无害，但之后却可能被滥用以达到恶意目的的程序。 这项附加措施可以进一步提高计算机的安全性，但也可能会阻止合法程序，因此默认情况下已将其禁用。

- ***扫描压缩包***（*默认情况下已启用*） -选中此框可扫描电子邮件附件中的压缩包的内容。

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

电子邮件附件报告

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

- ***报告受密码保护的存档*** - 受密码保护的存档（*ZIP 和 RAR 等*）不能进行病毒扫描；选中此框可将这类文档报告为具有潜在危险。

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

- ***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（*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具有潜在危险。

- ***将报告的附件移至隔离区管理*** - 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、含有宏的文件和 *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隔离区管理。

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



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

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



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

- ***移除所有可执行文件*** - 将删除所有 *exe 文件
- ***移除所有文档*** - 将删除所有 *doc、*docx、*xls、*xlsx 文件
- ***"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

可在***服务器***部分中编辑 Email Scanner 服务器参数：

- POP3 服务器
- SMTP 服务器
- IMAP 服务器

还可通过***添加新服务器***按钮对传入或传出的邮件定义新服务器。



在此对话框中，您可以使用 POP3 协议，对传入邮件设置新 Email Scanner 服务器：



- ***POP3 服务器名称*** - 您可以在此字段中指定新添加的服务器的名称（*若要添加 POP3 服务器，请在左侧导航菜单的 POP3 菜单项上单击鼠标右键*）。

- ***"登录类型"***-定义用于接收邮件的邮件服务器的确定方法：
  - ***自动*** - 将自动根据您的电子邮件客户端设置进行登录。
  - ***固定主机*** - 这种情况下，程序将始终使用此处指定的服务器。请指定邮件服务器的地址或名称。登录名保持不变。可以使用域名（*例如，pop.acme.com*）以及 IP 地址（*例如，123.45.67.89*）来表示名称。如果此邮件服务器使用非标准端口，则您可以在服务器名称后面指定此端口，二者之间用冒号隔开（*例如，pop.acme.com:8200*）。POP3 通信的标准端口为 110。
- ***其它设置*** - 用于指定更为详细的参数：
  - ***"本地端口"***-指定应在哪个端口允许来自邮件应用程序的通信。随后必须在您的邮件应用程序中将此端口指定为 POP3 通信端口。
  - ***连接*** - 在此下拉菜单中，您可以指定要使用何种连接（*常规*、*SSL/SSL 默认*）。如果选择 SSL 连接，则数据以加密方式发送，因而没有被第三方跟踪或监视的风险。此功能也是只有在目标邮件服务器支持它时才可用。
- ***电子邮件客户端 POP3 服务器激活*** - 选中/取消选中此项可激活或停用指定的 POP3 服务器



在此对话框中，您可以使用 SMTP 协议，对传出邮件设置新 Email Scanner 服务器：



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



在此对话框中，您可以使用 IMAP 协议，对发送邮件设置新 Email Scanner 服务器：



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

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

3.5.6. Web 浏览保护

LinkScanner 设置对话框可让您选中/取消选中以下功能：



- ***启用 Surf-Shield*** - (*默认情况下已启用*)：主动(*实时*)防范访问网站时遇到的漏洞利用网站。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。

3.5.6.1. Online Shield



Online Shield 对话框中有以下选项：

- ***启用 Online Shield***（*默认情况下已启用*） -用于彻底启用/停用 ***Online Shield*** 服务。 对于 ***Online Shield*** 的其它高级设置，请继续在名为 Web 保护的后续对话框中配置。
- ***启用 AVG Accelerator***（*默认情况下已启用*） -激活/停用 AVG Accelerator 服务。 通过 AVG Accelerator 可使在线视频播放更加流畅，还可使后续下载更加容易。 视频加速进程运行时，会通过系统托盘弹出窗口发出通知：



威胁通知模式

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



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：

- ***检查存档*** - *（默认情况下已禁用）*：扫描要显示的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）*：选中此框以激活对间谍软件和病毒的扫描。 间谍软件属于疑似恶意软件类软件：虽然它通常代表了安全风险，但有些程序也可能是被特意安装的。 建议保持此功能的激活状态，因为此功能会使计算机更加安全。
- ***报告可能不需要的应用程序的增强型集合*** - *（默认情况下已禁用）*： 选择此框可检测更多间谍软件：这类程序是指直接从制造商获得后极其安全而无害，但之后却可能被滥用以达到恶意目的的程序。 这项附加措施可以进一步提高计算机的安全性，但也可能会阻止合法程序，因此默认情况下已将其禁用。
- ***使用启发式扫描*** - *（默认情况下已启用）*： 使用启发式分析方法（*在虚拟的计算机环境中对已扫描对象的指令进行动态模拟*）扫描要显示的页面的内容。
- ***启用彻底扫描*** - *（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。
- ***扫描加密（TLS 和 SSL）网络通信*** - *（默认情况下已启用）*：保持选中以允许 AVG 也可扫描所有加密的网络通信，即通过安全协议（SSL 及其新版本 TLS）进行的所有连接。 这适用于使用 HTTPS 的网站及使用 TLS/SSL 的电子邮件客户端连接。 安全通信已经过加密，且进行扫描以发现是否有恶意软件，然后再次加密以安全传送到您的计算机。 在此选项中，您可以决定***包括来自带扩展验***

证 (EV) 证书 的服务器的通信并同时扫描来自带扩展验证证书的服务器的加密网络通信。 签发 EV 证书要求由认证中心进行广泛的验证，且使用此证书营运的网站因此更值得依赖 *（不太可能分发恶意软件）*。 由于此原因，您可以决定不扫描来自 EV 认证的服务器，这样将使加密的通信适当地加快。

- ***使用 Resident Shield 扫描下载的可执行文件*** - *（默认情况下已启用）*： 在下载可执行文件 *（扩展名通常为：exe、bat、com）后*，对其进行扫描。 Resident Shield 在下载前对文件进行扫描，以确保无任何恶意文件进入计算机。 然而，该扫描受到文件待扫描部分的 ***最大大小的限制*** - 参阅本对话框中的下一项目。 因此，大文件分部扫描，绝大多数可执行文件均属此类情况。 可执行文件可在电脑中执行多种任务，因此必须确保其 100% 安全。 为此，可在下载前分部扫描，并在下载完成之后再次立即扫描以确保安全。 建议您始终选中此选项。 如果禁用此选项，您仍可放心使用，AVG 将发现任何潜在的危险代码。 唯一的问题是它通常无法将可执行文件评估为组合体，因此它可能产生一些误报。

该对话框下方的滑块允许您定义 ***文件待扫描部分的最大大小*** - 如果显示的页面中包含文件，您甚至可以在将这些文件下载至计算机之前对其内容进行扫描。 但是，扫描大型文件需要一段时间，网页的下载过程可能会显著变慢。 可用滑块指定仍然需要使用 ***Online Shield*** 扫描的文件的大小上限。 即使所下载的文件大于指定大小，因而不会经过 Online Shield 扫描，您仍会受到保护：如果此文件受到感染，***Resident Shield*** 会立即检测到它。

3.5.7. Identity Protection

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

在 ***Identity Protection 设置*** 对话框中，您可以启用/禁用 Identity Protection 组件的以下基本功能：



***A 激活 Identity Protection** (默认情况下已启用) - 取消选中此项可禁用 Identity 组件。 **如无必要，强烈建议不要取消选中此框！** 激活 Identity Protection 后，您可以指定在检测到威胁时应如何处理：*

- ***始终提示** - 检测到威胁时会询问是否要将其移到隔离区中，以确保不会移除所要运行的应用程序。*
- ***自动隔离检测到的威胁** - 选中此复选框可指定要将可能会检测到的所有威胁都立即移到隔离区管理的安全空间中。 如果保留默认设置，则在检测到威胁时，程序将询问您是否应将其移至隔离区，以确保不会移除您要运行的应用程序。*
- ***自动隔离已知威胁** (默认情况下已启用) - 如果想将检测后认为是疑似恶意软件的所有应用程序都自动直接移到隔离区管理中，请保持此选项的选中状态。*

3.5.8. 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
- 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
- 外壳扩展扫描 - 直接从 Windows Explorer 环境中对选定对象进行的特定扫描
- 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

3.5.8.1. 扫描整个计算机

通过***扫描整个计算机***选项，可编辑软件供应商预先指定的某项扫描（即扫描整个计算机）的参数：



扫描设置

扫描设置区域提供了可以选择启用/禁用的扫描参数的列表：

- ***无需询问即修复/删除病毒感染***（*默认情况下已启用*） -如果在扫描期间发现病毒并且有修复方案，则可以自动对其进行修复。如果不能自动修复受感染文件，则会将受感染对象移到隔离区管理中。
- ***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*） -选中此框以激活对间谍软件和病毒的扫描。间谍软件属于疑似恶意软件类软件：虽然它通常代表了安全风险，但有些程序也可能是被特意安装的。建议保持此功能的激活状态，因为此功能会使计算机更加安全。
- ***详细报告可能不需要的程序的集合***（*默认情况下已禁用*） - 选择此框可检测更多间谍软件：这类程序是指直接从制造商获得后极其安全而无害，但之后却可能被滥用以达到恶意目的的程序。这项附加措施可以进一步提高计算机的安全性，但也可能会阻止合法程序，因此默认情况下已将其禁用。
- ***扫描跟踪 Cookie***（*默认情况下已禁用*） -此参数用于保证在扫描期间应检测 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*）。
- ***扫描内部存档***（*默认情况下已禁用*） -此参数用于保证在扫描时应检查存储在存档（如 ZIP 和 RAR 等文件）中的所有文件。
- ***使用启发式分析***（*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*）将成为在扫描期间的病毒检测方法之一。
- ***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。
- ***启用彻底扫描***（*默认情况下已禁用*） -在特定情况下（*怀疑计算机受到感染*），您可以选中此选项以激活最全面的扫描算法，该算法甚至会对计算机上极难被感染的区域进行扫描以确保绝对安全。不过要记住，此方法相当耗时。
- ***扫描 rootkit***（*默认情况下已启用*） - Anti-Rootkit 扫描用于在您的 PC 中搜索是否可能存在 rootkit（例如，可以在您的计算机中掩盖恶意软件活动的程序和技术）。如果检测到 Rootkit，并不一定意味着您的计算机已受到感染。有些情况下，特定的驱动程序或正常应用程序的组成部分可能会被误检测为 Rootkit。

您还应决定是否需要扫描

- ***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，不可能受到病毒感染*）。此外，您还可以通过扩展名指定应始终扫描的文件。
- 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

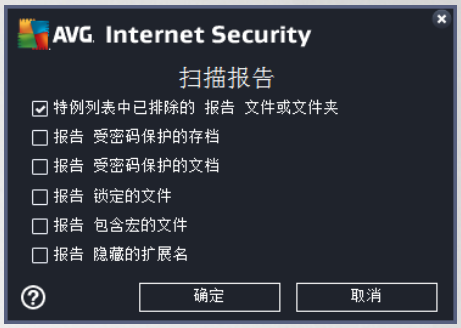
对此类文件进行扫描。

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，在此窗口中可以通过勾选若干项来定义应报告哪些扫描结果：



3.5.8.2. 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几乎完全相同，但是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。*

3.5.8.3. 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，请参见扫描 Windows 资源管理器一章：



该扫描的编辑选项与扫描整个计算机的编辑选项几乎完全相同。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***显示扫描进度和结果***部分，从中可指定是否能够从 AVG 用户界面中访问扫描进度和扫描结果。您还可以指定仅当在扫描期间检测到感染的情况下才应显示扫描结果。

3.5.8.4. 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。*

3.5.9. 计划

在***"计划"***区域中，您可以编辑以下各项的默认设置：

- 计划内扫描
- 指定更新计划
- 程序更新计划
- Anti-Spam 更新计划

3.5.9.1. 计划的扫描

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



接下来，名为***名称***的文本字段（*已对所有默认计划停用此字段*）会说明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**项上右键单击来添加新计划*），您可以自行指定名称，在这种情况下此文本字段将打开，以进行编辑。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区分开来。

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。有效的描述性名称应该类似于"系统区域扫描"等。此外，也没有必要在扫描名称中指定是对整个计算机的扫描，还只是对选定文件或文件夹的扫描。*

在此对话框中，可以进一步定义下列扫描参数：

计划运行频率

可在此指定新计划的扫描启动任务的时间间隔。此时间间隔的定义方式有三种：指定经过一段特定的时间后重复启动扫描（***运行时间间隔 ...***），或通过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（***计算机启动时运行***）。

高级计划选项

- ***如果已错过任务，则在计算机启动时运行*** - 如果您计划在特定时间运行任务，则此选项将确保：如果计算机在计划的时间处于关机状态，则在计算机下次启动时执行扫描。
- ***在计算机处于省电模式时依然运行*** - 即使计算机在计划的时间靠电池电量运行，也应执行任务。



设置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，并在扫描过程中应用其功能。***除非有必要更改这些设置，否则我们建议保留预定义的配置***：

- ***无需询问即修复/删除病毒感染***（*默认情况下已启用*）：如果在扫描过程中发现病毒，并且存在解决方案，则自动执行修复。如果不能自动修复受感染文件，则会将受感染对象移到隔离区管理中。
- ***报告可能不需要的应用程序和间谍软件威胁***（*默认情况下已启用*）：选中此框以激活对间谍软件和病毒的扫描。间谍软件属于疑似恶意软件类软件：虽然它通常代表了安全风险，但有些程序也可能是被特意安装的。建议保持此功能的激活状态，因为此功能会使计算机更加安全。
- ***报告可能不需要的应用程序的增强型集合***（*默认情况下已禁用*）：选择此框可检测更多间谍软件：这类程序是指直接从制造商获得后极其安全而无害，但之后却可能被滥用以达到恶意目的的程序。这项附加措施可以进一步提高计算机的安全性，但也可能会阻止合法程序，因此默认情况下已将其禁用。
- ***扫描跟踪 Cookie***（*默认情况下已禁用*）：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*）。
- ***扫描内部存档***（*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存档（如 ZIP 和 RAR 等文件）内也不例外。
- ***使用启发式分析***（*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*）将成为在扫描期间的病毒检测方法之一。

- ***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。
- ***启用彻底扫描***（*默认情况下已禁用*）：在特定情况下（*怀疑计算机受到感染*），您可以选中此选项以激活最全面的扫描算法，该算法甚至会对计算机上极难被感染的区域进行扫描以确保绝对安全。 不过要记住，此方法相当耗时。
- ***扫描 Rootkit***（*默认情况下已启用*）：Anti-Rootkit 扫描用于在您的计算机中搜索是否可能存在 Rootkit（可以在您的计算机中掩盖恶意软件活动的程序和技术）。 如果检测到 Rootkit，并不一定意味着您的计算机已受到感染。 有些情况下，特定的驱动程序或正常应用程序的组成部分可能会被误检测为 Rootkit。

您还应决定是否需要扫描

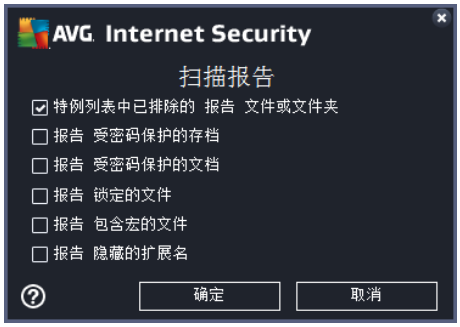
- ***所有文件类型***，选择此选项可以通过提供一列由逗号分隔（*保存后逗号会变成分号*）、不应扫描的文件扩展名来定义一些排除在扫描范围之外的特例。
- ***所选文件类型*** - 可以指定希望仅扫描可能受到感染的文件（*将不扫描不可能遭到感染的文件，例如某些纯文本文件或某些其它的非可执行文件*），其中包括媒体文件（*视频、音频文件 -如果将此框保留为未选中状态，则会进一步缩短扫描时间，因为这些文件通常很大，不可能受到病毒感染*）。 此外，您还可以通过扩展名指定应始终扫描的文件。
- 您也可以选择指定要***扫描不带扩展名的文件*** - 默认情况下此选项已启用；我们建议，除非确有必要更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

在此区域中，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*用户敏感性*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，在此窗口中可以通过勾选若干项来定义应报告哪些扫描结果：



计算机关闭选项

在***计算机关闭选项***部分，您可决定在结束运行扫描进程后是否自动关闭计算机。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***位置***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。

3.5.9.2. 定义更新计划

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



可在此对话框中设置定义更新计划的某些详细参数。名为***名称***的文本字段（*已对所有默认计划停用此字段*）显示程序供应商对此计划指定的名称。

计划运行频率

默认情况下，新的病毒定义更新可用时，将自动启动该任务（***自动运行***）。如果没有必要，我们建议切勿更改此配置！这样，您可将该任务设置为手动启动，并指定启动新安排的定义更新的时间间隔。上述时间安排的指定方式有两种：指定经过一段特定的时间后反复启动更新（***运行时间间隔 ...***），或通过定义确切的日期和时间（***在特定的时间运行***）。

高级计划选项

在此区域中，可以定义当计算机处于省电模式或完全关闭时，应该*不应*启动的定义更新的条件。

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 系统托盘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*）。

3.5.10. 更新

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



文件更新时间

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

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

更新后进行内存扫描

选中此复选框可保证，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 –（*默认情况下已启用*）在每次启动 AVG 程序更新前，都会创建一个系统还原点。如果更新过程失败并且您的操作系统崩溃，则您始终都可以利用此还原点将您的操作系统还原成其原始配置。可通过开始 *所有程序 附件 系统工具 系统还原*访问此选项，但建议仅限经验丰富的用户进行任何更

改！如果您要利用此功能，请将此复选框保持选中状态。

- ***使用 DNS 更新*** *(默认情况下已启用)*- 选中此选项后，一启动更新 **AVG Internet Security**，就会在 DNS 服务器中查找有关最新病毒数据库版本和最新程序版本的信息。然后就会仅下载并应用最小的不可或缺的所需更新文件。这样会最大程度地减小下载的数据总量，更新过程也会加快。

- ***需要确认才能关闭正在运行的应用程序****(默认情况下已启用)* -这可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*** *(默认情况下已启用)* -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。

3.5.10.1. 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：

- ***不使用代理*** - 默认设置
- ***'使用代理'***
- ***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：

- ***从浏览器执行*** - 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

3.5.10.2. 管理

更新管理 对话框中有两个选项，这两个选项分别可通过以下两个按钮显示出来：



- ***删除临时更新文件*** - 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*）

- ***将病毒数据库还原至上一版本*** - 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*)

3.5.11. 特例

在***特例***对话框中，您可定义特例，即 **AVG Internet Security** 将忽略的项。 通常，如果 AVG 连续将程序或文件检测为威胁或阻止安全网站为危险，则需要定义特例。 将此类文件或网站添加到此特例列表，AVG 将不会再进行报告或阻止。

请确保正在讨论的文件、程序或网站绝对安全！



如果已定义任何特例，则此对话框的图表中会显示特例列表。 每项旁边都会有一个复选框。 如果选中了某个复选框，则此特例会生效；如果未选中，则只是定义了此特例，但当前未使用。 通过单击一个列标题，您可以根据相应的标准排序允许项。

控制按钮

- ***添加特例*** - 单击此框可打开一个新对话框，您可在其中指定从 AVG 扫描中排除的项：



首先，将需要您定义对象的类型，是应用程序、文件、文件夹、URL 还是证书。然后，您将需要浏览磁盘以提供相应项目的路径或键入 URL。最后，您可选择哪些 AVG 功能应忽略所选对象（*Resident Shield*、*Identity Protection* 和 *扫描*）。

- ***编辑*** - 仅在已定义某些特例并在图表中列出时，此按钮才处于可用状态。然后，您可使用此按钮通过所选特例打开编辑对话框，并配置特例参数。
- ***删除*** - 使用此按钮可取消之前定义的特例。您可逐个删除特例或在列表中高亮显示特例块，然后取消已定义的特例。取消特例之后，AVG 会再次检查相应的文件、文件夹或 URL。请注意，仅会删除特例，不是文件或文件夹本身！
- ***全部删除*** - 使用此按钮以删除列表中所有定义的特例。

3.5.12. 隔离区管理



通过***隔离区维护***对话框，可定义关于管理隔离区管理中存储的对象的若干参数：

- ***限制隔离区大小***–使用滑块可设置隔离区管理的最大大小。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隔离区管理中的最大时长（***删除存储时间超过 ...天的文件***），以及隔离区管理中最大待存储文件数（***最大待存储文件数***）。

3.5.13. AVG 自我防护



自我防护可让 **AVG Internet Security** 保护其自身进程、文件、注册表项和驱动程序免遭变更或停用。 使用此类保护的主要原因是一些复杂的威胁尝试解除防病毒保护，然后肆意对您的计算机造成损害。

我们建议您保持此功能开启！

3.5.14. 隐私首选项

隐私首选项 对话框邀请您参加 AVG 产品改进，然后帮助我们提升对所有用户的保护程度。 您的报告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。 此报告会自动生成，因此不会给您带来任何不便。 此报告中不包括任何个人数据。 报告检测到的威胁是可选操作，但我们也确实请求您保持此选项的已启用状态。 这有助于我们为您和其它 AVG 用户改善保护功能。



在该对话框中，提供了以下选项：

- ***I'我愿意通过参与 AVG 产品改进计划，帮助 AVG 改进其产品*** *（默认情况下已启用）* - 如果您想帮助我们进一步改进 **AVG Internet Security**，则保持此复选框的选中状态。它可向 AVG 报告所有遇到的威胁，这样我们将能够从世界各地的所有参与者处收集有关恶意软件的最新信息，然后就会提升对所有用户的保护程度。报告会自动生成，因此不会引起任何不便，也不会向报告中添加个人数据。
    - ***允许发送经过用户确认的有关错误识别身份的电子邮件的数据据*** *（默认情况下已启用）* - 发送有关被错误识别为垃圾邮件的电子邮件或有关 Anti-Spam 服务未检测到的垃圾邮件的信息。当发送此类信息时，系统将要求您确认。
    - ***允许发送有关识别身份的或可疑威胁的匿名数据*** *（默认情况下已启用）* - 发送在计算机上检测到的有关任何可疑或确实危险的代码或行为模式 *（可能为病毒、间谍软件，或要访问的恶意网页）* 的信息。
    - ***允许发送有关产品使用情况的匿名数据*** *（默认情况下已启用）* - 发送有关应用程序使用情况的基本统计信息（例如，检测、已启动扫描、成功或不成功更新等项的数目）。
- ***允许在云中验证检测*** *（默认情况下已启用）* - 对检测到的威胁进行检查以确认是否真的受到感染，以免出现误报。
- ***I'd我愿意 AVG 通过打开 AVG Personalization 对我的体验进行个性化*** *（默认情况下为关闭）* - 此功能将匿名分析 PC 上安装的程序和应用程序的行为。根据这一分析，AVG 可为您提供恰好符合您需要的服务，以最大程度地确保您的安全。

3.5.15. 忽略错误状态

在 ***忽略错误状态*** 对话框中，可选中不想了解其情况的组件：



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

- 系统托盘图标 –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***忽略错误状态***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。 按***确定***按钮进行确认。

3.5.16. Advisor - 已知网络

AVG Advisor 包含监控您所连接到的网络的功能。如果发现了新网络（*带有已使用的网络名称，并让您感到困扰*），则它将通知您并建议您检查网络的安全性。 如果您确定未知网络安全，则可将其保存到此列表（*通过在检测到未知网络之后，AVG Advisor 托盘通知中提供的链接滑过系统托盘执行。 有关详细信息，请参见有关 AVG Advisor 的章节*）。 然后，AVG Advisor 将记住该网络的唯一属性（*特别是 MAC 地址*），，且下次不会显示通知。 系统会将连接的每个网络自动视为已知网络并添加到列表。 您可通过按***删除***按钮删除各个条目；然后，相应的网络就再次被视为未知且可能不安全的网络。

在此对话窗口中，您可选择系统视为已知的网络：



注意： *注意：AVG Advisor 中的已知网络功能在 Windows XP 64 位中不受支持。*

3.6. 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的高级参数。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编辑该组件的高级参数。此配置可以在基本或专家模式中显示。在您首次进入配置窗口时，它会在提供以下参数编辑的基本版本中打开：

- 常规
- 应用程序
- 文件和打印机共享

在此对话框的底部，您将看到***专家模式***按钮。按此按钮会在用于导航高级 Firewall 配置的对话框中显示更多选项。

- 高级设置
- 预定义网络
- 系统服务
- 日志

3.6.1. 常规

常规信息对话框提供所有可用 Firewall 模式的概述。 Firewall 模式的当前选项可通过从菜单中选择另一模式更改。

但是，所有 AVG Internet Security 组件均已由软件供应商为了提供最佳性能而设置好。除非确实有理由更改默认配置，否则请勿如此操作。对设置的任何更改只应当由经验丰富的用户执行。



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，具体级别可在相应的模式中查看。 简言之，Firewall 模式就是 Firewall 组件的一项特定配置，您可以使用多项此类预定义配置：

- ***自动*** - 在此模式中，Firewall 会自动处理所有网络通信。 您将不能做任何决定。 Firewall 将允许每个已知应用程序的连接，同时会为应用程序创建一个规则，指定应用程序可在以后始终连接。 对于其它应用程序，Firewall 将根据应用程序的行为决定允许还是阻止连接。 但在此类情况下，系统将不会创建规则，当应用程序再次尝试连接时，系统会再次检查应用程序。 ***建议大多数用户使用此不显眼的自动模式。***

- ***交互*** - 如果您想要完全控制进入或来自您计算机的所有网络通信，则推荐使用此模式。 Firewall 会将其控制且系统会在每次尝试通信或转移数据时通知您，让您任意允许或阻止这些尝试。 仅建议高级用户使用。

- ***阻止对 Internet 的访问*** - Internet 连接已完全阻止，您无法访问 Internet 且外面的人无法访问您的计算机。 仅建议在特殊情况下短时间使用。

- ***关闭 Firewall 防护*** - 禁用此项将启用进入到或来自您计算机的所有网络通信。 因此，这将使计算机很容易受到黑客攻击。 请仔细考虑此选项。

请注意，特定的自动模式也可在 Firewall 中使用。 当 计算机 或 Identity protection 组件被关闭，会使您的计算机会更容易受到攻击时，会静默激活此模式。 在此类情况下，Firewall 仅会自

动允许已知和绝对安全的应用程序。对于所有其他模式，将会询问您的决定。这就补偿了停用保护组件并保持您的计算机安全。

3.6.2. 应用程序

应用程序对话框列出了目前通过网络尝试通信的所有应用程序，以及所分配操作的图标：



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

- - 允许与所有网络通信
- - 阻止通信
- - 已定义高级设置

请注意，只有已安装的应用程序才会被检测到。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。对于后一种情况，您可以将您的回答作为一项永久规则保存下来（随后此规则将被列在该对话框中）。

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"。选择在应用程序尝试网络通信时应触发的操作：阻止（*始终阻止通信*）、允许（*始终允许通过任何网络通信*）、询问（*将会让您决定是否应允许或阻止通信*）。***这些项目的设置选项不同于普通应用程序，仅供经验丰富的用户使用。强烈建议不要修改这些设置！***

控制按钮

此列表可使用以下控制按钮进行编辑：

- ***添加*** - 用于打开空的对话框，以便定义新应用程序规则。
- ***编辑*** - 用于打开同一对话框，其中的数据用于编辑现有的一套应用程序规则。
- ***删除*** - 用于从列表中删除所选应用程序。

3.6.3. 文件和打印机共享

文件和打印机共享实际上意味着共享您在 Windows 中标记为 "已共享 "的任何文件或文件夹、常用磁盘设备、打印机、扫描仪和所有类似设备。 仅在认为安全的网络*（例如在家、在办公室或在学校）*中共享此类项目。 但是，如果您连接到公共网络 *（例如机场 Wi-Fi 或 Internet café）*，则您可能不想要共享。 AVG Firewall 可轻松允许或阻止共享，并可让您保存对已访问网站的选择。



在***文件和打印机共享***对话框中，您可编辑文件和打印机共享配置和当前已连接的网络。 使用 Window XP，网络名称对应您在第一次连接时为特定网络指定的名称。 使用 Windows Vista 及更高版本，会自动从网络和共享中心获取网络名称。

3.6.4. 高级设置

'高级设置'对话框中的任何编辑都仅限经验丰富的用户执行！



高级设置对话框可让您进入退出以下 Firewall 参数：

- ***允许从 Firewall 支持的虚拟机传入传出的所有通信*** - 支持在虚拟机（例如 VMWare）中进行网络连接。
- ***允许到虚拟专用网络 (VPN)*** 的所有通信 -支持进行 VPN 连接*（用于连接到远程计算机）*。
- ***记录未知的传入传出通信*** - 未知应用程序尝试的所有通信 *（传入传出）* 将记录在 Firewall 日志中。
- ***对所有应用程序规则禁用规则验证*** - Firewall 继续监视每个应用程序规则覆盖的所有文件。二进制文件发生修改时，Firewall 将再次尝试使用标准方式对应用程序的可信度进行确认，即验证其证书，在可信应用程序数据库中对其进行查找等。如果不能判定应用程序是安全的，Firewall 将进一步威胁基于所选模式的应用程序：
  - 如果 Firewall 在***自动模式***下运行，则默认情况下将允许该应用程序；
  - 如果 Firewall 在***交互模式下***下运行，则会阻止该应用程序，并显示询问对话框以询问用户决定如何处理该应用程序。

有关处理特定应用程序的所需程序当然可在应用程序对话框中对每个应用程序单独进行定义。

3.6.5. 预定义网络

'预定义网络'对话框中的任何编辑都仅限经验丰富的用户执行！



预定义网络对话框提供了您的计算机连接到的所有网络的列表。该列表中有关于检测到的各个网络的以下信息：

- ***网络*** - 其中有与计算机相连的所有网络的名称列表。
- ***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*** - - 打开一个新对话框窗口，您可在其中编辑新预定义的网络的参数，即提供 ***网络名称***和指定***IP 地址范围***：



- ***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*** - 用于从网络列表中删除所选网络的引用。

3.6.6. 系统服务

只有经验丰富的用户才能在‘系统服务和协议’对话框中进行编辑！



系统服务和协议对话框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：

- ***系统服务和协议*** - 此列用于显示相应系统服务的名称。
- ***操作*** - 此列用于显示代表所分配操作的图标：
  - o 允许与所有网络通信
  - o 阻止通信

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

用户定义的系统规则

若要打开一个新对话框以定义您自己的系统服务规则（*见下图*），请按***‘管理用户系统规则’***按钮。 如果您决定在系统服务和协议列表中编辑任意现有选项的配置，则会打开相同窗口。 此对话框顶部显示的是目前已编辑过的系统规则的所有详细信息的概况，底部显示的则是所选详细信息。 可通过相应按钮编辑、添加或删除规则详细信息：



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。 如果您不熟悉通信协议的类型、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。

3.6.7. 日志

"日志"对话框中的任何编辑都仅限经验丰富的用户执行！

在***日志***对话框中，您可以查看所有已记录的 Firewall 操作和事件的列表，以及显示在两个选项卡中相关参数的详细说明：

- ***流量日志*** - 此选项卡提供了尝试连接到网络的所有应用程序的活动相关信息。 对于每个项目，您将找到有关事件时间、应用程序名称、对应的记录操作、用户名、PID、流量方向、协议类型、远程及本地端口号的信息，以及有关本地和远程 IP 地址的信息。



- ***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。



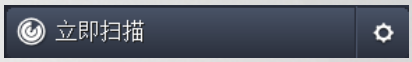
控制按钮

- ***'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。
- ***删除日志*** - 按此按钮可删除图表中的所有条目。

3.7. AVG 扫描

默认情况下，**AVG Internet Security** 不会执行扫描操作，因为第一次扫描执行完毕后（*将要求您启动*），就应该会得到 **AVG Internet Security** 常驻组件的严密保护，这些常驻组件始终处于警戒状态，根本不会让任何恶意代码进入计算机。当然，可以计划一个扫描，以便以固定时间间隔执行扫描，也随时均可按需手动启动扫描。

AVG 扫描界面可通过以图形方式划分成两个部分按钮从主用户界面中进行访问：



- ***立即扫描*** - 按此按钮可立即启动扫描整个计算机，并在自动打开的报告窗口中查看其进度和结果。



- ***选项*** - 选择此按钮（*以图形方式在绿色字段中显示为三条水平线*）可打开 ***扫描选项*** 对话框，您可在其中管理计划的扫描并编辑扫描整个计算机/扫描特定文件或文件夹的参数。



在 ***扫描选项*** 对话框中，您可看到三个主要的扫描配置部分：

- ***管理计划的扫描*** - 单击此选项可打开带有所有扫描计划概览的新对话框。 在定义自己的扫描之前，您只可以看到图表中列出的软件供应商预定义的某一个计划的扫描。 默认情况下，该扫描已关闭。 要进行开启，请在其上右键单击，从上下文菜单中选择*启用任务*选项。 启用计划的扫描之后，您就可通过*编辑扫描计划*按钮编辑其配置。 您也可单击*添加扫描计划*按钮创建您自己的新扫描计划。

- ***扫描整个计算机 设置*** - 可将此按钮划分为两部分。 单击*扫描整个计算机*选项可立即启动扫描整个计算机（*有关扫描整个计算机的详细信息，请参见名为预定义扫描 扫描整个计算机的相应章节*）。 单击*设置*部分将会转至扫描整个计算机的配置对话框。

- ***扫描特定的文件或文件夹 设置*** - 此按钮也可划分为两部分。 单击*扫描特定的文件或文件夹*选项可自动启动扫描计算机的所选区域（*有关扫描所选文件或文件夹的详细信息，请参见名为预定义扫描 扫描特定的文件或文件夹的相应章节*）。 单击*设置*部分将会转至扫描特定的文件或文件夹的配置对话框。

- ***扫描计算机是否存在 Rootkit/设置*** - 在标签为*扫描计算机是否存在 Rootkit* 按钮左侧可立即启动 Anti-rootkit 扫描（*有关 Rootkit 扫描的详细信息，请参阅名为预定义扫描 扫描计算机是否存在 Rootkit 的相应章节*）。 单击*设置*部分将会转至 Rootkit 扫描的配置对话框。

3.7.1. 预定义扫描

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

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

3.7.1.1. 扫描整个计算机

扫描整个计算机可用于扫描您的整个计算机是否存在感染和/或可能不需要的应用程序。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隔离区管理。在计算机上，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

扫描整个计算机可通过单击***立即扫描***按钮直接从主用户界面中启动。对于此类型的扫描，无需进一步配置任何特定设置，扫描将立即开始。您可在***扫描整个计算机正在进行中***对话框中***查看其进度和结果***（*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

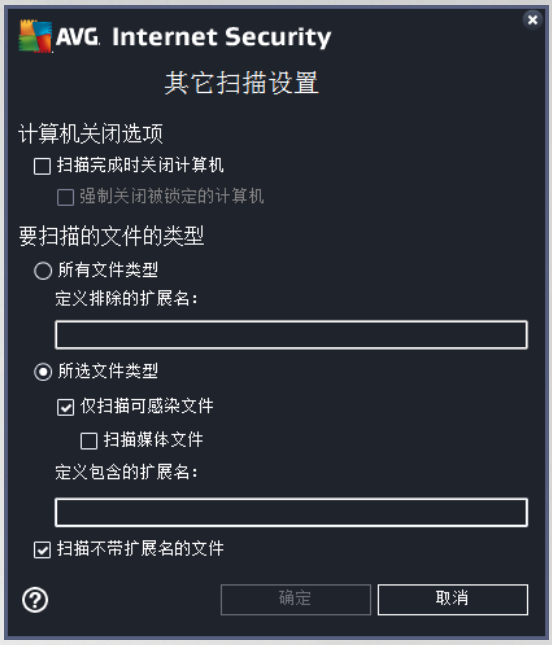
您可编辑***扫描整个计算机 -设置***对话框中***扫描整个计算机***配置（*可通过扫描选项对话框中的扫描整个计算机的设置链接访问此对话框*）。***建议保留默认设置，若非必要，请勿更改！***



在扫描参数列表中，您可以根据需要启用 禁用特定参数：

- ***无需询问即修复 删除病毒感染*** *（默认情况下已启用）* - 如果在扫描期间发现病毒并且有修复方案，则可以自动对其进行修复。 如果不能自动修复受感染文件，则会将受感染对象移到隔离区管理中。
- ***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）* - 选中此框以激活对间谍软件和病毒的扫描。 间谍软件属于疑似恶意软件类软件：虽然它通常代表了安全风险，但有些程序也可能是被特意安装的。 建议保持此功能的激活状态，因为此功能会使计算机更加安全。
- ***详细报告可能不需要的程序的集合*** *（默认情况下已禁用）* - 选择此框可检测更多间谍软件：这类程序是指直接从制造商获得后极其安全而无害，但之后却可能被滥用以达到恶意目的的程序。 这项附加措施可以进一步提高计算机的安全性，但也可能会阻止合法程序，因此默认情况下已将其禁用。
- ***扫描跟踪 Cookie*** *（默认情况下已禁用）* - 此参数用于指定应检测的 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）*。
- ***扫描内部存档*** *（默认情况下已禁用）* - 此参数用于定义在扫描时应检查存储在存档（如 ZIP 和 RAR 等）中的所有文件。
- ***使用启发式分析*** *（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）* 将成为在扫描期间的病毒检测方法之一。
- ***扫描系统环境*** *（默认情况下已启用）* - 扫描还将检查您计算机的系统区域。
- ***启用彻底扫描*** *（默认情况下已禁用）* - 在特定情况下 *（怀疑计算机受到感染）*，您可以选中此选项以激活最全面的扫描算法，该算法甚至会对计算机上极难被感染的区域进行扫描以确保绝对安全。 不过要记住，此方法相当耗时。
- ***扫描 Rootkit*** *（默认情况下已启用）*：将 Anti-Rootkit 扫描作为扫描整个计算机过程的一部分。 Anti-Rootkit 扫描还可以单独启动。

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



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

  - ***要扫描的文件的类型*** - 您也可决定是否要进行扫描：

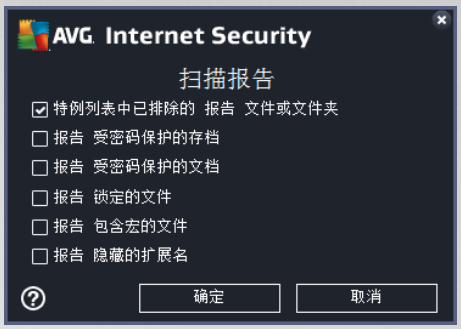
    - ***所有文件类型***，选择此选项可以通过列出不应扫描的文件扩展名（由逗号分隔）指定特例，不对其进行扫描；

    - ***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，不可能受到病毒感染*）。此外，您还可以通过扩展名指定应始终扫描的文件。

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

- ***调整扫描的完成速度*** - 您可以使用滑块更改扫描进程的优先级。默认情况下，此选项值设为*用户敏感性*级别，即自动确定资源的使用。另外，您也可以用较低的速度运行扫描进程，这意味着将最大限度地减少系统资源负荷（*如果您需要使用计算机，而不在乎扫描过程所持续的时间，则此选项将十分有用*）；也可以用较快的速度运行扫描，这会增加对系统资源的需求（*例如，在计算机暂时无人值守时*）。

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



***警告：** 这些扫描设置与新定义的扫描的参数相同 -有关说明请参见 AVG 扫描 扫描计划 扫描方式章节。 如果您决定更改**扫描整个计算机**的默认配置，则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。*

3.7.1.2. 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度与采用 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隔离区管理。 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可通过单击**扫描特定的文件或文件夹**按钮直接从扫描选项对话框中启动。 将打开一个名为***选择要扫描的特定文件或文件***的新对话框。 在您计算机的树结构中，选择您想要扫描的那些文件夹。 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

您可编辑***扫描特定的文件或文件夹 -设置***对话框中的***扫描特定的文件或文件夹配置***（*可通过扫描选项对话框的 扫描特定的文件或文件夹 中的 设置 链接访问此对话框*）。***建议保留默认设置，若非必要，请勿更改！***

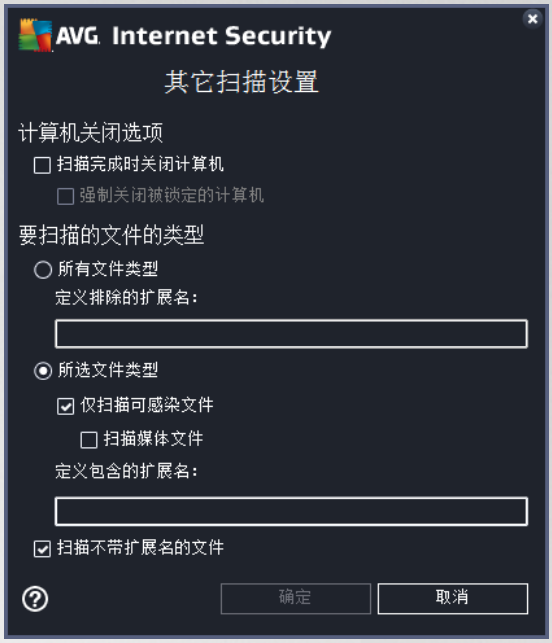


在扫描参数列表中，您可以根据需要启用 禁用特定参数：

- ***无需询问即修复 删除病毒感染***（*默认情况下已启用*）：如果在扫描过程中发现病毒，并且存在解决方案，则自动执行修复。如果不能自动修复受感染文件，则会将受感染对象移到隔离区管理中。
- ***报告可能不需要的应用程序和间谍软件威胁***（*默认情况下已启用*）：选中此框以激活对间谍软件和病毒的扫描。间谍软件属于疑似恶意软件类软件：虽然它通常代表了安全风险，但有些程序也可能是被特意安装的。建议保持此功能的激活状态，因为此功能会使计算机更加安全。
- ***报告可能不需要的应用程序的增强型集合***（*默认情况下已禁用*）：选择此框可检测更多间谍软件：这类程序是指直接从制造商获得后极其安全而无害，但之后却可能被滥用以达到恶意目的的程序。这项附加措施可以进一步提高计算机的安全性，但也可能会阻止合法程序，因此默认情况下已将其禁用。
- ***扫描跟踪 Cookie***（*默认情况下已禁用*）：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）*。
- ***扫描内部存档***（*默认情况下已启用*）：此参数定义扫描时应检查存储在内部存档（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*）将成为在扫描期间的病毒检测方法之一。
- ***扫描系统环境***（*默认情况下已禁用*）：扫描进程还会检查计算机的系统区域。
- ***启用彻底扫描***（*默认情况下已禁用*）：在特定情况下（*怀疑计算机受到感染*），您

可以选中此选项以激活最全面的扫描算法，该算法甚至会对计算机上极难被感染的区域进行扫描以确保绝对安全。 不过要记住，此方法相当耗时。

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

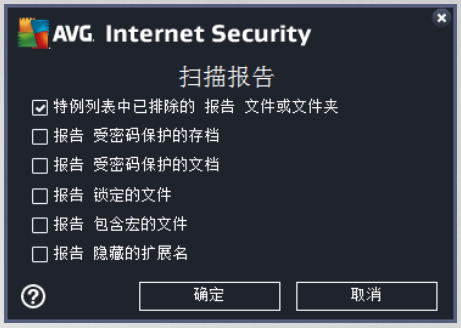


  - ***计算机关闭选项*** - 决定在扫描过程完成时是否应自动关闭计算机。 在确认此选项（***扫描完成时关闭计算机***）后，将激活一个新选项（***强制关闭锁定的计算机***），通过该选项，即使目前已锁定计算机也可关机。
  - ***要扫描的文件的类型*** - 应决定是否要进行扫描：
    - ***所有文件类型***，选择此选项可以通过列出不应扫描的文件扩展名（由逗号分隔）指定特例，不对其进行扫描；
    - ***所选文件类型*** - 可以指定希望仅扫描可能受到感染的文件（*将不扫描不可能遭到感染的文件，例如某些纯文本文件或某些其它的非可执行文件*），其中包括媒体文件（*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，不可能受到病毒感染*）。此外，您还可以通过扩展名指定应始终扫描的文件。
    - 您也可以选择决定***扫描不带扩展名的文件*** - 默认情况下此选项已启用；我们建议，除非确有必要更改，否则将其保持启用。 不带扩展名的文件相当可疑，应随时对此类文件进行扫描。

- ***调整扫描的完成速度*** - 您可以使用滑块更改扫描进程的优先级。 默认情况下，此选项值设为*用户敏感性*级别，即自动确定资源的使用。 另外，您也可以用较低的速度运行扫描进程，这意味着将最大限度地减少系统资源负荷（*如果您需要使用计算机，而不在乎扫描过程所持续的时间，则此选项将十分有用*）；也可以用较快的速度运行扫描，这会增加对系统资源的需求（*例如，在计算机暂时无人值守时*）。

- ***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，此配置将被用作您新计划的所有扫描的模板（所有自定义的扫描都基于扫描选定的文件或文件夹的当前配置）。*

3.7.1.3. 扫描计算机是否存在 Rootkit

扫描计算机是否存在 Rootkit 用于检测并有效删除危险 Rootkit（即可在您的计算机中掩饰恶意软件存在的程序和技术）。 Rootkit 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。 该扫描可以根据一组预定义的规则来检测是否存在 Rootkit。 如果找到 Rootkit，并不一定表示它已受到感染。 有时，Rootkit 会被用作驱动程序，或者是正当应用程序的组成部分。

启动扫描

扫描计算机是否存在 Rootkit 可通过在扫描选项对话框单击 ***扫描计算机是否存在 Rootkit*** 按钮直接启动。 将打开一个名为 ***Anti-rootkit 扫描正在进行*** 的新对话框，显示所启动扫描的进度：



编辑扫描配置

您可在 ***Anti-Rootkit 设置***对话框中编辑 Anti-Rootkit 扫描配置（*可通过扫描选项对话框中的"扫描计算机是否存在 Rootkit 扫描的"设置"链接访问此对话框*）。***建议保留默认设置，若非必要，请勿更改！***

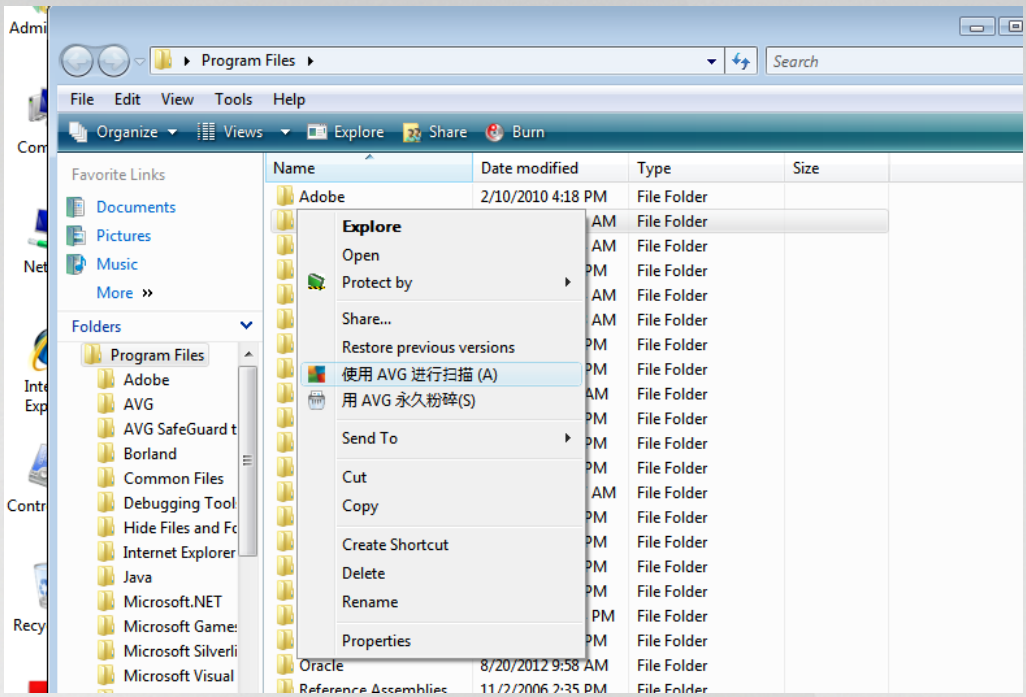


扫描应用程序和***扫描驱动程序***让您可以详细地指定 anti-rootkit 扫描应包含的内容。这些设置供高级用户使用；我们建议将所有选项都保持启用。还可以选择 Rootkit 扫描模式：

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

3.7.2. 扫描 Windows 资源管理器

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



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

3.7.3. 命令行扫描

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

若要从命令行启动 AVG 扫描，请在 AVG 的安装文件夹中运行以下命令：

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

3.7.3.1. 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:\ ***avgscanx /scan=C:\;D:***

3.7.3.2. 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，可使用 ***Ctrl+C*** 或 ***Ctrl+Pause*** 停止扫描过程。

3.7.3.3. 从图形界面启动的 CMD 扫描

在 Windows 安全模式下运行计算机时，还可以选择从图形用户界面中启动命令行扫描。



在安全模式中，自动从命令行运行扫描。此对话框只允许您在适当的图形界面中指定扫描参数。

首先选择您希望扫描的您的计算机区域。您可以决定选择预定义的 ***整个计算机扫描*** 或 ***扫描所选文件夹或文件*** 的选项。第三个选项，***快速扫描***，运行专为检查您的在安全模式中的计算机的指定扫描，检查您的计算机需要启动的所有关键区域。

下部分扫描设置可用于指定详细的扫描参数：默认全部选中，我们建议您一直这样做，仅在有特殊原因时，才取消选择某一参数。

- ***扫描 "可能不需要的程序 "***扫描间谍软件（区分于病毒）
- ***备用数据流 (仅用于 NTFS)***- 扫描 NTFS 备用数据流是一项 Windows 功能，被黑客攻击，可能会非法使用它来隐藏数据，特别是恶意代码。
- ***自动修复或删除感染*** - 所有可能的检测将从您的计算机中自动进行处理和修复 删除
- ***扫描活动的进程*** - 扫描被加载到计算机内存中的进程和应用程序
- ***扫描注册表*** –扫描 Windows 注册表
- ***启用 Master Boot Record 检查*** –扫描分区表和启动扇区

最后，在此对话框的底部，可指定扫描报告的文件名和类型。

3.7.3.4. CMD 扫描参数

以下是可用于命令行扫描的所有参数的列表：

- /? 显示有关此主题的帮助
- /@ 命令文件 文件名 /
- /ADS 扫描备用数据流 *（仅限 NTFS）*
- /ARC 扫描内部存档
- /ARCBOMBSW 报告重新压缩的存档文件
- /ARCBOMBSW 报告存档炸弹 *（反复压缩的存档）*
- /BOOT 启用 MBR/BOOT 检查
- /BOOTPATH 启用 QuickScan
- /CLEAN 自动清理
- /CLOUDCHECK 检查误报
- /COMP 扫描整个计算机
- /COO 扫描 cookie
- /EXCLUDE 将路径或文件排除在扫描范围之外
- /EXT 扫描这些扩展名 *(例如 EXT=EXE,DLL)*
- /FORCESHUTDOWN 扫描完成时强制关闭计算机
- /HELP 显示有关此主题的帮助
- /HEUR 使用启发式分析
- /HIDDEN 报告其扩展名已隐藏的文件
- /IGNLOCKED 忽略被锁定的文件
- /INFECTABLEONLY 仅扫描带可感染扩展名的文件
- /LOG 生成扫描结果文件
- /MACROW 报告宏 /
- /NOBREAK 不允许使用 Ctrl-Break 中止操作
- /NOEXT 不扫描这些扩展名 *(例如 NOEXT=JPG)*

- /PRIORITY 用于设置扫描优先级 (低、自动、高) (*请参见高级设置 扫描*)
- /PROC 扫描活动的进程
- /PUP 报告可能不需要的程序
- /PUPEXT 报告增强型可能不需要的程序的集合
- /PWDW 报告受密码保护的文件
- /QT 快速测试
- /REG 扫描注册表
- /REPAPPEND 附加到报告文件
- /REPOK 将未受感染的文件报告为"正常"
- /REPORT 将报告输出至文件 (*文件名*)
- /SCAN 扫描特定的文件或文件夹 (*/SCAN=路径 路径 (例如 /SCAN=C:\;D:\)*)
- /SHUTDOWN 扫描完成时关闭计算机
- /THOROUGHSCAN 启用彻底扫描
- /TRASH 将受感染的文件移至隔离区管理

3.7.4. 扫描计划

有了 **AVG Internet Security**，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。

可在通过扫描选项对话框中的 ***管理计划的扫描*** 按钮访问的 ***计划的扫描*** 对话库中创建/编辑扫描计划。在新 ***计划的扫描*** 对话框中，您可查看所有当前计划的扫描的完整概览：



在该对话框中，您可指定自己的扫描。使用***添加扫描计划***按钮创建您自己的新扫描计划。可在三个选项卡上编辑（）*计划扫描的参数或设置新计划*。

- 计划
- 设置
- 位置

在每个选项卡中，只需切换 "红绿灯"按钮 到，就可以直接暂时停用计划内测试，然后按需启用计划内测试：

3.7.4.1. 计划



在***计划***选项卡的顶部，您可找到一个文本字段，您可在其中指定当前正在定义的扫描计划

的名称。 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区分开来。 示例：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。

在此对话框中，可以进一步定义下列扫描参数：

- ***计划运行*** - 可在此指定新计划的扫描启动任务的时间间隔。 此时间间隔的定义方式有三种：指定经过一段特定的时间后重复启动扫描 *（运行时间间隔 ..）*，或通过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 *（计算机启动时运行）*。

- ***高级计划选项*** 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 系统托盘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（以彩色显示并带闪光），告诉您计划的扫描正在运行。 右键单击表示正在运行扫描的 AVG 图标，可打开一个上下文菜单。您可在此菜单中决定暂停甚至停止正在运行的扫描，还可以更改当前运行的扫描的优先级。

对话框中的控件

- ***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，然后返回到计划的扫描概览。 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。

- - 使用此对话框左上区域的绿色箭头返回到计划的扫描概览。

3.7.4.2. 设置



在 ***设置*** 选项卡的顶部，可找到一个文本字段，您可在其中指定当前正在定义的扫描计划的名称。 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区分开来。 示例：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

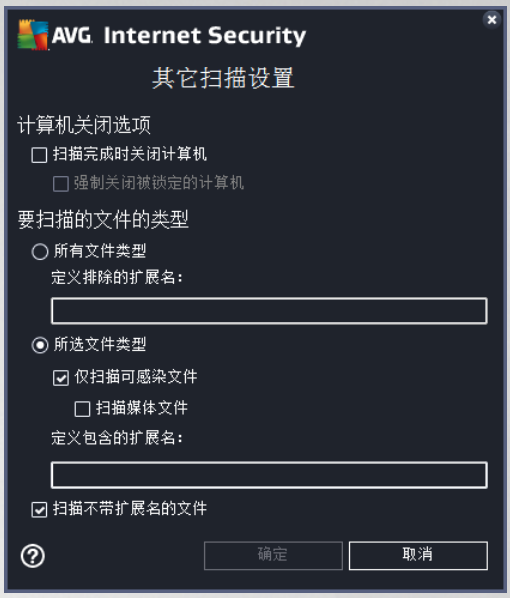
出扫描实际检查的内容。 相反， "系统区域扫描 "等名称就可以称得上是不错的描述性名称。

设置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。 ***除非有必要更改这些设置，否则我们建议保留预定义的配置***：

- ***无需询问即修复 删除病毒感染****（默认情况下已启用）：*如果在扫描过程中发现病毒，并且存在解决方案，则自动执行修复。 如果不能自动修复受感染文件，则会将受感染对象移到隔离区管理中。
- ***报告可能不需要的应用程序和间谍软件威胁****（默认情况下已启用）：*选中此框以激活对间谍软件和病毒的扫描。 间谍软件属于疑似恶意软件类软件：虽然它通常代表了安全风险，但有些程序也可能是被特意安装的。 建议保持此功能的激活状态，因为此功能会使计算机更加安全。
- ***报告可能不需要的应用程序的增强型集合****（默认情况下已禁用）：*选择此框可检测更多间谍软件：这类程序是指直接从制造商获得后极其安全而无害，但之后却可能被滥用以达到恶意目的的程序。 这项附加措施可以进一步提高计算机的安全性，但也可能会阻止合法程序，因此默认情况下已将其禁用。
- ***扫描跟踪 Cookie****（默认情况下已禁用）*：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*）。
- ***扫描内部存档****（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存档（如 ZIP 和 RAR 等文件）内也不例外。
- ***使用启发式分析****（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*）将成为在扫描期间的病毒检测方法之一。
- ***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。
- ***启用彻底扫描****（默认情况下已禁用）：*在特定情况下（*怀疑计算机受到感染*），您可以选中此选项以激活最全面的扫描算法，该算法甚至会对计算机上极难被感染的区域进行扫描以确保绝对安全。 不过要记住，此方法相当耗时。
- ***扫描 Rootkit****（默认情况下已启用）：*Anti-Rootkit 扫描用于在您的计算机中搜索是否可能存在 Rootkit（可以在您的计算机中掩盖恶意软件活动的程序和技术）。 如果检测到 Rootkit，并不一定意味着您的计算机已受到感染。 有些情况下，特定的驱动程序或正常应用程序的组成部分可能会被误检测为 Rootkit。

其它扫描设置

该链接将打开新的***其它扫描设置***对话框，您可在其中指定以下参数：



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

- ***要扫描的文件的类型*** - 应决定是否要进行扫描：

  - ***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受到感染的文件，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应始终扫描的文件。

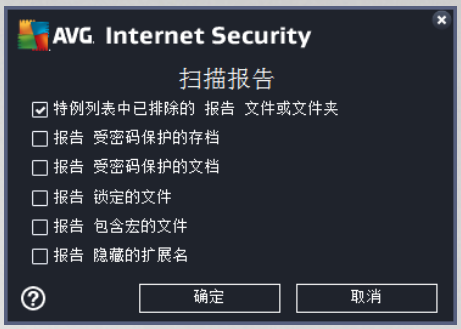
  - 您也可以选择指定要***扫描不带扩展名的文件*** - 默认情况下此选项已启用；我们建议，除非确有必要更改，否则将其保持启用。 不带扩展名的文件相当可疑，应随时对此类文件进行扫描。

调整扫描的完成速度

在此区域中，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*用户敏感性*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，在此窗口中可以通过勾选若干项来定义应报告哪些扫描结果：



对话框中的控件

- ***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，然后返回到计划的扫描概览。 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。

- - 使用此对话框左上区域的绿色箭头返回到计划的扫描概览。

3.7.4.3. 位置



在***位置***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此对话框顶部的文本字段中，下拉菜单将保留所选扫描日志以供日后使用。 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。 以下列出了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* C:\Documents and Settings\Default User\My Documents\
    - *对于 Windows Vista/7* : C:\Users\user\Documents\
- ***共享文档***
    - *对于 Win XP*: C:\Documents and Settings\All Users\Documents\
    - *对于 Windows Vista/7* : 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*)

对话框中的控件

- ***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，然后返回到计划的扫描概览。 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。
-  - 使用此对话框左上区域的绿色箭头返回到计划的扫描概览。

3.7.5. 扫描结果



扫描结果概览对话框提供了所有目前执行的扫描的结果的列表。 此图表提供有关每个扫描结果的以下信息：

- ***图标*** - 第一列将显示说明扫描状态的信息图标：
  - 未发现感染，扫描已完成
  - 未发现感染，扫描未完成即被中断
  - 发现感染但未予以修复，扫描已完成
  - 发现感染但未予以修复，扫描未完成即被中断
  - 发现感染且已修复或删除所有感染，扫描已完成
  - 发现感染且已修复或删除所有感染，扫描未完成即被中断
- ***名称*** - 此列提供相应扫描的名称。 它是两个 预定义扫描的其中一个, 或是您自己的计划的扫描。 。
- ***启动时间*** - 启动时间 -提供已启动的扫描的确切日期和时间。
- ***结束时间***结束时间 -提供已完成、已暂停或已中断的扫描的确切日期和时间。
- ***测试的对象数*** 测试的对象数 -提供所有已扫描对象的总数。
- ***感染数*** - 提供发现的已删除 总感染数。
- ***高 中 低*** - 随后的三列分别提供了发现的高、中、低严重性感染数。
- ***Rootkits*** - 提供扫描期间发现的 Rootkit 总数。

对话框控制项

查看详细信息 - 单击此按钮可查看有关所选扫描的详细信息 *（在图表上已突出显示）*。

删除结果 - 单击此按钮可从图表中删除所选的扫描结果信息。

- 使用此对话框左上区域的绿色箭头返回到包含组件 概述的主用户界面。

3.7.6. 扫描结果详细信息

要打开有关所选扫描结果的详细信息的概览，请单击扫描结果概览对话框中的***查看详细信息***按钮。 您将重新定向到用来详细描述有关相应扫描结果的同一对话框界面。 该信息分为三个选项卡：

- ***摘要*** - 此选项卡提供了关于扫描的基本信息：扫描是否已成功完成，是否已发现任何威胁以及对所发现对象的处理如何。
- ***详细信息*** - 此选项卡显示有关扫描的所有信息，包括有关任何检测到的威胁的详细信息。 将概览导出到文件让您将扫描结果保存为 csv 文件。
- ***检测*** - 如果在扫描期间检测到任何威胁，就会显示此选项，提供有关威胁的详细信息：

  信息严重性：并非真正威胁的信息或警告。 通常是包含受密码保护的宏、文档或存档的文档、锁定的文件等。

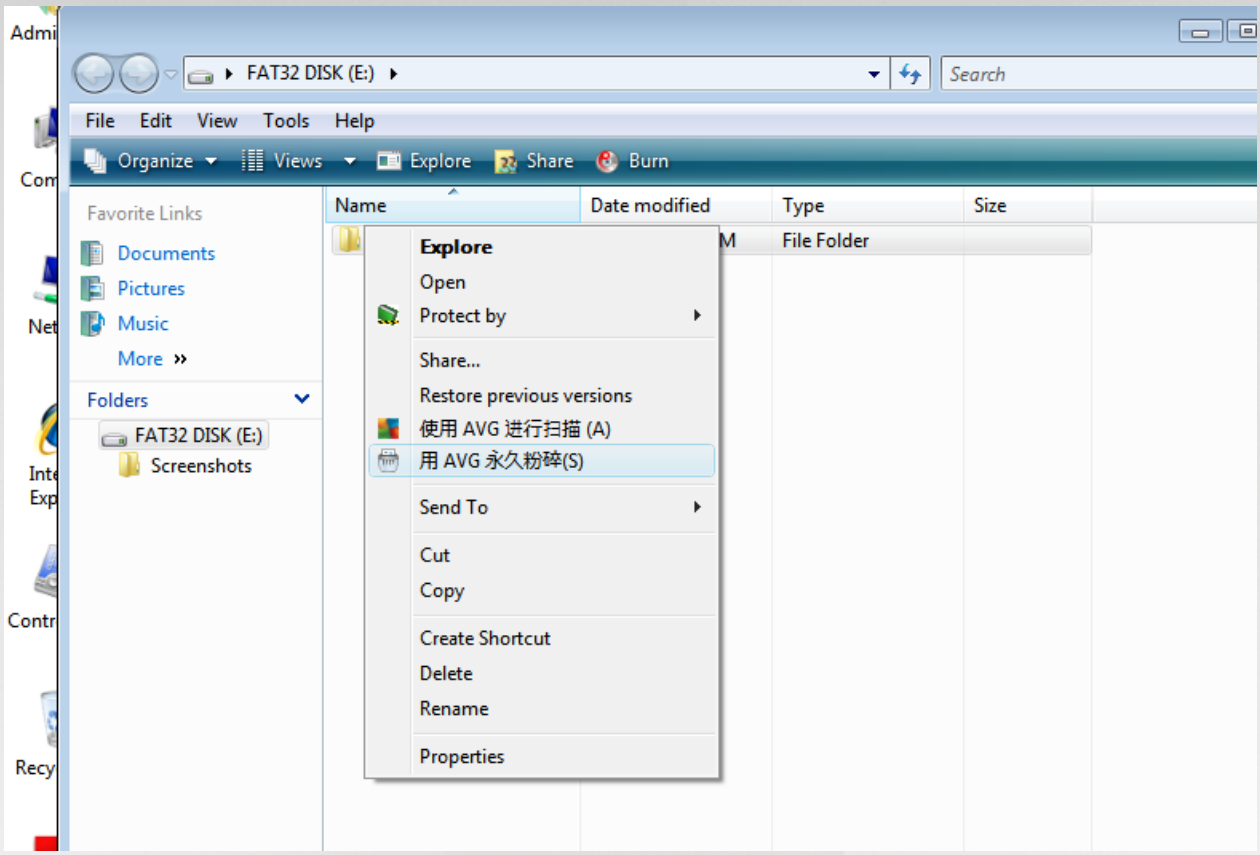
  中等严重性：通常是可能不需要的应用程序 *（例如广告软件）*或跟踪 Cookie

  高严重性：严重威胁，如病毒、特洛伊木马或漏洞利用等，还有通过启发式检测方法检测的对象，例如病毒库中未描述的威胁。

3.8. AVG File Shredder

AVG File Shredder 被设计为可绝对安全地删除文件，也就是说，即使使用高级软件工具，也完全不可能恢复它们。

要粉碎文件或文件夹，请在文件管理器 *（Windows 资源管理器，Total Commander 等等）*中使用右键单击它，然后从上下文菜单中选择***用 AVG 永久粉碎***。 也可粉碎回收站中的文件。 如果特定位置 *（例如，CD-ROM）*的特定文件无法可靠粉碎，则软件会提示您，或者上下文菜单中的相应选项将根本不可用。



请始终牢记：文件一旦被粉碎，就会永远消失。

3.9. 隔离区管理

隔离区管理是一种安全环境，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***隔离区管理***以待进一步处理。***隔离区管理***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，或将其放回原始位置。

隔离区管理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：

- ***添加日期*** - 提供检测到可疑文件并将其移至隔离区管理的日期和时间。
- ***威胁*** - 如果您确定在您的 **AVG Internet Security** 中安装 身份 组件，则将会在此部分中以图形方式提供各个发现的严重性：从无可非议 *三个绿色的点*（至非常危险 *（三个红色的点）*。您还可找到其感染类型及原位置的相关信息。*更多信息*链接会将您引导至一个页面，其中提供了在线病毒百科全书中检测到的所有威胁的详细信息。
- ***来源*** - 指定 **AVG Internet Security** 的哪一组件已检测到相应的威胁。
- ***通知*** - 在极少数情况下，在此列中可能出现某些注意事项，提供有关检测到威胁的详细注释。

控制按钮

可从***隔离区管理***界面中访问以下控制按钮：

- ***"还原"***-将受感染的文件移回其在磁盘上的原始位置
- ***还原为*** -用于将受感染的文件移至选定的文件夹。
- ***发送以进行分析*** -仅当您突出显示以上检测结果列表中的对象时，此按钮才会激活。 在这种情况下，您可选择将所选的检测结果发送至 AVG 病毒实验室以进行进一步的详细分析。 请注意，此功能仅主要用于发送误报，即被 AVG 检测为受感染或可疑，但您认为无害的文件。
- ***详细信息*** -有关 ***隔离区管理*** 中隔离的特定威胁的详细信息，请突出显示列表中的所选项并单击 ***详细信息*** 按钮，以便调用带有已检测的威胁的描述的新对话框。
- ***删除*** -将受感染的文件从 ***隔离区管理*** 中彻底移除（不可还原）。
- ***清空隔离区*** -彻底删除 ***隔离区管理*** 中的所有内容。 通过从***隔离区管理***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（*不是移到回收站*）。

3.10. 历史记录

历史记录部分包括有关所有过去事件（*例如更新、扫描、检测等*）的信息以及这些事件的报告。 可通过 ***选项 历史记录***项从主用户界面中访问此部分。 另外，所有已记录事件的历史记录分为以下部分：

- 扫描结果
- Resident Shield 结果
- 电子邮件保护结果
- Online Shield 结果
- 事件历史记录
- Firewall 日志

3.10.1. 扫描结果



扫描结果概述 对话框可通过**AVG Internet Security** 主窗口上条导航中的 ***选项/历史记录 扫描结果*** 菜单项访问。 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。

  注意： *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
- ***高 中*** - 这些列分别提供了已发现的高、中严重性的已删除 总感染数量。
- ***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）*
- ***Rootkit*** - 检测到的 rootkits 的数量

控制按钮

*'扫描结果概览'*对话框的控制按钮有：

- *'查看详细信息'*- 按此按钮可切换到扫描结果"对话框，以查看有关所选扫描操作的详细数据
- *'删除结果'*- 按此按钮可从扫描结果概览中删除所选扫描结果
- - 要切换回默认 AVG 主对话框 *（组件概述）*，请使用此对话框左上角的箭头

3.10.2. Resident Shield 结果

Resident Shield 服务是 ***计算机*** 组件的一部分，并可在复制、打开和保存文件时进行扫描。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，您可以查看有关已检测到并被认定为受感染对象的信息（*威胁*）和有关已识别感染的描述性事实（*描述*）。 *更多信息* 链接会将您引导至一个页面，其中提供了在线病毒百科全书中检测到的所有威胁的相关信息（如果已知）。在此对话框中，您也将看到有关如何处理检测到威胁的可用解决方法的概述。备选方案之一将被标记为推荐：***保护我（推荐）。如果可能，应始终勾选此选项！***

注意： *注：检测到的对象可能会大于隔离区管理中的可用空间限制。如果情况如此，则会在尝试将感染的对象移到隔离区管理时弹出警告消息，就所发生的问题发出通知。但隔离区大小是可以修改的。隔离区大小已被指定为硬盘实际大小的可调比例。要加扩大隔离区，请通过 AVG 高级设置 中的 "限制隔离区大小"选项，转到隔离区管理 对话框。*

在此对话框的底部区域，您可找到***显示详细信息***链接。单击此链接可打开一个新窗口，其中包含关于检测到感染时正在运行进程的详细信息，以及该进程的 识别号。

所有 Resident Shield 检测的列表在 ***Resident Shield 检测***对话框中提供概述。通过**AVG Internet Security** 主窗口上条导航中的***选项 / 历史记录 /Resident Shield 检测***菜单项可访问此对话框。此对话框提供了经 Resident Shield 检测而被评估为有危险并且已被修复或移至 隔离区管理的对象概述。



对于检测到的每个对象，提供了以下信息：

- ***威胁名称*** - 检测到的对象的描述（*甚至可能就是其名称*）及其位置。*更多信息*链接会将您引导至一个页面，其中提供了在线病毒百科全书中检测到的所有威胁的详细信息。
- ***状态*** - 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

控制按钮

- ***刷新*** - 用于更新 ***Online Shield 检测的结果列表***
- ***导出*** - 用于导出文件中的已检测对象的整个列表
- ***删除所选内容*** - 您可在列表中突出显示所选记录，并使用此按钮只删除这些所选项
- ***删除所有威胁*** - 使用此按钮删除此对话框中列出的所有记录
- ← - 要切换回默认 AVG 主对话框 *（组件概述）*，请使用此对话框左上角的箭头

3.10.3. Identity Protection 结果

Identity Protection 结果 对话框可通过主窗口 **AVG Internet Security** 上方导航中的***选项 /历史记录 /Identity Protection 结果***菜单项可访问此对话框。



此对话框提供了Identity Protection 组件检测到的所有结果的列表。 对于检测到的每个对象，提供了以下信息：

- ***威胁名称*** - 检测到的对象的描述 *（甚至可能就是其名称）*及其位置。 *更多信息*链接会将您引导至一个页面，其中提供了在线病毒百科全书中检测到的所有威胁的详细信息。
- ***状态*** - 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。 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***），以及删除感染检测到对象的所有条目（***清空列表***）。

控制按钮

Identity Protection 结果界面中提供有下列控制按钮：

- ***"刷新列表"*** - 更新检测到的威胁列表
- - 要切换回默认 AVG 主对话框 *（组件概述）*，请使用此对话框左上角的箭头

3.10.4. 电子邮件保护结果

电子邮件保护结果 对话框可通过主窗口 **AVG Internet Security** 上方导航中的***选项/历史记录 电子邮件保护结果***菜单项可访问此对话框。



此对话框提供了 Email Scanner 组件检测到的所有结果的列表。 对于检测到的每个对象，提供了以下信息：

- ***检测名称*** - 说明 *（可能是名称）*检测到的对象及其来源
- ***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
- ***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。 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***），以及删除感染检测到对象的所有条目（***清空列表***）。

控制按钮

Email 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
- - 要切换回默认 AVG 主对话框 *（组件概述）*，请使用此对话框左上角的箭头

3.10.5. Online Shield 结果

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



在此警告对话框中，您可以查看有关已检测到并被认定为受感染对象的信息（*威胁*）和有关已识别感染的描述性事实（*对象名称*）。 *更多信息*链接会将您重新定向到在线病毒百科全书，您可以在其中找到关于检测到感染的详细信息（如果已知）。 此对话框提供了以下控制元素：

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

可疑网页将不会打开，检测到的威胁将会记录到 ***Online Shield 检测结果*** 列表。 通过 **AVG Internet Security** 主窗口上条导航中的 ***选项 /历史记录 /Online Shield 检测结果*** 菜单项可访问此检测到的威胁的概述。



对于检测到的每个对象，提供了以下信息：

- ***威胁名称*** - 检测到的对象的描述（*可能甚至包括名称*）以及其来源（*网页*）；*更多信息*链接会将您引导至一个页面，其中提供了线病毒百科全书在中检测到的所有威胁的相关信息。
- ***状态*** - 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

控制按钮

- ***刷新*** - 用于更新 ***Online Shield 检测的结果列表***
- ***导出*** - 用于导出文件中的已检测对象的整个列表
- - 要切换回默认 AVG 主对话框 *（组件概述）*，请使用此对话框左上角的箭头

3.10.6. 事件历史记录



事件历史记录 对话框可通过主窗口 **AVG Internet Security** 上方导航中的***选项 /历史记录 事件历史记录*** 菜单项进行访问。 此对话框中显示了在 **AVG Internet Security** 运行期间发生的重要事件的摘要。 此对话框提供以下事件类型的记录：有关 AVG 应用程序更新的信息；有关扫描启动、结束或停止的信息（*包括自动执行测试*）；有关与病毒检测有关事件的信息（*通过 Resident Shield 或扫描*）并包括发生位置以及其他重要事件。

对于每个事件，将列出以下信息：

- ***事件日期和时间*** 用于说明事件发生的确切日期和时间。
- ***用户*** 用于说明目前已于发生事件时登录到系统中的用户的名称。
- ***来源*** 用于提供有关触发事件的源组件或 AVG 系统的其它部分的信息。
- ***事件说明***，用于提供实际情况的简短摘要。

控制按钮

- ***刷新列表*** - 按该按钮可刷新事件列表中的所有条目
- ***关闭*** - 按此按钮可返回到 **AVG Internet Security**主窗口

3.10.7. Firewall 日志

此对话框用于专家配置，我们建议不要更改任何设置，除非您完全清楚所作的更改！

在***日志***对话框中，您可以查看所有已记录的 Firewall 操作和事件的列表，以及显示在两个选项卡中相关参数的详细说明：

- ***流量日志*** - 此选项卡提供了尝试连接到网络的所有应用程序的活动相关信息。对于每个项目，您将找到有关事件时间、应用程序名称、对应的记录操作、用户名、PID、流量方向、协议类型、远程及本地端口号的信息，以及有关本地和远程 IP 地址的信息。



- ***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

- ***"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。
- ***删除日志*** - 按此按钮可删除图表中的所有条目。

3.11. AVG 更新

除非得到定期更新，否则任何一款安全软件都不能保证真的可以防止受到各类威胁的侵害！病毒编写者一直在寻找软件和操作系统中可以利用的新漏洞。每天都会出现新的病毒、新的恶意软件、新的黑客攻击。因此，软件供应商都在不断地发布更新和安全补丁，以修复被发现的任何安全漏洞。考虑到所有新涌现出来的计算机威胁，以及这些威胁的蔓延速度，定期更新 **AVG Internet Security** 至关重要。继续使用程序默认设置（已在其中配置好自动更新），这是最佳解决方法。请注意，如果 **AVG Internet Security** 的病毒数据库不是最新数据库，则程序不能检测到最新威胁！

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

为了尽可能提高安全性，**AVG Internet Security** 的默认更新计划是每四小时查找一次新病毒数据库更新。由于 AVG 更新并非依据任何固定的计划进行发布，而是要视新威胁的数量和严重程度而定，因此这种检查对于确保 AVG 病毒数据库始终处于最新状态很重要。

如果想要立即检查新更新文件，请使用主用户界面中的立即更新 快速链接。任何用户界面对话框中都始终有此链接。启动更新后，AVG 首先会核实是否有新的更新文件可用。如果有，**AVG Internet Security** 会开始下载这些文件，然后自行启动更新过程。系统将在 AVG 系统托盘图标上的滚动对话框显示更新结果的信息。

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

- 指定更新计划
- Anti-Spam 更新计划

3.12. 常见问题解答和技术支持

如果有关于 **AVG Internet Security** 应用程序方面的销售或技术问题，可用多种方法获取帮助。请从以下备选方法中进行选择：

- ***获取支持***：在 AVG 应用程序中就可以直接到达 AVG 网站的专用客户支持网页（*http://www.avg.com/*）。请选择 ***帮助 获取支持*** 主菜单项，通过可用支持途径重定向至 AVG 网站。要继续操作，请按该网页中的说明操作。
- ***支持***（*主菜单链接*）：AVG 应用程序菜单（*位于主用户界面顶部*）中有 ***支持*** 链接，

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

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

- ***AVG 网站支持中心***：也可在 AVG 网站 （*http://www.avg.com/*） 中查找所遇到的问题的解决方法。在***支持***部分，您可找到主题群组（用于处理销售和技术问题）的概述，还可发现一个结构化的常见问题解答部分及所有可用联系方式。

- ***AVG ThreatLabs***：特定的 AVG 相关网站 （*http://www.avgthreatlabs.com/website-safety-reports/*），是有关病毒问题的专业站点，提供有关在线威胁相关的结构化概览。其中也有关于删除病毒、间谍软件的说明，还有针对如何一直得到保护提出的建议。

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