Avira Antivirus Premium

用户手册

AVIRA

商标与版权

商标

Windows 是 Microsoft Corporation 在美国和其他国家/地区的注册商标。
所有其他品牌和产品名称均为其各自所有者的商标或注册商标。
在本手册中并未对受保护的商标特别进行标记。 但这并不意味着它们可以自由使用。

版权信息

第三方供应商提供的代码用于Avira Antivirus Premium。 对于将该代码提供给我们的版权所有者，我们表示衷心的感谢。
有关版权的详细信息，请参考 Avira Antivirus Premium 程序帮助中的第三方许可证 。

目录表

1. 简介 8

1.1 图标和强调字体 8

2. 产品信息 10

2.1 交付范围 10

2.2 系统要求 12

2.3 授权和升级 13

2.3.1 授权 13

2.3.2 延长许可证的有效期 14

2.3.3 正在升级 14

2.3.4 许可证管理器 15

3. 安装和卸载 17

3.1 安装类型 17

3.2 预安装 18

3.3 快速安装 19

3.4 自定义安装 22

3.5 测试产品安装 26

3.6 配置向导 28

3.7 更改安装 30

3.8 安装模块 30

3.9 卸载 31

4. Avira Antivirus Premium 概述 33

4.1 用户界面和操作 33

4.1.1 控制中心 33

4.1.2 游戏模式 37

4.1.3 任务栏图标 37

4.2 Avira SearchFree Toolbar 39

4.2.1 使用方法 39

4.2.2 选项 43

4.2.3 卸载 48

4.3 操作方法 49

4.3.1 激活许可证 50

4.3.2 激活产品 51

4.3.3 执行自动更新 52

4.3.4 启动手动更新 54

4.3.5 使用扫描配置文件扫描病毒和恶意软件 55

4.3.6 使用拖放操作扫描病毒和恶意软件 57

4.3.7 通过上下文菜单扫描病毒和恶意软件 57

4.3.8 自动扫描病毒和恶意软件 58

4.3.9 针对 Rootkit 和活动恶意软件的扫描 60
4.3.10 对检测到的病毒和恶意软件做出反应 60
4.3.11 处理已隔离的文件 (*.qua) 66
4.3.12 还原隔离区中的文件 68
4.3.13 将可疑文件移到隔离区 70
4.3.14 修改或删除扫描配置文件中的文件类型 70
4.3.15 创建扫描配置文件的桌面快捷方式 71
4.3.16 过滤事件 72
4.3.17 将电子邮件地址排除在扫描范围之外 73

5. Scanner 74

6. 更新 75

7. 常见问题解答、技巧 77

7.1 相关问题帮助 77

7.2 快捷键 82
7.2.1 在对话框中 82
7.2.2 在帮助中 83
7.2.3 在控制中心中 84

7.3 Windows 安全中心 87
7.3.1 常规 87
7.3.2 Windows 安全中心和 Avira 产品 87

7.4 Windows 操作中心 90
7.4.1 常规 90
7.4.2 Windows 操作中心和 Avira 产品 91

8. 病毒及其他 97
8.1 威胁类别 97
8.2 病毒及其他恶意软件 102
9. 信息与服务 107
9.1 联系地址 107
9.2 技术支持 107
9.3 可疑文件 108
9.4 误报 108
9.5 提供反馈以提高安全性 108
10. 参考：配置选项 110
10.1 Scanner 110
10.1.1 扫描 110
10.1.2 报告 121
10.2 Real-Time Protection 122
10.2.1 扫描 122
10.2.2 报告 135
10.3 更新 137
10.3.1 Web 服务器 137
10.4 Web Protection 140
10.4.1 扫描 140
10.4.2 报告 149
10.5 Mail Protection 150
10.5.1 扫描 150
10.5.2 常规 156
10.5.3 报告 157

10.6 儿童保护 159

10.7 手机保护 159

10.7.1 手机保护 159

10.8 常规 159

10.8.1 威胁类别 159

10.8.2 高级保护 160

10.8.3 密码 164

10.8.4 安全 166

10.8.5 WMI 168

10.8.6 事件 169

10.8.7 报告 169

10.8.8 目录 170

10.8.9 有声警报 171

10.8.10 警报 172

1. 简介

Avira 产品可针对病毒、蠕虫、木马、广告软件和间谍软件及其他危险为计算机提供保护。在本手册中将这些称为病毒、恶意软件（有害软件）和恶意程序。

本手册介绍程序的安装和操作。

如需了解更多选项和信息，请访问网站：
http://www.avira.cn

通过 Avira 网站，您可以：

- 访问有关其他 Avira 桌面程序的信息
- 下载最新的 Avira 桌面程序
- 下载最新的 PDF 格式产品手册
- 下载免费支持和修复工具
- 访问包罗万象的知识数据库和常见问题解答以排除故障
- 访问针对具体国家/地区的支持地址。

您的 Avira 团队

1.1 图标和强调字体

使用了以下图标：

图标/名称	说明
✓	放在执行一个操作所必须满足的条件之前。
▸	放在执行的操作步骤之前。

↪	放在上一操作之后的事件之前。
警告	当重要数据可能丢失时放在警告之前。
说明	放在指向特别重要信息的连接或者让avira产品更简单易用的提示技巧之前。

使用了以下强调字体：

强调字体	说明
斜体	文件名或路径数据。
	显示的软件界面元素（例如窗口区域或错误消息）。
粗体	可点击软件界面元素（例如菜单项、导航区域、单选框或单选按钮）。

2. 产品信息

本章包含有关购买和使用 Avira 产品的所有信息：

- 请参阅章节：交付范围
- 请参阅章节：系统要求
- 请参阅章节：授权和升级
- 请参阅章节许可证管理器

Avira 产品是一个全面而灵活的工具，可针对病毒、恶意软件、恶意程序以及其他威胁为您的计算机提供保护。

▸ 请注意以下信息：

警告

丢失重要数据通常会带来严重的后果。
再好的病毒防护程序也不能完全保证数据不会丢失。
出于安全考虑，请定期备份您的数据。

说明

只有最新的程序才能针对病毒、恶意软件、恶意程序以及其他威胁提供可靠和有效的保护。 通过自动更新可以确保 Avira 产品是最新的。
请对程序进行相应配置。

2.1 交付范围

您的 Avira 产品具有以下功能：

- 控制中心：用于监视、管理和控制整个程序；
- 中心配置：具有用户友好的标准选项和高级选项以及上下文相关帮助；

- Scanner（按需扫描）：具有使用配置文件控制的扫描和可配置的扫描，用于查找所有已知类型的病毒和恶意软件；
- 集成到 Windows Vista 用户帐户控制中，便于执行需要管理员权限的任务；
- Real-Time Protection（访问时扫描）：用于持续监视所有文件访问尝试；
- ProActiv 组件：用于永久监视程序操作（仅适用于 32 位系统）
- Mail Protection（POP3 Scanner、IMAP Scanner 和 SMTP Scanner）：用于永久检查电子邮件中是否存在病毒和恶意软件，包括检查电子邮件附件；
- Avira SearchFree Toolbar，一种集成于 Web 浏览器中的搜索工具栏，可提供便捷的搜索选项。 它还包含具有最常用 Internet 功能的小组件；
- Web Protection用于监视使用 HTTP 协议从 Internet 传输的数据和文件（监视端口为 80、8080、3128）；
- Avira Free Android Security 应用程序不仅提供防盗措施。 如果您将移动设备放错地方或者更糟的是移动设备被窃，该应用程序可以帮助您找回设备。 Avira Free Android Security 可以保护运行 Android 操作系统的蜂窝电话和智能手机。
- 集成隔离区管理：用于隔离和处理可疑文件；
- Rootkits Protection：用于检测在您的计算机系统中安装的隐藏的恶意软件 (Rootkit)（在 Windows XP 64 位）；
- 通过 Internet 直接访问关于检测到的病毒和恶意软件的详细信息；
- 采用单文件更新和增量 VDF 更新，可以方便快速地通过 Web 服务器从 Internet 更新程序、病毒定义和搜索引擎；
- 许可证管理器提供了用户友好的授权功能；
- 集成了计划程序，它可以用于规划一次性或重复的作业，例如更新或扫描；
- 通过启发式扫描方法等创新扫描技术（扫描引擎），达到极高的病毒和恶意软件侦测率；

- 对所有常规存档类型进行检测，包括嵌套存档检测和智能扩展检测；
- 提供高性能的多线程功能（同时高速扫描多个文件）；

2.2 系统要求

系统要求如下：

- 计算机最低配置为 1 GHz 奔腾处理器
- 操作系统
  - Windows XP，最新 SP（32 或 64 位）或者
  - Windows 7，最新 SP（32 或 64 位）或者
  - Windows 8，最新 SP（32 或 64 位）
- 至少 150 MB 可用硬盘存储空间（如果使用隔离区作为临时存储区，还需要更多空间）
- Windows XP 下至少需要 512 MB RAM
- Windows 7
- 对于程序安装：管理员权限
- 对于所有安装：Windows Internet Explorer 6.0 或更高版本
- 某些情况下，还需要有 Internet 连接（请参阅安装）

Avira SearchFree Toolbar

- 操作系统
  - Windows XP，最新 SP（32 或 64 位）或者
  - Windows 7，最新 SP（32 或 64 位）或者
  - Windows 8，最新 SP（32 或 64 位）
- Web 浏览器
  - Windows Internet Explorer 6.0 或更高版本
  - Mozilla Firefox 3.0 或更高版本
  - Google Chrome 18.0 或更高版本

说明

必要时请在安装 Avira SearchFree Toolbar 前卸载任何以前安装的搜索工具栏。 否则将无法安装 Avira SearchFree Toolbar。

Windows Vista 用户需了解的信息

在 Windows XP 上，很多用户都工作在管理员权限下。
但是，从安全角度来看，这样做并不合适，因为这样一来，病毒和恶意程序很容易侵入计算机。

因此，Microsoft 在 Windows Vista 中引入了“用户帐户控制”。
此功能能够为以管理员身份登录的用户提供更多保护：因此在 Windows Vista 中，管理员最初只有正常用户的权限。 在 Windows Vista 中，需要管理员权限才能执行的操作用信息图标进行了清楚地标记。
此外，用户必须明确确认所需操作。
然后只有在获得此权限后，用户权限才会提升，操作系统才会执行管理任务。

在 Windows Vista 中，Avira 产品需要管理员权限才能执行某些操作。
这些操作用以下符号标记：。
如果此符号也显示在按钮上，则需要管理员权限才能执行此操作。
如果当前用户帐户没有管理员权限，则 Windows Vista 的“用户帐户控制”对话框会要求您输入管理员密码。
如果没有管理员密码，则无法执行此操作。

2.3 授权和升级

2.3.1 授权

要使用 Avira 产品，您需要有一个许可证。 因此请接受许可条款。

该许可证以激活码的形式提供。 激活码是一个由字母和数字组成的代码，您将在购买 Avira 产品后收到激活码。 激活码包含许可证的准确数据，即许可使用的程序及其有效期。

如果您在 Internet 上购买了 Avira 产品，则会将激活码以电子邮件形式发送给您，或者在产品包装上将会提供此码。

要获得程序授权，请输入您的激活码以激活程序。 可以在安装过程中激活产品。不过，也可以在完成安装后，在**帮助 > 许可证管理**下运行许可证管理器以激活 Avira 产品。

2.3.2 延长许可证的有效期

当您的许可证即将到期，Avira 将发送一个上滑菜单来提醒您延长许可证的有效期。为此，您只需单击链接，随后将转至 Avira 在线商店。 不过，也可以在**帮助 > 许可证管理**下运行许可证管理器以延长您 Avira 产品许可证的有效期

如果您已经在 Avira 的许可证门户中注册，可以直接在网上通过**许可证概述**额外延长许可证的有效期，或选择许可证自动续期。

2.3.3 正在升级

在许可证管理器中，您可以对 Avira 桌面产品系列的产品进行升级。您无需手动卸载旧产品，然后再手动安装新产品。从许可证管理器中升级时，只需在“许可证管理器”输入框中输入待升级产品的激活码即可。 新产品将会自动安装。

为了使计算机拥有出色的可靠性和安全性，Avira 会发送弹出项，提醒您将您的系统升级至最新版本。仅需单击弹出项上的升级链接即可转到您的产品的指定升级网站。

您可以升级当前产品，或者获得更全面的产品。产品概述页面显示了您正在使用的产品是什么种类的，并使您能够将您的产品与其他 Avira 产品进行比较。 如果您需要更多信息，请单击产品名称旁的**信息**图标。

如果您想使用当前产品，请单击升级，立即开始下载最新版本。
如果您想获得更全面的产品，请单击产品列底部的购买按钮。 您将自动转至 Avira 在线商店，您可以在这里下订单。

> 说明
> 您可能需要管理员权限方可执行升级，具体取决于您的产品和操作系统。
> 执行升级前以管理员身份登录。

2.3.4 许可证管理器

使用 Avira Antivirus Premium 许可证管理器可以方便地安装 Avira Antivirus Premium 许可证。

Avira Antivirus Premium 许可证管理器

可以通过在文件管理器或激活电子邮件中双击许可证文件以选择该文件，然后按照屏幕上的相关说明安装许可证。

说明

Avira Antivirus Premium

许可证管理器将自动复制相关产品文件夹中相应的许可证。

如果已存在许可证，则会显示一条信息，询问是否替换现有许可证文件。

在这种情况下，现有许可证文件将被新许可证文件覆盖。

3. 安装和卸载

本章包含有关安装和卸载 Avira 产品的信息。

- 请参阅章节：预安装：要求、使计算机做好安装准备
- 请参阅章节：快速安装：根据默认设置进行标准安装
- 请参阅章节：自定义安装：可配置的安装
- 请参阅章节：测试产品安装
- 请参阅章节：配置向导
- 请参阅章节：更改安装
- 请参阅章节：安装模块
- 请参阅章节：卸载：卸载

3.1 安装类型

在安装过程中，可在安装向导中选择安装类型：

快速

- 程序文件将安装到 *C:¥Program Files* 下的默认文件夹中。
- 将采用默认设置安装 Avira 产品。 您可以使用配置向导定义自定义设置。

自定义

- 可选择安装各个程序组件（请参阅章节：安装和卸载 > 安装模块）。
- 可以为要安装的程序文件选择目标文件夹。
- 可禁止创建桌面图标和在开始菜单中创建程序组。
- 使用配置向导，您可以定义 Avira 产品的自定义设置，并在安装完成后启动自动执行的快速系统扫描。

3.2 预安装

说明

安装前，请检查您的计算机是否满足所有最低系统要求。

如果计算机满足所有要求，则可安装 Avira 产品。

预安装

✓ 关闭电子邮件程序。 此外，建议结束正在运行的所有应用程序。

✓ 确保未安装其他病毒防护解决方案。

各安全解决方案的自动保护功能可能会相互影响。

↳ Avira 产品会在计算机上搜索任何可能的不兼容软件。

↳ 如果检测到可能不兼容的软件，Avira 将生成这些程序的列表。

↳ 建议删除这些软件程序以免影响计算机的稳定性。

▸ 从列表中选择应从计算机中自动删除的所有程序对应的复选框，然后单击下一步。

▸ 必须手动确认卸载这些程序。 选择程序并单击下一步。

↳ 卸载一个或多个所选程序需要重新启动计算机。 重新启动后将继续安装。

警告

直到 Avira 产品安装结束，您的计算机才会受到保护。

安装

安装程序运行时，对话框中提供了非常清楚的说明。

每个窗口都包含一组按钮供您选择，以便控制安装过程。

几个最重要按钮的功能如下：

- **确定**：确认操作。
- **中止**：中止操作。

- 下一步：转到下一步。
- 上一步：转到上一步。

  - 建立 Internet 连接：要执行以下安装步骤，您必须具有 Internet 连接：
    - 通过安装程序下载最新的程序文件、扫描引擎以及最新的病毒定义文件（基于 Internet 的安装）
    - 激活程序
    - 如果需要，请在安装完成后执行更新
  - 如果您要激活程序，请准备好 Avira 产品的激活码或许可证文件。

> 说明
>
> **基于 Internet 的安装：**
> Avira Web 服务器提供了一个安装程序，用于进行基于 Internet 的程序安装，在执行这种安装之前，该程序将加载最新程序文件。此过程可确保使用最新的病毒定义文件安装 Avira 产品。
>
> **用安装软件包安装:**
> 安装软件包中含有安装程序和所有必要的程序文件。 使用安装软件包安装 Avira 产品时，未提供语言选择。 建议在安装之后更新病毒定义文件。

> 说明
>
> Avira 产品使用 HTTP 协议和端口 80（Web 通信）以及加密协议 SSL 和端口 443 与 Avira 的服务器通信，以激活产品。
> 如果您使用了防火墙，请确保防火墙不会阻止所需连接和/或传入或外发数据。

3.3 快速安装

安装您的 Avira 產品：

按兩下剛從網際網路下載的安裝檔案，或是插入程式光碟，以啟動安裝程式。

網際網路型態的安裝

↳ **歡迎**畫面出現。

- 按 **[下一步]** 繼續安裝。

  ↳ **[語言選擇]** 對話方塊隨即顯示。

- 選取您要用來安裝 Avira 產品的語言，並按 **[下一步]** 確認語言選擇。

  ↳ **[下載]** 對話方塊隨即顯示。 Avira 網路伺服器會開始下載所有必要的安裝檔案。
  [下載] 視窗會在下載結束時關閉。

使用安裝套件來安裝

↳ **[準備安裝]** 視窗隨即顯示。

↳ 這時會開始解壓縮安裝檔案。 安裝常式正式開始。

↳ **[選取安裝類型]** 對話方塊隨即顯示。

> 注意
> 快速安裝為預設值。 所有標準元件都將安裝，您無需自行設定。
> 若您想要執行自訂安裝，請參閱下列章節：安裝與解除安裝 > 自訂安裝。

- **[我要使用 Avira ProActiv 與 Protection Cloud 提升我的防護]**
  核取方塊已預先勾選 (組態 > 一般 > 進階防護)。 如果您不想加入 Avira 社群，請取消勾選此核取方塊。

  ↳ 如果您確認要加入 Avira 社群，Avira 會將偵測到的可疑程式資料傳送至 Avira 惡意程式碼研究中心。 此資料只會用於進階線上掃描和延伸及精簡偵測技術。
  您可以按一下 **ProActiv 與 Protection Cloud**
  連結了解更多有關延伸線上與雲端掃描的詳細資訊。

- 確認您已接受**使用者授權合約**。 如需了解**使用者授權合約**的詳細文字說明，請按一下 **EULA** 連結。

↳ **授權精靈**隨即開啟，而且會協助您啟用您的產品。

↳ 您可以在此設定 Proxy 伺服器。

- 必要時，按一下組態中的 **[Proxy 設定]**，並按 **[確定]** 確認設定。
- 如果您已經收到啟用代碼，請選取 **[啟用產品]** 並輸入啟用代碼。

  -或-

- 如果您沒有啟用代碼，請按一下**購買啟用代碼**連結。

  ↳ 您會移至 Avira 網站。

  或者，按一下**我已經有有效的授權檔案**連結。

  ↳ **[開啟檔案]** 對話方塊隨即顯示。

- 選取 *.KEY* 授權檔案，然後按一下 **[開啟]**。

  ↳ 啟用代碼會複製到授權精靈。

- 如果您想要測試產品，請繼續閱讀章節：測試產品安裝。
- 按 **[下一步]**。

  ↳ 安裝進度會顯示為綠色列。

- 按 **[下一步]**。

  ↳ **[成為百萬名 Avira SearchFree 使用者之一]** 對話方塊隨即出現。

- 如果您不想要安裝 Avira SearchFree Toolbar，請取消勾選 Avira SearchFree Toolbar 和 Avira SearchFree Updater **使用者授權合約**，而定義 **Avira SearchFree (search.avira.com)** 的項目就會成為您的瀏覽器首頁。

> 注意
> 必要時，在安裝 Avira SearchFree Toolbar 之前請先解除安裝以前安裝的搜尋工具列。 否則您將無法安裝 Avira SearchFree Toolbar。

- 按 **[下一步]**。

- ↳ Avira SearchFree Toolbar 的安装進度會顯示為綠色列。
- ↳ Avira 系統匣圖示位於工作列中。
- ↳ 如要確定有效的電腦防護，**更新程式**模組將搜尋可能的更新。
- ↳ **[Luke Filewalker]** 視窗隨即開啟並執行快速系統掃描。
  會顯示掃描的狀態與結果。

- 如果在掃描後要求您重新啟動電腦，請按一下 **[是]** 確定您的系統已受到完整保護。

安装成功之後，建議您檢查程式是否為最新狀態 (位於**控制中心**的*狀態*欄位中)。

- 如果您的 Avira 產品顯示您的電腦未受保護，請按一下 **[修正問題]**。
  - ↳ **[還原防護]** 對話方塊開啟。
- 啟動預設選項以最大化您系統的安全性。
- 必要時，請在之後執行完整的系統掃描。

3.4 自定义安装

安装 Avira 产品：

双击从 Internet 下载的安装文件或插入程序 CD，启动安装程序。

基于 Internet 的安装

- ↳ 显示欢迎屏幕。

- 单击**下一步**继续安装
  - ↳ 此时将显示语言选择对话框。
- 选择要用于安装 Avira 产品的语言并单击**下一步**确认语言选择
  - ↳ 此时将显示下载对话框。 安装需要的所有文件将通过 Avira Web 服务器下载。
  下载结束后，下载窗口将关闭。

使用安装软件包安装

↳ 显示准备安装窗口

↳ 此时将解压安装文件， 安装例程启动

↳ 此时将显示选择安装类型对话框。

> 说明
> 默认设置为快速安装。 将安装所有标准组件，您无法配置这些组件。
> 如果您要执行快速安装，请参阅章节：安装和卸载 > 快速安装。

- 选择自定义以安装单独的程序组件。
- 默认设置为我希望通过使用 Avira Proactiv 和 Protection Cloud 来增强保护效果对话框。 如果您不想参加 Avira 社区，请取消选中此复选框。
  - ↳ 如果您确认参加 Avira 社区，Avira 会在检测到可疑程序时向 Avira 恶意软件研究中心发送数据。
    此数据仅用于高级联机扫描以及扩展和完善监测技术。 可以单击链接 ProActiv 和 Protection Cloud 以获得有关扩展的联机和云扫描的更多详细信息。
- 确认接受最终用户许可协议。 若要阅读最终用户许可协议的文本，请单击 EULA 链接。
- 单击下一步。
  - ↳ 选择目标文件夹窗口打开。
  - ↳ 默认文件夹为 *C:¥Program Files¥Avira¥AntiVir Desktop¥*
- 单击下一步以继续。

  - 或者 -

  使用浏览按钮选择其他目标文件夹，并单击下一步进行确认。
  - ↳ 此时将显示安装组件对话框。
- 选择或取消选择列表中的组件并单击下一步进行确认，以便继续进行。

- 如果您选择安装 **Protection Cloud** 组件，但希望手动确认将哪些文件发送到 Cloud 进行分析，您可以启用**发送可疑文件至 Avira** 时手动确认选项。
- 单击**下一步**。
- 在下一个对话框中，可确定是否创建桌面快捷方式和/或是否在开始菜单中创建程序组。
- 单击**下一步**。
  - ↪ **许可向导**打开。

可以通过以下选项激活程序：

- 输入激活码。
  - ↪ 输入激活码，使用许可证激活 Avira 产品。
- 如果您没有激活码，请单击链接**购买激活码**。
  - ↪ 随即转到 Avira 网站。
- 选择**测试产品**选项
  - ↪ 如果选择**测试产品**，则在激活过程中将生成评估许可证，可用该许可证激活程序。您可以在一段时间段内测试 Avira 产品的所有功能（请参阅测试产品安装）。

说明

通过使用**我已拥有有效的许可证文件**选项，可以下载有效的许可证文件。
在使用有效的激活码激活产品的过程中，系统将会生成许可证密钥，并将此密钥保存在您的 Avira 产品的程序文件夹中。 如果已激活产品并希望重新安装 Avira 产品，请使用此选项。

说明

在 Avira 产品的一些销售版本中，产品中已包含了激活码。
因此，无需输入密钥激活产品。 如有必要，许可证向导中会显示激活码。

说明
为了激活程序，需建立与 Avira 服务器的连接。
在代理设置下，可配置通过代理服务器建立的 Internet 链接。

- 选择激活进程并单击下一步以确认。
- 如果您已经拥有有效的许可证文件，则直接转到章节“选择*我已拥有有效的许可证文件*选项”。

产品激活

→ 此时将打开一个对话框，您可在其中输入个人数据。

- 输入您的数据并单击下一步。
  → 已将您的数据传输至 Avira 服务器并进行扫描。 已使用您的许可证激活您的 Avira 产品。
  → 许可证数据即会显示在下一个窗口中。
- 单击下一步。
- 跳过下一章“选择*我已拥有有效的许可证文件*选项”。

选择选项“我已拥有有效的许可证文件”

→ 此时将打开一个对话框，以便加载许可证文件。

- 选择包含程序的许可证数据的 *.KEY* 许可证文件，并单击打开。
  → 许可证数据即会显示在下一个窗口中。
- 单击下一步。

完成激活或加载许可证文件后继续

→ 显示加入已使用 Avira SearchFree 的数百万 Avira 用户对话框。

- 如果您不想安装 Avira SearchFree Toolbar，请取消选中 Avira SearchFree Toolbar 和 Avira SearchFree Updater 的最终用户许可协议，以及将Avira SearchFree (search.avira.com)定义为您的浏览器主页的协议。

> 说明必要时请在安装 Avira SearchFree Toolbar 前卸载任何以前安装的搜索工具栏。 否则将无法安装 Avira SearchFree Toolbar。

- 单击下一步。
  - → Avira SearchFree Toolbar 的安装進度會顯示為綠色列。
  - → 安装向导已关闭，配置向导将打开。

3.5 测试产品安装

安装 Avira 产品：

双击从 Internet 下载的安装文件或插入程序 CD，启动安装程序。

基于 Internet 的安装

  - → 显示欢迎屏幕。
- 单击下一步继续安装
  - → 此时将显示语言选择对话框。
- 选择要用于安装 Avira 产品的语言并单击下一步确认语言选择
  - → 此时将显示下载对话框。 安装需要的所有文件将通过 Avira Web 服务器下载。下载结束后，下载窗口将关闭。

使用安装软件包安装

  - → 显示准备安装窗口
  - → 此时将解压安装文件， 安装例程启动

↳ 此时将显示选择安装类型对话框。

说明

默认设置为**快速安装**。 将安装所有标准组件，您无法配置这些组件。

如果您要执行**自定义安装**，请参阅章节：安装和卸载 > 自定义安装。

- 默认设置为**我希望通过使用 Avira Proactiv 和 Protection Cloud 来增强保护效果**对话框（配置 > 常规 > 高级保护）。 如果您不想参加 Avira 社区，请取消选中此复选框。

  ↳ 如果您确认参加 Avira 社区，Avira 会在检测到可疑程序时向 Avira 恶意软件研究中心发送数据。

  此数据仅用于高级联机扫描以及扩展和完善监测技术。 可以单击链接 **ProActiv 和 Protection Cloud** 以获得有关扩展的联机和云扫描的更多详细信息。

- 确认**接受最终用户许可协议**。 若要阅读**最终用户许可协议的文本**，请单击 **EULA** 链接。

- 单击**下一步**。

  ↳ 许可证向导打开并帮助您激活产品。

  ↳ 您可以在此处配置**代理服务器**。

- 单击**代理设置**以进行配置，单击**确定**以确认您的设置。

- 在许可证向导里选择**测试产品**，然后单击**下一步**。

- 将您的数据插入**注册***所需的字段*。 请决定是否订阅 **Avira 新闻通讯**，然后单击**下一步**。

  ↳ 通过一个绿条显示安装进度。

  ↳ 显示**加入已使用 Avira SearchFree 的数百万 Avira 用户**对话框。

- 如果您不想安装 Avira SearchFree Toolbar，请取消选中 Avira SearchFree Toolbar 和 Avira SearchFree Updater 的**最终用户许可协议**，以及将**Avira SearchFree (search.avira.com)定义为您的浏览器主页**的协议。

说明

必要时请在安装 Avira SearchFree Toolbar 前卸载任何以前安装的搜索工具栏。 否则将无法安装 Avira SearchFree Toolbar。

- 单击下一步。
  - ↳ Avira SearchFree Toolbar 的安装進度會顯示為綠色列。
- 将询问您是否重新启动计算机以激活 Avira 产品。 单击是，立即重新启动计算机。
  - ↳ Avira 任务栏图标位于任务栏中。
  - ↳ 您的评估许可证有效期还剩 31 天。

3.6 配置向导

用户定义的安装结束时，配置向导会打开。 通过配置向导，可以定义 Avira 产品的自定义设置。

- 在配置向导的欢迎窗口中，单击下一步以开始配置此程序。
  - ↳ 通过配置 AHeAD 对话框，可以选择 AHeAD 技术的检测级别。所选检测级别用于 Scanner（按需扫描）和 Real-Time Protection（访问时扫描）AHeAD 技术设置。
- 选择检测级别，并单击下一步继续安装。
  - ↳ 在下一个对话框选择扩展威胁类别中，可针对指定的威胁类别调整 Avira 产品的保护功能。
- 如果需要，可激活更多威胁类别并单击下一步继续安装。
  - ↳ 如果您已选择 Avira Real-Time Protection 安装模块，则会显示Real-Time Protection启动模式对话框。 可以指定 Real-Time Protection 的启动时间。每次计算机重新引导时，都将以指定的启动模式启动 Real-Time Protection。

说明

指定的 Real-Time Protection 启动模式保存在注册表中，无法通过“配置”进行更改。

说明

如果为 Real-Time Protection 选择了默认启动模式（正常启动）并使登录进程在启动时快速执行时，可能不会扫描被配置为启动时自动运行的程序，因为这些程序在 Real-Time Protection 完全启动前可能已经启动并运行。

- 启用所需选项，并单击下一步继续配置。
  - → 在下一个对话框系统扫描中，可启用或禁用快速系统扫描。
    在配置完成后、计算机重新引导前，将执行快速系统扫描，目的是扫描正在运行的程序和最重要的系统文件是否有病毒和恶意软件。
- 启用或禁用快速系统扫描选项并单击下一步继续配置。
  - → 在下一个对话框中，通过单击完成可结束配置。
  - → 接受指定和选择的设置。
  - → 如果已启用快速系统扫描选项，则会打开 Luke Filewalker 窗口。
    扫描程序将执行快速系统扫描。
- 如果扫描结束后询问您是否重新启动计算机，请单击是，以确保您的系统得到全面保护。

成功安装后，建议您在控制中心的状态字段中检查程序是否处于最新状态。

- 如果您的 Avira 产品显示您的计算机不安全，请单击修复问题。
  - → 随即打开修复防护对话框。
- 启用预设置选项以最大程度的提升您的系统的安全性。
- 如果正确，请随后执行全面系统扫描。

3.7 更改安装

您可以选择对当前 Avira 产品安装添加或删除程序组件（请参阅章节安装和删除 > 安装模块）。

如果要对当前安装添加或删除模块，可使用 **Windows 控制面板**中的**添加或删除程序**选项**更改/删除**程序。

选择您的 Avira 产品并单击**更改**。 在程序的**欢迎**对话框中，选择**修改**选项。
系统将指导您完成安装更改。

3.8 安装模块

在进行用户定义的安装或更改安装时，可选择、添加或删除以下安装模块。

- **Avira Antivirus Premium**
  此模块包含成功安装 Avira 产品所需的所有组件。
- **Real-Time Protection**
  Avira Real-Time Protection 在后台运行。
  如果可能，它将以“访问时扫描”模式在进行文件操作（如打开、写入和复制）时监视和修复文件。 只要用户执行文件操作（例如加载文档、执行和复制），Avira 产品就会自动扫描文件。 对文件重命名不会触发 Avira Real-Time Protection 执行扫描。
- **Mail Protection**
  Mail Protection
  是您的计算机与电子邮件服务器之间的接口，该服务器向电子邮件程序（电子邮件客户端）提供电子邮件下载。 Mail Protection
  作为所谓的代理在电子邮件程序与电子邮件服务器之间进行连接。
  所有传入电子邮件都路由至该代理，在此经过病毒和恶意程序扫描之后，转发到您的电子邮件程序。
  根据配置，该程序或者自动处理受感染的电子邮件，或者要求用户执行特定操作。
- **Rootkits Protection**
  Avira Rootkits Protection

检查计算机上是否已安装有这样的软件。这种软件侵入计算机系统后，常规的恶意软件防护方法无法再将其检测出来。

- **ProActiv**
  ProActiv 组件可监视应用程序操作，并向用户警告应用程序的可疑行为。
  这种基于行为的识别让您可以保护自身免受未知恶意软件的侵扰。 ProActiv 组件集成在 Avira Real-Time Protection 组件中。
- **Protection Cloud**
  Protection Cloud 是一种用于动态联机检测静态未知恶意软件的模块。
- **Web Protection**
  上网时，您使用 Web 浏览器向 Web 服务器请求数据。 从 Web 服务器传输的数据（HTML 文件、脚本和图像文件、Flash 文件、视频和音乐流等）通常直接进入浏览器缓存，从而显示在 Web 浏览器中，这意味着，Avira Real-Time Protection 无法进行访问时扫描。这样，病毒和恶意程序可以访问您的计算机系统。 Web Protection 称为 HTTP 代理，它监视数据传输端口（80、8080 和 3128），并扫描传输的数据中是否有病毒和恶意程序。
  根据配置，该程序可以自动处理受感染的文件或提示用户执行特定操作。
- **Shell Extension**
  扩展在 Windows 资源管理器的上下文菜单（单击鼠标右键时出现的菜单）中生成用 Avira 扫描所选文件菜单项。 使用该菜单项，可直接扫描文件或目录。

3.9 卸载

如果要从计算机中删除 Avira 产品，可使用 Windows 控制面板中的**添加或删除程序**选项来更改/删除程序。

若要卸载 Avira 产品（以 Windows 7 为例）：

- 通过 Windows 开始菜单打开**控制面板**。
- 双击**程序和功能**。
- 从列表中选择 Avira 产品，然后单击**卸载**。

↳ 系统将询问您是否确实要删除该程序。

- 单击是进行确认。

  ↳ 即会删除所有程序组件。

- 单击完成以结束卸载。

  ↳ 如果需要，将显示一个对话框，建议您重新启动计算机。

- 单击是进行确认。

  ↳ 即会卸载 Avira 产品，重新启动计算机后将删除程序的所有目录、文件和注册表项。

说明

Avira SearchFree Toolbar 不包含在卸载程序中，必须按上述详细步骤单独卸载。 要在 Firefox 中卸载，则须通过加载项管理器启用 Avira SearchFree Toolbar。卸载后，搜索工具栏不再集成于 Web 浏览器中。

4. Avira Antivirus Premium 概述

本章包含 Avira 产品的功能和操作概述。

- 请参阅章节用户界面和操作
- 请参阅章节 Avira SearchFree Toolbar
- 请参阅章节操作方法...?

4.1 用户界面和操作

通过三个程序界面元素操作 Avira 产品：

- 控制中心：用于监视和控制 Avira 产品
- 配置：配置 Avira 产品
- 任务栏的系统任务栏中的任务栏图标：打开控制中心和其他功能

4.1.1 控制中心

控制中心用于监视计算机系统的防护状态，以及控制和操作 Avira 产品的保护组件和功能。

控制中心窗口分为三个区域：**菜单栏**、**导航区域**和详细信息**状态窗口**：

- **菜单栏**：在控制中心菜单栏中，可以访问常规程序功能以及有关程序的信息。
- **导航区**：在导航区中，可以很容易地在控制中心的各部分之间进行切换。各部分包含程序组件的信息及功能，它们按照活动的顺序排列在导航栏中，例如，活动*PC 防护* - **Real-Time Protection**部分。
- **状态**：控制中心打开**状态**视图，在该视图中可以一目了然地看出计算机是否安全，如果计算机安全，可以查看活动组件的概况、上次备份日期以及上次系统扫描日期。**状态**视图还包含用于启动功能或操作的按钮，例如启动或停止 **Real-Time Protection**。

启动和关闭控制中心

若要启动控制中心，可以选择以下方法：

- 双击桌面上的程序图标
- 通过开始 > 程序菜单中的程序条目
- 通过 Avira 产品的任务栏图标

通过文件菜单中的关闭菜单命令或通过单击控制中心的“关闭”选项卡，可以关闭控制中心。

操作控制中心

在控制中心中导航

- 在导航栏中选择一个活动。
  - ↳ 即会打开该活动并显示其他部分。
    在视图中，该活动的第一部分为选中状态并会显示出来。
- 如果需要，单击其他部分可在详细信息窗口中显示此部分。

> 说明
> 您可以使用 [Alt] 键在菜单栏中启用键盘导航功能。
> 如果启用了键盘导航功能，则可以使用箭头键在菜单中移动。 可以使用 Return 键启用活动的菜单项。
> 若要在控制中心中打开或关闭菜单，或在菜单中导航，也可以使用以下组合键：[Alt] + 菜单或菜单命令中带下划线的字母。
> 如果要访问菜单、菜单命令或子菜单，请按住 [Alt] 键。

处理显示在详细信息窗口中的数据或对象：

- 突出显示要编辑的数据或对象。

  若要突出显示多个元素（列中的元素），请按住 Ctrl 键或 Shift 键选择这些元素。
- 单击详细信息窗口上部栏中的相应按钮可以编辑对象。

控制中心概述

- 状态：单击状态栏可以浏览产品的功能和性能（请参阅状态）。

- 在状态部分中，可以一目了然地看出哪些模块处于活动状态，这部分还提供了有关上次执行的更新的信息。

- *PC 防护*：在这一部分中，您将找到用于检查计算机系统上的文件中是否存在病毒和恶意软件的组件。
  - 在 Scanner 部分中，您可以轻松地配置和启动按需扫描。
    预定义的配置文件可以使用经过调整的默认选项进行扫描。
    同样，也可以通过手动选择（未保存）或通过创建用户定义的配置文件，根据您的个人需要调整病毒和恶意程序的扫描选项。
  - Real-Time Protection部分显示已经过扫描的文件的相关信息以及其他统计数据，您可以随时重置这些内容，并访问报告文件。
    实际上，“只需按一下按钮”即可获取有关上一次检测到的病毒或恶意程序的更多详细信息。

- *INTERNET 防护*：在这一部分中，您将找到用于保护您的计算机系统免遭 Internet 病毒和恶意软件及未授权网络访问的组件。
  - Web Protection 部分显示已经过扫描的 URL 和检测到的病毒的相关信息以及其他统计数据，您可以随时重置这些内容，并访问报告文件。
    实际上，“只需按一下按钮”即可获取有关上一次检测到的病毒或恶意程序的更多详细信息。
  - Mail Protection 部分显示Mail Protection扫描过的所有电子邮件及其属性和其他统计数据。

- *儿童保护*：在这一部分中，您可以找到能够确保您的孩子获得安全 Internet 体验的组件。

- *手机保护*：通过此部分可以重定向至 Android 设备的在线访问。
  - Avira Free Android Security 管理所有基于 Android 的设备。

- *管理*：在这一部分中，您将找到用于隔离和管理可疑或受感染文件的工具，以及用于规划定期执行任务的工具。

- 隔离区部分包含所谓的隔离区管理器。
  这是存放已放入隔离区的文件和要放入隔离区的可疑文件的中心位置。
  此外，还可以通过电子邮件将所选文件发送到 Avira 恶意软件研究中心。
- 在计划程序部分中，可以配置预定扫描和更新作业以及备份作业，并可以调整或删除现有作业。
- 在报告部分中，可以查看执行的操作的结果。
- 在事件部分中，可以查看由某些程序模块生成的事件。

4.1.2 游戏模式

如果计算机上的某个应用程序以全屏模式执行，您可以通过启用“游戏模式”有意暂停以弹出窗口和产品内消息形式显示的桌面通知。

可以启用“游戏模式”或者通过单击开/关按钮使其保持自动模式。
“游戏模式”默认设置为自动并显示为绿色。
默认设置将此功能设置为自动，因此每当您运行需要全屏模式的应用程序时，Avira 产品就会自动切换为“游戏模式”。

- 单击关按钮左侧的按钮以启用“游戏模式”。
  - “游戏模式”已启用并显示为黄色。

> 说明
> 建议暂时将默认设置关更改为自动全屏识别模式，否则您将无法收到有关网络事件和可能威胁的可见桌面通知及警告。

4.1.3 任务栏图标

安装后，任务栏的系统任务栏中会显示 Avira 产品任务栏图标：

图标	说明
	Avira Real-Time Protection 已启用,
	Avira Real-Time Protection已禁用或

任务栏图标显示了 Real-Time Protection 服务的状态。

通过任务栏图标的上下文菜单可以快速访问 Avira 产品的核心功能。
若要打开上下文菜单，请右键单击任务栏图标。

上下文菜单中的菜单项

- 启用 **Real-Time Protection**：启用或禁用 Avira Real-Time Protection。
- 启用 **Mail Protection**：启用或禁用 Avira Mail Protection。
- 启用 **Web Protection**：启用或禁用 Avira Web Protection。
- 启用 **Avira Antivirus Premium**：打开控制中心。
- **配置 Avira Antivirus Premium**：打开配置。
- **我的消息**：打开包含 Avira 产品的当前信息的弹出框。
- **我的通信设置**：打开产品消息订阅中心
- **开始更新**启动更新。
- **帮助**：打开联机帮助。
- **关于 Avira Antivirus Premium**：打开包含有关 Avira 产品的信息的对话框：产品信息、版本信息、许可证信息。
- **Internet 上的 Avira**：打开 Internet 上的 Avira 门户网站。 需要有活动的 Internet 连接才能执行此操作。

4.2 Avira SearchFree Toolbar

Avira SearchFree Toolbar 包含两个主要组件：Avira SearchFree 和工具栏。

Avira SearchFree Toolbar 作为加载项安装。 首次访问浏览器时（在 Firefox 和 Internet Explorer 中）会弹出一条消息，询问您是否允许安装此工具栏。
您必须接受方可成功安装 Avira SearchFree Toolbar。

Avira SearchFree 是一种搜索引擎，它包含一个链接到 Avira 网站和 Web、图像及视频频道的可点击 Aira 徽标。 这样可使 Avira 用户获得更安全的 Internet 导航。

此工具栏集成于 Web 浏览器中，它包含搜索框、链接到 Avira 网站的 Avira 徽标、两个状态显示、三个小组件和 **Options** 菜单。

- 搜索工具栏
  使用免费的搜索工具栏即可使用 Avira 搜索引擎快速搜索 Internet。
- 状态显示
  状态显示可提供 Web Protection 的状态信息和 Avira 产品的当前更新状态信息，并可帮助您识别保护 PC 所需采取的操作。
- 小组件
  Avira 提供三种具有最重要的 Internet 相关功能的小组件。 单击一下便可转到 Facebook 和电子邮件，或者可以确保安全 Web 浏览（仅 Firefox 和 Internet Explorer）。
- 选项
  可以使用 **Options** 菜单访问工具栏选项、清除历史记录、查找工具栏帮助和信息，还可通过 Web 浏览器直接卸载 Avira SearchFree Toolbar（仅 Firefox 和 Internet Explorer）。

4.2.1 使用方法

Avira SearchFree

可以使用 Avira SearchFree 定义任何数量的搜索词，以便浏览 Internet。

在搜索框中输入搜索词然后按 **Enter** 键或单击**Search**。 然后 Avira SearchFree 引擎会为您搜索 Internet 并在浏览器窗口中显示所有命中结果。

如需了解 Avira SearchFree 在 Internet Explorer、Firefox 和 Chrome 中的自定义配置方法，请转到选项。

状态显示

Web Protection

可以使用图标和消息来识别需要采用何种操作来保护 PC：

图标	状态显示	说明
	Web Protection	如果将光标移过图标时显示以下消息：*Avira Web Protection is active. Your browsing is protected.* 不需要进一步操作。
	Web Protection is inactive	如果将光标移过图标时显示以下消息：*Avira Web Protection is off. Click to find out how to turn it on.* ↳ 您将被重定向至我们的“知识库”文章。

	No Web Protection	如果将光标移过图标时显示以下消息之一： • *You do not have Avira Web Protection installed. Click to find out how to protect your browsing.* 如果未正确安装或卸载 Avira Antivirus 产品，则会显示此消息。 • *Web Protection is included for free with Avira Antivirus. Click to find out how to install it.* 如果未安装“Web Protection”或已卸载，则会显示此消息。 ↪ 两种情况下，都会将您重定向至 Avira 主页，您可以在此处下载 Avira 产品。
	Error	如果将光标移过图表时显示以下消息：*Avira reported an error. Click to contact Support for help.* ▸ 单击灰色图标或文本即可转到 Avira 支持页面。

小组件

Avira SearchFree 含有三个小组件，它们具有对当今 Internet Web 浏览而言最重要的功能：Facebook、电子邮件和 Browser Security。

Facebook

通过此功能可以收到来自 Facebook 的所有消息并保持更新。

电子邮件

如果单击工具栏中的电子邮件符号，则会显示一个下拉列表。
可以从中选择最常用的电子邮件提供商。

Browser Security

这个小组件只需单击一下即可提供您每日可能需要的所有 Internet 安全选项。
此选项仅适用于 Firefox 和 Internet Explorer。
在不同浏览器中，这些功能的名称有时也不同：

- *弹窗阻止程序*

如果启用此选项，则会阻止所有弹出窗口。

- *阻止 Cookies*

如果启用此选项，则不会在计算机上保存 Cookies。

- *隐私浏览 (Firefox)/InPrivate 浏览 (Internet Explorer)*

如果您不想在上网时在 Internet 上留下任何个人信息，请启用此选项。 此选项不适用于 Internet Explorer 7 和 8。

- *清除最近的历史记录 (Firefox) /删除浏览历史记录 (Internet Explorer)*

通过此选项可以擦除您的所有 Internet 活动痕迹。

Website Safety Advisor

Website Safety Advisor 可以在导航时提供安全排名。
您可以在访问时评价网站信誉，并检查该网站是否会造成低安全风险或高安全风险。
这个小组件还可提供有关网站的更多信息，例如谁是域名所有者，或者为什么该网站被归类为安全或危险。

Website Safety Advisor 的状态作为 Avira 任务栏图标显示在 Toolbar 和搜索结果中，与其他图标组合在一起：

图标	状态显示	说明
	Safe	对于安全网站，显示为绿色勾号。
	Low risk	对于具有低风险的网站，显示为黄色感叹号。
	High risk	对于具有高安全风险的网站，显示为红色停止标志。
	Unknown	状态未知时会显示绿色问号。
	Verifying	验证网站状态时会显示此标志。

Browser Tracking Blocker

Browser Tracking Blocker 可以在您上网时阻止跟踪程序收集您的信息。
此小组件允许您选择要阻止的跟踪程序和要允许的跟踪程序。

跟踪公司分为三类：

- 社会网络
- 广告网络
- 其他公司

4.2.2 选项

Avira SearchFree Toolbar 与 Internet Explorer、Firefox 和 Google Chrome 兼容，并且可以在这三种 Web 浏览器中配置：

- Internet Explorer 配置选项
- Firefox 配置选项
- Google Chrome 配置选项

Internet Explorer

在 Internet Explorer 中，选项菜单提供 Avira SearchFree Toolbar 的以下配置选项：

Toolbar options

Search

Avira search engine

在 Avira search engine菜单中，可以选择使用哪一种搜索引擎进行搜索。
搜索引擎对美国、巴西、德国、西班牙、欧洲、法国、意大利、荷兰、俄罗斯和英国可用。

Open searches in

在 Open searches in
选项菜单中，可以选择在何处显示搜索结果；在当前窗口、新窗口还是新选项卡中。

Display recent searches

如果启用 Display recent searches
选项，则可在搜索工具栏的文本输入框下方显示以前使用过的搜索词。

Auto clear recent search history when I close the browser

如果您不想保存以前的搜索并希望在关闭 Web 浏览器时清除搜索历史记录，则启用 Auto clear recent search history when I close the browser 选项。

More options

Select toolbar language

在 Select toolbar language 下，可以选择 Avira SearchFree Toolbar 的显示语言。
此工具栏提供英语、德语、西班牙语、法语、意大利语、葡萄牙语和荷兰语版。

说明

在可能的情况下，Avira SearchFree Toolbar 的默认语言与您的程序一致。如果工具栏不提供您的语言版本，则默认语言为英语。

Show button text labels

如果您想隐藏 Avira SearchFree Toolbar 图标旁的文本，则禁用 **Show button text labels**。

Clear history

如果您不想保存以前的搜索并希望立即清除历史记录，则启用 **Clear history**。

Help

单击 **Help** 即可访问含有与工具栏有关的常见问题解答 (FAQ) 的网站。

Uninstall

还可以在 Internet Explorer 中直接卸载 Avira SearchFree Toolbar：通过 Web 浏览器卸载

About

单击 **About** 即可显示所安装的 Avira SearchFree Toolbar 的版本。

Firefox

在 Firefox Web 浏览器中， **Options** 菜单提供 Avira SearchFree Toolbar 的以下配置选项：

Toolbar options

Search

Select Avira search engine

在 Avira search engine菜单中，可以选择使用哪一种搜索引擎进行搜索。
搜索引擎对美国、巴西、德国、西班牙、欧洲、法国、意大利、荷兰、俄罗斯和英国可用。

Display recent searches

如果启用 Display recent searches 选项，则可通过单击搜索工具栏中的箭头来显示以前使用过的搜索词。
如果您想再次显示搜索结果，则选择一个搜索词。

Auto clear recent search history when I close the browser

如果您不想保存以前的搜索并希望在关闭 Web 浏览器时清除搜索历史记录，则启用 Auto clear recent search history when I close the browser 选项。

Display Avira search results when I type keywords or invalid URLs into the browser address bar

如果启用此选项，则会启用搜索，每一次在 Web 浏览器地址栏中输入关键词或有效 URL 时，都会显示搜索结果。

More options

Select toolbar language

在 Select toolbar language 下，可以选择 Avira SearchFree Toolbar 的显示语言。
此工具栏提供英语、德语、西班牙语、法语、意大利语、葡萄牙语和荷兰语版。

> 说明
> 在可能的情况下，Avira SearchFree Toolbar 的默认语言与您的程序一致。
> 如果工具栏不提供您的语言版本，则默认语言为英语。

Show button text labels

如果您想隐藏 Avira SearchFree Toolbar 图标旁的文本，则禁用 **Show button text labels**。

Clear history

如果您不想保存以前的搜索并希望立即清除历史记录，则启用 **Clear history**。

Help

单击 **Help** 即可访问含有与工具栏有关的常见问题解答 (FAQ) 的网站。

Uninstall

还可以在 Firefox 中直接卸载 Avira SearchFree Toolbar：通过 Web 浏览器卸载。

About

单击 **About** 即可显示所安装的 Avira SearchFree Toolbar 的版本。

Google Chrome

在 Chrome Web 浏览器中，Avira 小红伞菜单下提供 Avira SearchFree Toolbar 的以下配置选项：

Help

单击 **Help** 即可访问含有与工具栏有关的常见问题解答 (FAQ) 的网站。

卸载说明

此处链接到的文章包含卸载工具栏所需的所有信息。

About

单击 **About** 即可显示已安装的 Avira SearchFree Toolbar 的版本。

显示/隐藏 Avira SearchFree Toolbar

单击此处即可在 Web 浏览器上隐藏或显示 Avira SearchFree Toolbar。

4.2.3 卸载

若要卸载 Avira SearFree Toolbar（以 Windows 7 为例）：

- 通过 Windows 开始菜单打开控制面板。
- 双击程序和功能。
- 选择列表中的 **Avira SearchFree Toolbar plus Web Protection** 并单击卸载。
  - ↳ 系统将询问您是否确实要卸载此产品。
- 单击是进行确认。
  - ↳ 即会卸载 Avira SearchFree Toolbar 已经 Web Protection，重新启动计算机后将删除 Avira SearchFree Toolbar 已经 Web Protection 的所有目录、文件和注册表项。

通过 Web 浏览器卸载

还可以选择在浏览器中直接卸载 Avira SearchFree Toolbar。 此选项仅适用于 **Firefox 和 Internet Explorer**：

- 在搜索工具栏中打开**Options**菜单。
- 单击**Uninstall**。
  - ↳ 如果您已打开 Web 浏览器，现在系统将请您关闭 Web 浏览器。
- 关闭 Web 浏览器并单击确定。
  - ↳ 即会卸载 Avira SearchFree Toolbar plus Web Protection，重新启动计算机后将删除 Avira SearchFree Toolbar plus Web Protection 的所有目录、文件和注册表项。

> 说明
> 请注意，必须在加载项管理器中启用工具栏方可卸载 Avira SearchFree Toolbar。

作为加载项卸载

此工具栏是作为加载项安装的，因此显然可以将其作为加载项卸载：

Firefox

单击**工具 > 加载项 > 扩展**。 可以在此处管理 Avira 加载项：启用或禁用工具栏以及卸载。

Internet Explorer

转到**管理加载项 > 工具栏和扩展**。 可以在此处启用和禁用 Avira SearchFree Toolbar，或者将其卸载。

Google Chrome

单击**选项> 扩展程序**即可轻松管理工具栏：启用、禁用或卸载。

4.3 操作方法

“操作方法”章节提供有关许可证和产品激活的简要说明以及有关 Avira 产品最新功能的信息。选择的短文用作有关 Avira 产品功能的概述。这些文章不替代此帮助中心中每个部分的详细信息。

4.3.1 激活许可证

若要激活 Avira 产品的许可证：

使用许可证文件 *.KEY* 激活 Avira 产品的许可证。 您可通过电子邮件从 Avira 获取该许可证文件。 许可证文件包含您在一个订购流程中所订购的所有产品的许可证。

如果尚未安装 Avira 产品：

- 请将许可证文件保存到计算机上的本地目录中。
- 安装 Avira 产品。
- 在安装期间，请输入许可证文件的保存位置。

如果已安装 Avira 产品：

- 请在文件管理器或激活电子邮件中双击许可证文件，在许可证管理器打开后，按照屏幕上的说明操作。

  - 或者 -

  在 Avira 产品的控制中心中，选择**帮助 > 许可证管理**菜单项

> 说明
> 在 Windows Vista 中，此时将显示“用户帐户控制”对话框。
> 如果需要，以管理员身份登录。 单击**继续**。

- 突出显示许可证文件并单击**打开**。

  ↪ 此时将显示一条消息。

- 单击**确定**进行确认。

  ↪ 许可证即会被激活。

- 如果需要，请重新启动系统。

4.3.2 激活产品

Avira 产品的激活方法如下：

使用有效的完整许可证激活

要使用完整许可证激活程序，您需要一个有效的激活码，其中包含您所购买的许可证的数据。 激活码已通过电子邮件发送给您，或者打印在产品包装上。

用评估许可证激活

使用自动生成的评估许可证激活 Avira 产品，使用这种许可证时，您可以在一段有限的时间内测试 Avira 产品的所有功能。

> 说明
> 若要激活产品或获取测试许可证，您需要有活动的 Internet 链接。
> 如果无法与 Avira 服务器建立连接，请检查所用防火墙的设置：通过 HTTP 协议和端口 80（Web 通信）以及通过加密协议 SSL 和端口 443 连接，使用此连接激活产品。 请确保您的防火墙未阻止传入和外发的数据。
> 首先请检查 Web 浏览器是否能访问网页。

下文描述了如何激活 Avira 产品：

如果尚未安装 Avira 产品：

- 安装 Avira 产品。
  - ↳ 在安装过程中，您需要选择激活选项
- **激活产品**：使用有效的完整许可证激活
- **测试产品**：使用评估许可证激活
- 输入激活码，使用完整许可证激活。
- 单击下一步确认选择激活过程。
- 如果需要，请输入您的个人数据进行注册，并单击下一步进行确认。
  - ↳ 许可证数据即会显示在下一个窗口中。 Avira 产品已启用。

- 继续**安装**。

如果已安装 Avira 产品：

- **在控制中心中**，选择**帮助 > 许可证管理菜**单项。
  - ↪ **此时将打**开 *许可证向导*，您**可在其中**选择**激活**选项。**后面的**产品**激活**步骤**与上述**过程**相同**。

4.3.3 执行自动更新

使用 Avira 计划**程序**创**建作**业**以自**动**更新** Avira 产品：

- **在控制中心中**，选择 *管理* **> 计划程序部分**。
- 单击 + **插入新作**业图标。
  - ↪ **此时将显示作业名称和说明**对话**框**。
- **提供作**业**名称**，**如果需要**，请**同时提供**说**明**。
- 单击**下一步**。
  - ↪ **此时将显示作业类型**对话**框**。
- **从列表中**选择**更新作**业。
- 单击**下一步**。
  - ↪ **此时将显示作业时间**对话**框**。
- 选择**更新**时间：

- **立即执行**
- **每天**
- **每周**
- **间隔**
- **一次**
- **登录**

说明

建议定期自动更新。 建议的更新间隔时间为2 小时。

- 如果需要，请根据选择指定日期。
- 如果需要，可选择其他选项（是否可用取决于作业类型）：

- **如果时间已过期则重复执行作业**
  执行在要求的时间未能执行（例如由于计算机断电）的过期作业。
- **当连接至 Internet（拨号）时启动作业**
  开始除按定义的频率外，建立 Internet 连接时也执行作业。

- 单击**下一步**。

  ↪ 此时将显示**选择显示模式**对话框。

- 选择作业窗口的显示模式：

- **不可见**：无作业窗口
- **最小化**：仅显示进度条
- **最大化**：显示整个作业窗口

- 单击**完成**。

  ↪ 新创建的作业就会显示在*管理* > **计划程序**部分的起始页面上，并且其状态为已启用（勾号）。

- 如果需要，可停用不打算执行的作业。

使用以下图标进一步定义作业：

查看作业属性

编辑作业

删除作业

启动作业

- 停止作业

4.3.4 启动手动更新

可通过多种方式手动启动更新：手动启动更新时，始终会更新病毒定义文件和扫描引擎。只有在 PC 保护 > 更新 > 产品更新下的配置中启用自动下载和安装产品更新选项才能进行产品更新

若要手动启动 Avira 产品更新：

- 右键单击任务栏中的 Avira 任务栏图标。
  - ↳ 此时将显示上下文菜单。
- 选择开始更新。
  - ↳ 此时将显示更新程序对话框。

- 或者 -

- 在控制中心中，选择状态。
- 在上一次更新字段中，单击开始更新链接。
  - ↳ 此时将显示“更新程序”对话框。

- 或者 -

- 在控制中心的更新菜单中，选择菜单命令开始更新。
  - ↳ 此时将显示“更新程序”对话框。

> 说明
> 建议定期自动更新。建议的间隔时间为 2 小时。

> 说明
> 您也可以通过 Windows 安全中心直接执行手动更新。

4.3.5 使用扫描配置文件扫描病毒和恶意软件

扫描配置文件是一组待扫描的驱动器和目录。

通过扫描配置文件执行扫描的方法如下：

使用预定义的扫描配置文件

如果预定义的扫描配置文件符合您的要求，可使用此方法。

自定义和应用扫描配置文件（手动选择）

如果要使用自定义的扫描配置文件进行扫描，可使用此方法。

创建并应用新的扫描配置文件

如果要创建自己的扫描配置文件，可使用此方法。

在不同操作系统中，提供了不同图标来启动用扫描配置文件进行的扫描：

- 在 Windows XP 中：

  此图标启动通过扫描配置文件进行的扫描。

- 在 Windows Vista 中：

  在 Microsoft Windows Vista 中，目前控制中心只有有限权限（例如对目录和文件的访问权）。在控制中心中，某些操作和文件访问只能通过扩展管理员权限执行。在每次开始通过扫描配置文件进行扫描时，都必须授予这些扩展管理员权限。

  - 此图标启动通过扫描配置文件进行的有限扫描。只会扫描已由 Windows Vista 授予访问权的目录和文件。
  - 此图标启动使用扩展管理员权限进行的扫描。确认后，将扫描所选扫描配置文件中的所有目录和文件。

使用扫描配置文件扫描病毒和恶意软件：

1. 转到控制中心并选择 *PC 保护 > System Scanner*。

↳ 此时将显示预定义的扫描配置文件。

- 选择预定义扫描配置文件之一。

  - 或者 -

  调整扫描配置文件手动选择。

  - 或者 -

  创建新的扫描配置文件

- 单击图标（Windows XP： 或 Windows Vista： ）。
- 此时将显示 **Luke Filewalker** 窗口，并启动系统扫描。

  ↳ 扫描完成时将显示结果。

如果要调整扫描配置文件：

- 在扫描配置文件中，展开手动选择文件树，以便打开要扫描的所有驱动器和目录。
  - 单击 **+** 图标：显示下一级目录。
  - 单击 **-** 图标：隐藏下一级目录。
- 通过单击相应目录级别的相关框，突出显示要扫描的节点和目录：

  可以使用以下目录选择方法：

  - 选择目录，包括子目录（黑色复选标记）
  - 仅选择一个目录的子目录（灰色复选标记，子目录带黑色复选标记）
  - 不选择目录（无复选标记）

如果要创建新的扫描配置文件：

- 单击图标 创建新配置文件。

  ↳ 配置文件新建配置文件即会显示在以前创建的配置文件下面。

- 如果需要，单击图标 以重命名该扫描配置文件。
- 通过单击相应目录级别的复选框，突出显示要保存的节点和目录。

可以使用以下目录选择方法：

- 选择目录，包括子目录（黑色复选标记）
- 仅选择一个目录的子目录（灰色复选标记，子目录带黑色复选标记）
- 不选择目录（无复选标记）

4.3.6 使用拖放操作扫描病毒和恶意软件

使用拖放操作系统地扫描病毒和恶意软件：

✓ Avira 产品的控制中心已打开。

▸ 突出显示要扫描的文件或目录。

▸ 使用鼠标左键将突出显示的文件或目录拖到**控制中心**中。

↳ 此时将显示 **Luke Filewalker** 窗口，并启动系统扫描。

↳ 扫描完成时将显示结果。

4.3.7 通过上下文菜单扫描病毒和恶意软件

通过上下文菜单系统地扫描病毒和恶意软件：

▸ 右键单击要扫描的文件或目录（例如在 Windows 资源管理器中，在桌面上或打开的 Windows 目录中执行此操作）。

↳ 此时将显示 Windows 资源管理器上下文菜单。

▸ 在上下文菜单中选择**使用 Avira 扫描所选文件**。

↳ 此时将显示 **Luke Filewalker** 窗口，并启动系统扫描。

↳ 扫描完成时将显示结果。

4.3.8 自动扫描病毒和恶意软件

> 说明
> 安装后，在计划程序中创建全面系统扫描扫描作业，以建议时间间隔自动执行全面系统扫描。

创建作业以自动扫描病毒和恶意软件：

- 在控制中心中，选择管理 > 计划程序部分。
- 单击图标 + 。
  - ↳ 此时将显示作业名称和说明对话框。
- 提供作业名称，如果需要，请同时提供说明。
- 单击下一步。
  - ↳ 此时将显示作业类型对话框。
- 选择扫描作业。
- 单击下一步。
  - ↳ 此时将显示选择配置文件对话框。
- 选择要扫描的配置文件。
- 单击下一步。
  - ↳ 此时将显示作业时间对话框。
- 选择扫描时间：

- 立即执行
- 每天
- 每周
- 间隔
- 一次
- 登录

- 如果需要，请根据选择指定日期。
- 如果需要，可选择以下附加选项（是否可用取决于作业类型）：

  如果时间已过期则重复执行作业

  执行在要求的时间未能执行（例如由于计算机断电）的过期作业。

- 单击**下一步**。

  ↪ 此时将显示**选择显示模式**对话框。

- 选择作业窗口的显示模式：

- **不可见**：无作业窗口
- **最小化**：仅显示进度条
- **最大化**：显示整个作业窗口

- 如果要在扫描完成时自动关闭计算机，请选择**作业完成后关闭计算机**选项。
  仅当显示模式设置为**最小化**或**最大化**时，此选项才可用。
- 单击**完成**。

  ↪ 新创建的作业就会显示在*管理* > *计划程序*部分的起始页面上，并且其状态为已启用（勾号）。

- 如果需要，可停用不打算执行的作业。

使用以下图标进一步定义作业：

查看作业属性

编辑作业

删除作业

启动作业

停止作业

4.3.9 针对 Rootkit 和活动恶意软件的扫描

若要扫描活动的 Rootkit，请使用预定义扫描配置文件扫描 **Rootkit 和活动恶意软件**。

系统地扫描活动的 Rootkit：

- 转到控制中心并选择 *PC 防护* **>Scanner**。
  - ↳ 此时将显示预定义的扫描配置文件。
- 选择预定义扫描配置文件扫描 **Rootkit 和活动恶意软件**。
- 如果需要，请单击该目录级别的复选框，突出显示要扫描的其他节点和目录。
- 单击图标（Windows XP： 或 Windows Vista： ）。
  - ↳ 此时将显示 **Luke Filewalker** 窗口，并启动系统扫描。
  - ↳ 扫描完成时将显示结果。

4.3.10 对检测到的病毒和恶意软件做出反应

对于 Avira 产品的各保护组件，可以在针对检测的操作部分下的配置中定义 Avira 产品如何对检测到的病毒或恶意程序做出反应。

Real-Time Protection 的 ProActiv 组件不提供可配置操作选项：始终在 **Real-Time Protection：可疑的应用程序行为** 窗口中提供检测通知。

Scanner 的操作选项：

交互式

在交互式操作模式中，Scanner 的扫描结果将显示在对话框中。
此选项默认设置为启用。

使用 **Scanner** 扫描时，在扫描完成后您会收到一个警报，其中列出了受影响的文件。
可以使用上下文菜单选择要对各种受感染文件执行的操作。
可以对所有受感染文件执行标准操作，也可以取消 Scanner。

自动

在自动操作模式中，当检测到病毒或恶意程序时，会自动执行此区域中选定的操作。

Real-Time Protection 的操作选项：

交互式

在交互式操作模式中，将拒绝数据访问并显示一个桌面通知。
在桌面通知中，您可以删除检测到的恶意软件，或使用详细信息按钮将恶意软件传给 Scanner 组件以进行进一步的病毒管理。
扫描程序将会打开一个包含检测通知的窗口，其中通过上下文菜单提供了各种用于管理受感染文件的选项（请参阅检测 > Scanner）：

自动

在自动操作模式中，当检测到病毒或恶意程序时，会自动执行此区域中选定的操作。

Mail Protection、Web Protection 的操作选项：

交互式

在交互式操作模式中，如果检测到病毒或恶意程序，则会出现一个对话框，您可以在其中选择要对受感染对象执行的操作。 此选项默认设置为启用。

自动

在自动操作模式中，当检测到病毒或恶意程序时，会自动执行此区域中选定的操作。

在交互式操作模式中，您可以对检测到的病毒和恶意程序做出反应，方法是：针对警报中的受感染对象选择操作，然后通过单击确认执行所选操作。

可选择以下用于处理受感染对象的操作：

说明
哪些操作可以选择取决于操作系统、报告检测的保护组件（Avira Real-Time

Protection、Avira Scanner、Avira Mail Protection、Avira Web Protection）以及检测的恶意软件类型。

Scanner 和 Real-Time Protection 的操作（非 ProActiv 检测）：

修复

修复文件。

只有受感染文件可修复时，此选项才可用。

重命名

用 *.vir 扩展名重命名文件。 因此不能再直接访问这些文件（例如，通过双击访问）。以后可修复文件并重新指定其原始名称。

隔离区

将文件打包为特殊格式 (*.qua) 并将其直接移到硬盘上的隔离区目录 *INFECTED* 中，这样就无法再直接访问该文件。
以后可在隔离区中修复此目录中的文件，必要时也可将其发送给 Avira。

删除

文件将被删除。 此过程比**覆盖并删除**快得多。
如果检测到启动扇区病毒，可通过删除启动扇区来删除病毒。 并写入新的启动扇区。

忽略

不采取进一步操作。 计算机上的受感染文件仍处于活动状态。

覆盖并删除

使用默认模板覆盖文件，然后将其删除。 文件将无法还原。

警告

这样可能导致数据丢失和操作系统损坏！ 只有在特殊情况下才应选择**忽略**选项。

始终忽略

针对 Real-Time Protection 检测的操作选项：Real-Time Protection 不采取进一步操作。 允许访问文件。
允许对此文件的所有进一步访问，并且不再提供进一步通知直到计算机重新启动或者病毒定义文件更新。

复制到隔离区

对检测到的 Rootkit 的操作选项：将检测到的 Rootkit 复制到隔离区。

修复启动扇区 | 下载修复工具

当检测到受感染启动扇区时：提供多个选项用于修复受感染的磁盘驱动器。 如果 Avira 产品无法执行修复，您可以下载用于检测和删除启动扇区病毒的专用工具。

> 说明
> 如果您对运行中的进程执行操作，则会先终止相关进程，然后再执行这些操作。

针对 ProActiv 组件检测的 Real-Time Protection 操作（通知应用程序的可疑行为）：

可信程序

应用程序将继续运行。 程序将被添加到允许的应用程序列表中，并从 ProActiv 组件的监视范围中排除。 当添加到允许的应用程序列表中时，监视类型将设为*内容*。这意味着只有应用程序的内容保持不变，才会从 ProActiv 组件的扫描范围中排除（请参阅 应用程序过滤 > 允许的应用程序）。

阻止程序一次

阻止应用程序，即终止应用程序。 但应用程序的其他操作将继续受 ProActiv 组件监视。

始终阻止此程序

阻止应用程序，即终止应用程序。 程序将被添加到被阻止程序列表中，并且不能再运行（请参阅 应用程序过滤：要阻止的应用程序）。

忽略

应用程序将继续运行。 但应用程序的其他操作将继续受 ProActiv 组件监视。

Mail Protection 操作：传入电子邮件

移到隔离区

将电子邮件（包括所有附件）移到隔离区。 受感染的电子邮件将被删除。
电子邮件的正文及所有附件将被替换为默认文本。

删除邮件

受感染的电子邮件将被删除。 电子邮件的正文及所有附件将被替换为默认文本。

删除附件

将受感染的附件替换为默认文本。
如果电子邮件的正文受到感染，则将其删除并将其替换为默认文本，
仅发送电子邮件本身。

将附件移到隔离区

将受感染的附件放在隔离区，然后将其删除（替换为默认文本）。 发送电子邮件正文。
可在以后通过隔离区管理器发送受感染的附件。

忽略

发送受感染的电子邮件。

警告
这将会导致病毒和恶意程序访问您的计算机系统。

只有在特殊情况下才应选择**忽略**选项。
请在邮件客户端禁用预览，不要通过双击打开任何附件！

Mail Protection 操作：外发电子邮件

将邮件移到隔离区(不发送)

将电子邮件与所有附件一起复制到隔离区，不发送电子邮件。
电子邮件仍留在电子邮件客户端的发件箱中。 电子邮件程序中会收到一条错误消息。
从电子邮件帐户中发出的所有其他电子邮件都将进行恶意软件扫描。

阻止发送邮件(不发送)

不发送电子邮件，它仍留在电子邮件客户端的发件箱中。
电子邮件程序中会收到一条错误消息。
从电子邮件帐户中发出的所有其他电子邮件都将进行恶意软件扫描。

忽略

发送受感染的电子邮件。

警告
如果采用这种方式，病毒和恶意程序可能侵入电子邮件收件人的计算机系统。

Web Protection 操作：

拒绝访问

向 Web 服务器请求的网站和/或传输的任何数据或文件都不会发送到 Web 浏览器。
Web 浏览器中会显示一条错误消息，指出访问已被拒绝。

移到隔离区

将 Web 服务器请求的网站和/或传输的所有数据或文件移到隔离区。
如果受感染文件具有参考价值，则可以从隔离区管理器恢复它，也可以根据需要将其发送给 Avira 恶意软件研究中心。

忽略

Web Protection 将向 Web 服务器请求的网站和/或传输的数据和文件转发给 Web 浏览器。

警告

这将会导致病毒和恶意程序访问您的计算机系统。

只有在特殊情况下才应选择**忽略**选项。

说明

建议您将所有无法修复的可疑文件移到隔离区。

说明

您也可以将由启发式扫描报告的文件发送给我们以进行分析。

例如，您可以将这些文件上传至我们的网站：http://www.avira.cn/sample-upload

您可以通过启发式扫描从名称 *HEUR/* 或 *HEURISTIC/*（它们是文件名的前缀）识别报告的文件，例如 *HEUR/testfile.**。

4.3.11 处理已隔离的文件 (*.qua)

处理已隔离的文件：

- 在控制中心中，选择*管理* > **隔离部分**。
- 检查涉及到哪些文件，以便在必要时从另一个位置将原先的文件重新加载到计算机。

如果要查看有关某个文件的更多信息：

- 突出显示该文件并单击 。
  - ↪ 此时将显示**属性**对话框，其中包含有关该文件的更多信息。

如果要重新扫描某个文件：

如果更新了 Avira 产品的病毒定义文件，且怀疑存在误报，则建议扫描文件。
这样，您就可以通过重新扫描确认误报和还原文件。

- 突出显示该文件并单击 。
  - ↳ 将使用系统扫描设置来扫描该文件是否存在病毒和恶意软件。
  - ↳ 扫描后，将显示重新扫描统计数据对话框，其中包含有关重新扫描之前和之后文件状态的统计数据。

删除文件：

- 突出显示该文件并单击 。
- 必须用是来确认您的选择。

如果要将文件上传到 Avira 恶意软件研究中心 Web 服务器以供分析：

- 突出显示要上传的文件。
- 单击 。
  - ↳ 此时将打开一个对话框，其中包含一个表单，供您输入联系数据。
- 输入所有必需的数据。
- 选择一个类型：可疑文件或怀疑误报。
- 选择响应格式：HTML、文本、HTML 和文本。
- 单击确定。
  - ↳ 即会以压缩格式将文件上传到 Avira 恶意软件研究中心 Web 服务器。

说明

在以下情况中，建议用 Avira 恶意软件研究中心进行分析。
启发式命中文件（可疑文件）：在扫描过程中， Avira 产品将某个文件分类为可疑文件并移到隔离区：在病毒检测对话框或扫描生成的报告文件中建议用 Avira 恶意软件研究中心分析此文件。
可疑文件：您认为某个文件可疑并因此将该文件移到隔离区，但对该文件进行扫

描却未发现病毒和恶意文件。
可疑误报：您认为检测到的病毒是误报：Avira
产品报告在某个文件中检测到问题，此文件很有可能感染了恶意软件。

说明
上传文件的大小限制：非压缩形式为 20 MB，压缩形式为 8 MB。

说明
一次只能上传一个文件。

如果要将隔离对象的属性导出到文本文件中：

- 突出显示该隔离对象并单击 。
  - ↪ 此时会打开文本文件 *quarantaene - Notepad*，其中包含来自所选隔离对象的数据。
- 保存该文本文件。

您也可以还原隔离区中的文件（请参阅章节：隔离：还原隔离区中的文件）。

4.3.12 还原隔离区中的文件

在不同操作系统中，由不同图标控制还原过程：

- 在 Windows XP 中：
  - 此图标将文件还原到其原来的目录。
  - 此图标将文件还原到您选择的目录。
- 在 Windows Vista 中：

  在 Microsoft Windows Vista 中，目前控制中心只有有限权限（例如对目录和文件的访问权）。

在控制中心中，某些操作和文件访问只能通过扩展管理员权限执行。
在每次开始通过扫描配置文件进行扫描时，都必须授予这些扩展管理员权限。

- 此图标将文件还原到您选择的目录。
- 此图标将文件还原到其原来的目录。
  如果访问此目录需要扩展管理员权限，则会出现相应的请求。

还原隔离区中的文件：

警告

这样可能导致数据丢失和操作系统损坏！
只有在特殊情况下才应使用还原所选对象功能。
只应还原再次扫描时可修复的文件。

✓ 已重新扫描和修复文件。

▸ 在控制中心中，选择**管理 > 隔离部分**。

说明

仅当文件扩展名为 *.eml 时才能使用 还原电子邮件和电子邮件附件。

将文件还原到其原来的位置：

▸ 突出显示文件并单击图标（Windows XP：、Windows Vista ）。

该选项不可用于电子邮件。

说明

仅当文件扩展名为 *.eml 时才能使用 还原电子邮件和电子邮件附件。

↳ 此时将显示一个消息，询问您是否要还原该文件。

▸ 单击**是**。

↳ 文件即会还原到它被移到隔离区之前所在的目录。

将文件还原到指定目录：

- 突出显示该文件并单击 。
  - ↳ 此时将显示一个消息，询问您是否要还原该文件。
- 单击**是**。
  - ↳ 此时将显示用于选择目录的 Windows 默认窗口*另存为*。
- 选择要将文件还原到的目录并确认。
  - ↳ 文件即会还原到所选目录。

4.3.13 将可疑文件移到隔离区

手动将可疑文件移到隔离区：

- 在控制中心中，选择*管理* > 隔离部分。
- 单击 。
  - ↳ 此时将显示用于选择文件的 Windows 默认窗口。
- 选择文件并单击**打开**进行确认。
  - ↳ 该文件将移到隔离区。

可以通过 Avira Scanner 扫描隔离区中的文件（请参阅章节：隔离：处理隔离的文件 (*.qua)）。

4.3.14 修改或删除扫描配置文件中的文件类型

在扫描配置文件中指定更多要扫描的文件类型或从扫描中排除特定文件类型（仅限手动选择和自定义扫描配置文件）：

✓ 在控制中心，转到 *PC 防护* >**Scanner** 部分。

- 右键单击要编辑的扫描配置文件。

↳ 此时将显示上下文菜单。

- 选择**文件过滤器**。
- 单击**上下文菜单**中右侧的小三角形，进一步展开该菜单。

  ↳ 此时将显示**默认值**、**扫描所有文件**和**用户定义**菜单项。
- 选择**用户定义**。

  ↳ 此时将显示**文件扩展名**对话框，其中包含要用扫描配置文件扫描的所有文件类型的列表。

如果要将某个文件类型排除在扫描范围之外：

- 突出显示该文件类型并单击**删除**。

如果要将某个文件类型添加到扫描范围之内：

- 突出显示该文件类型。
- 单击**插入**并在输入框中输入该文件类型的文件扩展名。

  最多可使用 10 个字符，且不要以点 (.) 开头， 可使用通配符（* 和 ?）。

4.3.15 创建扫描配置文件的桌面快捷方式

使用指向扫描配置文件的桌面快捷方式，可直接从桌面启动系统扫描，而无需访问 Avira 产品的控制中心。

创建指向扫描配置文件的桌面快捷方式：

✓ 在控制中心，转到 *PC 防护* >**Scanner** 部分。

- 选择要创建快捷方式的扫描配置文件。
- 单击图标 。

  ↳ 即会创建桌面快捷方式。

4.3.16 过滤事件

由 Avira 产品的程序组件生成的事件将显示在控制中心中的*管理* > 事件下（与 Windows 操作系统的事件显示相似）。 程序组件按字母顺序排列如下：

- 帮助程序服务
- Mail Protection
- Real-Time Protection
- 计划程序
- Scanner
- 更新程序
- Web Protection

显示以下事件类型：

- *信息*
- *警告*
- *错误*
- *检测*

过滤显示的事件：

1. 在控制中心中，选择*管理* > 事件部分。
2. 选中与程序组件对应的复选框以显示已启用组件的事件。

   - 或者 -

   取消选中与程序组件对应的复选框以隐藏已停用组件的事件。
3. 选中与事件类型对应的复选框以显示这些事件。

   - 或者 -

   取消选中与事件类型对应的复选框以隐藏这些事件。

4.3.17 将电子邮件地址排除在扫描范围之外

为了定义从 Mail Protection 扫描中排除的电子邮件地址（发件人）的列表（白名单）：

- 转到控制中心并选择 *INTERNET 防护* > **Mail Protection** 部分。
  - ↳ 该列表显示传入电子邮件。
- 突出显示要排除在 Mail Protection 扫描范围之外的电子邮件。
- 单击图标，将电子邮件排除在 Mail Protection 扫描范围之外：
- 将不再针对所选电子邮件地址扫描病毒和恶意程序。
  - ↳ 所选电子邮件发件人地址将包括在排除列表中，以后不再针对该地址扫描病毒、恶意软件。

警告

只应将完全可信的发件人的电子邮件地址排除在 Mail Protection 扫描范围之外。

说明

在 Mail Protection > 常规 > 例外下的配置中，可将其他电子邮件地址添加到排除列表中，也可从排除列表中删除电子邮件地址。

5. Scanner

使用 Scanner 组件，可执行针对性扫描（按需扫描）以查找病毒和恶意程序。
可使用以下方法扫描受感染的文件：

- **通过上下文菜单执行系统扫描**
  例如，如果您希望扫描单独的文件和目录，则建议通过上下文菜单执行系统扫描（右键单击按钮 - **使用 Avira 扫描所选文件**项）。
  通过上下文菜单执行系统扫描的另一个优点是无需先启动控制中心。
- **通过拖放执行系统扫描**
  将一个文件或目录拖入
  控制中心的程序窗口时，Scanner将扫描该文件或目录及其包含的所有子目录。
  如果希望扫描已保存（例如，保存在桌面上）的单独的文件和目录，建议采用此过程。
- **通过配置文件执行系统扫描**
  如果希望定期扫描特定的目录和驱动器（例如工作目录或经常存储新文件的驱动器），建议采用此过程。
  这样，只要选择使用相关的配置文件就可进行新扫描，而无需再次选择这些目录和驱动器。
- **通过计划程序执行系统扫描**
  通过计划程序可以执行由时间控制的扫描。

在扫描 Rootkit 和引导扇区病毒以及扫描活动进程时，需要执行特殊的过程。
可用选项如下：

- 通过扫描配置文件扫描 Rootkits **扫描 Rootkits 和活动恶意软件**
- 通过扫描配置文件**活动进程**扫描活动进程
- 通过**附加程序**菜单中的**启动记录扫描...**菜单命令扫描引导扇区病毒

6. 更新

防病毒软件是否有效取决于程序（尤其是病毒定义文件和扫描引擎）是否及时得到更新。为执行定期更新，Avira 产品中集成了更新程序组件。 更新程序确保了 Avira 产品始终处于最新状态，并能够处理每天出现的新病毒。 更新程序将更新以下组件：

- 病毒定义文件：

  病毒定义文件包含有害程序的病毒模式，Avira 产品使用这些模式来扫描病毒和恶意软件并修复受感染的对象。

- 扫描引擎：

  扫描引擎包含 Avira 产品用来扫描病毒和恶意软件的方法。

- 程序文件（产品更新）：

  产品更新的更新软件包对各个程序组件提供了额外的功能。

更新将检查病毒定义文件、扫描引擎和产品是否最新，并在必要时执行更新。
在更新产品后，可能必须重新启动计算机系统。
如果仅更新病毒定义文件和扫描引擎，则不必重新启动计算机。

当产品更新需要重启计算机时，您可以决定继续更新或稍后再提醒您这些更新。
如果您立即继续产品更新，您仍可以选择何时重启计算机。

如果您希望稍后再提醒您进行更新，病毒定义文件和扫描引擎将会更新，但产品更新并未完成。

> 说明
> 计算机重启后才能完成产品更新。
>
> 说明
> 出于安全考虑，更新程序会检查计算机的 Windows 主机文件是否被更改，例如，更新 URL

是否受恶意软件操纵，是否将更新程序引向恶意软件下载站点。 如果 Windows 主机文件被操纵，更新程序报告文件会指出这一点。

以以下间隔时间自动执行更新：2 小时。

在计划程序下的控制中心中，可创建要由“更新程序”按指定间隔执行的其他更新作业。也可手动启动更新：

- 在控制中心中：在更新菜单和状态部分中
- 通过任务栏图标的上下文菜单启动

通过制造商的 Web 服务器可从 Internet 获得更新。 连接 Avira 的下载服务器时，将默认使用现有网络连接。 可以在配置 > 更新下的“配置”中更改此默认设置。

7. 常见问题解答、技巧

本章包含有关故障排除的重要信息以及有关您的 Avira 产品的其他使用技巧。

- 请参阅章节相关问题帮助
- 请参阅章节快捷键
- 请参阅章节Windows 安全中心（Windows XP 和 Vista）或 Windows 操作中心 (Windows 7 和 Windows 8)

7.1 相关问题帮助

在此可找到有关可能问题的原因和解决方案的信息。

- 显示错误消息“*The license file cannot be opened*”（*无法打开许可证文件*）。
- 尝试启动更新时显示错误消息“*Connection failed while downloading the file ...*”（下载文件期间连接失败……）。
- 无法移动或删除病毒和恶意软件。
- 任务栏图标的状态为已禁用。
- 在执行数据备份时计算机速度极慢。
- 防火墙在激活后立即报告 Avira Real-Time Protection 和 Avira Mail Protection 。
- Avira Mail Protection 不工作。
- Mail Protection 已阻止通过 TLS 连接发送的电子邮件。
- Webchat 未运行：将不显示聊天消息

显示错误消息“*The license file cannot be opened*”（*无法打开许可证文件*）。

原因：该文件已加密。

- 若要激活许可证，无需打开许可证文件，请将其保存到程序目录中。

尝试启动更新时显示错误消息“*Connection failed while downloading the file ...*”（下载文件期间连接失败……）。

原因：Internet 连接处于不活动状态，因此无法与 Internet 上的 Web 服务器建立连接。

- 测试其他 Internet 服务（如 WWW）或电子邮件是否能正常运行。
  如果不能，则重新建立 Internet 连接。

原因：无法访问代理服务器。

- 检查代理服务器的登录信息是否已发生更改，在必要时根据配置对其进行调整。

原因：*update.exe* 文件未得到个人防火墙的完全认可。

- 确保 *update.exe* 文件得到个人防火墙的完全认可。

如果不能解决问题：

- 在 PC 防护 > 更新下检查配置中的设置（专家模式）。

无法移动或删除病毒和恶意软件。

原因：文件已由窗口加载并处于活动状态。

- 更新您的 Avira 产品。
- 如果使用的是 Windows XP 操作系统，请禁用“系统还原”。
- 以安全模式启动计算机。
- 开始配置您的 Avira 产品（专家模式）。
- 选择 **Scanner > 扫描 > 文件 > 所有文件**，并单击 **确定**以确认窗口。
- 开始扫描所有本地驱动器。
- 以正常模式启动计算机。
- 以正常模式执行扫描。
- 如果未发现任何其他病毒或恶意软件，则启用“系统还原”（如果系统提供该功能并且您需要使用它）。

任务栏图标的状态为已禁用。

原因：Avira Real-Time Protection 已禁用。

- 在控制中心中单击**状态**并启用 *PC 防护*区域中的 **Real-Time Protection**。

- 或者 -

- 右键单击任务栏图标，打开上下文菜单。 单击**启用 Real-Time Protection**。

原因：防火墙已阻止 Avira Real-Time Protection。

- 在防火墙配置中定义对 AntiVir Real-Time Protection 的常规认可。 Avira Real-Time Protection 仅对地址 127.0.0.1 (localhost) 有效。 不建立 Internet 连接。这同样适用于 Avira Mail Protection。

如果不能解决问题：

- 查看 Avira Real-Time Protection 服务的启动类型。
  如果需要，请启动服务：在任务栏中，选择开**始 > 设置 > 控制面板**。
  通过双击启动**服务**配置面板（在 Windows XP
  中，服务小程序位于*管理工具*子目录中）。 查找 *Avira Real-Time Protection* 项。
  必须输入自动作为启动类型，并输入已启动作为状态。
  如果需要，请通过选择相关行和**启动**按钮，手动启动该服务。
  如果显示错误消息，请查看事件显示内容。

在执行数据备份时计算机速度极慢。

原因：在备份过程中，Avira Real-Time Protection
扫描了备份过程正在使用的所有文件。

- 在配置中选择 **Real-Time Protection > 扫描 > 例外**（专家模式），并输入备份软件的进程名称。

防火墙在激活后立即报告 Avira Real-Time Protection 和 Avira Mail Protection。

原因：通过 TCP/IP Internet 协议与 Avira Real-Time Protection 和 Avira Mail Protection 进行通信。 防火墙会监视通过此协议建立的所有连接。

- 定义对 Avira Real-Time Protection 和 Avira Mail Protection 的常规认可。 Avira Real-Time Protection 仅对地址 127.0.0.1 (localhost) 有效。 不建立 Internet 连接。 这同样适用于 Avira Mail Protection。

Avira Mail Protection 不工作。

如果 Avira Mail Protection 产生问题，请借助以下检查列表检查 Avira Mail Protection 是否正常运行。

检查列表

- 检查邮件客户端是否通过 Kerberos、APOP 或 RPA 登录到服务器。 当前不支持这些验证方法。
- 检查您的邮件客户端是否通过 SSL（通常也称为 TSL – 传输层安全）向服务器报告。 Avira Mail Protection 不支持 SSL，因此将会终止任何加密 SSL 连接。 如果您要使用加密 SSL 连接，而不想让 Mail Protection 保护这些连接，您可以使用不受 Mail Protection 监视的端口进行连接。 可以在 **Mail Protection > Scan** 中的配置中配置受 Mail Protection 监视的端口。
- Avira Mail Protection 服务是否处于活动状态？ 如果需要，请启动服务：在任务栏中，选择开始 > 设置 > 控制面板。 通过双击启动服务配置面板（在 Windows XP 中，服务小程序位于*管理工具*子目录中）。 查找 *Avira Mail Protection* 项。 必须输入自动作为启动类型，并输入已启动作为状态。 如果需要，请通过选择相关行和启动按钮，手动启动该服务。 如果显示错误消息，请查看事件显示内容。 如果上述操作不成功，可能必须通过开始 > 设置 > 控制面板 > 添加或删除程序完全卸载 Avira 产品，重新启动计算机，然后重新安装 Avira 产品。

常规

当前无法保护通过 SSL（安全套接字层，通常也称为 TLS（传输层安全））加密的 POP3 连接，因而将忽略此类连接。

当前仅支持通过密码验证连接到邮件服务器， 不支持“Kerberos”和“RPA”。

Avira 产品不会检查外发电子邮件中是否存在病毒和恶意程序。

> 说明
> 建议您定期安装 Microsoft 更新，以修复任何安全上的缺陷。

Mail Protection 已阻止通过 TLS 连接发送的电子邮件。

原因：传输层安全（TLS：在 Internet 上传输数据的加密协议）此时不受 Mail Protection 支持。 可以选择以下方法发送电子邮件：

- 使用端口 25（由 SMTP 使用）以外的端口。 这样将绕开 Mail Protection 的监视。
- 在电子邮件客户端中关闭 TLS 加密连接并禁用 TLS 支持。
- 在 **Mail Protection > Scan** 中的配置中禁用（暂时） Mail Protection 对外发电子邮件的监视。

Webchat 无法运行：未显示聊天消息；正在浏览器中加载数据。

如果聊天基于“transfer-encoding: chunked”的 HTTP 协议，则在聊天期间可能出现这种现象。

原因：在将数据加载到 Web 浏览器之前，Web Protection 会首先彻底检查发送的数据中是否存在病毒和恶意程序。 在以“transfer-encoding: chunked”方式传输数据时，Web Protection 无法确定消息长度或数据量。

- 请输入 Web 聊天的 URL 配置作为例外（请参阅“配置” ：**Web Protection > 扫描 > 例外**）。

7.2 快捷键

利用键盘命令（也称为快捷键）可以在程序中快速地导航、检索各模块以及启动各项操作。

下面概述了可用的键盘命令。 有关键盘命令功能的更多说明，请参阅帮助的相应章节。

7.2.1 在对话框中

快捷键	说明
Ctrl + Tab **Ctrl + Page down**	在控制中心中导航 转到下一部分。
Ctrl + Shift + Tab **Ctrl + Page up**	在控制中心中导航 转到上一部分。
←↑→↓	在配置部分中导航 首先，用鼠标将光标置于配置部分。 在已标记下拉列表中的选项之间或在选项组的多个选项之间进行切换。
Tab	切换到下一个选项或选项组。
Shift + Tab	切换到上一个选项或选项组。
空格键	如果活动选项是复选框，则启用或停用该复选框。

Alt + 带下划线的字母	选择选项或启动命令。
Alt + ↓ F4	打开所选下拉列表。
Esc	关闭所选下拉列表。 取消命令并关闭对话框。
Enter	启动活动选项或按钮的命令。

7.2.2 在帮助中

快捷键	说明
Alt + Space	显示系统菜单。
Alt + Tab	在帮助与其他打开的窗口之间切换。
Alt + F4	关闭帮助。
Shift + F10	显示帮助的上下文菜单。
Ctrl + Tab	转到导航窗口中的下一部分。
Ctrl + Shift + Tab	转到导航窗口中的上一部分。

Page up	在索引或搜索结果列表中切换到显示在内容上方的主题。
Page down	在索引或搜索结果列表中切换到显示在内容中的当前主题下方的主题。
Page up **Page down**	在主题中进行浏览。

7.2.3 在控制中心中

常规

快捷键	说明
F1	显示帮助
Alt + F4	关闭控制中心
F5	刷新
F8	打开配置
F9	开始更新

扫描部分

快捷键	说明
F2	重命名所选配置文件
F3	使用所选配置文件启动扫描

F4	为所选配置文件创建桌面链接
Ins	创建新配置文件
Del	删除所选配置文件

隔离区部分

快捷键	说明
F2	重新扫描对象
F3	还原对象
F4	发送对象
F6	将对象还原为...
Return	属性
Ins	添加文件

Del	删除对象

计划程序部分

快捷键	说明
F2	编辑作业
Return	属性
Ins	插入新作业
Del	删除作业

报告部分

快捷键	说明
F3	显示报告文件
F4	打印报告文件
Return	显示报告
Del	删除报告

事件部分

快捷键	说明
F3	导出事件
Return	显示事件
Del	删除事件

7.3 Windows 安全中心

- Windows XP Service Pack 2 至 Windows Vista -

7.3.1 常规

Windows 安全中心检查计算机的状态，以便了解重要的安全领域。

如果在某个重要方面检测到问题（例如，防病毒程序过期），安全中心就会发出一条警报，并给出有关如何更好地保护计算机的建议。

7.3.2 Windows 安全中心和 Avira 产品

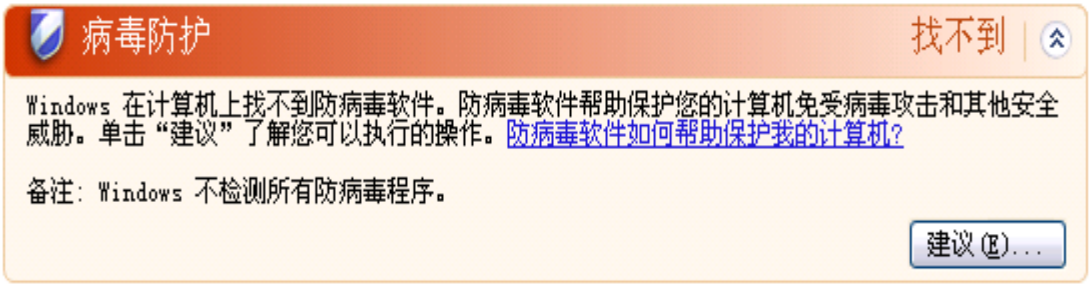
病毒防护软件/针对恶意软件提供保护

您可能会从 Windows 安全中心收到以下有关病毒防护的信息：

- 未找到病毒防护
- 病毒防护已过期
- 病毒防护已开启
- 病毒防护已关闭
- 病毒防护不受监视

未找到病毒防护

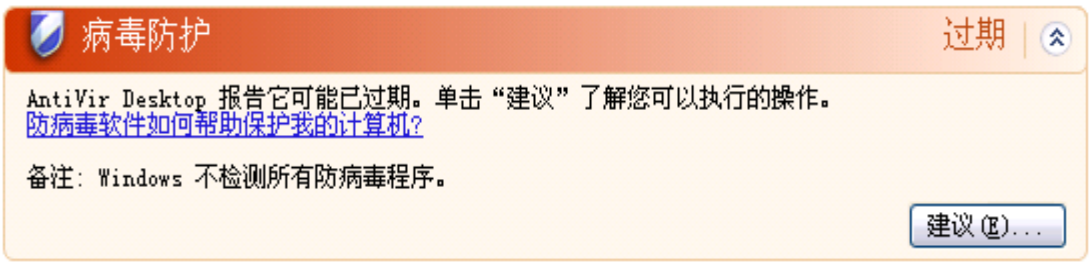
当 Windows 安全中心在您的计算机上未找到任何防病毒软件时，就会显示此 Windows 安全中心信息。



> 说明
>
> 在您的计算机上安装 Avira 产品即可针对病毒及其他恶意程序提供保护！

病毒防护已过期

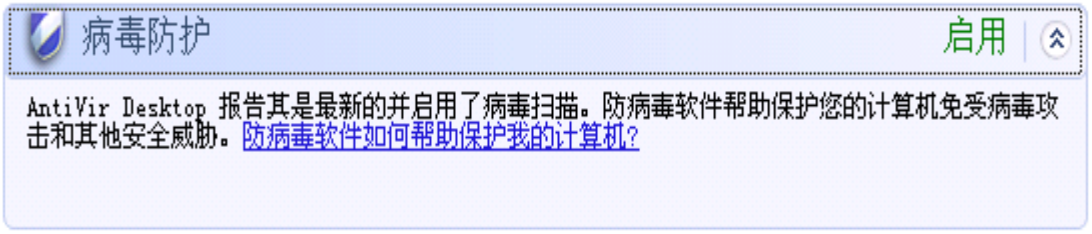
如果您已安装了 Windows XP Service Pack 2 或 Windows Vista，然后再安装 Avira 产品，或者在已安装有 Avira 产品 的系统上安装 Windows XP Service Pack 2 或 Windows Vista，则会收到以下消息：



> 说明
>
> 为了使 Windows 安全中心将您的 Avira 产品识别为最新产品，必须在安装后执行更新。 通过执行更新来更新系统。

病毒防护已开启

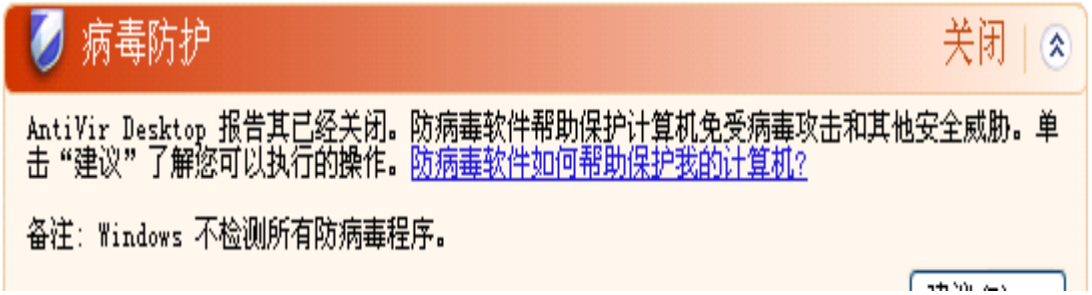
安装 Avira 产品并执行更新后，您会收到以下消息。



您的 Avira 产品现在处于最新状态且 Avira Real-Time Protection 已启用。

病毒防护已关闭

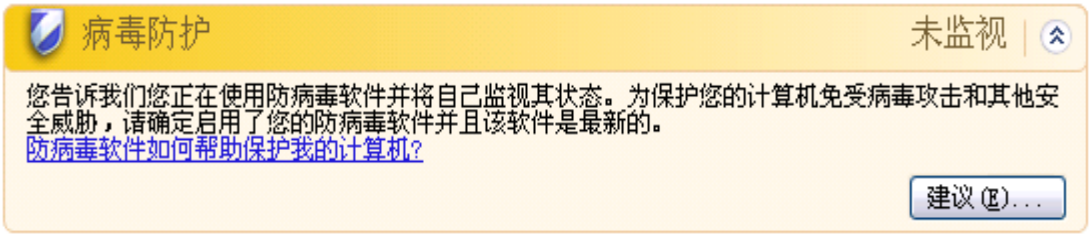
如果禁用 Avira Real-Time Protection 或停止 Real-Time Protection 服务，您将收到以下消息。



> 说明
>
> 您可以在控制中心的状态部分启用或禁用 Avira Real-Time Protection。您还可以看到，如果任务栏中的红伞张开，则表示 Avira Real-Time Protection 已启用。

病毒防护不受监视

如果从 Windows 安全中心收到以下消息，则表明您已决定要自己监视防病毒软件。



说明

Windows Vista 不支持此功能。

说明

您的 Avira 产品支持 Windows 安全中心。

可以随时通过建议按钮启用此选项。

说明

即使已安装了 Windows XP Service Pack 2 或 Windows Vista，您仍需要病毒防护解决方案。 尽管 Windows 会监视防病毒软件，它本身不包含任何防病毒功能。

因此，如果没有其他防病毒解决方案，就无法针对病毒和其他恶意软件提供保护！

7.4 Windows 操作中心

- Windows 7 和 Windows 8 -

7.4.1 常规

说明

从 Windows 7 开始，**Windows 安全中心更名为 Windows 操作中心。**

在这一部分中，您将找到所有安全选项的状态。

Windows 操作中心检查计算机的状态，以便了解重要的安全领域。
单击任务栏中的小旗或**控制面板 > 操作中心**即可直接访问操作中心。

如果在某个重要方面检测到问题（例如，防病毒程序过期），操作中心就会发出一条警报，并给出有关如何更好地保护计算机的建议。
这意味着，如果一切运行正常，您不会收到任何消息。 您仍然可以在 **Windows 操作中心**的**安全**项中查看计算机的安全状态。
Windows 操作中心还提供已安装程序管理选项供您选择（例如，*查看已安装的反间谍软件程序*）。

您甚至可以在**更改操作中心设置**中关闭警报消息（例如，*关闭有关间谍软件和相关防护的消息*）。

7.4.2 Windows 操作中心和 Avira 产品

病毒防护

您可能会从 Windows 操作中心收到以下有关病毒防护的信息：

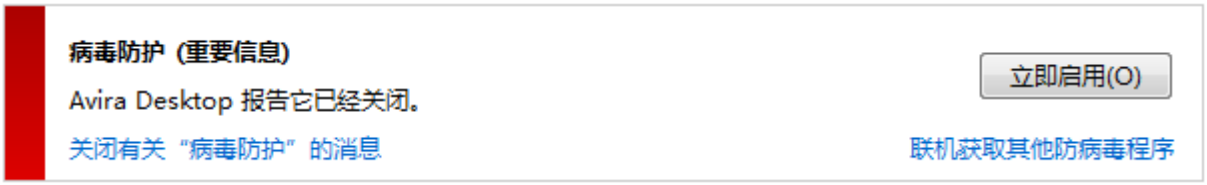
- Avira Desktop 报告它已处于最新状态且病毒扫描已开启。
- Avira Desktop 报告它已关闭。
- Avira Desktop 报告它已过期。
- Windows 在这台计算机上未找到防病毒软件。
- Avira Desktop 已过期。

Avira Desktop 报告它已处于最新状态且病毒扫描已开启

安装 Avira 产品并更新后，您不会从 Windows 操作中心收到任何消息。
但是如果您转到**操作中心 > 安全**，您可以看到：*Avira Desktop 报告它已处于最新状态且病毒扫描已开启。* 这意味着您的 Avira 产品现在处于最新状态且 Avira Real-Time Protection 已启用。

Avira Desktop 报告它已关闭。

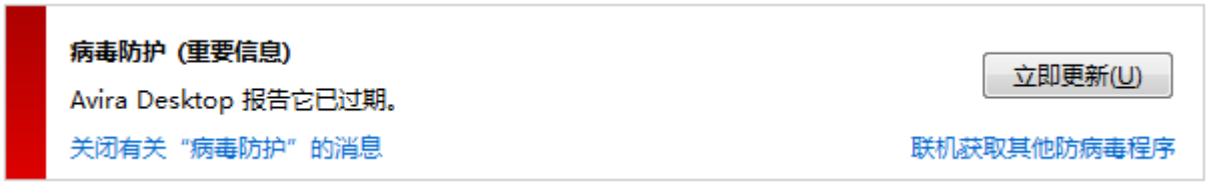
如果禁用 Avira Real-Time Protection 或停止 Real-Time Protection 服务，您将收到以下消息。



> 说明
>
> 您可以在 **Avira 控制中心**的状态部分启用或禁用 Avira Real-Time Protection。 您还可以看到，如果任务栏中的红伞张开，则表示 Avira Real-Time Protection 已启用。 单击 Windows 操作中心消息上的*立即打开*按钮，也可以启用 Avira 产品。
>
> 您将收到一条通知，该通知会询问您是否允许运行 Avira。
>
> 单击*是，我信任发布者并且想要运行此程序*，Real-Time Protection 将再次启用。

Avira Desktop 报告它已过期

如果您刚安装了 Avira 或由于某种原因，您的 Avira 产品的病毒定义文件、扫描引擎或程序文件未完成自动更新（比如，如果您对原本已安装了 Avira 产品的旧版 Windows 操作系统进行了升级），您将收到以下信息：



> 说明
>
> 为了使 Windows 操作中心将您的 Avira

产品识别为最新产品，必须在安装后执行更新。 通过执行更新来更新 Avira 产品。

Windows 在这台计算机上未找到防病毒软件

当 Windows 操作中心在您的计算机上未找到任何防病毒软件时，就会显示此 Windows 操作中心信息。

说明

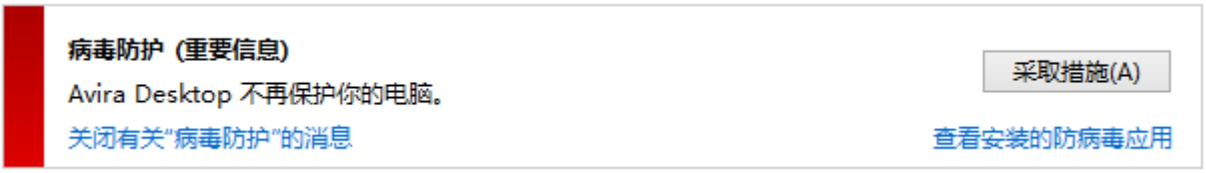
请注意该选项在 Windows 8 中不会出现，因为 Windows Defender 现在已预置了病毒防护功能。

说明

在您的计算机上安装 Avira 产品即可针对病毒及其他恶意程序提供保护！

Avira Desktop 已过期

当您的 Avira 产品许可证已过期时，就会显示此 Windows 操作中心信息。
如果您点击按钮继续订购，您将被重新定向至 Avira 网站，您可以由此购买一个新的许可证。



说明

请注意此选项仅适用于 Windows 8。

间谍软件和恶意软件防护

您可能会从 Windows 操作中心收到以下有关间谍软件防护的信息：

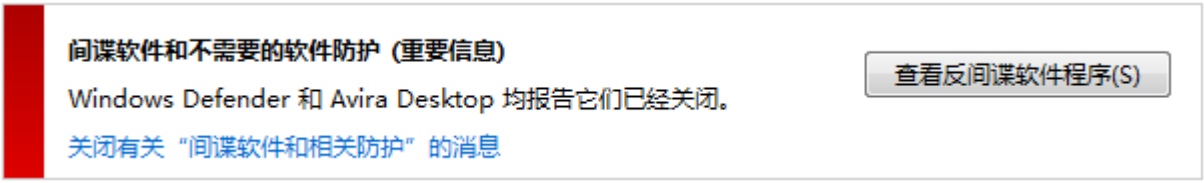
- Avira Desktop 报告它已开启。
- Windows Defender 和 Avira Desktop 都报告它们已关闭。
- Avira Desktop 报告它已过期。
- Windows Defender 已过期。
- Windows Defender 已关闭。

Avira Desktop 报告它已开启

安装 Avira 产品并更新后，您不会从 Windows 操作中心收到任何消息。
但是如果您转到**操作中心 > 安全**，您可以看到：*Avira Desktop 报告它已开启。*
这意味着您的 Avira 产品现在处于最新状态且 Avira Real-Time Protection 已启用。

Windows Defender 和 Avira Desktop 都报告它们已关闭

如果禁用 Avira Real-Time Protection 或停止 Real-Time Protection 服务，您将收到以下消息。

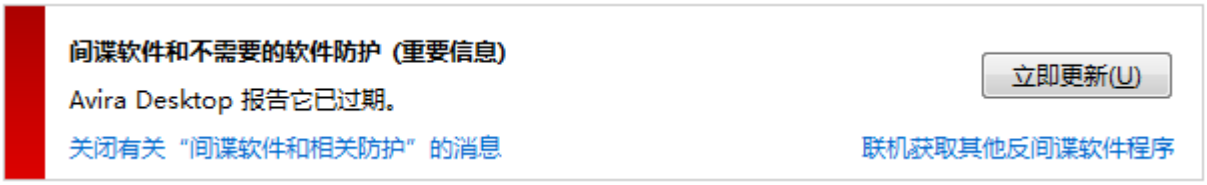


说明
您可以在 **Avira 控制中心**的**状态**部分启用或禁用 Avira Real-Time Protection。 您还可以看到，如果任务栏中的红伞张开，则表示 Avira Real-Time Protection 已启用。 单击 Windows 操作中心消息上的*立即打开*按钮，也可以启用 Avira 产品。
您将收到一条通知，该通知会询问您是否允许运行 Avira。

单击*是，我信任发布者并且想要运行此程序*，Real-Time Protection 将再次启用。

Avira Desktop 报告它已过期

如果您刚安装了 Avira 或由于某种原因，您的 Avira 产品的病毒定义文件、扫描引擎或程序文件未完成自动更新（比如，如果您对原本已安装了 Avira 产品的旧版 Windows 操作系统进行了升级），您将收到以下信息：

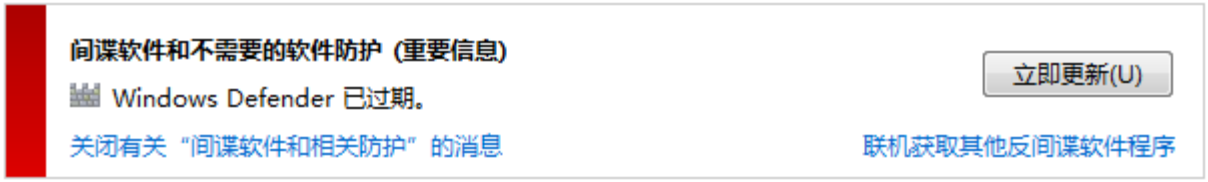


说明

为了使 Windows 操作中心将您的 Avira 产品识别为最新产品，必须在安装后执行更新。通过执行更新来更新 Avira 产品。

Windows Defender 已过期

如果 Windows Defender 已启用，您可能会收到以下消息。如果您已安装 Avira 产品，则不应出现此消息。请检查安装是否正确。



说明

Windows Defender 是来自 Windows 的预置防间谍和病毒软件解决方案。

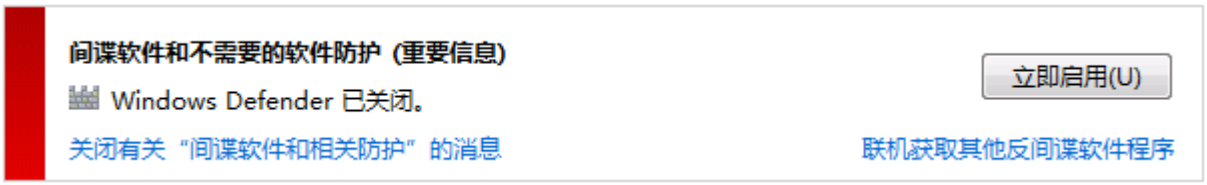
Windows Defender 已关闭

当 Windows 操作中心在您的计算机上未找到除操作系统默认集成的防病毒软件 (Windows Defender) 以外的任何其他防病毒软件时，就会显示此 Windows 操作中心信息。

如果您在此之前已在计算机上安装了某款防病毒软件，则此应用程序被禁用。

如果您已安装 Avira 产品，则不应出现此消息：应自动检测到 Avira。

请检查安装是否正确。



8. 病毒及其他

Avira Antivirus Premium 不仅可以检测病毒和恶意软件，还可以防御其他威胁。
在本部分中，您可以找到对各种恶意软件及其他威胁的概述，其中描述了它们的背景、行为以及它们准备给您造成的不愉快的意外。

相关主题：

- 威胁类别
- 病毒及其他恶意软件

8.1 威胁类别

广告软件

广告软件是一种通过弹出窗口或通过显示在计算机屏幕上的栏显示横幅广告的软件。
这些广告通常无法移除，因此始终可见。
通过连接数据，可分析用户的使用行为，从数据安全考虑，这是很有问题的。

Avira 产品能够检测到广告软件。
如果在威胁类别下的配置中选中**广告软件**选项，从而启用该选项，则 Avira 产品检测到广告软件时，会发出相应的警报。

广告软件/间谍软件

这种软件通常未获得用户确认或同意就显示广告，或是向第三方发送用户个人数据，因此属于恶意软件。

Avira 产品能够识别出“广告软件/间谍软件”。
如果在威胁类别下的配置中选中**广告软件/间谍软件**选项，从而启用该选项，则 Avira 产品检测到广告软件或间谍软件时，会发出相应的警报。

应用程序

术语 APPL（即 application），指的是使用时存在风险或来源可疑的应用程序。

Avira 产品能够识别出“应用程序 (APPL)”。
如果在威胁类别下的配置中选中**应用程序**选项，从而启用该选项，则 Avira 产品检测到此类行为时，会发出相应的警报。

后门客户端

为了窃取数据或操纵计算机，后门服务器程序会在用户毫无察觉的情况下潜入计算机。这种程序可由第三方使用后门控制软件（客户端）通过 Internet 或网络进行控制。

Avira 产品能够识别出“后门控制软件”。
如果在威胁类别下的配置中选中**后门控制软件**选项，从而启用该选项，则 Avira 产品检测到此类软件时，会发出相应的警报。

拨号器

Internet 上提供的某些服务是要付费的。 在德国，通过拨号器拨打 0190/0900（在奥地利和瑞士拨打 09x0；在德国，该号码在中期内设置更改为 09x0）是要付费的。
在计算机上安装后这些程序后，它们通过拨打相应的付费号码（其收费标准可能差异很大）来建立稳定的连接。

在电话费帐单中计入上网费用是合法的，对于用户而言，也是有利的。
不容置疑，真正的拨号器是用户有意使用的。
这样的拨号器只有征得用户同意后才安装在用户计算机上，而用户一定是以清楚无误的可见说明或请求表示同意的。 真正的拨号器的拨号过程清晰可见。
此外，真正的拨号器还会准确无误地计费。

很遗憾，还有一些拨号器在用户无法察觉的情况下安装在计算机上，来源可疑，甚至具有欺骗性。 例如，它们将 Internet 用户的默认数据通信链接替换为指向 ISP（Internet 服务提供商），只要建立连接，它们就会拨打收费（通常很贵）的 0190/0900 号码。

在下次收到电话帐单之前，受感染的用户可能不会注意到，在他的计算机上，0190/0900 恶意拨号器在每次连接时都拨打价格极高的号码，导致电话费用剧增。

建议您直接要求电话提供商阻止这些号码段，以立即防范恶意拨号器（0190/0900 拨号器）。

默认情况下，Avira 产品可以检测类似的拨号器。

如果在扩展威胁类别下的配置中选中**拨号器**选项，从而启用该选项，则在检测到拨号器时，您会收到相应的警报。 这样，您可以删除恶意 0190/0900 拨号器。
如果它并非恶意拨号器，可将它声明为例外文件，以便将来不再扫描该文件。

双扩展名文件

有些可执行文件以可疑的方式隐藏其真正的文件扩展名。
恶意软件通常采用这种伪装方法。

Avira 产品能够识别出“双扩展名文件”。
如果在威胁类别下的配置中选中**双扩展名文件**选项，从而启用该选项，则 Avira 产品检测到此类文件时，会发出相应的警报。

欺诈性软件

欺诈性软件也被称为“假杀毒软件”或“流氓软件”，它会佯称计算机受到病毒或恶意软件的感染。
这种软件看起来与专业防病毒软件十分相似，但它的真实意图是增加不可靠性或恐吓用户。
其目的是使受害者感觉受到即将发生的（不真实）危险的威胁并使他们为了消除威胁而付费。
有时还会误导受害者认为自己受到攻击，并指示他们执行某种操作，而实际上这种操作才是真正的攻击。

Avira 产品能够检测到假杀毒软件。
如果在威胁类别下的配置中选中**欺诈性软件**选项，从而启用该选项，则 Avira 产品检测到此类文件时，会发出相应的警报。

游戏

玩计算机游戏自有合适的地方，但不是在工作场所（也许午餐时间除外）。
然而，Internet
中存在众多可下载的游戏，很多公司员工和公职人员都会玩扫雷和纸牌游戏。 从 Internet 上可以下载大量的游戏。
电子邮件游戏也变得更受欢迎：网络上传播着各种各样的电子邮件游戏，从简单的棋类游戏到“舰队演习”（包括鱼雷对战）：通过电子邮件程序将相应的移动发送给对手，对手再回复邮件。

研究表明，从经济的角度看，花费在计算机游戏上的工作时间已达到了很高的比例。
因此，越来越多的公司自然会考虑如何禁止在工作场所玩计算机游戏。

Avira 产品能够识别出计算机游戏。
如果在威胁类别下的配置中选中游戏选项，从而启用该选项，则 Avira
产品检测到游戏时，会发出相应的警报。 现在，您可以直接删除它，游戏真正地结束了。

玩笑程序

玩笑程序只是为了吓人或提供点普通娱乐，不会造成危害，也不会复制。
加载玩笑程序后，计算机通常会在某一时刻突然播放出一段旋律或在屏幕上显示一些不寻常的东西。 举例来说，磁盘驱动器中的清洗机 (DRAIN.COM) 或屏幕吞噬程序 (BUGSRES.COM) 就是玩笑程序。

但是请注意： 所有玩笑程序症状也可能是源自病毒或特洛伊木马。
至少，用户会大吃一惊，或认为自己真的造成了损坏，从而陷入恐慌。

扩展包含扫描和识别例程，Avira
产品能够检测到玩笑程序，必要时可将这些程序作为恶意程序予以删除。
如果在威胁类别下的配置中选中玩笑程序选项，从而启用该选项，则检测到玩笑程序时，会发出相应的警报。

钓鱼

钓鱼（也称为品牌仿冒），是一种狡猾的数据窃取形式，其目标是 Internet 服务提供商、银行、网上银行服务和登记部门的客户或潜在客户。
当您在 Internet 上提交电子邮件地址、填写在线表单、访问新闻组或网站时，您的数据可能会被“Internet 网络蜘蛛”窃取，然后在未经您允许的情况下将其用于行骗或其他犯罪活动。

Avira 产品能够识别出“网络钓鱼”。
如果在威胁类别下的配置中选中**网络钓鱼**选项，从而启用该选项，则检测到此类行为时，会发出相应的警报。

侵犯私人领域的程序

有些软件可能会危害系统安全、启动恶意程序活动、损害隐私或窥探用户行为，因而属于恶意软件。

Avira 产品能够检测到存在“安全隐私风险”的软件。
如果在威胁类别下的配置中选中**侵犯私人领域的程序**选项，从而启用该选项，则 Avira 产品检测到此类软件时，会发出相应的警报。

非常规运行时压缩程序

使用非常规运行时压缩程序压缩的文件，以及据此分类为可疑文件的文件。

Avira 产品能够识别出“非常规运行时压缩程序”。
如果在威胁类别下的配置中选中**非常规运行时压缩程序**选项，从而启用该选项，则 Avira 产品检测到此类压缩程序时，会发出相应的警报。

8.2 病毒及其他恶意软件

广告软件

广告软件是一种通过弹出窗口或通过显示在计算机屏幕上的栏显示横幅广告的软件。
这些广告通常无法移除，因此始终可见。
通过连接数据，可分析用户的使用行为，从数据安全考虑，这是很有问题的。

后门程序

后门程序可以绕过计算机访问安全机制而获取对计算机的访问权限。

正在后台运行的程序通常可赋予攻击者无限的权限。
在后门程序的帮助下，攻击者可窃取用户的个人数据。
但后门程序主要用来在相关系统上安装更多的计算机病毒或者蠕虫。

引导区病毒

硬盘的引导区或主引导扇区主要感染引导区病毒。 它们覆盖系统运行所需的重要信息。
可能导致烦人的结果：计算机系统无法加载...

僵尸网络

僵尸网络的定义是（Internet 上）由相互通信的僵尸计算机组成的远程 PC 网络。
僵尸网络可能包含一系列在通用命令和控制结构下正在运行程序（通常是指蠕虫、特洛伊木马之类的程序）的被入侵的计算机。
僵尸网络的用途很多，包括“拒绝服务”攻击等，受感染 PC
的用户对它的存在常常不知情。
可能成为僵尸网络的主要是可连接成千上万计算机的网络，在这种网络中，总带宽将迅速超过大部分常规 Internet 访问带宽。

漏洞攻击

漏洞（安全漏洞）是一种计算机程序或脚本，它利用
Bug、缺陷或弱点在计算机系统中提升权限或拒绝服务。 例如，一种攻击形式是在
Internet 上利用伪造的数据包进行的攻击。 攻击者可侵入程序从而提升权限。

欺诈性软件

欺诈性软件也被称为“假杀毒软件”或“流氓软件”，它会佯称计算机受到病毒或恶意软件的感染。
这种软件看起来与专业防病毒软件十分相似，但它的真实意图是增加不可靠性或恐吓用户。
其目的是使受害者感觉受到即将发生的（不真实）危险的威胁并使他们为了消除威胁而付费。
有时还会误导受害者认为自己受到攻击，并指示他们执行某种操作，而实际上这种操作才是真正的攻击。

恶作剧程序

多年来，Internet 和其他网络的用户都收到过有关病毒传播的电子邮件警报。
这些警报通过电子邮件传播，要求用户必须将其发送给尽可能多的同事或其他用户，以便警告每个人应对“危险”。

蜜罐

蜜罐是安装在网络中的服务（程序或者服务器）。 其功能是监视网络攻击和日志攻击。
对合法的用户来说，这种服务是未知的，因此用户并不了解。
如果攻击者检查网络中的薄弱环节并使用蜜罐提供的服务，就会进行记录并发出警报。

宏病毒

宏病毒是一些用应用程序（如 WinWord 6.0 中的
WordBasic）的宏语言编写的小程序，一般情况下只会随着这个应用程序的文档传播。
正因如此，它们也被称作文档病毒。

为了处于活动状态，它们需要激活相应的应用程序并且执行其中一个被感染的宏。
与“普通”的病毒不同，宏病毒并不攻击可执行文件，但是会攻击相应宿主应用程序的文档。

网址嫁接

网址嫁接就是操纵 Web 浏览器的主机文件，将查询地址转向具有欺骗性的网站。
这种方式比传统的钓鱼更进一步。
使用网址嫁接技术的欺诈者运行自己的服务器机房，在那里，存储着假网站。
网址嫁接是各种类型的 DNS 攻击的一个概括性术语。
在操纵主机文件时，将借助特洛伊木马或病毒对系统进行特定的操纵。
这样，即使输入正确的网址，系统也只能访问假网站。

钓鱼

钓鱼的意思是钓取 Internet 用户的个人详细信息。
钓鱼者通常向受害人发送看起来很正式的信件（如电子邮件），意在引诱他们向自己透露机密信息，特别是网上银行帐户的用户名和密码或 PIN 和 TAN。
使用窃取的详细访问信息，钓鱼者冒充受害人的身份，用其名义进行交易。
有一点很清楚：银行和保险公司绝不会通过电子邮件、短信或电话询问信用卡号、PIN、TAN 或其他详细访问信息。

变形病毒

多态病毒是真正的伪装高手。 它们可以改变自己的编程代码，因此很难检测。

程序病毒

计算机病毒是一种在运行后能够将其自身附加到其他程序上并引起感染的程序。
病毒不像逻辑炸弹和特洛伊木马，病毒进行自我繁殖。
和蠕虫相比，病毒始终需要一个程序作为宿主，以在其中寄存恶性代码。
一般来说，宿主自身的程序运行不会改变。

Rootkits

Rootkit
是一组在计算机系统被侵入后安装的软件工具，用于隐藏侵入者登录信息、隐藏进程和记录数据，总而言之，使自己隐身。
它们会尝试更新已安装的间谍程序，重新安装被删除的间谍软件。

脚本病毒和蠕虫

这类病毒极易编写，可以扩散，只要采用适当的方法，几小时之内就可以通过电子邮件扩散到全世界。

脚本病毒和蠕虫使用 Javascript 和 VBScript
等脚本语言编写，将自身嵌入其他新脚本中，或者通过调用操作系统功能进行扩散。
它们经常经由电子邮件和文件（文档）交换扩散。

蠕虫是一种自我繁殖但并不感染宿主的程序。
因此蠕虫不会构成其他程序序列的组成部分。
通常，在采用严格安全措施的系统上，蠕虫是唯一可能侵入任何类型的破坏性程序的。

间谍软件

间谍软件之所以称为间谍程序，是因为它在用户不知情的情况下拦截或者部分控制一台计算机的操作。 间谍软件利用受感染计算机获取商业利益。

特洛伊木马（简称木马）

现在木马很常见。
木马包括那些貌似具有特定功能，但在运行后却露出本来面目的程序（在多数情况下，它们执行的是破坏性的功能）。 特洛伊木马无法复制自身，这与病毒和蠕虫不同。
大多数木马都有个让人感兴趣的名称（例如 SEX.EXE 或
STARTME.EXE），目的在于引诱用户启动木马。

执行后，特洛伊木马就会激活，然后执行破坏性操作，例如格式化硬盘。 Dropper 是一种特殊形式的特洛伊木马，它“投放”病毒，也就是说，它将病毒嵌入计算机系统中。

僵尸病毒

僵尸计算机是指被恶意程序感染、并且能够让黑客通过远程控制为犯罪目的而滥用的计算机。 受感染的 PC 按照命令启动“拒绝服务 (DoS)”攻击，例如发送垃圾邮件和钓鱼电子邮件。

9. 信息与服务

本章包含有关如何联系我们的信息。

- 请参阅章节联系地址
- 请参阅章节技术支持
- 请参阅章节可疑文件
- 请参阅章节误报
- 请参阅章节提供反馈以提高安全性

9.1 联系地址

如果您对于 Avira 产品范围有任何疑问或要求，我们很乐意提供帮助。 请参阅**帮助 > 关于 Avira Antivirus Premium** 下的控制中心，获得我们的联系地址。

9.2 技术支持

Avira 技术支持负责解答您的问题或解决技术问题，为您提供可靠的帮助。

我们提供全面的技术支持服务，所有必需的相关信息都可在我们的网站上找到：

http://www.avira.cn/premium-support

因此我们可以为您提供快速可靠的帮助，您应准备好以下信息：

- **许可证信息。** 您可以在**帮助 > 关于 Avira Antivirus Premium > 许可证信息**菜单项下的程序界面中找到此信息。 请参阅许可证信息。
- **版本信息。** 您可以在**帮助 > 关于 Avira Antivirus Premium > 版本信息**菜单项下的程序界面中找到此信息。 请参阅版本信息。
- 已安装的**操作系统版本**和所有 Service Pack。
- **已安装的软件包**，例如其他供应商的防病毒软件。

- 程序或报告文件中的准确消息。

9.3 可疑文件

我们的产品未检测到或删除的病毒或可疑文件都可发送给我们。 您可采用多种方式发送。

- 在 Avira Server Security Console
  的控制中心的隔离区管理器中标识文件，然后通过上下文菜单或相应按钮选择发送文件
  。
- 将电子邮件附件中所需的压缩文件（WinZIP、PKZip、Arj 等）发送至以下地址：
  virus-premium@avira.cn
  由于部分电子邮件网关使用了防病毒软件，您还应该对文件进行加密（别忘了将密码告诉我们）。
- 您还可以通过我们的网站将可疑文件发送给我们：http://www.avira.cn/sample-upload

9.4 误报

如果您认为 Avira
产品报告的某个有问题的文件很可能是“干净”的，则将相关压缩文件（WinZIP、PKZip、Arj）作为电子邮件附件发送到以下地址：

virus-premium@avira.cn

由于部分电子邮件网关使用了防病毒软件，您还应该对文件进行加密（别忘了将密码告诉我们）。

9.5 提供反馈以提高安全性

在 Avira，客户的安全性是头等大事。
因此，我们不仅有内部专家团队负责在发布产品之前测试每个 Avira
解决方案的质量和安全性。
我们还非常重视与可能出现产生的安全漏洞有关的迹象，并会认真对待。

如果您认为在我们的产品中发现了安全漏洞，请向我们发送电子邮件，地址如下：

vulnerabilities-premium@avira.cn

10. 参考：配置选项

配置参考介绍所有可用配置选项。

10.1 Scanner

配置的 **Scanner** 部分用于配置按需扫描 （仅在专家模式中提供选项。）

10.1.1 扫描

可以定义按需扫描例程的行为（仅在专家模式中可用的选项）。
如果选择某些目录进行扫描，则根据配置，Scanner 在扫描时可能会：

- 采用某种扫描优先级，
- 也扫描启动扇区和主内存，
- 扫描目录中的全部或所选文件。

文件

Scanner 可以使用过滤器，以便只扫描具有某一扩展名（类型）的文件。

所有文件

如果启用此选项，则针对所有文件扫描病毒或恶意程序（无论文件内容及文件扩展名如何）。 不使用文件过滤器。

> 说明
> 如果启用了**所有文件**，则无法选择**文件扩展名**按钮。

使用智能扩展

如果启用此选项，则程序会自动选择进行病毒或恶意程序扫描的文件。 这意味着 Avira 程序将根据文件内容决定是否扫描文件。

此过程比使用文件扩展名列表略慢，但更安全，原因是它不仅仅根据文件扩展名进行扫描。 此选项默认设置为启用，这是推荐设置。

> 说明
> 如果启用了**使用智能扩展**，则无法选择**文件扩展名**按钮。

使用文件扩展名列表

如果启用此选项，则只扫描具有指定扩展名的文件。
所有可能包含病毒和恶意程序的文件类型都已预设。
此列表可以通过按钮“**文件扩展名**”手动进行编辑。

> 说明
> 如果启用此选项并且从文件扩展名列表删除了所有的项，则按钮**文件扩展名**下会显示提示文本“*没有文件扩展名*”。

文件扩展名

通过此按钮可以打开一个对话框，其中显示在“**使用文件扩展名列表**”模式下扫描的所有文件扩展名。 系统设置了默认扩展名项，但您可以添加或删除这些项。

> 说明
> 请注意，不同版本软件的默认列表可能不同。

其他设置

扫描所选驱动器的启动扇区

如果启用此选项，则 Scanner 只扫描被选择进行系统扫描的驱动器的启动扇区。
此选项默认设置为启用。

扫描主启动扇区

如果启用此选项，则 Scanner 扫描系统中所用硬盘的主启动扇区。

忽略脱机文件

如果启用此选项，则在扫描过程中直接扫描会完全忽略所谓的脱机文件。
这意味着不会对这些文件进行病毒和恶意程序扫描。
脱机文件是被所谓的分级存储管理系统 (HSMS)
以物理方式移动的文件，例如，从硬盘移到磁带。 此选项默认设置为启用。

系统文件完整性检查

如果启用此选项，则在每次按需扫描过程中都会对最重要的 Windows
系统文件进行特殊的安全检查，看是否被恶意软件修改过。
如果检测到修改的文件，则会将其报告为可疑。 此功能会使用大量计算机容量。
这就是此选项默认设置为禁用的原因。

> 说明
> 此选项仅适用于 Windows Vista 和更高版本。

> 说明
> 如果您使用会根据您自己的需要来修改系统文件并调整引导或启动屏幕的第三方工具，则不应使用此选项。 这类工具的示例包括：Skinpacks、TuneUp 实用工具或 Vista Customization。

优化的扫描

如果启用此选项，则在 Scanner 扫描过程中会对处理器容量进行优化使用。
出于性能考虑，仅在标准级别记录优化扫描。

> 说明
> 此选项仅适用于多处理器系统。

跟踪符号链接

如果启用此选项，则 Scanner 进行的扫描会跟踪扫描配置文件或所选目录中的所有符号链接，并对这些链接的文件进行病毒和恶意软件扫描。

> 说明
> 此选项不包含任何快捷方式，而专指符号链接（由 mklink.exe 生成）或连接点（由 junction.exe 生成），这些在文件系统上是透明操作。

扫描前搜索 Rootkit

如果启用此选项并启动扫描，则 Scanner 会扫描 Windows 系统目录，看所谓的快捷方式中是否存在 Rootkit。
此进程不会对计算机进行像扫描配置文件“扫描 Rootkit”那样复杂的扫描以寻找活动的 Rootkit，但执行速度大大加快。
该选项仅更改所创建配置文件的设置。

> 说明
> Rootkits 扫描不能在 Windows XP 64 位

扫描注册表

如果启用此选项，则对注册表进行恶意软件引用扫描。
该选项仅更改所创建配置文件的设置。

忽略网络驱动器上的文件和路径

如果启用此选项，则按需扫描会排除与计算机连接的网络驱动器。
如果服务器或其他工作站本身受防病毒软件保护，则建议使用此选项。
此选项默认设置为禁用。

扫描进程

允许停止扫描程序

如果启用此选项，则可以随时使用“Luke Filewalker”窗口中的“停止”按钮终止病毒或恶意程序扫描。
如果禁用此设置，则“Luke Filewalker”窗口中的停止按钮显示灰色背景。
因此无法中途停止扫描进程！ 此选项默认设置为启用。

扫描程序优先级

对于按需扫描，Scanner 可以区分优先级。
只有当几个进程同时在工作站上运行时，此设置才有效。 此选择会影响扫描速度。

低

只有在没有其他进程需要计算时间的情况下，操作系统才会给 Scanner 分配处理器时间，即只要 Scanner 在运行，速度就是最大的。
总之，最好与其他程序一起工作：如果其他程序需要计算时间，则在 Scanner 继续在后台运行的情况下，计算机的反应速度更快。

正常

Scanner 以普通优先级执行。 操作系统给所有进程分配的处理器时间相同。
此选项默认设置为启用，这是推荐设置。
在某些情况下可能会影响其他应用程序的工作。

高

Scanner 具有最高的优先级。 与其他应用程序同时工作几乎是不可能的。 但 Scanner 会以最大速度完成其扫描。

针对检测的操作

可以定义“系统扫描程序”在检测到病毒或恶意程序时所进行的操作。
（仅在专家模式中提供选项。）

交互式

如果启用此选项，则 Scanner 扫描的结果显示在对话框中。 如果使用 Scanner 进行扫描，则完成扫描后您会收到一个警报，列出受感染的文件。

可以使用上下文菜单选择要对各种受感染文件执行的操作。
可以对所有受感染文件执行标准操作，也可以取消 Scanner。

> 说明
> 在 Scanner 通知中，默认已预先选择了**隔离区**操作。
> 可以通过上下文菜单选择更多操作。

自动

如果启用此选项，则在检测到病毒时不显示对话框。 Scanner 会根据此部分中预定义为主操作和辅助操作的设置作出反应。

执行操作前将文件复制到隔离区

如果启用此选项，则“系统扫描程序”会在执行请求的主操作或辅助操作之前创建一个备份副本。 此备份副本保存在隔离区中，如果文件具有参考价值，可以从隔离区还原。您还可以将备份副本发送给 Avira 恶意软件研究中心以进一步调查。

主操作

主操作是 Scanner 发现病毒或恶意程序时所执行的操作。
如果选择了“**修复**”选项却无法修复受感染文件，则执行在“**辅助操作**”下选择的操作。

> 说明
> 只有在选择了**主操作**下的**修复**设置时，才能选择**辅助操作**选项。

修复

如果启用此选项，则 Scanner 会自动修复受感染的文件。 如果 Scanner 无法修复受感染的文件，则会执行辅助操作下选择的操作。

> 说明
> 建议进行自动修复，但这意味着让 Scanner 修改工作站上的文件。

重命名

如果启用此选项，则 Scanner 会重命名文件。
因此不能再直接访问这些文件（例如，通过双击访问）。
可在以后修复文件并重新指定其原始名称。

Quarantine

如果启用此选项，则 Scanner 会将文件移到隔离区。
以后可以修复这些文件，或根据需要将文件发送给 Avira 恶意软件研究中心。

删除

如果启用此选项，则会删除文件。 此过程要比“覆盖并删除”快得多。

忽略

如果启用此选项，则允许访问文件并按原样保留文件。

警告
工作站上的受感染文件仍处于活动状态！ 它可能会对您的工作站造成严重危害！

覆盖并删除

如果启用此选项，则 Scanner 将使用默认模式覆盖文件，然后将其删除。
文件将无法还原。

辅助操作

只有在选择了“**主操作**”下的**修复**设置时，才能选择“**辅助操作**”选项。
通过此选项，现在可以决定在无法修复受感染文件时如何处理此文件。

重命名

如果启用此选项，则 Scanner 会重命名文件。
因此不能再直接访问这些文件（例如，通过双击访问）。
可在以后修复文件并重新指定其原始名称。

Quarantine

如果启用此选项，则 Scanner 会将文件移到隔离区。
以后可以修复这些文件，或根据需要将文件发送给 Avira 恶意软件研究中心。

删除

如果启用此选项，则会删除文件。 此过程要比“覆盖并删除”快得多。

忽略

如果启用此选项，则允许访问文件并按原样保留文件。

警告

工作站上的受感染文件仍处于活动状态！ 它可能会对您的工作站造成严重危害！

覆盖并删除

如果启用此选项，则 Scanner 将使用默认模式覆盖文件，然后将其删除（清除）。
文件将无法还原。

说明

如果选择**删除**或**覆盖并删除**作为主操作或辅助操作，应注意：对于启发式命中文件，不会删除受感染文件，但会将其移到隔离区。

存档

扫描存档时，Scanner
采用递归扫描方式：存档中的存档也会解压缩并进行病毒和恶意程序扫描。
会对文件进行扫描、解压缩并重新扫描。 （仅在专家模式中提供选项。）

扫描存档

如果启用此选项，则扫描存档列表中的所选存档。 此选项默认设置为启用。

所有存档类型

如果启用此选项，则选择并扫描存档列表中的所有存档类型。

智能扩展

如果启用此选项，则 Scanner 会检测文件是否为压缩文件格式（存档）（即使文件扩展名与通常的扩展名不同），并扫描存档。 但是，为此必须打开每个文件，而这会降低扫描速度。 例如：如果一个 *.zip 存档的文件扩展名为 *.xyz，则 Scanner 也会解压缩此存档并对其进行扫描。 此选项默认设置为启用。

> 说明
> 只支持存档列表中那些带标记的存档类型。

限制递归深度

解压缩和扫描递归文档需要大量占用计算机时间和资源。 如果启用此选项，则需要将多层压缩的存档的扫描深度限制为某一压缩级别数（最大递归深度）。 这会节省时间和计算机资源。

> 说明
> 为了发现存档中的病毒或恶意程序，Scanner 必须扫描到病毒或恶意程序所在的递归级别。

最大递归深度

为了输入最大递归深度，必须启用选项限制递归深度。 您可以直接输入所需递归深度，也可以使用输入字段右侧的箭头键。 允许的值为 1 到 99。 标准值为 20，这是推荐设置。

默认值

此按钮将还原存档扫描的预定义值。

存档

在此显示区域可以设置 Scanner 应扫描的存档。 为此，必须选择相关的项。

例外

Scanner 忽略的文件对象（仅在专家模式中可用的选项）。

此窗口中的列表包含 Scanner 进行病毒或恶意程序扫描时不应包含的文件和路径。

请在此输入尽可能少的例外，实际上应该只输入因某种原因不应包含在正常扫描中的文件。建议在将这些文件包含在此列表中之前，总是先对其进行病毒或恶意程序扫描。

> 说明
> 列表中的项的总字符数不能超过 6000 个。

> **警告**
> 这些文件不包含在扫描中！

> 说明
> 此列表中包含的文件记录在报告文件中。
> 请不时检查报告文件，看是否有未扫描的文件，因为您排除文件的原因可能已经不存在了。这种情况下，应该从此列表中删除此文件名。

输入框

在此输入框中，可以输入按需扫描中不包含的文件对象的名称。
默认设置为不输入任何文件对象。

...

此按钮将打开一个窗口，可以在其中选择所需文件或所需路径。
如果输入了一个具有完整路径的文件名，则只有此文件不进行病毒扫描。
如果输入的文件名没有路径，则具有此名称的所有文件（无论所在路径或驱动器）都不会进行扫描。

添加

使用此按钮可以将输入框中输入的文件对象添加到显示窗口中。

删除

此按钮可以从列表中删除所选项。 如果未选择任何项，则此按钮处于不活动状态。

启发式

此配置部分包含扫描引擎的启发式扫描设置 （仅在专家模式中提供选项）。

Avira
产品包含非常强大的启发式功能，可以主动发现未知的恶意软件，即在创建能够抵御破坏元素的特殊病毒特征之前，以及在发送病毒防护更新之前，就可以发现。
病毒检测对恶意软件的典型功能所影响的代码进行广泛的分析和调查。
如果所扫描的代码表现出这些功能特征，则将其报告为可疑代码。
这不一定意味着此代码就是恶意软件。 有时确实会发生误报。
如何处理受影响的代码由用户决定，例如，用户可以根据自己所了解的此代码是否值得信任来决定。

宏病毒启发式

宏病毒启发式

Avira 产品包含非常强大的宏病毒启发式功能。
如果启用此选项，则在修复时会删除相关文档中的所有宏；也可以选择只报告可疑文档，即您将收到警报。 此选项默认设置为启用，这是推荐设置。

高级启发式分析和检测 (AHeAD)

启用 AHeAD

Avira 程序包含十分强大的以 Avira AheAD
技术体现的启发式扫描功能，也可以检测未知的（新的）恶意软件。
如果启用此选项，您可以定义此启发式扫描具有多大的“攻击性”。
此选项默认设置为启用。

低检测级别

如果启用此选项，则检测较为常见的恶意软件，在这种情况下发出误报的风险较低。

中检测级别

此选项包含具有较低误报风险的强检测级别。
如果选择使用此启发式扫描，则默认设置为中级。

高检测级别

如果选择此选项，则检测非常少见的恶意软件，但也有可能误报。

10.1.2 报告

Scanner 具有全面的报告功能。 您可以借此获得有关按需扫描结果的精确信息。
报告文件包含所有系统项以及按需扫描的警报和消息 （仅在专家模式中提供选项）。

> 说明
> 为了能够确定 Scanner
> 已执行的操作，当检测到病毒或恶意程序时，应启用专家模式配置中的报告文件
> 。

报告

关闭

如果启用此选项，则 Scanner 不报告按需扫描的操作和结果。

默认

如果启用此选项，Scanner 将记录相关文件的名称及其路径。
此外，当前扫描的配置、版本信息和有关被许可人的信息也写入报告文件中。

扩展

如果启用此选项，除默认信息之外，Scanner 还会记录警报和提示。
报告中还包含一个“(cloud)”后缀，以便识别来自 Protection Cloud 的检测。

完整

如果启用此选项，Scanner 还记录所有扫描的文件。
此外，还会在报告文件中包含有关的所有文件及警报和技巧。

> 说明
> 如果您在任何时候必须给我们发送报告文件（用于故障排除），请在此模式下创建此报告文件。

10.2 Real-Time Protection

配置的**Real-Time Protection**部分用于配置访问时扫描。
（仅在专家模式中提供选项）。

10.2.1 扫描

您通常会希望不断监视自己的系统，为此使用 Real-Time Protection（= 和访问时 Scanner）。
这样，您就可以在工作中随时扫描所有复制或打开的文件以发现病毒和恶意程序
（仅在专家模式中提供选项）。

文件

Real-Time Protection 可以使用过滤器，以便只扫描具有某一扩展名（类型）的文件。

所有文件

如果启用此选项，则针对所有文件扫描病毒或恶意程序（无论文件内容及文件扩展名如何）。

> 说明
> 如果启用了**所有文件**，则无法选择**文件扩展名**按钮。

使用智能扩展

如果启用此选项，则程序会自动选择进行病毒或恶意程序扫描的文件。
这意味着程序将根据文件内容决定是否扫描文件。
此过程比**使用文件扩展名列表**略慢，但更安全，原因是它不仅仅根据文件扩展名进行扫描。

> 说明
> 如果启用**使用智能扩展**，则无法选择**文件扩展名**按钮。

使用文件扩展名列表

如果启用此选项，则只扫描具有指定扩展名的文件。
所有可能包含病毒和恶意程序的文件类型都已预设。
此列表可以通过按钮“**文件扩展名**”手动进行编辑。
此选项默认设置为启用，这是推荐设置。

> 说明
> 如果启用此选项并且从文件扩展名列表删除了所有的项，则按钮**文件扩展名**下会显示提示文本“没有文件扩展名”。

文件扩展名

通过此按钮可以打开一个对话框，其中显示在“**使用文件扩展名列表**”模式下扫描的所有文件扩展名。系统设置了默认扩展名项，但您可以添加或删除这些项。

> 说明
> 请注意，不同版本软件的文件扩展名列表可能不同。

扫描模式

在此定义文件扫描时间。

读取时扫描

如果启用此选项，则在应用程序或操作系统读取或执行文件之前 Real-Time Protection 会先扫描文件。

写入时扫描

如果启用此选项，则在写入文件时 Real-Time Protection 会扫描文件。
您只能在此进程结束后才能再次访问文件。

读取和写入时扫描

如果启用此选项，则在打开、读取和执行前以及在写入后 Real-Time Protection 会扫描文件。 此选项默认设置为启用，这是推荐设置。

驱动器

监视网络驱动器

如果启用此选项，则扫描诸如服务器卷、对等驱动器等网络驱动器（映射驱动器）上的文件。

说明
为避免过度降低计算机性能，应该只在特例情况下才启用选项监视网络驱动器。

警告
如果禁用此选项，则不监视网络驱动器。 将不再为它们防护病毒或恶意程序！

说明
在网络驱动器上执行文件时，Real-Time Protection 会扫描文件，这不受监视网络驱动器选项设置的影响。
在某些情况下，即使已禁用监视网络驱动器选项，在打开网络驱动器上的文件时也会对其进行扫描。 原因：这些文件是用“执行文件”权限访问的。
如果希望从 Real-Time Protection

扫描中排除这些文件，甚至排除网络驱动器上已执行的文件，则请在排除文件对象列表中输入这些文件（请参阅 Real-Time Protection > 扫描 > 例外）。

启用缓存

如果启用此选项，则可以在 Real-Time Protection 的缓存中使用网络驱动器上被监视的文件。
监视网络驱动器而不缓存的功能更安全，但不如通过缓存来监视网络驱动器有效。

存档

扫描存档

如果启用此选项，则会扫描存档。 会对压缩文件进行扫描、解压缩并重新扫描。
此选项默认设置为停用。 存档扫描受递归深度、扫描文件数量和存档大小的限制。
您可以设置最大递归深度、扫描文件数量和最大存档大小。

说明
此选项默认设置为停用，因为此进程对计算机性能有很高要求。
一般建议使用按需扫描检查存档。

最大递归深度

扫描存档时，Real-Time Protection 采用递归扫描方式：存档中的存档也会解压缩并进行病毒和恶意程序扫描。
您可以定义递归深度。 递归深度的默认值为 1，这是推荐设置：扫描直接位于主存档中的所有文件。

最大文件数量

扫描存档时，可以限制在存档中扫描的最大文件数量。
所扫描的最大文件数量的默认值为 10，这是推荐设置。

最大大小 (KB)

扫描存档时，可以限制扫描时所解压缩的最大存档大小。 建议采用 1000 KB 的标准值。

针对检测的操作

可以定义 Real-Time Protection 在检测到病毒或恶意程序时所进行的操作（仅在专家模式中提供选项）。

交互式

如果启用此选项，则在 Real-Time Protection 检测到病毒或恶意程序时会显示桌面通知。
您可以删除检测到的恶意软件，或者通过“详细信息”按钮访问其他可能的病毒处理操作。 这些操作会显示在对话框窗口中。 此选项默认设置为启用。

允许的操作

在此显示框中，可以指定要作为进一步的操作显示在对话框窗口中的病毒管理操作。
为此必须启用相应选项。

修复

Real-Time Protection 会尽可能修复受感染文件。

重命名

Real-Time Protection 会对文件进行重命名。
因此不能再直接访问这些文件（例如，通过双击访问）。
可在以后修复此文件，并将其改回原有文件名。

Quarantine

Real-Time Protection 会将文件移到隔离区。
如果文件具有参考价值，则可以从隔离区管理器恢复它，也可以根据需要将其发送给 Avira 恶意软件研究中心。
隔离区管理器中可能提供更多选择选项，具体情况因文件而异。

删除

文件将被删除。 此过程要比**覆盖并删除**快得多（请参阅下文）。

忽略

允许访问文件，并且将忽略此文件。

覆盖并删除

Real-Time Protection 使用默认模式覆盖文件，然后将其删除。 文件将无法还原。

> **警告**
> 如果将 Real-Time Protection 设置为**写入时扫描**，则不会写入受感染文件。

默认

此按钮可用于选择在检测到病毒时对话框中默认启用的操作。
选择默认要启用的操作，然后单击“**默认**”按钮。

> 说明
> 不能选择**修复**作为默认操作。

单击此处可以获得更多信息。

自动

如果启用此选项，则在检测到病毒时不显示对话框。 Real-Time Protection 会根据此部分中预定义为主操作和辅助操作的设置作出反应。

执行操作前将文件复制到隔离区

如果启用此选项，则 Real-Time Protection 会在执行请求的主操作或辅助操作之前创建一个备份副本。
此备份副本保存在隔离区中。
如果此副本具有参考价格，则可以从隔离区管理器还原它。 您还可以将备份副本发送给 Avira 恶意软件研究中心。
隔离区管理器中可能提供更多选择选项，具体情况因对象而异。

主操作

主操作是 Real-Time Protection 发现病毒或恶意程序时所执行的操作。
如果选择了“**修复**”选项却无法修复受感染文件，则执行在“**辅助操作**”下选择的操作。

说明

只有在选择了**主操作**下的**修复**设置时，才能选择**辅助操作**选项。

修复

如果启用此选项，则 Real-Time Protection 会自动修复受感染的文件。 如果 Real-Time Protection 无法修复受感染的文件，则会执行**辅助操作**下选择的操作。

说明

建议进行自动修复，但这意味着让 Real-Time Protection 修改工作站上的文件。

重命名

如果启用该选项，则 Real-Time Protection 会重命名文件。
因此不能再直接访问这些文件（例如，通过双击访问）。
可在以后修复文件并重新指定其原始名称。

Quarantine

如果启用该选项，则 Real-Time Protection 会将文件移到隔离区。
以后可以修复此文件夹中的文件，或根据需要将文件发送给 Avira 恶意软件研究中心。

删除

如果启用此选项，则会删除文件。 此过程要比**覆盖并删除**快得多。

忽略

如果启用此选项，则允许访问文件并按原样保留文件。

警告

工作站上的受感染文件仍处于活动状态！ 它可能会对您的工作站造成严重危害！

覆盖并删除

如果启用该选项，则 Real-Time Protection 将使用默认模式覆盖文件，然后将其删除。 文件将无法还原。

拒绝访问

如果启用该选项，并启用报告功能，则 Real-Time Protection 仅在报告文件中输入检测结果。 此外，如果启用该选项，Real-Time Protection 会在事件日志中写入一个日志项。

警告

如果将 Real-Time Protection 设置为写入时扫描，则不会写入受感染的文件。

辅助操作

只有在选择了主操作下的修复设置时，才能选择辅助操作选项。
通过此选项，现在可以决定在无法修复受感染文件时如何处理此文件。

重命名

如果启用该选项，则 Real-Time Protection 会重命名文件。
因此不能再直接访问这些文件（例如，通过双击访问）。
可在以后修复文件并重新指定其原始名称。

Quarantine

如果启用该选项，则 Real-Time Protection 会将文件移到隔离区。
以后可以修复这些文件，或根据需要将文件发送给 Avira 恶意软件研究中心。

删除

如果启用此选项，则会删除文件。 此过程要比覆盖并删除快得多。

忽略

如果启用此选项，则允许访问文件并按原样保留文件。

警告

工作站上的受感染文件仍处于活动状态！ 它可能会对您的工作站造成严重危害！

覆盖并删除

如果启用该选项，则 Real-Time Protection
将使用默认模式覆盖文件，然后将其删除。 文件将无法还原。

拒绝访问

如果启用该选项，则不会写入受感染的文件，Real-Time Protection
仅在报告文件中输入检测结果。 此外，如果启用该选项，Real-Time Protection
会在事件日志中写入一个日志项。

说明

如果选择**删除**或**覆盖并删除**作为主操作或辅助操作，请注意：对于启发式命中文件，不会删除受感染文件，但会将其移到隔离区。

更多操作

使用事件日志

如果启用此选项，则每次检测都会在 Windows 事件日志中添加一项。 可以在 Windows 事件查看器中调用这些事件。 此选项默认设置为启用
（仅在专家模式中可用的选项）。

例外

通过这些选项，可以配置 Real-Time Protection（访问时扫描）的例外对象。
相关对象就不会包含在访问时扫描中。 在访问时扫描过程中，Real-Time Protection
可以根据要忽略的进程列表忽略对这些对象的文件访问。
这一点很有用，例如，可以在数据库或备份解决方案中加以利用
（仅在专家模式中提供选项）。

指定要忽略的进程和文件对象时请注意：列表按从上到下的顺序处理。
列表越长，则为每个访问处理列表所需的处理器时间就越多， 因此，请尽可能缩短列表。

Real-Time Protection 忽略的进程

对此列表中进程的所有文件访问都从 Real-Time Protection 的监视范围中排除。

输入框

在此字段中输入实时扫描要忽略的进程的名称， 默认设置为不输入任何进程。

进程的指定路径和文件名最多只应包含 255 个字符。 最多可以输入 128 个进程。
列表中的项的总字符数不能超过 6000 个。

输入进程时，接受 Unicode 符号。 因此可以输入含特殊符号的进程或目录名称。

必须按以下格式输入驱动器信息：[驱动器盘符]:\

冒号 (:) 仅用于指定驱动器。

指定进程时，可以使用通配符 *（任何数量的字符）和？（单个字符）。

```
C:\Program Files\Application\application.exe
C:\Program Files\Application\applicatio?.exe
C:\Program Files\Application\applic*.exe
C:\Program Files\Application\*.exe
```

为了避免从 Real-Time Protection
的监视范围中全局排除进程，仅包含以下字符的指定是无效的：*（星号）、？（问号）、/（斜线）、\（反斜线）、.（句点）、:（冒号）。

可以选择从 Real-Time Protection 的监视范围中排除无完整详细路径的进程，
例如：application.exe

但是这仅适用于可执行文件位于硬盘驱动器上的进程。

对于可执行文件位于连接的驱动器（例如网络驱动器）上的进程，必须输入完整的详细路径。 请注意针对连接的网络驱动器的例外的注释信息。

对于可执行文件位于动态驱动器上的进程，不指定任何例外。
动态驱动器用于可移动磁盘，例如 CD、DVD 或 USB 存储器。

警告

请注意，列表中记录的进程所进行的所有文件访问都将从病毒和恶意程序扫描中排除。

此按钮将打开一个窗口，可以在其中选择可执行文件。

进程

“进程”按钮将打开“进程选择”窗口，其中显示正在运行的进程。

添加

使用此按钮可以将输入框中输入的进程添加到显示窗口中。

删除

使用此按钮从显示窗口中删除所选进程。

Real-Time Protection 忽略的文件对象

对此列表中对象的所有文件访问都从 Real-Time Protection 的监视范围中排除。

输入框

在此框中可以输入访问时扫描中不包含的文件对象的名称。
默认设置为不输入任何文件对象。

列表中所有项的总字符数不能超过 6000 个。

指定要忽略的文件对象时，可以使用通配符 *（任何数量的字符）和？（单个字符）：也可以排除个别文件扩展名（包含通配符）：

```
C:\Directory\*.mdb
*.mdb
*.md?
*.xls*
C:\Directory\*.log
```

目录名必须以反斜线 \ 结束。

如果排除一个目录，则其所有子目录也自动被排除。

对于每个驱动器，最多可以通过输入完整路径（以驱动器字母开头）来指定 20 个例外。 例如：

```
C:\Program Files\Application\Name.log
```

无完整路径的例外的最大字符数为 64。 例如：

```
*.log
\computer1\C\directory1
```

对于作为另一个驱动器上的目录而装入的动态驱动器，必须使用例外列表中的集成驱动器所用的操作系统的别名，例如：

```
\Device\HarddiskDmVolumes\PhysicalDmVolumes\BlockVolume1\
```

如果使用装入点本身，例如，`C:\DynDrive`，则仍然会对此动态驱动器进行扫描。您可以从 Real-Time Protection 的报告文件确定要使用的操作系统的别名。

...

此按钮将打开一个窗口，可以在其中选择要排除的文件对象。

添加

使用此按钮可以将输入框中输入的文件对象添加到显示窗口中。

删除

使用此按钮从显示窗口中删除所选文件对象。

指定例外时请注意更多信息：

为了也排除用短 DOS 文件名（DOS 命名规则 8.3）访问的对象，还必须在列表中输入相关的短文件名。

包含通配符的文件名不得以反斜线结束。 例如：
`C:\Program Files\Application\applic*.exe\`
这样的输入是无效的，并且不会被当作例外对待！

关于针对连接的网络驱动器的例外，请注意：如果使用连接的网络驱动器的盘符，则不从 Real-Time Protection 的扫描范围中排除指定的文件和文件夹。 如果例外列表中的 UNC 路径与连接网络驱动器所使用的 UNC 路径不同（例外列表中指定了 IP 地址，而连接网络驱动器时指定了计算机名称），则不会从 Real-Time Protection 的扫描范围中排除指定的文件和文件夹。 确定相关 UNC 路径在 Real-Time Protection 报告文件中的位置：

`\\<Computer name>\<Enable>\` - OR - `\\<IP address>\<Enable>\`

可以确定 Real-Time Protection 扫描受感染文件时使用的路径在 Real-Time Protection 报告文件中的位置。 请在例外列表中指定完全相同的路径。

按以下方式处理：在 Real-Time Protection > 报告下的配置中设置 Real-Time Protection 的协议功能以完成。 再通过启用的 Real-Time Protection 访问文件、文件夹、装入的驱动器或连接的网络驱动器。 然后可以从Real-Time Protection报告文件中读取要使用的路径。 可以在控制中心的本地保护 > Real-Time Protection 下访问报告文件。

启发式

此配置部分包含扫描引擎的启发式扫描设置 （仅在专家模式中提供选项）。

Avira

产品包含非常强大的启发式功能，可以主动发现未知的恶意软件，即在创建能够抵御破坏元素的特殊病毒特征之前，以及在发送病毒防护更新之前，就可以发现。

病毒检测对恶意软件的典型功能所影响的代码进行广泛的分析和调查。

如果所扫描的代码表现出这些功能特征，则将其报告为可疑代码。

这不一定意味着此代码就是恶意软件。 有时确实会发生误报。

如何处理受影响的代码由用户决定，例如，用户可以根据自己所了解的此代码是否值得信任来决定。

宏病毒启发式

宏病毒启发式

Avira 产品包含非常强大的宏病毒启发式功能。
如果启用此选项，则在修复时会删除相关文档中的所有宏；也可以选择只报告可疑文档，即您将收到警报。 此选项默认设置为启用，这是推荐设置。

高级启发式分析和检测 (AHeAD)

启用 AHeAD

Avira 程序包含十分强大的以 Avira AheAD 技术体现的启发式扫描功能，也可以检测未知的（新的）恶意软件。
如果启用此选项，您可以定义此启发式扫描具有多大的“攻击性”。
此选项默认设置为启用。

低检测级别

如果启用此选项，则检测较为常见的恶意软件，在这种情况下发出误报的风险较低。

中检测级别

此选项包含具有较低误报风险的强检测级别。
如果选择使用此启发式扫描，则默认设置为中级。

高检测级别

如果选择此选项，则检测非常少见的恶意软件，但也有可能误报。

10.2.2 报告

Real-Time Protection
包含广泛的日志记录功能，能够为用户或管理员提供有关检测类型和方式的精确说明。
（仅在专家模式中提供选项。）

报告

此组可用于决定报告文件的内容。

关闭

如果启用此选项，则Real-Time Protection不创建日志。
建议只有在特例情况下才关闭日志记录功能，比如在试验多种病毒或恶意程序时。

默认

如果启用此选项，则 Real-Time Protection
会在报告文件中记录重要信息（所关注的检测、警报和错误），并且忽略次要信息以使记录更清晰可读。 此选项默认设置为启用。

扩展

如果启用此选项，则 Real-Time Protection 会在报告文件中也记录次要信息。

完整

如果启用此选项，则 Real-Time Protection
会在报告文件中记录所有可用信息，包括文件大小、文件类型、日期等。

限制报告文件

将大小限制为 n MB

如果启用此选项，则可以将报告文件限制为某一大小。 允许的值为 1 到 100 MB。
在限制报告文件的大小时，允许大约 50 KB
多余空间，以尽可能减少系统资源的使用。 如果日志文件大小比指定大小多 50 KB
以上，则会删除旧项，直到达到指定大小减 50 KB。

缩短之前备份报告文件

如果启用此选项，则在缩短报告文件之前会先行备份。

在报告文件中写入配置

如果启用此选项，则在报告文件中记录访问时扫描的配置。

说明
如果未指定任何报告文件限制，则当报告文件大小达到 100MB

时会自动创建新的报告文件。 可创建较早报告文件的备份。
最多可保存三份较早报告文件的备份。 最早的备份最先删除。

10.3 更新

在更新部分中，可以配置自动接收更新。 可以指定各种更新时间间隔，。

自动更新

n 天/小时/分钟

在此框中，可以指定自动更新执行的时间间隔。
要更改更新时间间隔，请在此框中突出显示一个时间选项，然后使用输入框右侧的箭头键进行更改。

连接到 Internet (拨号) 时启动作业

如果启用此选项，则除了指定的更新时间间隔以外，每次建立 Internet 连接时也会执行更新作业 （仅在专家模式中提供此选项）。

如果时间已过期则重复执行作业

如果启用此选项，则执行在指定的时间未能执行（例如由于计算机关机）的过期更新作业（仅在专家模式中提供此选项）。

10.3.1 Web 服务器

Web 服务器

可以直接通过 Internet 上的 Web 服务器进行更新 （仅在专家模式中提供选项）。

Web 服务器连接

使用现有连接 (网络)

如果通过网络使用连接，则会显示此设置。

使用下列连接

如果单独定义您的连接，则会显示此设置。

更新程序会自动检测哪种连接选项可用。 不可用的连接选项将变灰，无法启用。
可以手动建立拨号连接（例如通过 Windows 中的电话簿项）。

用户

输入所选帐户的用户名。

密码

输入此帐户的密码。 出于安全考虑，在此空白处键入的实际字符将由星号 (*) 替代。

> 说明
> 如果您忘记了现有的 Internet 帐户名或密码，请与 Internet 服务提供商联系。

> 说明
> 目前更新程序无法通过所谓的拨号工具（例如 SmartSurfer、Oleco 等）进行自动拨号。

终止为更新设置的拨号连接

如果启用此选项，则一旦成功完成下载便自动中断为更新而建立的拨号连接。

> 说明
> 此选项仅适用于 Windows XP。
> 在较新的操作系统中，一旦完成下载便总是终止为更新打开的拨号连接。

代理设置

代理服务器

不使用代理服务器

如果启用此选项，则不会通过代理服务器建立您与 Web 服务器的连接。

使用代理系统设置

如果启用此选项，则会使用当前的 Windows 系统设置，通过代理服务器与 Web 服务器连接。 在**控制面板 > Internet 选项 > 连接 > LAN 设置**中配置 Windows 系统设置以使用代理服务器。 还可以在 Internet Explorer 的**附加程序**菜单中访问 Internet 选项。

警告

如果您使用的代理服务器要求身份验证，则在**使用此代理服务器**选项中输入所有所需数据。 **使用代理系统设置**选项只能用于不要求身份验证的代理服务器。

使用此代理服务器

如果 Web 服务器连接采用代理服务器，可以在此输入相关信息。

地址

请输入连接 Web 服务器时要使用的代理服务器的计算机名称或 IP 地址。

端口

请输入连接 Web 服务器时要使用的代理服务器的端口号。

登录名

输入用户名以登录代理服务器。

登录密码

在此输入您在代理服务器上的相关登录密码。
出于安全考虑，在此空白处键入的实际字符将由星号 (*) 替代。

示例：

地址：`proxy.domain.com`端口：`8080`

地址：`192.168.1.100`端口：`3128`

10.4 Web Protection

配置 > Internet 保护中的 Web Protection 部分用于配置 Web Protection。

10.4.1 扫描

Web Protection 能够帮助您防护通过从 Internet 加载到 Web 浏览器的网页进入计算机的病毒或恶意软件。 可以使用**扫描**选项设置 Web Protection 组件的行为。 （仅在专家模式中提供选项。）

扫描

启用 IPv6 支持

如果启用此选项，Web Protection 将支持 Internet 协议第 6 版。 此选项不可在 Windows 8 系统中用于新安装或更改的安装。

驱动式保护

驱动式保护允许您进行设置以阻止 I 帧，也称内嵌帧。 I 帧是 HTML 元素，即 Internet 网页中界定网页区域的元素。 I 帧可用于以浏览器子窗口中的独立文档的形式加载和显示不同的网页内容（通常为其他 URL）。 I 帧大多用于横幅广告。 在某些情况下，I 帧被用来隐藏恶意软件。 在这类情况下，I 帧的区域在浏览器中大多不可见或几乎不可见。 **阻止可疑 I 帧**选项可以检查和阻止 I 帧的加载。

阻止可疑的 I 帧

如果启用此选项，则会按照某一条件扫描所请求的网页上的 I 帧。 如果所请求的网页上存在可疑的 I 帧，则会阻止此 I 帧。 在 I 帧窗口中会显示错误消息。

针对检测的操作

可以定义 Web Protection 在检测到病毒或恶意程序时所进行的操作。 （仅在专家模式中提供选项。）

交互式

如果启用此选项，则在按需扫描过程中如果检测到病毒或恶意程序，将显示一个对话框，可以在其中选择如果处理受感染的文件。 此选项默认设置为启用。

显示进度条

如果启用此选项，并且网站内容下载超过了 20 秒的超时设置，则会显示带进度条的桌面通知。
此桌面通知专为具有更大数据量的下载网站而设计：如果用 Web Protection 上网冲浪，则不会在 Internet 浏览器中进行网站内容增量式下载，因为网站内容在 Internet 浏览器中显示之前要先进行病毒和恶意软件扫描。 此选项默认设置为禁用。

单击此处可以获得更多信息。

自动

如果启用此选项，则在检测到病毒时不显示对话框。 Web Protection 会根据此部分中预定义为主操作和辅助操作的设置作出反应。

主操作

主操作是 Web Protection 发现病毒或恶意程序时所执行的操作。

拒绝访问

向 Web 服务器请求的网站和/或传输的任何数据或文件都不会发送到 Web 浏览器。 Web 浏览器中会显示一条错误消息，指出访问已被拒绝。 如果启用报告功能，Web Protection 会将检测结果记录到报告文件中。

移到隔离区

如果检测到病毒或恶意软件，则会将向 Web 服务器请求的网站和/或传输的数据和文件移到隔离区中。
如果受感染文件具有任何参考价值，则可以从隔离区管理器恢复它，也可以根据需要将其发送给 Avira 恶意软件研究中心。

忽略

Web Protection 将向 Web 服务器请求的网站和/或传输的数据和文件转发给 Web 浏览器。 允许访问文件，并且将忽略此文件。

警告

工作站上的受感染文件仍处于活动状态！ 它可能会对您的工作站造成严重危害！

阻止的请求

在阻止的请求中，可以指定 Web Protection 将阻止的文件类型和 MIME 类型（传输数据的内容类型）。 Web 过滤器可用于阻止已知的钓鱼和恶意软件 URL。Web Protection 能够阻止从 Internet 向您的计算机系统传输数据（仅在专家模式中提供选项）。

Web Protection 将阻止以下文件类型/MIME 类型

Web Protection 将阻止列表中的所有文件类型和 MIME 类型（传输数据的内容类型）。

输入框

在此框中输入希望 Web Protection 阻止的 MIME 类型和文件类型的名称。对于文件类型，请输入文件扩展名，例如，.htm。 对于 MIME 类型，请指定媒体类型及（如果适用）子类型。这两个语句用一条斜线分隔，例如，video/mpeg 或 audio/x-wav。

说明

但是，您的计算机的 Internet 浏览器可以从 Internet 向本地下载已作为临时 Internet 文件存储在您的系统中并受 Web Protection 阻止的文件。 临时 Internet 文件由 Internet 浏览器保存在计算机上，目的是可以更快速地访问网站。

说明

如果将受阻止文件和 MIME 类型列表输入到 Web Protection > 扫描 > 例外下排除的文件和 MIME 类型列表中，则会将其忽略。

> 说明
> 输入文件类型和 MIME 类型时可以使用通配符（*，表示任何数量的字符，或者 ?，表示单个字符）。

MIME 类型：媒体类型示例：

- `text` = 表示文本文件
- `image` = 表示图形文件
- `video` = 表示视频文件
- `audio` = 表示声音文件
- `application` = 表示与特定程序链接的文件

排除的文件和 MIME 类型示例

- `application/octet-stream` = Web Protection 阻止应用程序/八位字节流 MIME 类型文件（可执行文件 *.bin、*.exe、*.com、*dll、*.class）。
- `application/olescript` = Web Protection 阻止应用程序/olescript MIME 类型文件（ActiveX 脚本文件 *.axs）。
- `.exe` = Web Protection 阻止所有扩展名为 .exe（可执行文件）的文件。
- `.msi` = Web Protection 阻止所有扩展名为 .msi（Windows Installer 文件）的文件。

添加

此按钮可用于将 MIME 和文件类型从输入字段复制到显示窗口中。

删除

此按钮可以从列表中删除所选项。 如果未选择任何项，则此按钮处于不活动状态。

Web 过滤器

Web 过滤器基于一个内部数据库，此数据库根据内容对 URL 进行分类，并且每天都会更新。

启用 Web 过滤器

如果启用此选项，将阻止所有与 Web 过滤器列表中所选类别匹配的 URL。

Web 过滤器列表

在 Web 过滤器列表中，可以选择 Web Protection 将阻止其 URL 的内容类别。

> 说明
> 对于 Web Protection > 扫描 > 例外下排除的 URL 列表中的项，将忽略 Web 过滤器。

> 说明
> **垃圾邮件 URL** 是通过垃圾电子邮件发送的 URL。
> **欺诈/欺骗**类别涵盖有关“订阅到期”的网页和提供商隐藏了费用的其他服务项目。

例外

这些选项可用于根据 URL（Internet 地址）的 MIME 类型（传输数据的内容类型）和文件类型设置 Web Protection 扫描例外。 Web Protection 将忽略 MIME 类型和指定的 URL，即在将这些数据传输到您的计算机系统时不会对其进行病毒和恶意软件扫描（仅在专家模式中提供选项）。

Web Protection 跳过的 MIME 类型

在此字段中可以选择 Web Protection 扫描过程中忽略的 MIME 类型（传输数据的内容类型）。

Web Protection 跳过的文件类型/MIME 类型 (用户定义)

Web Protection 在扫描过程中将忽略此列表中的所有 MIME 类型（传输数据的内容类型）。

输入框

在此框中可以输入 Web Protection 在扫描过程中忽略的 MIME 类型和文件类型的名称。对于文件类型，请输入文件扩展名，例如，**.htm**。对于 MIME 类型，请指定媒体类型及（如果适用）子类型。这两个语句用一条斜线分隔，例如，**video/mpeg** 或 **audio/x-wav**。

说明

输入文件类型和 MIME 类型时可以使用通配符（*，表示任何数量的字符，或者 ?，表示单个字符）。

警告

将扩展名列表上的所有文件类型和内容类型下载到 Internet 浏览器中时，不会对阻止的请求（在 Web Protection > 扫描 > 阻止的请求中阻止的文件和 MIME 类型列表）进行进一步扫描或者 Web Protection 不会进行进一步扫描：对于排除列表上的所有项，忽略要阻止的文件和 MIME 类型列表中的项。不会进行病毒和恶意软件扫描。

MIME 类型：媒体类型示例：

- `text` = 表示文本文件
- `image` = 表示图形文件
- `video` = 表示视频文件
- `audio` = 表示声音文件
- `application` = 表示与特定程序链接的文件

排除的文件和 MIME 类型示例：

- `audio/` = Web Protection 扫描排除所有音频媒体类型文件
- `video/quicktime` = Web Protection 扫描排除所有 Quicktime 子类型视频文件（*.qt、*.mov）

- .pdf = Web Protection 扫描排除所有 Adobe PDF 文件。

添加

此按钮可用于将 MIME 和文件类型从输入字段复制到显示窗口中。

删除

此按钮可以从列表中删除所选项。 如果未选择任何项，则此按钮处于不活动状态。

Web Protection 跳过的 URL

Web Protection 扫描排除此列表中的所有 URL。

输入框

可以在此框中输入要从 Web Protection 的扫描范围中排除的 URL（Internet 地址），例如 www.domainname.com。 可以指定 URL 的一部分，使用开始或结束句点表示域级别：.domainname.com 表示域的所有页面和所有子域。用任何具有结束句点的顶级域（.com 或 .net）表示网站： domainname. 用任何具有结束句点的顶级域（.com 或 .net）表示网站：domainname.。
如果如果指定的字符串不包含开始或结束句点，则会将此字符串理解为顶级域，例如，net 表示所有 NET 域（www.domain.net）。

说明

在指定 URL 时还可以使用通配符 *表示任何数量的字符。
还可以组合使用开始或结束句点和通配符以表示域级别：
.domainname.*
*.domainname.com
.*name*.com（有效但不推荐）
如果指定时不用句点，例如 *name*，
则将其理解为顶级域的一部分，但不建议这样做。

警告

将排除的 URL 列表上的所有网站下载到 Internet 浏览器中时，Web 过滤器或 Web Protection 不进行进一步扫描：对于排除的 URL 列表中的所有项，忽略 Web 过滤器中的项（请参阅 Web Protection > 扫描 > 阻止的请求）。
不会进行病毒和恶意软件扫描。 因此应该只将可靠的 URL 从 Web Protection 扫描中排除。

添加

此按钮可用于将输入字段中的 URL（Internet 地址）复制到查看器窗口中。

删除

此按钮可以从列表中删除所选项。 如果未选择任何项，则此按钮处于不活动状态。

示例：跳过的 URL

- `www.avira.com` -OR- `www.avira.com/*`
  = 从Web Protection的扫描范围中排除具有域 `www.avira.com` 的所有 URL：*www.avira.com/en/pages/index.php*、*www.avira.com/en/support/index.html*、*www.avira.com/en/download/index.html* 等。
  不排除具有域 `www.avira.de` 的 URL。
- `avira.com` -OR- `*.avira.com`
  = 从 Web Protection 的扫描范围中排除具有二级和顶级域 `avira.com` 的所有 URL：它表示 `.avira.com` 的所有现有子域：*www.avira.com*、*forum.avira.com*等。
- `avira.` -OR- `*.avira.*`
  = 从 Web Protection 的扫描范围中排除具有二级域 `avira` 的所有 URL：它表示 `.avira` 的所有现有顶级域或子域：*www.avira.com*、*www.avira.de*、*forum.avira.com* 等。
- `.*domain*.*`
  从 Web Protection 的扫描范围中排除含有二级域且二级域具有字符串域的所有 URL：*www.domain.com*、*www.new-domain.de*、*www.sample-domain1.de*……

- net -OR- *.net
  = 从 Web Protection 的扫描范围中排除具有顶级域 net 的所有 URL：*www.name1.net*、*www.name2.net* 等。

警告

请尽可能精确地输入您想从 Web Protection 扫描中排除的 URL。
避免指定整个顶级域或二级域的一部分，因为在排除设置下指定全局名称可能会导致从 Web Protection 扫描中排除传播恶意软件和不需要的程序的 Internet 页面。 建议至少指定完整的二级域和顶级域：domainname.com

启发式

此配置部分包含扫描引擎的启发式扫描设置 （仅在专家模式中提供选项）。

Avira

产品包含非常强大的启发式功能，可以主动发现未知的恶意软件，即在创建能够抵御破坏元素的特殊病毒特征之前，以及在发送病毒防护更新之前，就可以发现。
病毒检测对恶意软件的典型功能所影响的代码进行广泛的分析和调查。
如果所扫描的代码表现出这些功能特征，则将其报告为可疑代码。
这不一定意味着此代码就是恶意软件。 有时确实会发生误报。
如何处理受影响的代码由用户决定，例如，用户可以根据自己所了解的此代码是否值得信任来决定。

宏病毒启发式

Avira 产品包含非常强大的宏病毒启发式功能。
如果启用此选项，则在修复时会删除相关文档中的所有宏；也可以选择只报告可疑文档，即您将收到警报。 此选项默认设置为启用，这是推荐设置。

高级启发式分析和检测 (AHeAD)

启用 AHeAD

Avira 程序包含十分强大的以 Avira AheAD 技术体现的启发式扫描功能，也可以检测未知的（新的）恶意软件。如果启用此选项，您可以定义此启发式扫描具有多大的“攻击性”。此选项默认设置为启用。

低检测级别

如果启用此选项，则检测较为常见的恶意软件，在这种情况下发出误报的风险较低。

中检测级别

此选项包含具有较低误报风险的强检测级别。如果选择使用此启发式扫描，则默认设置为中级。

高检测级别

如果选择此选项，则检测非常少见的恶意软件，但也有可能误报。

10.4.2 报告

Web Protection 包含广泛的日志记录功能，能够为用户或管理员提供有关检测类型和方式的精确说明。

报告

此组可用于决定报告文件的内容。

关闭

如果启用此选项，则Web Protection不创建日志。建议只有在特例情况下才关闭日志记录功能，比如在试验多种病毒或恶意程序时。

默认

如果启用此选项，则 Web Protection 会在报告文件中记录重要信息（所关注的检测、警报和错误），并且忽略次要信息以使记录更清晰可读。 此选项默认设置为启用。

高级

如果启用此选项，则 Web Protection 会在报告文件中也记录次要信息。

完整

如果启用此选项，则 Web Protection
会在报告文件中记录所有可用信息，包括文件大小、文件类型、日期等。

限制报告文件

将大小限制为 n MB

如果启用此选项，则可以将报告文件限制为某一大小；可能的值为：允许的值为 1 到 100MB。 在限制报告文件的大小时，允许大约 50 KB
多余空间，以尽可能减少系统资源的使用。 如果日志文件大小比指定大小多 50 KB 以上，则会删除旧项，直到达到指定大小减 20%。

在报告文件中写入配置

如果启用此选项，则在报告文件中记录访问时扫描的配置。

> 说明
> 如果未指定任何报告文件限制，则当报告文件大小达到 100MB 时会自动删除旧项。 直到报告文件大小达到 80MB。

10.5 Mail Protection

配置的 **Mail Protection** 部分用于配置 Mail Protection。

10.5.1 扫描

使用 Mail Protection 对传入电子邮件进行病毒和恶意软件扫描。 可以使用 Mail Protection 对外发电子邮件进行病毒和恶意软件扫描。

扫描传入电子邮件

如果启用此选项，则对传入电子邮件进行病毒和恶意软件。 Mail Protection 支持 POP3 和 IMAP 协议。 使 Mail Protection 能够监视由您的电子邮件客户端用来接收电子邮件的收件箱帐户。

监视 POP3 帐户

如果启用此选项，则在指定端口上监视 POP3 帐户。

监视的端口

在此字段中应该输入 POP3 协议要用作收件箱的端口。 多个端口之间用逗号分隔（仅在专家模式中提供此选项）。

默认

此按钮将指定端口重置为默认的 POP3 端口 （仅在专家模式中提供此选项）。

监视 IMAP 帐户

如果启用此选项，则在指定端口上监视 IMAP 帐户。

监视的端口

在此字段中应该输入 IMAP 协议要用作收件箱的端口。 多个端口之间用逗号分隔（仅在专家模式中提供此选项）。

默认

此按钮将指定端口重置为默认的 IMAP 端口 （仅在专家模式中提供此选项）。

扫描外发电子邮件 (SMTP)

如果启用此选项，则对外发电子邮件进行病毒和恶意软件扫描。

监视的端口

在此字段中应该输入 SMTP 协议要用作发件箱的端口。 多个端口之间用逗号分隔（仅在专家模式中提供此选项）。

默认

此按钮将指定端口重置为默认的 SMTP 端口 （仅在专家模式中提供此选项）。

> 说明
> 要验证所使用的协议和端口，请在您的电子邮件客户端程序中调用电子邮件帐户的属性。 大多使用默认端口。

启用 IPv6 支持

如果启用此选项，Web Protection 将支持 Internet 协议第 6 版（此选项仅可用于专家模式，不可在 Windows 8 系统中用于新安装或更改的安装。）

针对检测的操作

这部分配置包含有关 Mail Protection 在电子邮件或附件中发现病毒或恶意程序时所执行操作的更多设置。（仅在专家模式中提供选项。）

> 说明
> 在传入电子邮件和外发电子邮件中发现病毒时都会执行这些操作。

交互式

如果启用此选项，则在电子邮件或附件中检测到病毒或恶意程序时，将显示一个对话框，可以在其中选择如何处理相关的电子邮件或附件。 此选项默认设置为启用。

显示进度条

如果启用此选项，则在下载电子邮件的过程中 Mail Protection 会显示一个进度条。仅当启用“交互式”选项时才能启用此选项。

自动

如果启用此选项，则在发现病毒或恶意程序时不再通知您。 Mail Protection 会根据此部分中定义的设置作出反应。

受感染的电子邮件

当 Mail Protection

在电子邮件发现病毒或恶意程序时执行为“*受感染的电子邮件*”选择的操作。

如果选择了选项“**忽略**”，则还可以在受“*感染的附件*”下选择在附件中检测到病毒或恶意程序时所用的处理进程。

删除

如果启用此选项，则在检测到病毒或恶意程序时会自动删除受感染的电子邮件。

此电子邮件的文本正文将被替换为下面所提供的默认文本。

对于包含的所有附件也是如此，它们也替换为默认文本。

忽略

如果启用此选项，则即使检测到病毒或恶意程序，也仍然忽略受感染的电子邮件。

但是您可以决定如何处理受感染的附件。

移到隔离区

如果启用此选项，则在检测到病毒或恶意程序时，会将包括所有附件在内的整个电子邮件放到隔离区中。 如果需要，以后可以将其还原。 受感染的电子邮件本身将被删除。

此电子邮件的文本正文将被替换为下面所提供的默认文本。

对于包含的所有附件也是如此，它们也替换为默认文本。

受感染的附件

只有在选择了“*受感染的电子邮件*”下的**忽略**设置时，才能选择“*受感染的附件*”选项。 通过此选项，现在可以决定在附件中检测到病毒或恶意程序时如何处理。

删除

如果启用此选项，则在检测到病毒或恶意程序时，将删除受感染的附件，并将其替换为默认文本。

忽略

如果启用此选项，则即使检测到病毒或恶意程序，也仍然忽略并发送附件。

警告

如果选择此选项，则 Mail Protection 不会防护病毒和恶意程序。

只有清楚自己的操作目的时，才可以选择此项。
请在电子邮件程序中禁用预览，绝不能通过双击打开附件！

移到隔离区

如果启用此选项，则将受感染的附件放到隔离区中，然后将其删除（将其替换为默认文本）。 如果需要，以后可以还原受感染的附件。

更多操作

这部分配置包含有关 Mail Protection
在电子邮件或附件中发现病毒或恶意程序时所执行操作的更多设置
（仅在专家模式中提供选项）。

说明
这些操作专门供在传入电子邮件中检测到病毒时执行。

已删除和移动的电子邮件的默认文本

此框中的文本作为消息插入电子邮件中以替代受感染的电子邮件。 您可以编辑此消息。文本最多可以包含 500 个字符。

您可以使用下列组合键进行格式化：

Ctrl + Enter = 插入换行符。

默认

此按钮在编辑框中插入预定义的默认文本。

已删除和移动的附件的默认文本

此框中的文本作为消息插入电子邮件中以替代受感染的附件。 您可以编辑此消息。文本最多可以包含 500 个字符。

您可以使用下列组合键进行格式化：

Ctrl + Enter = 插入换行符。

默认

此按钮在编辑框中插入预定义的默认文本。

启发式

此配置部分包含扫描引擎的启发式扫描设置 （仅在专家模式中提供选项）。

Avira
产品包含非常强大的启发式功能，可以主动发现未知的恶意软件，即在创建能够抵御破坏元素的特殊病毒特征之前，以及在发送病毒防护更新之前，就可以发现。
病毒检测对恶意软件的典型功能所影响的代码进行广泛的分析和调查。
如果所扫描的代码表现出这些功能特征，则将其报告为可疑代码。
这不一定意味着此代码就是恶意软件。 有时确实会发生误报。
如何处理受影响的代码由用户决定，例如，用户可以根据自己所了解的此代码是否值得信任来决定。

宏病毒启发式

Avira 产品包含非常强大的宏病毒启发式功能。
如果启用此选项，则在修复时会删除相关文档中的所有宏；也可以选择只报告可疑文档，即您将收到警报。 此选项默认设置为启用，这是推荐设置。

高级启发式分析和检测 (AHeAD)

启用 AHeAD

Avira 程序包含十分强大的以 Avira AheAD
技术体现的启发式扫描功能，也可以检测未知的（新的）恶意软件。
如果启用此选项，您可以定义此启发式扫描具有多大的“攻击性”。
此选项默认设置为启用。

低检测级别

如果启用此选项，则检测较为常见的恶意软件，在这种情况下发出误报的风险较低。

中检测级别

此选项包含具有较低误报风险的强检测级别。
如果选择使用此启发式扫描，则默认设置为中级。

高检测级别

如果选择此选项，则检测非常少见的恶意软件，但也有可能误报。

10.5.2 常规

例外

扫描例外

此表显示从 Mail Protection 扫描中排除的电子邮件地址的列表（白名单）。

> 说明
> 此例外列表专门用于 Mail Protection 对传入电子邮件的扫描。

扫描例外

输入框

在此框中输入要添加到不扫描的电子邮件地址列表中的电子邮件地址。
根据您的设置，Mail Protection 以后将不再扫描该电子邮件地址。

添加

使用此按钮可以将在输入框中输入的电子邮件地址添加到不扫描电子邮件地址列表中。

删除

此按钮可以从列表中删除突出显示的电子邮件地址。

电子邮件地址

不再扫描的电子邮件。

恶意软件

如果启用此选项，将不再对电子邮件地址进行恶意软件扫描。

向上

您可以使用此按钮将突出显示的电子邮件地址移到更高的位置。
如果没有突出显示的项或突出显示的地址处于列表中的第一位置，则此按钮不会启用。

向下

您可以使用此按钮将突出显示的电子邮件地址移到更低的位置。
如果没有突出显示的项或突出显示的地址处于列表中的最后位置，则此按钮不会启用。

缓存

Mail Protection 缓存包含有关在控制中心的 **Mail Protection** 下作为统计数据显示的已扫描电子邮件的数据 （仅在专家模式中提供选项）。

缓存的最大电子邮件数量

此字段用于设置 Mail Protection 在缓存中存储的电子邮件的最大数量。
电子邮件从最早的开始删除。

存储电子邮件的最长天数

在此框中输入电子邮件的最大存储天数。 此天数后将会从缓存中删除电子邮件。

清空缓存

单击此按钮可以删除缓存中存储的电子邮件。

10.5.3 报告

Mail Protection 包含广泛的日志记录功能，能够为用户或管理员提供有关检测类型和方式的精确说明。（仅在专家模式中提供选项。）

报告

此组可用于决定报告文件的内容。

关闭

如果启用此选项，则Mail Protection不创建日志。
建议只有在特例情况下才关闭日志记录功能，比如在试验多种病毒或恶意程序时。

默认

如果启用此选项，则 Mail Protection
会在报告文件中记录重要信息（所关注的检测、警报和错误），并且忽略次要信息以使记录更清晰可读。 此选项默认设置为启用。

扩展

如果启用此选项，则 Mail Protection 会在报告文件中也记录次要信息。

完整

如果启用此选项，则 Mail Protection 会在报告文件中也记录次要信息。

限制报告文件

将大小限制为 n MB

如果启用此选项，则可以将报告文件限制为某一大小；可能的值为：允许的值为 1 到 100MB。 在限制报告文件的大小时，允许大约 50 KB
多余空间，以尽可能减少系统资源的使用。 如果日志文件大小比指定大小多 50 KB 以上，则会删除旧项，直到达到指定大小减 50 KB。

缩短之前备份报告文件

如果启用此选项，则在缩短报告文件之前会先行备份。

在报告文件中写入配置

如果启用此选项，则在报告文件中记录 Mail Protection 配置。

说明

如果未指定任何报告文件限制，则当报告文件大小达到 100MB 时会自动创建新的报告文件。 可创建较早报告文件的备份。 最多可保存三份较早报告文件的备份。 最早的备份最先删除。

10.6 儿童保护

使用 Avira 的 *儿童保护* 功能可确保您的孩子或使用计算的其他人获得安全的 Internet 体验。

10.7 手机保护

10.7.1 手机保护

不仅能够保护计算机系统不受恶意软件和病毒侵害，还能保护用 Android 操作系统运行的智能手机免遭丢失和偷窃。 使用 Avira Free Android Security 还可以阻止骚扰电话或 SMS。 仅需将通话记录、SMS 记录和联系人列表中的电话号码添加到黑名单中，或者手动创建您要阻止的联系人。

有关更多信息，请访问我们的网站：

http://www.avira.com/android

10.8 常规

10.8.1 威胁类别

选择扩展威胁类别（仅在专家模式中提供选项）

Avira 产品可帮助您防御计算机病毒。 此外，您还可以根据下列扩展威胁类别进行扫描。

- 广告软件
- 广告软件/间谍软件
- 应用程序

- 后门客户端
- 拨号器
- 双扩展名文件
- 欺诈性软件
- 游戏
- 玩笑程序
- 钓鱼
- 侵犯私人领域的程序
- 非常规运行时压缩程序

通过单击相关的框，可以启用（有复选标记）或禁用（无复选标记）所选类型。

全选

如果启用此选项，则会启用所有类型。

默认值

此按钮将还原预定义的默认值。

> 说明
> 如果禁用了一个类型，则不再指出被识别为相关程序类型的文件。
> 不会在报告文件中创建项。

10.8.2 高级保护

ProActiv（仅在专家模式中可用的选项）。

启用 ProActiv

如果启用此选项，将对系统上的程序进行监视，并检查它们是否具有可疑操作。
如果检测到典型的恶意软件行为，您就会收到消息。
您可以阻止此程序，或者选择忽略以继续使用此程序。

监视进程不包括：分类为可靠的程序，允许的应用程序过滤器中默认包含的可靠且签名的程序，以及您添加到允许的应用程序过滤器中的所有程序。

ProActiv 可抵御新的未知威胁，对于这些威胁，还没有任何病毒定义或启发式信息可用。
ProActiv 技术集成在 Real-Time Protection 组件中，可观察并分析所执行的程序操作。
检查程序的行为中是否存在典型的恶意软件行为模式：操作类型和操作序列。
如果某个程序表现出典型的恶意软件行为，则将其作为检测到的病毒对待：可以选择阻止此程序，或者选择忽略此通知并继续使用此程序。
您可以将此程序分类为可靠，并将其添加到允许程序的应用程序过滤器中。
可以使用始终阻止命令，将此程序添加到阻止程序的应用程序过滤器中。

ProActiv 组件使用 Avira 恶意软件研究中心开发的规则集来识别可疑行为。 此规则集由 Avira GmbH 数据库提供。 ProActiv 会将任何可疑程序的相关信息发送到 Avira 数据库中以作记录。 安装 Avira 时，您可以选择禁止将数据传输到 Avira 数据库中。

> 说明
> ProActiv 技术尚不可用于 64 位系统！

Protection Cloud（仅在专家模式中可用的选项）。

启用 Protection Cloud

将所有可疑文件的指纹发送给 Protection Cloud 进行动态联机检查。
立即将可执行文件识别为干净、受感染或未知。

Protection Cloud 可用作观察整个用户库的网络攻击企图的中心位置。
将计算机访问的文件与云端存储的文件的指纹进行匹配。
在云端完成的扫描更多，因此防病毒应用程序所要求的处理能力更低。

运行快速系统扫描作业时会生成文件位置列表，此列表经常成为恶意软件的目标。
此列表包含运行进程、启动时运行的程序以及服务。 会生成每个文件的指纹并将其发送到 Protection Cloud，然后分类为“干净”或“恶意软件”。 未知程序文件会上传到 Protection Cloud 进行分析。

发送可疑文件至 Avira 时手动确认

可以看到应发送给 Protection Cloud 的可疑文件列表，而且可以选择要发送哪些文件。

阻止的应用程序

在*要阻止的应用程序*下，可以输入要划分为有害并希望 AntiVir ProActiv 默认阻止的应用程序。 所添加的应用程序不能在计算机系统上执行。
也可以选择**始终阻止此程序**。

要阻止的应用程序

应用程序

此列表包含您通过配置或通过通知 ProActiv 组件而输入的分类为有害的所有应用程序。 此列表中的应用程序会被Avira ProActiv 阻止，并且不能在计算机系统上执行。
在启动被阻止的程序时，会显示一条操作系统消息。 Avira ProActiv 根据指定的路径和文件名来识别要阻止的应用程序，而与它们的内容无关。

输入框

在此框中输入要阻止的应用程序。
要识别应用程序，必须指定完整的路径、文件名和文件扩展名。
路径必须显示应用程序所在的驱动器或以环境变量开头。

此按钮将打开一个窗口，可以在其中选择要阻止的应用程序。

添加

使用“**添加**”按钮，可以将输入框中指定的应用程序传输到要阻止的应用程序列表中。

> 说明
> 无法添加操作系统的正确操作所必需的应用程序。

删除

“删除”按钮用于从要阻止的应用程序列表中删除突出显示的应用程序。

允许的应用程序

*要跳过的应用程序*部分列出了从 ProActiv 组件的监视范围中排除应用程序：分类为可靠且默认包含在列表中的签名的程序，分类为可靠且添加到应用程序过滤器中的所有应用程序：可以将允许的应用程序添加到配置中的列表中。 也可以选择使用 Real-Time Protection 通知中的**可信程序**选项，通过 Real-Time Protection 通知将应用程序添加到可疑程序行为中。

要跳过的应用程序

应用程序

此列表包含从 ProActiv 组件的监视范围中排除的应用程序。
在默认安装设置中，此列表包含来自可靠提供商的已签名应用程序。
可以通过配置或通过 Real-Time Protection 通知，添加您认为可信的应用程序。
ProActiv 组件使用路径、文件名和内容来识别应用程序。
我们建议对内容进行检查，因为恶意软件可以通过更新等更改方式添加到程序中。
可以从指定的类型确定是否应执行内容检查：对于“*内容*”类型，在从 ProActiv 组件的监视范围中排除按路径和文件名指定的应用程序之前，会先检查对文件内容的更改。 如果文件内容被修改，ProActiv 组件会再次监视此应用程序。
对于“*路径*”类型，在从 Real-Time Protection 的监视范围中排除应用程序之前，不会执行任何内容检查。
要更改排除类型，请单击所显示的类型。

警告

只有在特例情况下才应用*路径*类型。
恶意代码可以通过更新而添加到应用程序中。
最初无害的应用程序会变成恶意软件。

说明

默认情况下，有些可信应用程序（例如，包括 Avira 产品的所有应用程序组件）即使未包含在此列表中，也会从 ProActiv 组件的监视范围中排除。

输入框

在此框中输入要从 ProActiv 组件的监视范围中排除的应用程序。
要识别应用程序，必须指定完整的路径、文件名和文件扩展名。
路径必须显示应用程序所在的驱动器或以环境变量开头。

此按钮将打开一个窗口，可以在其中选择要排除的应用程序。

添加

使用“**添加**”按钮，可以将输入框中指定的应用程序传输到要排除的应用程序列表中。

删除

“**删除**”按钮用于从要排除的应用程序列表中删除突出显示的应用程序。

10.8.3 密码

可以使用密码保护 Avira 产品的不同区域。
如果分配了密码，则每次要打开受保护区域时都会让您输入密码。

密码

输入密码

在此输入所需密码。 出于安全考虑，在此空白处键入的实际字符将由星号 (*) 替代。
密码最多只能包含 20 个字符。
分配密码后，如果输入的密码不正确，程序会拒绝访问。 空白框表示“没有密码”。

确认

在此重新输入密码以对上面输入的密码进行确认。
出于安全考虑，在此空白处键入的实际字符将由星号 (*) 替代。

> 说明
> 密码区分大小写！

受密码保护的区域（仅在专家模式中可用的选项）

可以使用密码保护 Avira 产品的不同区域。
通过单击相关的框，可以根据需要针对个别区域禁用或重新启用密码请求。

受密码保护的区域	功能
控制中心	如果启用此选项，则启动控制中心时需要预定义的密码。
启用/停用 Real-Time Protection	如果启用此选项，则启用或禁用 Avira Real-Time Protection 时需要预定义的密码。
启用/停用 Mail Protection	如果启用此选项，则启用/禁用 Mail Protection 时需要预定义的密码。
启用/停用 Web Protection	如果启用此选项，则启用/禁用 Web Protection 时需要预定义的密码。
Quarantine	如果启用此选项，则会启用所有受密码保护的隔离区管理器区域。 通过单击相关的框，可以根据个别区域的要求禁用或重新启用密码要求。
还原受影响的对象	如果启用此选项，则还原对象时需要预定义的密码。

重新扫描受影响的对象	如果启用此选项，则重新扫描对象时需要预定义的密码。
受影响对象的属性	如果启用此选项，则显示对象属性时需要预定义的密码。
删除受影响的对象	如果启用此选项，则删除对象时需要预定义的密码。
向 Avira 发送电子邮件	如果启用此选项，则向 Avira 恶意软件研究中心发送对象以供检查时需要预定义的密码。
配置	如果启用此选项，则只有在输入预定义的密码后才能配置程序。
安装/卸载	如果启用此选项，则安装或卸载程序时需要预定义的密码。

10.8.4 安全

仅在专家模式中提供选项。

自动运行

阻止自动运行功能

如果启用此选项，则对所有已连接的驱动器（包括 USB 存储器、CD 驱动器、DVD 驱动器和网络驱动器）禁止执行 Windows 自动运行功能。 通过 Windows 自动运行功能，会在加载或连接时立即读取数据介质或网络驱动器上的文件，因此可以自动启动和复制文件。
此功能安全风险极高，因为恶意软件和恶意程序可以通过自动启动功能进行安装。
自动运行功能对 USB 存储器尤其危险，因为 USB 存储器上的数据可随时进行更改。

排除 CD 和 DVD

如果启用此选项，则对 CD 和 DVD 驱动器允许自动运行功能。

警告

如果您确信您只使用可信的数据介质，则只需对 CD 和 DVD 驱动器禁用自动运行功能。

系统防护

防止 Windows 主机文件被更改

如果启用此选项，Windows 主机文件将受到写保护。 无法再进行操作。 例如，恶意软件无法将您重定向到不希望访问的网站。 此选项默认设置为启用。

产品保护

说明

如果未使用用户定义的安装选项安装 Real-Time Protection，产品保护选项将不可用。

防止进程被意外终止

如果启用此选项，则会保护程序的所有进程不被病毒或恶意软件意外终止，或阻止用户（例如任务管理器）“不受控制地”加以终止。 此选项默认设置为启用。

高级进程保护

如果启用此选项，则程序所有进程都会受到高级选项的保护，防止它被意外终止。 高级进程保护与简单进程保护相比，所需的计算机资源要多得多。 此选项默认设置为启用。 要禁用此选项，必须重新启动计算机。

说明

密码保护不适用于 Windows XP 64 位！

警告

如果启用进程保护，则可能会与其他软件产品发生交互问题。
在这种情况下请禁用进程保护。

防止对文件和注册表项进行操作

如果启用此选项，则会保护程序的所有注册项和所有程序文件（二进制文件和配置文件）不被随意操作。
操作保护需要防止用户或外部程序对注册表项或程序文件进行写入、删除及（在某些情况下）读取访问。 要启用此选项，必须重新启动计算机。

警告

请注意，如果禁用此选项，受特定类型恶意软件感染的计算机可能会修复失败。

说明

启用此选项后，只能通过用户界面更改配置（包括更改扫描或更新请求）。

说明

文件和注册项保护不适用于 Windows XP 64 位！

10.8.5 WMI

仅在专家模式中提供选项。

Windows Management Instrumentation 支持

Windows Management Instrumentation 是一种基本的 Windows 管理技术，它使用脚本和编程语言提供对 Windows 系统的本地和远程的读写访问。Avira 产品通过接口支持 WMI

并提供数据（状态信息、统计数据、报告、计划的请求等）及事件。 WMI 提供从此程序下载操作数据的选项和

启用 WMI 支持

如果启用此选项，则可以通过 WMI 从此程序下载操作数据。

10.8.6 事件

仅在专家模式中提供选项。

事件数据库大小限制

将大小限制为最大 n 项

如果启用此选项，则事件数据库中所列事件的最大数量可以限制为某一大小；可能的值为：100 至 10000 项。 如果超出输入项的数量限制，将会删除最早的项。

删除所有早于 n 天的事件

如果启用此选项，则在某一时间段后会删除事件数据库中所列的事件；可能的值为：1 至 90 天。 此选项默认设置为启用，默认值为 30 天。

无限制

如果启用此选项，则不限制事件数据库的大小。
但是，在程序界面中的“事件”下，最多显示 20,000 项。

10.8.7 报告

仅在专家模式中提供选项。

限制报告数量

将数量限制为最大 n 个

如果启用此选项，则可以将报告的最大数量限制为某一数值。 允许的值为 1 到 300。
如果超出指定数量，则会删除最早的报告。

删除 n 天以前的所有报告

如果启用此选项，则在特定天数后会自动删除报告。 允许的值为 1 至 90 天。此选项默认设置为启用，默认值为 30 天。

无限制

如果启用此选项，则不限制报告数量。

10.8.8 目录

仅在专家模式中提供选项。

*临时*路径

使用默认系统设置

如果启用此选项，将使用系统设置来处理临时文件。

> 说明
> 以 Windows XP 为例，可以在开始 > 设置 > 控制面板 > 系统 > 索引卡“高级”按钮“环境变量”中查看临时文件在系统中的保存位置。这里会显示当前注册用户的临时变量（TEMP、TMP）和系统变量（TEMP、TMP）及其相关的值。

使用下列目录

如果启用此选项，则使用输入框中显示的路径。

输入框

在此输入框中，输入程序用来存储临时文件的路径。

此按钮将打开一个窗口，可以在其中选择所需的临时路径。

默认

此按钮将还原临时路径的预定义目录。

10.8.9 有声警报

仅在专家模式中提供选项。

当 Scanner 或 Real-Time Protection 检测到病毒或恶意软件时，会在交互操作模式下响起有声警报。

您现在可以选择启用或停用有声警报，并为警报选择替代的波形文件。

> 说明
>
> Scanner的操作模式在配置中的 Scanner > 扫描 > 针对检测的操作下的配置中设置。 Real-Time Protection的操作模式在 Real-Time Protection > 扫描 > 针对检测的操作下的配置中设置。

不警告

如果启用此选项，则在 Scanner 或 Real-Time Protection 检测到病毒时不会发出有声警报。

使用 PC 扬声器 (仅交互模式)

如果启用此选项，则在 Scanner 或 Real-Time Protection 检测到病毒时会以默认信号发出有声警报。 有声警报通过 PC 的内部扬声器播放。

使用下列 WAVE 文件(仅交互模式)

如果启用此选项，则在 Scanner 或 Real-Time Protection 检测到病毒时会以所选波形文件发出有声警报。
所选波形文件通过所连接的外部扬声器播放。

波形文件

在此输入框中可以输入所选音频文件的名称和关联路径。
作为标准设置会输入程序的默认有声信号。

...

此按钮将打开一个窗口，可以在其中借助文件管理器选择所需文件。

测试

此按钮用于测试所选波形文件。

10.8.10 警报

Avira 产品为某些事件生成所谓的弹出式桌面通知，提供有关成功或失败程序序列（例如更新）的信息。 在警报中，可以启用或禁用特定事件的通知。

通过桌面通知，可以在弹出框中直接禁用通知。 可以在警报配置窗口中重新启用通知。

更新

如果最后一次更新超过 n 天则发出警报

在此框中，可以输入自上次更新以来允许经过的最大天数。
如果经过了指定的天数，则在控制中心的状态下将为更新状态显示红色的图标。

若病毒定义文件过时则显示通知

如果启用此选项，则在病毒定义文件不是最新时，您将收到警报。
在警报选项的帮助下，您可以配置在上次更新超过 n 天时警报的临时间隔。

警告 / 注意以下情况

使用的是拨号连接

如果启用此选项，则当拨号器在计算机上通过电话或 ISDN 网络建立拨号连接时，您会收到桌面通知警报。
存在这样的危险：此连接由未知的恶意拨号器建立，并且可能是收费的。
（请参阅病毒及其他 > 威胁类别：拨号器）

文件已成功更新

如果启用此选项，则在每次成功执行了更新并更新了文件时，您都会收到桌面通知。

更新失败

如果启用此选项，则在每次更新失败时您都会收到桌面通知：无法创建与下载服务器的连接或无法安装更新文件。

不需要更新

如果启用此选项，则在每次启动更新但由于您的程序是最新的而无需安装文件时，您都会收到桌面通知。

品牌和产品名称均为其各自所有者的商标或注册商标。在本手册中并未对受保护的商标特别进行标记。但这并不表示可以随意使用这些商标。

我们在编写此手册时做了大量细致的工作。但是，并不排除设计和内容中存在错误的可能。
未经 Avira Operations GmbH & Co. KG 事先书面许可，禁止对本出版物或者其中的部分内容进行复制及翻印。

如因修正错误或技术变动进行更改，恕不另行通知。

AVIRA

live free.™

© 2013 Avira Operations GmbH & Co. KG。保留所有权利。
www.avira.com