Avira AntiVir Premium

用户手册

AVIRA

商标与版权

商标

AntiVir 是 Avira GmbH 的注册商标。
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。 但这并不表示可以随意使用这些商标。

版权信息

Avira AntiVir Premium 使用了第三方提供的代码。 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 AntiVir Premium 帮助中“第三方许可”下的内容。

目录

1 简介 1

2 图标和强调字体 2

3 产品信息 3

3.1 交付范围 3
3.2 系统要求 4
3.3 授权和升级 4

4 安装和卸载 6

4.1 安装 6
4.2 更改安装 10
4.3 安装模块 11
4.4 卸载 11

5 AntiVir Premium 概述 13

5.1 用户界面和操作 13
5.1.1 控制中心 13
5.1.2 配置 15
5.1.3 任务栏图标 18
5.2 操作方法 18
5.2.1 激活产品 18
5.2.2 执行自动更新 19
5.2.3 启动手动更新 21
5.2.4 按需扫描：使用扫描配置文件扫描病毒和恶意软件 21
5.2.5 按需扫描：使用拖放操作扫描病毒和恶意软件 23
5.2.6 按需扫描：通过上下文菜单扫描病毒和恶意软件 23
5.2.7 按需扫描：自动扫描病毒和恶意软件 23
5.2.8 按需扫描：针对 Rookit 及活动恶意软件的扫描 24
5.2.9 对检测到的病毒和恶意软件做出反应 25
5.2.10 隔离:处理已隔离的文件 (*.qua) 28
5.2.11 隔离:还原隔离区中的文件 29
5.2.12 隔离:将可疑文件移到隔离区 31
5.2.13 扫描配置文件:修改或删除扫描配置文件中的文件类型 31
5.2.14 扫描配置文件:创建扫描配置文件的桌面快捷方式 31
5.2.15 事件：过滤事件 32
5.2.16 MailGuard：将电子邮件地址排除在扫描范围之外 32

6 扫描程序 35

7 更新 36

8 常见问题解答、技巧 37

8.1 相关问题帮助 37
8.2 快捷键 40
8.2.1 在对话框中 40
8.2.2 在帮助中 40

8.2.3 在控制中心中 41
8.3 Windows 安全中心 42
8.3.1 常规 42
8.3.2 Windows 安全中心和 AntiVir 程序 43
9 病毒及其他 45
9.1 扩展威胁类别 45
9.2 病毒及其他恶意软件 47
10 信息与服务 50
10.1 联系地址 50
10.2 技术支持 50
10.3 可疑文件 50
10.4 误报 51
10.5 您的反馈将会增强安全性 51
11 参考：配置选项 52
11.1 扫描程序 52
11.1.1 扫描 52
11.1.1.1. 针对检测的操作 54
11.1.1.2. 例外 56
11.1.1.3. 启发式 57
11.1.2 报告 58
11.2 Guard 59
11.2.1 扫描 59
11.2.1.1. 针对检测的操作 60
11.2.1.2. 更多操作 62
11.2.1.3. 例外 63
11.2.1.4. 启发式 65
11.2.2 ProActiv 66
11.2.2.1. Application filter:要阻止的应用程序 67
11.2.2.2. Application filter:Permitted applications（应用程序过滤器：允许的应用程序） 68
11.2.3 报告 69
11.3 MailGuard 69
11.3.1 扫描 70
11.3.1.1. 针对检测的操作 70
11.3.1.2. 其他操作 72
11.3.1.3. 启发式 72
11.3.2 常规 73
11.3.2.1. 例外 73
11.3.2.2. 缓存 74
11.3.3 报告 74
11.4 WebGuard 75
11.4.1 扫描 75
11.4.1.1. 针对检测的操作 76
11.4.1.2. 锁定的请求 77
11.4.1.3. 例外 78
11.4.1.4. 启发式 80

11.4.2 报告 81
11.5 更新 82
11.5.1 启动产品更新 82
11.5.2 重新启动设置 83
11.6 常规 84
11.6.1 威胁类别 84
11.6.2 密码 85
11.6.3 安全 86
11.6.4 WMI 87
11.6.5 代理 88
11.6.6 目录 88
11.6.7 事件 89
11.6.8 限制报告数量 89
11.6.9 有声警报 89
11.6.10 警告 90

1 简介

AntiVir 程序可针对病毒、蠕虫、特洛伊木马、广告软件、间谍软件及其他风险为计算机提供保护。在本手册中，这些风险称为病毒、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。

有关更多选项和信息，请访问我们的网站：

http://www.avira.cn

在 Avira 网站上，您可以.....

访问有关其他 AntiVir 桌面程序的信息

下载最新的 AntiVir 桌面程序

下载 PDF 格式的最新产品手册

下载免费支持和修复工具

访问我们丰富的知识库和常见问题解答以进行故障排除

访问特定于国家或地区的支持地址

Avira 团队

2 图标和强调字体

使用了以下图标：

图标/名称	说明
✓	放在必须在执行操作之前满足的条件之前。
▶	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	放在提示关键数据丢失危险的警告之前。
说明	放在链接之前，该链接指向特别重要的信息或让 AntiVir 程序更简单易用的技巧。

使用了以下强调字体：

强调字体	说明
草写体	文件名或路径数据。
	显示的软件界面元素（例如，窗口标题、窗口字段或选项框）。
粗体	单击的软件界面元素（例如，菜单项、部分或按钮）。

3 产品信息

本章包含有关购买和使用 AntiVir 产品的所有信息：

请参阅以下章节：交付范围

请参阅以下章节：系统要求

请参阅以下章节：授权

请参阅以下章节：许可证管理器

AntiVir 程序是全面而灵活的工具，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：

说明

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。请通过自动更新确保您的 AntiVir 程序是最新的。请对程序进行相应配置。

3.1 交付范围

您的 AntiVir 程序具有以下功能：

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

扫描程序（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

Guard（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，在 Windows 2000 下不可用）

MailGuard（POP3 扫描程序、IMAP 扫描程序 和 SMTP 扫描程序）对电子邮件提供针对病毒和恶意软件的永久检查。同时包括电子邮件附件检查

WebGuard，用于监视使用 HTTP 协议从 Internet 传入的数据和文件（监视端口 80、8080 和 3128）

集成隔离区管理，用于隔离和处理可疑文件

Rootkit 保护，用于检测安装在计算机系统上的隐藏恶意软件 (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）

3.2 系统要求

系统要求如下：

计算机至少需要配备 266 MHz Pentium 处理器
操作系统
Windows XP SP2（32 或 64 位）或
Windows Vista（32 或 64 位，SP 1）
Windows 7（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 256 MB RAM
Windows Vista、Windows 7 下至少需要 1024 MB RAM
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）

3.3 授权和升级

要使用 AntiVir 产品，您需要有一个许可证。因此请接受许可条款。

该许可证以激活密钥的形式提供。激活密钥是一个由字母和数字组合而成的代码，您将在购买 AntiVir 产品后收到此代码。激活密钥包含许可证的准确数据，即许可使用的程序及其有效期。

如果您是在 Internet 上购买的 AntiVir 程序，激活密钥将以电子邮件的形式发送给您，或者将在产品包装上提供此密钥。

要获得程序授权，请输入您的激活密钥以激活程序。可以在安装过程中激活产品。也可以在安装后从许可证管理器的帮助::许可证管理下激活 AntiVir 程序。

在许可证管理器中，您可以对 AntiVir 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。

以下产品升级可以通过许可证管理器自动执行：
将 Avira AntiVir Personal 升级到 Avira AntiVir Premium
将 Avira AntiVir Personal 升级到 Avira Premium Security Suite

将 Avira AntiVir Premium 升级到 Avira Premium Security Suite

4 安装和卸载

本章包含有关安装和卸载 AntiVir 程序的信息。
请参阅以下章节：安装：条件、安装类型、安装
请参阅以下章节：安装模块
请参阅以下章节：修改安装
请参阅以下章节：卸载：卸载

4.1 安装

在安装之前，请检查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 AntiVir 程序。

说明
在安装过程中，您可以选择创建还原点。还原点的用途是将操作系统重置为安装前的状态。如果要使用此选项，请确保操作系统允许创建还原点：
Windows XP：“系统属性”->“系统还原”：禁用**禁用系统还原**选项。
Windows Vista/Windows 7：“系统属性”->“计算机保护”：在**保护设置**区域中，突出显示安装系统的驱动器，然后单击**配置**按钮。在**系统保护**窗口中，启用**还原系统设置和以前版本的文件**选项。

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` 下的指定默认文件夹中。
AntiVir 程序将使用默认设置进行安装。您可以使用配置向导定义自定义设置。

用户定义

可选择安装各个程序组件（请参阅以下章节：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，可以定义 AntiVir 程序的自定义设置，并在安装完成后自动启动快速系统扫描。

开始安装之前

- ▶ 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。
- ▶ 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，在安装完成后执行更新
- ▶ 当您要激活 AntiVir 程序时，请将该程序的许可证密钥放在方便取用的位置。

说明
基于 Internet 的安装：
对于基于 Internet 的程序安装，Avira GmbH Web 服务器将提供一个安装程序，该安装程序将在安装之前加载最新的程序文件。此过程可确保安装的 AntiVir 程序包含最新的病毒定义文件。
使用安装软件包安装：
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时，没有为 AntiVir 程序提供语言选择。建议在安装之后更新病毒定义文件。

说明
为了激活产品，AntiVir 程序使用 HTTP 协议和端口 80（Web 通信）以及加密协议 SSL 和端口 443 与 Avira GmbH 服务器通信。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。

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。

安装 AntiVir 程序：

- ▶ 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

此时将显示*欢迎*...对话框。

- ▶ 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 AntiVir 程序的语言，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 GmbH 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

安装向导将打开，显示 *Avira AntiVir Premium* 对话框。

- ▶ 单击*接受*开始安装。

此时将解压安装文件。安装例程启动。

此时将显示*欢迎*...对话框。

- ▶ 单击**下一步**。

继续进行基于 Internet 的安装和使用安装软件包的安装

此时将显示包含许可协议的对话框。

▶ 确认您接受许可协议并单击**下一步**。

此时将显示*生成序列号*对话框。

▶ 如果需要，请确认在更新过程中已生成并传输了一个随机序列号，并单击**下一步**。

此时将显示*选择安装类型*对话框。

▶ 启用**快速安装**或**用户定义安装**选项。如果要创建还原点，请启用**创建系统还原点**选项。单击**下一步**确认设置。

用户定义的安装

此时将显示*选择目标目录*对话框。

▶ 单击**下一步**以确认指定的目标目录。

- 或者 -

使用**浏览**按钮选择其他目标目录，并单击**下一步**进行确认。

此时将显示*安装组件*对话框：

▶ 启用或禁用所需组件，并单击**下一步**进行确认。

如果已选择安装 ProActiv 组件，则会显示 *AntiVir ProActiv 社区*窗口。您可以选择确认加入 Avira AntiVir ProActiv 社区：如果启用此选项，则 Avira AntiVir ProActiv 会向 Avira 恶意软件研究中心发送 ProActiv 组件检测到的可疑程序的相关数据。这些数据仅用于高级在线扫描以及扩展和优化检测技术。使用**更多信息**链接可以获取有关扩展在线扫描的更多详细信息。

▶ 启用或禁用加入 AntiVir ProActiv 社区的选项，并单击**下一步**进行确认。

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**。

▶ 跳过接下来的“快速安装”部分。

快速安装

此时显示 *AntiVir ProActiv 社区*窗口。您可以选择确认加入 Avira AntiVir ProActiv 社区：如果启用此选项，则 Avira AntiVir ProActiv 会向 Avira 恶意软件研究中心发送 ProActiv 组件检测到的可疑程序的相关数据。这些数据仅用于高级在线扫描以及扩展和优化检测技术。使用**更多信息**链接可以获取有关扩展在线扫描的更多详细信息。

▶ 启用或禁用加入 AntiVir ProActiv 社区的选项，并单击**下一步**进行确认。

继续：快速安装和用户定义安装

打开许可证向导。

可通过以下方法激活程序。

– 输入激活密钥。

输入激活密钥，使用许可证激活 AntiVir 程序。

– 选择**产品测试**选项

如果选择**产品测试**，则在激活过程中将生成用于激活程序的评估许可证。您可以在一段时间段内测试 AntiVir 程序的所有功能。

说明
通过使用**有效的 hbedv.key 许可证文件**选项，可以下载有效的许可证文件。在使用有效的激活密钥激活产品的过程中，系统将会生成许可证密钥，并将此密钥保存在 AntiVir 程序的程序目录中。如果已激活产品并希望重新安装 AntiVir 程序，请使用此选项。

说明
在 AntiVir 产品的一些销售版本中，产品中已包含激活密钥。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密钥。

说明
要激活程序，需要与 Avira GmbH 服务器建立连接。在**代理设置**下，可配置通过代理服务器建立的 Internet 链接。

► 选择激活过程，并单击**下一步**进行确认。

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**

您的数据将传输到 Avira GmbH 服务器并接受扫描。您的 AntiVir 程序即通过许可证激活。

许可证数据即会显示在下一个窗口中。

► 单击**下一步**。

► 跳过下面介绍“通过选择**可用的 hbedv.key** 选项进行激活”的章节。

选择“可用的有效 hbedv.key”选项

此时将打开一个对话框，以便加载许可证文件。

► 选择包含程序许可证数据的许可证文件 hbedv.key，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

即会安装程序功能。对话框中会显示安装进度。

在下一个对话框中，可以选择是否在安装后打开自述文件以及重新启动计算机。

► 根据需要进行选择，并单击*完成*结束安装。

此时将关闭安装向导。

继续：用户定义的安装
配置向导

如果您选择用户定义的安装，则在下面一步中将打开配置向导。通过配置向导，可以定义 AntiVir 程序的自定义设置。

► 在配置向导的欢迎窗口中，单击**下一步**以开始程序配置。

通过*配置 AHeAD* 对话框，可以选择 AHeAD 技术的检测级别。所选检测级别用于扫描程序（按需扫描）和 Guard（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 AntiVir 程序的保护功能。

▶ 如果需要，可激活更多威胁类别，并单击 *下一步*继续安装。

如果您选择了 AntiVir Guard 安装模块，则将显示 *Guard 启动模式*对话框。您可以指定 Guard 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 Guard。

说明
指定的 Guard 启动模式保存在注册表中，无法通过"配置"进行更改。

▶ 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，可通过单击*完成*结束配置。

▶ 单击*完成*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。

继续：快速安装和用户定义安装

如果您在安装向导的最后部分选择了**重新启动计算机**选项，计算机将重新启动。

如果您在安装向导中选择了**显示 Readme.txt** 选项，则在重新启动计算机后将显示自述文件。

成功安装之后，建议您在控制中心中的*概述::状态*下检查程序是否是最新的。

▶ 如果需要，请执行更新以确保病毒定义文件是最新的。

▶ 然后，执行全面系统扫描。

4.2 更改安装

您可以选择对当前 AntiVir 程序安装单独添加或删除程序组件（请参阅以下章节：安装和卸载::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**选项来**更改/删除**程序。

选择 AntiVir 程序并单击**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。

4.3 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。

AntiVir Premium

此模块包含成功安装 AntiVir 程序所需的所有组件。

AntiVir Guard

AntiVir Guard 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），AntiVir 程序就会自动扫描文件。重命名文件不会触发 AntiVir Guard 扫描。

AntiVir ProActiv

ProActiv 组件可监视应用程序操作，并向用户警告可疑应用程序行为。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 组件已集成到 AntiVir Guard 中。

AntiVir MailGuard

MailGuard 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。MailGuard 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。

AntiVir WebGuard

在网上冲浪时，会使用 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，AntiVir Guard 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。WebGuard 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。

AntiVir Rootkit 防护

AntiVir Rootkit 防护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。

Shell 扩展

Shell 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“使用 AntiVir 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。

4.4 卸载

如果要从计算机中删除 AntiVir 程序，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。

卸载 AntiVir 程序（例如在 Windows XP 和 Windows Vista 中）：

- 通过 Windows **开始**菜单打开**控制面板**。
- 双击**程序**（Windows XP：**软件**）。
- 在列表中选择 AntiVir 程序，然后单击**删除**。

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**以完成卸载。

  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。

系统即会卸载 AntiVir 程序，重新启动计算机后将删除该程序的所有目录、文件和注册表项。

5 AntiVir Premium 概述

本章包含 AntiVir 程序的功能和操作概述。
请参阅以下章节：界面和操作
请参阅以下章节：操作方法

5.1 用户界面和操作

可以通过三个程序界面元素操作 AntiVir 程序：
控制中心：监视和控制 AntiVir 程序
配置：配置 AntiVir 程序
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

5.1.1 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 AntiVir 程序的保护组件和功能。

控制中心窗口分为三个区域：**菜单栏**、**导航栏**和详细信息窗口**视图**：
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该程序的信息。
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。各部分包含不同程序组件的信息及功能，按照不同活动组织在导航栏中。示例：活动*概述* - **状态**部分。

视图：此窗口显示导航区中选定的部分。根据所选部分，可以在详细信息窗口上部的栏中找到用于执行功能和操作的按钮。数据或数据对象显示在各部分的列表中。通过单击定义列表排序方式的框，可对这些列表进行排序。

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 AntiVir 程序的任务栏图标。

通过**文件**菜单中的**关闭**菜单项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。

- 或 -

▶ 通过*视图*菜单选择某个部分。

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

概述：在**概述**中，可以找到用于监视 AntiVir 程序功能的所有部分。

- 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。此外，您还可以查看您拥有的许可证是否有效。
- 在事件部分中，可以查看由特定程序模块生成的事件。
- 在报告部分中，可以查看所执行操作的结果。

本地保护：在**本地保护**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。

– 在扫描部分中，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标准选项运行扫描。同样，也可以通过手动选择（不保存）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。

– Guard 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。

在线保护：在**在线保护**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。

– MailGuard 部分显示 MailGuard 扫描过的所有电子邮件及其属性和其他统计数据。

– WebGuard 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。

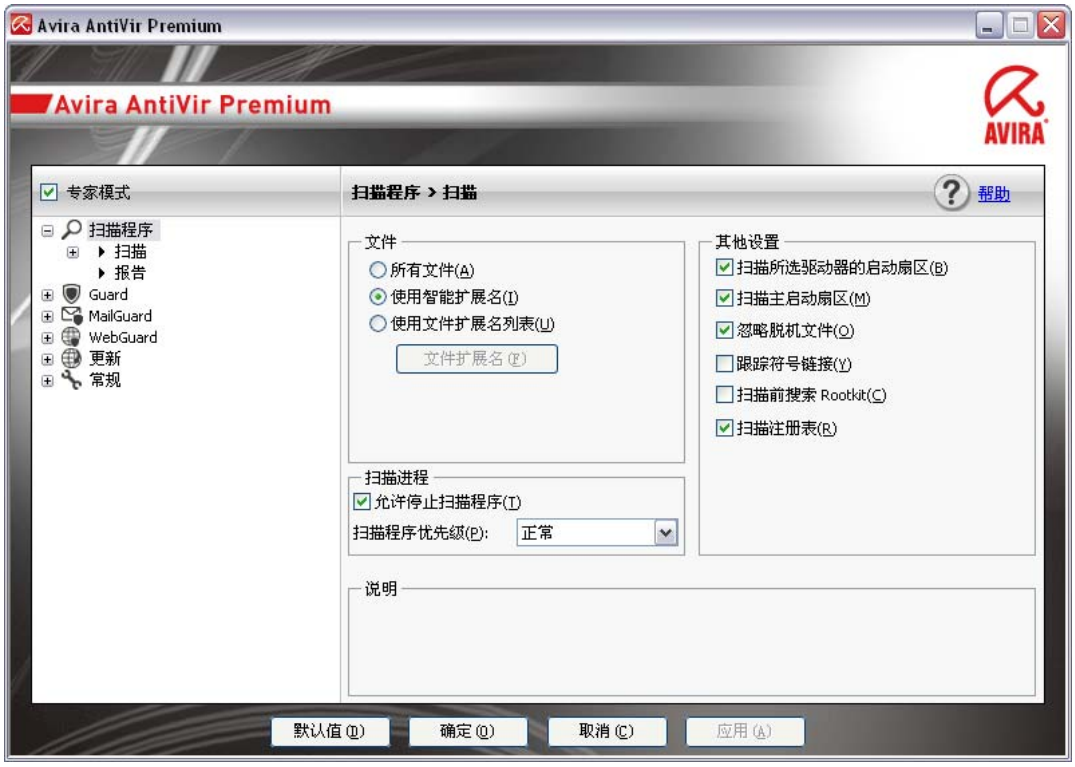
管理：在**管理**中，您将找到用于隔离和管理可疑或受感染文件的工具，以及用于规划定期执行任务的工具。

– 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，并可以调整或删除现有作业。

5.1.2 配置

在“配置”中，可以为 AntiVir 程序定义设置。安装后，AntiVir 程序配置有标准设置，可确保为您的计算机系统提供最佳保护。不过，如果计算机系统需要，或您对 AntiVir 程序有特定需求，可能意味着您需要调整该程序的保护组件。



“配置”将打开一个对话框：可以通过“确定”或“应用”按钮保存配置设置，通过单击“取消”按钮删除设置，或通过使用“默认值”按钮还原默认配置设置。可在左侧的导航栏中选择各配置部分。

访问配置

可以选择多种方法来访问配置：

通过 Windows“控制面板”。

通过 Windows 安全中心（Windows XP Service Pack 2 及以上版本）。

通过 AntiVir 程序的任务栏图标。

在 控制中心中通过附加程序 | 配置菜单项。

在 控制中心中通过配置按钮。

说明

如果要通过控制中心中的**配置**按钮访问配置，请转到控制中心中活动部分的配置注册。必须启用专家模式才能选择各配置注册。在这种情况下，会显示一个对话框，要求您启用专家模式。

配置操作

在配置窗口中导航，就像在 Windows 资源管理器中一样：

- ▶ 单击树结构中的一个条目，以在详细信息窗口中显示相应的配置部分。
- ▶ 单击条目前面的加号，展开配置部分并在树结构中显示配置子部分。
- ▶ 若要隐藏配置子部分，请单击已展开配置部分前面的减号。

说明

若要启用或禁用“配置”选项及使用按钮，也可以使用以下组合键：[Alt] + 选项名或按钮说明中带下划线的字母。

说明

只有在专家模式下才显示所有配置部分。启用专家模式可以查看所有配置部分。专家模式可用密码进行保护，密码必须在激活过程中定义。

如果要确认“配置”设置：

- ▶ 单击**确定**。

  即会关闭配置窗口并接受设置。

  - 或者 -

- ▶ 单击**接受**。

  设置得以应用。配置窗口仍处于打开状态。

如果要完成配置而不确认设置：

- ▶ 单击**取消**。

  即会关闭配置窗口并放弃设置。

如果要将所有配置设置还原为默认值：

- ▶ 单击**还原默认值**。

  所有配置设置均还原为默认值。在还原默认设置后，所有修改和自定义项都将丢失。

配置选项概述

提供了以下配置选项：

扫描程序：按需扫描配置

扫描选项

针对检测的操作

文件扫描选项

按需扫描例外

按需扫描启发式

报告功能设置

Guard：访问时扫描配置

扫描选项

针对检测的操作

访问时扫描例外

访问时扫描启发式

报告功能设置

MailGuard：MailGuard 配置

扫描选项：启用 POP3 帐户、IMAP 帐户、外发电子邮件 (SMTP) 监视

针对恶意软件的操作

MailGuard 扫描启发式

MailGuard 扫描例外

缓存配置，清空缓存

报告功能设置

WebGuard：WebGuard 配置

扫描选项，启用和禁用 WebGuard

针对检测的操作

阻止的访问：恶意文件类型和 MIME 类型、针对已知恶意 URL（恶意软件、网络钓鱼等）的 Web 过滤器

WebGuard 扫描例外：URL、文件类型、MIME 类型

WebGuard 启发式

报告功能设置

常规：

适用于按需扫描和访问时扫描的扩展风险类别

访问控制中心和“配置”的密码保护

安全：更新状态显示、系统全面扫描状态显示、产品保护

WMI：启用 WMI 支持

事件日志配置

报告功能配置

所用目录设置

更新：下载服务器连接配置，产品更新设置

组件的网络警报配置

在检测到恶意软件时发出的有声警报的配置

5.1.3 任务栏图标

安装后，任务栏的系统任务栏中会显示 AntiVir 程序的任务栏图标：

图标	说明
	AntiVir Guard 已启用，
	AntiVir Guard 已禁用，

任务栏图标显示 Guard 务的状态。

通过任务栏图标的上下文菜单可以快速访问 AntiVir 程序的核心功能。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

激活 AntiVir Guard：启用或禁用 AntiVir Guard。

启用 AntiVir MailGuard：.启用或禁用 AntiVir MailGuard。

启用 AntiVir WebGuard：启用或禁用 AntiVir WebGuard。

启动 AntiVir：打开控制中心。

配置 AntiVir：打开配置

开始更新启动更新。

帮助：打开联机帮助。

关于 AntiVir Premium：打开一个对话框，其中包含有关 AntiVir 程序的信息：产品信息、版本信息和许可证信息。

Internet 上的 Avira：打开 Internet 上的 Avira Web 门户网站。需要有活动的 Internet 连接才能执行此操作。

5.2 操作方法

5.2.1 激活产品

可通过以下方法激活 AntiVir 产品：

– 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密钥，密钥中包含您所购买的许可证的数据。激活密钥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 AntiVir 程序，使用这种许可证时，您可以在一段有限的时间内测试 AntiVir 程序的所有功能。

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 GmbH 的服务器建立连接，请检查所使用的防火墙设置：激活产品时将使用 HTTP 协议和端口 80（Web 通信）以及加密协议 SSL 和端口 443 进行连接。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。

下面介绍如何激活 AntiVir 程序：

如果尚未安装 AntiVir 程序：

▶ 安装 AntiVir 程序。

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

▶ 输入激活密钥，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。此时您的 AntiVir 程序已启用。

▶ 继续安装。

如果已安装 AntiVir 程序：

▶ 在控制中心中，选择菜单项**帮助::许可证管理**。

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。

5.2.2 执行自动更新

使用 AntiVir 计划程序创建作业以自动更新 AntiVir 程序：

▶ 在控制中心中，选择**管理::计划程序**。

▶ 单击 *使用向导创建新作业*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
建议定期和经常更新。建议的更新间隔为：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）：

– **建立 Internet 连接时也启动作业**

除按定义的频率外，建立 Internet 连接时也执行作业。

– **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：

– **最小化**：仅显示进度条
– **最大化**：显示整个作业窗口
– **隐藏**：不显示作业窗口

▶ 单击**完成**。

新建的作业即会显示在**管理器::扫描**部分的开始页面中，且处于启用状态（带复选标记）。

▶ 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：

查看作业的属性

修改作业

删除作业

启动作业

停止作业

5.2.3 启动手动更新

可使用不同方法手动启动更新：手动启动更新后，始终会更新病毒定义文件和扫描引擎。仅当激活**下载和自动安装产品更新**选项时才会进行产品更新，该选项位于“配置”中的常规::更新下

手动启动 AntiVir 程序更新：

- 右键单击任务栏中的 AntiVir 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**概述::状态**部分。
- 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。建议的更新间隔为：2 小时.

说明
您也可以通过 Windows 安全中心直接执行手动更新。

5.2.4 按需扫描：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 和 2000 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：

- 转到控制中心并选择**本地保护::扫描**。

  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，并启动按需扫描。

  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）
  - 选择目录，但不选择子目录（绿色复选标记）
  - 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 **创建新配置文件**图标。

  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）
- 选择目录，但不选择子目录（绿色复选标记）
- 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）

5.2.5 按需扫描：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：

AntiVir 程序的控制中心已打开。

- 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，并启动按需扫描。

扫描完成时将显示结果。

5.2.6 按需扫描：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 AntiVir 扫描所选文件**。

此时将显示 *Luke Filewalker* 窗口，并启动按需扫描。

扫描完成时将显示结果。

5.2.7 按需扫描：自动扫描病毒和恶意软件

说明
完成安装后，系统将会在计划程序中创建*完整系统扫描*扫描作业：完整系统扫描将以建议的时间间隔自动执行。

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：

– **最小化**：仅显示进度条
– **最大化**：显示整个作业窗口
– **隐藏**：不显示作业窗口

▶ 如果要在扫描完成时自动关闭计算机，请选择*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**。

新建的作业即会显示在*管理器::计划程序*部分的开始页面中，且处于启用状态（带复选标记）。

▶ 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：

查看作业的属性

修改作业

删除作业

启动作业

停止作业

5.2.8 按需扫描：针对 Rookit 及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 及活动恶意软件*。

系统地扫描活动的 Rootkit：

- 转到控制中心并选择**本地保护::扫描程序**。

  此时将显示预定义的扫描配置文件。

- 选择预定义的扫描配置文件**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，并启动按需扫描。

  扫描完成时将显示结果。

5.2.9 对检测到的病毒和恶意软件做出反应

对于 AntiVir 程序的各个保护组件，可以在“配置”中的*针对检测的操作*部分下定义 AntiVir 程序如何对检测到的病毒或恶意程序做出反应。

对于 Guard 的 ProActiv 组件没有可配置的操作选项：检测通知始终在 *Guard: 可疑应用程序行为*窗口中提供。

扫描程序的操作选项：

交互式

在交互式操作模式中，扫描程序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**扫描程序扫描**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，也可以取消扫描程序。

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的所选操作。

Guard 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扫描程序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::扫描程序）：

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。

MailGuard 和 WebGuard 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的所选操作。

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：针对显示在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

可选操作取决于操作系统、报告检测的保护组件（AntiVir Guard、AntiVir 扫描程序、AntiVir MailGuard 和 AntiVir WebGuard）以及检测到的恶意软件类型。

扫描程序和 Guard 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。

移到隔离区

将文件打包为特殊格式 (*.qua) 并将其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 GmbH。

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。

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。

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。

忽略

不需要进一步操作。计算机上的受感染文件仍处于活动状态。

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

用于 Guard 检测的操作选项：Guard 不需要进一步操作。允许对文件的访问。允许对文件的进一步访问，并且不再提供通知，直到重新启动计算机或更新病毒定义文件。

复制到隔离区

用于 Rootkit 检测的操作选项：将检测到的文件复制到隔离区中。

修复启动扇区 | 下载修复工具

当检测到受感染启动扇区时的操作选项：有多个选项可用于修复受感染的磁盘。如果 AntiVir 程序无法执行修复，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，则会先终止这些进程，然后再执行操作。

针对 ProActiv 组件检测的 Guard 操作（通知应用程序的可疑操作）：

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（请参阅配置::Guard::ProActiv::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（请参阅配置::Guard::ProActiv::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。

MailGuard 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

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

将受感染的附件放入隔离区，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

这样，病毒和恶意程序可以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！

MailGuard 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。

WebGuard 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

WebGuard 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
这样，病毒和恶意程序可以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，可以将这些文件上载到我们的网站：http://www.avira.cn/sample-upload
通过文件名前缀标记 *HEUR/* 或 *HEURISTIC/* 可以确定由启发式扫描报告的文件，例如：*HEUR/testfile.**。

5.2.10 隔离: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::隔离区**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 AntiVir 程序的病毒定义文件，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 。

将使用按需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*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 。

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。

▶ 选择类型：**可疑文件**或**误报**。

▶ 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，建议由 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，AntiVir 程序已将一个文件分类为可疑文件，并将它移到隔离区：在病毒检测对话框或扫描所生成的报告文件中，已提出了由 Avira 恶意软件研究中心分析该文件的建议。

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。

误报：您认为某个检测到的病毒是误报：AntiVir 程序报告在一个文件中检测到恶意软件，但该文件不太可能感染恶意软件。

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 。

此时会打开一个文本文件，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：

请参阅以下章节：隔离:还原隔离区中的文件

5.2.11 隔离: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 和 2000 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::隔离区**部分。

说明
仅当文件扩展名为 **.eml* 时，才能使用选项 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所需的图标（Windows 2000/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，才能使用选项 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。

- 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。

5.2.12 隔离: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::隔离区**部分。
- ▶ 单击 。

  此时将显示用于选择文件的 Windows 默认窗口。
- ▶ 选择文件并确认。

  该文件将移到隔离区。

可使用 AntiVir 扫描程序扫描隔离区中的文件：

- 请参阅以下章节：隔离:处理已隔离的文件 (*.qua)

5.2.13 扫描配置文件: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）：

在控制中心中，转到**本地保护::***扫描*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**添加**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 ?）代替字符。

5.2.14 扫描配置文件: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，可直接从桌面启动按需扫描，而无需访问 AntiVir 程序控制中心。

创建指向扫描配置文件的桌面快捷方式：

在控制中心中，转到**本地保护::***扫描*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。

5.2.15 事件：过滤事件

由 AntiVir 程序的程序组件生成的事件将显示在控制中心中的**概述::事件**下（与 Windows 操作系统的事件显示类似）。程序组件包括：

更新程序
计划程序
Guard
MailGuard
扫描程序
WebGuard
帮助程序服务
ProActiv

显示以下事件类型：

信息
警告
错误
检测

过滤显示的事件：

▶ 在控制中心中，选择**概述::事件**。

▶ 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。

▶ 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。

5.2.16 MailGuard：将电子邮件地址排除在扫描范围之外

定义白名单，即排除在 MailGuard 扫描范围之外的电子邮件地址（发件人）：

▶ 转到控制中心并选择**在线保护::MailGuard** 部分。

该列表显示传入电子邮件。

▶ 突出显示要排除在 MailGuard 扫描范围之外的电子邮件。

▶ 单击图标，将相应电子邮件排除在 MailGuard 扫描范围之外：

以后，不会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 MailGuard 扫描范围之外。

说明
在“配置”中的 MailGuard ::常规::例外下，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。

6 扫描程序

使用扫描程序组件，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：

通过上下文菜单进行按需扫描

在某些情况下（例如希望扫描单独的文件和目录），建议通过上下文菜单执行按需扫描（右键单击**使用 AntiVir 扫描所选文件**菜单项）。通过上下文菜单执行按需扫描的另一个优点是无需先启动控制中心。

通过拖放操作进行按需扫描

将一个文件或目录拖入控制中心的程序窗口时，扫描程序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。

通过配置文件进行按需扫描

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。

通过计划程序进行按需扫描

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 Rootkit 和活动恶意软件*扫描 Rootkit。

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**扫描引导扇区病毒**菜单命令扫描引导扇区病毒

7 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，AntiVir 中集成了更新程序组件。更新程序可确保您的 AntiVir 程序始终处于最新状态，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，AntiVir 程序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 AntiVir 程序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和扫描引擎是否最新，并在必要时执行更新。根据配置中的设置，更新程序还会执行产品更新或通知您有可用产品更新。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。

说明

出于安全考虑，更新程序会检查计算机的 Windows 主机文件是否被修改，检查更新 URL 是否被恶意软件操纵，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。

更新以下面的时间间隔自动执行：2 小时.您可以通过配置（配置::更新）编辑或禁用自动更新。

在控制中心的“计划程序”下，可创建由“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 GmbH 的下载服务器时，将默认使用现有网络连接。在常规::更新下的配置中可以更改此默认设置。

8 常见问题解答、技巧

本章包含有关 AntiVir 程序使用疑难解答及更多技巧的重要信息。

请参阅以下章节：疑难解答

请参阅以下章节：键盘命令

请参阅以下章节：Windows 安全中心

8.1 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）。

AntiVir MailGuard 不工作。

通过 TSL 连接发送的电子邮件已被 MailGuard 阻止。

Web 聊天未运行：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，而应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，请重新建立 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 得到个人防火墙的完全认可。

如果不能解决问题：

- 在“配置”（专家模式）中的常规::更新您的设置下检查设置。

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 AntiVir 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。
- 启动 AntiVir 程序和“配置”（专家模式）。
- 选择选择程序::扫描::文件::所有文件，然后使用**确定**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:AntiVir Guard 已禁用。

- 在控制中心，在 AntiVir Guard 区域的概述::状态部分中，单击**启用**链接。

原因:AntiVir Guard 已被防火墙阻止。

- 在防火墙配置中定义对 AntiVir Guard 的常规认可。AntiVir Guard 只能使用地址 127.0.0.1（本地主机）。未建立 Internet 连接。这同样适用于 AntiVir MailGuard。

如果不能解决问题：

- 检查 AntiVir Guard 服务的启动类型。如果需要，请启用该服务：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 2000 和 Windows XP 中，服务小程序位于“管理工具”子目录中）。找到 *Avira AntiVir Guard* 条目。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，AntiVir Guard 会扫描备份过程使用的所有文件。

- 在“配置”（专家模式）中选择 Guard::扫描::例外，然后输入备份软件的进程名。

在激活后，我的防火墙会立即报告 AntiVir Guard 和 AntiVir MailGuard。

原因:通过 TCP/IP Internet 协议与 AntiVir Guard 和 AntiVir MailGuard 进行通信。防火墙将会监视通过此协议建立的所有连接。

- 在防火墙配置中定义对 AntiVir Guard 和 AntiVir MailGuard 的常规认可。AntiVir Guard 只能使用地址 127.0.0.1（本地主机）。未建立 Internet 连接。这同样适用于 AntiVir MailGuard。

AntiVir MailGuard 不工作。

如果 AntiVir MailGuard 出现问题，请通过以下检查列表检查 AntiVir MailGuard 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 向服务器报告（通常也成为 TSL – 传输层安全）。AntiVir MailGuard 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 MailGuard 保护这些连接，您可以使用不受 MailGuard 监视的端口进行连接。MailGuard 监视的端口可以在 MailGuard::扫描下的配置中进行配置。
- AntiVir MailGuard 服务是否处于活动状态？如果需要，请启用该服务：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 2000 和 Windows XP 中，服务小程序位于“管理工具”子目录中）。找到 *Avira AntiVir MailGuard* 条目。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 AntiVir 程序，重新启动计算机，然后重新安装该程序。

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。当前不支持“Kerberos”和“RPA”。
- AntiVir 程序不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。

通过 TSL 连接发送的电子邮件已被 MailGuard 阻止。

原因:传输层安全（TLS：在 Internet 上传输数据的加密协议）此时不受 MailGuard 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。这将绕过 MailGuard 的监视。
- 在电子邮件客户端中关闭 TSL 加密连接并禁用 TSL 支持。
- 在 MailGuard::扫描下的配置中（临时）禁用 MailGuard 的外发电子邮件监视。

Web 聊天未运行：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，WebGuard 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，WebGuard 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”：WebGuard::例外）。

8.2 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。

8.2.1 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。
← ↑ → ↓	在各个配置部分中导航 首先，请使用鼠标将焦点设置到某个配置部分中。
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。
← ↑ → ↓	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。
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。

8.2.2 在帮助中

快捷键	说明
Alt + 空格键	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。

8.2.3 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...
返回	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
返回	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
返回	显示报告
Del	删除报告

事件部分

快捷键	说明
F3	导出事件
返回	显示事件
Del	删除事件

8.3 Windows 安全中心

- Windows XP Service Pack 2 或更高版本 -

8.3.1 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。

8.3.2 Windows 安全中心和 AntiVir 程序

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

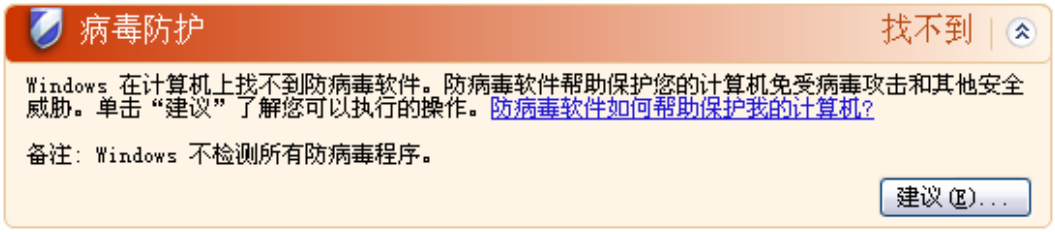
病毒防护已开启

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。

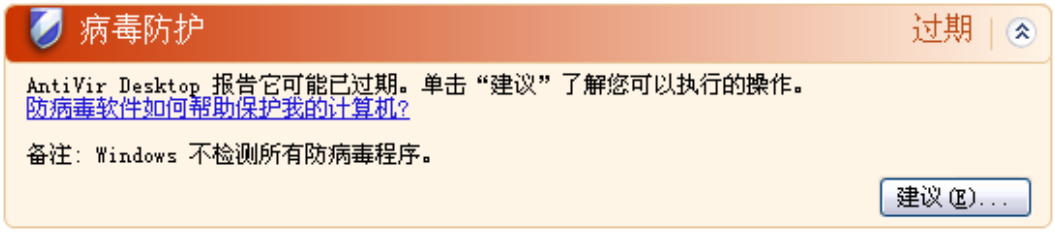


说明

在您的计算机上安装 AntiVir 程序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 Windows XP Service Pack 2 或 Windows Vista，然后再安装 AntiVir 程序；或者在已安装有 AntiVir 程序的系统上安装 Windows XP Service Pack 2 或 Windows Vista，则会收到以下消息：

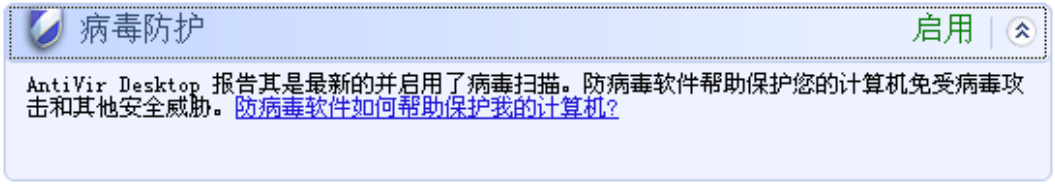


说明

为了使 Windows 安全中心将 AntiVir 程序识别为最新产品，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

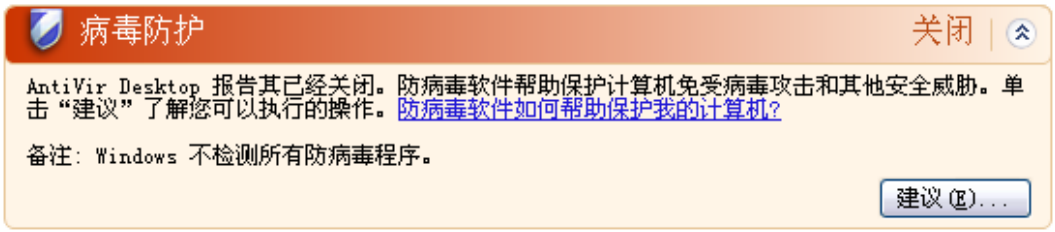
安装 AntiVir 程序并进行更新后，您会收到以下消息：



AntiVir 程序现在是最新的，并且已启用 AntiVir Guard。

病毒防护已关闭

如果禁用 AntiVir Guard 或停止 Guard 服务，则会收到以下消息。



说明

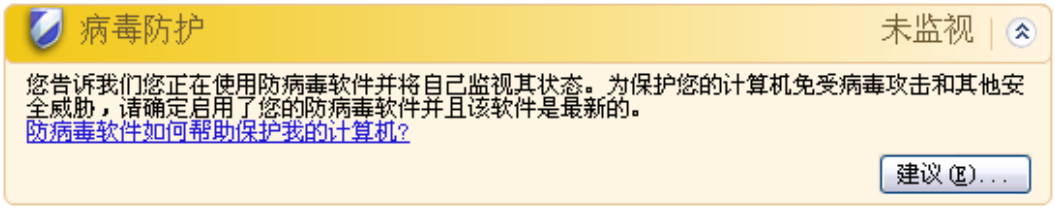
可以在控制中心的概述::状态部分中启用或禁用 AntiVir Guard。此外，如果任务栏中的红色小伞打开，也说明 AntiVir Guard 已启用。

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

AntiVir 程序支持 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 XP Service Pack 2 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，就无法针对病毒及其他恶意软件提供保护！

9 病毒及其他

9.1 扩展威胁类别

拨号器 (DIALER)

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会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，它们会换掉 Internet 用户与 ISP（Internet 服务提供商）之间的默认数据通信链接，然后，只要建立连接，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。

建议您要求电话提供商直接阻止这个号码段，从而立即防范恶意拨号器（0190/0900 拨号器）。

默认情况下，AntiVir 程序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。

游戏 (GAMES)

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越来越流行：各种游戏在大量传递，从简单的象棋到“舰队演习”（包括鱼雷战斗）：相应的游戏操作通过电子邮件程序发送给游戏伙伴，对方再对此做出回应。

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。

AntiVir 程序可识别计算机游戏。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，则在 AntiVir 程序检测到游戏时，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 (JOKES)

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。

AntiVir 程序扩展包含扫描和识别例程，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，则在检测到玩笑程序时会发出相应的警报。

安全隐私风险 (SPR)

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。

AntiVir 程序能够检测到存在“安全隐私风险”的软件。如果在扩展威胁类别下的配置中选中**安全隐私风险**选项，从而启用该选项，则在 AntiVir 程序检测到这样的软件时，会发出相应的警报。

后门客户端 (BDC)

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。

AntiVir 程序可识别“后门控制软件”。如果在扩展威胁类别下的配置中选中**后门控制软件 (BDC)** 选项，从而启用该选项，则在 AntiVir 程序检测到这样的软件时，会发出相应的警报。

广告软件/间谍软件 (ADSPY)

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。

AntiVir 程序可识别“广告软件/间谍软件”。如果在扩展威胁类别下的配置中选中**广告软件/间谍软件 (ADSPY)** 选项，从而启用该选项，则在 AntiVir 程序检测到这样的软件时，会发出相应的警报。

非常规运行时压缩程序 (PCK)

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。

AntiVir 程序可识别“非常规运行时压缩程序”。如果在扩展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，则在 AntiVir 程序检测到这样的压缩程序时，会发出相应的警报。

双扩展名文件 (HEUR-DBLEXT)

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。

AntiVir 程序可识别“双扩展名文件”。如果在扩展威胁类别下的配置中选中**双扩展名文件** (HEUR-DBLEXT) 选项，从而启用该选项，则在 AntiVir 程序检测到此类文件时，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。
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 爬网蜘蛛”窃取，然后不经您许可地用于欺诈或其他罪行。

AntiVir 程序可识别“钓鱼”。如果在扩展威胁类别下的配置中选中**钓鱼**选项，从而启用该选项，则在 AntiVir 程序检测到这样的行为时，会发出相应的警报。

应用程序(APPL)

术语 APPL 指的是使用时存在风险或来源可疑的应用程序。

AntiVir 程序可识别“应用程序 (APPL)”。如果在扩展威胁类别下的配置中选中**应用程序 (APPL)** 选项，从而启用该选项，则在 AntiVir 程序检测到这样的行为时，会发出相应的警报。

9.2 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。

启动扇区病毒

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。其中一种麻烦的结果是：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，包括发动“拒绝服务”攻击等，受感染 PC 的用户对它的存在常常不知情。僵尸网络的潜在危害主要在于，该网络可能达到数千台计算机的规模，其总带宽可以堵塞大多数常规的 Internet 访问。

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攻击。攻击者可侵入程序从而提升权限。

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。警报要求收件人发送给所有认识的同事和其他用户，以提醒每个人应对“危险”，这些警报就通过电子邮件进行扩散了。

蜜罐

蜜罐是安装在网络中的服务（程序或者服务器）。它的功能是监控网络和记录攻击。对合法的用户来说，这种服务是未知的，因此用户并不了解。如果攻击者发现网络中的薄弱环节并使用蜜罐提供的服务，蜜罐就会记录攻击行为并发出警报。

宏病毒

宏病毒是一些用应用程序的宏语言（如 WinWord 6.0 中的 WordBasic）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。与通常意义上的病毒不同，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。

多态病毒

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。

Rootkit

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：隐形存驻。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。特洛伊木马是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（多为执行破坏性功能）。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。

10 信息与服务

本章包含有关如何联系我们的信息。

请参阅以下章节：联系地址

请参阅以下章节：技术支持

请参阅以下章节：可疑文件

请参阅以下章节：误报

请参阅以下章节：提供反馈以提高安全性

10.1 联系地址

如果您对于 AntiVir 产品范围有任何疑问或要求，我们很乐意提供帮助。如需我们的联系地址，请参阅控制中心的帮助::关于 Avira AntiVir Premium。

10.2 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

为了我们能够提供快速可靠的帮助，您应当准备好以下信息：

许可证信息。可在帮助::关于 Avira AntiVir Premium::许可证信息菜单下的程序界面中找到此信息

版本信息。可在帮助::关于 Avira AntiVir Premium::版本信息菜单项下的程序界面中找到此信息。

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**。

10.3 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 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菜单项发送文件。

将必要文件以压缩形式（WinZIP、PKZip 和 Arj 等）作为电子邮件附件发送到以下地址：
vulnerabilities-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）。

您也可通过我们的网站向我们发送可疑文件：http://www.avira.cn/sample-upload

10.4 误报

当 AntiVir 程序报告在一个文件中检测到恶意软件时，如果您认为该文件很可能是“干净的”，请将相关的文件以压缩形式（WinZIP、PKZip 和 Arj 等）作为电子邮件附件发送到以下地址。
vulnerabilities-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）。

10.5 您的反馈将会增强安全性

在 Avira，客户的安全至关重要。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 GmbH 解决方案的质量和安全性，我们还非常重视与可能出现的安全漏洞有关的迹象，并会严肃对待。

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，地址为：
vulnerabilities-premium@avira.cn

11 参考：配置选项

配置参考介绍所有可用配置选项。

11.1 扫描程序

“配置”的“扫描程序”部分用于配置按需扫描。

11.1.1 扫描

您可以在此定义按需扫描的扫描例程的基本行为。如果选择某些目录进行按需扫描，则根据配置，扫描程序在扫描时可能会：
采用某种扫描强度（优先级），
也扫描启动扇区和主内存，
扫描某些或全部启动扇区和主内存，
扫描目录中的全部或所选文件。

文件

扫描程序可以使用过滤器，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。

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 AntiVir 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“No file extensions”（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，则扫描程序会扫描被选择进行按需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，则扫描程序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。

重要提示
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，则在扫描程序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。如果

跟踪符号链接

如果启用此选项，则扫描程序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。此选项不受 Windows 2000 支持并已经停用。

重要提示
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，则扫描程序会扫描 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。

重要提示
Rootkit 扫描不能在 Windows XP 64 位中使用！

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。

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，扫描程序可以区分优先级。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，操作系统才会给扫描程序分配处理器时间，即只要扫描程序在运行，速度就是最大的。总之，其他程序的工作得到优化：如果其他程序需要计算时间，则在扫描程序继续在后台运行的情况下，计算机的反应速度更快。此选项默认设置为启用，这是推荐设置。

中

扫描程序以普通优先级执行。操作系统给所有进程分配的处理器时间相同。在某些情况下可能会影响其他应用程序的工作。

高

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

11.1.1.1. 针对检测的操作

针对检测的操作

可以定义扫描程序在检测到病毒或恶意程序时所进行的操作。

交互式

如果启用此选项，则扫描程序扫描的结果显示在对话框中。如果使用扫描程序进行扫描，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，也可以取消扫描程序。

说明
在“扫描程序”通知中，默认已预先选择了“移到隔离区”操作。可以通过上下文菜单选择更多操作。

单击此处可以获得更多信息。

自动

如果启用此选项，则检测到病毒时不会显示任何对话框。扫描程序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。

备份到隔离区

如果启用此选项，则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

主操作是扫描程序发现病毒或恶意程序时所执行的操作。如果选择了**"修复"**选项但无法修复受感染的文件，则执行**"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，则扫描程序会自动修复受感染的文件。如果扫描程序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，但这意味着让扫描程序修改工作站上的文件。

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。

覆盖并删除

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

重命名

如果启用此选项，则扫描程序会重命名文件。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。

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！

隔离

如果启用此选项，则扫描程序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。

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。

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。

覆盖并删除

如果启用此选项，则扫描程序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。

重命名

如果启用此选项，则扫描程序会重命名文件。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。

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！

隔离

如果启用此选项，则扫描程序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。

说明
如果选择**删除**或**覆盖并删除**作为主操作或辅助操作，您应该注意以下方面：在启发式扫描发现病毒时，不会删除受感染的文件，而是将其移到隔离区中。

扫描存档时，扫描程序使用递归扫描：对于存档中的存档也将解压缩并扫描病毒和恶意程序。会对文件进行扫描、解压缩并重新扫描。

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，则扫描程序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。示例：如果一个 *.zip 存档的文件扩展名为 *.xyz，则扫描程序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
只支持在存档列表中标记的存档类型。

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，扫描程序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扫描程序应扫描的存档。为此，必须选择相关的项。

11.1.1.2. 例外

扫描程序要忽略的文件对象

此窗口中的列表包含扫描程序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。

说明
如果将一个完整的分区添加到文件对象列表中，则只有那些直接保存在此分区下的文件才会从扫描中排除，这不适用于相应分区上的子目录中的文件：
示例：要跳过的文件对象：`D:\` = `D:\file.txt` 将从扫描程序扫描中排除，而 `D:\folder\file.txt` 不会从扫描中排除。

11.1.1.3. 启发式

这部分配置包含扫描引擎的启发式扫描设置。

AntiVir 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

AntiVir 产品包含十分强大的宏病毒启发式扫描。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

AntiVir 程序包含十分强大的以 AntiVir 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，则会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

如果选择使用此启发式扫描，则此选项默认设置为启用。

高检测级别

如果启用此选项，则检测未知程度高得多的恶意软件，不过也可能发生误报。

11.1.2 报告

扫描程序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。

说明
为使您能够确定在检测到病毒或恶意程序时扫描程序执行了什么操作，始终应该创建报告文件。

报告

关闭

如果启用此选项，则扫描程序不报告按需扫描的操作和结果。

默认

如果启用此选项，扫描程序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。

高级

如果启用此选项，除默认信息之外，扫描程序还会记录警报和提示。

完整

如果启用此选项，扫描程序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。

11.2 Guard

配置的“Guard”部分用于配置访问时扫描。

11.2.1 扫描

您通常会希望不断监视自己的系统。为此，请使用 Guard（= 访问时扫描程序）。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。

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 Guard 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 Guard 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 Guard 会扫描文件。此选项默认设置为启用，这是推荐设置。

文件

Guard 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。

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
如果启用了智能扩展，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“**文件扩展名**”按钮手动进行编辑。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**文件扩展名**按钮下会显示提示文本“No file extensions”（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。

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，Guard 使用递归扫描：对于存档中的存档也将解压缩并扫描病毒和恶意程序。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：将对直接位于主存档内的所有存档进行扫描。

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。

11.2.1.1. 针对检测的操作

针对检测的操作

可以定义 Guard 在检测到病毒或恶意程序时所进行的操作。

交互式

如果启用此选项，则在 Guard 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中。这些操作会显示在对话框中。此选项默认设置为启用。

单击此处可以获得更多信息。

自动

如果启用此选项，则检测到病毒时不会显示任何对话框。Guard 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。

备份到隔离区

如果启用此选项，则 Guard 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。如果该副本的信息有价值，则可以从隔离区管理器将它还原。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 Guard 发现病毒或恶意程序时所执行的操作。如果选择了**"修复"**选项但无法修复受感染的文件，则执行**"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 Guard 会自动修复受感染的文件。如果 Guard 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 Guard 修改工作站上的文件。

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。

覆盖并删除

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

重命名

如果启用该选项，则 Guard 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。

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！

拒绝访问

如果启用此选项，并启用报告功能，则 Guard 仅在报告文件中输入检测结果。此外，如果启用此选项，则 Guard 会在事件日志中写入一项。

隔离

如果启用此选项，则 Guard 会将文件移到隔离区中。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。

辅助操作

只有在选择了**"主操作"**下的**"修复"**选项时，才能选择**"辅助选项"**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。

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。

覆盖并删除

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

重命名

如果启用该选项，则 Guard 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。

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！

拒绝访问

如果启用此选项，并启用报告功能，则 Guard 仅在报告文件中输入检测结果。此外，如果启用此选项，则 Guard 会在事件日志中写入一项。

隔离

如果启用此选项，则 Guard 会将文件移到隔离区中。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。

说明

如果选择**删除**或**覆盖并删除**作为主操作或辅助操作，您应该注意以下方面：在启发式扫描发现病毒时，不会删除受感染的文件，而是将其移到隔离区中。

11.2.1.1.2. 更多操作

通知

事件日志

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。

自动启动

阻止自动启动功能

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 自动启动功能。 通过 Windows 自动启动功能，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。但是，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。自动启动功能对 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 驱动器允许自动启动功能。

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 驱动器禁用自动启动功能。

11.2.1.3. 例外

通过这些选项，可以配置 Guard（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，Guard 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。
在指定要忽略的进程和文件对象时请注意以下方面：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。

Guard 要忽略的进程

对此列表中进程的所有文件访问都从 Guard 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。

说明
最多可以输入 128 个进程。

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

说明
您可以选择从 Guard 的监视范围中排除进程，而无需输入完整路径详细信息。
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。
不要为可执行文件位于动态驱动器上的进程指定任何例外。动态驱动器是指可移动磁盘，如 CD、DVD 或 USB 存储器。

说明
必须按如下方式输入驱动器信息：[驱动器号]:\
冒号 (:) 仅用于指定驱动器。

说明
在指定进程时，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
为了避免以全局方式从 Guard 的监视范围中排除进程，仅包含以下字符的规范是无效的：*（星号）、?（问号）、/（正斜杠）、\（反斜杠）、.（句点）、:（冒号）。

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

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。不会排除 Windows 资源管理器和操作系统本身。会忽略列表中相应的项。

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。

Guard 要忽略的文件对象

对此列表中对象的所有文件访问都从 Guard 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。

说明
在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）：也可以排除具体的文件扩展名（使用通配符）：
C:\Directory*.mdb
*.mdb
*.md?
.xls
C:\Directory*.log

说明
目录名必须以反斜线 \ 结束，否则视为文件名。

说明
列表中所有项的总字符数不能超过 6,000 个。

说明
如果排除一个目录，则其所有子目录也自动被排除。

说明
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

说明
如果动态驱动器挂载为另一个驱动器的目录，必须使用例外列表中的该集成驱动器所在操作系统的别名：
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 Guard 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

使用此按钮可以从显示窗口中删除所选文件对象。

在指定例外时请注意更多信息：

说明

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。

说明

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\
```

此项无效，不会作为例外处理！

说明

您可以在 Guard 报告文件中找到 Guard 用于扫描受感染文件的路径。请在例外列表中指定完全相同的路径。操作方法如下：在配置中的 Guard::报告下将 Guard 的协议功能设置为**完整**。现在通过激活的 Guard 访问文件、文件夹、装入的驱动器。然后，您就可以从 Guard 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::Guard 下访问报告文件。

排除进程示例：

application.exe

从 Guard 扫描中排除 application.exe 进程，无论该进程位于哪个硬盘驱动器以及位于哪个目录。

C:\Program Files1\Application.exe

从 Guard 扫描中排除位于路径 C:\Program Files1 下 application.exe 文件的进程。

C:\Program Files1*.exe

从 Guard 扫描中排除位于路径 C:\Program Files1 下的可执行文件的所有进程。

排除文件示例：

*.mdb

从 Guard 扫描中排除所有扩展名为“mdb”的文件

.xls

从 Guard 扫描中排除所有扩展名以“xls”开头的所有文件，例如扩展名为 .xls 和 .xlsx 的文件。

C:\Directory*.log

从 Guard 扫描中排除位于路径 C:\Directory 下所有扩展名为“log”的日志文件。

-

11.2.1.4. 启发式

这部分配置包含扫描引擎的启发式扫描设置。

AntiVir 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

AntiVir 产品包含十分强大的宏病毒启发式扫描。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

AntiVir 程序包含十分强大的以 AntiVir 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，则会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

如果选择使用此启发式扫描，则此选项默认设置为启用。

高检测级别

如果启用此选项，则检测未知程度高得多的恶意软件，不过也可能发生误报。

11.2.2 ProActiv

Avira AntiVir 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 Guard 组件中，可观察并分析所执行的程序操作。此技术会针对典型的恶意软件操作模式来检查程序的行为：操作和操作序列的类型。如果程序表现出了恶意软件的典型行为，就会进行一次病毒检测：您可以选择阻止此程序，或者忽略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。Avira AntiVir ProActiv 会将检测到的任何可疑程序的相关信息发送到 Avira 数据库中以作记录。您可以选择禁止将数据传输到 Avira 数据库中

说明

ProActiv 技术目前还不适用于 64 位系统！Windows 2000 不支持 ProActiv 组件。

常规

Enabling Avira AntiVir ProActiv（启用 Avira AntiVir ProActiv）

如果启用此选项，将对计算机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。

加入 AntiVir ProActiv 社区可增强计算机的安全性。

如果启用此选项，则 Avira AntiVir ProActiv 会向 Avira 恶意软件研究中心发送有关可疑程序的数据，并且在某些情况下，还会发送有关可疑程序文件（可执行文件）的数据，以进行高级在线扫描。经过评估后，这些数据会添加到 ProActiv 行为分析规则集中。通过这种方式，您就加入了 Avira ProActiv 社区，并对 ProActiv 安全技术的持续改进和优化作出了贡献。 如果禁用此选项，则不会发送任何数据。这对 ProActiv 功能没有任何影响。

单击此处了解更多信息。

可以通过此链接访问一个 Internet 页面，在该页面中可以获取有关高级在线扫描的详细信息。在高级在线扫描过程中传输的所有数据都包含在该 Internet 页面中。

11.2.2.1. Application filter:要阻止的应用程序

在 *Application filter:Applications to be blocked*（应用程序过滤器：要阻止的应用程序）下，可以输入要划分为有害并希望 Avira 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*选项，通过 Guard 的可疑程序行为通知将程序添加到阻止的应用程序过滤器中。

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 AntiVir ProActiv 阻止，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 AntVir 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。

11.2.2.2. Application filter:Permitted applications（应用程序过滤器：允许的应用程序）

Application filter:Permitted applications（应用程序过滤器：允许的应用程序）部分列出从 ProActiv 组件的监视范围中排除的应用程序：分类为可靠且默认包含在此列表中的已签名程序，分类为可靠且添加到此应用程序过滤器中的所有应用程序： 可以在“配置”中向此列表中添加允许的应用程序。也可以使用 Guard 通知中的**可信程序**选项，通过 Guard 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生产商的已签名应用程序。可以通过配置或通过 Guard 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，因为恶意代码可以通过更新等更改方式添加到程序中。可以根据指定的类型确定是否应该进行内容检查：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 Guard 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使用*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 AntiVir 程序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。

11.2.3 报告

Guard 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 Guard 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 Guard 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 Guard 会在报告文件中也记录次要信息。

完整

如果启用此选项，则 Guard 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：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
如果尚未指定任何报告文件限制，则在报告文件达到 100MB 时会自动创建新报告文件。会创建旧报告文件的备份。会最多保存旧报告文件的三个备份。首先删除最旧的备份。

11.3 MailGuard

“配置”的“MailGuard”部分用于配置 MailGuard。

11.3.1 扫描

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

扫描

打开 MailGuard

如果启用此选项，则 MailGuard 会监视电子邮件通信。MailGuard 是一种代理服务器，可检查您使用的电子邮件服务器与您计算机系统上的电子邮件客户端程序之间的数据通信：默认情况下会对传入电子邮件进行恶意软件扫描。 如果禁用此选项，则仍会启动 MailGuard 服务，但禁用 MailGuard 进行的监视。

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扫描。MailGuard 支持 POP3 和 IMAP 协议。使 MailGuard 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。

默认

此按钮将指定端口重置为默认的 POP3 端口。

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。

默认

此按钮将指定端口重置为默认的 IMAP 端口。

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。

默认

此按钮将指定端口重置为默认的 SMTP 端口。

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。

11.3.1.1. 针对检测的操作

这部分配置包含有关 MailGuard 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设置。

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。

针对检测的操作

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 MailGuard 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。MailGuard 会根据此部分中定义的设置作出反应。

主操作

主操作是 MailGuard 在电子邮件中发现病毒或恶意程序时所执行的操作。如果选择了选项“**忽略电子邮件**”，则还可以在“**受感染的附件**”下选择用于处理在附件中检测到的病毒或恶意程序的过程。

删除电子邮件

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。

隔离电子邮件

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。

忽略电子邮件

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：

受影响的附件

只有在选择了"**主操作**"下的"**忽略电子邮件**"设置时，才能选择"**受感染的电子邮件**"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。

隔离

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，可在以后还原受感染的附件。

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 MailGuard 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！

11.3.1.2. 其他操作

这部分配置包含有关 MailGuard 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其他设置。

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：

Strg + 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：

Strg + 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。

11.3.1.3. 启发式

这部分配置包含扫描引擎的启发式扫描设置。

AntiVir 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

启用宏病毒启发式

AntiVir 产品包含十分强大的宏病毒启发式扫描。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

AntiVir 程序包含十分强大的以 AntiVir 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，则会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

如果选择使用此启发式扫描，则此选项默认设置为启用。此选项默认设置为启用，这是推荐设置。

高检测级别

如果启用此选项，则检测未知程度高得多的恶意软件，不过也可能发生误报。

11.3.2 常规

11.3.2.1. 例外

扫描例外

此表显示从 AntiVir MailGuard 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 MailGuard 对传入电子邮件的扫描。

状态

图标	说明
	将不再对此电子邮件地址进行恶意软件扫描。

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。

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，MailGuard 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。

11.3.2.2. 缓存

缓存

MailGuard 缓存包含有关在控制中心的 MailGuard 下作为统计数据显示的已扫描电子邮件的数据。

缓存的最大电子邮件数量

此字段用于设置 MailGuard 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。

Maximum storage period of an email in days（电子邮件的最大存储天数）

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。

11.3.3 报告

MailGuard 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 MailGuard 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 MailGuard 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 MailGuard 会在报告文件中也记录次要信息。

完整

如果启用此选项，则 MailGuard 会在报告文件中记录所有信息。

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：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 MailGuard 配置。

说明

如果尚未指定任何报告文件限制，则在报告文件达到 100MB 时会自动创建新报告文件。会创建旧报告文件的备份。会最多保存旧报告文件的三个备份。首先删除最旧的备份。

11.4 WebGuard

“配置”的“WebGuard”部分用于配置 WebGuard。

11.4.1 扫描

WebGuard 能够帮助您防护通过从 Internet 加载到网页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*标题设置 WebGuard 组件的行为。

扫描

启用 WebGuard

如果启用此选项，则会对您使用 Internet 浏览器请求的网页进行病毒和恶意软件扫描。WebGuard 能够监视使用 HTTP 协议通过端口 80、8080、3128 从 Internet 传输的数据。如果检测到受感染的网页，则会阻止加载此网页。如果禁用此选项，则会保持启动 WebGuard 服务，但禁用病毒和恶意软件扫描。

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。

默认

如果启用此选项，则会阻止具有可疑内容的 I 帧。

高级

如果启用此选项，则会阻止具有可疑内容的 I 帧和使用方式可疑的 I 帧。如果 I 帧非常小并因而在浏览器中不可见或几乎不可见，或者 I 帧位于网页上不寻常的位置，则这种 I 帧使用方式将视为可疑。

11.4.1.1. 针对检测的操作

针对检测的操作

可以定义 WebGuard 在检测到病毒或恶意程序时所进行的操作。

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，可以在其中选择如何处理受感染的文件。此选项默认设置为启用。

单击此处可以获得更多信息。

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。此桌面通知是特别为下载数据量较大的网站而设计的：如果用 WebGuard 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。

自动

如果启用此选项，则检测到病毒时不会显示任何对话框。WebGuard 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 WebGuard 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，WebGuard 会将检测结果记录到报告文件中。

隔离

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参考价值，则可以从隔离区管理器恢复该文件，也可以根据需要将其发送给 Avira 恶意软件研究中心。

忽略

WebGuard 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！

11.4.1.2. 锁定的请求

在**锁定的请求**中，可以指定 WebGuard 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。WebGuard 能够阻止从 Internet 向您的计算机系统传输数据。

File types / MIME types to be blocked by WebGuard (user-defined)
（WebGuard 阻止的文件类型/MIME 类型 (用户定义)）

WebGuard 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 WebGuard 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 文件存储在您的计算机系统中并受 WebGuard 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 WebGuard::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
在输入文件类型和 MIME 类型时不能使用通配符（* 表示任何数量的字符，? 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

示例：排除的文件和 MIME 类型

`application/octet-stream` = WebGuard 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` = WebGuard 阻止应用程序/olescript MIME 类型文件（ActiveX 脚本文件 *.axs）。

`.exe` = WebGuard 阻止所有扩展名为 .exe（可执行文件）的文件。

`.msi` = WebGuard 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 WebGuard 将阻止其 URL 的内容类别。

说明

对于 WebGuard::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。“欺诈和欺骗”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。

11.4.1.3. 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 WebGuard 扫描例外。WebGuard 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。

WebGuard 跳过的 MIME 类型

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

文件类型/WebGuard 跳过的 MIME 类型 (用户定义)

WebGuard 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 WebGuard 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

在输入文件类型和 MIME 类型时不能使用通配符（* 表示任何数量的字符，? 表示单个字符）。

警告

排除列表中的所有文件和内容类型下载到 Internet 浏览器中时，WebGuard 都不会进一步进行阻止的访问扫描（WebGuard::扫描::阻止的访问中阻止的文件和 MIME 类型列表）：对于排除列表中所有的项，将会忽略那些要阻止的文件和 MIME 类型项。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

例如：排除的文件和 MIME 类型

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

WebGuard 跳过的 URL

WebGuard 扫描排除此列表中的所有 URL。

输入框

在此框中，可以输入要从 WebGuard 扫描中排除的 URL（Internet 地址），例如 **www.domainname.com**。您可以指定 URL 的一部分，使用开始或结束的句点来指示域级别：.domainname.com 表示此域的所有网页和所有子域。用结束句点表示任何顶级域（.com 或 .net）网站：domainname.。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。您也可以将开始或结束句点与通配符结合使用来表示域级别：
.domainname.*
*.domainname.com
.*name*.com（有效但不建议使用）
不包含句点的名称（例如 *name*）被视为顶级域的一部分，因此不建议使用。

警告

排除的 URL 列表中的所有网站下载到 Internet 浏览器中时，Web 过滤器或 WebGuard 都不会进一步扫描：对于排除的 URL 列表中所有的项，将忽略 Web 过滤器中的项（请参阅 WebGuard::扫描::阻止的访问）。不会进行病毒和恶意软件扫描。因此应该只将可靠的 URL 从 WebGuard 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。

例如：跳过的 URL

www.avira.com -或- www.avira.com/*

= WebGuard 扫描将排除具有域“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
WebGuard 扫描不排除具有域“www.avira.de”的 URL。

`avira.com` -或- `*.avira.com`

= WebGuard 扫描将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.`-或- `*.avira.*`

= WebGuard 扫描将排除具有二级域“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*.*`

= WebGuard 扫描将排除其二级域包含字符串“domain”的所有 URL：www.domain.com、www.new-domain.de、www.sample-domain1.de ...

`net` -或- `*.net`

= WebGuard 扫描将排除具有顶级域“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 WebGuard 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 WebGuard 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

11.4.1.4. 启发式

这部分配置包含扫描引擎的启发式扫描设置。

AntiVir 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

AntiVir 产品包含十分强大的宏病毒启发式扫描。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

AntiVir 程序包含十分强大的以 AntiVir 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，则会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

如果选择使用此启发式扫描，则此选项默认设置为启用。

高检测级别

如果启用此选项，则检测未知程度高得多的恶意软件，不过也可能发生误报。

11.4.2 报告

WebGuard 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 WebGuard 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 WebGuard 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 WebGuard 会在报告文件中也记录次要信息。

完整

如果启用此选项，则 WebGuard 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：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少 20%。

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
如果尚未指定任何报告文件限制，则在报告文件达到 100MB 时会自动删除旧项。会一直删除项，直至报告文件的大小达到 80 MB。

11.5 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，也可以启用或停用自动更新。

自动更新

启用

如果启用此选项，将按照指定的时间间隔，为启用的事件执行自动更新。

Automatic update every n days/hours/minutes（每隔 n 天/小时/分钟进行自动更新）

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。

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。

11.5.1 启动产品更新

在**产品更新**下，配置如何处理产品更新或可用产品更新的通知。

产品更新

自动下载和安装产品更新

如果启用此选项，则只要有产品更新，更新组件就会下载并自动安装。病毒定义文件和扫描引擎的更新不受此设置的影响。此选项的条件是：对更新进行了完全配置并与下载服务器有开放连接。

下载产品更新。如果需要重新启动，则在系统重新启动后安装更新；否则将立即安装。

如果启用此选项，则只要有产品更新，就会进行下载。如果不需要重新启动，则在下载完更新文件之后，会自动安装此更新。如果产品更新要求您重新启动计算机，则在下一次用户控制重新启动系统之后执行此更新，而不是在下载完更新文件之后立即执行。这样做，当用户在其计算机上工作时，就不会受到重新启动的打扰。病毒定义文件和扫描引擎的更新不受此设置的影响。此选项的条件是：对更新进行了完全配置并与下载服务器有开放连接。

Notification when new product updates are available（有新的产品更新时发出通知）

如果启用此选项，则在有新产品更新时会用电子邮件通知您。病毒定义文件和扫描引擎的更新不受此设置的影响。此选项的条件是：对更新进行了完全配置并与下载服务器有开放连接。您会通过桌面弹出窗口收到更新程序的通知，控制中心的“概述::事件”下也会收到更新程序的警报。

Notify again after n day(s)（在 n 天后再通知一次）

在此框中输入天数，如果在首次通知之后没有安装产品更新，则经过此天数后将再次通知您有可用的产品更新。

不下载产品更新

如果启用此选项，则更新程序不会自动进行产品更新，也不会通知有产品更新可用。病毒定义文件和搜索引擎的更新不受此设置的影响。

重要提示

每次更新时都会更新病毒定义文件和搜索引擎，这不受产品更新设置的影响（请参阅更新一章）。

说明

如果您启用了某个自动产品更新选项，则可以在重新启动设置下进一步配置重新启动通知和取消选项。

11.5.2 重新启动设置

当 AntiVir 程序进行产品更新时，可能必须重新启动计算机系统。如果您在常规::更新::产品更新下选择了自动产品更新，则可以在**重新启动设置**下选择不同的重新启动通知和重新启动取消选项。

说明

请注意，如果常规::更新::产品更新下的配置中要求重新启动计算机，则重新启动设置将允许您从两种执行产品更新的选项中进行选择。

当更新可用时自动执行需要重新启动计算机的产品更新：当用户在计算机上工作时执行更新和重新启动。 如果启用此选项，选择具有取消选项或提醒功能的重新启动例程可能会很有帮助。

在下一次重新启动系统时执行需要重新启动计算机的产品更新：在用户启动了计算机并登录后执行更新和重新启动。对于此选项，建议选择自动重新启动例程。

重新启动设置

Restart the computer after n seconds（在 n 秒后重新启动计算机）

如果启用此选项，则在执行完产品更新后的指定时间间隔时**自动**执行必需的重新启动。将显示一条倒计时消息，并且没有可取消计算机重新启动的选项。

Reminder message for restart every n seconds（每隔 n 秒显示一次重新启动的提示消息）

如果启用此选项，则在执行完产品更新后**不会**自动执行必需的重新启动。在指定的时间间隔后，您会收到无取消选项的重新启动通知。这些通知让您确认计算机重新启动，或者选择**“再次提醒我”**选项。

询问是否应重新启动计算机

如果启用此选项，则在执行完产品更新后**不会**自动执行必需的重新启动。您只会收到一条消息，其中提供了选项用于直接执行重新启动或取消重新启动例程。

重新启动计算机而不进行询问

如果启用此选项，则在执行完产品更新后**自动**执行必需的重新启动。您不会收到任何通知。

可以直接通过 Internet 上的 Web 服务器进行更新。

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

更新程序当前尚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 RDT 连接。

说明

在 Vista 下不提供此选项。在 Vista 下，每当完成更新后都会立即终止为更新而建立的拨号连接。

11.6 常规

11.6.1 威胁类别

所选的威胁类别

AntiVir 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。

后门客户端 (BDC)

拨号器 (DIALER)

游戏 (GAMES)
玩笑程序 (JOKES)
安全隐私风险 (SPR)
广告软件/间谍软件 (ADSPY)
非常规运行时压缩程序 (PCK)
双扩展名文件 (HEUR-DBLEXT)
钓鱼
应用程序(APPL)

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。

11.6.2 密码

可以使用密码在不同区域中保护 AntiVir 程序。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”。

Confirm password（确认密码）

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

AntiVir 可以用密码保护个别区域。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 Guard	如果启用此选项，则启用或禁用 AntiVir Guard 时需要预定义的密码。
启用/停用 MailGuard	如果启用此选项，则启用/禁用 MailGuard 时需要预定义的密码。
启用/停用 WebGuard	如果启用此选项，则启用/禁用 WebGuard 时需要预定义的密码。
隔离	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。
重新扫描受感染的对象	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。
启用专家模式	如果启用此选项，则启用专家模式时需要预定义的密码。
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。

11.6.3 安全

更新

Alert if last update older than n day(s)（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。如果经过了此天数，则在控制中心的“状态”下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。

产品保护

说明
如果未使用用户定义的安装选项安装 Guard，则产品保护选项不可用。

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（例如通过任务管理器）“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，则程序的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。

重要提示
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表项和所有程序文件（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，如果启用此选项，则对受特定类型恶意软件感染的计算机的修复可能会失败。

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）。

重要提示
文件和注册项保护不适用于 Windows XP 64 位！

11.6.4 WMI

Windows Management Instrumentation 支持

Windows Management Instrumentation 是一种基本的 Windows 管理方法，这种方法使用脚本和编程语言提供对 Windows 系统设置的本地和远程读写访问。AntiVir 程序通过接口支持 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 为您提供了选项，用于从程序下载操作数据

启用 WMI 支持

如果启用此选项，则可以通过 WMI 从程序下载操作数据。

11.6.5 代理

代理服务器

不使用代理服务器

如果启用此选项，则您与 Web 服务器的连接不会通过代理服务器建立。

使用 Windows 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::局域网设置**下将 Windows 系统设置配置为使用代理服务器。也可以访问 Internet Explorer 的“附加程序”菜单中的“Internet 选项”。

警告

如果使用需要身份验证的代理服务器，请在选项*使用此代理服务器*下输入所有所需数据。*使用 Windows 系统设置*选项只能用于不使用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

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

输入用于登录代理服务器的用户名。

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

11.6.6 目录

临时路径

在此输入框中，输入程序用来存储临时文件的路径。

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

可以在以下路径（以 Windows XP 为例）看到系统保存临时文件的位置：开始/设置/控制面板/系统/“高级”索引卡/“环境变量”按钮。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。

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。

11.6.7 事件

事件数据库大小限制

Limit maximum number of events to n entries（将最大事件数限制为 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。

Delete events older than n day(s)（删除早于 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 到 90 天。此选项默认设置为启用，默认值为 30 天。

Do not limit size of event database (delete events manually)（不限制事件数据库大小 (手动删除事件)）

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。

11.6.8 限制报告数量

限制报告数量

Limit the number to n units（将数量限制为 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。

Delete all reports more than n day(s) old（删除所有超过 n 天的报告）

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 到 90 天。此选项默认设置为启用，默认值为 30 天。

Do not limit number of reports (manually delete reports)（不限制报告数量 (手动删除报告)）

如果启用此选项，则不限制报告数量。

11.6.9 有声警报

有声警报

当扫描程序或 Guard 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
扫描程序的操作模式在配置中的扫描程序::扫描::针对检测的操作下设置。Guard 的操作模式在配置中的Guard::扫描::针对检测的操作下设置。

不警告

如果启用此选项，则在扫描程序或 Guard 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，则在扫描程序或 Guard 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 WAV 文件 (仅交互模式)

如果启用此选项，则在扫描程序或 Guard 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。

11.6.10 警告

AntiVir 程序为特定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*警告*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。在*警告*中可以取消禁用通知。

警告

在使用拨号连接时

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）。

在成功更新文件时

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。

在更新失败时

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。更新失败的原因可能是无法与下载服务器创建连接，或无法安装更新文件。

无需更新

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。

© Avira Operations GmbH & Co. KG。保留所有权利。

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。

2011 年第 3 季度发行

AVIRA

live free.™

© 2011 Avira Operations GmbH & Co. KG. All rights reserved
www.avira.com