AVG 9.0 Email Server Edition

用户手册

文档修订 **90.4 (31. 3. 2010)**

目录

1. 简介

本用户手册就是全面的 **AVG 9.0 Email Server Edition** 文档。

祝贺您购买 **AVG 9.0 Email Server Edition**!

AVG 9.0 Email Server Edition 是一系列屡获殊荣的 AVG 产品之一，旨在全面保护 PC，让用户高枕无忧。与所有其它 AVG 产品一样，**AVG 9.0 Email Server Edition** 经过了彻头彻尾的重新设计，以一种更具用户友好性、更高效的新方式提供 AVG 享有盛名、备受信赖的安全保护。

AVG 旨在保护您的计算和网络活动。请尽享 AVG 的全面保护。

注意：本文档中有特定 E-mail Server Edition 的特性说明。如果需要了解有关其它 AVG 特性的信息，请参阅 Internet Security 版用户指南，其中有全部所需详细信息。可从 http://www.avg.com 下载该指南。

2. AVG 安装要求

2.1. 支持的操作系统

AVG 9.0 Email Server Edition 意在保护在以下操作系统中运行的电子邮件服务器：

- Windows 2008 Server Edition（x86 和 x64）
- Windows 2003 Server（x86 和 x64）SP1
- Windows 2000 Server SP4 + 更新汇总 1

2.2. 受支持的电子邮件服务器

支持以下电子邮件服务器：

- ***MS Exchange 2000 Server Service Pack 1 或更高版本***

  注意： 对于 Exchange 2000 Server，必须先应用 Service Pack 1 或更高版本，然后才能使用 AVG engine；**AVG for MS Exchange 2000/2003 Server** 采用 VSAPI 2.0（或者 2.5 和 Exchange 2003 Server）应用程序接口（Service Pack 1 中有该接口）。

- ***MS Exchange 2003 Server***
- ***MS Exchange 2007 Server***
- ***MS Exchange 2010 Server***
- ***AVG for Kerio MailServer*** – 6.7.2 和更高版本

2.3. 硬件要求

针对 **AVG 9.0 Email Server Edition** 的最低硬件要求是：

- Intel Pentium CPU 1.5 GHz
- 500 MB 可用硬盘空间（用于安装）
- 512 MB RAM 内存

针对 **AVG 9.0 Email Server Edition** 的推荐硬件要求是：

- Intel Pentium CPU 1.8 GHz
- 600 MB 可用硬盘空间（用于安装）
- 512 MB RAM 内存

2.4. 卸载早期版本

如果您安装了旧版的 AVG Email Server，则需要手动卸载它，然后才能安装 **AVG 9.0 Email Server Edition**。必须使用标准的 Windows 功能手动卸载这一早期版本。

- 在 *"开始"/"设置"/"控制面板"/"添加或删除程序"* 菜单中，从已安装软件列表中选择相应的程序。请务必选择正确的 AVG 程序进行卸载。在卸载 AVG File Server Edition 之前，需要先卸载 Email Server Edition。
- 在卸载 Email Server Edition 之后，您可以继续卸载 AVG File Server Edition 的早期版本。您可以通过 *"开始"/"所有程序"/"AVG"/"卸载 AVG"*
- 如果您先前使用的是 AVG 8.x 或更早的版本，请不要忘记还要卸载单个服务器插件。

  注意：有必要在卸载过程中重新启动存储服务。

  "Exchange 插件" - 在安装了插件的文件夹中运行带有 /uninstall 参数的 setupes.exe。

  如 C:\AVG4ES2K\setupes.exe /uninstall

  "Lotus Domino/Notes 插件" - 在安装了插件的文件夹中运行带有 /uninstall 参数的 setupln.exe。

  如 C:\AVG4LN\setupln.exe /uninstall

2.5. MS Exchange Service Pack

由于 **AVG for MS Exchange 2000/2003 Server** 使用的是 VSAPI 2.0/2.5 病毒扫描界面，因此必须在您的系统上使用 MS Exchange 2000 Server Service Pack 1 或更高版本。请访问以下链接获取 MS Exchange 2000 Server Service Pack 最新版本：

MS Exchange 2000 Server Service Pack:

http://www.microsoft.com/technet/prodtechnol/exchange/downloads/2000/sp3/default.mspx

MS Exchange 2003 Server 不需要使用任何附加的 Service Pack，但是，建议您尽可能使用最新的 Service Pack 和修补程序来更新自己的系统，以确保获得最佳的安全保护。

MS Exchange 2003 Server Service Pack（可选）：

http://www.microsoft.com/exchange/evaluation/sp2/overview.mspx

在开始安装时，会检查所有系统库版本。如果需要安装更新的库，安装程序会使用 .delete 扩展名来重命名旧库。这些旧库会在重新启动系统后被删除。

MS Exchange 2007 Server Service Pack（可选）：

http://www.microsoft.com/downloads/details.aspx?FamilyID=44c66ad6-f185-4a1d-a9ab-473c1188954c&displaylang=en

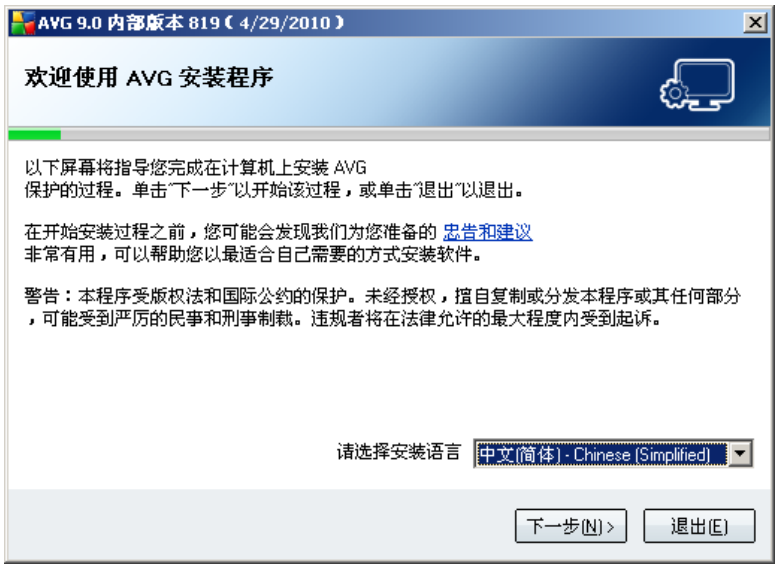
3. AVG 安装过程

若要将 AVG 安装到您的计算机上，您需要获得最新的安装文件。您可以使用您的盒装版所含光盘中的安装文件，但此文件可能已过时。因此我们建议在线获取最新的安装文件。可从 AVG 网站 (http://www.avg.com/download?prd=msw) 下载安装文件。

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

将安装文件下载并保存到您的硬盘驱动器上之后，您就可以启动安装过程。安装过程就是一系列对话框窗口，各个窗口中显示了有关每一步该如何操作的简短说明。下面，我们提供了对各个对话框窗口的说明：

3.1. 启动安装



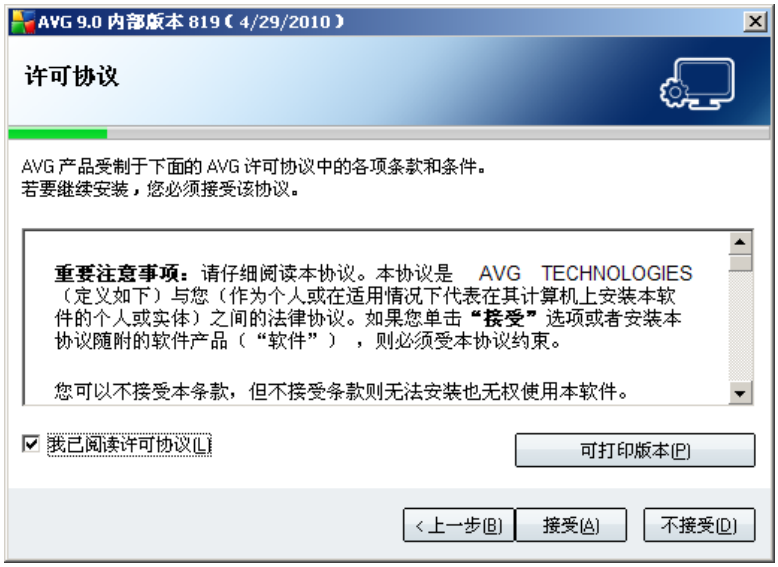
开始安装时会显示"*欢迎*"窗口。在此窗口中您需要选择要在此安装过程中使用的语言。在此对话框窗口的下部，可以找到"*选择您的安装语言*"项，请从相应的下拉菜单中选择所需的语言。接下来请按"*下一步*"按钮进行确认，然后接着按下一对话框的说明操作。

注意：稍后在安装过程中，也能为应用程序界面选择其它语言。

3.2. 许可协议

*"许可协议"*对话框提供了 AVG 许可协议的全文。请仔细阅读，然后通过选中*"我已阅读许可协议"*复选框并按*"接受"*按钮确认您已阅读、理解并接受此协议。如果您不同意此许可协议，请按*"不接受"*按钮，安装过程会立刻终止。

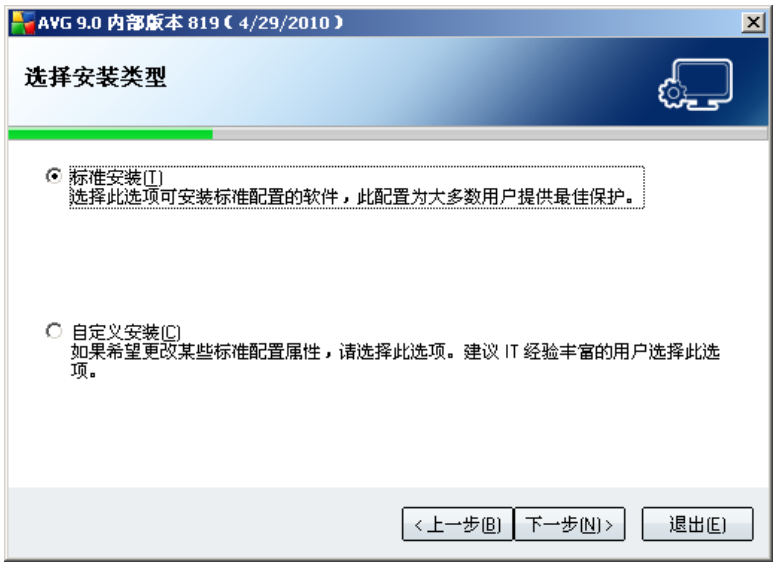
使用*"可打印版本"*按钮在另一适于打印的窗口中打开许可协议。



3.3. 正在检查系统状态

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

3.4. 选择安装类型



*"选择安装类型"*对话框提供了以下两个安装选项供您选择：*标准安装*和*自定义安装*。

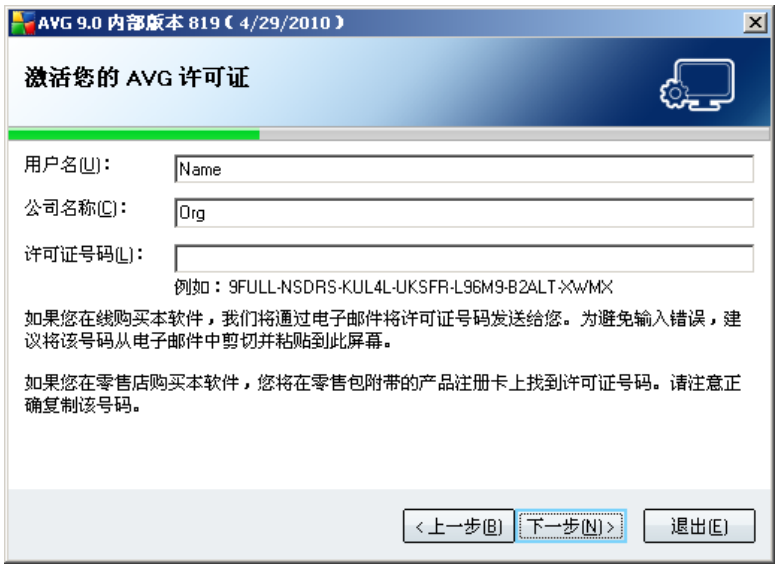
对于大多数用户而言，强烈建议执行*标准安装*，该安装方式会采用程序供应商预定义的设置以完全自动的方式安装 AVG。这种配置可提供最佳的安全性，同时又会使资源得到最优利用。今后如果需要更改配置，您始终都可以直接在 AVG 应用程序中完成。

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

3.5. 激活 AVG

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

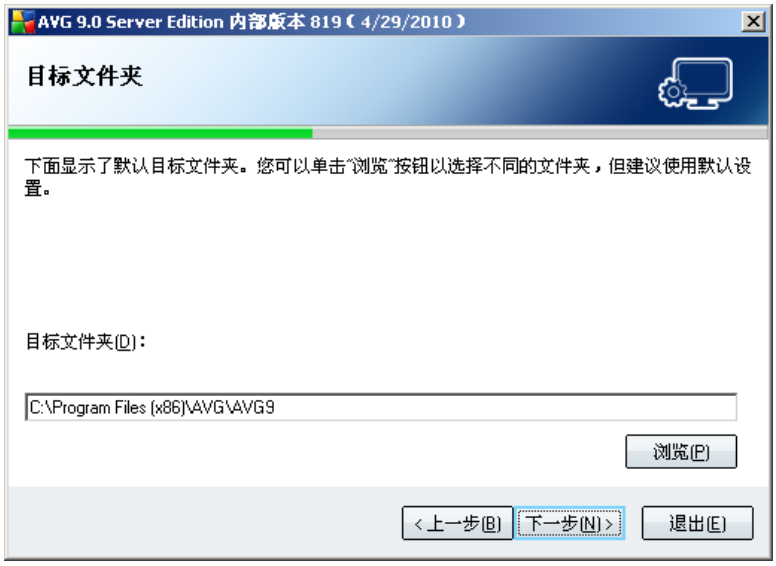
然后，在*"许可证号码"*文本字段中输入您的许可证号码。许可证号码将在您在线购买 AVG 之后通过确认电子邮件发送给您。您必须完全按照如图所示键入号码。如果存在数字形式的许可证号码（在电子邮件中），建议使用复制和粘贴方法插入它。



按"*下一步*"按钮继续执行安装过程。

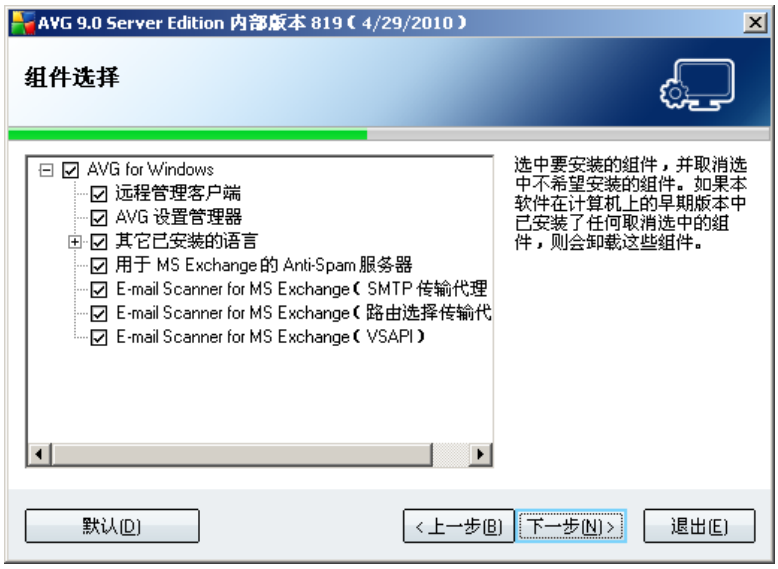
如果在上一步中您选择的是标准安装，则系统会直接重定向到"*安装摘要*"对话框中。如果您选择的是自定义安装，则接下来显示的将是"*目标文件夹*"对话框。

3.6. 自定义安装 - 目标文件夹



在"*目标文件夹*"对话框中，您可以指定应将 AVG 安装到的位置。默认情况下，AVG 会被安装到 C: 驱动器上的"Program Files"文件夹中。如果您要更改此位置，请使用"*浏览*"按钮来显示驱动器结构，然后选择相应的文件夹。按"*下一步*"按钮以确认。

3.7. 自定义安装 - 组件选择



"*组件选择*"对话框显示了可以安装的所有 AVG 组件的概览。如果默认设置不适合您，您可以删除/添加特定的组件。

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

- ***Remote Administration*** *组件* - 如果想要将 AVG 连接到一个 AVG DataCenter (AVG Network Edition)，则需要选中此选项。

  注意：只能远程管理列表中提供的服务器组件！

- ***AVG Settings Manager*** - 一个主要适用于网络管理员的工具，用于复制、编辑和分发 AVG 配置。可将配置保存到便携设备（USB 闪存驱动器等）中，然后可通过手动或其它方法应用到所选的工作站。

- *其它安装语言* - 您可以指定应该安装的 AVG 安装语言。选中"*其它安装语言*"项，然后从相应的菜单中选择所需的语言。

各个服务器组件的基本概述：

- ***Anti-Spam Server for MS Exchange***

  可检查所有传入的电子邮件并将不需要的电子邮件标记为"垃圾邮件"。它采用多种分析方法来处理每一封电子邮件，可在最大程度上阻止不需要的电子邮件。

- ***E-mail Scanner for MS Exchange（路由选择传输代理）***

  可检查通过 MS Exchange HUB 角色路由的所有传入、传出和内部电子邮件。

  可用于 MS Exchange 2007，并且仅在使用 HUB 角色时才安装。

- ***E-mail Scanner for MS Exchange（SMTP 传输代理）***

  可检查所有通过 MS Exchange SMTP 接口传送的电子邮件。

  仅适用于 MS Exchange 2007，并且在使用 EDGE 和 HUB 角色时均可安装。

- ***E-mail Scanner for MS Exchange (VSAPI)***

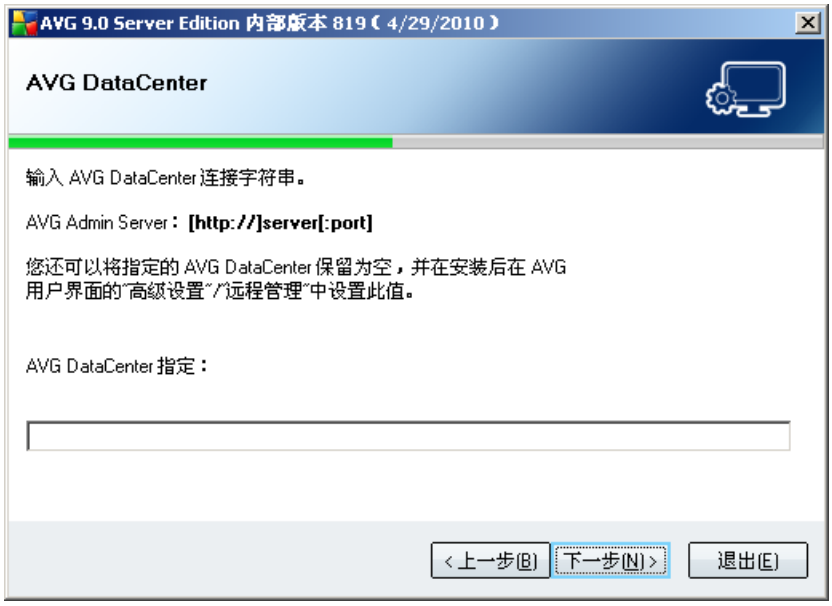
  可检查所有存储在用户邮箱中的电子邮件。如果检测到病毒，则会将其移至病毒库中或完全删除。

注意：有多个适用于 MS Exchange 2007 和 MS Exchange 2003 的不同选项。

按"*下一步*"按钮以继续。

3.8. 自定义安装 - DataCenter

如果您在模块选择过程中选中了*远程管理组件*模块，则可以在此屏幕中定义用于连接到 AVG DataCenter 的连接字符串。

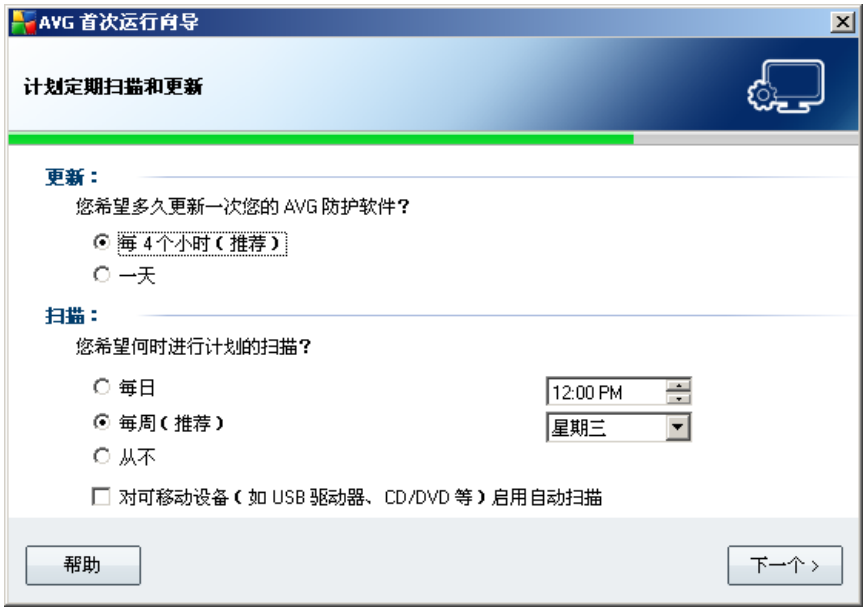


3.9. 安装

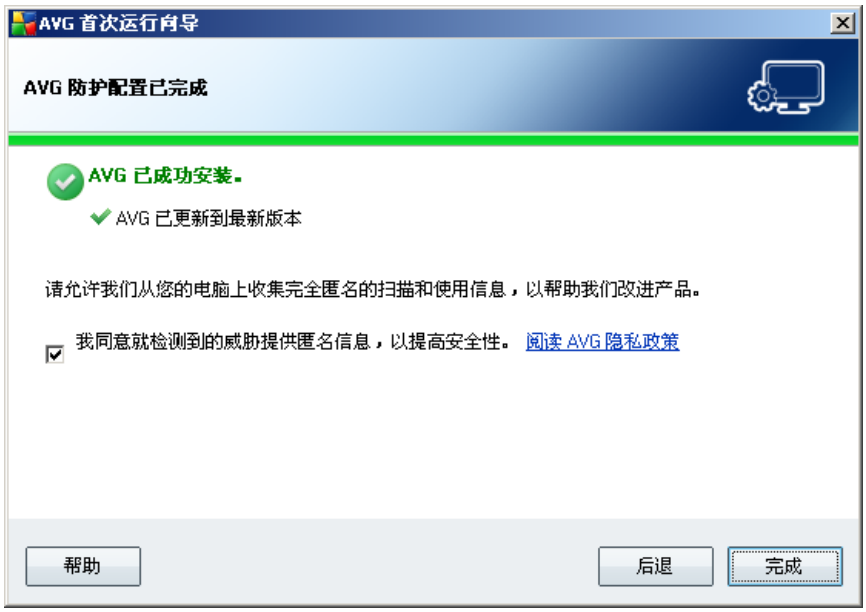
"*正在安装*"对话框用于显示安装过程的进度，不需要进行任何干预。请等待安装过程完成，然后系统会将您重定向到"*安装完成*"对话框。

3.10. 完成安装

"首次运行向导"会在安装过程中自动启动，必须执行几个简单的步骤以填写信息，然后才能结束安装：

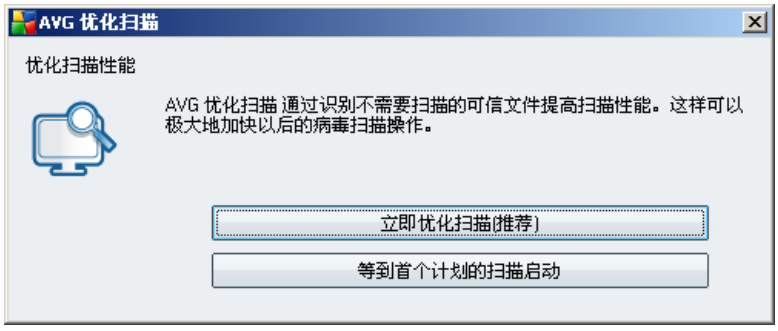


在"*计划定期扫描和更新*"对话框中，请设置检查是否有新的更新文件可用的时间间隔，并定义应启动计划的扫描的时间。建议保留默认值。按"*下一步*"按钮以继续。



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

会又显示一个**"*AVG 优化扫描*"**对话框。扫描优化功能用于搜索已从中检测到相应文件（*目前包括 *.exe、*.dll 和 *.sys 文件*）的*"Windows"*和*"Program Files"*文件夹，以及保存有关这些文件的信息。下次访问时不会再对这些文件进行扫描，这样会大幅缩短扫描时间。



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

AVG 现已被安装到您的计算机上并且可完全正常运行。此程序正以完全自动模式在后台运行。

要对电子邮件服务器逐一设置保护措施，请按相应章节操作：

- ***E-mail Scanner for MS Exchange Server 2007/2010***
- ***E-mail Scanner for MS Exchange Server 2000/2003***
- ***AVG for Kerio MailServer***

4. E-mail Scanner for MS Exchange Server 2007/2010

4.1. 概述

AVG for MS Exchange Server 2007 配置选项作为服务器组件完全集成在 AVG 9.0 Email Server Edition 中。

各个服务器组件的基本概述：

- ***Anti-Spam - Anti-Spam Server for MS Exchange***

  可检查所有传入的电子邮件并将不需要的电子邮件标记为"垃圾邮件"。它采用多种分析方法来处理每一封电子邮件，可在最大程度上阻止不需要的电子邮件。

- ***EMS（路由选择）- E-mail Scanner for MS Exchange（路由选择传输代理）***

  可检查通过 MS Exchange HUB 角色路由的所有传入、传出和内部电子邮件。

  可用于 MS Exchange 2007，并且仅在使用 HUB 角色时才安装。

- ***EMS (SMTP) - E-mail Scanner for MS Exchange（SMTP 传输代理）***

  可检查所有通过 MS Exchange SMTP 接口传送的电子邮件。

  仅适用于 MS Exchange 2007，并且在使用 EDGE 和 HUB 角色时均可安装。

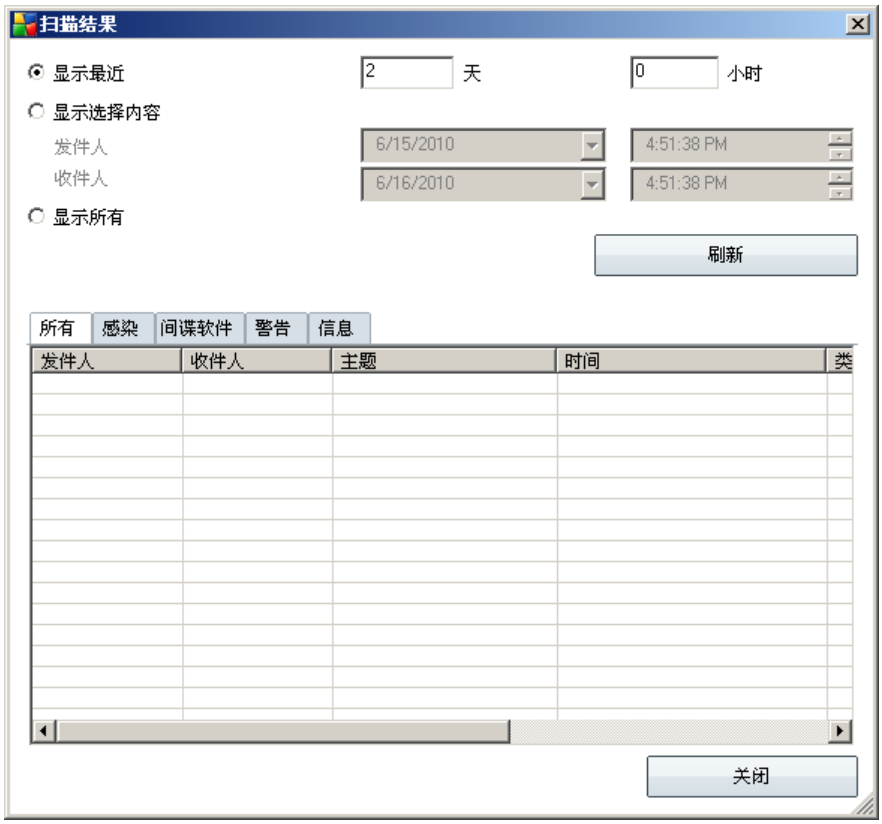
- ***EMS (VSAPI) - E-mail Scanner for MS Exchange (VSAPI)***

  可检查所有存储在用户邮箱中的电子邮件。如果检测到病毒，则会将其移到病毒库中或完全删除。

双击所需的组件以打开其界面。所有组件均可共享以下常用控制按钮和链接，但 Anti-Spam 组件除外：

- *扫描结果*

  会打开一个新对话框，您可以从中查看扫描结果：



您可以在此查看划分到不同选项卡中的消息，这些选项卡是根据消息的严重性来划分的：有关修改严重性和报告的信息，请参见各个组件的配置。

默认情况下，仅会显示前两天的扫描结果。通过修改以下选项可更改显示期限：

- *显示前* - 可插入所选天数和时数。
- *显示选择内容* - 可选择自定义时间和日期间隔。
- *显示所有* - 可显示整个时段的扫描结果。

可用*"刷新"*按钮重新加载扫描结果。

- *刷新统计值* - 可更新上面显示的统计数据。
- *重置统计值* - 可将所有统计数据重置为零。

功能按钮包括：

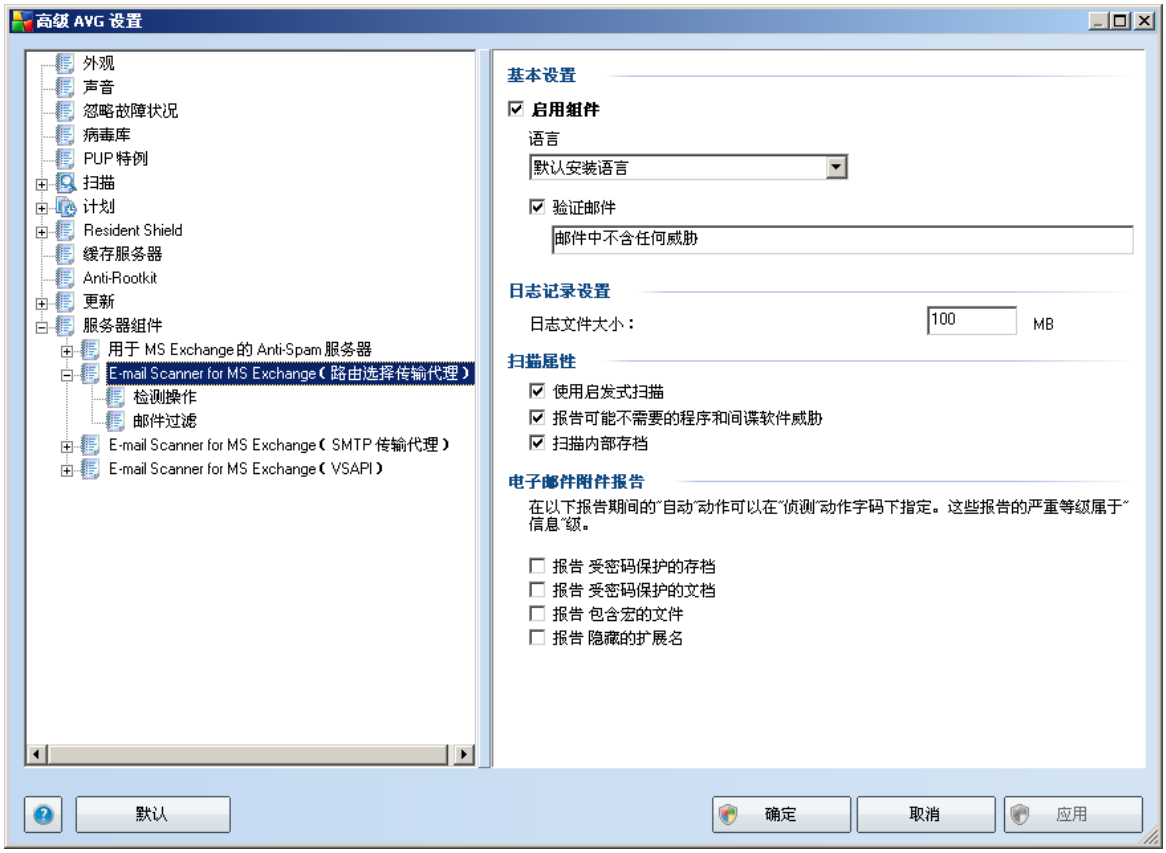
- *设置* - 可用此按钮打开组件设置。
- *后退* - 按此按钮可返回到"服务器组件概述"。

您将会在以下章节找到更多有关所有组件不同设置的信息。

4.2. E-mail Scanner for MS Exchange（路由选择传输代理）

要打开 ***E-mail Scanner for MS Exchange（路由选择传输代理）*** 设置，请从该组件的界面中选择"*设置*"按钮。

在"*服务器组件*"列表中，选择"***E-mail Scanner for MS Exchange（路由选择传输代理）***"列表项：



"*基本设置*"部分中有以下选项：

- *启用组件* - 取消选中状态可禁用整个组件。
- *语言* - 用于选择最合意的组件语言。
- *验证邮件* - 如果要向所有扫描过的邮件中添加验证说明，请选中此选项。可在下一字段中对消息进行自定义。

"*日志记录设置*"部分：

- *日志记录大小* - 用于选择最合意的日志文件大小。默认值：100 MB。

"*扫描属性*"部分：

- *使用启发式扫描* - 选中此框可在扫描过程中启用启发式分析法。
- *报告可能不需要的程序和间谍软件威胁* - 选中此选项可报告是否有可能不需要的程序和间谍软件。
- *扫描内部存档* - 选中此选项可让扫描程序也对已经过存档的文件（zip、rar 等）内部进行扫描。

通过"*电子邮件附件报告*"部分可选择应该在扫描过程中报告的项目。如果已选中，所有含此类项目的电子邮件的邮件主题中都会有 [INFORMATION] 标签。这是默认配置，可以轻松地在"*检测操作*"的"*信息*"部分中修改（请见下文）。

可用选项如下：

- *报告受密码保护的存档*
- *报告受密码保护的文档*
- *报告包含宏的文件*
- *报告隐藏的扩展名*

下面的树结构中也有以下子项：

- *检测操作*
- *邮件过滤*

4.3. E-mail Scanner for MS Exchange（SMTP 传输代理）

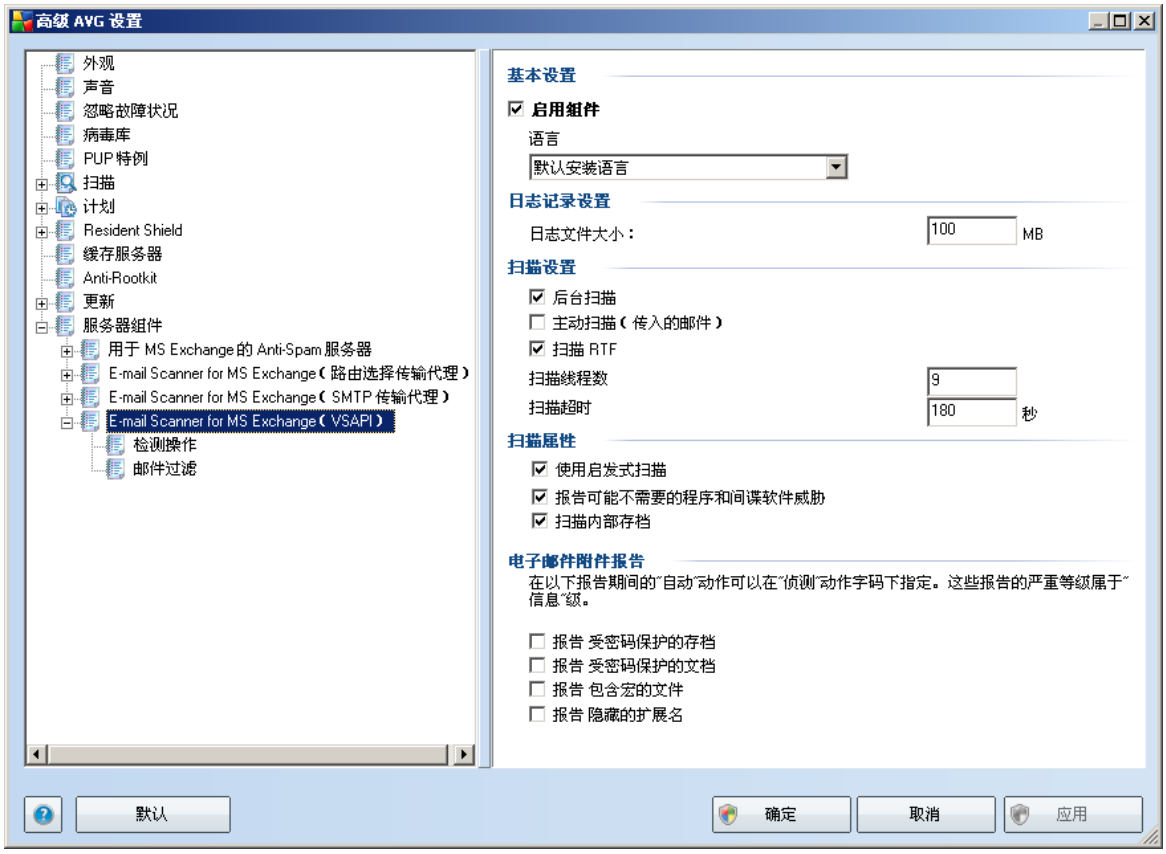
*"E-mail Scanner for MS Exchange（SMTP 传输代理）"*的配置与采用路由选择传输代理时完全相同。有关更多信息，请参见上面的 *E-mail Scanner for MS Exchange（路由选择传输代理）*一章。

下面的树结构中也有以下子项：

- *检测操作*
- *邮件过滤*

4.4. E-mail Scanner for MS Exchange (VSAPI)

此项中有 ***E-mail Scanner for MS Exchange (VSAPI)*** 设置。



*"基本设置"*部分中有以下选项：

- *启用组件* - 取消选中状态以禁用整个组件。
- *语言* - 用于选择最合意的组件语言。

*"日志记录设置"*部分：

- *日志记录大小* - 用于选择最合意的日志文件大小。默认值：100 MB。

*"扫描设置"*部分：

- *后台扫描* – 可以在此启用或禁用后台扫描进程。后台扫描是 VSAPI 2.0/2.5 应用程序界面的功能之一。它提供 Exchange 通讯数据库的多线程扫描。每当用户邮箱文件夹中出现未用最新 AVG 病毒库更新扫描的邮件，都会将其提交给 AVG for Exchange 2007 Server 进行扫描。扫描与搜索未检查对象的工作同时进行。

  每个数据库均使用一个特定的低优先级线程，这样可以保证始终优先执行其它任务（如 Microsoft Exchange 数据库中的电子邮件存储）。

- *主动扫描(传入邮件)*

  可在此启用或禁用 VSAPI 2.0/2.5 的主动扫描功能。如果已将某一封邮件传送到某个文件夹中，但客户端并未发出请求，则会执行这种扫描。

  一旦邮件被提交到 Exchange 存储空间，就会以低优先级将其放入全局扫描队列（最多 30 封邮件）。会以先进先出 (FIFO) 方式对其进行扫描。如果访问仍在队列中的邮件，则会将其优先级改为高优先级。

  注：溢出消息会继续发出，直到不扫描 Exchange 存储空间为止。

注：即使禁用"后台扫描"和"主动扫描"这两个选项，访问邮件时执行的扫描程序也仍会在用户尝试用 MS Outlook 客户端下载邮件时处于活动状态。

- *扫描 **RTF*** - 可在此处指定是否应该扫描 RTF 类文件。
- *扫描线程数* - 扫描进程默认情况下启用多线程工作，通过一定程度的并行提高总体扫描性能。您可以在此更改线程数量。

  默认线程数的算法是："number_of_processors"乘以 2 + 1。

  最小线程数的算法是：（"number of processors"+ 1）除以 2。

  最大线程数的算法是："number of processors"乘以 5 + 1。

  如果线程数不大于最小值或不小于最大值，则会使用默认值。

- *扫描超时* - 用一个线程访问正在扫描的邮件的最长连续时间间隔（以秒为单

位，默认值是 180 秒）。

"*扫描属性*"部分：

- *使用启发式扫描* - 选中此框可在扫描过程中启用启发式分析法。
- *报告可能不需要的程序和间谍软件威胁* - 选中此选项可报告是否有可能不需要的程序和间谍软件。
- *扫描内部存档* - 选中此选项可让扫描程序也对已经过存档的文件（zip、rar 等）内部进行扫描

通过"*电子邮件附件报告*"部分可选择应该在扫描过程中报告的项目。默认配置都可以轻松地在"*检测操作*"的"*信息*"部分中修改（请见下文）。

可用选项如下：

- *报告受密码保护的存档*
- *报告受密码保护的文档*
- *报告包含宏的文件*
- *报告隐藏的扩展名*

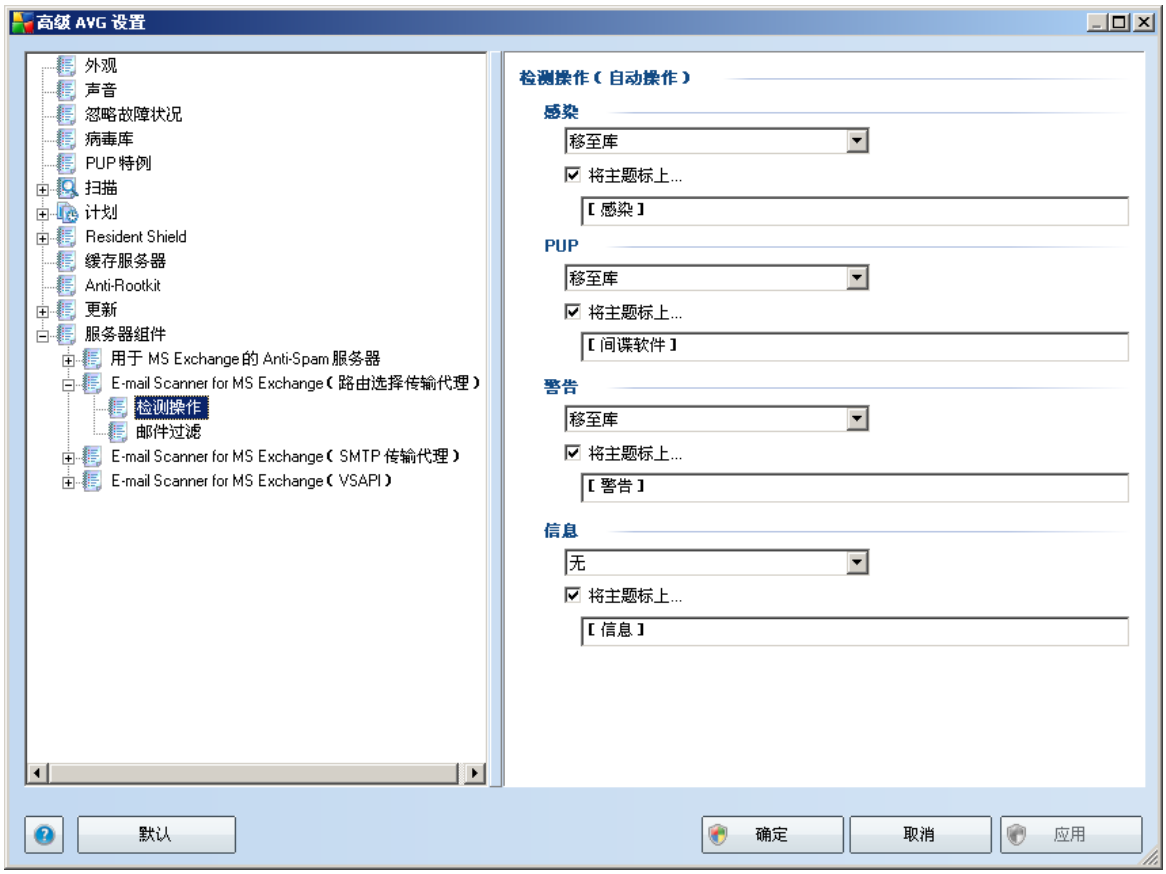
一般而言，其中的某些特性是用户对 Microsoft VSAPI 2.0/2.5 应用程序接口服务作的扩展。有关 VSAPI 2.0/2.5 的详细信息，请参阅以下链接（也请参阅能通过所引用的链接访问的链接）：

- http://support.microsoft.com/?scid=kb%3Bzh-cn%3B328841&x=9&y=12 - 有关 Exchange 和防病毒软件之间的交互作用的信息
- http://support.microsoft.com/?scid=kb%3Bzh-cn%3B823166&x=12&y=15 - 有关 Exchange 2003 Server 应用程序中的其它 VSAPI 2.5 特性的信息

下面的树结构中也有以下子项：

- *检测操作*
- *邮件过滤*

4.5. 检测操作



在"*检测操作*"子项中，可以选择会在扫描过程中执行的自动操作。

可将这些操作用于以下项：

- *感染*
- ***PUP (可能不需要的程序)***
- *警告*
- *信息*

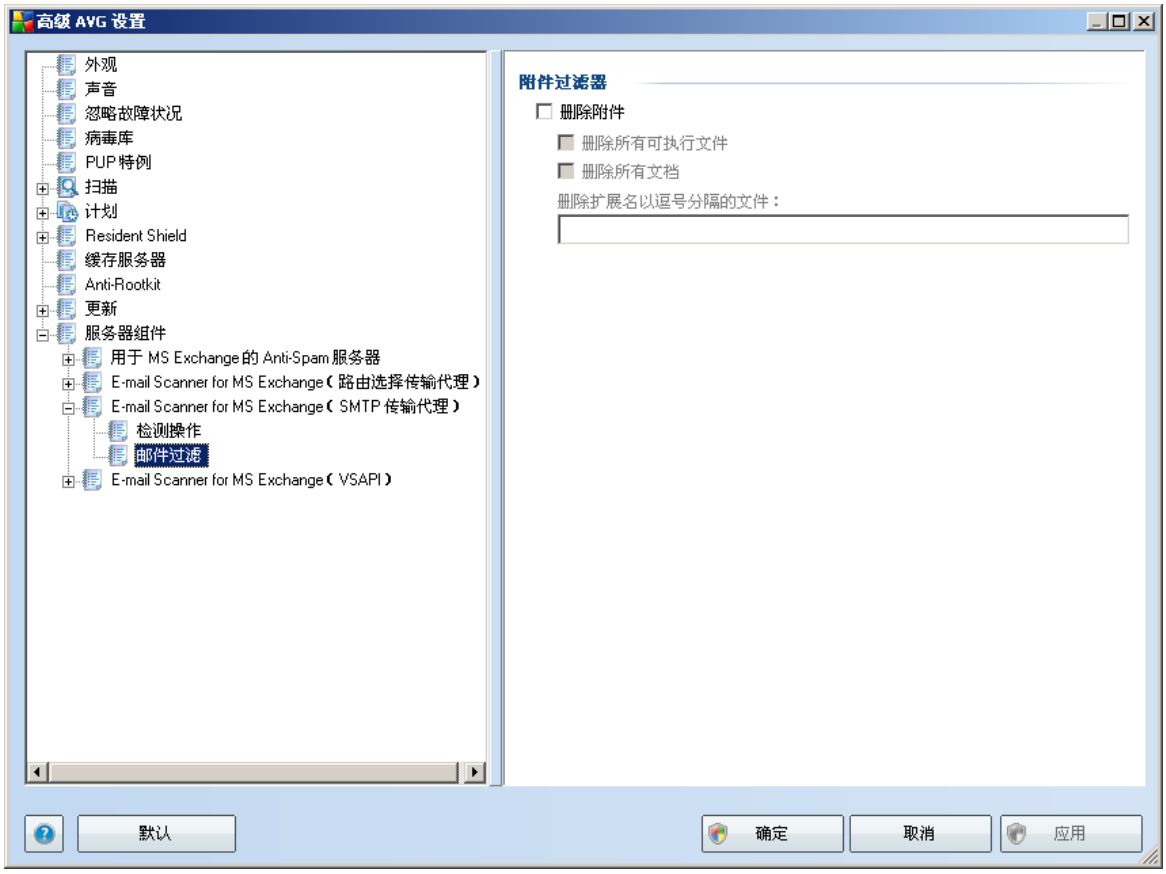
可用下拉菜单对每一项选择操作：

- *无* - 不会执行任何操作。
- *移至库* - 会将特定威胁移到病毒库中。
- *删除* - 会删除特定威胁。

对于含有特定项/威胁的邮件，要选择自定义主题文本，请选中*"将主题标上..."*框，然后填入最合意的主题文本。

注意：最后提到的特性不能用于 E-mail Scanner for MS Exchange VSAPI。

4.6. 邮件过滤



可在*"邮件过滤"*子项中选择应该自动删除的附件（如果有）。可用选项如下：

- *删除附件* - 选中此框可启用该特性。

- *删除所有可执行文件* - 用于删除所有可执行文件。
- *删除所有文档* - 用于删除所有文档文件。
- *删除带有以下扩展名(用逗号分隔)的文件* - 请将所要自动删除的文件的扩展名填入该框。请用逗号分隔各个扩展名。

5. E-mail Scanner for MS Exchange Server 2000/2003

5.1. 概述

E-mail Scanner for MS Exchange Server 2000/2003 配置选项作为服务器组件完全集成在 AVG 9.0 Email Server Edition 中。

服务器组件包括以下内容：

各个服务器组件的基本概述：

- ***Anti-Spam - Anti-Spam Server for MS Exchange***

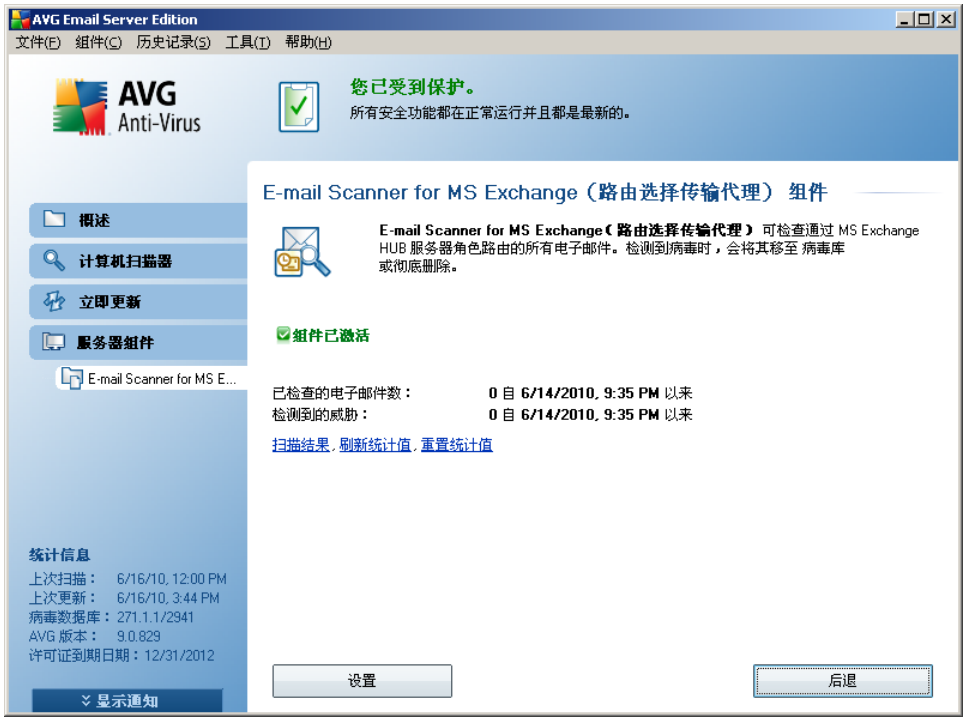
  可检查所有传入的电子邮件并将不需要的电子邮件标记为"垃圾邮件"。它采用多种分析方法来处理每一封电子邮件，可在最大程度上阻止不需要的电子邮

件。

- ***EMS (VSAPI) - E-mail Scanner for MS Exchange (VSAPI)***

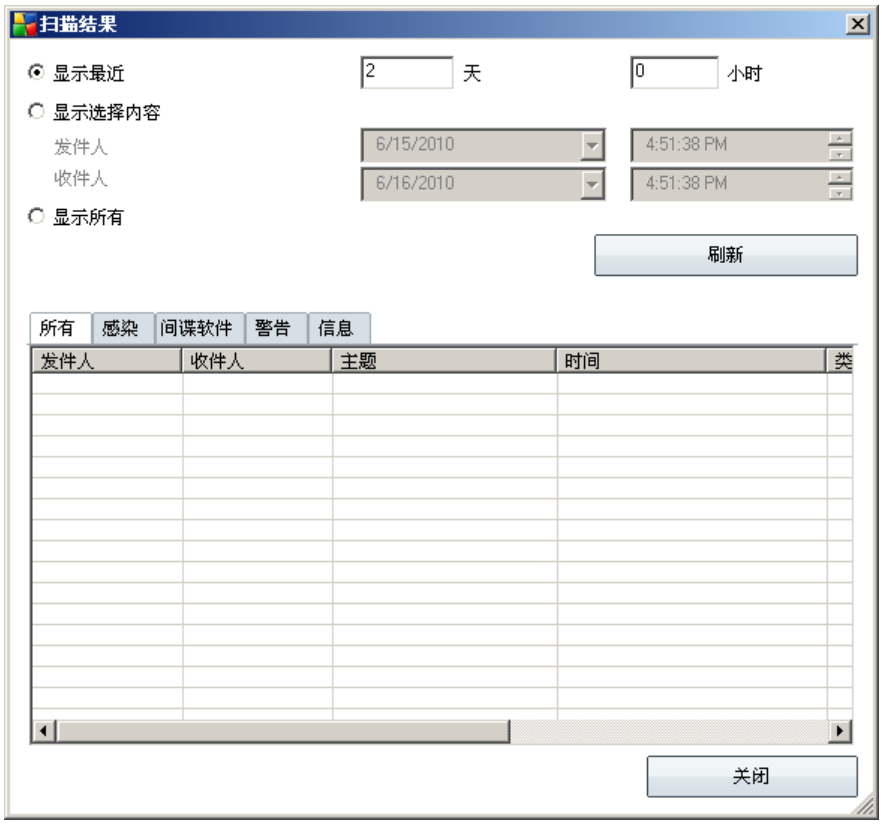
  可检查所有存储在用户邮箱中的电子邮件。如果检测到病毒，则会将其移到病毒库中或完全删除。

双击所需的组件以打开其界面。所有组件均可共享以下常用控制按钮和链接，但 Anti-Spam 组件除外：



- *扫描结果*

  会打开一个新对话框，您可以从中查看扫描结果：



您可以在此查看划分到不同选项卡中的消息，这些选项卡是根据消息的严重性来划分的：有关修改严重性和报告的信息，请参见各个组件的配置。

默认情况下，仅会显示前两天的扫描结果。通过修改以下选项可更改显示期限：

- *显示前* - 可插入所选天数和时数。
- *显示选择内容* - 可选择自定义时间和日期间隔。
- *显示所有* - 可显示整个时段的扫描结果。

可用*"刷新"*按钮重新加载扫描结果。

- *刷新统计值* - 可更新上面显示的统计数据。
- *重置统计值* - 可将所有统计数据重置为零。

功能按钮包括：

- *设置* - 可用此按钮打开组件设置。
- *后退* - 按此按钮可返回到"服务器组件概述"。

您将会在以下章节找到更多有关所有组件不同设置的信息。

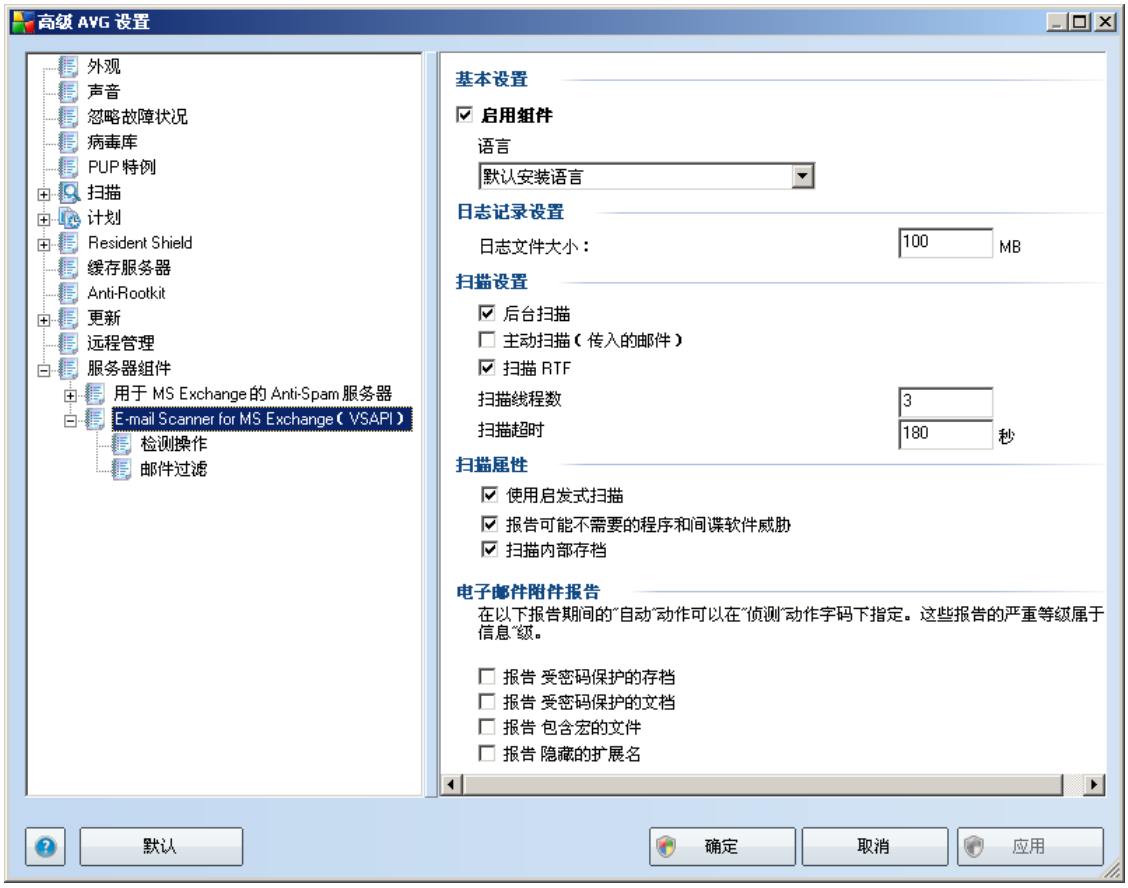
5.2. VSAPI 2.0

Virus Scanning **API 2.0**（MS Exchange 2000 Server 中提供的 VSAPI 2.0）不允许您删除受感染的电子邮件文件。由于无法删除病毒感染的电子邮件附件，因此可以更改该附件名称：AVG for Exchange 2000/2003 Server 会将 .virusinfo.txt 扩展名附加到原始文件名之后。该文件内容将被发现已知病毒的消息所覆盖。如果直接在邮件中发现了病毒，那么邮件的整个正文将被一则"在此邮件中发现病毒"的注释消息所覆盖。

Virus Scanning **API 2.5**（*MS Exchange 2003 Server 中提供的 VSAPI 2.5*）还允许您删除受感染的邮件。您可以在 AVG for MS Exchange 2000/2003 Server 配置对话框中设置此功能。

5.3. E-mail Scanner for MS Exchange (VSAPI)

此项中有 ***E-mail Scanner for MS Exchange (VSAPI)*** 设置。



"*基本设置*"部分中有以下选项：

- *启用组件* - 取消选中状态可禁用整个组件。
- *语言* - 用于选择最合意的组件语言。

"*日志记录设置*"部分：

- *日志记录大小* - 用于选择最合意的日志文件大小。默认值：100 MB。

"*扫描设置*"部分：

- *后台扫描* – 可以在此启用或禁用后台扫描进程。后台扫描是 VSAPI 2.0/2.5 应用程序界面的功能之一。它提供 Exchange 通讯数据库的多线程扫描。每当用户邮箱文件夹中出现未用最新 AVG 病毒库更新扫描的邮件时，都会将其提交给 AVG for Exchange 2007 Server 进行扫描。扫描与搜索未检查对象的工作同时进行。

  每个数据库均是使用一个特定的低优先级线程，这样可以保证始终优先进行其它任务（如 Microsoft Exchange 数据库中的电子邮件存储）。

- *主动扫描(传入邮件)*

  可在此启用或禁用 VSAPI 2.0/2.5 的主动扫描功能。如果已将某一封邮件传送到某个文件夹中，但客户端并未发出请求，则会执行这种扫描。

  一旦将邮件提交到 Exchange 存储空间，就会将其放入全局扫描队列（将其优先级设置为低优先级，最多 30 封邮件）。会以先进先出 (FIFO) 方式对其进行扫描。如果访问仍在队列中的邮件，则会将其优先级改为高优先级。

  注：溢出消息会继续发出，直到不扫描 Exchange 存储空间为止。

注：即使禁用"后台扫描"和"主动扫描"这两个选项，访问邮件时执行的扫描程序也仍会在用户尝试用 MS Outlook 客户端下载邮件时处于活动状态。

- *扫描 **RTF*** - 可在此处指定是否应该扫描 RTF 类文件。
- *扫描线程数* - 扫描进程默认情况下启用多线程工作，通过一定程度的并行提高总体扫描性能。您可以在此更改线程数量。

  默认线程数的算法是："number_of_processors"乘以 2 + 1。

  最小线程数的算法是：（"number of processors"+ 1）除以 2。

  最大线程数的算法是："number of processors"乘以 5 + 1。

  如果线程数不大于最小值或不小于最大值，则会使用默认值。

- *扫描超时* - 用一个线程访问正在扫描的邮件的最长连续时间间隔（以秒为单位，默认值是 180 秒）。

*"扫描属性"*部分：

- *使用启发式扫描* - 选中此框可在扫描过程中启用启发式分析法。
- *报告可能不需要的程序和间谍软件威胁* - 选中此选项可报告是否有可能不需要的程序和间谍软件。
- *扫描内部存档* - 选中此选项可让扫描程序也对已经过存档的文件（zip、rar

等）内部进行扫描。

通过"*电子邮件附件报告*"部分可选择应该在扫描过程中报告的项目。默认配置都可以轻松地在"*检测操作*"的"*信息*"部分中修改（请见下文）。

可用选项如下：

- *报告受密码保护的存档*
- *报告受密码保护的文档*
- *报告包含宏的文件*
- *报告隐藏的扩展名*

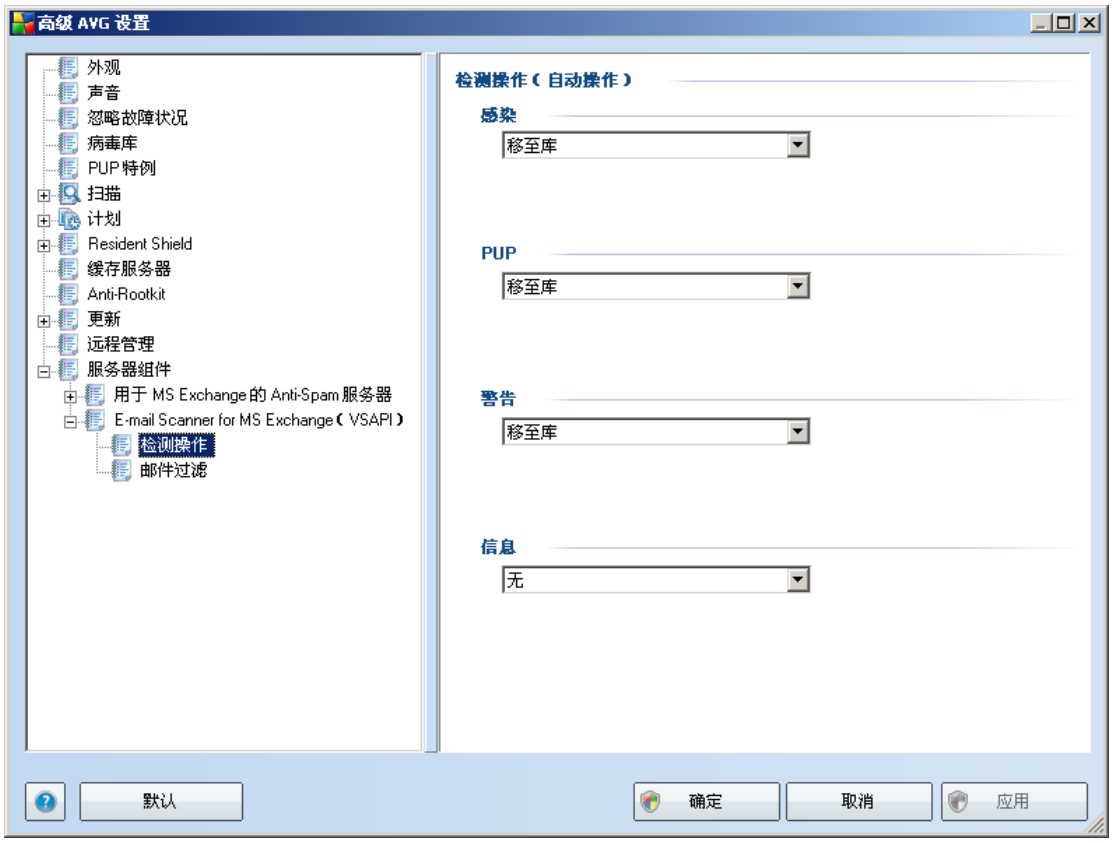
一般而言，所有这些特性都是用户对 Microsoft VSAPI 2.0/2.5 应用程序接口服务作的扩展。有关 VSAPI 2.0/2.5 的详细信息，请参阅以下链接（也请参阅能通过所引用的链接访问的链接）：

- http://support.microsoft.com:80/support/kb/articles/Q285/6/67.ASP - 有关 Exchange 2000 Server Service Pack 1 中的 VSAPI 2.0 的总体说明
- http://support.microsoft.com/default.aspx?scid=kb;en-us;328841&Product=exch2k - 有关 Exchange 和防病毒软件之间的交互作用的信息
- http://support.microsoft.com/default.aspx?scid=kb;en-us;823166 - 有关 Exchange 2003 Server 应用程序中的其它 VSAPI 2.5 特性的信息

下面的树结构中也有以下子项：

- *检测操作*
- *邮件过滤*

5.4. 检测操作



在*"检测操作"*子项中，可以选择会在扫描过程中执行的自动操作。

这些操作可用于以下项：

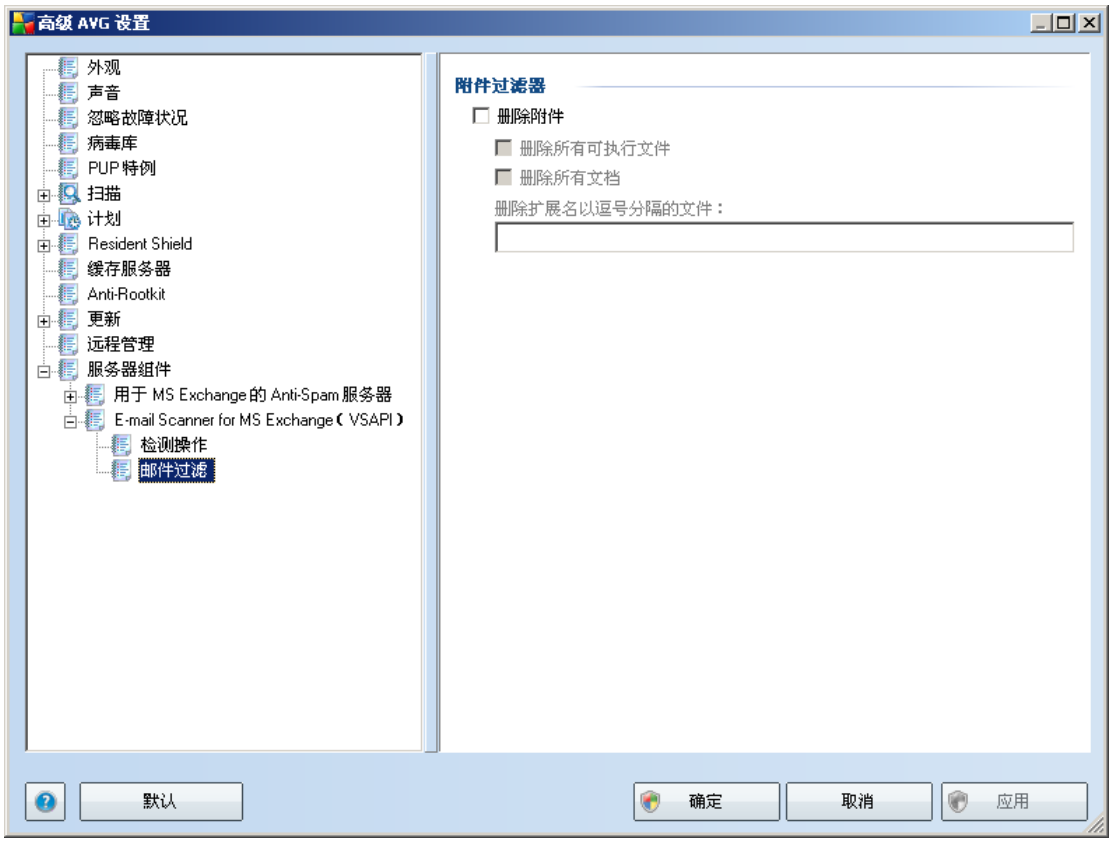
- *感染*
- ***PUP (可能不需要的程序)***
- *警告*
- *信息*

用下拉菜单为每一项选择操作：

- *无* - 不会执行任何操作。

- *移至库* - 会将特定威胁移到病毒库中。
- *删除* - 会删除特定威胁。

5.5. 邮件过滤



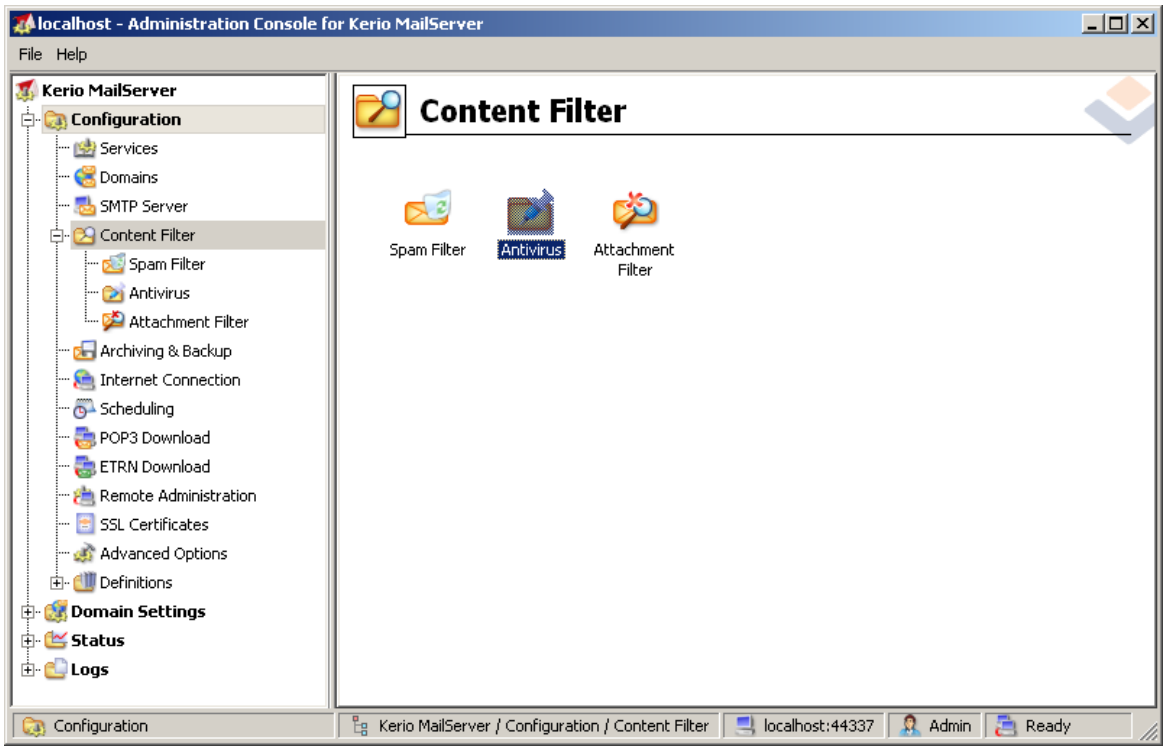
可在"*邮件过滤*"子项中选择应该自动删除的附件（如果有）。可用选项如下：

- *删除附件* - 选中此框可启用该特性。
- *删除所有可执行文件* - 用于删除所有可执行文件。
- *删除所有文档* - 用于删除所有文档文件。
- *删除带有以下扩展名(用逗号分隔)的文件* - 请将所要自动删除的文件的扩展名填入该框。请用逗号分隔各个扩展名。

6. AVG for Kerio MailServer

6.1. 配置

防病毒保护机制已直接集成到 Kerio MailServer 应用程序中。为了通过 AVG 扫描引擎激活 Kerio MailServer 电子邮件保护措施，请启动 Kerio Administration Console 应用程序。在该应用程序窗口左侧的控制树中，选择"Configuration"分支下的"Content Filter"子分支：

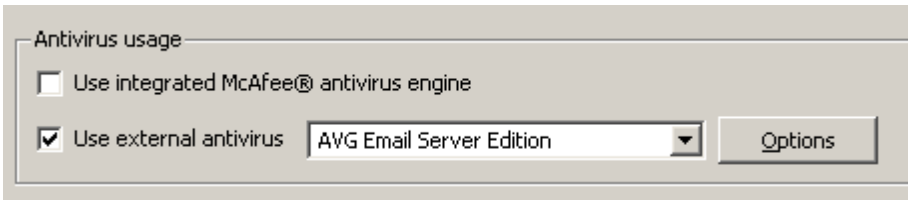


单击"Content Filter"项会显示一个对话框，其中有三项：

- ***Spam Filter***
- ***Antivirus***（请见 ***Antivirus*** 部分）
- ***Attachment Filter***（请见 ***Attachment Filter*** 部分）

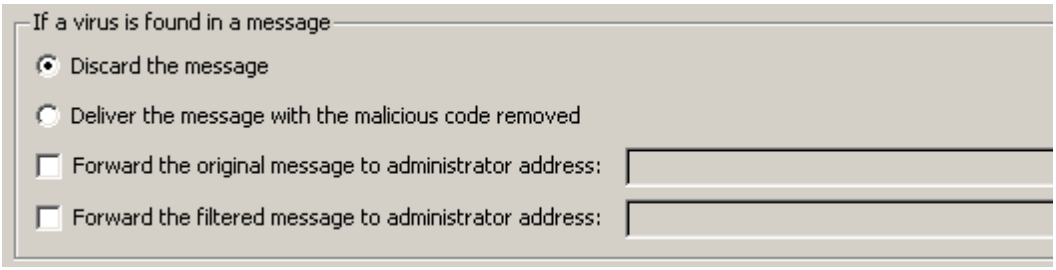
6.1.1. 防病毒

要激活 AVG for Kerio MailServer，请选中"使用外部防病毒软件"复选框，然后从配置窗口的"防病毒软件使用情况"框中的外部软件菜单中选择"AVG Email Server Edition"项：



可在以下部分中指定要对受感染或已滤掉的邮件执行的操作：

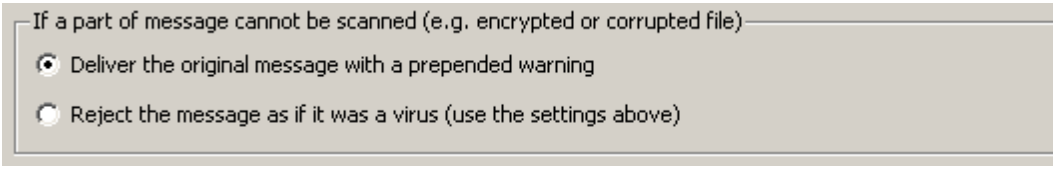
- *如果邮件中有病毒*



此框用于指定检测到邮件中有病毒，或者已由附件过滤器滤掉邮件时所要执行的操作：

  - *丢弃邮件* - 选中后会删除受感染或已滤掉的邮件。
  - *清除恶意代码后再传递邮件* - 选中后会向收件人传递邮件，但不带可能有害的附件。
  - *向管理员的地址转发原始邮件* - 选中后会向地址文本字段中所指定的地址转发受到病毒感染的邮件
  - *向管理员的地址转发已滤掉的邮件* - 选中后会向地址文本字段中所指定的地址转发已滤掉的邮件

- *如果无法对邮件的一部分进行扫描（例如，文件已加密或已受损）*

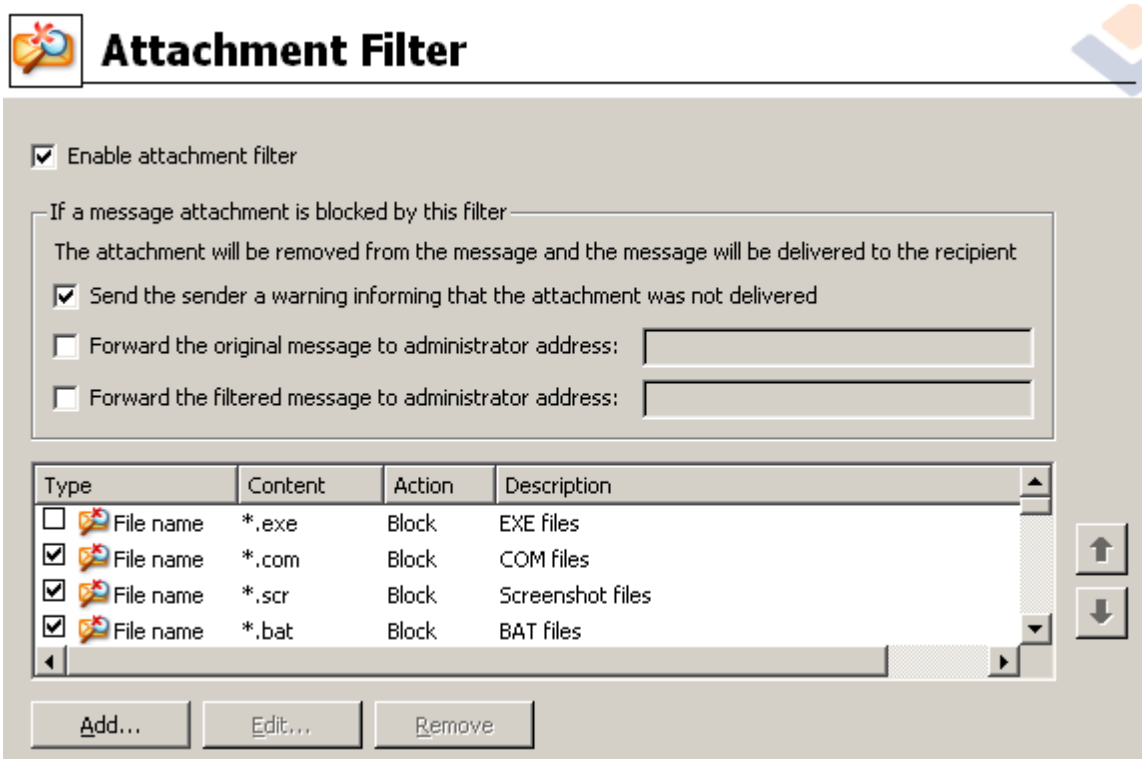


此框用于指定不能对邮件或附件的一部分进行扫描时所要执行的操作：

- *传递原始邮件时发出准备好的警告* - 不检查就传递邮件（或附件）。会向用户发出警告，说明邮件中可能仍含病毒。
- *如同病毒一样拒绝邮件* - 系统的反应方式会与检测到病毒时相同（也就是说，传递邮件时不带任何附件或拒绝传递邮件）。此选项很安全，但几乎不可能传递由密码保护的档案。

6.1.2. 附件过滤器

"附件过滤器"菜单中列有各种附件定义：



通过选中/取消选中"启用附件过滤器"复选框，可启用/禁用邮件附件过滤功能。也

可更改以下设置：

- *向发件人发送警告，说明未传递附件*

  发件人会从 Kerio MailServer 收到警告，说明发件人发送的邮件含有病毒，或者已经禁止传递邮件附件。

- *向管理员的地址转发原始邮件*

  无论指定的电子邮件地址是本地还是外部地址，都会向指定的电子邮件地址转发邮件（按原样发送，即发送时带有受感染或受禁附件）。

- *向管理员的地址转发已滤掉的邮件*

  会向指定的电子邮件地址转发邮件，但不带受感染或受禁附件（除了下面的所选操作）。借此可以验证防病毒和/或附件过滤器的运行是否正常。

扩展名列表中每项都有四个字段：

- *类型* - 用于指定附件种类，附件种类取决于"内容"字段中所指定的扩展名。可供选择的类型包括"文件名"或"MIME 类型"。可在此字段中选择相应的框，以便在进行附件过滤时包括/排除该项。

- *内容* - 可在此指定要滤掉的文件的扩展名。可在此使用操作系统通配符（例如字符串"*.doc.*"表示任何扩展名为 .doc 的文件，后面的扩展名不限）。

- *操作* - 用于指定要对特定附件执行的操作。可供选择的操作包括"接受"（接受附件）和"阻止"（会按已禁用附件列表上方所指定的处理方式执行操作）。

- *说明* - 附件说明在此字段中定义。

通过按"删除"按钮会从列表中删除项。通过按**"*添加...*"**按钮可再向列表中添加一项。也可通过按**"*编辑...*"**按钮编辑原有记录。然后就会显示以下窗口：

- 可在"说明"字段中编写要滤掉的附件的简短说明。
- 可在"如果邮件含有以下类型的附件"字段中选择附件类型（"文件名"或"MIME 类型"）。也可从所提供的扩展名列表中选择特定扩展名，或者直接键入扩展名通配符。

可在"则"字段中决定是要阻止还是接受所定义的附件。

7. Anti-Spam 配置

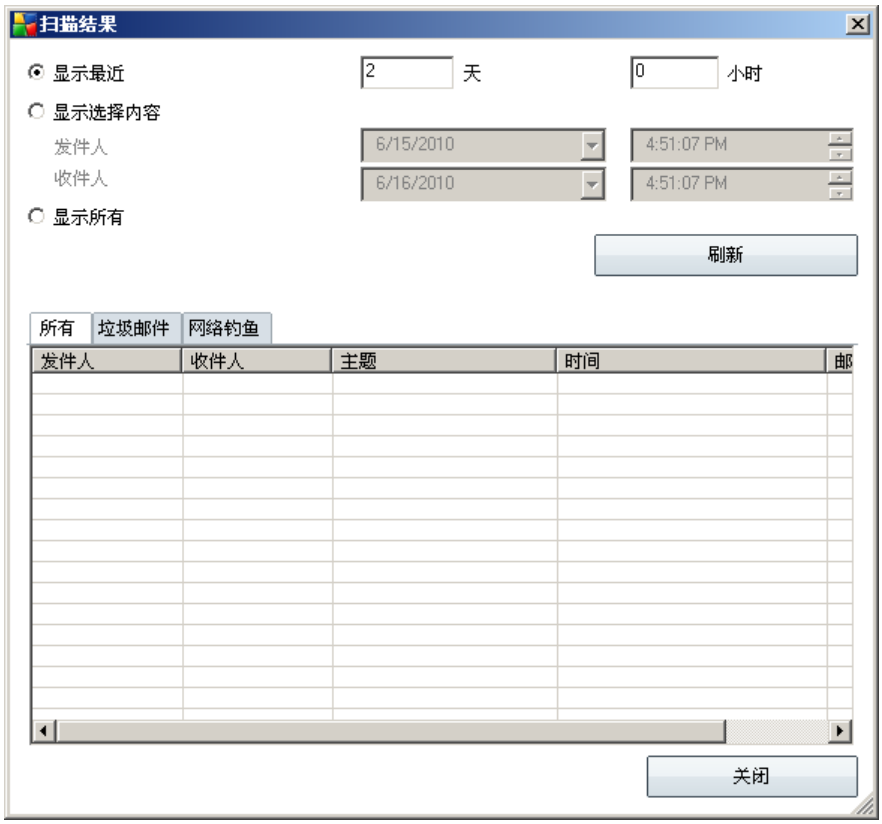
7.1. Anti-Spam 界面

Anti-Spam *服务器组件的对话框在"服务器组件"*部分（左侧菜单）中。其中有关于服务器组件功能的简短说明，有关其当前状态的信息（*Anti-Spam Server for MS Exchange 组件已激活。*），以及某些统计信息。

可用链接：

- *扫描结果*

  用于打开一个新对话框，从中可查看反垃圾邮件扫描结果：



可在此查看检测后确定为"垃圾邮件"(不需要的邮件)或"仿冒"尝试(力图窃取个人资料、用于办理银行事务的详细信息、身份等)的邮件。默认情况下,仅会显示前两天的扫描结果。通过修改以下选项可更改显示期限:

- *显示前* - 可插入所选天数和时数。
- *显示选择内容* - 可选择自定义时间和日期间隔。
- *显示所有* - 可显示整个时段的扫描结果。

可用"*刷新*"按钮重新加载扫描结果。

- *刷新统计值* - 可更新上面显示的统计数据。
- *重置统计值* - 可将所有统计数据重置为零。

功能按钮包括:

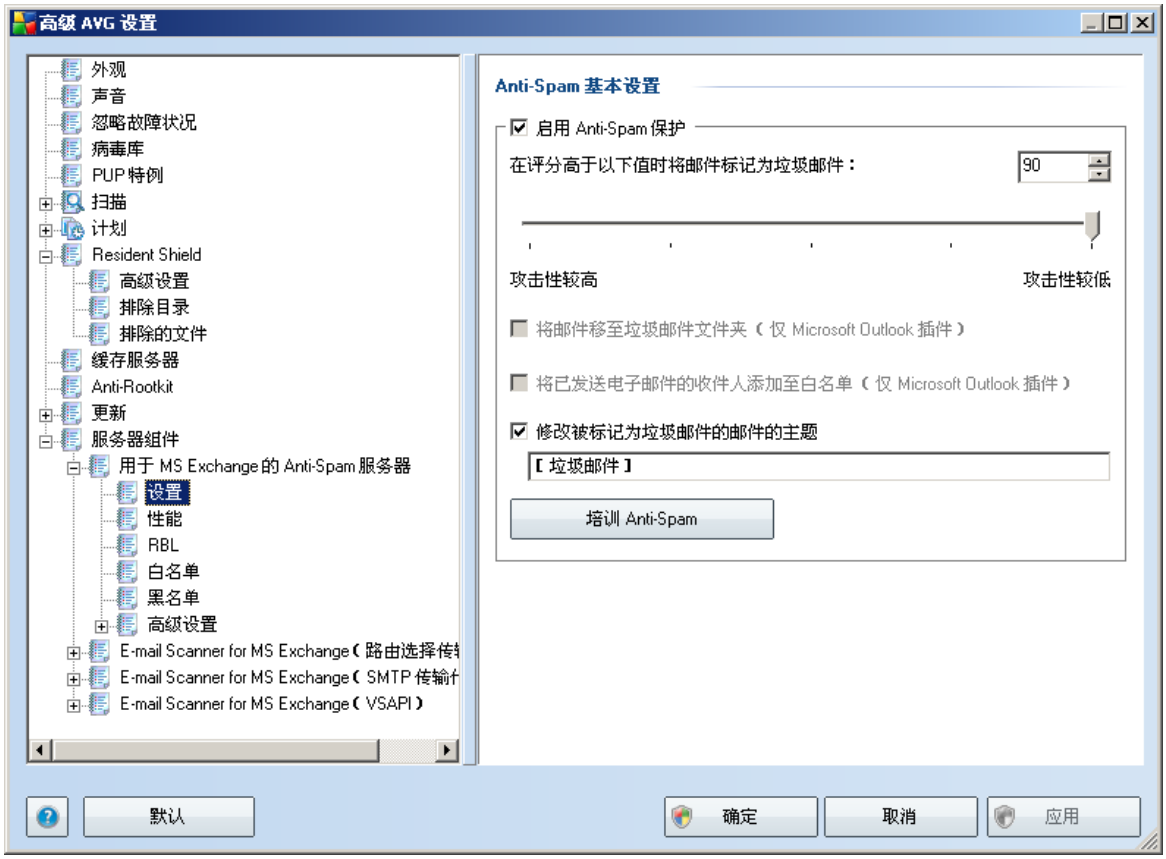
- *设置* - 可用此按钮打开 Anti-Spam 设置。
- *后退* - 按此按钮可返回到"服务器组件概述"。

7.2. Anti-Spam 原理

垃圾邮件是指未经请求的电子邮件，大多以宣传产品或服务为目的，采取群发方式，每次寄给大量的电子邮件地址，充斥收件人的邮箱。垃圾邮件并不包括那些已征得消费者同意而发送的合法的商业电子邮件。垃圾邮件不仅令人厌烦，而且往往含有诈骗信息、病毒或冒犯性内容。

Anti-Spam 可检查所有传入的电子邮件并将不需要的电子邮件标记为"垃圾邮件"。它采用多种分析方法来处理每一封电子邮件，可在最大程度上阻止不需要的电子邮件。

7.3. 反垃圾邮件设置



在*"Anti-Spam 基本设置"*对话框中，可以选中*"启用 Anti-Spam 保护"*复选框，以允许/禁止对电子邮件通信内容进行反垃圾邮件扫描。

在此对话框中，您还可以选择较为严格或较为宽松的评分措施。***Anti-Spam*** 过滤器根据多项动态扫描技术为每封邮件指定一个分值（*即该邮件的内容与垃圾邮件的相似度*）。可以调整*"分数不小于以下值时将邮件标记为垃圾邮件"*设置，方法是键入相应的值（*0 到 100*）或向左或向右移动滑块（*使用滑块时，值的范围限制在 50-90 之间*）。

一般而言，我们建议将阈值设置在 50 至 90 之间，如果您确实不知道设为何值，建议设置为 90。下面对评分阈值进行了大致介绍：

- *介于 **90** 和 **99** 之间的值* - 大多数传入的电子邮件都将正常传送（而不会被标记为垃圾邮件）。最容易识别的垃圾邮件将被过滤掉，但大量的垃圾邮件可能仍被允许传入。
- *介于 **80** 和 **89** 之间的值* - 将过滤掉很有可能是垃圾邮件的电子邮件。有些并非垃圾邮件的邮件也可能会被错误地过滤掉。
- *介于 **60** 和 **79** 之间的值* - 这些值被认为是相当严格的配置。将过滤掉可能是垃圾邮件的电子邮件。并非垃圾邮件的邮件也可能会被捕获到。
- *介于 **1** 和 **59** 之间的值* - 非常严格的配置。并非垃圾邮件的电子邮件很有可能会被当成真正的垃圾邮件而被捕获到。正常使用时不推荐此阈值范围。
- ***0** 值* - 在此模式中，仅会接收到来自*白名单*中的发件人的电子邮件。任何其它电子邮件都将被视为垃圾邮件。*正常使用时不推荐此阈值范围。*

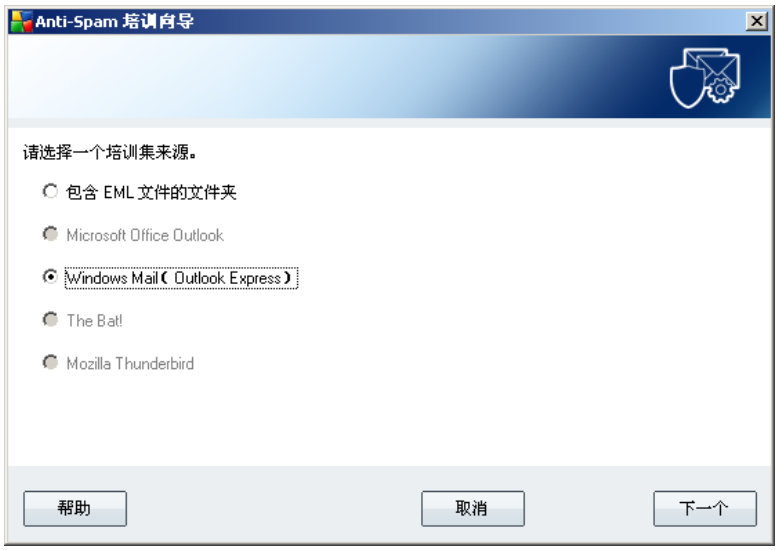
可进一步指定检测到的垃圾邮件的处理方式：

- *修改标记为垃圾邮件的邮件主题* - 对于被检测到为垃圾邮件的所有邮件，如果您希望在它们的标题字段中用特定的词或字符对它们进行标记，请勾选此复选框；可以在激活的相应文本字段中键入所需的文本。

*"Anti-Spam 培训"*按钮用于打开 ***Anti-Spam 培训向导***，下一章中对此向导进行了详细说明。

7.3.1. Anti-Spam 培训向导

***Anti-Spam** 培训向导*的第一个对话框要求您选择打算用于培训的电子邮件来源。通常情况下，您需要使用已被误标记为垃圾邮件的电子邮件，或尚未被识别出来的垃圾邮件。



有以下选项可供选择：

- *特定的电子邮件客户端* - 如果使用的是某种列出的电子邮件客户端（*MS Outlook*、*Outlook Express*、*The Bat!*、*Mozilla Thunderbird*），只须选择相应的选项即可
- *"包含 **EML** 文件的文件夹"*– 如果您使用的是任何其它电子邮件程序，首先应将这些邮件保存至特定文件夹（以 *.eml 格式*），或者确保您知道电子邮件客户端邮件文件夹的位置。然后选择*"包含 **EML** 文件的文件夹"*，这样您下一步就能找到所需的文件夹

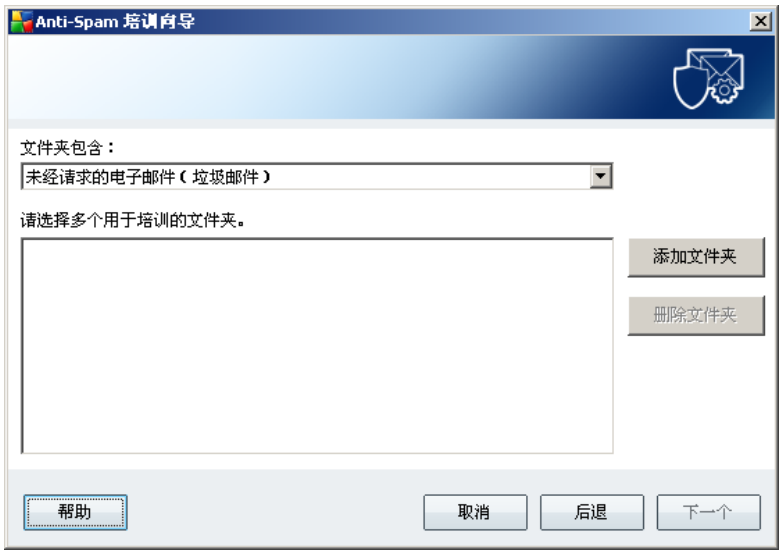
为加快并简化培训过程，最好事先对各文件夹中的电子邮件进行整理，以使您将用于培训的文件夹仅包含培训邮件（要么是需要的邮件，要么是不需要的邮件）。但并非必需进行整理，因为您可以稍后对这些电子邮件进行过滤。

选择相应选项，然后单击*"下一步"*继续按向导提示操作。

7.3.2. 选择包含邮件的文件夹

本步骤中显示的对话框取决于您之前所做的选择。

包含 **EML** 文件的文件夹



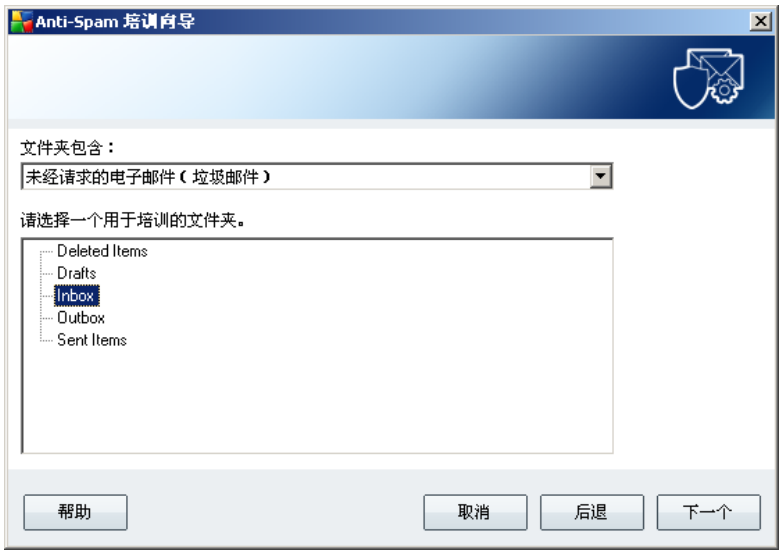
在此对话框中，请选择您要用于培训的邮件所在的文件夹。按"*添加文件夹*"按钮以找到包含 .eml 文件（*已保存的电子邮件*）的文件夹。所选的文件夹随后便会显示在此对话框中。

在"*文件夹包含*"下拉菜单中，设置以下两个选项之一：所选文件夹包含的是需要的电子邮件（*非垃圾邮件*），还是未经请求便发来的电子邮件（*垃圾邮件*）。请注意，在下一步中您可以过滤这些邮件，所以该文件夹现在不必仅包含培训电子邮件。您还可以通过单击"*删除文件夹*"按钮从此列表中删除不需要的选定文件夹。

完成后，请单击"*下一步*"，然后接着设置*邮件过滤选项*。

特定的电子邮件客户端

在您确认其中一个选项后，将显示新的对话框。



注：对于 Microsoft Office Outlook，系统会提示您先选择 MS Office Outlook 配置文件。

在**"文件夹包含"**下拉菜单中，设置以下两个选项之一：所选文件夹包含的是需要的电子邮件（*非垃圾邮件*），还是未经请求便发来的电子邮件（*垃圾邮件*）。请注意，在下一步中您可以过滤这些邮件，所以该文件夹现在不必仅包含培训电子邮件。所选电子邮件客户端的导航树已被显示在此对话框的主体区域。请在此树中找到所需的文件夹，然后用鼠标突出显示它。

完成后，请单击**"下一步"**，然后接着设置*邮件过滤选项*。

7.3.3. 邮件过滤选项

在此对话框中，您可以进行电子邮件过滤设置。

如果您确定所选文件夹仅包含您要用于培训的邮件，请选择*"所有邮件（无过滤）"*选项。

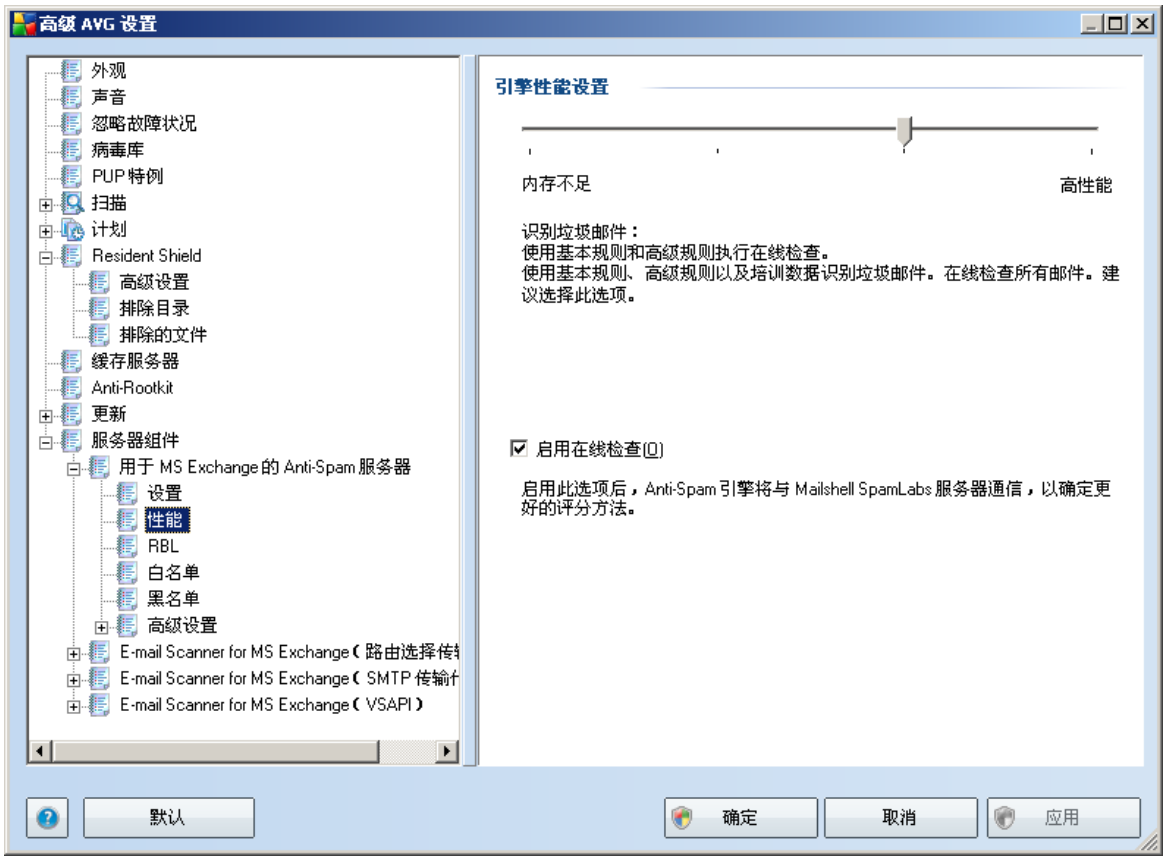
如果您不确定此文件夹中包含哪些邮件，并且希望此向导对每一封邮件都向您询问（以便您决定是否要将它用于培训），请选中*"对每封邮件均进行询问"*选项。

若要进行更高级的过滤，请选择*"使用过滤器"*选项。您可以填写要在电子邮件主题和/或发件人字段中搜索的一个词（*名称*）、词的一部分或词组。与所输入的条件完全匹配的所有邮件都将被用于培训，不再进行提示。

注意！：当您在两个文本字段中都填入内容时，只与其中一个条件匹配的地址也将被用于培训。

选择适当的选项后，请单击*"下一步"*。接下来显示的对话框将仅用于提供信息，告知您此向导已做好邮件处理准备。若要开始培训，请再次单击*"下一步"*按钮。随后便依据前面选择的条件开始培训。

7.4. 性能



*"引擎性能设置"*对话框（*左侧导航区域中的"性能"项链接到此对话框*）提供了 ***Anti-Spam*** 组件的性能设置。向左或向右移动滑块可更改扫描性能的高低，最左侧为*"低内存占用"*模式，最右侧为*"高性能"*模式。

- *低内存占用* - 在扫描过程中识别垃圾邮件时，不使用任何规则。只使用培训数据进行识别。在一般使用情形中不建议采用此模式，除非计算机硬件配置非常低。

- *高性能* - 采用此模式时将占用大量内存。在扫描过程中，将使用以下功能来识别垃圾邮件：规则和垃圾邮件数据库缓存、基本规则和高级规则、垃圾邮件制造者的 IP 地址和垃圾邮件制造者数据库。

默认情况下，*"启用在线检查"*项已启用。这样可通过与 Mailshell 服务器进行通信（即，将扫描到的数据与在线的 Mailshell 数据库进行比较），实现更为精确的垃圾邮件检测效果。

通常情况下，若非必要，建议保留默认设置。对此配置的任何更改都只应由专家级用户进行！

7.5. RBL

"RBL"项用于打开一个名为**"*实时黑名单*"**的编辑对话框：

在此对话框中，您可以启用/禁用**"*查询 RBL 服务器*"**功能。

RBL（*实时黑名单*）服务器是一台承载着一个大型数据库的 DNS 服务器，该数据库中存储着已知的垃圾邮件发件人。启用此功能后，会根据 RBL 服务器数据库来验证所有电子邮件，如果有邮件与数据库中的任何条目相同，则会将该邮件标记为垃圾邮件。

RBL 服务器数据库包含最新的垃圾邮件指纹，以便进行最佳、最准确的垃圾邮件检测。如果用户收到 Anti-Spam 引擎通常无法检测到的大量垃圾邮件，则此功能对他们来说尤为有用。

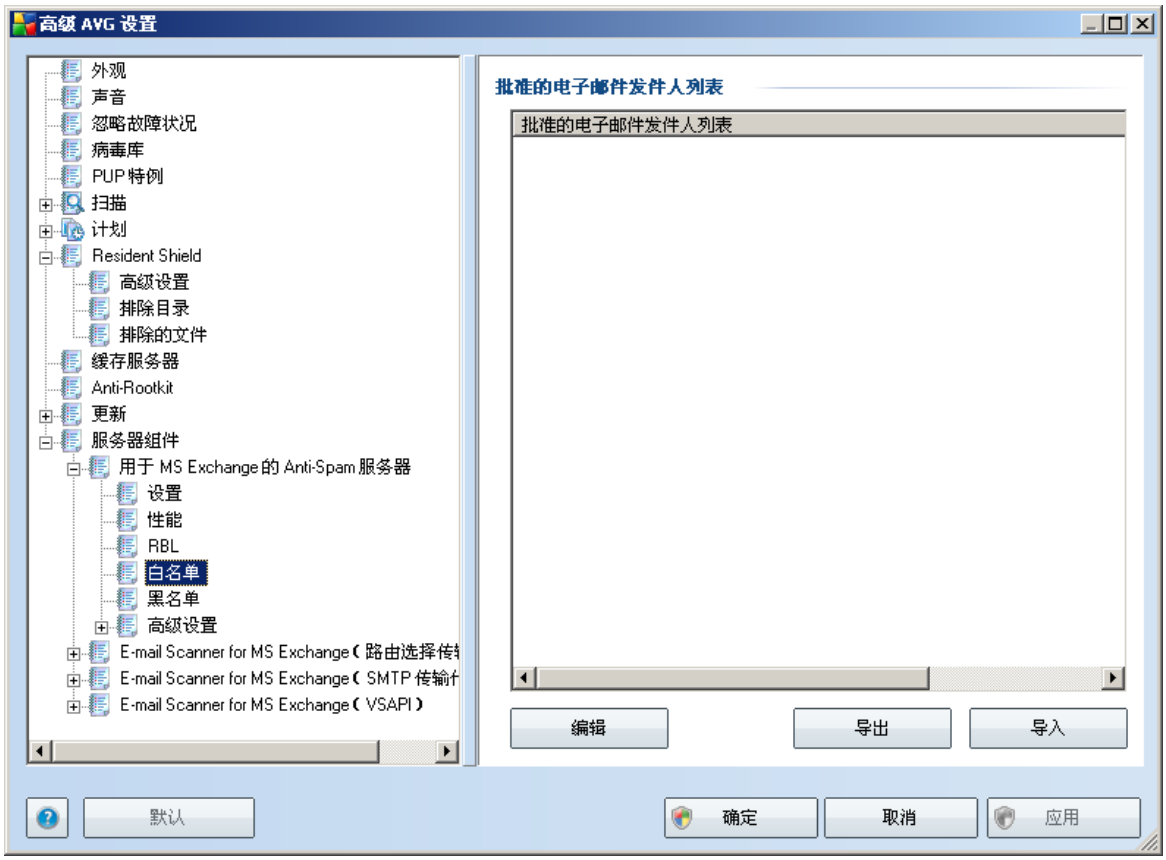
可在*"RBL 服务器列表"*中定义特定 RBL 服务器位置。默认情况下，会指定两个 RBL 服务器地址。除非您是一位富有经验的用户，并且确实需要更改这些设置，否则建议您保留默认设置！

注：在有些系统上以及有些配置条件下，启用此功能可能会降低电子邮件接收速度，因为每一封邮件都必须对照 RBL 服务器数据库进行验证。

不会将任何个人数据发送到此服务器！

7.6. 白名单

单击"白名单"*项可打开一个对话框，其中显示了已经过核准的发件人电子邮件地址和域名的全局列表，来自这些发件人及域名的邮件绝不会标记为*垃圾邮件***。



在此编辑界面中，您可以整理一个您确定绝不会向您发送不需要的邮件（垃圾邮件）的发件人名单。您还可以整理一个您知道不会产生垃圾邮件的完整域名（如 *avg.*

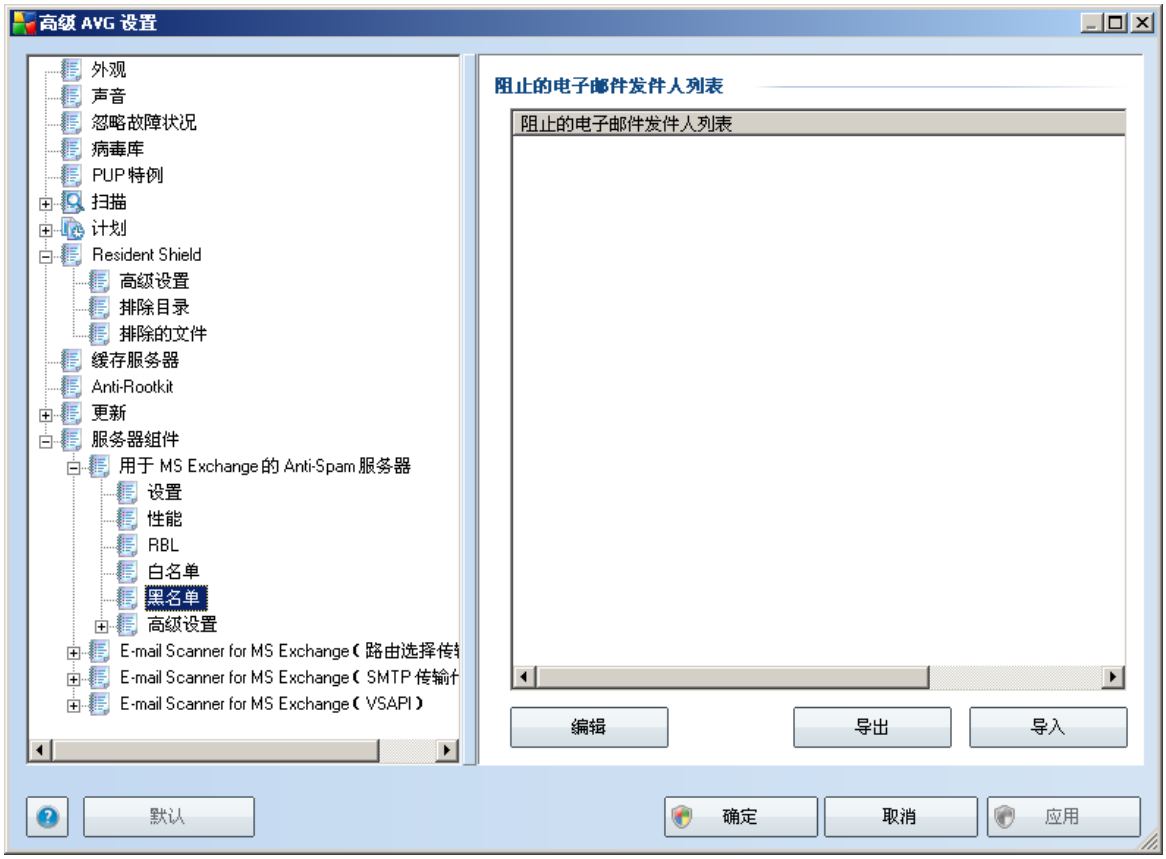
com）列表。

准备好一个这样的发件人和/或域名列表之后，您就可以通过以下任一方法输入它们：直接输入每个电子邮件地址或一次性导入整个地址列表。有下列控制按钮可供使用：

- ***编辑** - 按此按钮可打开一个对话框，从中可手动列出地址（也可使用复制和粘贴功能）。每行请插入一项内容（发件人或域名）。*
- **"*导入*"-** 如果您已经准备好一个包含电子邮件地址/域名的文本文件，您可以通过选择此按钮直接将其导入。该输入文件必须采用纯文本格式，并且每行只能包含一项内容（地址或域名）。
- **"*导出*"-** 如果您决定导出这些记录以用于某种用途，您可以按此按钮进行导出。所有记录都将被保存到一个纯文本文件中。

7.7. 黑名单

*"黑名单"*选项用于打开一个对话框，其中列有已阻止的发件人的所有电子邮件地址和域名，这些发件人发送的邮件始终都会标记为垃圾邮件。



在此编辑界面中，您可以整理一个预期会向您发送不需要的邮件（垃圾邮件）的发件人名单。您还可以整理一个您预期会发来垃圾邮件的完整域名（如 *spammingcompany.com*）列表。来自所列出的地址/域的所有电子邮件都将被标识为垃圾邮件。

准备好一个这样的发件人和/或域名列表之后，您就可以通过以下任一方法输入它们：直接输入每个电子邮件地址或一次性导入整个地址列表。有下列控制按钮可供使用：

- *编辑 - 按此按钮可打开一个对话框，从中可手动列出地址（也可使用复制和粘贴功能）。每行请插入一项内容（发件人或域名）。*

- *"导入"*- 如果您已经准备好一个包含电子邮件地址/域名的文本文件，您可以通过选择此按钮直接将其导入。该输入文件必须采用纯文本格式，并且每行只能包含一项内容（地址或域名）。

- *"导出"*- 如果您决定导出这些记录以用于某种用途，您可以按此按钮进行导出。所有记录都将被保存到一个纯文本文件中。

7.8. 高级设置

通常情况下，若非必要，建议保留默认设置。任何配置更改都只应由专家级用户进行！

如果您依然认为自己需要对 Anti-Spam 配置进行高级更改，请遵照在用户界面中直接提供的说明操作。一般而言，在每一个对话框中都会有一项特定的功能，您可以对其进行编辑 – 其说明总是被包含在该对话框本身中：

- *缓存* – 指纹、域声誉、LegitRepute

- *培训* - 词语条目上限、自动培训阈值、权重

- *过滤* – 语言列表、国家/地区列表、批准的 IP、阻止的 IP、阻止的国家/地区、阻止的字符集、冒牌发件人

- ***RBL*** – RBL 服务器、多重攻击、阈值、超时、最大 IP 数

- ***Internet 连接*** - 超时、代理服务器、代理服务器身份验证

8. AVG Settings Manager

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

该工具包括在 AVG 安装内容中，能通过 Windows"开始"菜单使用：

"所有程序"/"AVG 9.0"/"AVG Settings Manager"

- *编辑本计算机的* ***AVG*** *配置*

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

- *加载并编辑* ***AVG*** *配置文件*

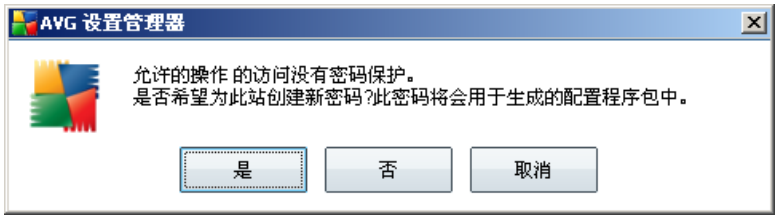
  如果已有 AVG 配置文件 (.pck)，则可用此按钮打开该文件进行编辑。一通过*"确定"*或*"应用"*按钮确认所作的更改，就会用新设置替换该文件！

- *将文件上的配置应用到此计算机上的* ***AVG***

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

- *将本地 **AVG** 配置存储到文件中*

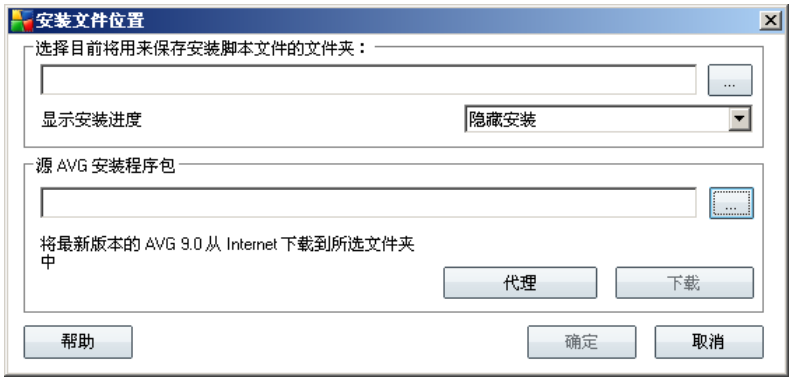
  可用此按钮保存本地 AVG 安装内容的 AVG 配置文件 (.pck)。如果未对允许执行的操作设置密码，则可能会显示以下对话框：



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

- *克隆 **AVG** 安装*

  用此选项可通过创建有自定义选项的安装程序包精确复制本地 AVG 安装内容。要继续操作，请先选择要从中保存安装脚本的文件夹。



  然后从下拉菜单中选择以下某个选项：

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

  可用"*下载*"按钮直接将最新可用 AVG 安装程序包从 AVG 网站下载到所选文件

夹中，也可将 AVG 安装程序包手动放入该文件夹。

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

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

9. 常见问题解答和技术支持

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

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