AVG Email Server Edition 2013

用户手册

文档修订 2013.01 (20.11.2012)

目录

1. 简介

本用户手册提供全面的 **AVG Email Server Edition 2013** 文档。

祝贺您购买 AVG Email Server Edition 2013！

AVG Email Server Edition 2013 是一系列屡获殊荣的 AVG 产品之一，旨在全面保护服务器，让用户高枕无忧，安全无虞。与所有其它 AVG 产品一样，**AVG Email Server Edition 2013** 经过了彻底的重新设计，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 旨在保护您的计算机和网络活动。请尽享 AVG 的全面保护。

***注：**本文档中有特定电子邮件服务器版本的特性说明。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 Email Server Edition 2013 意在保护在以下操作系统中运行的邮件服务器：

- Windows 2008 Server Edition（x86 和 x64）
- Windows 2003 Server（x86 和 x64）SP1

2.2. 受支持的电子邮件服务器

支持以下邮件服务器：

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

2.3. 硬件要求

针对 **AVG Email Server Edition 2013** 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 Email Server Edition 2013** 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 Email Server Edition 2013**。必须使用标准的 Windows 功能手动卸载这一早期版本。

- 在开始菜单***开始/设置/控制面板/添加或删除程序***中，从已安装软件列表中选择相应的程序（或者您可以通过***开始/所有程序/AVG/卸载 AVG*** 菜单轻松执行此操作）。
- 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

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

MS Exchange 2003 Server Service Pack（可选）：

http://www.microsoft.com/en-us/download/details.aspx?id=9664

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。这些旧数据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

MS Exchange 2010 Server Service Pack（可选）：

http://www.microsoft.com/en-us/download/details.aspx?id=28190

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。

该产品有两个安装软件包，分别适用于 32 位操作系统（标记为 x86）和 64 位操作系统（标记为 x64）。确保对特定的操作系统使用正确的安装软件包。

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。该号码可在光盘包装上找到。如果您是以在线方式购买 AVG 拷贝，那么许可证号码已通过电子邮件发送给您。

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，您可选择要在此安装过程中使用的语言并单击***下一步***按钮。

稍后在安装过程中，还可以为应用程序界面选择其它语言。

3.2. 许可协议

您可在此对话框中阅读许可条款。使用***可打印版本***按钮可在新窗口中打开许可证文本。点击***接受***按钮进行确认并继续进入下一个对话框。

3.3. 激活您的许可证

在***激活您的 AVG 许可证***对话框中，您需要填写您的许可证号码。

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。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），建议使用复制粘贴方法插入它。

按 ***下一步*** 按钮继续执行安装过程。

3.4. 选择安装类型

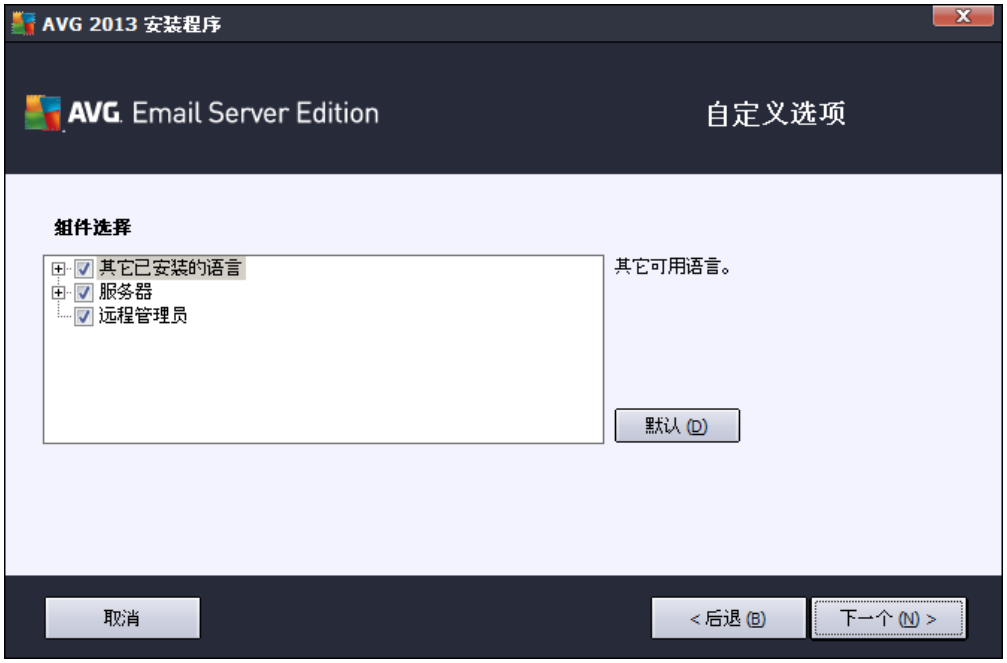
选择安装类型 对话框提供了以下两个安装选项供您选择：***快速安装*** 和 ***自定义安装***。

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

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

选择自定义安装后，***目标文件夹***一节将会在此对话框的底部显示。这可让您指定应安装 AVG 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。

3.5. 自定义安装 - 自定义选项



组件选择部分显示了所有可安装的 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！

- ***远程管理员*** - 如果想要将 AVG 连接到一个 AVG DataCenter (AVG Network Edition)，则需要选中此选项。
- ***其它已安装的语言*** - 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（位于***服务器***分支下）：

- ***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。

- ***Email 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。

- ***Email 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。（在使用 EDGE 和 HUB 角色时均可安装）。

- ***Email Scanner for MS Exchange (VSAPI)***

  可检查存储在用户邮箱中的所有电子邮件。如果检测到病毒，则会将其移至隔离区中或完全删除。

Exchange 2003 的用户仅可使用 Anti-Spam 和 Email Scanner (VSAPI) 组件。

按***下一步***按钮以继续。

3.6. 完成安装

如果您在模块选择过程中选择了***远程管理员***模块，则可以在最后的屏幕中定义用于连接到 AVG DataCenter 的连接字符串。

此对话框还可让您决定是否要参加产品改进计划，该计划用于收集有关所检测到威胁的匿名信息，以便提高 Internet 的整体安全程度。如果您同意此声明，请选中***我同意参与 AVG 产品改进计划提高我的安全程度，以符合 AVG 隐私政策***选项 *默认情况下已确认此选项*)。

单击**完成**按钮确认所作的选择。

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。

4. 安装后

安装完成后会立即显示 ***AVG Email Server Edition 2013*** 主屏幕：

只可手动使用 ***AVG Email Server Edition 2013*** 特定功能进行处理；AVG 桌面手册中描述了所有其他组件和设置。要访问主服务器组件对话框，请单击***服务器***按钮。您将会看到以下屏幕：

请注意，仅当您使用的是 MS Exchange 2007 或更高版本，所有服务器组件才可用 除非在安装过程期间您选择不安装某些服务器组件）。MS Exchange 2003 仅支持 Anti-Spam 和 Email Scanner (VSAPI) 组件。

要对邮件服务器逐一设置保护措施，请按相应章节操作：

- ***Email Scanners for MS Exchange***
- ***Anti-Spam Server for MS Exchange***
- ***AVG for Kerio MailServer***

5. E-mail Scanners for MS Exchange

5.1. 概述

各 Email Scanner 服务器组件的基本概述：

- ***EMS（路由选择）- Email 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 2007/2010，并且仅在使用 HUB 角色时才可安装。

- ***EMS (SMTP) - Email 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 2007/2010，并且在使用 EDGE 和 HUB 角色时均可安装。

- ***EMS (VSAPI) - Email Scanner for MS Exchange (VSAPI)***

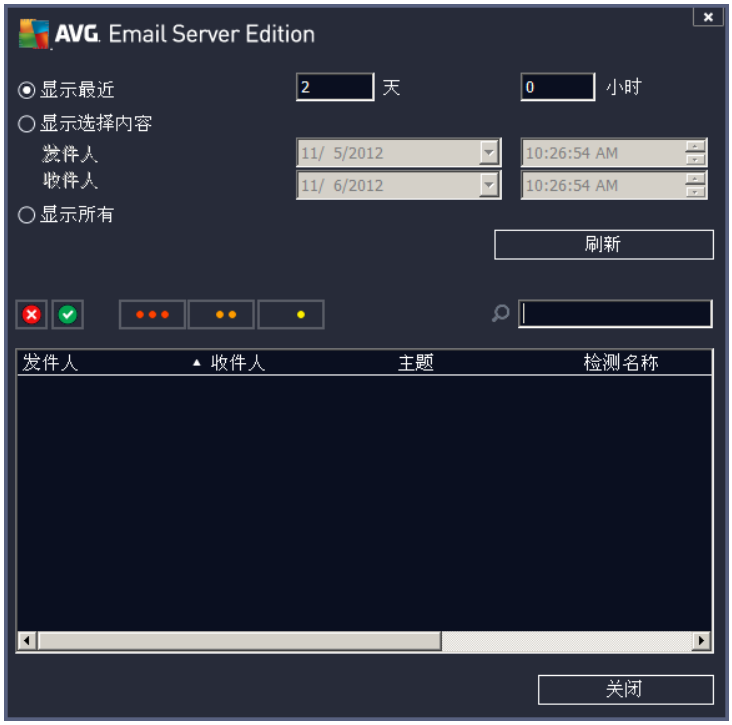
  可检查存储在用户邮箱中的所有电子邮件。如果检测到病毒，则会将其移至隔离区中或完全删除。

单击所需的组件图标以打开其界面。所有组件均共享以下公共控制按钮和链接：

- ***已启用/已禁用*** - 单击此按钮将会启用/禁用所选组件 如果组件已启用，则此按钮和文本为绿色；如果未启用，则为红色）。

- ***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：

- ***显示最近*** - 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。

单击***设置***工作按钮可打开所选组件的高级设置 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. E-mail Scanner for MS Exchange（路由选择传输代理）

要打开 ***Email 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 ***Email 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*** - 取消选中状态以禁用整个组件。
- ***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。

"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。
- ***报告增强型可能不需要的程序*** - 选中此框可检测更多间谍软件：程序直接从制造商处获得时极其安全而无害，但之后却可能被滥用以达到恶意目的，或者程序始终是无害的，但可能并不需要（各种工具栏等）。这项附加措施可以进一步提高计算机的安全性，但也可能会阻止合法程序，因此默认情况下已将其禁用。注意：该检测功能是以前选项中没有的，因此，如果要抵御基本类型的间谍软件，请始终选中以前的框。
- ***扫描压缩包*** - 选中此选项可让扫描程序也对存档文件（zip、rar 等）的内部进行扫描。

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***

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

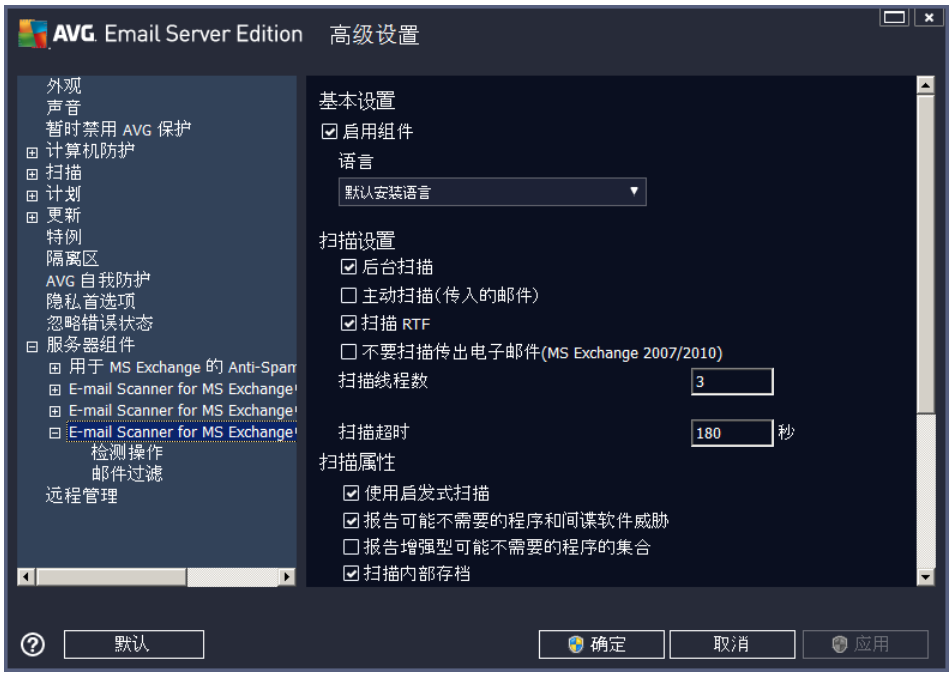
Email Scanner for MS Exchange(SMTP 传输代理)的配置与采用路由选择传输代理时完全相同。有关更多信息，请参见上面的 ***Email Scanner for MS Exchange（路由选择传输代理）***一章。

下面的树结构中也有以下子项：

- ***检测操作***
- ***邮件过滤***

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

此项中有 ***Email 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。

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 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。

溢出消息会继续发出，直到不扫描存储空间为止。

即使同时禁用***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在用户尝试用 MS Outlook 客户端下载邮件时仍处于活动状态。

- ***扫描 RTF*** - 可在此处指定是否应该扫描 RTF 类文件。
- ***不要扫描传出电子邮件 (MS Exchange 2007/2010)*** - 在同时安装 VSAPI 和路由传输代理（[路由 TA](#)）服务器组件（可以是安装在同一台服务器，也可以是安装在两台不同的服务器上）时，可能会出现对传出邮件扫描两次的情况。第一次扫描由 VSAPI 按访问扫描程序完成，第二次则由路由选择传输代理完成。这可能在一定程度上降低服务器性能，并可能导致电子邮件发送略微延迟。如果您确定已同时安装并激活这两个服务器组件，可通过选中该框并禁用 VSAPI On-access 扫描程序来避免这种对传出电子邮件扫描两次的问题。
- ***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。

- ***报告增强型可能不需要的程序*** - 选中此框可检测更多间谍软件：程序直接从制造商处获得时极其安全而无害，但之后却可能被滥用以达到恶意目的，或者程序始终是无害的，但可能并不需要（各种工具栏等）。这项附加措施可以进一步提高计算机的安全性，但也可能会阻止合法程序，因此默认情况下已将其禁用。注意：该检测功能是以前选项中没有的，因此，如果要抵御基本类型的间谍软件，请始终选中以前的框。

- ***扫描内部存档*** - 选中此选项可让扫描程序也对存档文件（zip、rar 等）的内部进行扫描。

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/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***

5.5. 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。

这些操作可用于以下项：

- ***高严重性检测*** - 自我复制和传播的恶意代码，通常直到造成破坏时才会被发觉。
- ***中等严重性检测*** - 一般而言，既包括确实威胁严重的程序，也包括对您的隐私存在潜在威胁的程序。
- ***信息严重性检测*** - 包括所有检测到但不能归入上述任何类别的潜在威胁。

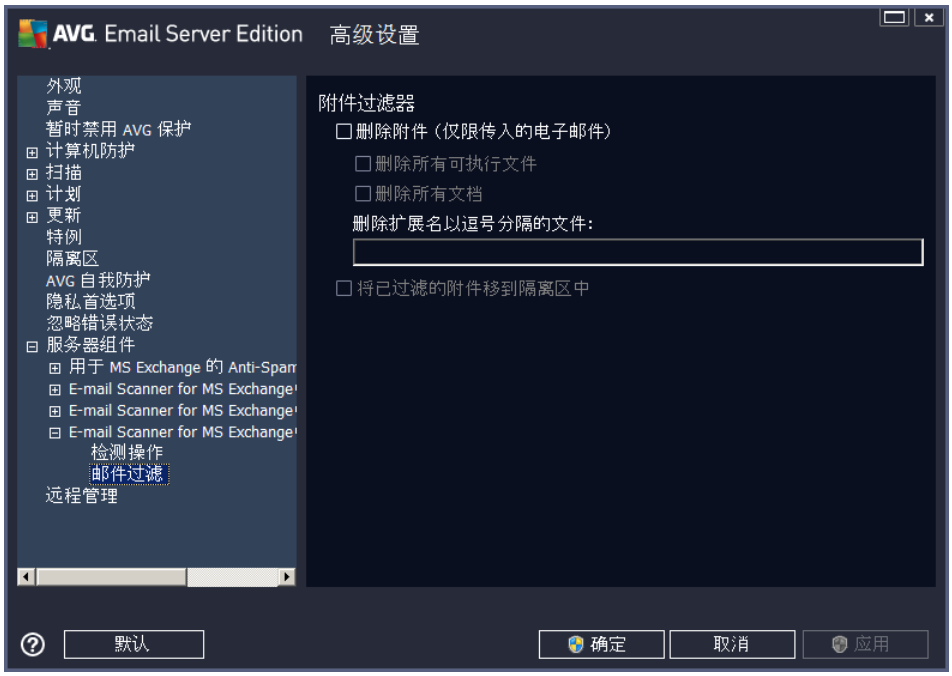
用下拉菜单为每一项选择操作：

- ***无*** - 不会执行任何操作。
- ***隔离*** - 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，然后填入最合意的值。

最后提到的功能不能用于 Email Scanner for MS Exchange VSAPI。

5.6. 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。
- ***将已过滤的附件移到隔离区中*** - 如果不希望完全移除已过滤的附件，则选中此项。选中此框后，在此对话框中选中的所有附件都将自动移入病毒库隔离区环境。它是存储潜在恶意文件的安全位置 - 您可以查看和检查它们而不会危害您的系统。可以从 **AVG Email Server Edition 2013** 主界面的上方菜单中访问病毒库。只需左键单击***选项***菜单项，并从下拉菜单中选择***病毒库***菜单项。

6. Anti-Spam Server for MS Exchange

6.1. 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，发送至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。

6.2. Anti-Spam 界面

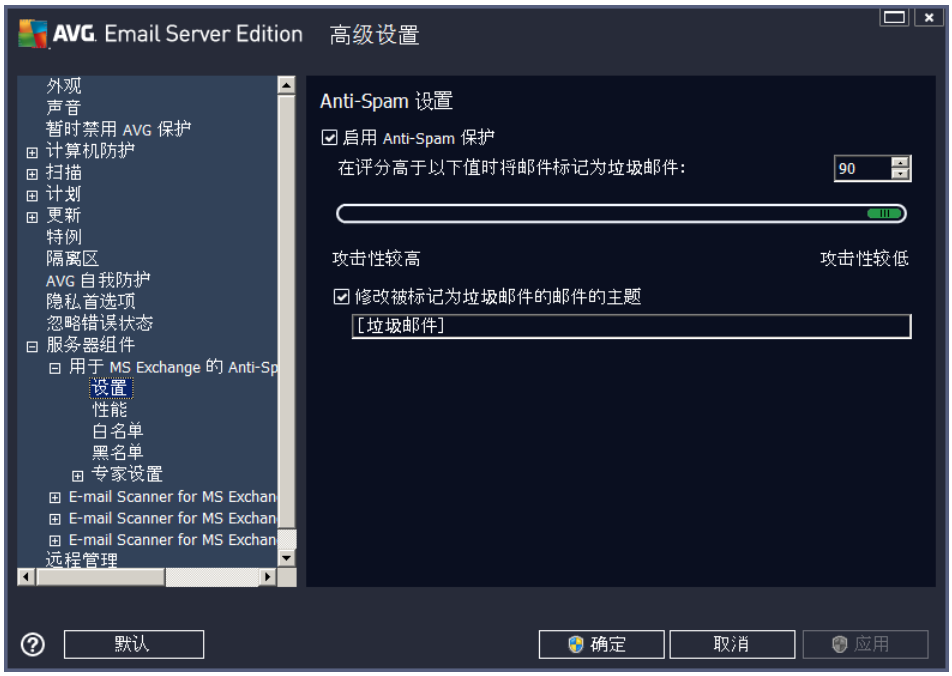
此对话框包含有关服务器组件功能的简短信息和有关其当前状态（*已启用/已禁用*）的信息及一些统计。

提供的按钮和链接：

- ***已启用/已禁用*** - 单击此按钮将会启用/禁用所选组件（如果组件已启用，则此按钮和文本为绿色；如果未启用，则为红色）。
- ***刷新统计值*** - 可更新上面显示的统计数据。
- ***设置*** - 使用此按钮打开高级 Anti-Spam 设置。

6.3. 反垃圾邮件设置

6.3.1. 设置



在此对话框中，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 *(50 到 90)* 或向左或向右移动滑块。

下面对评分阈值进行了大致介绍：

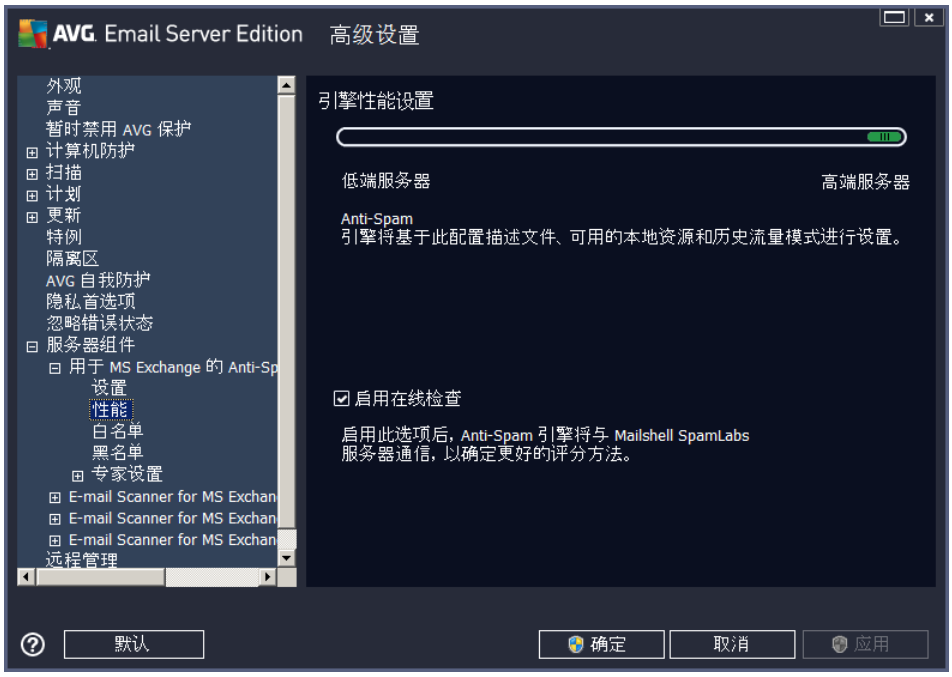
- ***值 90*** - 大多数传入的电子邮件都将正常传送（而不会被标记为垃圾邮件）。最容易识别的垃圾邮件将被过滤掉，但大量的垃圾邮件可能仍被允许传入。
- ***介于 80 和 89 之间的值*** - 将过滤掉很有可能是垃圾邮件的电子邮件。有些并非垃圾邮件的邮件也可能会被错误地过滤掉。
- ***介于 60 和 79 之间的值*** - 这些值被认为是相当严格的配置。将过滤掉有可能是垃圾邮件的电子邮件，也有可能会拦截非垃圾邮件。
- ***介于 50 和 59 之间的值*** - 非常严格的配置。并非垃圾邮件的电子邮件很有可能会被当成真正的垃圾邮件而被捕获到。为了正常使用，不建议采用此阈值范围。

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。
- ***在报告错误检测之前询问*** - 前提是您在安装过程中同意了参与产品改进计划 - 此计划有助于我们从世界各地的所有参与者处收集有关最新威胁的最新信息，然后我们就会以更严密的

保护回报大家 - 即允许向 AVG 报告检测到的威胁。系统会自动处理报告过程。不过，您可以选中此复选框，确认您希望在向 AVG 报告任何检测到的垃圾邮件之前向您询问，以确保该邮件确实应该分类为垃圾邮件。

6.3.2. 性能



引擎性能设置对话框 *(通过左侧导航区域中的**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***低端服务器***模式，最右侧为***高端服务器***模式。

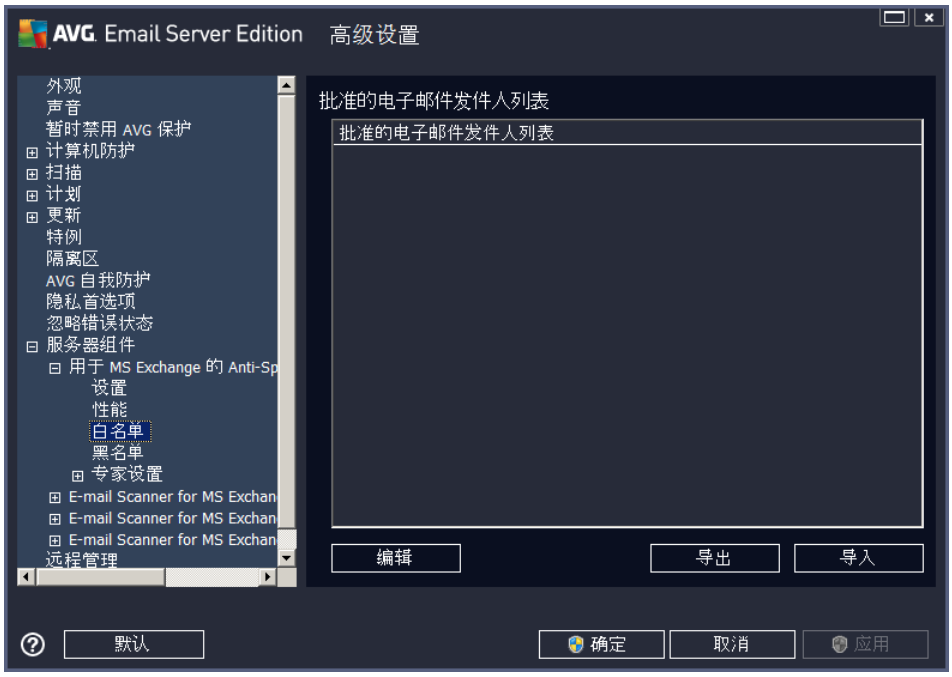
- ***低端服务器*** - 在扫描过程中识别垃圾邮件时，不使用任何规则。只使用培训数据进行识别。在一般使用情形中不建议采用此模式，除非计算机硬件配置非常低。
- ***高端服务器*** - 采用此模式时将占用大量内存。在扫描过程中，将使用以下功能来识别垃圾邮件：规则和垃圾邮件数据库缓存、基本规则和高级规则、垃圾邮件制造者的 IP 地址和垃圾邮件制造者数据库。

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！

6.3.3. 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。



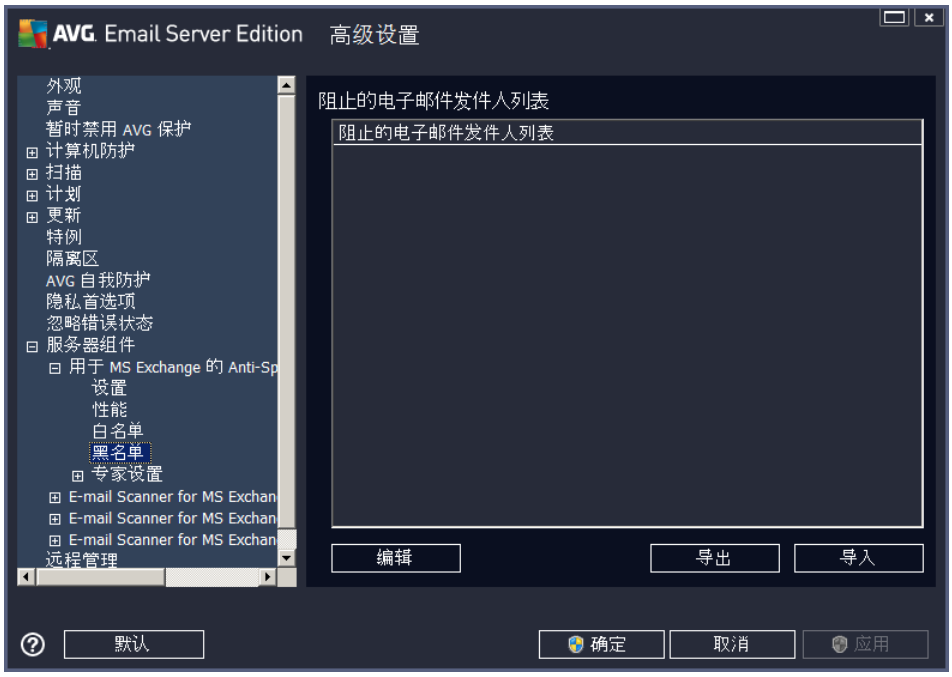
在此编辑界面中，您可以整理一个您确定绝不会向您发送不需要的邮件（垃圾邮件）的发件人名单。您还可以整理一个您知道不会产生垃圾邮件的完整域名（如 *avg.com*）列表。

这样的发件人和/或域名列表一准备好，就可以通过以下任一方法输入发件人和/或域名：直接输入每个电子邮件地址或一举导入整个地址列表。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*复制粘贴法*）。每行请插入一项内容（发件人或域名）。
- ***导入*** - 通过选择此按钮可以导入现有的电子邮件地址。输入文件可以是文本文件（采用纯文本格式，并且内容中每行只能包含一个项目 - 地址、域名）、WAB 文件，或者可以从 Windows 地址簿或 Microsoft Office Outlook 中完成导入。
- ***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。

6.3.4. 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认定为垃圾邮件。

这样的发件人和/或域名列表一准备好，就可以通过以下任一方法输入发件人和/或域名：直接输入每个电子邮件地址或一举导入整个地址列表。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*复制粘贴法*）。每行请插入一项内容（发件人或域名）。
- ***导入*** - 通过选择此按钮可以导入现有的电子邮件地址。输入文件可以是文本文件（采用纯文本格式，并且内容中每行只能包含一个项目 - 地址、域名）、WAB 文件，或者可以从 Windows 地址簿或 Microsoft Office Outlook 中完成导入。
- ***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。

6.3.5. 专家设置

此分支包含大量用于 Anti-Spam 组件的设置选项。这些设置仅面向经验丰富的用户，通常是需要对反垃圾邮件保护措施进行详尽配置，以便对邮件服务器实施最严密保护的网络管理员。因此，我们未对各个对话框提供其它帮助信息；但是，在用户界面中直接对每个选项作了简短说明。

如果您对 Spamcatcher (MailShell Inc.) 的高级设置不是非常熟悉，我们强烈建议您不要更改任何设置。更改不当可能会导致性能严重降低或组件功能失常。

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

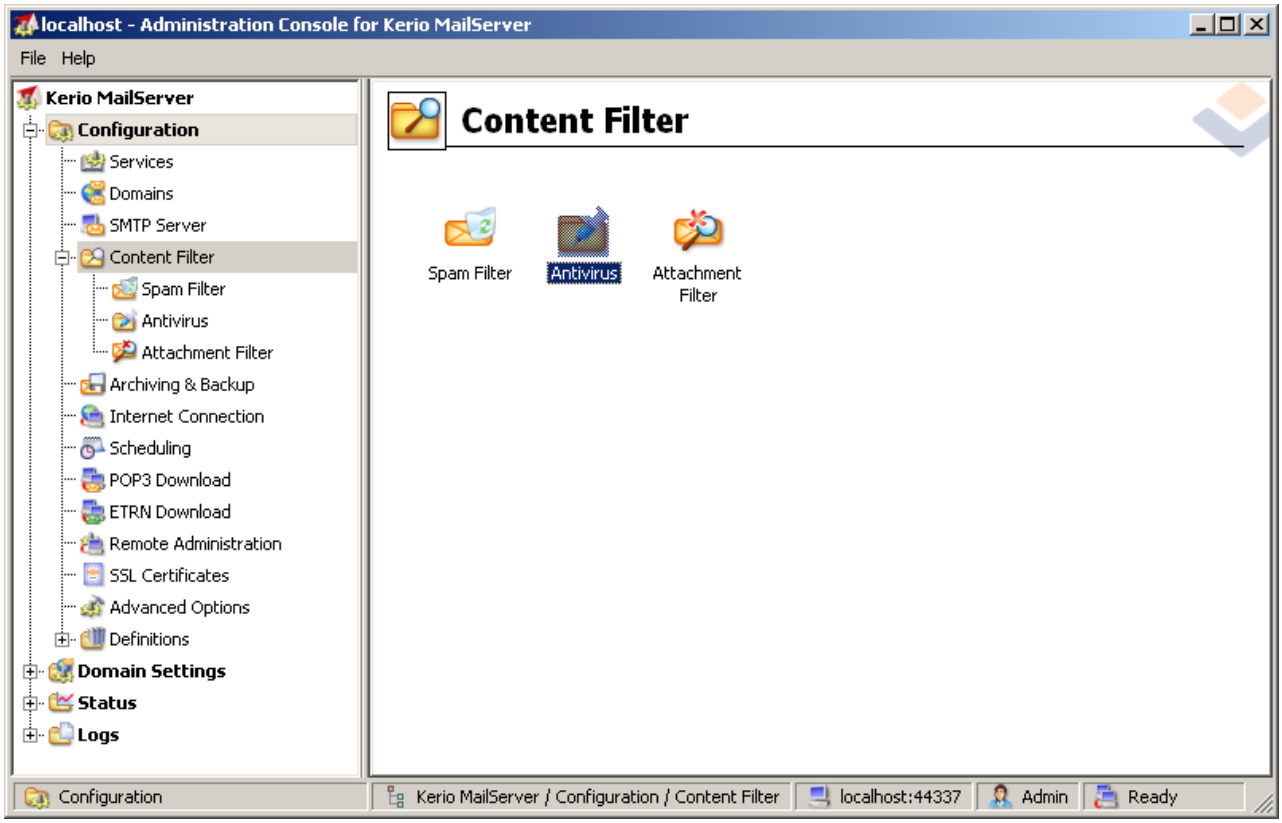
作。一般而言，在每一个对话框中都会有一项特定的功能，您可以进行编辑 –其说明总是包含在该对话框本身中：

- ***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

7. AVG for Kerio MailServer

7.1. 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：

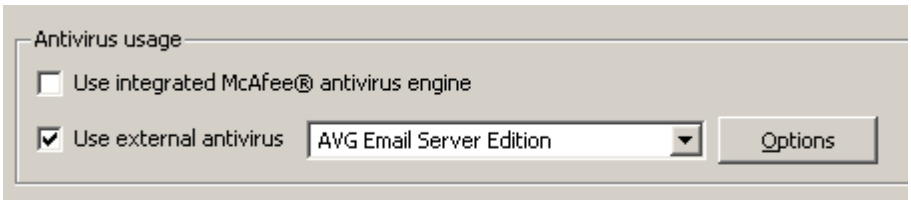


单击 "Content Filter" 项会显示一个对话框，其中有三项：

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

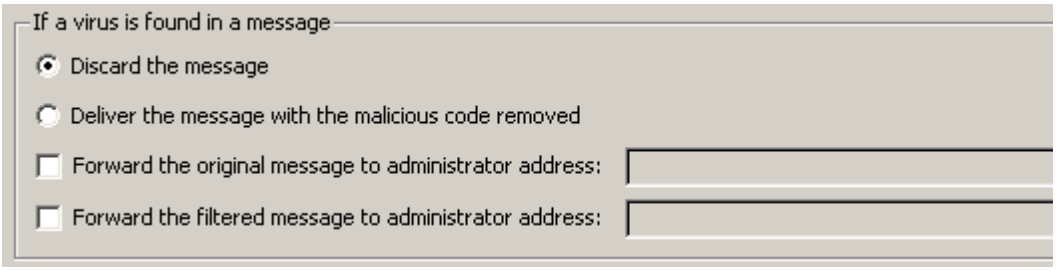
7.1.1. 防病毒

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：

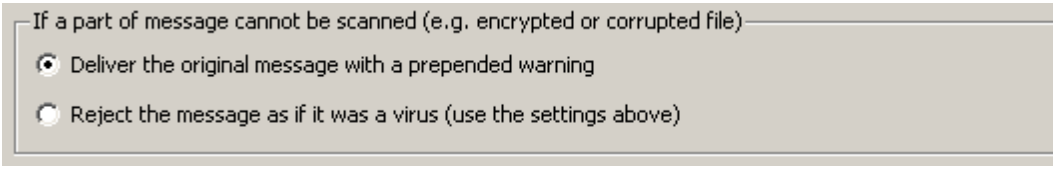
- ***如果邮件中有病毒***



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）***



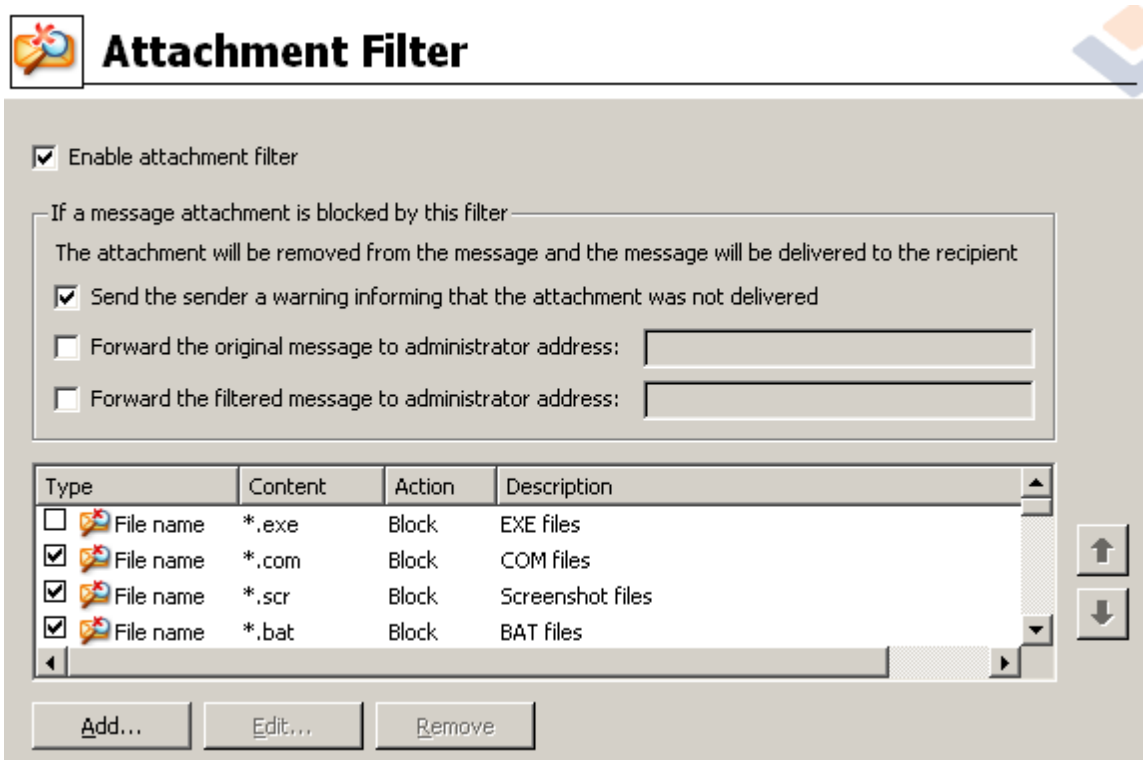
此框用于指定不能对邮件或附件的一部分进行扫描时所要执行的操作：

  - ***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。

7.1.2. 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。

8. 常见问题解答和技术支持

任何关于 AVG 的问题，无论是商业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。