我们为数字世界提供保护


# 安装及使用手册

**集成组件：**

防病毒
反间谍软件
防火墙
反垃圾邮件

# 目 录

# 1. ESET NOD32 安全套装 4.0

ESET NOD32 安全套装 4.0 是第一款真正高度集成的计算机安全系统，引领了整合式安全软件的新兴潮流。内置新版 TheatSense®扫描引擎，继承了 ESET NOD32 安全套装的快速和精准优势，量身定制的个人防火墙和防垃圾邮件模快紧密结合。一套智能的防御系统，对危害计算机安全的恶意软件和攻击，保持着时刻的警惕。

ESET NOD32 安全套装 4.0 绝不像某些产品那样，只是对多款功能性产品进行简单堆砌和捆绑。经过我们的长期努力在保证最优防护效果的基础上，对系统资源占用保持到最小,这是一款两者完美结合的产品。基于人工智能的高级主动防御技术，有效保护系统免于病毒、间谍软件、木马、蠕虫、广告程序、RootKit、网络攻击和渗透，同时不会降低系统性能或干扰用户使用计算机。

## 1.1 新特性

ESET NOD32 安全套装 4.0 推出的全新构架，完美展示了我公司多位专家长期以来的开发经验，在保证最小系统要求的前提下，达到最大化的监测效果。复合安全方案包含多个模块，支持高级选项设置。下表对这些模块进行简要介绍。

**▪ 防病毒与反间谍软件**

此功能模块使用 ThreatSense®扫描内核。ThreatSense®首次应用在 ESET NOD32 安全套装中，并屡获殊荣。ThreatSense®内核在全新的 ESET NOD32 安全套装 4.0 构架中的得到了进一步优化和改进。

| 特性 | 描述 |
|---|---|
| 清除能力更强 | 本防病毒系统可以在无需用户介入的情况下，智能清理和删除检测到的大部分威胁 |
| 后台扫描模式 | 计算机扫描可以在后台进行，绝不会拖慢机器性能。 |
| 升级文件体积更小 | 核心的优化使升级文件与 2.7 版相比更小巧，同时增强了对升级文件的保护，免于受损。 |
| 常见电邮客户端保护 | 目前不仅可以扫描 MS Outlook 的入站邮件，同时还支持 Outlook Express、Windows Mail 、Windows Live Mail 和 Mozilla Thunderbird |
| 其它的小改进 | -支持对文件系统的直接访问，实现高速的海量数据扫描<br>-拦截对感染文件的访问<br>-优化对包括 Vista 在内的 Windows 安全中心的支持 |

**▪ 个人防火墙**

个人防火墙可以监测本地计算机与网络中其他计算机间的所有通讯。ESET 个人防火墙包括如下列出的高级功能。

| 特性 | 描述 |
|---|---|
| 底层网络通讯扫描 | 对数据链底层网络通讯进行扫描，使个人防火墙有能力检测到各种其他途径很难检测到的攻击。 |
| IPv6 支持 | 个人防火墙可以显示 IPv6 地址，同时允许用户为它们创建规则。 |
| 可执行文件监控 | 监测所有可执行文件的修改，避免文件感染带来的威胁，同时可以允许数字签名程序修改文件。 |
| 文件扫描支持 HTTP 和 POP3 | 将文件扫描集成于 HTTP 与 POP3 应用协议中。保护用户上网冲浪和下载 Email 时的网络安全。 |
| 入侵检测系统 | 具备识别网络通讯和各类网络攻击特征的能力，允许用户选择是否自动拦截此类通讯。 |
| 支持交互、自动、和基于规则三种模式 | 用户可以选择防火墙自动处理，也可以通过交互行为设定进出站规则。“策略”模式下的网络通讯，完全依照用户或网络管理员预先设定的规则执行。 |
| 全面超越 Windows 内置防火墙 | 全面超越 Windows 内置防火墙的同时，与 Windows 安全中心交互，以便用户了解自己的安全状态。ESET NOD32 安全套装 安装程序在默认状态下会关闭 Windows 的内置防火墙。 |

**▪ 反垃圾邮件**

反垃圾邮件模块，能够过滤来路不明的邮件，提高网上交流的安全性和舒适性。

| 特性 | 描述 |
| --- | --- |
| 入站邮件分值系统 | 所有的入站信件依照分值系统，从 0（非垃圾邮件）到 100（垃圾邮件）的标准打分，邮件将根据评分结果，转移到垃圾邮件夹或由用户创建的定制文件夹。入站邮件可以并行扫描。 |
| 支持多种扫描技术 | 贝叶斯分析技术<br>规则式扫描技术<br>全球特征数据库比对 |
| 与电邮客户端全面整合 | 反垃圾防护支持 Microsoft Outlook, Outlook Express、Windows Mail Windows Live Mail 和 Mozilla Thunderbird clients 客户端 |
| 可以手动分检垃圾邮件 | 可以手动标记电邮是否为垃圾邮件。 |

## 1.2 系统要求

为使 ESET NOD32 安全套装和 ESET NOD32 安全套装商业版正常运行，需要系统硬件和软件最低配置如下：

ESET NOD32 安全套装 4.0 :

| | |
| --- | --- |
| Windows 2000, XP | 400MHz处理器<br>32位/64位系统(x86 / x64)<br>128 MB RAM系统内存<br>130MB可用硬盘空间<br>Super VGA (800 × 600)显示分辨率 |
| Windows Vista | 1GHz 处理器<br>32位/64位系统(x86 / x64)<br>512MB RAM系统内存<br>130MB可用硬盘空间<br>Super VGA (800 × 600)显示分辨率 |

- **其它新增功能**

| 特性 | 描述 |
| --- | --- |
| ESET SysRescue | 用户可以通过 ESET SysRescue 来创建包含 ESET NOD32 的 CD/DVD/USB 启动盘，因为启动盘独立于操作系统，因此可以用来清除系统中难于清除的病毒。 |
| ESET SysInspector | ESET SysInspector 可以用来全面检查您的电脑。现在已经被集成到 ESET NOD32 4.0 产品中。如果您的电脑发生状况，可以通过此工具生成日志。我们的工程师可以通过分析日志来了解具体状况。 |
| 文档防护 | 此模块用来在打开或者通过 IE 下载 Microsoft Office 文件前预扫描 |
| 自我保护 | 新增加的自我保护功能能防止 ESET NOD32 本身被病毒破坏或者关闭。 |
| 用户界面 | 新增加了文字模式界面，允许用户通过键盘来操作 ESET NOD32.改进了和其它屏幕读取软件的兼容性，提供了更好的操作简易性。 |

# 2. 安　装

在开始安装前，请关闭所有运行中的其他程序。安装 ESET NOD32 安全套装之前，强烈建议您在安装之前卸载其他已经安装的防病毒程序，以避免发生冲突。

## 2.1 开始安装

下载完成后双击安装程序将开始进行安装。请按照安装步骤的提示点击‘**下一步**’，依次完成：授权许可、安装模式的设定、，然后您将看到以下激活码输入页面：


请在以上激活码输入界面中填写您的产品激活码，邮箱以及您的姓名。在输入完成后，点击**“下一步”**完成激活。如果激活成功，程序将显示您的产品有效期以及您的激活时输入的个人信息。如果激活失败则会显示相应的失效原因。在激活成功后，请按照安装提示点击**“下一步”依次**完成后续步骤。


点击“完成”后整个安装过程即结束，ESET NOD32 将开始保护您的电脑。

如果您的电脑没有连接到互联网，ESET NOD32 安全套装将无法激活，您可以稍后再通过点击桌面上的激活快捷图标来完成激活；如果您的产品将到有效期或者已经过期，您可以通过续费来延长您的有效期，请点击 windows 系统左下角的**“开始——程序——ESET——ESET Smart Security——产品续费”**来进行续费操作。

## 2.2 计算机扫描

安装 ESET NOD32 安全套装后，应对计算机进行扫描，查看是否存在病毒。在主菜单中选择计算机扫描，然后再程序主窗口中选择标准扫描即可。关于扫描计算机的更多信息，请参阅**‘计算机扫描’**一章。

# 3. 入门指南

本章将对 ESET NOD32 安全套装及其基本设置进行简要描述。

## 3.1 用户界面介绍

ESET NOD32 安全套装的主窗口分为两个主要部分。左侧的的栏目提供了清晰、易用的主菜单，主窗口右侧的显著位置显示了主菜单对应项的相关信息。

下面是对主菜单按钮的描述：

**防护状态**----显示了 ESET NOD32 安全套装的防护状态信息。如果激活了高级模式，所有防护模块的状态都会得到显示。可以单击相应模块查看它的当前状态。

**计算机扫描**--此选型允许用户设置和进行手动扫描。

**更新**---------选择此项进入管理病毒库更新的升级模块。

**设置**---------选择此项调整您的计算机安全级别。如果激活了**高级模式**：还将显示防病毒、反间谍、个人防火墙和反垃圾邮件模块的子菜单。

**工具**---------此选项仅在高级模式下可用。可以访问日志、隔离区、计划任务和 SysInspector。

**帮助和支持**--选择此项可以访问帮助文档、ESET 知识库、ESET 网站，提交求助信息以及联系客服部门等。

ESET NOD32 安全套装用户界面允许用户在标准模式和高级模式间切换。通过 ESET NOD32 安全套装主窗口左下角的显示链接，可以在两种模式间自由切换。请点击这个按钮来选择想要的模式。


标准模式中提供了对基本功能的访问，适合普通操作的应用，而不显示各种高级选项。


切换至‘**高级模式**’则会在主菜单添加‘**工具**’选项。‘**工具**’菜单允许用户访问**计划任务、隔离区**，或浏览 ESET NOD32 安全套装日志文件和进行系统快照（SysInspector）的相关操作。

**注意**：本指南以下内容只适用于高级模式。

### 3.1.1 检查系统运行状态

点击主菜单顶层的这个选项，可以浏览‘**防护状态**’。窗口右侧将显示 ESET NOD32 安全套装的运行状态摘要，同时出现三个子菜单：‘**病毒和间谍软件防护**’、‘**个人防火墙**和**反垃圾邮件**’模块。选择任一项浏览对应防护模块的详细信息。


如果启用的模块工作正常，他们将用绿色的勾号表示。反之则显示红色叹号或橙色的提示图标。该模块的其他有关信息显示在窗口的上方，同时显示的还有推荐的解决方案。要改变某个模块的状态，在主菜单中点击‘**设置**’，并单击需要操作的模块。

### 3.1.2 程序工作不正常该如何处理？

ESET NOD32 安全套装 4 如果在各防护模块中检测到错误，将在‘**防护状态**’窗口中显示相关信息，同时提供相关的解决方案。

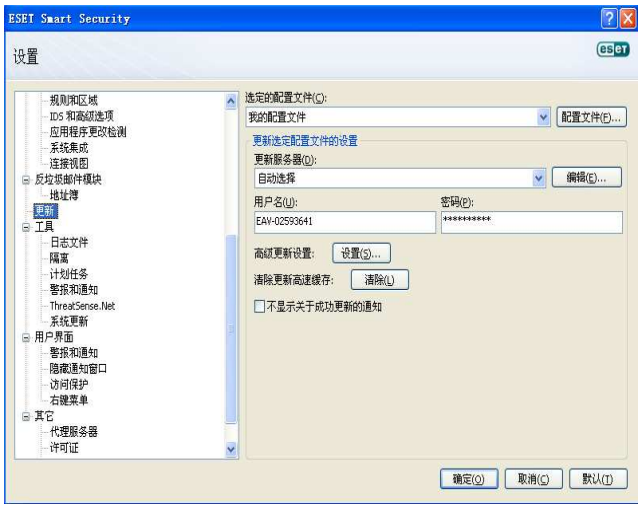

如果已知问题列表和解决方案不能解决问题，请点击‘**帮助和支持**’查看帮助文件或搜索 ESET 知识库。如果您仍然没有找到解决方法，您可以向 ESET 客户服务提交支持请求。我们的专家将根据您的反馈尽快回复您的问题，给您及时、有效的建议。

## 3.2 更新设置

对病毒特征数据库和程序组件的更新，是有效防护恶意代码的重要组成部分，因此它们的设置和运行请给予特别的关注。在主窗口中请选择‘**更新**’，单击主窗口中的‘**更新病毒库**’，来立即查询当前是否有可用更新。‘**用户名和密码设置**’将显示输入用户名和密码的对话框。

用户名和密码是在激活产品时由系统自动设定的，不能随意更改。如果您的用户名和密码已经过期或者被误修改，请用主界面的‘**产品激活**’入口重新激活一个有效的产品激活码。


‘**高级设置**’窗口（快捷键 F5）包含升级设置的其他详细选项。‘**更新服务器**’下拉列表应设置为自动选择。诸如更新模式、代理服务器连接等高级更新设置选项，请点击‘**设置**’按钮。



### 3.2.1 新建更新任务

在主菜单点击更新后，在显示的信息窗口可以点击‘**更新病毒库**’的方式进行手动更新。

也可以通过排程的方式进行更新。配置排程任务时，请点击‘**工具**’>‘**计划任务**’。默认状态下，ESET NOD32 安全套装自动运行以下任务：

----定期自动更新
----拨号连接后自动更新
----用户登录后自动更新

上述提到的每项更新任务都可以人工编辑，以满足您的需要。除默认更新任务外，您也可以按照您的需要，新建自定义更新任务。关于新建和配置更新任务的细节，请参阅‘**计划任务**’一章。

### 3.2.2 代理服务器设置

如果您在安装 ESET 安全套装的系统上，使用代理服务器中转您的 Internet 连接，代理服务器必须在高级设置（F5）中指定。在高级设置中点击 ‘**其他**’>‘**代理服务器**’进入代理服务器设置窗口。选中‘**使用代理服务器**’复选框，输入 IP 地址、端口和认证信息。


如果您没有这些信息，您可以通过点击‘**检测代理服务器**’按钮，ESET NOD32 安全套装会尝试自动检测代理服务器设置。

**注意：**在不同的升级配置中，代理服务器选型可能不同。如果您遇到这种情况，可以到高级升级设置中配置代理服务器。

## 3.3 设置信任域

信任域设置是在网络环境下保护您的计算机的重要步骤。您可以通过在信任域中允许共享，来允许其他用户访问您的计算机。依次单击‘**设置**’>‘**个人防火墙**’>‘**修改您的计算机在网络中的保护模式**’，在出现的窗口中，您可以配置计算机在网络中的保护模式。

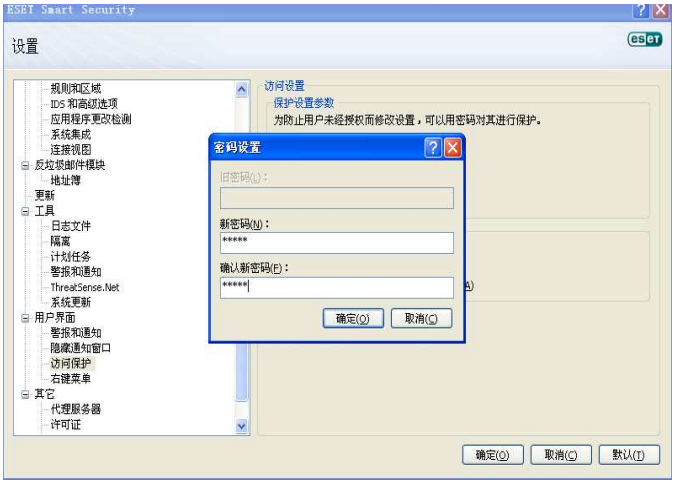

在 ESET NOD32 安全套装安装后，或每当计算机接入新的网络时，ESET NOD32 安全套装会完成对信任域的检测。因此在大多数情况下，用户不需设置信任域。

默认设置下，在检测到新的域后，ESET NOD32 安全套装将显示对话框允许您设置该域的防护等级。

**警告！**信任域设置错误将给您的计算机带来风险。
**注意：**默认情况下，信任域中的工作站有权访问共享文件和打印机，同时启用 RPC 通讯，允许远程桌面共享。

## 3.4 设置密码保护

为使您公司的安全策略充分发挥作用，ESET NOD32 安全套装的设置非常重要。非法修改这些设置可能影响您系统的稳定性和安全性。您可以在主菜单中依次单击‘**设置**>**高级设置**>**用户界面**>**访问保护**’点击‘**设置密码...**’按钮，并再次输入确认，然后点击确定。设置完毕后，对 ESET 安全套装设置的任何更改，都需要输入密码才能完成。




## 4.1 病毒和间谍软件防护保护

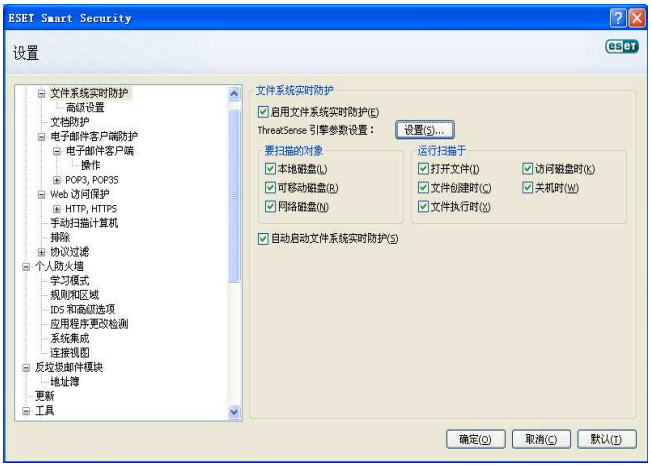
防病毒保护通过控制文件、电邮和互联网通信来阻止有害的系统攻击。当检测到恶意代码威胁时，防病毒组件将首先对其进行拦截然后清除、删除或将其移动至隔离区，从而有效地消灭病毒威胁。

### 4.1.1 文件系统实时防护

文件系统实时防护控制系统中所有与病毒相关的事件。计算机上所有的文件在打开、创建或运行前都会被扫描。文件实时监控系统在操作系统启动时自动加载。

#### 监控设置

文件实时监控检查所有类型的介质时，文件监控会因不同的事件而触发。文件监控利用了 ThreatSense® 技术进行检测（如在 ThreatSense ®引擎的设置部分中所描述）。对新建文件和现有文件的监控可以采用不同的规则，前者可以应用更严格的监控。




#### 要扫描的对象

默认情况下，为寻找潜在的威胁，程序会扫描所有对象。

**本地磁盘**----管理所有的系统硬盘驱动器
**可移动磁盘** - 软盘、USB 存储设备等
**网络磁盘**----扫描所有映射驱动器

我们建议您保留默认设置，仅在某些特定的情况下

修改，例如某些对象在接受扫描时，数据传输速度会明显降低。

**触发扫描**

默认情况下，打开的所有文件在执行和创建时都会进行扫描。为使您的计算机得到最大文件实时防护效果，我们建议您保留默认设置。

访问磁盘时选项提供了访问磁盘时对其引导区的监控。关机时选项提供关机时对硬盘引导区的监控。尽管目前引导型病毒已经很少见了，我们仍然推荐您开启这些设置，因为被各种来源的引导型病毒感染的可能性仍是存在的。

**用于新建或修改文件的其它 ThreatSense®参数.**

与已存在的文件相比，新建文件或新修改文件被感染的可能性相对较高。这正是 ESET 安全套装程序在扫描这些文件时提供额外参数的原因。对于新建文件，在使用普通特征扫描的同时，还启用了高级启发式扫描，极大提升了病毒检测率。除了新建文件，扫描对象还包括自解压文件（SFX）和加壳程序（压缩后的可执行文件）。默认情况下，压缩文件扫描为 10 层，而且不论其实际规模大小都会进行检查。您可以取消默认设置，修改压缩文件扫描设置。

**用于已存在的文件的其它 ThreatSense 参数**

默认情况下，文件执行时并不启用高级启发式扫描。然而在某些情况下，您可能需要启用此功能（勾选**文件被执行时启用高级启发式扫描**）。请注意，开启高级启发式扫描可能使一些程序的执行速度变慢。

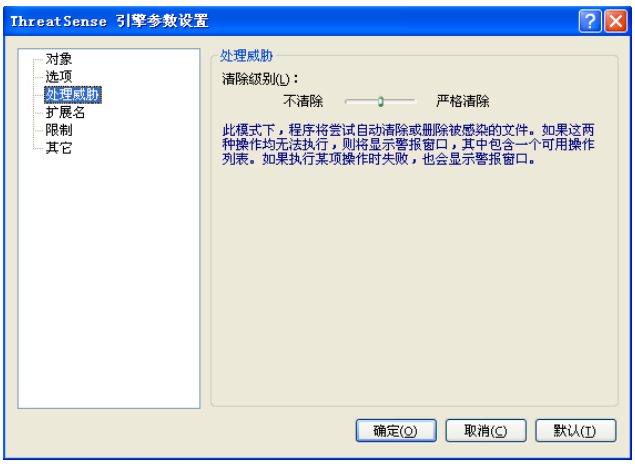
**处理威胁**

实时防护有三个清除等级（访问时请依次点击‘**文件系统实时防护**’部分的‘**设置...**’按钮和‘**处理威胁**’节点）。

第一级为每个检测到的病毒显示警报窗口，列举可选操作。用户需要为每个文件分别选择处理方式。这一级别是为懂得遇到入侵时该如何处理的高级用户设计的

默认级别是自动选择和执行预置操作（由感染类型决定）。对感染文件的检测和删除操作，将通过屏幕右下角的屏幕消息通知用户。然而，如果染毒文件存在于包含正常文件的压缩包中，将不会被自动删除。不符合预定规则的目标，同样不会自动处理。

第三个级别是强化设置 - 所有被感染的目标都会被清除。鉴于这一级别可能导致正常文件的丢失，我们建议您只在必要情况下使用。




**何时修改实时监控配置**

实时防护是保持系统安全最重要的部分，所以请谨慎修改相关设置。我们建议用户，除非特殊情况下不要修改其参数。特殊情况包括实时防护与某一程序或与其他反毒软件互相冲突的情况。

在 ESET NOD32 安全套装安装完成后，所有的设置都已经过优化，以便为用户提供最高级别的系统安全。

可以通过点击文件实时监控窗口‘**高级设置>病毒和间谍软件防护>文件系统实时防护**’右下角的‘**默认**’按钮来还原默认设置。

**检查实时监控**

可以使用 eicar.com 测试文件，检查实时监控系统的工作是否正常、能否同步检测到病毒等。文件是由 EICAR 公司（欧洲计算机防病毒研究机构）制作，用以测试防毒程序的功能。文件 eicar.com 可以由 http://www.eicar.org/download/eicar.com 获得。

**注意:** 在进行实时防护检测前，需要先禁用防火墙。在开启状态下，防火墙将监测，并阻止该文件的下载。

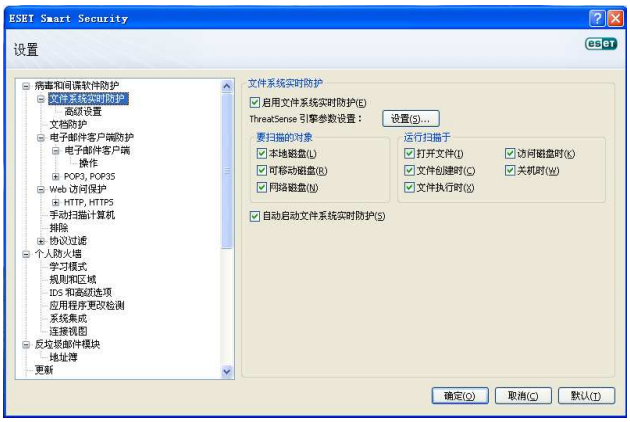
**实时防护无效怎么办**

本章我们将描述实时监控可能产生的问题以及该如何解决它们。

**实时监控被禁用**

如果实时监控被用户不慎禁用，您需要将其重新打开。在‘**设置 > 病毒和间谍软件防护**’主程序窗口中勾选‘**启用文件系统实时防护**’。

如果实时监控没有在每次开机时自动加载，可能是由于禁用了自动启动文件系统实时防护选项造成的。开启此选项，请转到‘**高级设置**’（F5）界面，点击‘**文件系统实时防护**’。确定位于在高级设置窗口底部的‘**自动启动文件系统实时防护**’的复选框已经选中。




**如果实时监控不能检测和清除病毒**

请确认您的计算机上是否安装了其他的反毒软件。如果两种实时监控程序同时启用，它们可能发生冲突。我们建议您卸载您系统上其它的防病毒程序。

**实时监控不能启动**

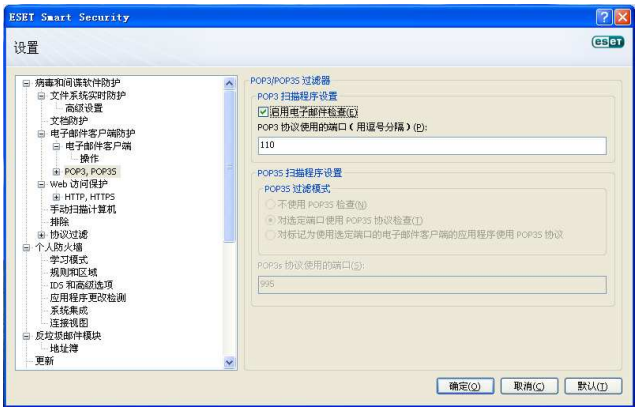
如果实时监控在系统启动时不能初始化（‘**自动启动文件系统实时防护**’选项已经启用），原因可能是 ESET 安全套装与其它程序间的冲突。遇到这种情况，请咨询我们 ESET 客服中心的专家解答。

## 4.1.2 电子邮件客户端防护

电子邮件防护提供了对 POP3 协议电邮通讯的管理。通过使用 Microsoft Outlook 插件，ESET NOD32 安全套装可以控制邮件客户端的所有通信（POP3、MAPI、 IMAP、HTTP）。对于入站邮件，程序会使用 ThreatSense ®扫描引擎提供的各种高级扫描手段进行检测。这意味着在没有与病毒库特征对比之前，对恶意程序的检测已经在进行了。对 POP3 协议通讯的扫描是独立于您的邮件客户端的。

**检测 POP3**

对于邮件客户端而言，POP3 协议是接收邮件时使用最广泛的协议。无论您使用的是何种邮件客户端，ESET NOD32 安全套装 都可以提供对该协议的防护。邮件监控模块随系统自动启动，之后常驻内存。为了让该模块能正常工作，请先确认它已经开启。POP3 检测将自动执行，无需重新配置邮件客户端。默认状态下，所有经由 110 端口的通讯都将被扫描。当然如果必要，还可以添加其它通讯端口。端口间请使用逗号作为界定符。加密通讯将不会监控。



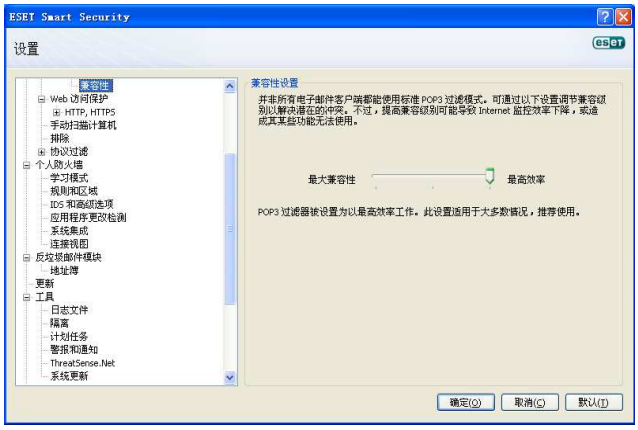

**兼容性**

某些电邮程序在经由 POP3 过滤后可能会遇到问题（例如：如果使用网速较慢的连接进行接收，POP3 检测可能造成客户端超时）。遇到这种情况，可以尝试调整监控方式。降低监控级别能改善清除的速度。您可以转到‘**病毒和间谍软件防护**> **电子邮件防护**>**POP3，POP3S**>**兼容性**’来调整 POP3 过滤的级别。

如果已经启用‘**最高效率**’，有害代码将从感染的消息中移除，原邮件的主题前将插入所感染病毒相关的信息（‘**删除**’或‘**清除**’选项被激活，‘**严格**’或‘**默认**’清除级别必须启用）。

‘**中等兼容级别**’更改了消息收取的方式。邮件会逐步传输到客户端，全部传输完毕后，才进行扫描。然而这个监控级别增加了感染的危险。清除和处理标签消息的级别（将扫描摘要添加到邮件的标题和正文）与最佳效率选项的设置是一致的。

‘**最大兼容性**’中，程序将通过警告窗口提示用户收到感染病毒的邮件。主题和邮件正文中不会添加感染信息，同时邮件中的病毒不会被自动移除。感染文件的删除必须由用户在客户端中完成。



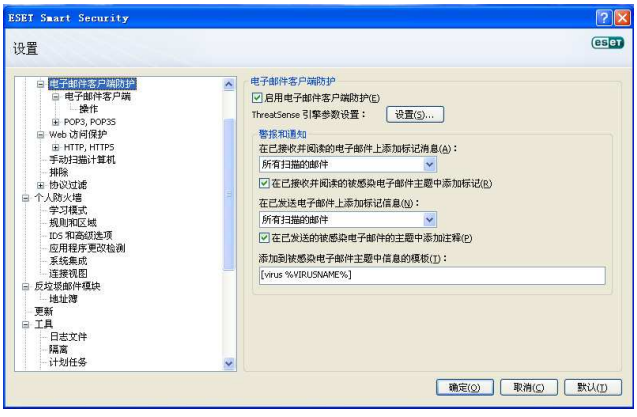

### 与电子邮件客户端整合

与邮件客户端集成后，安全套装将加强对邮件中恶意代码的防护。

如果邮件客户端支持，可以在ESET 安全套装中开启整合功能。在激活整合功能后，ESET 安全套装反垃圾邮件工具栏将直接嵌入邮件客户端中，实现更有效的邮件保护。点击‘**设置**>**高级设置**>**其它**>**电子邮件客户端集成**’对话框，允许您激活与客户端的整合。目前支持的客户端包括：Microsoft Outlook、Outlook Express、Windows Mail、Windows Live Mail 和 Mozilla Thunderbrid。

如果您在使用电子邮件客户端时发现系统变慢，您可以尝试勾选‘**禁用对收件箱内容更改的检查**’项，这种情况一般在您使用Kerio Outlook Connector Store 程序查阅邮件时发生。

通过在‘**高级设置**（F5）>**病毒和间谍软件防护**>**电子邮件客户端防护**’中选中‘**启用电子邮件客户端防护**’复选框可以启动邮件防护。




### 追加消息标记到邮件正文

每封 ESET NOD32 安全套装接收的邮件，都可以在邮件主题和正文添加扫描标签。这项功能为收件人增加了可靠性，如果发现病毒，它可以提供关于指定邮件和发件人风险级别的有用信息。

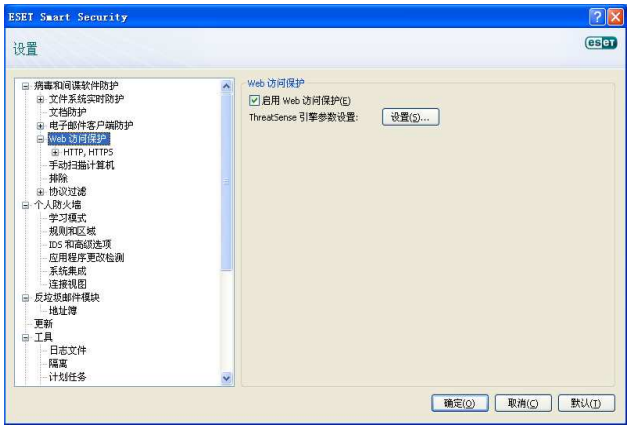
关这一功能的选项可以在‘**高级设置**>**病毒和间谍软件防护**>**电子邮件防护**’中找到。程序不但可以在已接收邮件和已读邮件中添加标签，还可以追加标记消息到已发送邮件。用户也能够决定将标签添加到所有邮件、仅感染邮件或不添加。同时允许用户追加标记到被感染邮件的原标题。要实现这一点，选择‘**在已接收并阅读的被感染电子邮件中添加标记**’和‘**在已发送的被感染电子邮件的主题中添加注释**’。

### 移除病毒

接收到被感染邮件时系统会显示警告窗口。窗口中显示了发件人的名称，被感染邮件和病毒的名称。在窗口的底部，显示针对检测对象的可用操作包括：‘**清除**’、‘**删除**’和‘**离开**’。我们建议您尽量选择‘**清除**’或‘**删除**’，在特殊情况下，当您需要接收被感染文件，可以选择‘**离开**’。如果启用‘**严格清除**’模式，弹出窗口将不显示操作选项。

## 4.1.3 Web 访问防护

Internet 连接个人计算机的普遍性，使它不幸成为恶意代码传播的主要途径。因此，Web 防护功能是必要的。我们强烈建议您激活启用 Web 访问防护选项。该选项位于‘**高级设置**（F5）>**病毒和间谍软件防护**>**Web 访问防护**’中。




### HTTP 和 HTTPS

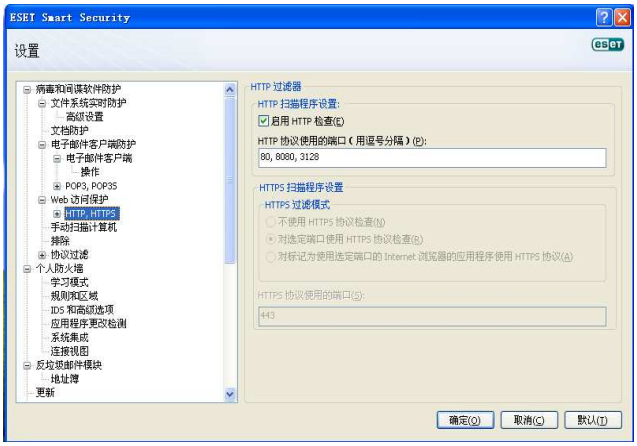
WEB 访问保护通过监控浏览器和远程服务器间的数据通信，并符合 HTTP（超文本传输协议）和 HTTPS（加密通信）的规则。默认情况下，ESET NOD32 安全套装 4 的标准设置支持绝大多数浏览器，当然您

也可以修改对 HTTP 的监控设置（‘**Web 访问防护**’> ‘**HTTP，HTTPS**’）。在 HTTP 过滤器设置窗口中，您可以通过设定 HTTP 检查选项来启用或禁用 HTTP 检查。您还可以定义系统的 HTTP 通信端口，默认状态下端口 80、8080 和 3128 均为 HTTP 端口。HTTPS 过滤模式有以下几种方式：

**不使用 HTTPs 协议检查**：不检查加密通信

**对选定端口使用 HTTPs 协议检查**：仅检查 HTTPS 协议定义的端口

**对标记为使用选定端口的 Internet 浏览器的应用程序使用 HTTPS 协议**：仅检查选定端口的特定浏览器

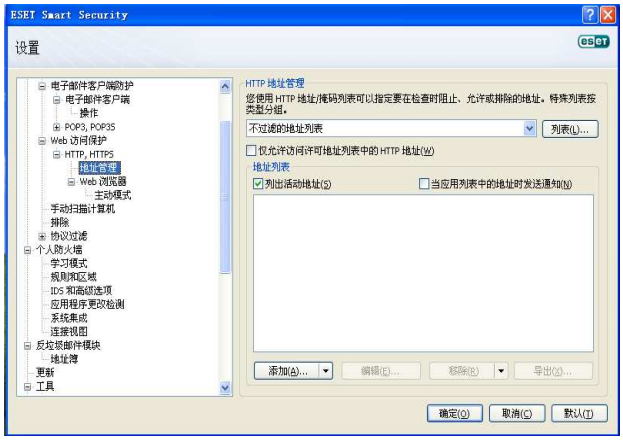



**地址管理**

在本部分，您可以使用 HTTP 地址指定要在检查时阻止，允许或排除的地址。

您可以利用‘**添加**’，‘**编辑**’，‘**移除**’和‘**导出**’这些按钮来管理地址列表。‘**阻止的地址**’列表中的网站将不能访问，而‘**不过滤的地址**’列表中的地址将免受恶意代码检查。如果您启用‘**仅允许访问许可地址列表中的 HTTP 地址**’，则仅仅在本地址列表中的网站可以访问，而所有其他的 HTTP 地址会被拦截。

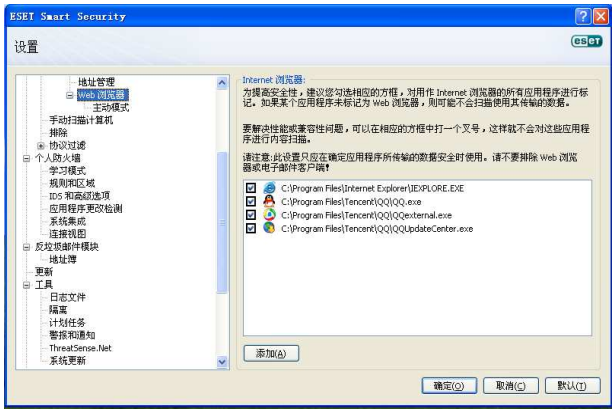
在所有列表中通配符 *（星号）和？（问号）都可以使用。*代表任意字符串，？代表任意字符。您应谨慎使用“不过滤的地址”列表，该列表中应该只能添加可信任的安全地址。同时还应注意通配符*和？在列表中的正确使用。要使列表生效，请选择‘**列出活动地址**’。您还可以选择‘**当应用列表中的地址时发送通知**’，这样在浏览器访问这些地址时将弹出通知窗口。




**Web 浏览器**

ESET NOD32 安全套装 4 包含网页浏览器支持，通过该功能用户可以定义哪些程序是浏览器、哪些不是。被用户指定为浏览器的程序，其所有通讯不分端口，都将受到监测。

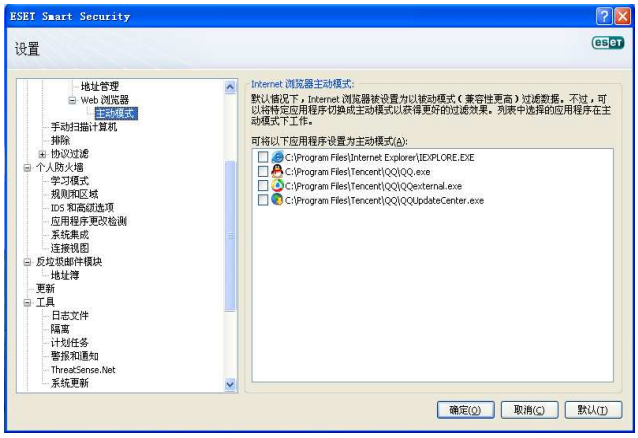
浏览器支持特性是对 HTTP 检查的一种补充，因为 HTTP 检查仅限于预定的端口，而很多 Internet 服务使用了动态端口或未知端口。为了处理这种情况，浏览器支持可以忽略连接参数，直接建立对这些端口通信的监控行为。




标记为网页浏览器程序的列表，可以直接在‘**HTTP**’节点下‘**Web 浏览器**’子菜单中找到。这个部分还包含主动模式子菜单。通过它可以设置对网络浏览器的检查模式。‘**主动模式**’之所以非常有用，是因为它将传输的数据作为整体来检测。如果没有开启该模式，各个程序的通讯将逐步分批监测，这样就降低了数据验证过程的效率，但同时为列表中的程序提供了更好的兼容性。如果使用中没有遇到问题，我们推荐您通过选中相关程序旁的复选框来启用活动模式

**注意**：Windows Vista_Service Pack 1 和 Windows Server 2008 操作系统使用新的 Windows 过滤平台来检查网络通信。由于 Windows 过滤平台使用了特殊的

监测技术，Web 浏览器章节无法使用。




## 4.1.4 计算机扫描

如果您怀疑计算机已经受到了感染(例如行为不正常)，请运行手动扫描，检查您的计算机是否存在病毒。从计算机安全的角度来说，系统扫描不能仅仅在怀疑中毒时才运行，需要定期进行，并将其作为一种常规安全措施。定期扫描可以检测到在文件保存过程中实时扫描没能及时发现的病毒，在计算机受到感染或病毒库不可用时可能遇到这种情况。

我们推荐您一个月运行按需扫描一到两次，扫描可以通过‘**工具>计划任务**’设定为计划。

### 扫描的类型

扫描共分为两种类型。‘**智能扫描**’无需对扫描参数进一步配置，可以立即开始对系统的扫描。‘**自定义扫描**’允许用户使用自定义扫描参数，对文件路径中的任一目标进行扫描。


### 智能扫描

标准扫描是一种方便用户的扫描方式。它允许用户快速开始对计算机的扫描，无需用户介入感染文件清除过程。它的主要优点是容易操作，无需设定细节。标准扫描检查本地驱动器上的所有文件（不包括电子邮件和压缩文件），并自动清除或删除病毒。清除的级别自动设定为默认。

标准扫描中的预设，是为希望快速简单地运行计算机扫描的用户而设计的。它提供了有效的扫描和清除方案，不需要进一步的配置过程。

### 自定义扫描

如果您希望指定包括扫描目标和扫描方式等在内的扫描参数，自定义扫描是您的最佳选择。自定义扫描的优势在于，您可以设定详细的扫描参数。您的设置可以保存为用户定义设置，这在反复使用相同参数进行扫描的情况下非常有用。

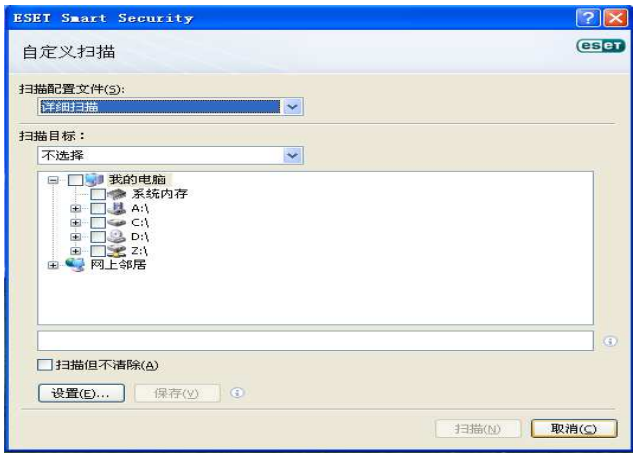
使用自定义模式进行计算机扫描，适用于有使用经验的高级用户。

### 扫描目标

扫描目标下拉菜单允许您对文件，文件夹或驱动器进行病毒扫描。

通过使用快捷目标菜单选项，您可以选择如下对象：

**按配置文件设置**-按已选的配置文件中预设的目标
**可移动媒体**-----软盘、USB 存储设备、CD/DVD
**本地驱动器**-----扫描系统所有硬盘分区
**网络驱动器**-----所有的映射驱动器
**不选择**---------取消所有选择




直接输入目标文件或文件夹路径，可以精确指定扫描对象。另外系统浏览器中列出了本机所有的可用设备，也可以在系统浏览器中选择目标。

**扫描配置文件**

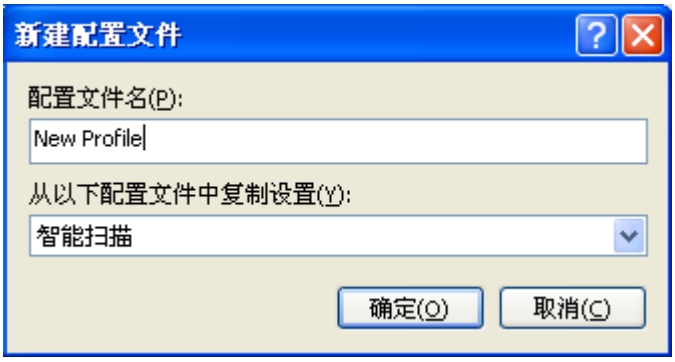
常用计算机扫描参数可以保存为用户自定义设置。这些预设的配置可以在将来的扫描中重复使用。我们推荐您经常使用几套设置，就创建几种自定义设置。

转到‘**高级设置**（F5）>**手动扫描计算机**’点击‘**配置文件…**’按钮，右侧将显示已有的扫描预设列表和创建选项。下方的‘**ThreatSense ®引擎参数设置**’，描述了扫描设置中的每个参数，这将帮助您创建适合您自己的扫描预设。

**例如：**

设想您要创建属于自己的扫描预设，系统‘**智能扫描**’恰好部分适合您。但您并不希望运行对加壳程序和广告软件类程序的扫描，并希望应用‘**严格清除**’模式。

在‘**配置文件**窗口中点击‘**添加**’按钮，在配置文件名中输入您创建的名称，并选从以下配置文件中‘**复制设置下拉菜单**’中选择‘**智能扫描**’。然后调整剩余参数，直到适合您的要求。




## 4.1.5 协议过滤

ThreatSense 扫描引擎为应用协议 HTTP 和 POP3 提供防病毒保护，它无缝集成了所有先进的恶意软件扫描技术。无论是互联网浏览器或电子邮件客户端运行时都会自动保护。以下选项可用于协议过滤（如果已经‘**启用应用程序协议内容过滤**’选项）：

**HTTP 和 POP3 端口**：启动此选项只过滤已定义的 HTTP 和 POP3 端口。

**标记为 Internet 浏览器和电子邮件客户端的应用程序**：启用此选项只过滤已标记为浏览器（‘**Web 访问保护**’>‘**HTTP，HTTPS**’>‘**Web 浏览器**’）和电子邮件客户端（‘**电子邮件客户端保护**’>‘**POP3，POPS**’>‘**电子邮件客户端**’）的应用程序。

**标记为 Internet 浏览器和电子邮件客户端的端口和应用程序**：对端口和浏览器都进行恶意软件扫描

**注意**：在 Windows Vista 的 Service Pack 1 版本和 Windows Server 2008 中使用了一种新的过滤协议，因此，此部分对以上两种版本并不适用。

SSL

在使用 ESET NOD32 安全套装 4 时，您可以检查封装在 SSL 协议中的各种协议。您可以使用不同的扫描模式对 SSL 保护通信使用的信任凭证，身份不明的证书，或已被 SSL 保护协议排除的证书进行通信检查。

**总是扫描 SSL 协议**-选择此选项来扫描所有受保护的 SSL 通信，除非通信所用的数字证书在排除列表中。在建立一个新通信时，如果通信使用的是未知的数字签名，则通信将被自动过滤，且用户将不会收到任何通知。当用户访问服务器时使用的是一个不被信任的证书但是用户已经将它添入了受信任的证书列表中 ，则此通讯将被允许，而且通讯内容会受到检查。

**询问未访问过的站点（未知证书）**-如果您进入了一个新的受 SSL 保护的网站（用未知证书），我们将弹出一个带操作选择的对话框。这种模式可让您创建一个不用被扫描的 SSL 证书列表。

**不扫描 SSL 协议-如果选择此项**-将不会对 SS1 通信进行扫描。

**如果证书无法通过受信任的根证书颁发机构验证**

**询问证书的有效性**-提示用户选择一个要采取的动作。

**阻止使用这些证书的通信**-终止使用这些证书的连接。

**信任的证书**

除了受信任的根证书证书颁发机构存储的证书外，您也可以创建一个自定义的受信任的证书列表，在**设定（F5 键）‘协议过滤>SSL>证书>信任的证书’**中编辑。

**排除的证书**

此排除列表中包含的证书都被认为是安全的。ESS 4 将不扫描通过此列表中证书加密的数据，我们建议

您在把证书加入此列表前确保要访问的网站是安全的或者没有必要进行内容过滤。

### 4.1.6 ThreatSense ® 引擎参数设置

ThreatSense ® 是一种技术的名称，它由多种威胁检测方法构成。这项技术是前摄性的，也就是说它在新型病毒扩散的第一时间内提供保护。这项技术结合了多种手段（如代码分析，代码模拟、通用特征码、病毒特征码），能够协同工作，从而极大提升系统的安全。该扫描引擎有能力同时检测多个数据流，让效率和检测率到达最大化。此外 ThreatSense ® 已经成功的解决了 Rootkit 问题。

ThreatSense ® 技术设置选项，允许用户指定如下几个扫描参数：

----**目标文件类型和扩展名**
----**综合运用不同扫描手段**
----**清除级别等**

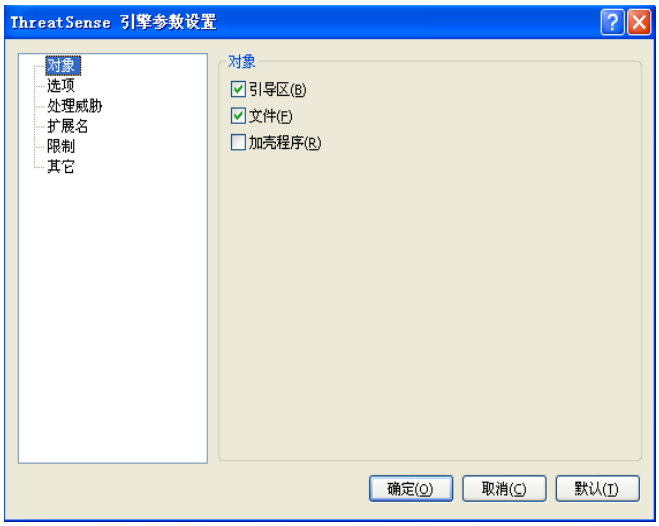
在任意 ThreatSense ®组件（见下）的设置窗口中，单击‘**设置…**’按钮可以进入对 ThreatSense ® 的设置。不同的安全脚本可能需要不同的设置，考虑到这一点，ThreatSense ® 可以在如下组件中得到独立配置。

----**文件系统实时防护**
----**系统启动文件检查**
----**电子邮件防护**
----**Web 访问防护**
----**计算机扫描**

ThreatSense ®参数已经针对每个组件高度优化，对他们的修改将极大地影响系统运行。例如，将参数总是设置为扫描加壳程序，或在实时文件系统防护中启用高级启发式扫描，都将导致系统运行缓慢（通常只有新建文件，才会应用以上扫描方式）。因此我们推荐您保留默认设置，不要修改除计算机扫描以外任何组件的 ThreatSense ® 参数。

#### 对象设置

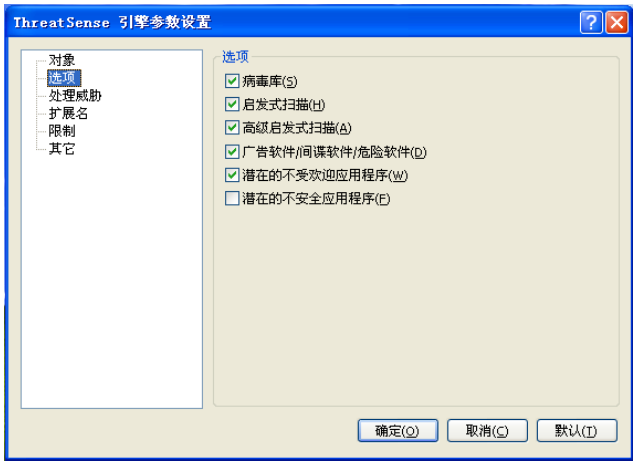
对象设置允许您定义对那些文件类型进行病毒扫描。




**系统内存**-----扫描可能感染内存的病毒
**引导区**-------扫描引导区，寻找隐匿在主导区记录 MBR 中的病毒
**文件**---------提供对所有通用文件类型的扫描（程序、图片、声音、影视、数据库等文件类型）
**电子邮件**-----扫描电子邮件文件类型
**压缩文件**-----提供对压缩文件（.rar，.zip，.arj，.tar，等.）中文件的扫描。
**自解压文件**---扫描自解压文件中的文件，自解压文件通常以.exe 后缀名存在。
**加壳程序**-----加壳程序（与自解压文件不同）在内存中解压，包括标准的静态壳(UPX、yoda、ASPack、FGS 等)。

#### 选项

在选项区域，用户可以选择对系统进行扫毒时使用的方法。有下选项可用：



**病毒库**--利用病毒特征码，能够准确、可靠的检测和识别病毒名称。

**启发式扫描**-启发式是指一种启发式算法,它可以分析程序的恶意行为。启发式的主要优点，在于检测新型恶意程序的能力，这些程序过去从未出现过，或从未录入已知的病毒库名单中。

**高级启发式扫描**-高级启发式结合了一种由 ESET 开发的独特启发式算法，优化了对高级语言编写的计算机蠕虫和木马的侦测。正是由于有了高级启发式，ESET 程序的检测能力高于一般的杀软。

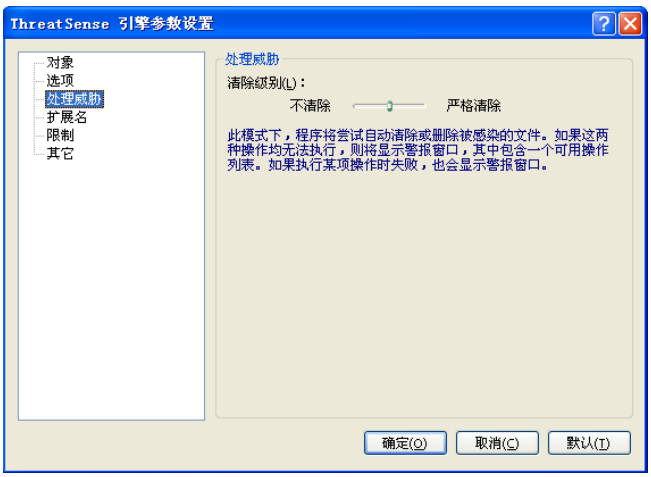
**广告软件/间谍软件/危险软件**--这一类软件包含隐秘非法收集用户敏感信息的软件，以及显示广告内容的软件。

**潜在的不安全应用程序**--潜在的不安全应用程序是指一类商业化的合法软件，包括远程访问工具等程序,这也正是默认状态下禁用对其检测的原因。

**潜在不受欢迎的应用程序**--潜在不受欢迎的应用程序并不一定是有害的。但它们计算机的性能可能产生负面影响。这类程序通常会在安装前征求用户同意。但安装后系统运行效率（与安装前相比）可能会受到影响，最常见的是弹出让人讨厌的广告窗口、激活并运行隐藏进程、增加系统资源消耗、改变搜索结果,还有程序与远程服务器间的通讯等。

## 处理威胁

处理威胁设置将决定扫描器在清除被感染文件时的行为。有 3 个级别的清除可用：




**不清除**--感染的文件不会被自动清除。程序会显示警告窗口，允许用户选择动作。

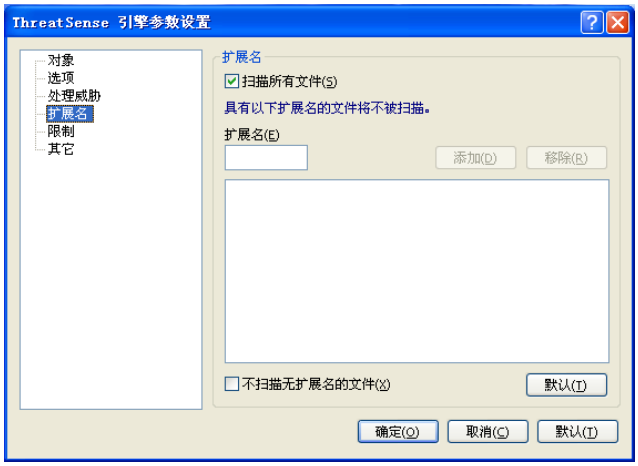
**默认级别**--程序将试图自动清除或删除感染文件，如果自动处理操作不适用，程序将让用户选择接下来的操作。如果首选操作没能成功完成，程序也会显示可用操作，供用户选择。

**严格清除**--程序将清除所有的感染文件（包括压缩文件）。唯一的例外是系统文件。如果清除没有成功,用户可以在弹出的警告窗口中选择一个操作。

**警告**--在默认状态下，只有内部文件全部被感染的压缩文件才会被删除。只要文件中仍然存在合法文件，该压缩文件就不会被删除。如果在严格清除模式下，发现被感染的压缩文件，整个压缩文件都将被删除，即使其中仍存在合法文件。

## 扩展名

扩展名是文件名的一部分被英文句点隔开。扩展名定义了文件的类型和内容。在 ThreatSense ®引擎的扫描参数设置部分,允许用户自定义扫描的文件类型。




默认情况下文件扫描时，会忽略文件扩展名。任何扩展名都可以被添加到排除扫描列表。如果‘**扫描所有文件**’的选项未选中，列表将转而显示所有目前已扫描过的扩展名。通过‘**添加**’和‘**移除**’按钮您可以允许或禁用针对特定扩展名的扫描。

选中‘**扫描无扩展名文件**’选项，将允许扫描不存在扩展名的文件。如果对某一类型文件的扫描，导致使用该类型文件的应用程序运行不正常，这种情况下请在扫描中排除相关文件扩展名。例如：在运行 MS Exchange 服务程序时，在扫描中设置排除包括.edb、.eml 和.tmp 在内的扩展名是非常明智的。

## 限制

您可以利用限制功能来指定被扫描文件的最大大小和压缩文件嵌套层数：

**单个文件最大体积（字节）**

确定了被扫描文件的最大尺寸,防病毒模块只会扫描那些比指定大小小的文件。我们建议您不要更改默

认设置，除非您有特殊的需求。

**单个文件最大扫描时间（秒）**

如果用户在此设定了扫描的最大时长，当扫描时间超过设定值时，反病毒模块将停止扫描该文件，无论扫描是否已经完成。

**压缩文件嵌套层数**

指定对压缩文件的最大扫描深度。我们建议您不要更改默认值 10 。如果压缩文件嵌套层数多过设定值，对该文件的扫描将终止，压缩文件将不会被继续扫描。

**压缩文件中的最大文件大小**

此选项允许您指定在压缩文件中要扫描的最大文件大小，如果压缩文件中的文件大过设定值时，压缩文件将不会被继续扫描。

**其他**

**扫描交换数据流（ADS）**

交换数据流（ADS）是 NTFS 文件系统所使用的文件和文件夹的额外信息，这些数据信息是不可见的，而且普通扫描技术也无法扫描。许多恶意程序为了躲避杀毒软件检测而伪装成 NTFS 数据流。

**以低优先级运行后台扫描**

每个扫描进程都要消耗一定的系统资源。如果您正在运行高负荷的其它应用程序，您可以选择以低优先级运行后台扫描以节省您的系统资源。

**记录所有对象**

选中此选项，日志文件将显示所有被扫描过的文件，包括正常文件。

**保存上一个访问时戳**

启用此选项以保留扫描文件原始的访问时间，而不对其进行更新。

**启用智能优化**

智能优化的目的是优化对您系统的扫描过程。它能提高扫描速度，而且不会减少安全性。

**滚动扫描日志**

您可以选择启用/禁用日志滚动。如果启用，扫描信息将会在显示窗口向上滚动。

**在单独窗口中显示扫描完成通知**

将会打开一个独立窗口显示扫描信息结果。

### 4.1.7 发现病毒

病毒可能自不同的渠道进入系统：网页、共享文件夹、电邮、远程计算机设备（USB 外接存储盘，CD，DVD，软盘等）。

如果您的系统表现出感染恶意软件的迹象，例如：运行缓慢，经常死机等，我们推荐您进行以下操作：
----打开 ESET NOD32 安全套装，单击‘**计算机扫描**’（详情参照标准扫描）
----在扫描完成后，浏览日志，查看扫描文件数、感染文件数及清除文件数。

如果您只想扫描磁盘的某个部分，请点击‘**自定义扫描**’并选择扫描对象。

举例说明 ESET 安全套装处理病毒的过程：设想实时文件监控在默认清除级别下已经检测到病毒，它将试图清除或删除文件。如果预置中没有定义操作选项，将弹出消息窗口请用户选择。通常可用选项包括‘**清除**’、‘**删除**’和‘**离开**’。我们不推荐选择离开，因为这样感染的文件将得不到处理。例外的情况也有，例如当您十分确信文件是无害的，并被错误的识别为病毒。


**清除与删除**

当合法文件受到病毒攻击，并被感染了有害代码时，首选尝试清除感染文件，来恢复文件到正常状态。如果文件中只包含有恶意代码，则系统会将其删除。

**删除压缩文件中的文件**

在默认清除模式下，只有内部文件全部被感染时压缩文件才会被删除。换言之，只要文件中仍然存在合法文件，该压缩文件就不会被删除。需要注意的是，在严格清除模式下，系统将忽略文件中的其它文件，只要有一个被感染文件，该压缩文件即被删除。

## 4.2 个人防火墙

个人放火墙用来控制整个网络中进出系统的所有通讯。这是根据确定的过滤规则，通过允许或拦截网络连接来实现的。防火墙提供了对远程攻击的防护，并允许某些服务访问网络，同时还为 HTTP 及 POP3 协议提供了病毒防护的基础。这些功能是计算机安全中不可或缺的一部分。

### 4.2.1 过滤模式

ESET NOD32 安全套装防火墙有五种模式可选。防火墙的行为将根据所选的模式发生变化。过滤模式同时影响程序与用户交互的程度。

过滤可以运行在以下五种模式：

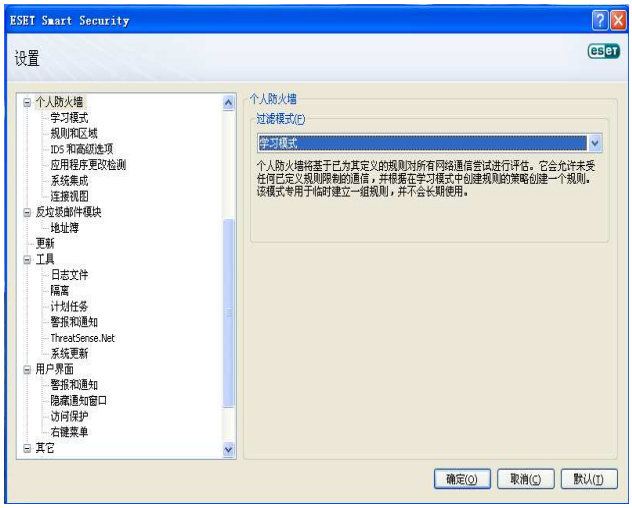
▪ **自动模式** 是默认模式。适合注重简单、易用的用户，防火墙的使用中无需设置规则，自动模式允许特定系统的所有出站连接，拦截由网络端发起的所有新的主动连接。

**·包含例外的自动模式** 除了具有所有自动模式的功能外，您还可以设置自定义规则。

▪ **交互模式** 允许您为防火墙量身定制网络配置。当防火墙检测到通讯，而现存的规则中没有定义该通讯时，防火墙将显示对话窗口，报告未知的网络连接。窗口中同时给出了允许和拒绝的选项，用户的选择以新建规则的形式被防火墙记住。如果用户此时选择创建新规则，以后所有相同连接都会根据这一规则得到允许或拒绝。

**▪基于策略的模式** 将阻止所有未在规则中定义为允许的连接。这一模式让高级用户可以仅允许需要的和安全的连接。所有其它未定义连接都将被个人防火墙阻止。

**▪学习模式** 学习模式能自动创建和保存规则,它适合个人防火墙的初始配置，因为 ESET NOD32 安全套装能根据已有参数自动设置创建保存规则，因此它不需要您的参与。学习模式并不安全，并仅适用于所有规则的已经建立的基础上。




### 4.2.2 阻止所有网络通信：断开网络

**阻止所有网络通信：断开网络连接**选项是唯一可以确定拦截所有连接的选项，任何出入站连接都会被个人防火墙所拦截而不给出任何提示。只有在您怀疑系统中存在严重的安全风险、需要迫使系统立即离线时，才有必要使用该选项。

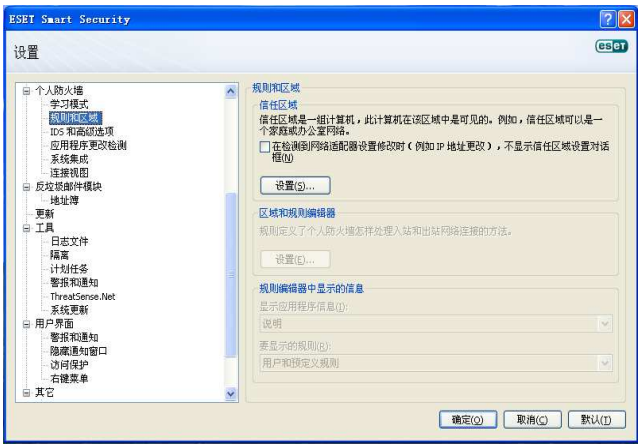

### 4.2.3 禁用过滤:允许所有通信

禁用过滤选项与前面提到的阻止所有网络通信功能恰好相反。如果选中，个人防火墙中所有的过滤选项都会被关闭，并允许所有出入站连接。从网络方面来看，此时的防火墙形同虚设。

### 4.2.4 配置和使用规则

规则代表了一整套用来判断所有网络连接的条件，以及与条件相对应的动作所组成的集合。在个人防火墙中您可以设置规则，定义某个连接建立后，防火墙应采取的动作。

转至**高级设置**（F5）>**个人防火墙**>‘**规则和区域**’可以显示当前的配置。在**规则和区域**编辑区中单击‘**设置**’进入规则设置。（如果防火墙工作在**自动过滤**模式下，这些选项将不可用。）




在‘**规则和区域**’的设置窗口中会显示对当前的规则或域的摘要（取决于您当前所在的选项卡）。这个窗口可以被分为两个部分：窗口的上半部简要列出了所有规则，下半部分显示了当前所选规则的详细情况。允许用户配置规则的‘**新建**’、‘**编辑**’和‘**删除**’按钮则位于窗口的最底部。

如果从通讯的方向来考虑，连接可以分为入站连接和出站连接两类。入站连接是由远程主机发起的，试图与本地系统建立连接。出站连接工作的方式恰好相反，由本地计算机连接一台远程计算机。

如果发现新的未知通讯，您必须谨慎考虑是否允许或拒绝该连接。未经请求的、不安全的、情况不明的连接会对系统的安全构成威胁。如果有此类连接成功建立，我们建议您特别注意远程一方的地址等信息，以及试图进入您系统的应用程序。很多病毒都会尝试发送隐私数据或下载其他有害代码到工作站。个人防火墙允许用户检测和终止这些连接。

## 新建规则

当安装访问网络的新程序时，或对已存在的连接进行修改（远程端口等）时，需要创建新的规则。


确认您已选择规则选项卡，然后在‘**规则和区域**’设置窗口中点击新建按钮，程序将弹出允许指定新规则的新对话框。窗口的顶部包括三个选项卡：

**常规**：指定规则的名称、方向、动作和协议。方向可以是入站或出站（或者出入站），动作表示允许或拦截指定的连接。

**本地**：显示本地的连接。包括本地端口的数目和范围，以及通讯的程序名称。

**远程**：此选项卡包含远程端口的相关信息（端口范围），同时允许用户为规则设定一组远程地址或域。


添加规则的一个很好实例就是允许 Internet 浏览器接入网络。此时需要提供以下信息：

在‘**通用**’选项卡中，允许通过 TCP & UDP 协议的出站通讯

在‘**本地**’选项卡中添加代表您浏览器的进程（例如：对于 Internet Explorer，就是 iexplore.exe ）

如果您希望允许标准的 www 服务，在‘**远程**’选项卡中只启用 80 端口即可。

#### 4.2.4.2 编辑规则

选择‘**编辑**’按钮可以编辑选定的规则。上面提到的所有参数（新建规则一章中提到的）都可以得到修改。

每当监控参数发生改变时，都有必要修改规则。因为假使规则不符合当前情况，相应动作也就无法应用，指定的连接也可能被拒绝。这可能导致某些程序运行中出现问题，例如远端更换网络地址或连接端口等。

### 4.2.5 区域的设置

区域代表一系列的网络地址的集合，这些地址构成了一个逻辑组。指定组中的每个地址都被分配相同的规则，这些规则是集中为组设置的。信任域就是组的一个例子。信任域代表一组被用户信任且不受防火墙拦截的网络地址。

这些区域可以在‘**区域与规**’设置窗口内的‘**区域**’选项卡进行设置。点击新建按钮，在新开的窗口中输入域的名称、描述和一组网络地址。

### 4.2.6 创建连接-侦测

个人防火墙能够侦测所有创建的网络连接。防火墙当前运行模式（自动，交互，基于策略）决定了新规则将采取的动作。在自动或基于策略为当前模式时，防火墙将执行预置动作，无需用户干涉。交互模式将显示一个信息窗口，报告检测到的新网络连接和关于该连接的相关信息。用户可以允许或拒绝（拦截）该连接。如果您在对话框中总是反复的允许同一连接，我们建议您为该连接创建规则。您可以通过选择记住操作（创建规则）选项，将该动作作为新的防火墙规则保存。如果将来防火墙检测到相同的连接，它将自动应用此规则。


请谨慎创建新的规则，并只允许安全的连接。如果允许了所有的连接，个人防火墙将形同虚设。以下是连接的参数：

**远程**：只允许连接到已知的信任地址。

**应用程序**：允许未知程序或进程连接网络是不明智的。

**端口**：经由公共端口（例如：Web 端口 80）的通讯通常是安全的。


病毒为了达到扩散目的，经常利用 Internet 偷偷连接感染远程系统。正确配置的防火墙将成为阻止有害代码攻击、防护系统的有力工具。

### 4.2.7 日志

ESET NOD32 安全套装个人防火墙日志能够记录所有的重要事件。您可以直接在主菜单中单击**工具>日志文件**，在下拉菜单中选择 **ESET 个人防火墙日志**查看。

日志是发现错误和识别系统攻击的有力工具，应该得到合理的重视。ESET 个人防火墙日志文件包含以下数据：

**事件发生的日期和时间**
**事件的名称**
**来源和目标地址**
**网络通讯协议**
**规则和蠕虫名称（如果能成功识别）**
**应用程序**

对这些数据的深入分析将有助于找出危及系统安全的企图。很多其它的因素也有助于分析潜在的安全风险（例如来自某未知地址过于频繁的连接、多次尝试建立连接、未知程序的网络通讯、使用异常的端口等），使用户将这些风险降至最低。

## 4.3 反垃圾邮件

如今，广告推介邮件，即垃圾邮件，已成为电子通信行业最大的问题之一，占据着整个电子邮件通讯量的 80%以上。垃圾邮件防护模块正是解决这一问题的有效解决方案，通过一些极其有效的预订规则，能够对垃圾邮件达到出色的过滤效果。


垃圾邮件检测遵循的重要规则之一，就是通过预设受信地址名单（白名单）和垃圾邮件地址名单（黑名单），有效识别垃圾邮件的能力。您电子邮件客户端中的所有联系人地址，以及用户标记为安全的信箱地址，将自动加入白名单。

检测垃圾邮件主要的方法，是对电子邮件信息属性进行扫描。收到的邮件将通过基本的反垃圾邮件规则（电文定义、统计启发式判断原理、识别算法以及其他的独特方法）进行扫描，得出的综合指数将用来判定是其否为垃圾邮件。

本产品对垃圾邮件的过滤同时使用贝叶斯过滤技术。用户在标记垃圾邮件与否的同时，建立了相关类别的词汇数据库。数据库越大，得出的过滤结果就越准确。上述方法的综合运用，使得本产品提供很高的垃圾邮件识别率。

ESET NOD32 安全套装 4 支持对 Microsoft Outlook，Outlook Express，Windows Mail，Windows Live Mail 和 Mozilla Thunderbird 的垃圾邮件防护。

### 4.3.1 垃圾邮件启发式判断技术

垃圾邮件启发式判断技术指的是上面提到的贝叶斯过滤技术。该技术能够在用户标记垃圾邮件与否的同时，根据重要单个字词的变化，学习领会并协助判断垃圾邮件。因此，用户标记更多的邮件是否为垃圾邮件，贝叶斯过滤的结果就越准确。

将已知联系人地址加入白名单，能够避免来自这些地址的邮件被过滤掉。

#### 将地址加入白名单

与用户频繁通信的联系人地址可以加入安全地址列表（白名单）。加入白名单的地址发出的邮件，不会标记为垃圾邮件。添加邮件地址到白名单的方法是，右键单击该邮件，在出现的 ESET 安全套装菜单选项中选择‘**添加到白名**’；也可以在邮件客户端程序上方 ESET 安全套装反垃圾邮件工具条中，点击‘**受信任地**’。使用类似的方法，也可以添加邮件地址到黑名单。列入黑名单的邮件地址所发出的邮件，都会标记为垃圾邮件。

#### 标记垃圾邮件

您邮件客户端收到的任何邮件，都可以标记为垃圾邮件。标记垃圾邮件的方法是，右键单击该邮件，在出现的菜单选项中点击‘ESET Smart Security > 将

**所选邮件重新分类为垃圾邮件**’也可以在邮件客户端中的 ESET Smart Security 反垃圾邮件工具条中，点击‘**垃圾邮件**’即可。


重新归类为垃圾邮件的信息会自动转移到‘**垃圾邮件**’文件夹，但发信人的邮件地址并不会添加到黑名单中。采用类似的方法，也可以将某邮件归类为‘**非垃圾邮件**’。如果将垃圾邮件夹中的邮件归类为非垃圾邮件，该邮件会自动转移到原始文件夹。将某封邮件标记为非垃圾邮件时，不会自动添加发信人到白名单中。

## 4.4 计划任务

开启 ESET 安全套装高级模式进入计划任务设置。‘**计划任务**’在 ESET 安全套装主菜单‘**工具**’栏下。计划任务列表中可以看到所有排程任务以及相关的属性配置信息，例如预设任务的日期、时间和自定义扫描选项。


默认状态下，计划任务中显示以下排程：

**定期自动更新**
**拨号连接后自动更新**
**用户登录后自动更新**
**自动启动文件检查**
**自动启动文件检查**

编辑现有计划任务时（默认和用户自定义），右键点击任务选择‘**编辑…**’，或者选中需要编辑的任务，点击‘**编辑…**’按钮。

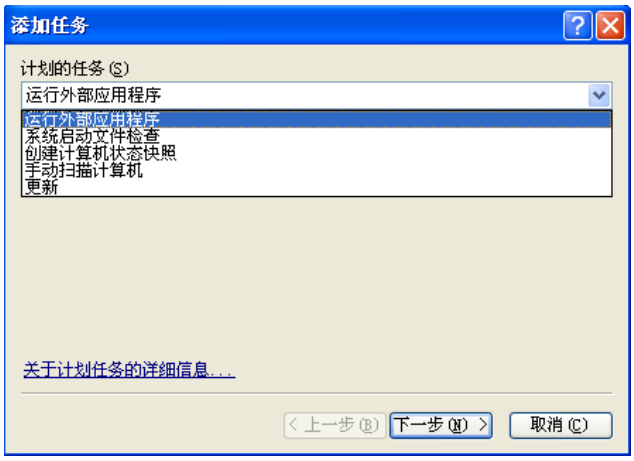
### 4.4.1 计划任务的目的

计划任务能够按照预先的配置和属性信息，管理和执行任务排程。配置和属性信息包括诸如日期、时间、自定义扫描方面的设置信息，以便在执行任务时调用。

### 4.4.2 新建任务

在‘**计划任务**’中新建任务，请点击‘**添加…**’按钮，或者右键点击从右键菜单中选择‘**添加…**’。计划任务共有五类型供选择：

**运行外部应用程序**
**系统启动文件检查**
**创建计算机状态快照**
**手动扫描计算机**
**更新**




由于手动扫描计算机和程序更新是最常用到的任务排程，在此举例说明如何添加更新任务。

从计划任务下拉菜单中选择‘**更新**’，点击‘**下一步**’并在‘**任务名称**’一栏中输入任务名称。接下来选择任务的执行频率，分为以下几种选项：只一次、重复执行、每日、每周和事件触发。根据选择的不同频率，您需要输入相应的更新参数。下一步选择当任

务在预定时间无法执行时，应当采取的行动，有以下三个选项可供选择：

---**延至下次预定时间**

---**尽快执行任务**

---**如果自上次执行任务至今已超过指定时间间隔则立即执行任务**

点击下一步，出现关于该任务配置信息的预览窗口，以特定参数执行任务会自动得到启用。单击完成按钮。

出现选择通过自定义属性执行任务排程的对话框。这里您可以指定主任务属性或可选任务属性，后者是在主任务属性无法执行的情况下运行。在更新配置文件窗口点击确定，新建排程任务将会添加到当前排程任务列表中。

## 4.5 隔离

隔离的主要任务是将受感染的文件安全储存起来。如果染毒文件不能清除，或者不能、不便删除的话，以及 ESET NOD32 安全套装出现误报等的情况，应当隔离起来。

用户可以选择任意文件进行隔离。这种情况尤其适用于扫描引擎无法检测到、但却有可疑行为的文件。隔离文件可以上报给 ESET 病毒实验室，进行进一步地分析。


储存在隔离文件夹中的文件，可以以表格的形式查阅，列出了隔离的日期和时间、染毒文件原来的路径、文件字节数大小、隔离原因（用户添加）、感染病毒的数量（如压缩包，包含多个感染文件）等等。

### 4.5.1 隔离文件

删除的有毒文件，程序会自动隔离起来（如果您没有取消报警提示框中相关选项的话）。如有必要，您也可以点击‘**隔离**’按钮，手动隔离任意可疑文件。手动操作时，原始文件并不会从原来的地址移除。隔离操作也可以通过右键菜单的形式实现，即在隔离窗口中右键单击选择‘**隔离**’。

### 4.5.2 恢复隔离文件

隔离文件也可以恢复到原始位置。恢复时请使用‘**恢复**’功能，具体是在隔离窗口中右键点击相关文件，在右键菜单中选择‘**恢复**’。右键菜单同时提供了‘**恢复到**’选项，通过此选项您可以将文件恢复到原始删除地址以外的路径。

**注意：**如果程序错误地隔离了无害文件，请在恢复后将此文件添加到信任区域，以排除防毒组件对其进一步扫描，并上报文件样本到 ESET 客户服务中心。

### 4.5.3 提交隔离文件

如果您隔离了程序未检测到的可疑文件，或者文件因为程序误报（比如通过启发式代码分析）遭到隔离，请上报文件样本到 ESET 病毒实验室。从隔离区中上报文件，请右键点击该文件，从右键菜单中选择‘**提交文件进行分析**’。

## 4.6 日志文件

日志文件记录了程序所有的重要事件，并提供已检测到威胁的综合信息。日志记录是进行系统分析、威胁检测和故障诊断的必要工具。日志的记录过程在后台静默运行，无需用户干预。日志记录的内容是按照具体设置而定的，用户可以从 ESET NOD32 安全套装界面中，直接查阅文本信息、日志和进行压缩历史日志的操作。


日志文件可以从ESET NOD32 安全套装主窗口打开，方法是点击‘**工具**’>‘**日志文件**’。使用窗口顶端的日志下拉菜单选择需要查看的日志种类。日志分为以下类型：

**检测到的威胁**---使用这一选项查看关于病毒检测的所有相关事件。

**事件**---该选项是为协助系统管理员和用户解决问题而设计的。ESET NOD32 安全套装的所有重要行为都在事件日志中记录。

**手动扫描计算机**---所有完成的扫描结果都在此窗口显示。双击任意记录可以显示相关按需扫描的细节。

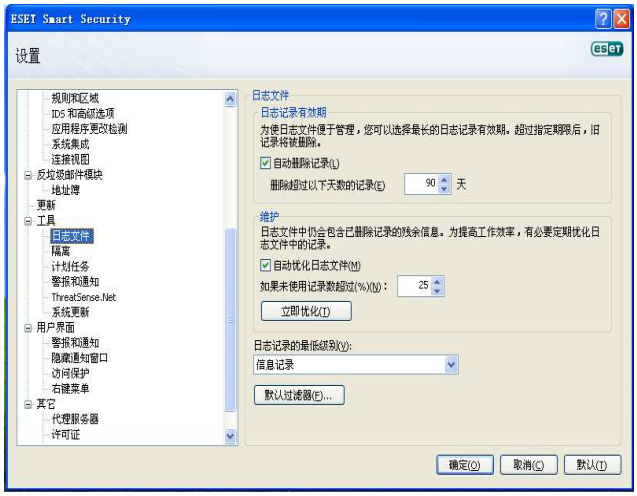
**ESET 个人防火墙日志**---记录了所有和防火墙相关的事件和攻击记录。分析防火墙日志可帮助您及时发现黑客对系统的渗透企图，以防止您的系统被非法访问。

### 4.6.1 日志维护

ESET 安全套装中日志的配置可以从程序主界面进入。点击‘**设置>进入高级设置界面>工具>日志文件**’。日志文件的配置有以下选项：

**删除记录**---自动删除储存超过特定天数的日志记录。
**自动优化日志文件**---未使用记录超过特定的百分比，则允许自动整理日志文件占用的磁盘碎片。

**最低日志记录级别**---规定日志记录的对象级别，选项有：
**关键警告**---仅记录严重错误（无法启动模块等） 。
**错误**---仅记录‘文件下载错误’的信息，同时包括‘严重错误’ 。
**警告**---记录严重错误和警告信息 。
**信息记录**---记录通知信息，包括成功更新信息和上述所有记录信息 。
**诊断记录**---记录协助微调程序设置的相关信息，同时包括上述所有记录信息。




## 4.7 用户界面设置

ESET NOD32 安全套装的用户界面设置可以进行调整，以便更好地适应您工作环境的需要。在 ESET 安全套装 高级设置中的‘**用户界面**’单元，可以进入相关的配置选项。

‘**用户界面**’单元里，用户可以按照需要转入‘**高级模式**’。‘**高级模式**’提供了更为丰富的设置，用户在这里能够对 ESET 安全套装进一步地设置。

如果图形化元素减缓了计算机运行状态或引发其他问题，应关闭图形化用户界面选项。对于存在视觉障碍的用户来说，因为可能与一些显示程序存在冲突，有时也需要关闭图形化界面。

如果您想取消 ESET 安全套装的启动动画显示，请在启动选项中关闭‘**启动时显示启动画面**’。

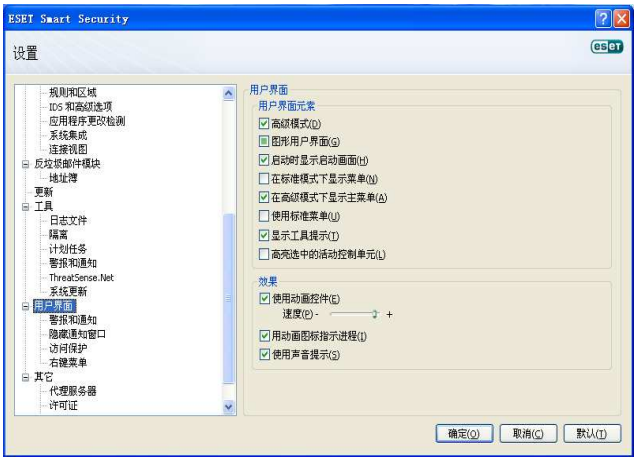
ESET 安全套装主程序窗口顶端的标准菜单，可以‘**在标准模式下显示主菜单**’激活或禁用。

如果‘**显示工具提示**’的话，当光标移动到任意选

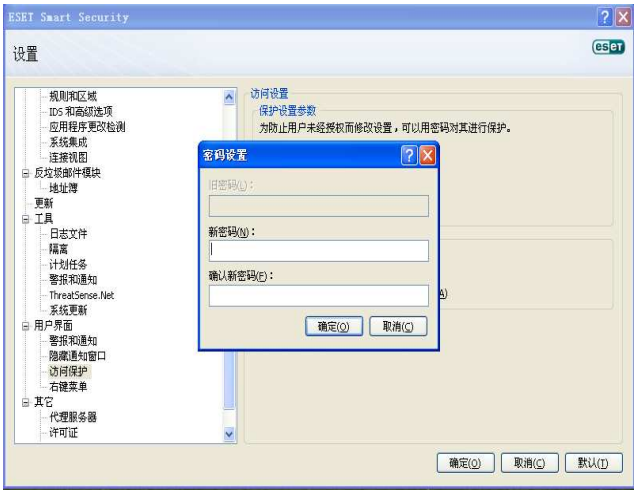
择时都会出现简短的描述。‘**高亮选中的活动控制单元**’选项，能够使系统高亮显示鼠标当前活动范围内的任一单元，鼠标点击后高亮单元即被激活。

需要减缓或加快动态效果时，选择‘**使用动画控件**’选项，将‘**速度滑杆**’进行左右调整。

需要允许动态图标显示不同操作进度时，请勾选‘**用动画图标指示进程**’复选框。如果希望重要事件以声音提示，情选择‘**使用声音提示**’选项。




‘**用户界面**’功能还包括使用密码保护 ESET NOD32 安全套装设置参数的选项。这一选项在‘**用户界面**’下的‘**访问保护**’子菜单中。为使您的系统得到最优的防护效果，必须对程序进行正确配置。他人擅自修改可能导致重要数据的损失。要输入保护设置参数的密码，请点击‘**输入密码…**’。



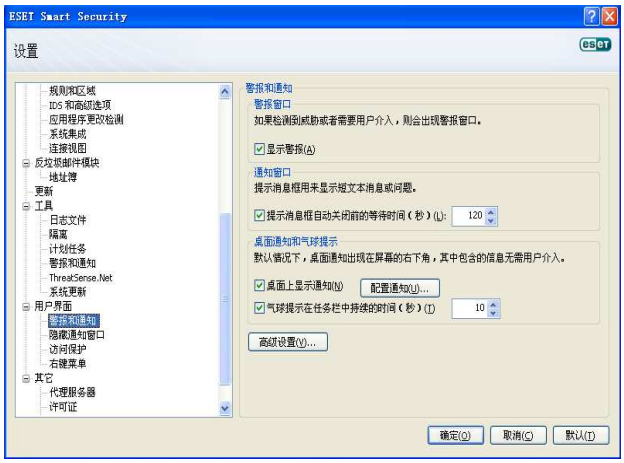

## 4.7.1 警报和通知

‘**用户界面**’下的警报和通知单元，可以用来设置 ESET 安全套装对报警提示信息和系统通知信息的处理方式。

首先是‘**显示警报**’。关闭这一选项会取消所有报警提示窗口，只适用于个别特殊情况。对于大多数用户来说，建议保留该选项的缺省设置（开启）。

需要在指定时间后自动关闭弹出窗口，请选择‘**提示消息框自动关闭前的等待时间（秒）**’选项。如果用户没有手动关闭消息框的话，程序会在指定的时间之后自动关闭消息框。

桌面和气球提示信息是通知类消息，无需用户干预。此类消息在屏幕的右下方的提示区域显示。需要显示桌面通知信息时，请选择‘**桌面上显示通知**’的选项。更为详细的设置 - 显示通知信息的时间和显示窗口的透明度，请点击‘**配置通知**’按钮进行修改。点击‘**预览**’钮，可以对通知信息进行预览。在‘**气球提示在任务栏中持续的时间（秒）**’选项中，可以对气球通知信息显示的时间进行设置。




点击‘**高级设置**’按钮可以查看更多设置项，如‘**仅显示需要用户介入的信息**’选项允许您开启或关闭无需用户干预的报警提示和通知信息。如果选择‘**在全屏模式下运行应用程序时仅显示需要用户交互的通知**’，可以让您在全屏模式下工作时少被打扰。您可以在‘**要显示事件的最低级别**’下拉框中，选择要显示的警告与通知的严重级别。

该单元的最后选项，就是为多用户环境指定通知信息的不同对象。‘**对于多用户系统，在以下用户的屏幕上显示通知**’一栏，允许指定接收 ESET NOD32 安全套装重要通知信息的用户，一般为系统或网络管理员。由于全部系统提示都汇总给管理员，该选项尤其适用于终端服务器配置使用。

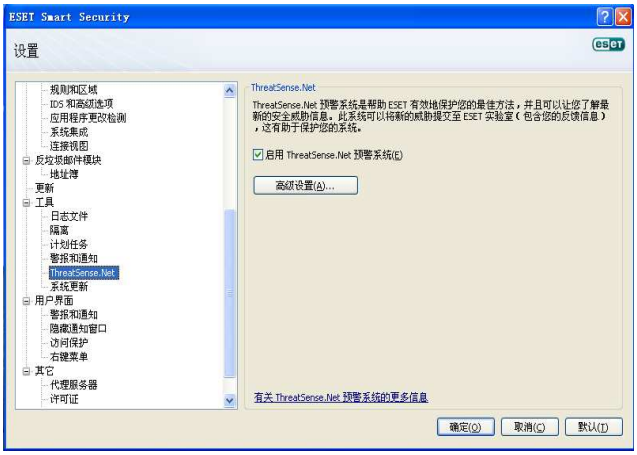
## 4.8 ThreatSense .Net

ThreatSense.Net 预警系统是帮助 ESET 同步、持续收集病毒最新感染情况的工具。双向的 ThreatSense.Net 预警系统的建立只有一个目的：帮助我们更好地防护您的系统。为确保在新型威胁出现的同时收集到相关信息，最有效的方式是与尽可能多的用户联网，令用户计算机反馈威胁分布状况。有两种选项：

您可以选择不开启 ThreatSense.Net 预警系统。关闭此选项后，软件功能不会发生任何变化。您仍然得到我们提供的最优防护效果。

默认设置下，ESET NOD32 安全套装将在上报可疑文件至 ESET 病毒实验室做详细分析前，询问用户确认。需要注意的是，包含.doc 和.xls 等扩展名的文件一旦感染病毒，总是会在发送样本中做相应的排除。您也可以根据个人或公司的需要，自定义添加其他文件扩展名，以避免发送这些扩展名的文件。

ThreatSense.Net 设置可以从高级设置界面进入，位于‘**工具**’>‘**ThreatSense.Net**’。勾选‘**开启 ThreatSense.Net 预警系统**’复选框，以便激活‘**高级设置…**’按钮进一步设置。




### 4.8.1 可疑文件

‘**可疑文件**’选项卡允许您设置将威胁样本上报到 ESET 实验室的具体方式，以便这些样本得到进一步分析。

样本的上报可以设置为无需询问用户的自动模式。选择这一选项后，程序会在后台自动发送可疑文件。如果您希望查看发送的文件名称并予以确认的话，请选择‘**提交前询问**’选项。


如果您不希望发送任何文件样本，请选择‘**不提交文件进行分析**’。需要注意的是，选择不上报文件样本进行分析时，不会影响向 ESET 提交统计信息。统计信息的设置在单独的界面，将在下一章描述。

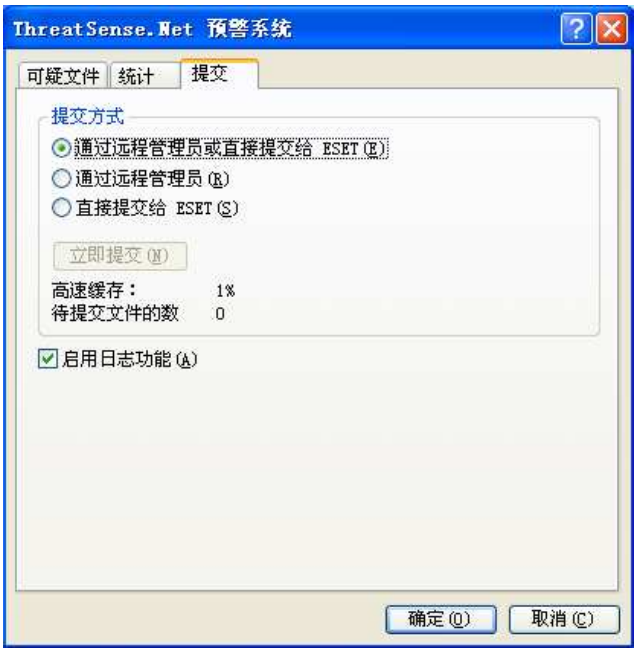
**排除过滤**

并非所有的文件都必须上报后以供分析。排除过滤设置能够对特定文件和文件夹进行排除，避免上报。例如，可以对包含个人隐私信息的文件进行排除，如文档和工作表等。默认状态下，对最常见的文件类型进行排除（Microsoft Office, Open Office），排除类型也可以根据需要添加。

### 4.8.2 上报

在本单元中，您可以选择可疑文件和统计信息是否‘**通过远程管理员或直接提交给 ESET**’。选择‘**通过远程管理员或直接提交给 ESET**’提交选项，可以确保可疑文件和统计信息能够成功提交给 ESET。选择这一选项后，程序将尝试以各种途径提交文件和统计信息。通过远程管理服务器提交可疑文件，是将文件和统计信息发送到远程管理服务器。这样做，能够保证相关文件和信息中转给 ESET 病毒实验室。如果选择‘**直接提交给 ESET**’选项，程序将把所有可疑文件和统计信息直接发送给 ESET 病毒实验室。

# 5. 保存设置



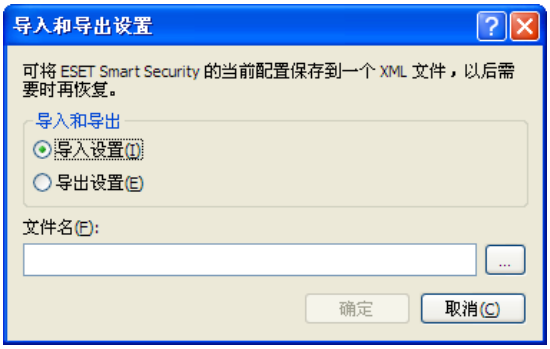

当存在未上报的文件时，这里的设置窗口会出现‘**现在上报**’按钮。点击此按钮即可立即提交文件和统计信息。

‘**启用日志功能**’复选框，程序会记录文件和统计信息的上报情况。在每次提交可疑文件或统计信息之后，会在事件日志中自动生成记录。

本章节描述 ESET NOD32 安全套装便于高级用户使用的一些功能。这些功能的设置选项只有‘**高级模式**’可见。开启‘**高级模式**’的方法是，在程序主界面窗口左下角点击‘**切换到高级模式**’，也可以在键盘上按下 **CTRL + M** 组合键。

在 ESET 安全套装‘**高级模式**’下的‘**设置**’单元中，可以导出或导入当前的配置信息。

导出和导入都是采用.xml 文件类型。导出和导入功能尤其适用于需要保存 ESET 安全套装当前设置，以便日后使用（无论如何原因）的用户。导出设置对于希望在多个系统上使用相同设置的用户，也非常有用，因为只需要再次导入.xml 文件即可。




## 5.1 导出设置

导出设置是非常容易的。如果您想保存 ESET NOD32 安全套装当前的设置，请点击‘**设置**’ > ‘**导入和导出设置**’。选择‘**导出设置**’选项，输入导出设置文件的名称，点击‘**…**’浏览按钮确定在计算机上保存设置文件的位置。

## 5.2 导入设置

导入设置的步骤基本相同。选择导入和导出设置，然后选择导入设置选项。点击‘**…**’浏览按钮，指向您想导入的设置文件。

## 5.3 ESET SysInspector

‘ESET SysInspector’程序可以彻底的检查您的系统，并综合多种方式呈现所搜集的数据。例如已安装的驱动和程序，重要的注册键和网络连接等信息，可以帮助您调查可疑的系统行为。这些行为可能由软件或硬件的兼容问题所引起亦或为病毒感染所致

ESET 开发了两个版本的 SysInspector。 其便携版 (SysInspector.exe) 可以自 ESET 网站免费下载。 集成版包含在 ESET Smart Security 4 中。 需要打开‘**SysInspector**’时，请激活左下角的高级模式并单击工具—> SysInspector。两个版本在功能和控制操作上完全相同。唯一的不同是对日志输出的管理方式。便携版可以以 XML 格式导出并保存系统快照。 导出功能在内置版的 SysInspector 中同样可用。此外,您可以在‘**ESET Smart Security 4**’>‘**工具**’>‘**SysInspector**’中方便的保存系统快照。

ESET SysInspector 扫描计算机时，需要耗费些许时间.该过程可能需要 10 秒到几分钟的时间，具体取决于您的硬件配置,操作系统以及计算机中所安装软件的数量。

### 5.3.1 界面外观与程序用法

为了方便使用，程序的主窗口被分为四个部分 – 操作控制部分位于主窗口的顶部，左侧为内容导航区，右侧中部为描述区，右下角为各项的细节。


### SysInspector 的操作控制

本部分包括对 ‘ESET SysInspector 中所有可用控制项目的介绍’。

**文件**---通过单击此处，您可以保存当前的报告状态以备随后分析研究，也可打开先前保存过的报告。如果希望发送系统报告，推荐您在生成报告时选择适合发送。 该模式下生成的报告将忽略敏感信息。

**提示**：您可以通过将先前保存的报告拖拽到主窗口中，来让 ESET SysInspector 打开它们。

**树**---可以展开或关闭所有节点

**列表**---包含方便的浏览功能以及在线搜索等其他功能。

**重要**---红色标亮的项目为未知项,这也是程序将其标记为潜在危险的原因。项目呈红色并不意味着您可以删除该文件。在删除前， 请务必确认文件确实存在危险或非必要文件。

**帮助**---包含有关程序及其功能的信息。

**详细信息**---对主窗口其他部分中所显示的数据做出调整，使程序更加易用。 在基本模式中，您可以找到解决系统常见问题所需的信息。适中模式 可显示较少使用的细节信息，完整模式可显示解决特定问题所需的所有信息。

**项目过滤**---项目过滤最适于查找系统中的可疑文件或注册键。调整滑竿可以按风险等级过滤所显示的项目。 滑竿处于最左端时 （风险等级 1）SysInspector 将显示所有项目。 随着滑竿向右移动，SysInspector 将过滤掉低于当前风险等级的所有项目，仅显示与当前风险等级相比更为可疑的项目。 当滑竿位于最右端时，程序将仅显示所有已知的有害项目。

所有风险等级处于 6 – 9 的项目都可能带来安全隐患。

**提示：**通过与滑竿上的颜色进行比较,可以快速确定各项目的风险等级。

**搜索**

搜索可以通过名称或名称的一部分,快速定位指定的项目。 搜索的结果显示在描述区中。

**返回**---单击向前/向后箭头,可以返回到描述窗格中之前显示的内容。

**状态区**---显示导航区中的当前节点。

SysInspector 内容导航

ESET SysInspector 将各种信息归纳到数个被称之为节点的基本单元。 如果可用，您可以通过将这些节点展开，查看其子节点来获得更多的信息。需要展开或折叠一个节点时，只需- 双击节点名称，点击+或节点名称旁的-。在浏览导航区内树形结构中的节点和子节点的同时，您可以在描述窗格中看到每个节点的不同详情。在您浏览描述窗格中的各个项目时，各项的细节信息会显示在详情窗格中。

下面是对内容导航区中各个主要节点以及它们在描述窗格与详情窗格中的相关信息的描述。

**运行中的进程**---该节点包括报告生成时，有关正在运行的程序和进程的信息。描述窗格中包括各个进程的额外细节，例如进程所使用的动态运行库，它们在系统中的位置，程序的名称，厂商, 文件的风险等级等。

详情窗格中包括描述窗格里所选项目的额外信息，例如文件的大小、HASH 等

**提示：**操作系统包含多个重要的内核组件，它们 7 天 24 小时时刻运行，为其它用户程序提供最基本的也是最重要的功能。 某些情况下，这些进程的路径在 ESET SysInspector 工具中会显示为以 \??\ 开头。这些符号为进程提供了预启动优化;对系统无害，因此并非显示错误。

**网络连接**---描述窗口中包括一系列进程和程序，它们借助导航区中指定的协议(TCP 或 UDP)，连接远程地址，进行网络通信。 您还可以检查 DNS 指派中所指派的 IP 地址。

详情窗格包括描述窗格中所选项目的补充信息，例如文件的大小、HASH 等。

**主要的注册键**---包括一系列注册键，这里选取的注册键多与系统出现的各种问题有关，例如指定开机时自启动程序的注册键，指定浏览器助手程序(BHO)的注册键等。

描述窗格中可以看到选定注册键中所指定的文件。详情窗格中显示有更多的细节信息。

**服务**---描述窗格中包括一系列已注册为 Windows 服务的文件。您也许需要检查服务所设置的启动方式以及详情窗格中文件的详细信息。

**驱动**---安装于系统中的一系列驱动。

**重要文件**---描述窗格将显示与 Microsoft Windows 操作系统相关的各重要文件的内容。

**系统信息**---包括有关系统软、硬件和环境变量以及用户权限的详尽信息。

**文件**---Program Files 文件夹中的一系列重要文件。 有关特定文件的其他信息，可以在描述和详情窗格中找到。

**关于**---ESET SysInspector 的有关信息

**比较功能**

比较功能允许用户比较两个现存日志。该功能将输出两份日志间的一系列不同之处.它适合记录系统中发生的变化 - 例如您可能会在其中发现有害代码的活动踪迹。

运行后，程序会创建一份新的日志，并显示在新的窗口中。通过‘**文件**’> ‘**保存日志**’可以将日志保存到文件中。生成的日志文件可以在日后打开或浏览。需要打开日志文件时，请使用菜单‘**文件**’>‘**打开日志**’。ESET SysInspector 的主窗口每次只显示一份日志。

如需比较两份日志，其原则是您可以将当前的一份活动日志与另一份保存过的日志文件进行比较。需要比较日志时，请使用选项‘**文件**’> ‘**保存日志**’，并选择‘**选取文件**’。程序将比较所选日志和当前主窗口中的活动日志。产生的结果被称为对比日志，它可以揭示两份日志间的差异。

**提示：**如果您在比较文件时，选择‘**文件**’> ‘**保存日志**’，并将日志保存为 ZIP 文件，则两份日志都会被保存。当您以后打开此文件时，程序将自动进行对比。

ESET SysInspector 会在所显示的项目旁，使用符号来区分所比较日志间的不同。标记为-的项目仅存在于活动日志中，而无法在打开的对照日志中找到。另一方面标记+的项目仅存在于打开的对照日志中，活动日志中却没有。

对项目旁所有标记的描述:

新增值,不存在于之前的日志中 。
含有新增值的树形结构 。
消失值, 仅存在于之前的日志中。
含有消失值的树形结构 。
值 / 文件 已经发生改变 。
含有已变化值/文件的树形结构 。
风险等级已降低/在先前的日志中更高。
风险等级已升高/在先前的日志中更低。

解说部分显示于左下角,它描述了所有符号的含义并显示接受比较的日志的名称


任何比较日志都可以被保存以备日后打开。

**例如:**

先生成一份日志来记录系统原始信息,并将其保存为 previous.xml. 在系统发生改变后打开 SysInspector 让其生成一份新日志。将其保存为文件 current.xml。

为了跟踪两份日志间的差异,点击‘**文件**’>‘**保存日志**’。 程序将生成比较日志,其中显示有两份日志间的差异。

同样的操作可以通过如下命令行参数来实现:

SysInspector.exe current.xml previous.xml

**ESET Smart Security 4 中的 SysInspector**

ESET Smart Security4 中启动 SysInspector 时,单击‘**工具**’>‘**SysInspector**’。SysInspector 窗口中的(日志)管理系统与计算机扫描/计划任务部分非常相似。对于系统快照的各项操作-创建、查看、比较、删除以及导出-可以通过点击鼠标迅速完成。

系统监视窗口包含有关已创建快照的基本信息,例如创建时间, 简短注释, 创建用户, 快照状态。

需要‘**比较**’、‘**添加**’或‘**删除**’快照时,使用位于 SysInspector 窗口中,快照列表底端的相应按钮即可。 这些选项同时存在于右键菜单中。需要浏览选中的系统快照时,请使用右键菜单中的‘**查看**’选项。 需要导出选中的快照到文件中时, 右键单击并选择‘**导出**....’ 下面是对可用选项的的详细描述:

**对比**---可以对比两份现存日志。适合跟踪当前日志与先前日志间的区别。为使该项目生效, 您必须选择两份快照以便对比。

**添加**---可以创建新快照。在此之前您必须为新快照输入一段简短的注释。了解(当前)快照创建的进度百分比, 请查看状态列。所有已完成快照的状态都会被标记为已创建。

**删除**---从列表中删除项目。

**显示**---显示所选的快照或者您也可以通过双击显示所选的项目。

**导出**---保存选中项目到 XML 文件 (同时支持经过压缩的版本)。

## 5.4 ESET 应急工具

ESET 恢复光盘 (ERCD) 创建工具, 可以创建包含 ESET Smart Security 4 (ESS) 的可引导磁盘。 ESET 恢复光盘的主要优点在于可以使 ESS 独立于宿主系统运行,同时获得对磁盘和整个文件系统的直接访问。它的存在让删除正常状态下, 例如在系统运行时无法移除的病毒成为可能。

### 5.4.1 最低系统需求

ESET 恢复光盘 (ESR) 工作在基于 Windows Vista 的 Microsoft Windows 预安装环境 (Windows PE) 2.x 版上。 Windows PE 是免费软件包 Windows Automated Installation Kit (Windows AIK)的一部分, 因此在创建 ESR 前必须安装 Windows AIK 。 限于 Windows PE 对 32 位系统的支持 ESR 只能在 32 位版的 ESS/EAV 中创建。 ESR 支持 AIK 1.1 或更高。ESR 在 ESS/ENA 4.0 或更高版本中可用。 ESR 在 ESS/EAV 4.0 或更高版本中可用。

### 5.4.2 如何创建恢复光盘

如果系统满足创建 ESET 恢复光盘（ESR）的最低要求，创建任务很容易完成，启动 ESR 向导， 单击**‘开始’>‘程序’>‘ESET’>‘ESET Smart Security 4’>‘ESET 系统恢复’。**

首先，向导会检查 Windows AIK 和创建可引导介质所需的适合驱动器是否存在。

在下一步中，选择创建 ESR 的目标介质，除了使用 CD/DVD/USB ，您还可以选择保存 ESR 到 ISO 文件。 随后，您可以将 ISO 镜像刻录到 CD/DVD 上，或以其他方式使用(例如在类似 VMWare 或 Virtualbox 的虚拟机中使用)。

在确定了所有参数后,您将在 ESET 系统恢复向导的最后一步中看到编译预览。 检查各项参数无误，开始编译。可用的选项包括:文件夹、ESET 反病毒、高级、可引导 USB 设备、刻录。

**文件夹**

**临时文件夹**---是存放 ESET 系统恢复光盘编译过程中所需文件的工作文件夹。

**ISO 文件夹**---是在编译结束后保存生成的 ISO 镜像的文件夹。

本选项卡的列表中显示有所有本地驱动器和已映射的网络驱动器，以及其中的可用空间。 如果此处的某些文件夹处于可用空间吃紧的驱动器上，建议您为其选择其他可用空间多的驱动器。否则编译过程可能因为磁盘剩余空间不足而中途退出。

**外置程序**---允许您指定额外的程序，这些程序将在计算机从系统恢复光盘引导成功后，安装或运行。

**包含外置程序**---允许向系统恢复光盘中添加外置程序。

**已选文件夹**---需要加入系统恢复盘中的程序所在的文件夹。

**ESET 反病毒**

在 ESET 系统恢复光盘的创建上, 您有两种 ESET 文件的来源可选，这里的文件将被编译器所使用。

**ESS 文件夹**---计算机中已安装 ESET 产品，所在文件夹中已有的文件。

**MSI 文件**---使用 MSI 安装包中的文件。

**预设**---您可以使用以下两种用户名及密码来源:

**从已安装的 ESS 中获得**---用户名密码将复制自当前已安装的 ESET Smart Security 4 或 ESET NOD32 3.0。

**来自用户**---使用用户在相应文本框中输入的用户名和密码

**提示**: ESET 系统恢复光盘中的 ESET Smart Security 4 或 ESET NOD32 反病毒可以从 Internet 或正在运行 ESET 恢复光盘的电脑上已安装的 ESET 安全产品中获得更新。

**“高级”选项卡**

**高级选项卡**可以根据您的计算机内存，优化 ESET 系统恢复光盘。 选择 **512 MB 或更多**可以让光盘将内容载入操作系统内存 RAM。 如果您选择**不足 512 MB**, WinPE 运行时将总是访问恢复光盘。

**外置驱动**---在此区域中您可以为指定的硬件（通常是网卡）添加驱动。 尽管 WinPE 基于 Windows Vista SP1 ，而 Vista 又支持大容量硬盘，但有时 WinPE 却无法识别相关硬件，您需要手动添加驱动。共有两种方式可以将驱动导入 ESET 系统恢复的编译过程 – 手动方式（**添加按钮**）和自动方式（**自动搜索按钮**）。手动指定时，您需要选择相应的 .inf 文件所在的路径(相应的 *.sys 文件也必须存放在该目录中)。 自动导入的情况下程序会在指定计算机的操作系统中自动查找驱动。我们仅在您的系统恢复光盘创建时所用的电脑和使用时所用的电脑相同时，推荐您使用自动搜索功能。 ESET 系统恢复程序在创建时会将驱动导入编译过程,使用户随后无需另行查找驱动。

**可引导 USB 设备**

如果选择 USB 设备作为目标介质，(在有多的 USB 设备可用的情况下)您可以在可引导 USB 设备选项卡中选择一个可用的 USB 介质。

**警告:** 选中的 USB 设备将在 ESET 系统恢复光盘的创建过程中被格式化，也就意味着设备上的所有的

数据都将被删除。

**刻录**

如果选择了 CD/DVD 作为目标介质,您可以在刻录选项卡中指定附加的刻录参数。

**删除 ISO 文件**---选择此项，将在 ESET 恢复光盘创建后删除 ISO 文件。

**启用删除**---可以选择快速删除或完全删除。

**刻录设备**---选择刻录用的驱动器。

**警告**:此为默认选项. 如果选择了使用可擦除 CD/DVD，其上包含的所有数据都将被删除。

介质部分包括与当前 CD/DVD 中已插入介质有关的信息。

**刻录速度**---使用下拉菜单选择所需的刻录速度选择刻录速度时应考虑您设备的刻录能力和所使用的 CD/DVD 碟片类型。

### 5.4.3 ESET 系统恢复工具的使用方法

为了能够有效的使用应急 CD/DVD/USB，您必须保证计算机能从 ESET 系统恢复用的可引导介质启动。引导顺序可以从 BIOS 修改。 或者您可以根据主板/BIOS 的不同在计算机启动时-通常是-通过 F9-F12 键呼出启动菜单。

启动成功后,ESS/EAV 将(自动)启动。由于 ESET 系统恢复程序只能在特定的情形下使用，常规 ESS/EAV 中的一些防护模块和程序功能并非必需；程序的功能表被缩减到只剩下 计算机扫描、更新、和设置中的某些部分。能够升级病毒签名库是 ESET 系统恢复最重要的功能。我们建议您在进行扫描前首先为程序升级。

### ESET 系统恢复工具的应用

设想网络中的计算机被能够修改可执行文件(EXE)的病毒所感染。ESS/ENA 能够清理所有受感染的文件，但 explorer.exe 除外，此文件甚至在安全模式中，也无法清理。

这是由于 explorer.exe, 作为系统的重要进程，在安全模式下仍然会运行。ESS/EAV 无法对该文件执行任何操作，因此它会一直受到感染。

遇到这样的场景,你可以使用 ESET 系统恢复来解决问题。ESET 系统恢复程序无需宿主操作系统的任何组件。因此它能处理(解毒，删除)硬盘上的任何文件。