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
个人防火墙
反垃圾邮件

目　录

1. ESET NOD32 安全套装

ESET NOD32 安全套装 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 ThreatSense®扫描引擎，继承了 ESET NOD32 防病毒软件的快速和精准优势，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 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 NOD32 防病毒软件中，并屡获殊荣。ThreatSense®内核在全新的 ESET NOD32 安全套装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和Windows Mail。
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 -拦截对感染文件的访问 -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 规则式扫描技术 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和Windows Mail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:

Windows 2000, XP	400MHz处理器 32位/64位系统(x86 / x64) 128 MB RAM系统内存 35MB可用硬盘空间 Super VGA (800 × 600)显示分辨率
Windows Vista	1 GHz 处理器 32位/64位系统(x86 / x64) 512MB RAM系统内存 35MB可用硬盘空间 Super VGA (800 × 600)显示分辨率

2. 安　装

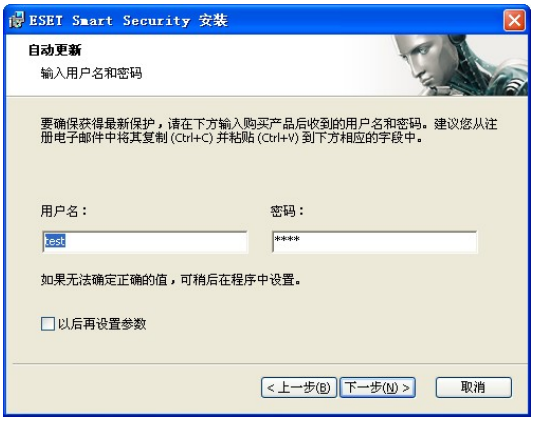
您可以从 ESET 网站上下载 ESET NOD32 安全套装安装程序。您得到的是以 ess_nt**_***.msi (ESET NOD32 安全套装)为名称的安装包。运行安装程序，安装向导将指引您完成基本的设置工作。安装过程有两种类型可选，分别提供了不同程度的安装细节。

1. **典型安装**
2. **自定义安装**

2.1 典型安装

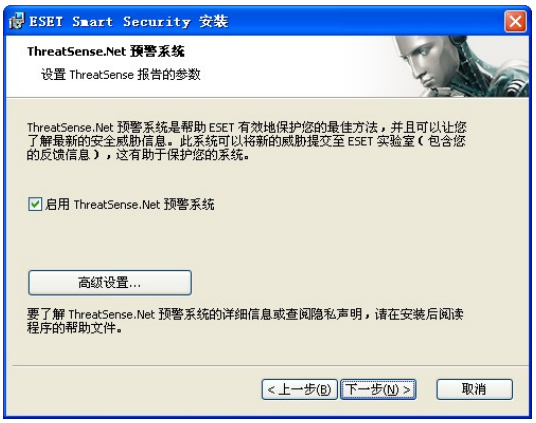
典型安装推荐希望以默认设置完成安装的用户使用。默认设置提供了最大限度的保护，这一点尤其适用于不想进行细节设置的用户。

第一步，也是非常重要的一步，需要输入更新所需的用户名和密码。为使系统得到最新的防护，这一步是关键。



在相应的文本框中输入您在购买或注册 ESET 产品后收到的用户名和密码。如果您目前还未得到用户名和密码，请选择**‘以后再设置参数’**。用户名和密码可以随时在程序中输入。

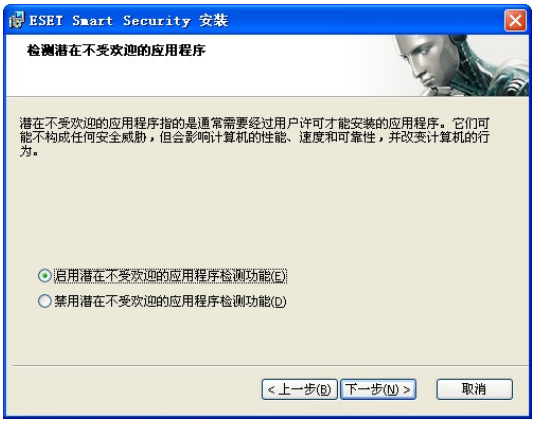
安装的下一步是配置 Thread Sense.Net 预警系统。ThreadSense.Net 预警系统，能够保证 ESET 及时获得最新的病毒库，从而尽快为客户提供有效防护。该系统允许向 ESET 病毒实验室提交最新的病毒样本，供 ESET 分析处理并加入病毒特征库。



默认状态下，启用 **ThreatSense.Net 预警系统**的复选框是选中的，已经激活这一功能。点击‘**高级设置…**’可以修改提交可疑文件的细节设定。

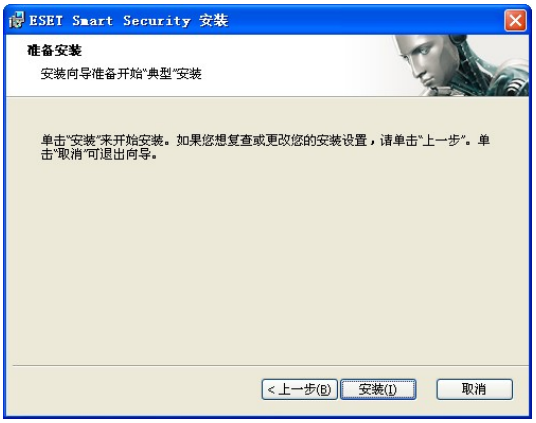
安装过程的下一步是设置是针对不受欢迎软件检测的。不受欢迎软件不一定是恶意的，但却常会对系统运行带来负面的影响。这类程序通常会捆绑其他程序，在安装过程中很难注意到。尽管这些程序在安装过程中常会给出提示，但却容易在未经同意的情况下就安装在系统上。

选择**‘启用潜在不受欢迎的应用程序检测功能’**来允许 ESET NOD32 安全套装 检测此类威胁（推荐）。



典型安装的最后一步是确认安装开始，只需点击‘**安装**’

按钮即可。



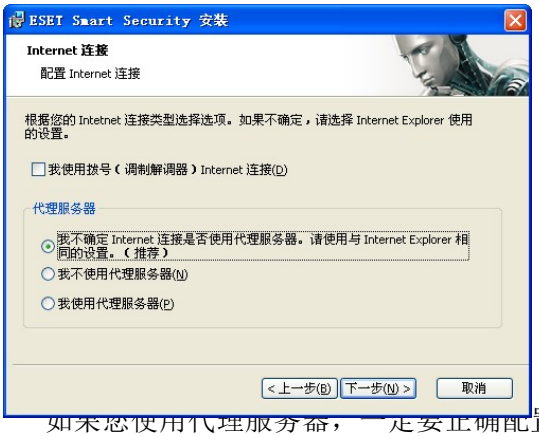
2.2 自定义安装

自定义安装是为有软件配置经验并希望在安装时就进行高级设置的用户设计的。

第一步，选择安装路径。默认状态下，程序会被安装至“**C:\Program Files\ESET\ESET NOD32 安全套装\ “**。点击‘**浏览…**’来更改路径（不推荐）。

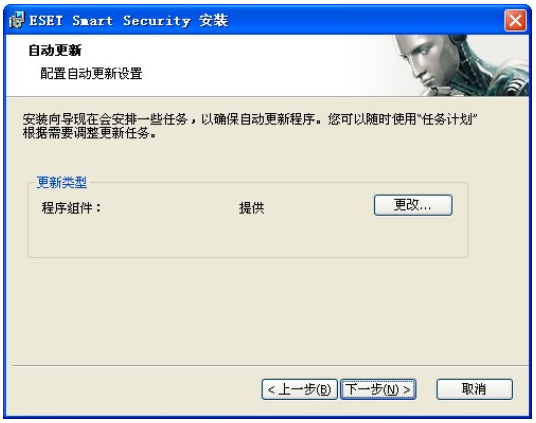
下一步，输入您的用户名密码。这一步与典型安装中的步骤相同（见第 7 页）。

输入您的用户名和密码后，单击‘**下一步**’设置您的网络连接。



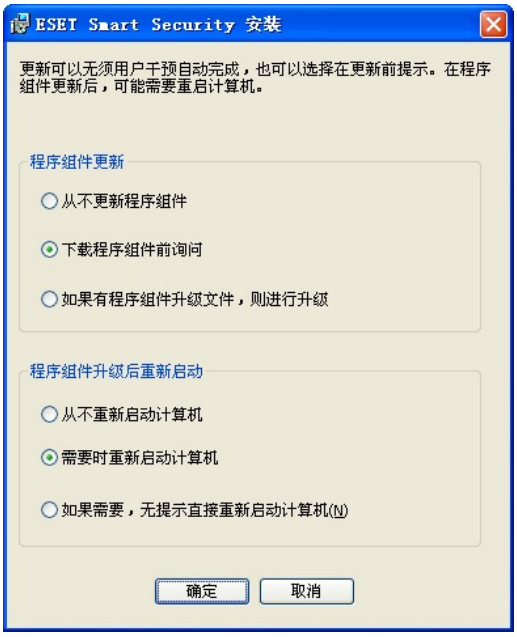
如果您使用代理服务器，一定要正确配置代理服务器，确保病毒库能通过网络正常更新。如果您不使用代理，选择相应项即可。如果您不清楚自己是否使用代理服务器连入网络，保留默认的‘**与 Internet Explorer 相同的设置**’点击下一步即可。

欲设置代理服务器，请选择‘**我使用代理**’并点击下一步。在地址栏中输入代理服务器的 IP 地址或 URL，指定代理服务器的端口（默认为 3128）。如果代理服务器需要验证，您还需输入有效的用户名和密码，以便连接代理服务器。如果需要，也可以使用与 Internet Explorer 相同的代理设置。只要点击‘**应用**’按钮即可。



点击**下一步**，继续设置自动更新。这里您可以设置系统处理程序组件自动更新的方式。单击‘**更改**’进入高级设置。

如果您不希望程序组件更新，请选择‘**永不更新程序组件**’。如果启用‘**下载程序组件前询问**’选项，系统将在下载程序组件前显示确认窗口。需要无提示自动升级程序组件，请选择‘**有组件更新时，自动更新程序组件**’。



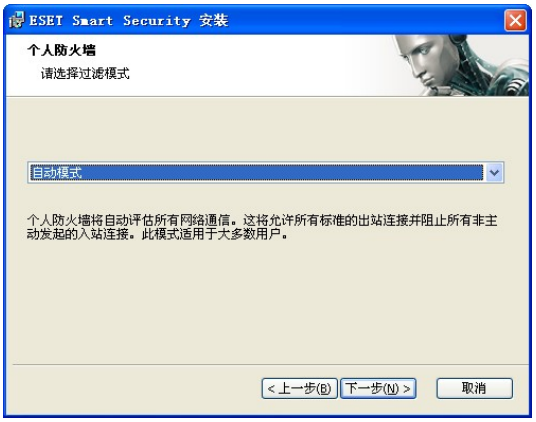
注意：在程序组件更新后，通常系统会要求重启。推荐的设置是：**需要时重新启动计算机**。

安装的下一步是输入保护程序设置参数的密码。选择一个您希望用来保护设置的密码，再次输入并确认。

设置 ThreatSense.Net 预警系统，以及**不受欢迎软件检测设置**与前面讲述的典型安装相同，因此不再赘述。

自定义安装的最后一步是**选择ESET个人防火墙的过滤模式**。有三种候选模式：

- **自动**
- **交互**
- **基于规则**



推荐大部分用户使用**自动模式**。该模式允许所有标准出站连接（使用预置规则自动分析），未经允许的入站连接将自动阻止。

交互模式适合于高级用户。该模式根据用户设置的规则处理网络通信。对未经定义的通讯，程序将询问用户允许还是拒绝连接。

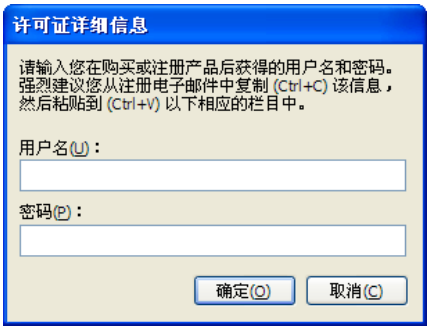
基于规则模式，是根据管理员创建的预置规则监测网络通讯的。如果缺乏与之对应的规则，程序会自动阻止连接，而用户不会收到提示。我们只推荐网络管理员选择该模式。

安装的最后一步，将出现确认同意安装的窗口。

2.3 输入用户名密码

为了达到最佳的性能，程序的自动更新非常重要。只有在升级设置中输入正确的用户名和密码，才能更新病毒库或程序组件。

如果您没有在安装时输入您的用户名和密码，您现在仍可以修改。在程序的主窗口中单击**更新**，然后单击‘**用户名和密码设置**’，在许可证详细信息窗口中输入您收到的用户名和密码。



2.4 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，然后在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、隔离区和计划任务。
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**’可以向主菜单添加‘**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。

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，他们将用绿色的对勾符号表示。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。

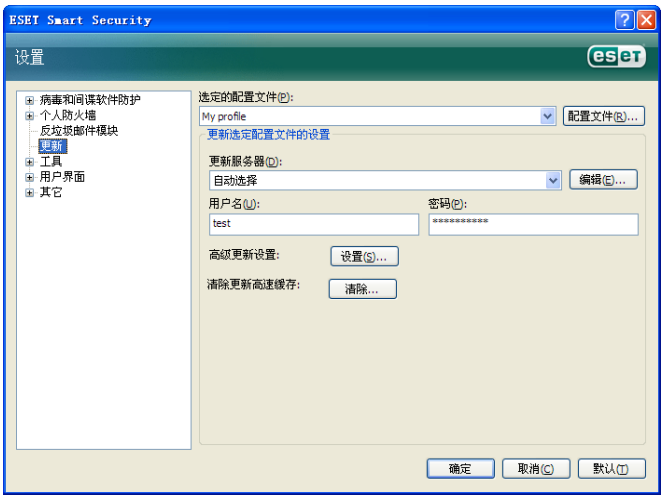
如果已知问题列表和解决方案不能解决问题，请点击‘**帮助和支持**’查看帮助文件或搜索 ESET 知识库。如果您仍然没有找到解决方法，您可以向 ESET 客户服务提交支持请求。我们的专家将根据您的反馈尽快回复您的问题，给您及时、有效的建议。

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。

如果用户名和密码在 ESET NOD32 安全套装安装时已经输入过，此时不会再提示输入。

‘**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。

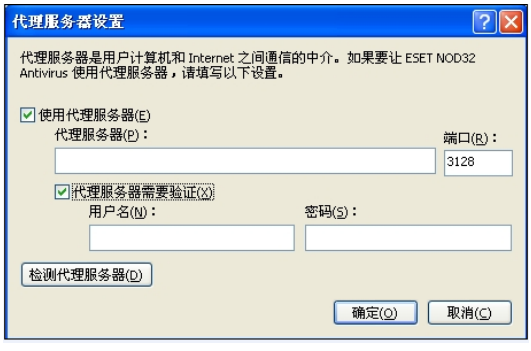
也可以通过排程的方式进行更新。配置排程任务时，请点击‘**工具**’>‘**计划任务**’。默认状态下，ESET NOD32 安全套装自动运行以下任务：

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 NOD32 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

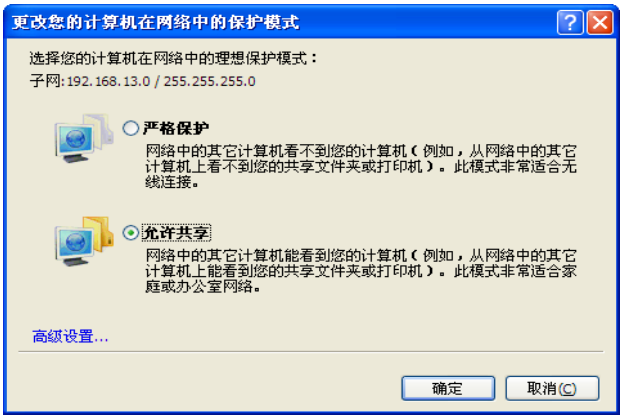
信任域设置是在网络环境下保护您的计算机的重要步骤。您可以通过在信任域中允许共享，来允许其他用户访问您的计算机。依次单击‘**设置**’>‘**个人防火墙**’>‘**修改您的计算机在网络中的保护模式**’，在出现的窗口中，您可以配置计算机在网络中的保护模式。

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。

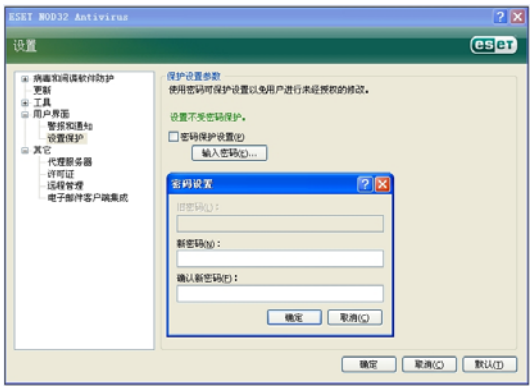
警告！信任域设置错误将给您的计算机带来安全风险。

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>设置保护**’点击‘**输入密码...**’按钮，并再次输入确认，然后点击确定。设置完毕后，对 ESET NOD32 安全套装设置的任何更改，都需要输入密码才能完成。



4. 运行 ESET NOD32 安全套装

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。

4.1.1.1 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。

4.1.1.1.1 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。

4.1.1.1.2 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。

4.1.1.1.3 用于新建文件的其它 ThreatSense®参数.

与已存在的文件相比，新建文件被感染的可能性相对较高。这正是 ESET NOD32 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）。

4.1.1.1.4 高级设置

为了在使用实时防护的同时把对系统性能的影响降至最小，已经被 ESS 扫描过的文件不会再被反复扫描（在被修改前）。但每次病毒库更新后，ESS 都会对其重新进行扫描。这一行为可以通过使用优化扫描选项进行配置。如果这一选项被禁用，所有文件在每次被访问时都将被扫描。

默认状态下，实时防护在系统启动时自动加载，提供不间断的扫描。在特定情况下（例如：与其他实时监控有冲突），可以通过禁用自动启动文件系统实时防护选项，来终止实时防护。

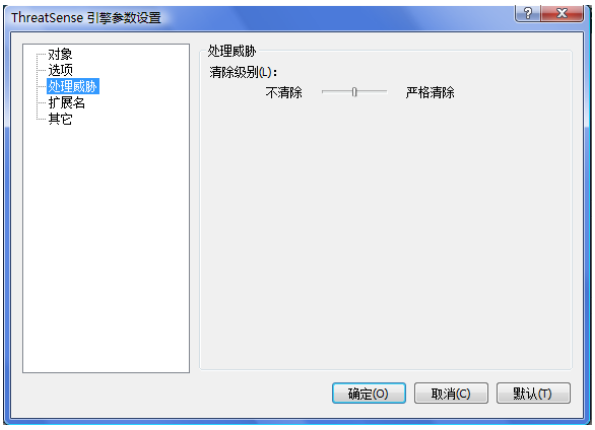
4.1.1.2 处理威胁

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。



4.1.1.3 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。

4.1.1.4 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，用以测试反毒程序的功能。文件 eicar.com 可以由如下网址获得 http://www.eicar.org/download/eicar.com。

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。

4.1.1.5 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'**主程序窗口中的文件系统实时防护区域内单击'**启用'**即可。

如果实时监控在启动时没有初始化，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

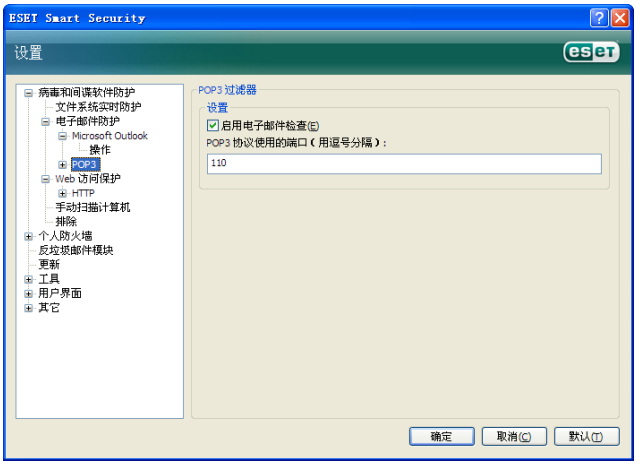
如果实时监控在系统启动时不能初始化（**'自动启动文件系统实时防护'**选项已经启用），原因可能是 ESET NOD32 安全套装与其它程序间的冲突。遇到这种情况，请咨询我们 ESET 客服中心的专家解答。

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。

4.1.2.1 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。



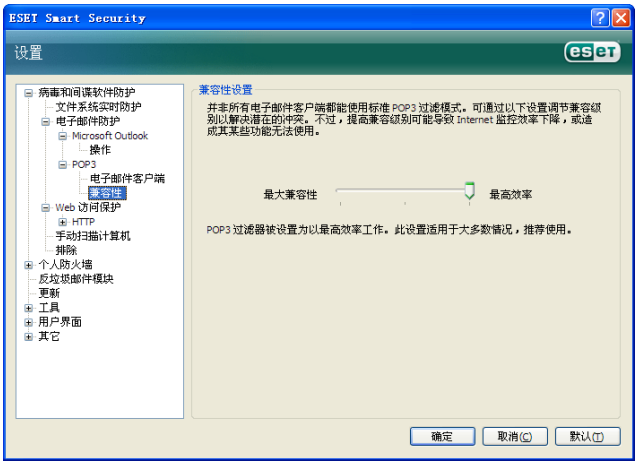
4.1.2.1.1 兼容性

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>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。



4.1.2.2 与 Microsoft Outlook、Outlook Express 和 Windows Mail 整合

与邮件客户端集成后，ESET NOD32 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 NOD32 安全套装中开启整合功能。在激活整合功能后，ESET NOD32 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 和 Windows Mail。

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

4.1.2.2. 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。

有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’**。

标签内容可以在染毒邮件标签字段模板中进行修改。修改可以改善对被感染邮件的自动分拣过程，因为邮件

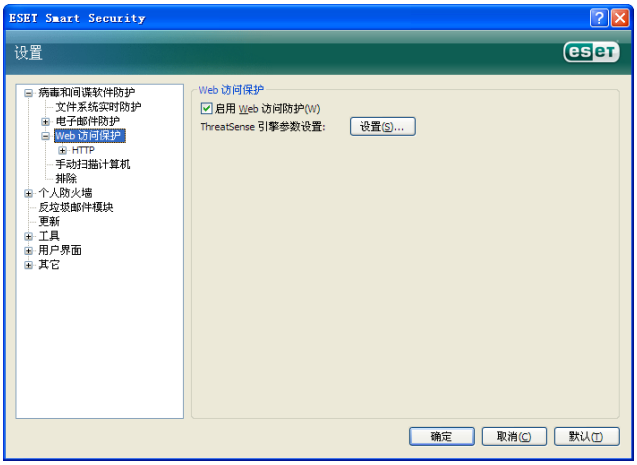
客户端（如果客户端支持）允许您根据特定的主题，设置过滤器并分拣邮件至特定的文件夹。

4.1.2.3 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，系统将显示没有可用选项的信息窗口。

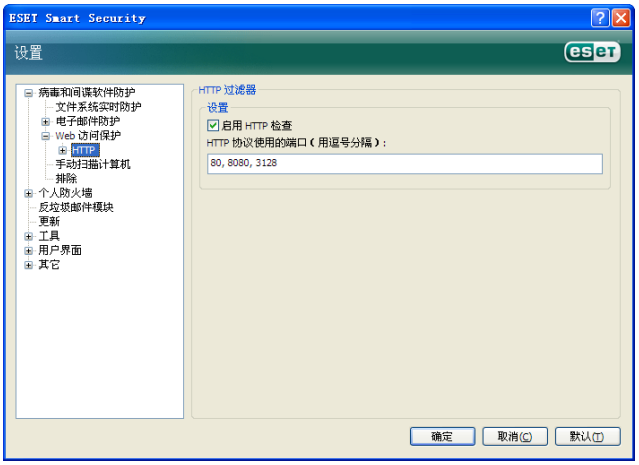
4.1.3 Web 访问防护

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。



4.1.3.1 HTTP

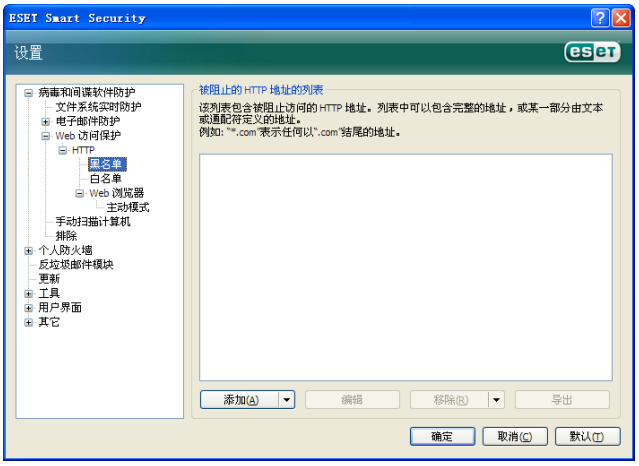
Web 访问防护的首要功能，是根据 HTTP 协议的相关规则，监控浏览器和远程服务器间的数据通讯。ESET NOD32 安全套装在默认情况下，使用浏览器普遍支持的 HTTP 标准。您也可以在这里对 HTTP 监控设置做出部分修改：‘**Web 访问防护>HTTP** ‘。在 HTTP 过滤器设置窗口中，您可以通过启用 HTTP 检查选项来启用或禁用 HTTP 检查。您还可以定义系统的 HTTP 通信端口，默认状态下端口 80、8080 和 3128 均为 HTTP 端口。通过使用逗号界定符，添加额外的 HTTP 端口，这些端口中的 HTTP 流量都会自动被监测和扫描。



4.1.3.1.1 拦截和排除的地址

HTTP 检查设置，允许您创建自定义黑名单列表和白名单列表。

两个窗口中都包含添加、编辑、移除和导出按钮，允许您轻松地管理和维护指定地址的列表。如果用户请求的地址存在于拦截列表中，用户将不可能访问该地址；另一方面，排除列表中的地址将免受恶意代码检查。在两表中通配符 *（星号）和？（问号）都可以使用。* 代表任意字符串，？代表任意字符。您应谨慎编辑排除列表，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。

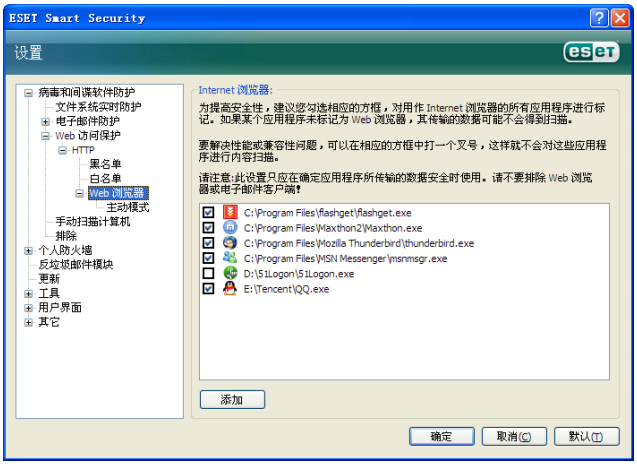


4.1.3.1.2 Web 浏览器

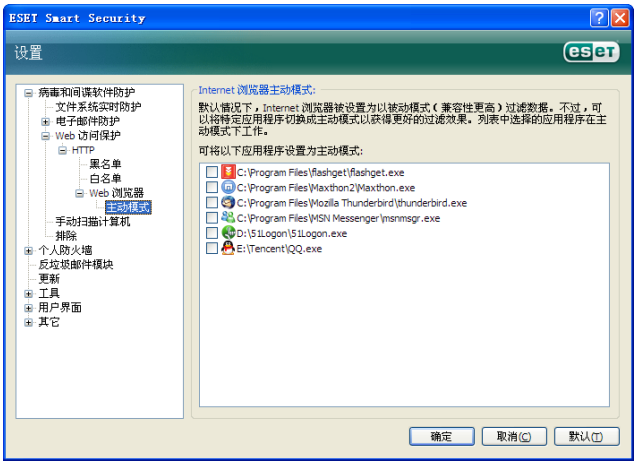
ESET NOD32 安全套装包含网页浏览器支持，通过该功能用户可以定义哪些程序是浏览器、哪些不是。被用户指定为浏览器的程序，其所有通讯不分端口，都将受到监测。

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。



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。

4.1.4.1 扫描的类型

扫描共分为两种类型。标准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。

4.1.4.1.1 标准扫描

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。要了解更多关于清除类型的信息，请看‘**清除**’一节。

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。

4.1.4.1.2 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。

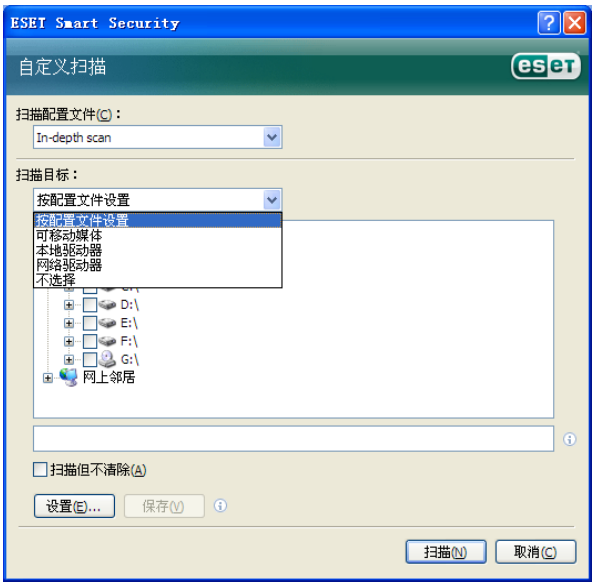
4.1.4.2 扫描目标

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：

本地驱动器- 扫描系统所有硬盘分区

可移动媒体- 软盘、USB 存储设备、CD/DVD
网络驱动器- 所有的映射驱动器



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。

4.1.4.3 扫描预设

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）**>计算机扫描‘** 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 Smart scan 预设恰好部分适合您。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 Smart scan。然后调整剩余参数，直到适合您的要求。

4.1.5 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

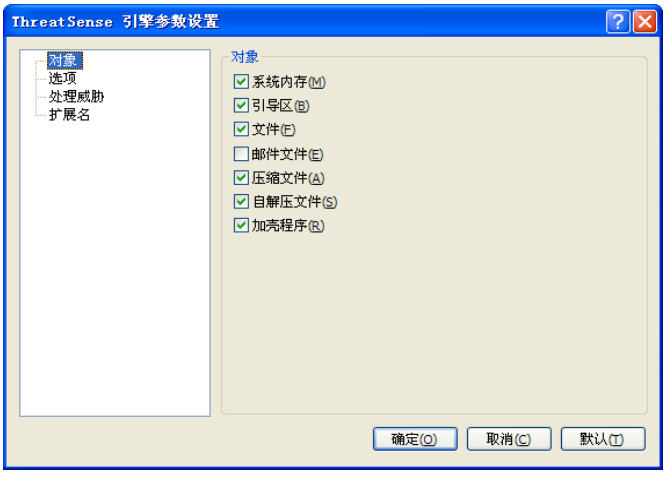
在任意 ThreatSense ®组件（见下）的设置窗口中，单击‘**设置…**’按钮可以进入对 ThreatSense ® 的设置。不同的安全脚本可能需要不同的设置，考虑到这一点，ThreatSense ® 可以在如下组件中得到独立配置。

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。

4.1.5.1 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）

邮件文件- 扫描电子邮件文件类型

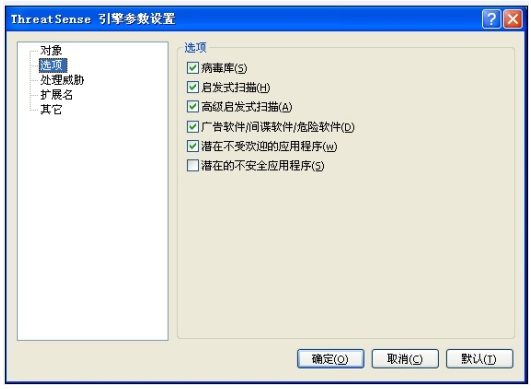
压缩文件-提供对压缩文件（.rar, .zip, .arj, .tar, 等.）中文件的扫描。

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）。

4.1.5.2 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。

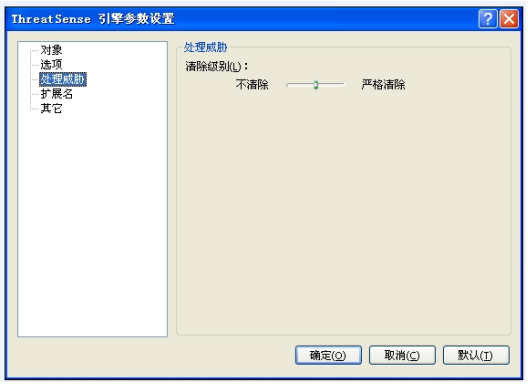
广告软件/间谍软件/危险软件 - 这一类软件包含隐秘非法收集用户敏感信息的软件，以及显示广告内容的软件。

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。

4.1.5.3 清除

清除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。

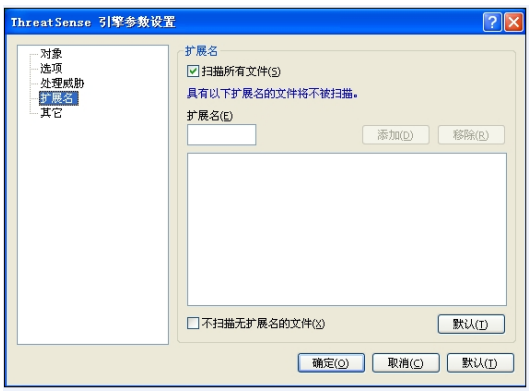
默认级别：程序将试图自动清除或删除感染文件，如果自动处理操作不适用，程序将让用户选择接下来的操作。如果首选操作没能成功完成，程序也会显示接下来的操作，供用户选择。

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。

4.1.5.4 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。

4.1.6 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
单击标准扫描（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 NOD32 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 安全套装防火墙有三种模式可选。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三种模式：

- **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。
- **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。

4.2.2 拦截所有通讯：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。

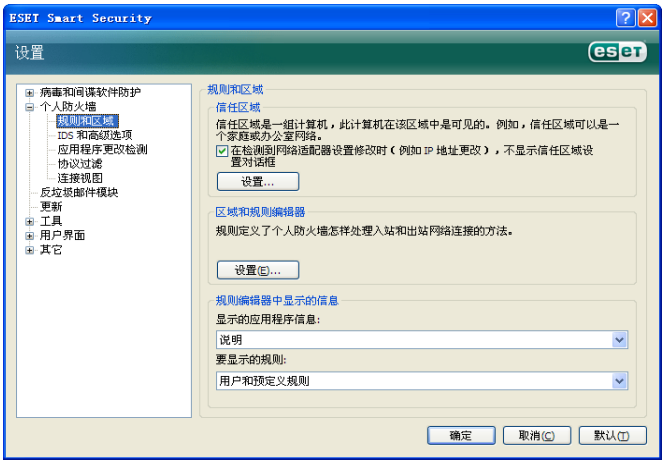
4.2.3 禁用过滤允许所有通信

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。）



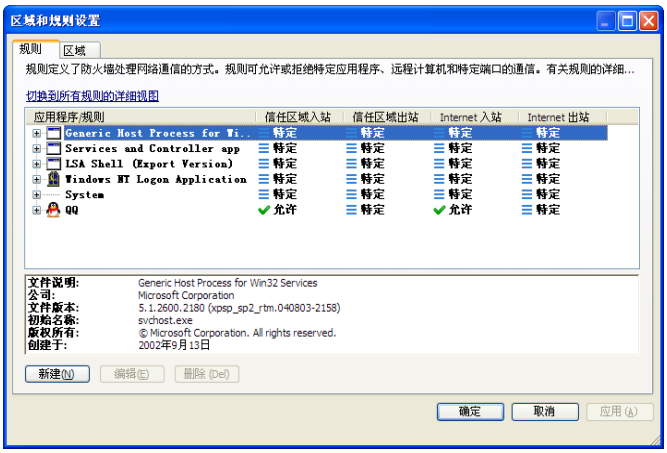
在‘**规则和区域**’的设置窗口中会显示对当前的规则或域的摘要（取决于您当前所在的选项卡）。这个窗口可以被分为两个部分：窗口的上半部简要列出了所有规则，下半部分显示了当前所选规则的详细情况。允许用户配置规则的新建、编辑和删除按钮则位于窗口的最底部。

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。

4.2.4.1 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。

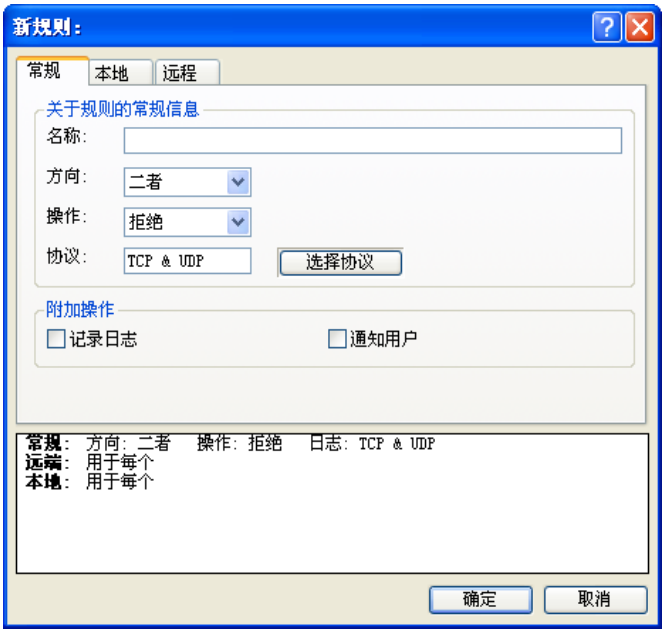


确认您已选择规则选项卡，然后在‘**规则和区域**’设置窗口中点击新建按钮，程序将弹出允许指定新规则的新对话框。窗口的顶部包括三个选项卡：

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，相应的动作也就无法应用，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‘**区域与规则**’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 隐秘连接感染远程系统。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 安全套装支持对 Microsoft Outlook，Outlook Express 和 Windows Mail 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。

4.3.1.1 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 NOD32 安全套装菜单选项中选择‘**添加到白名单**’；也可以在邮件客户端程序上方 ESET NOD32 安全套装反垃圾邮件工具条中，点击‘**受信任地址**’。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。

4.3.1.2 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 NOD32 安全套装高级模式进入计划任务设置。计划任务在 ESET NOD32 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。

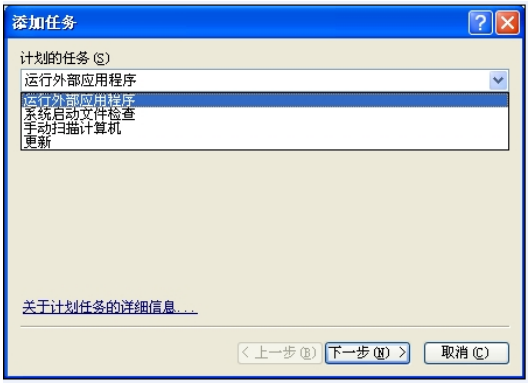
4.4.1 计划任务的目的

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…**’。计划任务共有四种类型供选择：

运行外部应用程序
系统启动文件检查
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‘**添加…**’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‘**添加…**’。

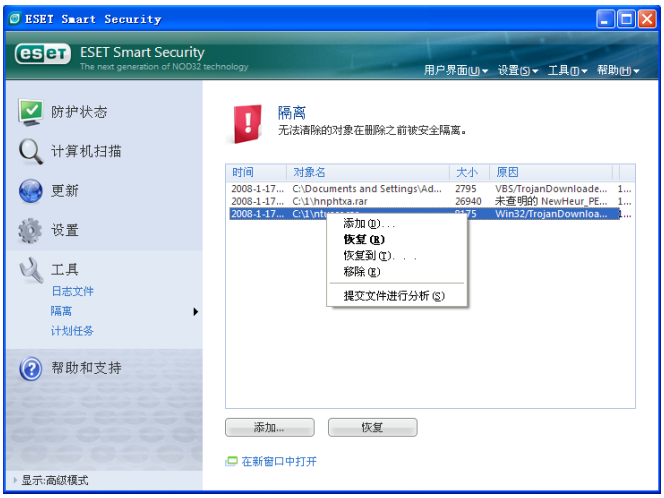
4.5.2 恢复隔离文件

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。

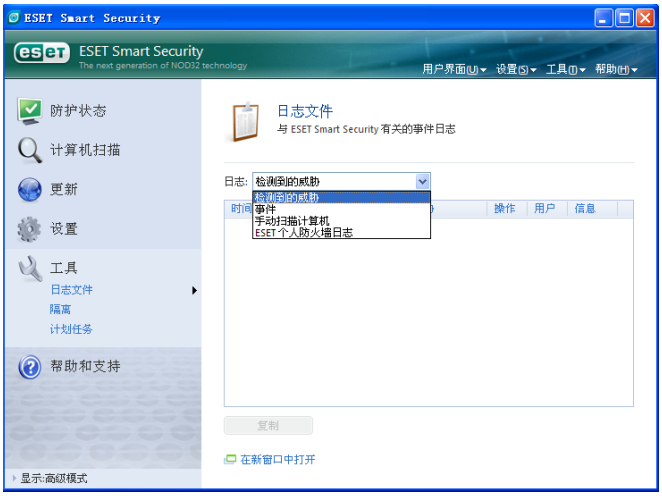
4.5.3 提交隔离文件

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：

1. **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。
2. **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。
3. **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。

不同种类的日志所显示的信息，都可以通过选择事件并点击‘**复制**’按钮的方式，拷贝到剪贴板中。您可以使用 CTRL 和 SHIFT 键选择多项事件。

4.6.1 日志维护

ESET NOD32 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：

自动删除记录：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：

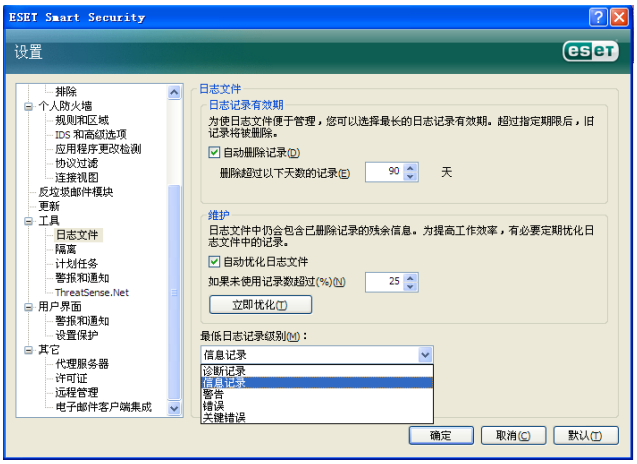
关键错误 – 仅记录严重错误（无法启动杀毒防护等）

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 NOD32 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 NOD32 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。

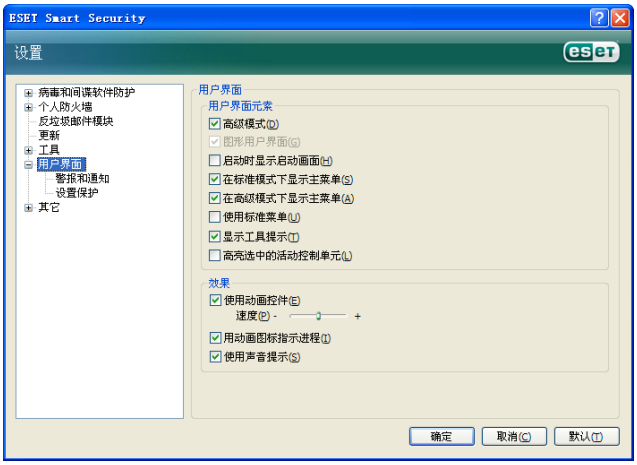
如果您想取消 ESET NOD32 安全套装的启动动画显示，请在启动选项中关闭‘**启动时显示启动画面**’。

ESET NOD32 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。

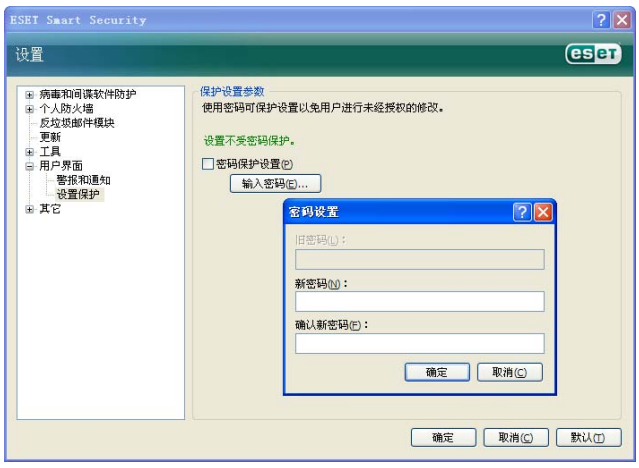
如果‘**显示工具提示**’的话，当光标移动到任意选择时都会出现简短的描述。‘**高亮选中的活动控制单元**’选项，能够使系统高亮显示鼠标当前活动范围内的任一单元，鼠标点击后高亮单元即被激活。

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‘**设置保护**’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…**’。



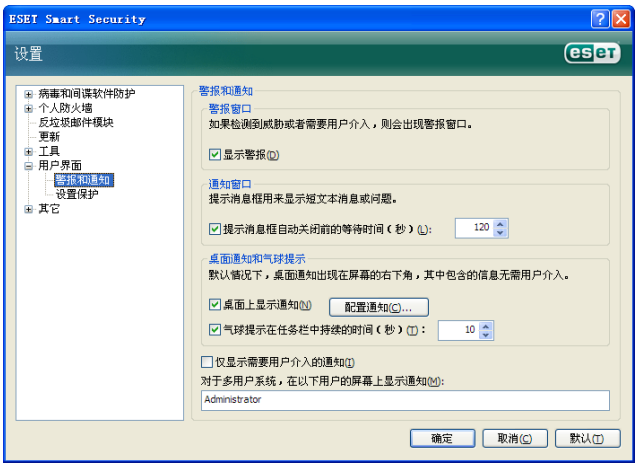
4.7.1 警报和通知

‘**用户界面**’下的警报和通知单元，可以用来设置 ESET NOD32 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**’按钮，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。



在‘**警报和通知**’设置窗口的底部，有‘**仅显示需要用户介入的信息**’选项。这一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。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

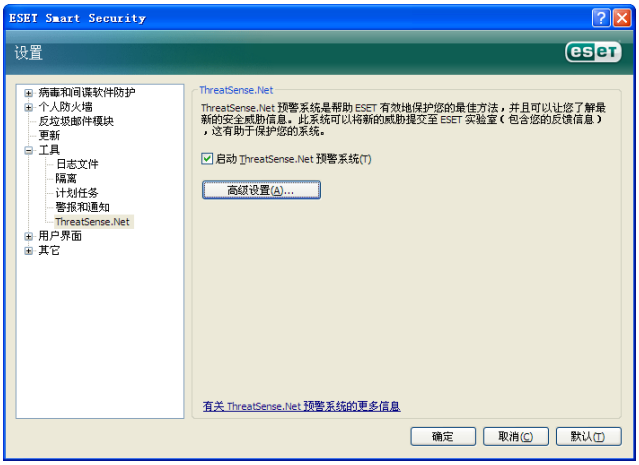
ThreatSense.Net 预警系统是帮助 ESET 同步、持续收集病毒最新感染情况的工具。双向的 hreatSense.Net

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。

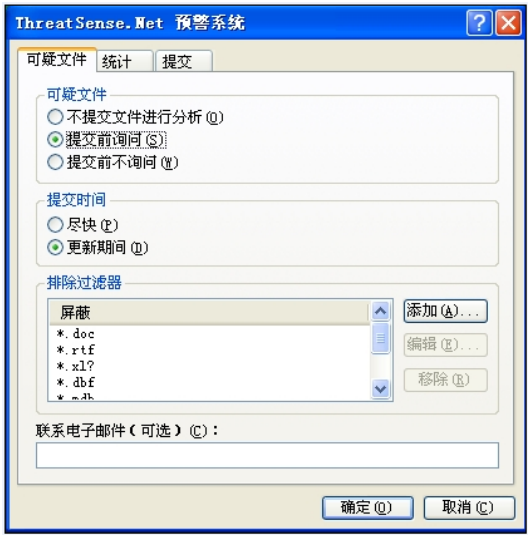
ThreatSense.Net 设置可以从高级设置界面进入，位于‘**工具**’> **ThreatSense.Net**。勾选**开启 ThreatSense.Net 预警系统**复选框，以便激活**高级设置…**按钮进一步设置。



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。



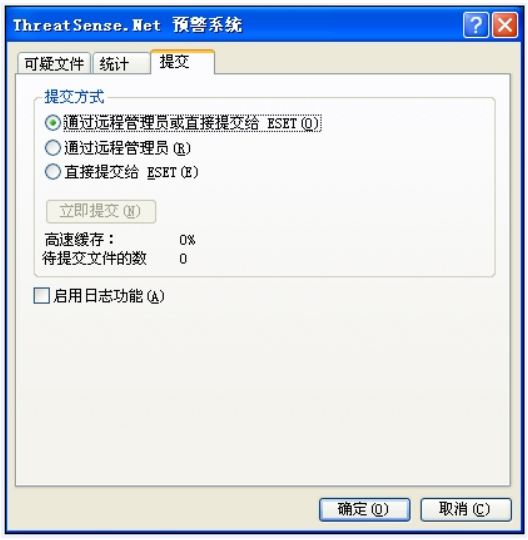
如果您不希望发送任何文件样本，请选择‘**不提交文件进行分析**’。需要注意的是，选择不上报文件样本进行分析时，不会影响向 ESET 提交统计信息。统计信息的设置在单独的界面，将在下一章描述。

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。



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。

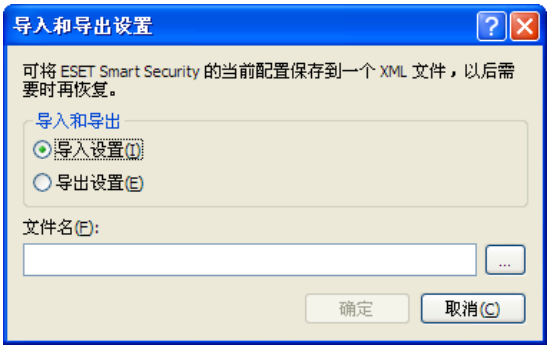
‘**启用日志功能**’复选框，程序会记录文件和统计信息的上报情况。在每次提交可疑文件或统计信息之后，会在事件日志中自动生成记录。

5. 保存设置

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 NOD32 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 NOD32 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。