Comodo 互联网安全套装多语言版

Comodo Internet Security 是 Comodo 公司出品的互联网安全套装，由杀毒软件和防火墙组成的套装软件，简称 CIS。可以有效防御病毒、木马和来自网上的安全危险。CIS 终身免费，安装程序可以让用户自定义安装防火墙和杀毒软件。

主要特点

Defense+主动防御系统

针对 root-kits、进程间内存注入、键盘记录等真正防弹保护；

在加载到您计算机的内存之前，鉴别所有程序的完整性；

未知或不受信的应用程序尝试运行或安装时，随时警报通知；

在病毒、木马及间谍软件进入您的系统前进行阻断；

防止重要系统文件和注册表键值受到未认证的修改。

高级网络防火墙引擎

科摩多互联网安全套装专业版防火墙为出入站威胁提供最高级别的边界安全—— 这意味着您对付黑客、恶意软件和身份小偷拥有了最强大的保护。我们做出改进添加了如下新特性

隐身模式让您的 PC 对碰运气的端口扫描完全隐身；

基于自动检测可信区域的向导；

预定义的防火墙规则帮助您快速实施安全规则；

诊断分析您的系统与防火墙潜在的冲突。

全面的病毒防护

在台式机、笔记本和网络工作站上检测并消除病毒

实时、按访问扫描的持久保护；

高度可配的按需扫描器允许您随时对任何文件、文件夹或驱动器进行检查；

与 Windows 操作系统无缝集成，允许扫描“闲置的”特殊对象；

每日自动更新病毒库；

在隔离区隔离可疑文件以阻止进一步感染；

内建调度器允许您在适当的时间运行扫描；

易用性——安装并忘记它——科摩多杀毒在后台保护您

直观的图形用户界面

汇总界面给您一览无余的安全设定；

方便而快捷的在防火墙各个模块间导航；

简单的点击设置 ——没有不合理的学习过程；

新版完全重新设计的安全规则界面——您可以快速的为全局或分别设置每个应用程序访问权限的粒度和特权。防火墙也同样包括预设规则及向导帮助简化规则设置过程。

扩展功能

应用程序行为分析

科摩多互联网安全套装提供一种高级的协议驱动层面的保护特性——从根据上保护您的 PC 不受使用专有协议驱动的木马侵害。

事件日志

科摩多互联网安全套装大力改进的日志管理模块——允许用户使用多种自定义的过滤器导出反病毒、防火墙和 Defense+ 行为记录。初学者或高级用户都将从这个基础的故障排除特性中获益匪浅。

预警功能

科摩多互联网安全套装就其它数百万用户对每个弹出警报的反应情况提供了一个报告，这将指导您在产生警报时决定应该允许或阻止某一项活动。科摩多互联网安全套装有聪明而拥有专业知识的用户群，所以，来自他们的反馈信息能对不知道如何是好的新手提供指引。登录后，您的反馈信息也同样被上传到服务器上以指导其它人。

集成内存防火墙

科摩多互联网安全套装内建了科摩多内存防火墙的缓冲区溢出保护功能。当发生缓冲区溢出攻击企图时，CIS 将产生一条弹出警报，为数据窃取、计算机崩溃、系统损害及其它缓冲区溢出攻击可能导致的情况提供保护。

'学习模式'和'干净 PC'模式

这些模式让防火墙和主机入侵防御系统为您已经确认信任的新的应用程序组件自动创建“允许”规则，因此您不会为这些可信的程序收到无意义的警报。防火墙能够学习它们如何工作，只有当它确实检测到可疑行为时才会提醒您。

应用程序识别数据库（广泛而专有的应用程序安全列表）

防火墙包含一个被称为“科摩多安全列表数据库”的安全可执行程序白名单。这个数据库检查每个可执行程序的完整性，当有潜在危险时，防火墙将向您报警。这是一种新的防护级别，传统的防火墙只根据已知恶意软件黑名单中检测有害的应用程序——经常错过可能发生零日攻击的恶意软件变种。

随着防火墙的持续更新，目前科摩多安全列表中已有超过 1,000,000 个应用程序，成为安全产业中最大的安全列表之一。

对重要进程的自身防护

病毒和木马经常尝试着关闭您计算机的安全应用程序以便它们的操作避开检测。防火墙安全套装保护了自己的注册表键值、系统文件及进程，因此恶意软件绝不可能关闭或破坏这些已安装的程序。

下载地址：

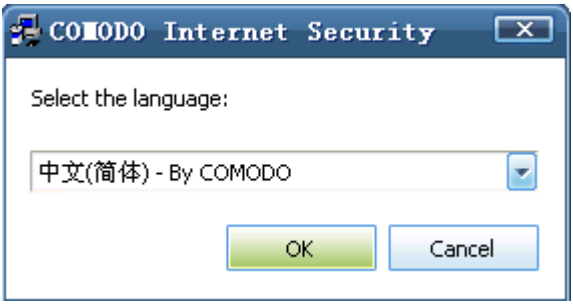
http://www.bannedbook.org/forum42/topic3156.html

禁书网 大陆直连 https://goo.gl/C6xxGf 看 禁书禁闻禁文禁网禁片禁歌禁曲

安装

双击执行程序进行安装，语言选择中文

CIS_Setup_3.9.76924.507_XP_Vista_x32.exe



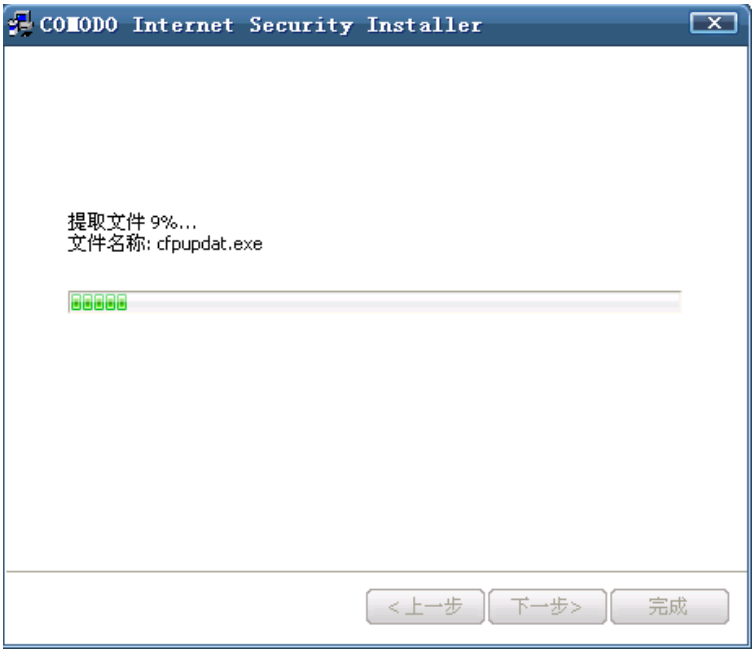
下一步

接受许可协议

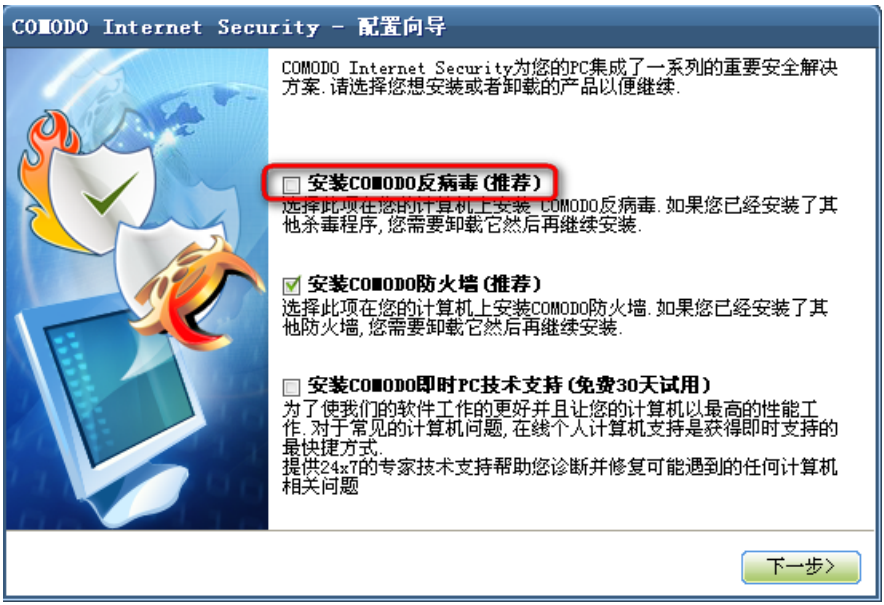

COMODO Internet Security Installer
许可协议
请仔细阅读下面的许可协议
按 PAGE DOWN 键查看剩下的协议.
END USER LICENSE AGREEMENT
Comodo Desktop Security Software
THIS AGREEMENT CONTAINS A BINDING ARBITRATION CLAUSE. PLEASE READ THE AGREEMENT CAREFULLY BEFORE ACCEPTING ITS TERMS AND CONDITIONS.
IMPORTANT ?PLEASE READ THESE TERMS CAREFULLY BEFORE DOWNLOADING OR USING ANY OF COMODO桁 DESKTOP SECURITY SOFTWARE. BY DOWNLOADING, INSTALLING, OR USING COMODO桁 DESKTOP SECURITY SOFTWARE OR BY CLICKING ON 捏 ACCEPT?BELOW, YOU AGREE THAT YOU HAVE READ THIS AGREEMENT, THAT YOU UNDERSTAND IT, AND THAT YOU ACCEPT ITS TERMS. IF YOU DO NOT AGREE TO THESE TERMS, DO NOT DOWNLOAD OR INSTALL ANY OF COMODO桦 DESKTOP SECURITY SOFTWARE AND DO NOT CLICK 捏 ACCEPT?
您接受软件许可协议的所有条款吗?如果您选择'我拒绝',安装将结束.如果您必须选择'我接受',将继续安装 COMODO Internet Security.
< 上一步
我接受
我拒绝

下一步


COMODO Internet Security Installer
选择目标文件夹
选择安装程序的目标文件夹
安装包将安装 COMODO Internet Security 到下面的目录.
安装到这个目录请点下一步.安装到别的目录,请点浏览并选择另一个目录.
目标目录
C:\Program Files\COMODO\COMODO Internet Security
浏览...
驱动器'C'上的磁盘状态
要求空间: 194.50 MB
可用空间: 4373.50 MB
< 上一步
下一步>
完成

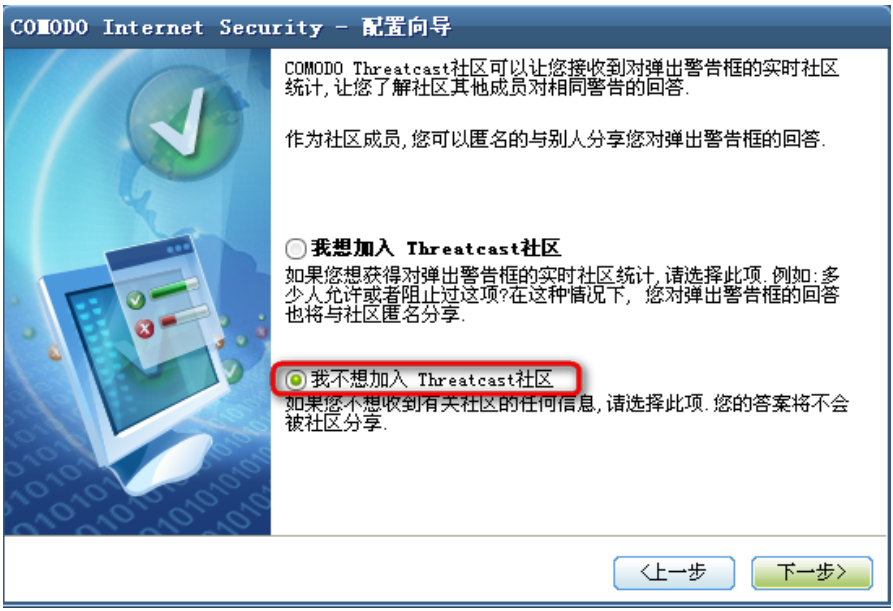


如果您已经安装了杀毒软件，建议不选择安装杀毒模块，取消勾选，下一步




COMODO Internet Security - 配置向导
COMODO Internet Security 有很多强大的功能，当它被安装后，您将看到它将影响弹出警告框的数量.
防火墙
这个选项是为需要企业级强度网络防火墙的用户提供的.
防火墙主动防御与优化
这个选项提供最佳的网络安全防护，添加保护对抗恶意软件通常使用的绕过防火墙软件的方法.
防火墙与最大主动防御
这个选项提供最高的安全防护，包括漏洞保护和对抗恶意软件威胁.
〈上一步
下一步〉

选择不加入，下一步

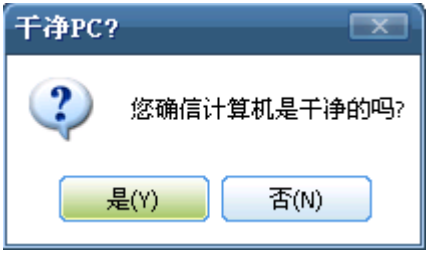

COMODO Internet Security - 配置向导
COMODO Threatcast社区可以让您接收到对弹出警告框的实时社区统计，让您了解社区其他成员对相同警告的回答.
作为社区成员，您可以匿名的与别人分享您对弹出警告框的回答.
我想加入 Threatcast社区
如果您想获得对弹出警告框的实时社区统计，请选择此项. 例如：多少人允许或者阻止过这项?在这种情况下，您对弹出警告框的回答也将与社区匿名分享.
我不想加入 Threatcast社区
如果您不想收到有关社区的任何信息，请选择此项. 您的答案将不会被社区分享.
〈上一步
下一步〉

取消这三个勾，下一步

下一步

如果系统是干净的，取消病毒扫描，完成

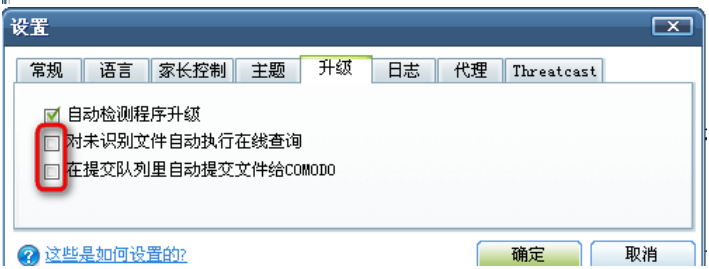
如果系统是干净的，点确定完成安装



点完成，重启计算机

检测私有网络，直接点确定就可以

需要设置的地方



科摩多互联网安全套装主界面

说明

防火墙

默认设置为安全模式 在此模式下，对于“**安全**”程序，防火墙将自动学习并创建通信的规则。对于未知程序，防火墙将阻止其访问网络，并弹出一条警告信息。此模式——**在容易管理的连接警告数量下，整合了最高级别的安全。**

当然这要依赖于科摩多互联网安全套装内置的**安全可执行程序白名单**，目前列表中已有超过 1,000,000 个应用程序

学习模式：：防火墙将学习所有程序的网络活动并自动创建允许规则。在此模式下，您不会收到任何警告信息。

所以只有您百分之百确认在您计算机上安装的所有应用程序都是安全的，才可以采取此模式进行学习

提示：当您第一次运行某个信任网络程序时，可以临时使用这个设置，当防火墙学习这个程序行为并自动为它们创建“允

许”规则后，在切换到您原来的模式。

自定义规则模式 只有用户定义的程序可以上网，防火墙不会学习任何应用程序行为。也不会自动为这些程序创建规则。当应用程序尝试建立连接时，您将随时收到警告信息。

这是最安全的模式，不过需要一定的经验，建议高级用户使用，而初级用户建议使用安全模式

Defense+

Defense+默认采用干净 PC 模式，**干净 PC 模式** 的前提是你的电脑必须干净，**此模式** 假设你的电脑硬盘里的当前所有程序是安全的，并学习它们的活动，一般不会提示；而所有新安装在系统中的可执行文件受到监测和控制。干净 PC 模式大大简化了操作难度，加上科摩多内置的白名单，使新手使用科摩多成为可能

对于新建立、更新、修改的可执行文件(包括 exe、dll、sys 等)，都会被加入 **等待审核的文件** 等待用户审核。
等待审核的文件 的文件是不信任的，任何动作都将会提示。为了保证系统安全，在**干净 PC 模式**下，必须 100% 确认这些文件是安全的，才能从待审核区移**除**，一旦移出待审核区，这些文件将会成为安全的，Comodo 对以后的一般操作都不会提示。对于不确认的，请保留到 **等待审核的文件** 直到最后确认是否安全。对于不存在的或者临时文件，可以用 **清理** 移除。 对于不安全的，直接在资源管理器里彻底删除。

学习模式 Defense+将监视并学习所有的可执行文件的动作并自动创建‘允许’规则直到安全级别被调整。在‘学习模式’下您将不会收到任何的 Defense+ 警告。

提示：暂时的启用该模式可以方便首次运行一个（未知，但值得信赖的）应用程序。这将禁止一切 Defense+ 警告，同时科摩多互联网安全套装的学习这些应用程序在您计算机上运行时需要的组件并且为它们自动创建'允许'规则。学习之后千万不要忘记切换到您原来的模式

安装模式 此模式给了程序最大的权限，一般只在安装绝对信任的程序时采用。安装完成以后要记得切换回来

安全模式：只有白名单中的程序被认为是安全的，Defense+将学习他们的活动并为之创建规则。对于非认证的、身份不明的应用程序，您将收到警报。

如果您不能确定系统是否干净，安全模式是最佳选择--它结合了最高级别的安全性和易于管理的 Defense+ 警告。而对于干净的系统的用户，我们建议您使用干净 PC 模式

如何应答报警窗口

询问框安全等级

询问框安全等级分为三类，以黄，橘，红三色表示。可以帮助用户判断，但是这只是辅助之用，还需要结合安全评估进一步分析方可做出允许或阻止选择。

黄色报警------低威胁报警。在大多数时候你可以允许这些网络连接请求或行为请求。这个等级默认对安全请求是自动勾选（记住我的选择）选项的。

橘色报警------中度威胁报警。请仔细阅读安全评估后再做出决定。这个警报可能是信任程序的无害进程或活动，也可能是恶意软件的攻击。如果你知道这个程序是安全的你通常可以选择允许，如果你不清楚这个程序执行的动作或连接是否安全你可以阻止它。这里我的建议是如果有进程或动作不清楚，可以百度或狗狗来了解下，对判断很有帮助。

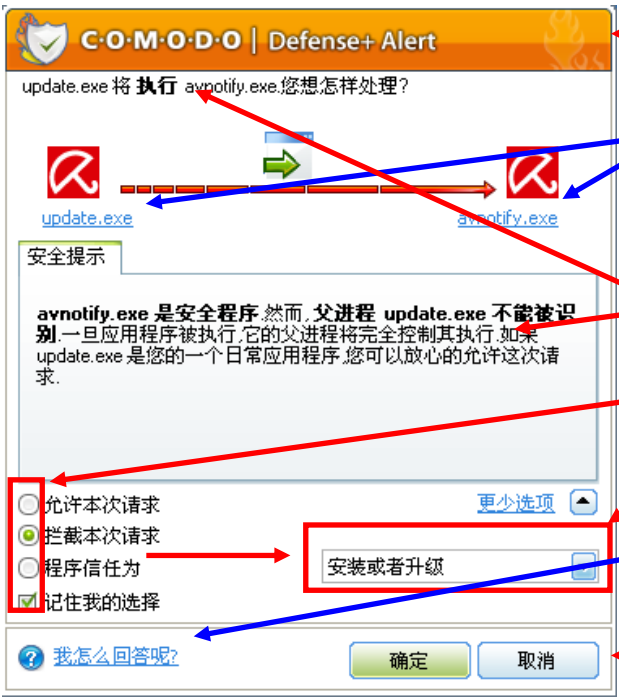
红色报警------高威胁报警。这个报警显示了类似木马病毒或其他恶意软件活动的高度可疑行为。在允许此活动前请仔细阅读提供的信息，慎重决定，不能确定的话百度 GOOGIE 是你的好帮手哦

Defense+预置规则

安装或升级——〉赋有极大权限，只在安装信任程序时使用

系统程序——〉不用解释了吧

高威胁报警



中度威胁报警

查看程序属

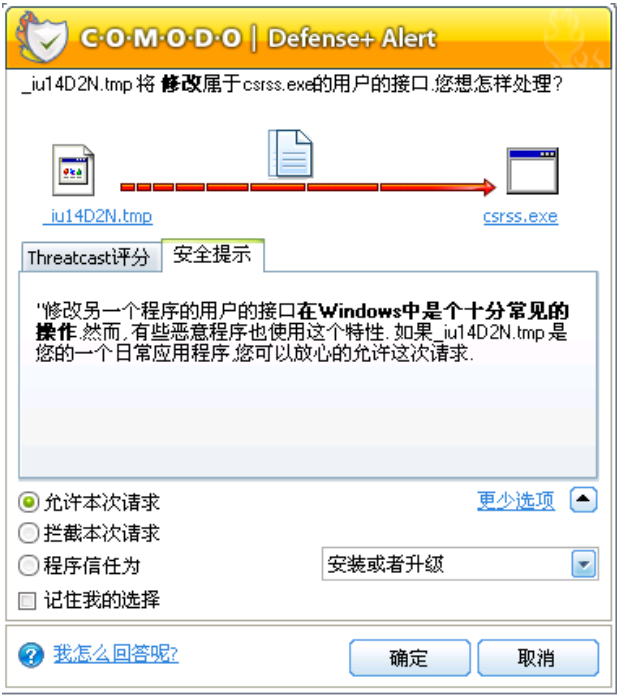
安全评估

动作

预置规则

帮助

点取消为拦截一次



低威胁报警

信任程序——〉允许一切，不是信任的程序不要使用此规则

上面三个预置规则都要慎用

受限程序——〉对于未知程序可采用此规则，不过因为受到限制，很多程序可能不能正常运行

隔离程序——〉应用此规则后，程序将被监禁，不能运行

对于行为监控询问

报警窗口出现以后，首先查看父、子两个应用程序，是否是自己熟悉的，对于不熟悉的，可以通过察看其属性来辅助判断，再通过**安全等级**（低、中、高），配合**安全评估**来决定采取的动作。

Comodo 能够识别数百万种安全程序，如果程序被认为是安全的（安全评估里可以看见），你可以选择允许。同样如果程序是未知的或不能识别的 comodo 也会在安全评估里直接告诉，

对于信任的程序，可以直接套用信任程序规则，省去了以后询问的麻烦。

如果是你平常经常用的程序，你可以允许它的动作请求，并勾选**记住我的选择**，这样以后就不会再弹出警报了。

如果是你没有见过的程序，请慎重决定，最好先阻止，但是不要选记住，也可以点取消，取消代表阻止一次。然后百度 google 搜索一下有关信息，下次出现这个询问是就知道怎么做了。

如果不是安装程序请不要把程序归为'Installer or Updater'（安装升级）类型。因为这个类型给予了程序最大的权限，如果你必须使用可以暂时选择此类型，但请不要选中“记住”选项。

需要留意的弹出警告

Defense+

1、 修改 Windows 系统程序、explorer、安全软件、IE、其它浏览器内存空间

2、 对于安装驱动要十分小心，因为一般程序是不会安装驱动的，除非安全软件和安装特定的设备驱动。 不认识的程序安装驱动一律阻止，一旦安装加载驱动，程序将获得和 HIPS 一样的底层权限，拥有这种权限的程序可以使 HIPS 的保护部分或全部失效。

3、 访问物理内存，一般程序也不会有的行为。直接访问物理内存也可以获得很高的系统特权。一般直接阻止。

4、 底层磁盘，一般程序也用不到，直接阻止。

5、 底层键盘，不认识的程序，直接阻止。防止键盘记录。

6、 对于不认识的程序，修改注册表自启动、服务驱动、映像劫持 直接阻止。

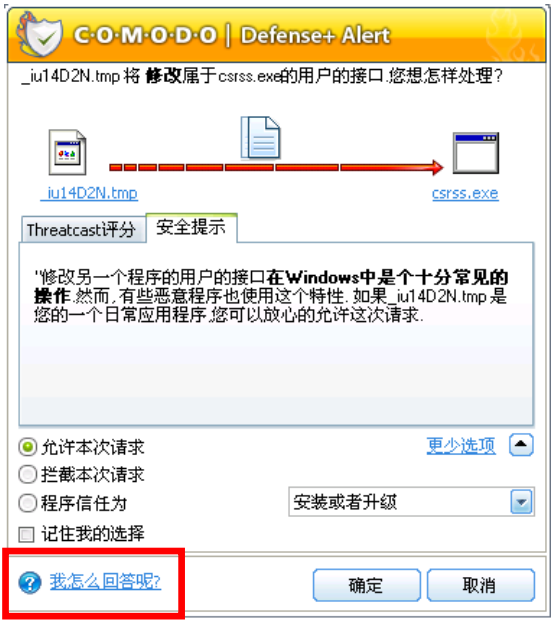
7、 对于 COM 接口 Pseudo COM Interfaces - Privileges 提升权限，一般程序很少用到，最好阻止。LocalSecurityAuthority.Debug 提升权限到 Debug 直接阻止，非常重要，除非是完全信任的程序 LocalSecurityAuthority.SystemTime 修改系统时间直接阻止。 通常只允许 rundll32 修改系统时间。LocalSecurityAuthority.Restore 系统还原，可以绕过已设置的文件、注册表权限，非系统程序直接阻止。Pseudo COM Interfaces - Privileges 下的所有项，对于不认识的程序，直接阻止。 Service Control Manager (\RPC Control\ntsvcs) 涉及到对服务的管理，不认识的程序直接阻止。

防火墙安全提示

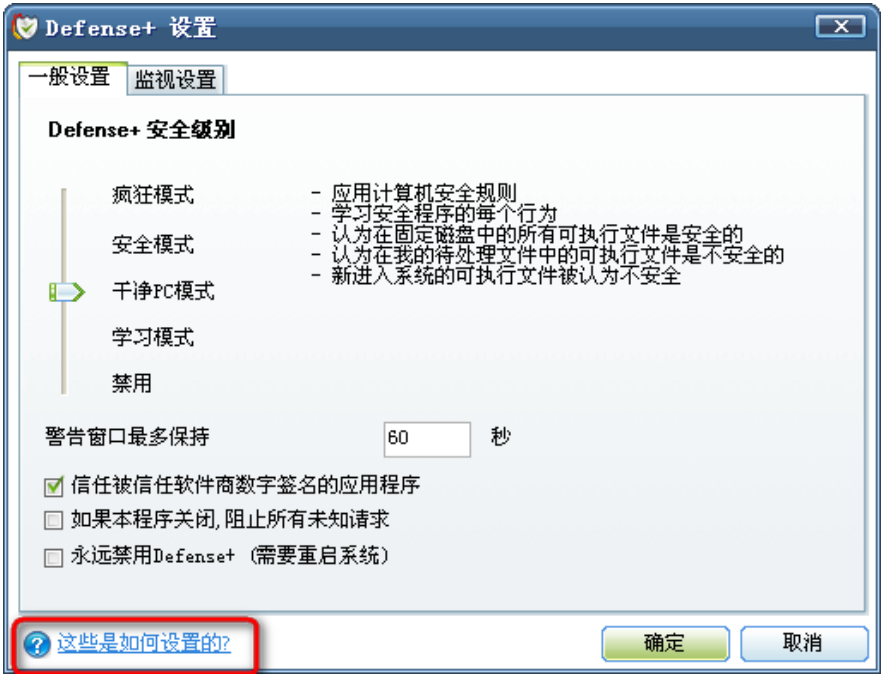
防火墙提示和 D+差不多，这里也可以直接套用预置规则，就不多讲了，记住一点，不认识的程序一律阻止 Blocked Application

解决问题的方法

自带帮助



不明白的地方可以直接点击窗口左下方的帮助连接

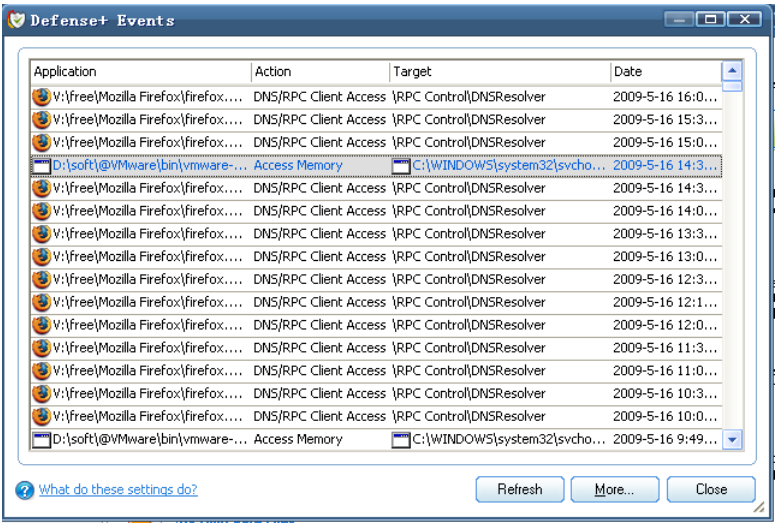


[片禁歌禁曲]

查看日志

当系统或程序出现莫名其妙的问题时，不要忘了及时查看日志，看看是否是科摩多阻止造成的

下图中火狐被阻止访问 DNS，利用代理破网没有问题，直接上网恐怕不行了——**Defense+日志**



——防火墙日志