

ZoneAlarm 8.0.298 防火墙汉化版安装使用教程

目 录

- 1 ZA8.0 防火墙使用要点 1
- 2 ZA 防火墙的自动安装..... 3
 - 2.1 准备工作..... 3
 - 2.2 自动安装步骤 4
 - 2.3 可能会遇到的安装问题 5
 - 2.4 第一次启动 ZA 的判断 6
- 3 ZA 防火墙界面布局和简单设置..... 9
 - 3.1 主要界面布局和设置..... 9
 - 3.2 程序控制界面和功能说明 14
- 4 设置程序访问网络和处理警告提示信息..... 16
 - 4.1 常见程序网络访问对话框举例..... 16
 - 4.2 常见程序的信任水平设置参考 20
 - 4.3 中英文对照表的使用（用于英文警告框） 20
 - 4.4 常见的红色英文警告对话框的设置..... 23
- 5 清除 ZA 防火墙的痕迹 26
- 6 设置防火墙防止误连禁网（参考） 27
- 7 ZA 各版本卸载及其它（参考） 30
 - 7.1 ZA 5.5 版本卸载 30
 - 7.2 ZA 8.0 版本卸载（卸载必看） 30
 - 7.3 关于几个精简掉的安装选项..... 32
 - 7.4 手动安装英文版和汉化..... 32
 - 7.5 无法自动或手动安装的解决..... 38

如有不足和需要完善之处请反馈给我们以便继续完善

防火墙是必须要安装的一个软件。具有防止网络黑客入侵本机、设置本地程序网络权限、和防止木马泄漏信息的作用。由于 ZoneAlarm 防火墙（简称 ZA）使用简单，兼容性好，因此这里推荐使用 ZA 防火墙。以前的 ZA5.5 对目前的木马基本没有防护能力，因此，如果想达到相对好一些的防木马效果，就需要安装较新的版本了，例如 ZA 8.0.298，ZA8 支持 XP/Vista 系统。

ZoneAlarm 8.0.298 请破网访问下面地址下载

<http://tiandixing.org/viewtopic.php?f=25&t=69193>

解压缩之后会得到安装程序 za_en80298.exe，这个文件的校验值如下：

MD5: AC18B2800D90C2648AC52BE782AACD88

SHA1: 376FF1A054F73C5B97123781980026C5A9C8ECD6

如果你从其它途径得到相同校验值的安装程序也可以使用。

1 ZA8.0 防火墙使用要点

这里先把这个使用要点放在前面，请先大概的浏览一遍，有不清楚的地方没有关系，看完教程再回过头来熟悉一遍就比较清楚了。

新增: ZA 防火墙和 Mcafee 在一些电脑可能存在冲突，导致系统运行缓慢，如果出现此情况建议换用其它组合。

新增: ZA 的小版本号之间的升级可以忽略，例如从 8.0.059 版本升级到 8.0.298 版本，如果手动升级，则会自动还原为英文版本。建议关闭更新检查。

新增: 完善了自动安装程序；解决了组件窗口中删除组件导致 ZA 直接退出的问题（汉化问题）。如果希望升级到最新版本，请卸载以前版本，从新启动计算机之后再安装此版本。

- **重要:** 良好的使用习惯是任何系统纯净的前提，也是在技术层面安全使用计算机的保证。平时只运行可靠的程序，不运行安全性和来源未知的程序，这种情况下，即使安装普通的杀毒软件和普通的防火墙软件，也能够使计算机处于安全状态。
- 一定要开启自动更新安装最新的系统补丁，系统补丁的重要性甚至要高于杀毒软件和防火墙软件。（不联网的计算机，不需要安装防火墙软件和升级系统补丁，但是需要安装一个杀毒软件和升级病毒库）
- 安装好 ZA8 后，第一次启动计算机时，可能需要相对长一些的时间才能

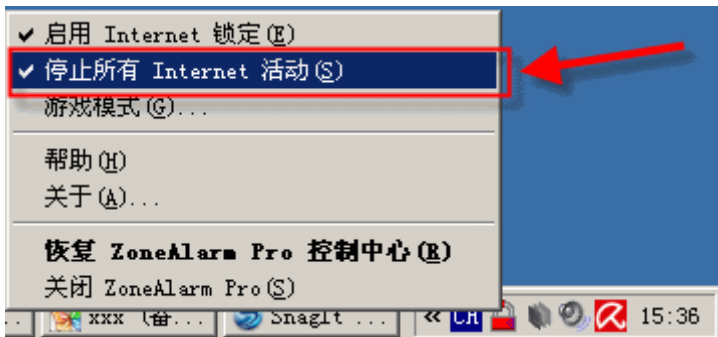
进入到桌面和显示 ZA 图标，以后再启动的时候就会好很多。有的环境 ZA 可能会延长从开机到启动到系统桌面的时间。**如果计算机内存不超过 256MB，不建议安装 ZA8.0 版本，否则可能系统运行速度会比较慢。**

- 建议安装前先备份一下系统，避免安装 ZA 后遇到问题无法解决的情况。例如安装后发现系统异常缓慢，卸载 ZA8 后却发现无法再安装以前版本的 ZA 防火墙软件了，这时就可以恢复系统备份来解决这个问题。
- 防火墙提示发现新网络时，如果您对照这个网络不熟悉，就把它添加到 Internet 区域。
- 防火墙安装好后要知道哪些程序可以访问网络，千万不能见到任何程序都允许，这和不安装防火墙没有什么区别。可以允许访问网络的程序有破网软件、浏览器、下载软件、杀毒软件，除了上面几类之外的程序，不认识的程序要访问网络，就禁止它们。
- ZA 会对可疑或危险的行为会有红色的英文警告框，对这些程序的处理见 4.2 常见程序的信任水平设置参考、4.3 中英文对照表的使用(用于英文警告框)、4.4 常见的红色英文警告对话框的设置
- 程序控制—主页—智能防护顾问：这个功能在设置为自动和手动的时候，可能会发送运行程序的一些特征信息到 ZA 的服务器，从安全角度考虑请关闭这个功能。
- 由于 ZA8 卸载程序存在缺陷，请在卸载 ZA8 的时候，先执行汉化包中的卸载 ZA 前执行.CMD 备份信息，具体见 7.2 小节 ZA 8.0 版本卸载 内容。
- 因为破网时保存的一些 html 文件在打开时有的会有联网情况，所以上完网，如果想打开以前保存的 html 等网页文件，建议启用停止所有 Internet 活动（右键点 ZA 图标，选择 停止所有 Internet 活动）。



停止后，ZA 图标变为一个红色的小锁头，停止所有 Internet 活动前面会增加一个对勾

启用时，鼠标再点带有对勾的**停止所有 Internet 活动**项目就可以了



2 ZA 防火墙的自动安装

2.1 准备工作

安装前最好是创建一个系统备份，以便在遇到故障的时候快速恢复系统。

如果安装时有防护软件提示 C:\WINDOWS\system32\drivers\etc\hosts 被批处理程序修改，请选择允许。

如果在自动安装的过程中出现各种问题而导致无法成功安装和汉化的，请参考教程后面的（[7.4 手动安装英文版和汉化](#)）小节内容。

1) 复制安装程序到汉化包中

解压缩下载的汉化包文件 ZA8_ins.rar，得到的文件夹结构如下：



把官方下载到的 20 多 MB 的 zapSetup_80_298_000_en.exe 或者 za_en80298.exe 文件复制到批处理命令所在的文件夹。其它文件作用：

[System32](#)、[ZoneAlarm](#)：汉化文件的文件夹；

[中英文对照表.TXT](#)：出现英文提示时，参考这个获取翻译；

[卸载 ZA 前执行.CMD](#)：ZA8 在卸载前请执行这个备份系统的卸载项目；

自动安装.CMD：执行自动安装和汉化的批处理命令。

2) 判断是否需要安装 KB943232 补丁

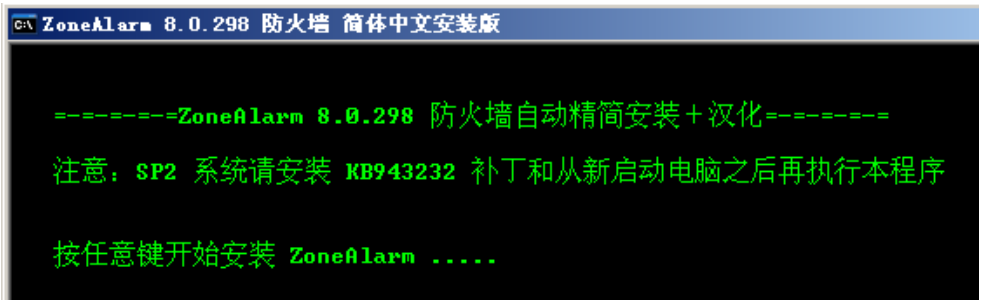
Windows XP SP2 系统，必须先安装 WindowsXP-KB943232-x86-ENU.exe 补丁（右键点桌面的**我的电脑**图标一属性，例如下图显示的就是 Windows XP SP3 版本，如果显示的是 Windows XP SP2 就需要安装这个补丁了），从新启动计算机之后再运行**自动安装.CMD** 这个批处理命令，否则无法安装 ZA 防火墙。（KB943232 补丁安装过程：双击运行 WindowsXP-KB943232-x86-ENU.exe，弹出对话框选下一步，选择 I Agree 之后下一步，之后点完成按钮重启计算机）。



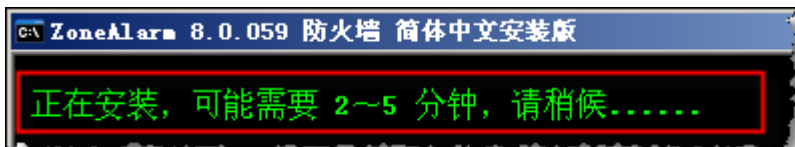
2.2 自动安装步骤

如果遇到无法自动安装的情况，请参考教程（7.4 手动安装英文版和汉化）小节的第二部份 手动复制汉化文件 操作。

如果安装有以前版本的 ZoneAlarm，请卸载以前安装的版本（见教程最后面的第 7 小节），卸载和从新启动计算机之后，双击运行汉化包中的**自动安装**文件，运行后显示界面如下，看到这个界面，按任意键开始安装。



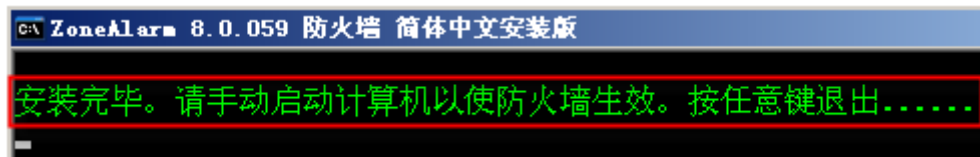
整个安装过程是自动的，安装时会显示一个黑色的 DOS 窗口，窗口中显示“正在安装，可能需要 2~5 分钟，请稍候.....”。请不要关闭这个窗口。



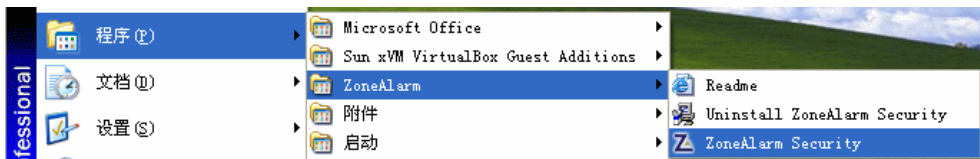
安装的时候，在屏幕右下角的通知栏处会有一个小电视似的图标，如图



安装完毕，屏幕右下角的小电视图标消失，同时 DOS 窗口会提示“安装完毕。请手动启动计算机以使防火墙生效。按任意键退出.....”。



批处理命令安装完毕之后先不要从新启动计算机，执行「开始」菜单\程序\ZoneAlarm\ZoneAlarm Security 启动程序（如果没有这个菜单显示，说明 ZA 没有安装上，参考教程(7.5 无法自动或手动安装的解决)小节内容）

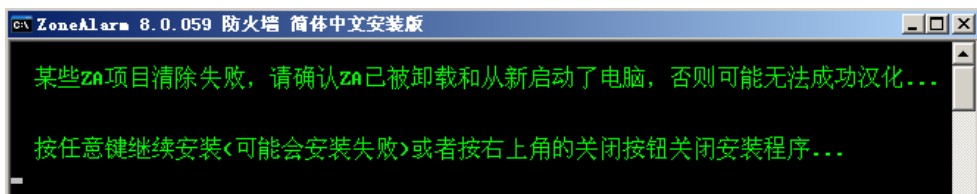


2.3 可能会遇到的安装问题

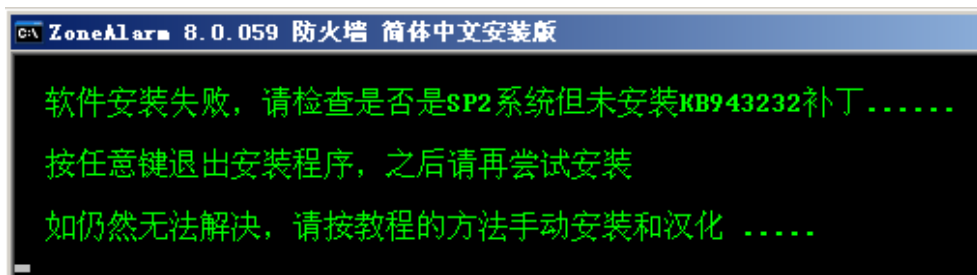
如果提示未发现安装程序，表明当前目录下面没有安装程序，请复制到当前目录后再运行批处理安装命令。



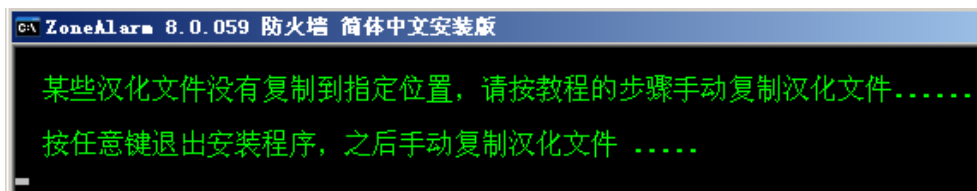
如果显示“某些 ZA 项目清除失败...”这样的提示，表明 ZA 的一些残留的项目没有被删除，可能是 ZA 没有被卸载，这时请关闭批处理命令检查一下。例如是否卸载 ZA 后没有从新启动计算机，或者是有 ZA 的进程如 vsmon.exe 正在运行之中。（以下几个对话框标题的版本号会有不同，内容一致）



（可能会出现）如果批处理命令显示“**软件安装失败...**”，如下图所示，表明软件没有真正安装上，请检查系统是否是 SP2 系统，如果是可能还没有安装 KB943232 补丁，安装这个补丁后从新启动计算机，再执行这个批处理命令。如果是 SP3 系统，请再执行一次批处理安装命令，如果仍然无法解决问题，请参考教程(7.5 无法自动或手动安装的解决)小节内容。



（可能会出现）如果显示“**某些汉化文件没有复制到指定位置...**”，请再运行一遍批处理命令，如无法解决请参考教程（7.4 手动安装英文版和汉化）小节的第二部份 手动复制汉化文件 操作。



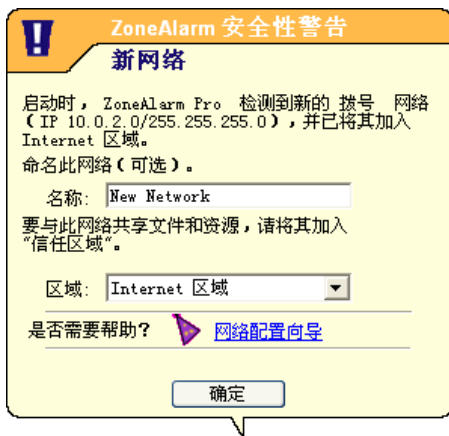
2.4 第一次启动 ZA 的判断

启动ZA之后，ZA可能会提示发现新网络，对任何新网络，如果您不确认，请选择 **保留在 Internet 区域** 之后点 **确定** 按钮添加到 Internet 区域。

以后可以在防火墙主界面点 **防火墙—区域** 来查看和设置这个区域。如果对话框界面显示的是英文，说明没有安装成功，请卸载ZA，从新启动计算机之后再执行自动安装命令。实在无法解决的，请按照图中位置选择第一项之后按OK按钮关闭对话框，之后参考教程（7.4 手动安装英文版和汉化）小节的第二部份 手动复制汉化文件 操作。



如果上面对话框选取消，会弹出下面的信息，加入 Internet 区域即可（如果共享了打印机和文件，需要把可以访问此资源的计算机 IP 加入信任区域。）



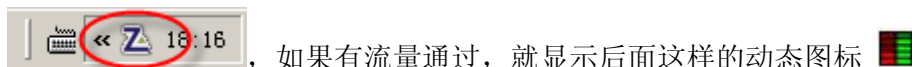
之后就会显示 ZA 的主界面，这样就完成了 ZA 的安装，虽然还没有从新启动计算机，但 ZA 防火墙已经可以使用了，只是 ZA 的自我保护还没有生效。

ZA 主界面左侧有一个侧边栏，所有的功能都可以通过点击侧边栏上的文字按钮来切换。这里看到侧边栏一共有四个项目：概述、防火墙、程序控制、警报和日志，点击某一个项目，这个项目就会展开同时其它项目关闭。

当点击某个项目的子项目时（例如对 **概述** 而言，**主页**、**产品信息**、**首选项**就是它的子项目），该子项目前面就会有一个箭头→表示被选择状态。



ZA 防火墙在通知栏的图标如下，双击这个图标也可以启动 ZA 的主界面。

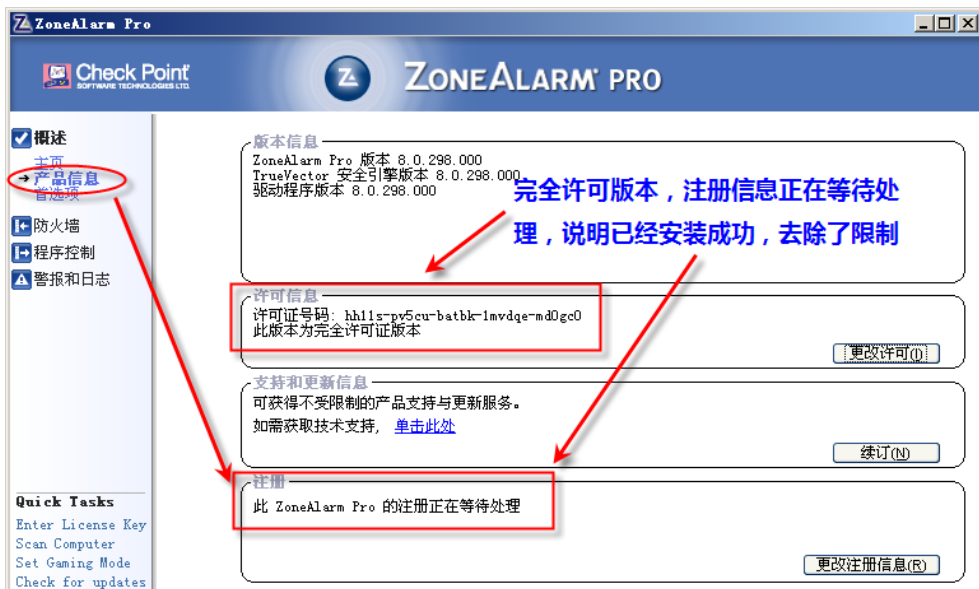


如果鼠标右键点这个图标，弹出菜单中选择“恢复 ZoneAlarm Pro 控制中心”就可以显示 ZA 的主界面了。

安装后，ZA 防火墙在系统中占有两个进程 vsmon.exe 和 zlclient.exe。

vmware.exe	Administrator	01	26,444 K	15,452 K
vmware-vmx.exe	Administrator	00	193,128 K	11,220 K
vsmon.exe	SYSTEM	00	19,792 K	17,608 K
winlogon.exe	SYSTEM	00	4,208 K	6,076 K
zlclient.exe	Administrator	00	2,836 K	18,216 K

ZA 的 概述—产品信息 中，始终会显示“此 ZoneAlarmPro 的正在等待处理”，这就表明已经安装成功了可以正常使用了，但对功能没有影响。



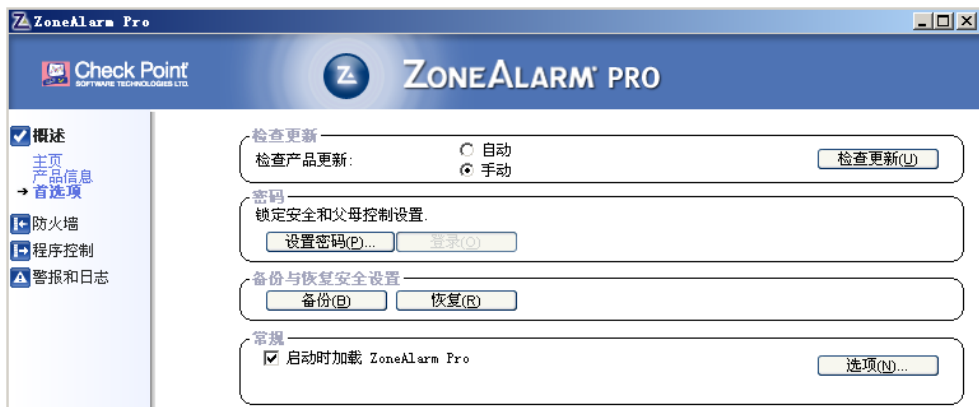
3 ZA 防火墙界面布局和简单设置

精简安装后防火墙主界面的最左侧，有四个功能按钮，分别为：概述、防火墙、程序控制、警报和日志，这里对这几个界面布局叙述如下。

3.1 主要界面布局和设置

1) 概述一首选项：

“检查更新”建议选择“手动”，ZA 的检查更新其实就是下载新版本，但是安装以后会变成英文版本，一般小版本号之间的升级都可以忽略。



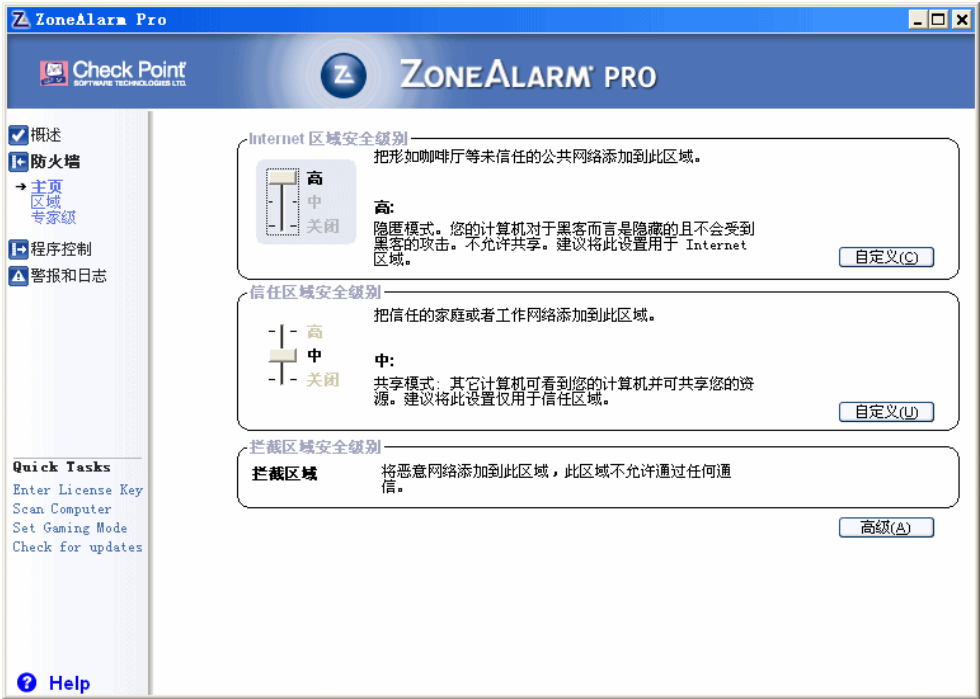
“备份与恢复安全设置”这里可以备份和恢复 ZA 的设置（包括防火墙和

程序控制等)，兼具清除痕迹的功能（在没有破网的时候创建一个没有任何破网软件痕迹的备份，破网后恢复这个备份的同时也会清除破网痕迹）；

选择“备份”的时候会弹出一个对话框让您选择备份文件的存放位置，默认扩展名是 xml，以后恢复的时候，点“恢复”按钮，在打开文件对话框里面，浏览并双击以前备份的 xml 文件就会恢复备份。

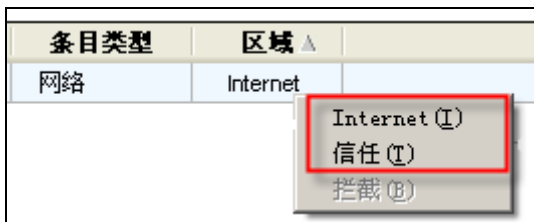
2) 防火墙—主页：

下面图中的设置就是默认设置，“Internet 区域安全级别”的级别是 高，默认设置就可以了，而且也一定要保持 Internet 区域安全级别为 高。



3) 防火墙—区域：

这里可以显示的是 Internet 区域和信任区域（如果添加了）的情况。也可以自己添加 Internet 区域或者是信任区域。如果设置错了，也可以在区域栏目点一下鼠标左键，在弹出的区域类型里面从新选择区域。



设置 127.0.0.1 信任区域的方法见教程的第 6 小节,有需要的可以参考。



4) 程序控制—主页:



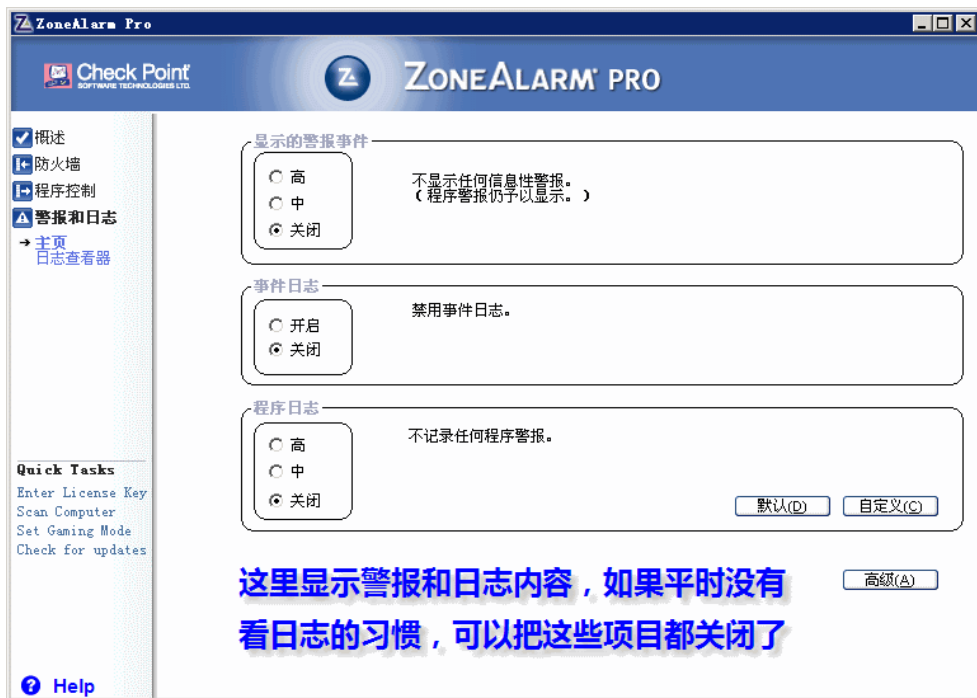
关于智能防护顾问：这个功能在设置为自动和手动的时候，可能会发送运行程序的一些特征信息到 ZA 的服务器，从安全角度考虑请关闭这个功能。这个功能使用批处理自动安装后是关闭的。请安装后再检查一遍。

5) 警报和日志一主页：

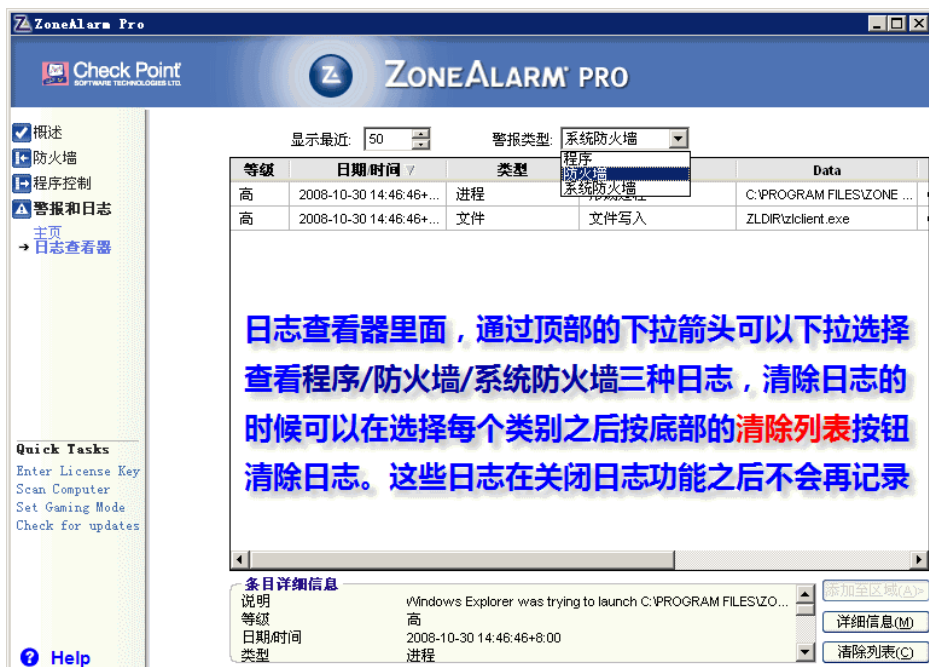
这里默认设置是开启的，如果平时不看日志，建议关闭，这样也不会留下相关的痕迹。

如果开启日志，可以在警报和日志一日志查看器里面看到日志信息。

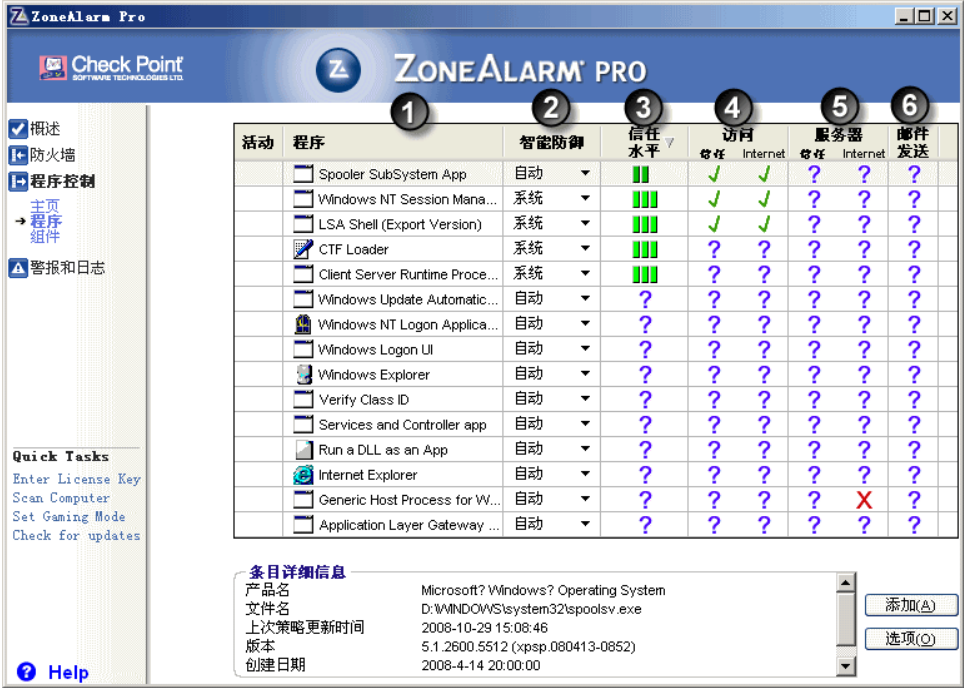
在日志查看器里面，可以通过下拉箭头选择查看程序、防火墙、系统防火墙的日志，清除这些日志的时候，可以切换到各个日志界面，之后点清除列表可以清除已经记录的日志。



在退出ZA的情况下，[无影无踪](#)可以清除这些日志。在关闭日志的情况下，这些日志信息讲会被清除。



3.2 程序控制界面和功能说明



1) 程序控制—程序（见上图）:

所有运行的程序都会在这里显示，主要内容可以分为六列：

① 程序名称，选择程序之后，在窗口底部可以看到程序的路径版本等信息，右键点程序，也可以选择属性选项来查看文件的具体信息；

② 智能防御：这里一般不需要特别配置；

③ 信任水平：对程序可执行操作范围的设定，一会详细叙述；

④ 对程序访问信任区域和 Internet 区域的设置，✔ 表示允许，✘ 表示禁止，？ 表示询问；




⑤ 对于程序是否可以担任服务器的设定，✔ 表示允许，✘ 表示禁止，？ 表示询问；

⑥ 程序是否可以发送邮件（除了邮件客户端都可以阻止）

在程序栏目，鼠标右键点击某个程序，弹出右键菜单中选择属性，就会显示这个程序的路径和提示信息等参数。

2) 程序控制—程序—访问、服务器




4访问 和 **5服务器**，用于控制程序的联网权限，需要在访问网络的时候手动设置。

如果在访问或服务器栏目，鼠标左键点击对应某个程序的  /  /  图标，会弹出下面的权限设置菜单，点击哪个项目就会设置网络权限为哪个类型。

程序	智能防御	信任水平 ▾	访问		服务器	
			信任	Internet	信任	Internet
 Internet Explorer	自动 ▾					
 Guard GUI Applicati...	自动 ▾					
 Generic Host Proce...	自动 ▾					
 Firefox	自动 ▾					

 允许 (A)
 拦截 (B)
 询问 (C)

访问和服务器栏目都有三个设置选项：

-  此程序被允许访问网络/担任服务器；
-  表示询问程序访问网络/担任服务器的权限；
-  此程序被拒绝访问网络/担任服务器

说明：即使是在关闭职能防御顾问的情况下，由于 ZA 内置了一些系统程序的白名单信息，因此对于可靠的程序，ZA 有时会自动设置为允许。ZA 自动设置的程序不属于安全隐患，但是可以手动再设置回来。

3) 程序控制—程序—信任水平


3信任水平 里面包含的是高级程序控制的规则，控制的是程序间的调用权限，这个权限一般不需要手动设置，在有程序遇到请求许可的时候，ZA 会根据用户在对话框里面的选择自动设置信任水平。在**信任水平**栏目某一程序对应行点鼠标左键，会弹出如下菜单：


智能防御	信任水平 ▾	访问
定义 ▾		
动 ▾		
动 ▾		
动 ▾		
动 ▾		
动 ▾		


 超级
 信任
 限制
 询问
 终止
 无执行


共有六个设置选项，用来控制程序间的调用权限：


无要求，权限最高，不会监控程序，此程序可以执行任何行为

 超级权限，允许任何程序执行任何可疑和信任的活动并且不会提示窗口，ZA 里面对于少数可信的系统进程会自动设置为超级权限，一般没有特殊情况，自己不要设置这个权限。

 信任权限，信任的程序可以执行可疑操作而不会弹出询问窗口，而对于未知程序执行此类可疑操作时必须询问权限

 限制的权限，允许程序执行可信任的操作，但是会直接禁止其的危行为

 询问，当 ZA 认为程序可能执行可疑行为时，会弹出 Suspicious Behavior 警告对话框

 终止，禁止此程序执行

关于一些程序信任水平的设置和判断见教程的4.2/4.3/4.4小节。

关于端口封闭：有一些文章谈到了封闭端口来增强安全性，对于个人计算机而言，安装 ZA 和把 Internet 区域安全级别设置为“高”的情况下，ZA 是禁止所有端口通讯的，只有当本机程序被授权访问网络时，才开放对应程序需要的端口，因此不必额外封闭端口。

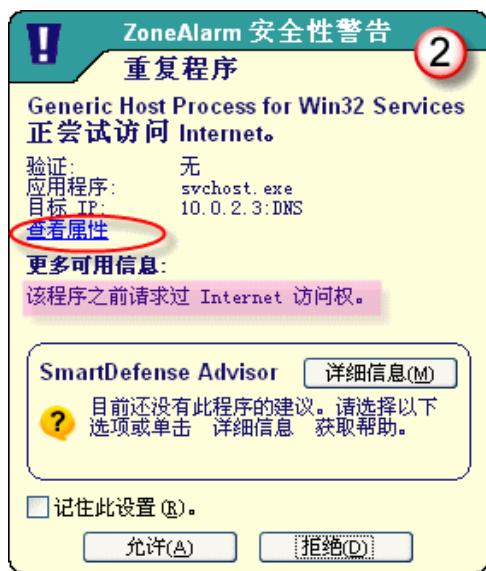
4 设置程序访问网络和处理警告提示信息

4.1 常见程序网络访问对话框举例

当一个程序要访问网络时，ZA 会弹出对话框提示这个程序要访问网络，由您来决定这个程序的网络许可，下面举例说明。

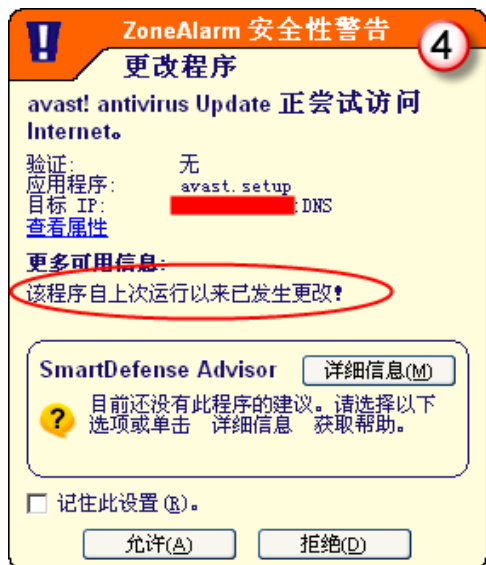
Generic Host Process for Win32 Services 正尝试访问 Internet 图①

点目标 IP 下的 [查看属性](#) 文字按钮（下面右图红圈位置所示），可以调用系统的文件属性对话框，会打开系统的文件属性对话框，可以了解这个程序的路径和版本等信息。如果遇到不认识的程序，查看属性可以获取其位置以便辅助判断。本例中，程序名称：`svchost.exe`，位置：`C:\WINDOWS\system32`。



对话框以不同颜色显示，顶部会显示程序类别(如图①中红圈处显示)：

新程序：如图①。对话框顶部的提示是“新程序”，同时防火墙会提示这个程序初次首次访问网络，提示对话框颜色显示为橘黄色。一般新安装完系统就会有这个 `svchost.exe` 的提示，这个是和自动更新以及 DNS 解析有关的，如果不允许会无法上网。



重复程序：图②表示 `svchost.exe` 要访问网络，对话框顶部的提示是“重

复程序”，表示这个程序以前曾经访问过网络，对话框显示颜色为青色。由于我这里知道这个程序是可信的，所以这里选择允许。

服务器程序：如图③所示，担任服务器的程序提示对话框为靛蓝色。在弹出的小方框中选择“拒绝”按钮就会拒绝其担任服务器。如果在询问对话框中选择“记住此设置”后点“拒绝”按钮，以后防火墙自动拦截此行为而不再提示。在以后的使用中，除了破网软件，莲花代理这样可靠的软件之外，其它的任何程序要担任服务器时，都一律禁止。

更改程序：ZA 防火墙可以对程序是否改变做判断。图④对话框颜色是红色了，对话框的顶部提示为“**更改程序**”，这是因为升级了 avast! 杀毒软件的版本序，我们知道这次改变是可信的，因此选择允许。如果您正在上网的时候，弹出这样红色的询问对话框，而在确认没有对上网程序做任何修改的情况下，这时需要谨慎一些，这时建议检查一下病毒看看有没有异常。

如果程序提示想要接受来自 Internet 的连接，例如 svchost.exe，这个时候可以看到对话框颜色是靛蓝色，也就是说这个程序要担任服务器，没有特殊情况，请禁止并记忆就好。



此外还有几个访问类型，说明如下：

Generic Host Process for Win32 Services 访问 255.255.255.255:DHCP 遇到这个提示，**选择允许**，这和获取 IP 地址有关，如果禁止了有可能在有的路由环境出现问题。

Generic Host Process for Win32 Services 访问 239.255.255.250:Port 1900 拒绝就可以。



一般我们在“程序控制”的“程序”栏目中，可以看到所有要上网程序的通过或拒绝状态，我们在这里可以对程序的上网许可进行设置。

对允许通过的程序，在“访问”栏目下选两个“√”，在“服务器”下选两个“X”，在“邮件发送”下选“X”，例如图中的 IE 浏览器；

活动	程序	智能防御	信任水平	访问		服务器		邮件发送	
				信任	Internet	信任	Internet		
	Free Download Ma...	自定义 ▼	?	√	√	X	X	X	
	Freemate, Fast and ...	自定义 ▼	?	√	√	√	√	?	
	Generic Host Proce...	自定义 ▼	?	√	√	X	X	X	
	Internet Explorer	自定义 ▼	?	√	√	X	X	X	
	Microsoft Office W...	自定义 ▼	?	X	X	X	X	X	

对于破网软件，由于破网软件需要担任服务器，并且是可信的，就在“访问”和“服务器”栏目下选四个“√”，例如图中的小鸽子图标的自由门软件；

对于 Generic Host Process for Win32 Services（这里对应图中的第三项）在服务器位置选两个“X”，在访问位置选两个“√”（即不允许 Generic Host Process for Win32 Services 担任服务器，但允许它访问 Internet，如果不允许它访问 Internet，在不破网的时候会无法打开常人网站）。

对不允许通过的程序，例如 Word 程序，在所有栏目下都选“X”，其它和破网无关的软件也同样不允许访问网络（破网的时候，如果复制内容到 Word 中，有时 Word 会提示连接网络，请一定阻止，否则可能会导致直接连接禁网）。


如果提示 Spooler Subsystem App 访问网络，程序名称是 spoolsv.exe，是打印机共享联网请求，请选择禁止，因为有利用这个漏洞的木马。

在所有的程序中，除了 Generic Host Process for Win32 Services 允许访问网络、浏览器允许访问网络、下载软件允许访问网络、破网软件允许访问网络和担任服务器之外，其它的程序都可以设置为禁止访问网络。

4.2 常见程序的信任水平设置参考

在出现红色的程序权限设置对话框提示的时候（见 4.3 小节的第一个图片），需要在对话框里面设置是否允许程序执行一些行为，设置以后，在 ZA 的程序控制一程序的信任水平栏目就会相应的出现改设置结果。

因此对于一些程序，需要区分是**信任水平**的权限，还是**联网权限**，两者是不同的。信任水平里面的权限主要控制程序对系统或者其它程序操作（例如是否允许程序修改桌面背景，是否允许程序修改IE主页，信任水平的对话框为红色提示对话框），但不带有IP地址等网络信息；联网权限是允许程序是否可以访问网络或者担任服务器的，提示对话框都带有目标IP和程序对网络访问的提示（例如首次访问网络、重复程序、担任服务器等等）。

信任水平的建议设置：启动ZA，在程序控制的程序里，找到CTF Loader（如果没有则添加C:\WINDOWS\system32\ctfmon.exe），设置信任水平为超级；找到Windows Explorer（如果没有就添加C:\WINDOWS\explorer.exe），设置信任水平为超级。这样设置以后会减少一些提示。

下面几个程序，如果遇到提示对话框允许就可以了，括号里面的是路径：

Run a DLL as an App (C:\WINDOWS\system32\rundll32.exe)

Windows NT Session Manager (C:\WINDOWS\system32\smss.exe)

LSA Shell (Export Version) (C:\WINDOWS\system32\lsass.exe)

Client Server Runtime Process (C:\WINDOWS\system32\csrss.exe)

Generic Host Process for Win32 Services (C:\WINDOWS\system32\svchost.exe)

上面的几个程序中，除了 svchost.exe，其它的都不需要访问网络。如果是给别人装机，建议把上面的这些程序都设置一下，再把一些常用的程序设置好网络权限，之后备份一下安全设置，然后教他如何恢复安全设置，这样比较合适一些。

4.3 中英文对照表的使用（用于英文警告框）

ZA 新版本引入了系统防火墙，监控一些针对系统的恶意行为，此类警告对话框以红颜色表示。由于这些提示信息无法汉化，因此刚刚接触这些的网友可能有些不适应。为了便于大家使用，这里把这些无法在软件界面中显示的英文制作成一个中英文对照表，就是压缩包中的 **中英文对照表.TXT** 文件，

遇到此类的英文可以到那里去查询。红色警告信息看起来很多，其实只有 30 多类，根据对照表可以很容易的找到实际含义。这里举个例子来说明。

下面这个对话框是 ZA 对小红伞升级程序的警告。中间的提示是英文，我们这里演示一下如何找到这些英文的实际涵义：



顶部的 **SUSPICIOUS BEHAVIOR** 在对照表中查到涵义为 **可疑行为**。中间的英文提示信息如下：

Antivirus Scheduler is trying to launch C:\Program Files\Avira\AntiVir PersonalEdition Classic\avwsc.exe, or use another program to gain access to privileged resources

对照表中不包含文件名、文件路径、文件描述这些具体的文件信息（这些都使用%process_name%这样的替代符号表示），而只包含动作信息，例如【**进程 A**】正在试图读取和修改物理内存 这样的行为，【**进程 A**】在每个警告对话框里面都不一定相同，而读取和修改物理内存这样的动作才是需要查询的。

接下来说一下如何去掉这些具体文件信息：

点对话框的 **查看属性** 调出系统属性对话框，定位到程序的描述部份

看到描述是 **Antivirus Scheduler**，这个程序描述就是警告对话框最前面的信息。之后再把提示信息里面的（C:\Program Files\Avira\AntiVir PersonalEdition Classic\avwsc.exe）具体路径和文件名去掉。就成了：

is trying to launch, or use another program to gain access to privileged resources



那么下面就可以根据这个提示来在[中英文对照表.TXT](#)中搜索了。使用记事本打开对照表，编辑一查找一在要查找内容处输入要查找的内容。原则就是搜索连续的两个或更多的英文单词，但不要带标点也不要使用被标点分隔的单词，同时尽量使用信息尾部的单词搜索。例如这里提取尾部的[privileged resources](#)，搜索得到：

%process_name% is trying to launch %target_process%, or use another program to gain access to privileged resources

〔进程 A〕正在试图启动〔进程 B〕，或者使用其它程序获取特权资源

%process_name% was trying to launch %target_process%, or use another program to gain access to privileged resources

〔进程 A〕曾经试图启动〔进程 B〕，或者使用其它程序获取特权资源

%process_name% was prevented from launching %target_process%, or use another program to gain access to privileged resources

〔进程 A〕已被阻止启动〔进程 B〕或使用其它程序获取特权资源的行为

每个动作都会搜索到三个关联的行为，%process_name%、%target_process%这样的包含在两个 % 之间的单词是变化的（对应文件名和路径信息等）。注意红色阴影的部份是这些行为的不同之处，再根据前面提取的其它单词对照红色阴影部份，找到完全对应的翻译。

%process_name% is trying to launch %target_process%, or use another program to gain access to privileged resources

〔进程 A〕正在试图启动〔进程 B〕，或者使用其它程序获取特权资源

再把前面去掉的程序信息和文件名等对应回来，这句话就翻译成：

Antivirus Scheduler 正在试图启动 C:\Program Files\Avira\AntiVir PersonalEdition Classic\ avwsc.exe，或者使用其它程序获取特权资源

因为我们知道 Antivirus Scheduler（对应程序 sched.exe）是小红伞的程序，是可信的，所以这个提示框里面选择“应用这个设置到这个程序显示的所有

可疑行为”并选择允许，以后就不会再提示这个警告信息了。

小结：这样的英文提示看起来有难度，实际上对照这里提供的翻译可以确定具体的涵义了。如果感觉对照翻译也有难度，可以点击警告对话框里面的“[查看属性](#)”文字连接查看程序的属性。根据文件的路径来推断文件是否是安全的。

4.4 常见的红色英文警告对话框的设置

对于前面的程序间访问，ZA 会对可疑或危险的行为提出警告，一般的，对于新安装的系统里面的此类程序警告，都是可以允许的。处理这些警告对话框的时候，对于这些警告信息是否允许，主要看这个程序的路径等信息判断。如果是常规的系统程序，可以允许，如果这个文件的路径很奇怪，例如在临时文件夹或者 IE 的临时文件夹，那可能就需要注意了，只要不是手动运行的可以确认安全的，一律禁止。例如下面这样的路径下，都需要注意。

C:\Documents and Settings\Administrator\Local Settings\Temp\
C:\Documents and Settings\...\Temp\Temporary Internet Files\

这些警告对应信任水平里面的权限设置。对于此类的警告对话框，如果在警告对话框里面选择允许，则程序被赋予超级权限，如果选择拒绝，程序被赋予受限权限。

实例 1: `wmiadap.exe` 警告（全新系统，新安装 ZA 后提示）



搜索关键字 `its process` 并根据上下文，定位到：

```
%process_name% is trying to communicate with %target_process% by  
opening its process
```


〔进程 A〕正在试图通过开启〔进程 B〕的进程的方式与之通讯
翻译之后就是：

wmiadap.exe 正在试图通过开启 smss.exe 的进程的方式与之通讯

操作：系统全新无毒，wmiadap.exe 是系统程序，所以可以选择允许。

实例 2:CTF Loader (ctfmon.exe) 警告（全新系统，新安装 ZA 后提示）



搜索 user beha（不一定要写全），结合上下文，定位到

%process_name% is attempting to monitor user activities on this computer. If allowed it may try to track or log keystrokes (user input), mouse movements/clicks, web sites visited, and other user behaviors

〔进程 A〕试图监视此计算机上的用户行为。如果允许，它可能会追踪或记录键盘击键(用户输入的)、鼠标移动或点击、访问的网站，以及其他用户行为。

翻译：CTF Loader (ctfmon.exe) 试图监视此计算机上的用户行为。如果允许，它可能会追踪或记录键盘击键(用户输入的)、鼠标移动或点击、访问的网站，以及其他用户行为。

操作：CTF Loader (ctmon.exe) 是输入法控制程序，允许并记忆。

实例 3:记事本程序操作 CTF Loader (ctfmon.exe)



搜索关键字 **its process** 并根据上下文，定位和翻译：

记事本 (notepad.exe) 正在试图通过开启 ctfmon.exe 的进程的方式与之通讯

操作：所有的允许键盘输入的程序都有可能这个提示，只要这个程序是您运行的和熟悉的，就可以记忆并允许。

实例 4: explorer.exe (C:\WINDOWS\explorer.exe) 行为

如果遇到 explorer.exe 的提示，如果不是访问网络的可选择允许。如果不点允许，可能会导致系统反映缓慢等情况，有时系统甚至会失去响应。对于新系统，建议安装 ZA 后，在程序控制里面浏览到 C:\WINDOWS\explorer.exe 并设置其信任水平为超级。



如果计算机使用一段时间以后，执行开始菜单中的项目，出现下面提示：



那么可能是C:\WINDOWS\explorer.exe被赋予了受限权限，如下图

	Internet Explorer	自动	▼	?	?	?	?	?	?
	Windows Explorer	自定义	▼	█	?	?	?	?	?

请在 ZA 的程序控制里面，找到 Windows Explorer 并设置其信任水平为信任或者超级。会解决前面的错误提示。

实例 5: 无影无踪 (wywz.exe) 提示

这里就不贴图了，无影无踪软件由于有些操作会涉及到结束 explorer 进程，因此也有这个提示，选择允许即可。

5 清除 ZA 防火墙的痕迹

由于上网的程序在 ZA 里面都有记录，因此上网后可以按如下方法清除程序在 ZA 中留下的痕迹。

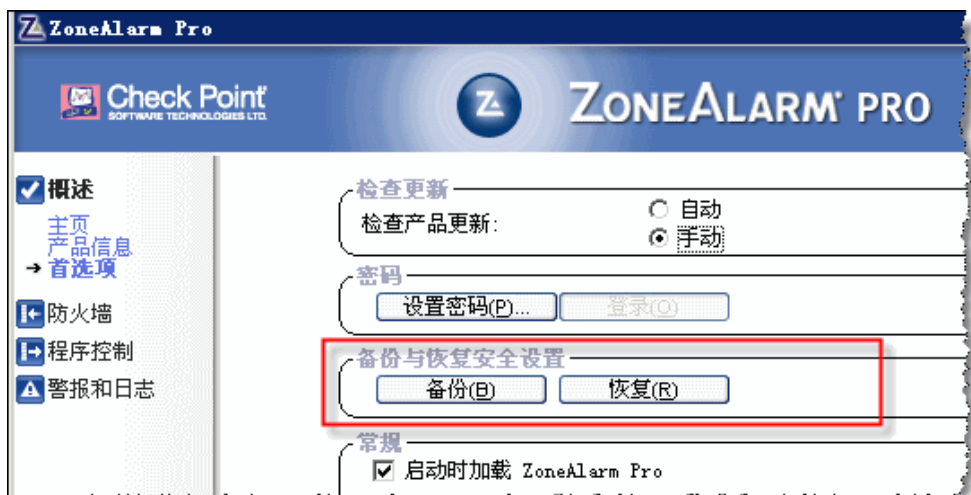
使用“备份恢复安全设置”清除痕迹（推荐）

备份步骤：打开防火墙界面，点击 **概述—首选项**，在“备份和恢复安全设置”里，点击“备份”按钮，浏览到备份文件要保存的位置，保存即可。这样就创建了一个包括程序许可的备份。

清除步骤：按照上面的步骤来到“首选项”，然后点击“恢复”按钮，浏览找到这个备份文件的位置，ZA 便会开始恢复，恢复完毕就会提示恢复成功的信息，这时就会清除所有的上网软件信息并恢复到备份时的状态。

实际操作时，就是先把没有敏感程序的配置备份出来，用完敏感程序后恢复一下即可。如果您的敏感程序很少，就一两个，也可以在程序列表里，鼠标指向敏感程序，然后单击右键，选择删除。

这种方法操作简单，也可以实现防火墙中信任区域和 Internet 区域的等设置备份恢复。ZA 的备份里面储存了系统文件的信息，如果把一台计算机上的 ZA 设置备份恢复到其它机器上，在系统文件差异较大的情况下，可能无法成功恢复。



恢复备份后，会清除程序列表中的痕迹，此外还需清除日志信息，在**警报和日志一日志查看器** 里面，通过顶部的下拉箭头可以下拉选择查看程序/防火墙/系统防火墙三种日志，选择每种类类别之后按底部的**清除列表**按钮清除日志。也可以在警报和日志界面关闭日志记录，关闭之后这些日志就不会再记录了。

手动或使用“无影无踪”清除

因为上网的程序就那几个，也好识别，在“程序控制”的“程序”栏目中找到这些程序。由于 ZA 会记录所有运行过的程序，所以最好先点一下“访问”栏目的标题排序，之后点一下第一个许可为“？”的程序，再下拉滚动条选择，之后按住 shift 键的同时，鼠标点击最后一个许可为“？”的程序，之后按 Delete 键删除，弹出对话框确认即可，接着再删除破网相关的程序。然后切换到“组件”页，鼠标点击第一行，之后用鼠标下拉滚动条至最底部，按下 shift 键的同时，鼠标点击最后一个项目，之后按 Delete 键删除（删除组件项目不影响程序的访问网络权限）。

此外无影无踪软件设置开机启动后，也可以实现对 ZA 设置的清除，但是设置稍嫌复杂，有需要的可以自行设置。

6 设置防火墙防止误连禁网（参考）

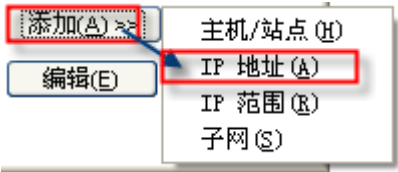
有时候，会在没有使用破网软件加密的情况下，不小心点击了禁网的连接，比如有时退出了破网软件但没有关闭打开的网页，有的网页是自动刷新的，就会发生这种情况，或者您自己忘记了已经关闭了破网软件，从而又点击了已打开网页中的禁网连接。那么如何避免这种情况的发生呢？

首先，准备 2 个浏览器，比如 IE 和火狐，一个用来平常上网，另一个用来破网访问禁网；比如假定我们平常用火狐访问普通网站，破网时用 IE 访问禁网。并且使用 FDM 破网下载。

可以这样设置防火墙，首先将 127.0.0.1 设为信任区域：

名称	IP 地址/站点	条目类型	区域 ▲
新网络	10.0.2.0/255.255.255.0	网络	Internet
127	127.0.0.1	IP 地址	信任

方法是先点 **防火墙-区域** 切换到区域页面。之后再点该页面右下角的“添加”按钮==>选择“IP 地址”



新对话框里面，“区域”选“信任”，“IP 地址”输入 127.0.0.1==>“说明”位置随意添加一些说明（例如这里输入 127）==>确定

添加 IP 地址

添加

请填写以下字段将 IP 地址添加至您的信任区域或拦截区域。请命名此 IP 地址以备日后参考，这样您就可以总是能够判断哪些是您信任的，哪些不是。

区域

信任

IP 地址

127 . 0 . 0 . 1

说明

127

确定

取消

设置 127 信任区以后，访问 127 开头的本地地址时防火墙就明确的提示访问信任区域了(如果不设置，防火墙会把 127 开头的地址提示为 Internet 区域，所以即使只设置 127 信任区也能增加一些安全性)。

接下来在程序设置的“程序”栏目里，将您用来破网的软件一律设置为禁止访问 Internet，但允许访问 127.0.0.1 信任区域。因为通过破网软件访

问禁网时浏览器是不需要直接访问 Internet 的，浏览器的连接请求都是发给 127.0.0.1 的本地破网软件端口，然后再由破网软件访问 Internet。

这样一来，即使在退出破网软件时不小心点了禁网连接，我们自己的防火墙就给挡住了，不会将连接请求发出去，从而避免了不安全的连接请求。在使用破网软件时禁止浏览器直接访问 Internet 也是一个防止 Java 等控件探测真实 IP 的方法，可以避免 java 等控件绕过破网软件直接连出去，这样设置后，即使不禁用 java，也能防住 Java 控件的探测。

以 IE 和 FDM 为例，在防火墙的程序控制里，设置程序的访问权限(关键)：

活动	程序 ▲	智能防御	信任水平	访问		服务器		邮件发送	
				信任	Internet	信任	Internet		
	Firefox	自定义 ▼	?	✓	✓	✗	✗	✗	
	Free Download Ma...	自定义 ▼	?	✓	✗	✗	✗	✗	
	Freemove, Fast and ...	自定义 ▼	?	✓	✓	✓	✓	?	
	Generic Host Proce...	自定义 ▼	?	?	?	?	✗	✗	
	Internet Explorer	自定义 ▼	?	✓	✗	✗	✗	✗	
	Microsoft Office W...	自定义 ▼	?	✗	✗	✗	✗	✗	

对于破网软件或者莲花代理等辅助软件，由于其本身要访问外部网络，请允许访问 Internet 区域。也就是说破网软件不要放在 127.0.0.1 区域。设置以后，不允许破网软件之外的任何程序访问 Internet 区域。

自由门软件设置应为： ✓ ✓ ✓ ✓ ?

莲花代理软件设置为： ✓ ✓ ✓ ✓ ?

IE 正确的设置应为： ✓ X X X X

FDM 正确的设置应为： ✓ X X X X

Generic Host Process for Win32 Services 设置应为： ? ? ? X X

Microsoft Office Word 正确的设置应为： X X X X X

其余程序除破网软件外都禁止。每个人的网络情况都不一样，有的人可能 Generic Host Process for Win32 Services 和 Windows Explorer 也要放行。（要选“？”而不要选勾，这样就可以全面控制每一步，当出现不正常情况时随时停止）这样 IE 和 FDM 就不允许直接访问 Internet，只能访问信任区域 127.0.0.1，也就是必须要走破网软件的代理，否则上不了网。

除了在防火墙里设置好程序权限之外，下载软件等列表中的程序也要设置好 127.0.0.1 破网软件代理才行。例如，需要在破网前手动设置 FDM 的代理为破网软件代理。否则无法联网。

您也可以使用前面说的备份恢复设置方法，创建两个备份，一个是没有

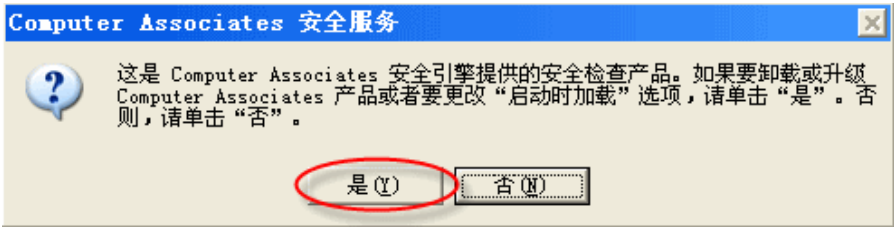
使用破网软件时的备份，一个是防止误连的备份，破网的时候恢复到破网备份，破网之后恢复到没有破网时候的备份来快速清除痕迹。

7 ZA 各版本卸载及其它（参考）

7.1~7.5 小节的内容仅在需要的时候参考，只看一下每个小节的标题就可以了，没有涉及到的时候不需要仔细看。

7.1 ZA 5.5 版本卸载

- 1) 「开始」菜单\程序\Zone Labs\Uninstall Zone Labs Security
- 2) 弹出确认提示框，点“是”



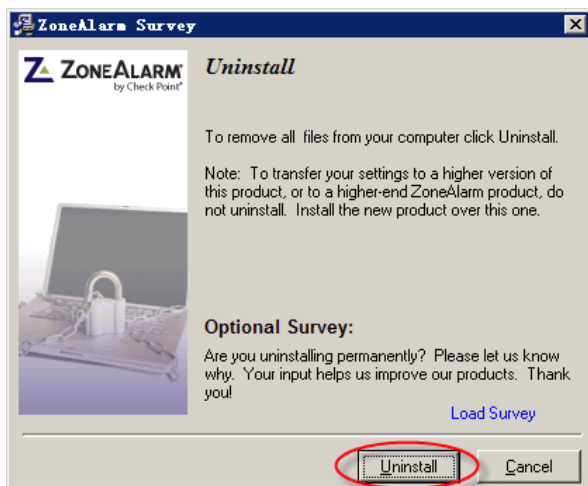
还有一种版本是 eTrust 版本，在「开始」菜单\程序\eTrust Personal Firewall 里面找 Uninstall 卸载

7.2 ZA 8.0 版本卸载（卸载必看）

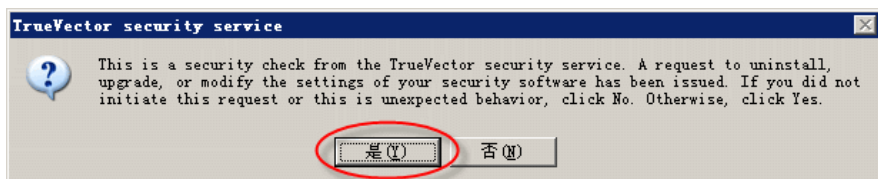
根据反馈，有的计算机在卸载 ZA8 之后出现其它软件的卸载项丢失的情况，比较可能是卸载程序的缺陷，为避免清除这些卸载项，目前只能提前备份这些卸载项，在卸载 ZA8.0 之前运行一下压缩包中的 **卸载 ZA 前执行.CMD**，会生成一个名字叫 **ZA 卸载项目备份.reg** 的文件，卸载 ZA 后，执行一下“开始—设置—控制面板—添加/删除程序”，如果发现里面的卸载项被清空了，请双击 **ZA 卸载项目备份.reg** 恢复丢失的卸载项。

具体卸载过程：

- 1) 「开始」菜单\程序\ZoneAlarm\Uninstall ZoneAlarm Security
- 2) 对话框选择“Uninstall”



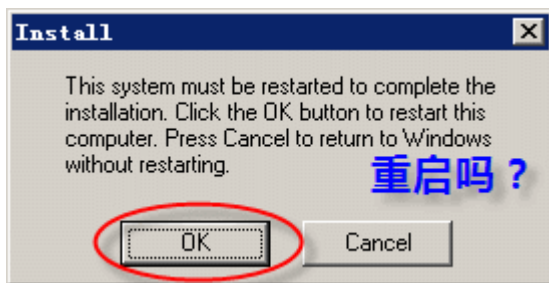
3) 再弹出对话框继续点 “是”



4) 卸载成功提示



5) 最后会提示重启，如果点 OK 按钮就重启了



7.3 关于几个精简掉的安装选项

为了减小资源占用,自动安装去掉了反间谍监控/邮件监控/id 锁定/隐私保护,安装后的内存占用大概在 20-25MB,推荐使用。尤其是老机器。根据一些反馈,推测 ZA 的主程序内置了这些功能的某些关键之处,虽然精简了这些内容,而隶属于精简项目的有些功能还在起实际作用。

反间谍模块,占资源多,界面无法汉化,有时会导致 CPU 占用异常,如果是对英文不熟悉就不要安装这个模块了,此功能和有些杀毒软件功能重合。

邮件防护,如果您使用了比较好的杀毒软件,这个功能也可以去掉。如果杀毒软件者带有邮件保护,请不要安装或安装后关闭这个模块。根据反馈,即使精简了这个模块,在收发邮件时相关的功能还在起作用。

隐私保护,包括cookie控制,广告控制和可移动代码控制。这个项目有时会影响一些破网软件的使用。隐私保护的缓存清除器采用的是非安全删除。可移动代码控制(Mobile Code Control)有时会使浏览器无法下载某些文件。在一些论坛,需要把Cookie control和Ad Blocking调到中才可以显示图片。有反馈说世界通在ZA开启隐私控制的情况下速度很慢关闭隐私保护即可。而破网时的IP泄漏和ZA的隐私保护没有必然的关联。

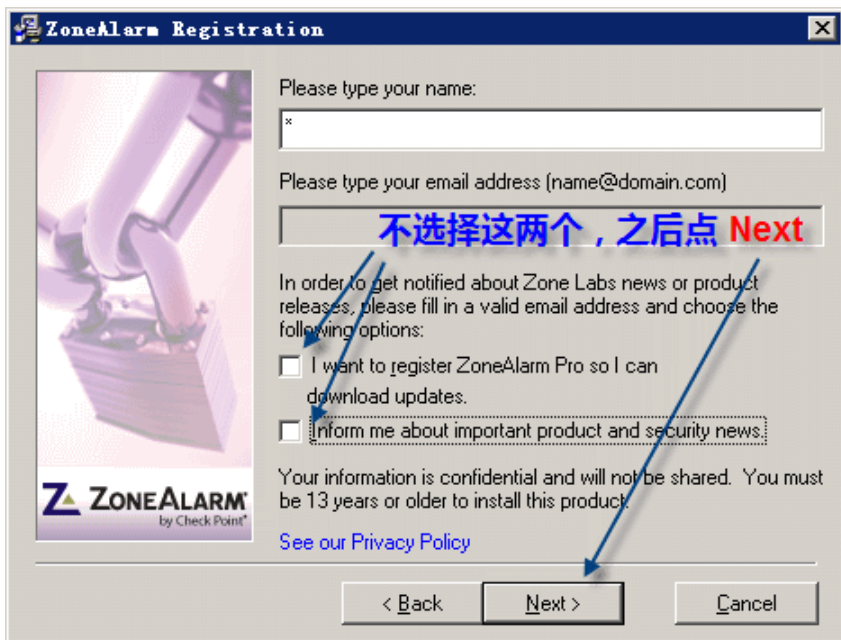
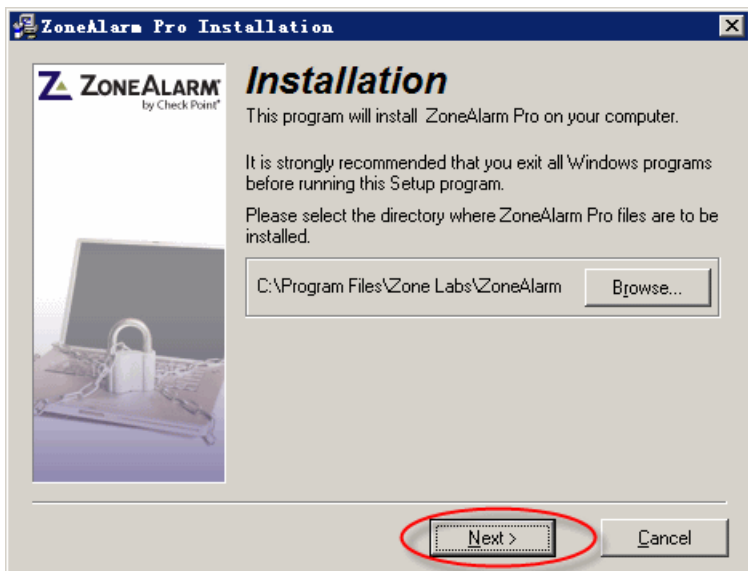
ID 锁定,多数人都是关闭的。

7.4 手动安装英文版和汉化

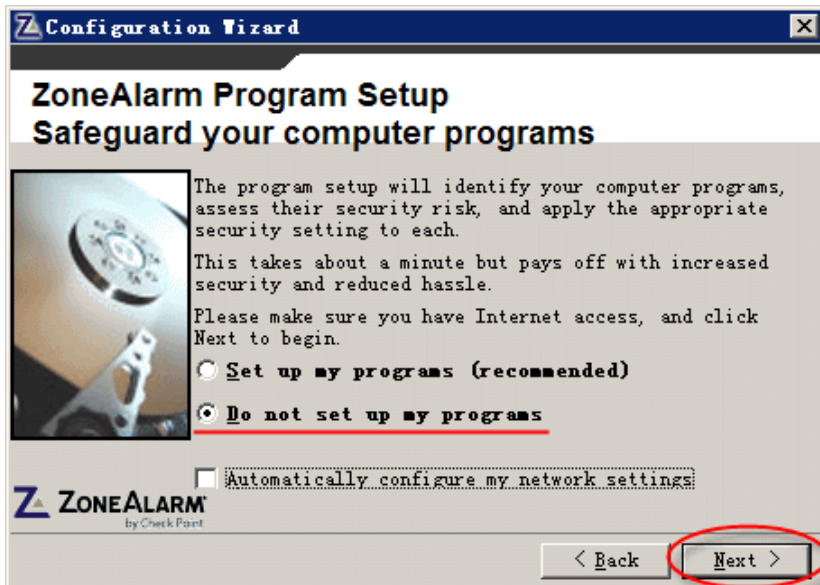
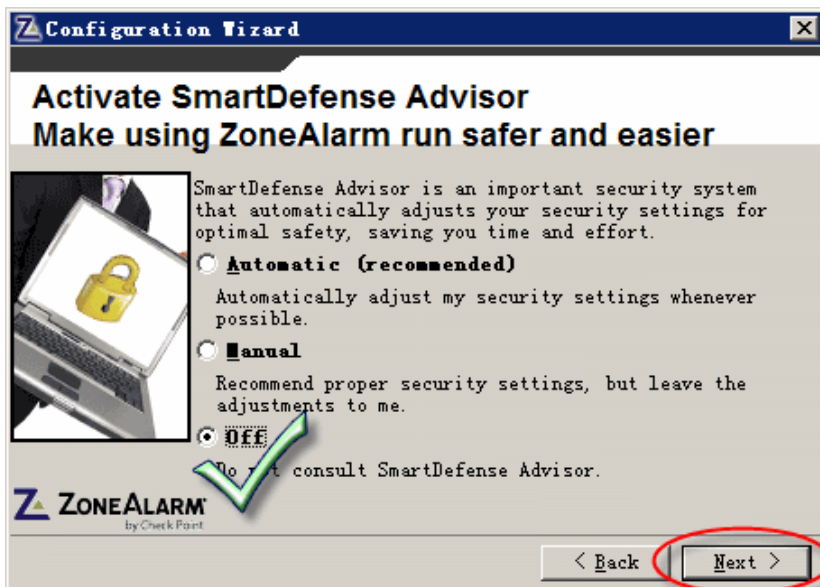
在有些机器里面,可能会出现无法自动安装的情况,这时请手动运行安装程序安装,之后执行批处理的第三个选项,只安装汉化补丁和手动输入序列号注册。步骤如下:

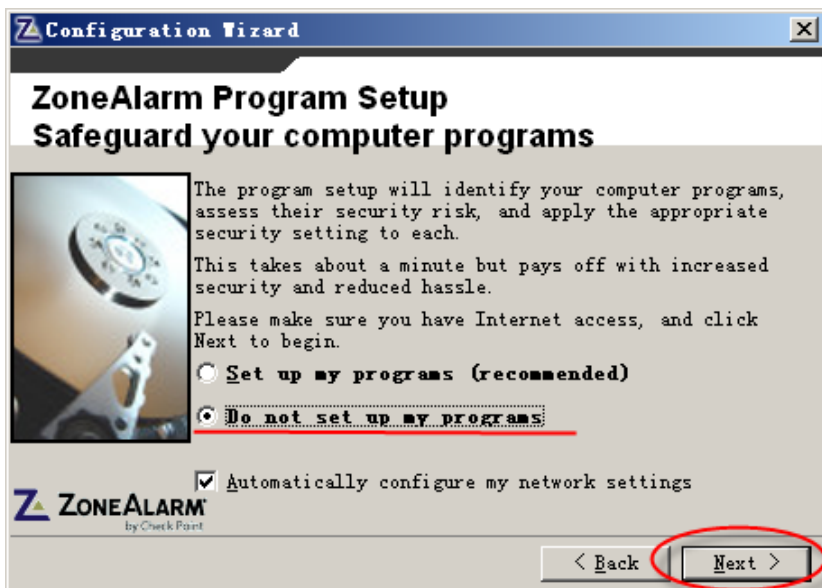
1) 安装英文原版

双击运行 zapSetup_80_059_000_en.exe 开始安装

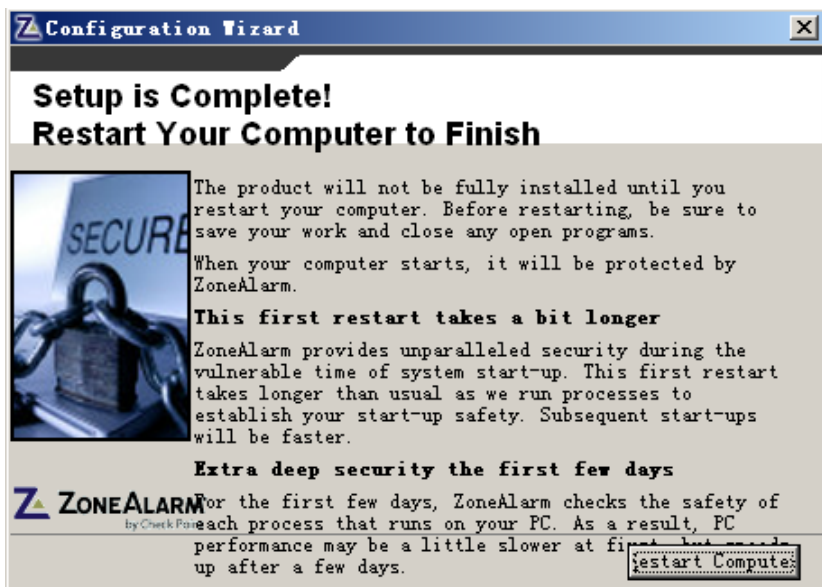








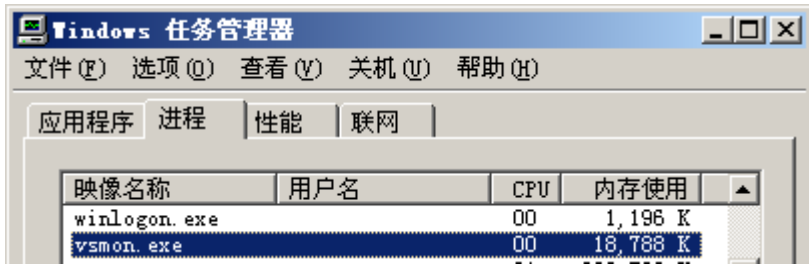
最后提示重启计算机



这个步骤中，不点任何按钮，按键盘的 Ctrl+ALT+DEL 组合键，显示任务管理器，在“应用程序”中，选择 Configuration Wizard 并选择结束任务。



之后在“进程”里找到 vsmon.exe 并按底部的“结束任务”按钮结束它。



之后开始手动复制汉化文件。

2) 手动复制汉化文件

复制压缩包中 ZoneAlarm 目录下的文件到

`C:\Program Files\Zone Labs\ZoneAlarm\`

复制 System32\Zonelabs\目录下的文件到

`C:\WINDOWS\system32\ZoneLabs\`

复制 System32\VSINIT.DLL 到下面两个位置

`C:\WINDOWS\system32\vsinit.dll`

`C:\Program Files\Zone Labs\ZoneAlarm\repair\vsinit.dll`

复制文件之后双击汉化包 System32 目录下的[中文界面设置.reg](#)，弹出对话框点“是”按钮把中文语言设置信息导入注册表。

如果是多系统，这里的 c 盘对应您当前的系统盘，例如 D/E 等

同样，对于自动安装没能成功汉化的情况，显示的是英文界面，在从新启动计算机前，执行前面操作完成汉化，如果是安装 ZA 后已经从新启动过计算机，请在开机滴的一声响过之后按键盘的【F8】键，随后在启动菜单中选择启动安全模式，之后再执行前面操作。

如果自动安装过程中计算机自动从新启动，而导致显示的界面为英文的，也可以在进入安全模式之后执行前面的手动汉化操作。

复制文件后，执行「开始」菜单\程序\ZoneAlarm\ZoneAlarm Security，就会显示 2.2 自动安装 小节最后面的几个对话框。以及启动 ZA 防火墙界面。

7.5 无法自动或手动安装的解决

如果批处理安装结束，在程序菜单中没有 ZA 的项目，说明没有安装成功，如果是 SP2 系统，请确认已经安装了前面所说的 KB943232 补丁，如果没有请手动安装这个补丁之后重启计算机，然后再执行批处理安装命令。

如果仍然无法解决问题，请尝试如下操作：

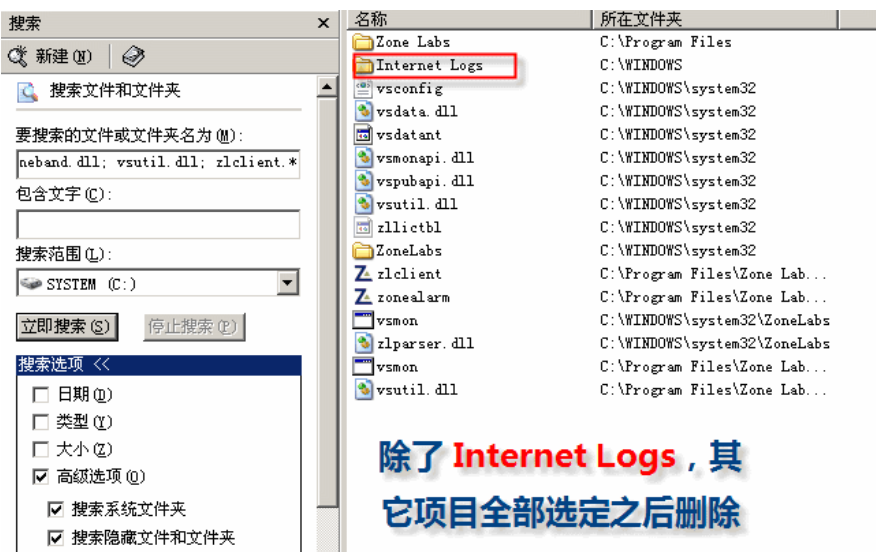
开始—搜索—有文件或文件夹，搜索范围，下拉选择系统盘（一般是 C）

选择高级选项，勾选“搜索系统文件夹”、“搜索隐藏的文件和文件夹”、“搜索子文件夹”，将下面绿色字全部复制，粘贴到搜索对话框的 要搜索的文件或文件夹名为 下面的输入框中，之后点 立即搜索

Zone labs; "zone labs"; "Internet logs"; vsconfig.xml; vsdata.dll; vsdata95.vxd; vsdatant.sys; vsmon.*; vsmonapi.dll; vsnetutils.dll; vspubapi.dll; zaplus.*; zapro.*; zllictbl.dat; zlparser.dll; zonealarm.exe; zoneband.dll; vsutil.dll; zlclient.*

删除找到的所有文件和文件夹，c:\WINDOWS\Internet Logs\里面有删除不了的，不用管。以上操作之后再尝试自动安装或者手动安装。

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



除了 Internet Logs，其它项目全部选定之后删除