

# 微点主动防御软件 2.0 使用手册

北京东方微点信息技术有限责任公司

福建东方微点信息安全有限责任公司

---

第 1 页 共 44 页

北京市海淀区蓝靛厂东路 2 号金源时代购物中心 B 区写字楼 1608 室 100097  
电话: (010)59798298-515 传真: 010-88891696

# 目录

第 1 章.	安装卸载 .....	4
1.1	适用环境 .....	4
1.2	安装 .....	4
1.3	卸载 .....	6
第 2 章.	注册激活 .....	7
2.1	注册 .....	7
2.2	查询使用时间 .....	8
第 3 章.	主界面 .....	8
3.1	普通模式 .....	9
3.2	专家模式 .....	10
3.3	系统托盘图标 .....	10
第 4 章.	设置 .....	12
4.1	常规 .....	12
4.2	扫描 .....	14
4.3	防火墙 .....	15
4.4	程序访问网络策略 .....	15
4.5	可信程序 .....	16
4.6	升级 .....	16
4.7	隔离区 .....	19
第 5 章.	防火墙 .....	21
5.1	程序访问网络策略 .....	21
5.2	防火墙 .....	22
第 6 章.	报警处理 .....	26
6.1	病毒报警 .....	26
6.2	其他报警 .....	27

---

第 7 章. 专家模式 .....	28
7.1 系统分析 .....	29
7.2 网络分析 .....	36
7.3 注册表分析 .....	38
第 8 章. 服务与支持 .....	39
8.1 生成技术支持信息 .....	39
8.2 自助服务 .....	40
8.3 在线问题反馈 .....	40
8.4 人工服务 .....	40
附录 .....	41
附录一 常见问题 .....	41

## 第1章. 安装卸载

### 1.1 适用环境

#### 1) 计算机的硬件性能要求

处理器: Intel Pentium II 450MHz

内存: 128M 以上

硬盘: 300M 以上剩余空间

#### 2) 适用的操作系统

适用于: Microsoft Windows 2000/XP/2003/2008/vista/7 32 位 (x86)

Microsoft Windows 7 64 位 (x64)

Microsoft Windows 2003 SP2 64 位 (x64)

Microsoft Windows 2008 64 位 (x64)

支持语言: 简体中文, 英文

### 1.2 安装

#### 1) 光盘安装

首先, 请将购买的本软件安装光盘取出并放入计算机光驱;

其次, 系统默认自动播放光盘动画, 出现动画界面后请选择“安装微点主动防御软件”;

最后, 弹出安装界面后, 按照安装提示信息进行操作即可完成安装。

- 【提示一】语言选择, 请根据系统具体语言环境进行相应选择;



图 1

- 【提示二】 序列号输入，请参考使用手册首页授权卡刮开信息认真填写；



图 2

- 【提示三】 产品注册，（请参看注册激活）若暂时不想对软件进行注册，可在产品注册窗口单击“取消”，继续进行软件的安装；建议立即注册本软件，以便能及时更新；
- 【提示四】 完成安装，安装完成后，需要重新启动计算机才能正常运行。在重启前，不会对系统提供安全防护，建议用户安装完成后，立即重启计算机。安装后未重新启动计算机前，请不要启动微点软件，以免发生意外现象。



图 3

## 2) 下载安装

你也可以到官方网站下载本软件安装包：

<http://www.micropoint.com.cn/download/download.php?site=localsite>

安装注意事项请参考【光盘安装】相关提示信息。

## 1.3 卸载

### 1) 微点主动防御软件提供了自动卸载的功能，操作步骤如下：

- 【第一步】单击【开始】->【程序】->【Micropoint】->【卸载微点主动防御软件】，打开【欢迎使用微点主动防御软件卸载向导】（如下图）；



图 4

- 【第二步】单击【下一步】，卸载程序将自动停止软件服务，并卸载与本软件有关的所有程序文件，如下图所示；



图 5

- 【第三步】卸载完成，本软件提示（如下图）“卸载本程序需重启，是否现在重启？”，单击“是”，重新启动计算机，即可完全卸载本软件。



图 6

- 2) 卸载程序，也可以使用 Windows XP 控制面板中的“添加/删除程序”选项，或者 Windows Vista 或 Windows 7 控制面板中的“卸载程序”选项。

## 第2章. 注册激活

### 2.1 注册

请在线注册本软件，注册后可以进行软件的升级。

- 【第一步】注册前请检查网络，确保你的计算机已经连接到互联网上；
- 【第二步】详细阅读【产品注册】详细信息区中提示信息，依据提示信息，正确输入各项内容（如下图）；

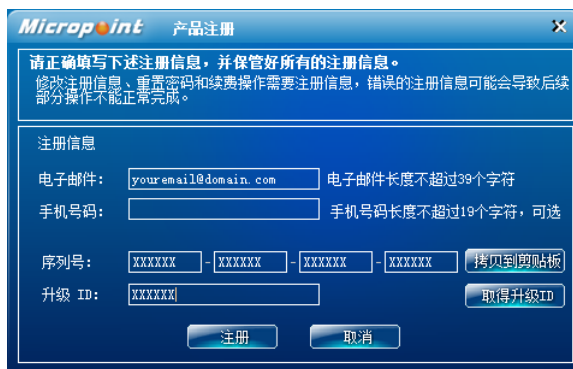


图 7

- 【第三步】信息输入完成后，单击“注册”，请等待东方微点注册服务器返回信息；



图 8

- 【第四步】单击“确认”按钮，微点主动防御软件提示如下图，表示软件已经成功注册。



图 9

微点提示：请妥善保存你注册时输入的电子邮件、手机号码、序列号、升级 ID 等信息，便于你以后重新安装本软件注册使用。

## 2.2 查询使用时间

打开微点主动防御软件主界面，查看右下角服务信息位置，显示软件的剩余使用时间。

## 第3章. 主界面

微点主动防御软件针对不同需求的用户提供了两种管理模式主界面，便于用户管理、设置监控模式、查看栏



截日志，甚至进一步分析和判断系统的安全性。

### 3.1 普通模式

普通模式，即适用于广大普通计算机用户的管理模式，本模式下无需用户操控，实时动态显示用户计算机上的安全事件及所有软件运行、网络访问、资源占用情况。结构及名称如下图：



图 10

1) 【①工具栏】 — 为用户提供常用功能的快捷按钮如下图：



图 11

- 可信：协助用户手工添加可信任的程序，详细请参阅第 4.5 的【可信程序】。
- 隔离区：快捷打开病毒隔离区窗口。详细设置请参阅 4.7【隔离区】。
- 日志：快捷打开日志窗口，便于用户查看当前安全报告。
- 设置：快捷打开设置窗口。详细请参阅第 4【设置】。

2) 【②安全状况统计】 — 为方便用户了解当前计算机的安全状况：

- 主动防御安全报告：动态实时显示用户当前计算机所发生的安全事件。
  - 监控和分析正在运行的软件：系统当前进程自动分类显示，便于用户掌握系统上软件运行情况。
  - 监控和分析本机所有的网络连接：实时详细报告系统中所有正在运行进程的访问网络情况，方便用户掌握系统上网络访问情况。
- 3) 【③状态栏】 — 显示微点主动防御软件当前版本号及更新时间。
  - 4) 【④服务信息】 — 显示微点主动防御软件产品类型、剩余使用时间、修改注册信息服务、升级服务、续订/订购服务。
  - 5) 【⑤系统性能】 — 显示微点主动防御软件资源占用及操作系统资源占用情况。
  - 6) 【⑥界面模式切换按钮】 — 用于进行主界面模式切换的按钮，两种模式：普通模式（默认）、专家模式（详细信息请参阅第 7【专家模式】）。
  - 7) 【⑦帮助】 — 显示微点主动防御软件帮助、关于等信息。
    - 密码设置：设置主界面管理密码，防止其他用户未经本人允许修改本地计算机上微点的设置。
    - 换肤：主界面更换皮肤，目前提供四种界面方案：蓝色畅想、哈勃星空、暗夜星空、碧雨幽兰。
    - 导入导出设置：方便用户备份和导入对微点所做的各种设置，用户可根据需要自定义导出内容。
    - 生成技术支持信息：提取与问题有关系的系统信息，并自动压缩成一个报告文档，便于用户查看及上报微点工程师分析。
    - 帮助：查看微点软件帮助文档。
    - 关于：查看微点软件版本信息。

## 3.2 专家模式






专家模式，即适用于计算机爱好者、专业工程师、计算机相关行业从业人员用户的管理模式，本模式下用户可通过软件提供的各种安全辅助工具，手动分析系统整体运行情况，排除潜在的安全隐患，甚至解决在使用计算机过程中所遇到的各种问题，详细信息请参阅第 7【专家模式】。

## 3.3 系统托盘图标

微点主动防御软件启动后，会在系统托盘处显示微点主动防御软件的图标，托盘图标的不同状态表示微点主动防御软件不同的监控状态。

### 1) 系统托盘图标

 — 监控状态：正在监控系统中的进程。

-  — 暂停状态：已暂时停止实时监控，在此状态下微点主动防御软件不对系统提供防护功能。
-  — 报警状态（红色图标）：监测到系统中有害程序或可疑程序。
-  — 过期状态（灰色图标）：软件已经过期。
-  — 正在升级（红色闪动箭头）：正在进行升级。
-  — 升级完成（绿色闪动箭头）：升级完成，正在退出升级程序。

## 2) 右键菜单

另外，为了方便用户的操作，微点主动软件在系统托盘处提供了丰富的右键操作功能。

鼠标右键单击系统托盘处的图标，打开右键菜单，如下图：



图 12

- **【启动/暂停】** — 打开或暂时关闭微点主动防御软件监控。
- **【启动/停止防火墙】** — 启动或停止防火墙功能。默认情况下，不开启防火墙功能。
- **【注册】** — 打开“注册”窗口。详细参阅 2.1 **【注册】**。
- **【升级】** — 单击后立即升级。
- **【续费】** — 打开续费窗口。
- **【报警信息】** — 显示计算机本次启动后的报警信息记录。窗口内的信息将在关机时自动清除。如下图：



图 13

- 【主界面】— 打开应用程序的主界面。
- 【访问微点主页】— 单击进入微点公司官方网站。
- 【退出】— 关闭微点主动防御软件，退出后微点主动防御软件不再对系统提供安全保护。

## 第4章. 设置

普通用户无需做特殊设置，直接使用默认设置即可。如有特殊需求，可参考如下设置项进行设置。

### 4.1 常规



图 14

### 1) 安全防护级别

微点主动防御软件安全防护级别包含标准和增强，个人版用户推荐采用“增强”设置，以保证您的上网安全。

### 2) 发现木马/病毒后的处理方式

在发现木马、病毒时有三种处理方式：询问后处理、自动处理、采用静默方式，默认选项是“询问后处理”。

- 询问后处理：发现木马、病毒，弹出警示框提示用户，并由用户选择处理方式。弹出窗口按照预先设定的“询问等待时间”保留一定的显示时间，以使用户查看报警窗口的信息。
- 询问等待时间：指警示框的显示时间。默认是 48 秒，用户可自己定制 10-300 秒内的任意时间值；然后单击“应用”按钮，即可完成设置。
- 自动处理：发现木马、病毒，自动拦截危害行为并根据用户选择的处理方式进行处理，同时弹出警示框提示用户；处理方式包含忽略和自动清除。
- 采用静默方式：发现木马、病毒，自动拦截危害行为并删除程序文件到隔离区中，不弹出警示框提示用户。
- 清除失败后的处理方式：病毒清除失败后的处理方式，包含忽略和删除。
- 对截获的未知木马/病毒样本：对于确认删除的未知病毒样本，微点主动防御软件提供三种处理方式：自动传送、智能询问处理、不传送，默认的处理方式是“自动传送”。
  - 自动传送 — 即自动将捕获到的未知病毒样本提交给微点公司。
  - 智能询问处理 — 捕获到未知病毒时，弹出信息提示框，询问用户是否将样本提交给微点公司。
  - 不传送 — 不发送未知病毒样本到微点公司。
- 报警声音：发现木马、病毒时是否播放报警声音提示。

### 3) 附加功能

- 启用 U 盘扫描功能

即当插入 U 盘等移动存储设备时，自动检测移动设备接入并提示是否进行病毒扫描。

- 显示启动界面

微点主动防御软件在每次启动时，会弹出一个动态启动界面，提示用户已经启动微点主动防御软件，用户可根据情况自行选择启动时是否显示该启动界面。

- 启用手动扫描功能



即在微点主动防御软件主界面工具栏，显示手动扫描快捷按钮；启用后可以直接在微点主界面通过快捷按钮方式打开扫描窗口，手动选择整个硬盘或指定路径进行扫描杀毒。

- 显示动态托盘图标

即在系统托盘区，以动态方式（黄球循环滚动）显示微点主动防御软件的托盘图标。若取消此勾选，则以静态方式显示微点主动防御软件的托盘图标，用户可自行选择是否显示动态托盘图标。

- 防篡改系统时间

即保护系统时间不被修改。启动“防篡改系统时间”后，则禁止对系统时间进行修改设置。默认状态下，不启用此功能，用户可根据需要选择是否启用。

- 全屏免打扰模式

即启用全屏免打扰模式后，当您运行游戏、视频或其他程序的全屏操作时，微点主动防御软件会自动屏蔽报警及提示信息，升级延后处理。

## 4.2 扫描

基于特征码扫描技术并结合虚拟机、启发式技术，通过手动选择操作的方式，可由用户指定对特定盘符、文件夹、文件进行病毒扫描检测。



图 15

- 1) 扫描的文件类型：选择要扫描的文件类型，默认扫描所有文件。

- 所有文件：扫描所有文件。
  - 程序文件：只扫描程序文件。
  - 自定义类型：自定义要扫描的扩展名文件类型，点击右边的“设置”按钮，打开“自定义扩展名”窗口，默认设置只扫描易被病毒感染的常见文件类型，您可以点击“添加”或“删除”按钮增加或者删除文件扩展名：
    - 【添加】：添加要扫描的扩展名。
    - 【删除】：删除文件扩展名列表中的扩展名。
    - 【默认】：恢复默认设置的自定义扩展名。
- 2) **高级设置：默认启用虚拟机扫描、开启一般启发、扫描压缩文件。**
- 启用虚拟机扫描：启用虚拟机扫描可以提高对木马、病毒的检测，单击右侧的“设置”按钮可以设置虚拟机扫描超时长度，默认超时时间为 30 秒，超时后自动跳过执行下一个文件的扫描。您可以根据需求在 1 秒到 60 秒这个时间段进行更改。
  - 启用启发式扫描：即启用启发式扫描技术进行扫描，启发式扫描技术是一种可以提高木马、病毒检测率的反病毒技术。启发式扫描包含一般启发和高度启发，单击右侧的“设置”按钮进行设置，默认开启一般启发，对安全要求较高的用户可开启高度启发。
  - 扫描压缩文件：对压缩文件进行扫描。单击右侧的“设置”按钮，可以对压缩文件的扫描深度及压缩文件大小进行设置，默认压缩文件扫描深度是 5 层，压缩文件大小不限制。
- 3) **发现病毒处理方式：**
- 完成后提示：即扫描任务完成后，在扫描列表中显示检测到的病毒木马。由用户选择是否处理。您可以在扫描列表中单击右键菜单或者选择扫描窗口中的按钮进行处理。
  - 自动处理：自动处理包含“自动清除”和“如果清除失败则删除”。
- 4) **恢复默认设置：恢复默认设置即恢复到初始设置。**

## 4.3 防火墙

详细请参阅第 5.2 的【防火墙】。

## 4.4 程序访问网络策略

详细请参阅第 5.1 的【程序访问网络策略】。

## 4.5 可信程序

可信程序是由用户自己认可的一切可信任的程序文件，可信程序由用户自己添加。对于添加到“可信程序”列表中的程序文件，微点主动防御软件对其以可信模式监控。【可信程序】窗口，如下图：



图 16

【可信程序】的操作包含：添加、删除。

### 1) 添加策略

在【可信程序】窗口中，单击“添加”按钮，或单击鼠标右键选择“添加策略”，选择要添加为可信程序的程序文件，选定后单击“打开”完成可信程序的添加。

### 2) 删除策略

在【可信程序】窗口中，选中要删除的可信程序，单击“删除”按钮或单击右键菜单中的“删除策略”，则删除选中的可信程序。

单击右键菜单中“全部删除”，删除列表中所有的可信程序。

## 4.6 升级

微点主动防御软件的升级包含特征库的升级和程序升级。请您及时升级以便微点主动防御软件能够给您更安全的防护。

- 特征库的升级是对病毒特征库的升级。



- 程序升级是对微点主动防御软件程序文件的升级。

单击【设置】中的【升级】，打开升级设置标签页，如下图所示：



图 17

如图显示的是默认的升级设置方式，普通用户可直接采用默认的设置方式进行升级，无须更改。

## 1) 升级方式

微点主动防御软件提供了如下三种升级方式供用户选择：

- 自动实时升级

默认的升级方式，启用“自动实时升级”，在网络连接正常的情况下，微点主动防御软件直接连接到东方微点网站自动下载升级数据，并自动升级。微点公司建议用户采用“自动实时升级”方式实时对微点软件进行更新，更好的对您的系统安全提供防护。

- 定时升级

指在设定的时间间隔内，定时对微点主动防御软件进行升级，微点主动防御软件默认定时升级时间的时间间隔是 14 天，用户可自行修改定时升级时间间隔，微点主动防御软件将在你设定的时间间隔里自动下载升级文件，并自动升级。

- 手动升级

手动升级即关闭微点主动防御软件的自动升级功能。设置手动升级后，需要升级微点主动防御软件的时候可单击主界面右下角服务信息区的“立即升级”按钮或系统托盘微点图标右键菜单中的“升级”进行

升级。

## 2) 代理服务器设置

用户若采用代理服务器的方式进行升级，就需要设置代理服务器，详情可咨询你的上网服务提供商或网络管理员。

- 使用系统代理设置

系统代理是指当前系统正在使用的代理（一般是 Internet Explorer 正在使用的代理地址），单击右边的“使用系统代理设置”，软件会自动提取系统代理相关设置信息，无需用户手工输入，单击“应用按钮”完成系统代理设置。

- 手动设置代理服务器

当用户使用特定的代理服务器时，在代理服务器选项中，选择代理类型（Sock4、Sock5、HTTP），然后对代理服务器的相关参数进行设置：

- 【代理服务器地址】 — 代理服务器的 IP 地址。
- 【端口】 — 代理服务器提供的代理服务的端口号（0—65535）。
- 【用户名】 — 访问代理服务器的用户名。
- 【密码】 — 访问代理服务器的密码。
- 【域】 — 代理服务器的域名，如 micropoint.com。

- 测试代理服务器

代理服务器设置完毕，请单击“测试代理连接”按钮测试你设置的代理服务器是否能够正常使用。

## 3) 使用默认

单击“使用默认”按钮，自动恢复升级设置为默认设置。

## 4) 高级设置

单击“高级”按钮，打开如下图。

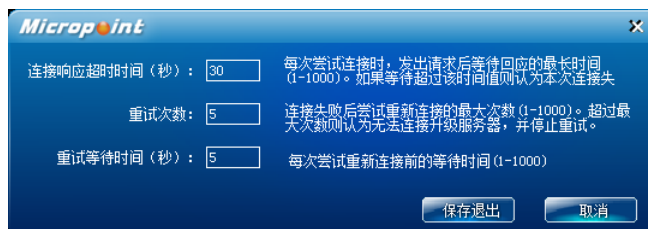


图 18

在“高级”设置窗口中包含的信息：连接响应超时时间、重试次数、重试等待时间，用户可根据实际情况进行修改。

## 4.7 隔离区

微点主动防御软件对于确认删除的木马、病毒直接将其删除到微点主动防御软件的【隔离区】，放置在【隔离区】中的文件都经过特殊格式保存，不会对系统造成任何影响。用户可以对隔离区的文件进行备份、恢复、删除以及样本上报等管理。单击主界面【工具栏】“隔离区”按钮打开隔离区如下图。

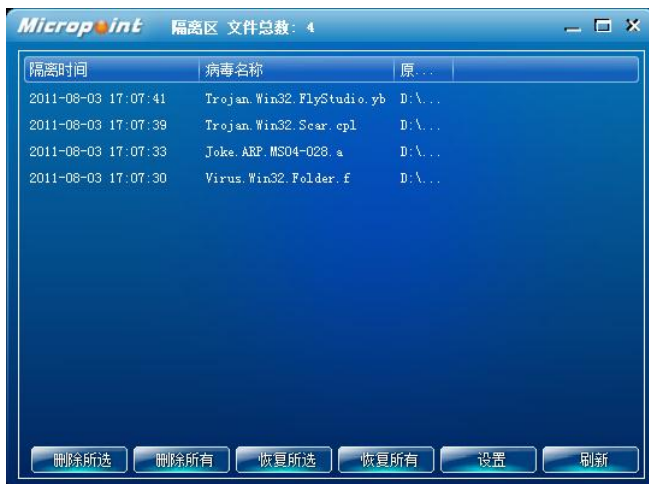


图 19

### 1) 隔离区文件管理

- 恢复所选 — 将隔离区列表中选定的文件恢复到原目录。
- 全部恢复 — 将隔离区列表中的所有隔离文件全部恢复到原目录。
- 删除所选 — 将选定的隔离文件从隔离区列表中彻底删除。
- 全部删除 — 彻底删除当前隔离区列表中的所有隔离文件。
- 上报样本 — 将隔离区列表中的病毒文件上报给东方微点公司。
- 另存为 — 将隔离区信息列表中的选定的文件另存到指定目录。
- 设置 — 设置隔离区空间的大小以及隔离区的存储路径。

### 2) 隔离区设置

隔离区详细信息区右键菜单选择“设置”，打开如下图设置窗口。



图 20

- 隔离区存储路径:

单击“浏览”按钮，在磁盘中选择隔离文件的存储位置。

- 隔离区尺寸设置

- 自动调整隔离区大小

默认的设置方式，即隔离文件可存储在磁盘自由使用区内，隔离区空间的大小只跟磁盘的自由使用区的大小有关。

- 限定隔离区大小

即对隔离区的大小作限制，隔离文件只能存储在限定的空间中，拖动隔离区尺寸设置图中的分割线来设置隔离区、自由使用区、分区保留区的大小。

- 【隔离区】— 用来存储被隔离病毒的空间。
- 【自由使用区】— 用于扩充隔离区的使用空间。
- 【分区保留区】— 磁盘保留的空间。
- 【当前分区空闲空间】— 隔离区所在的磁盘分区的剩余空间。

### 3) 保存设置

单击“应用”按钮，保存对隔离区更改设置。

**微点提示：**当隔离区内各文件字节之和超过隔离区空间后，微点会自动删除最早的隔离文件，放入新的隔离文件。

## 第5章. 防火墙

### 5.1 程序访问网络策略

【程序访问网络策略】是对系统中试图访问网络的进程设置访问网络规则，保证系统的网络安全。



图 21

【程序访问网络策略】信息区的操作包含：添加、修改、删除。

#### 1) 添加策略

- 【第一步】进程选择：单击“添加”按钮，在系统中选择要添加的应用程序。
- 【第二步】设置规则：添加应用程序后，单击“打开”，设置程序的访问网络规则，如下图。



图 22

- 允许访问网络 — 允许所选程序访问网络；
  - 禁止访问网络 — 禁止所选程序访问网络；
  - 访问网络时询问 — 所选程序发生访问网络行为时，弹出警示框提示用户是否允许访问网络。
- 【第三步】单击“确定”，完成程序规则的添加。

## 2) 修改策略

在程序规则信息区中，选择要修改的规则，直接单击“修改”按钮或单击右键菜单中的“修改策略”，则弹出【修改程序规则】对话框修改新的规则，然后单击“确定”，修改完成。

## 3) 删除策略

在程序规则信息区中，选择要删除的规则，直接单击“删除”按钮或单击右键菜单中的“删除策略”，删除所选策略。

单击右键菜单中的“全部删除”，删除列表中的所有策略。

## 4) 启用智能防火墙

通过微点主动防御软件的动态仿真反病毒专家系统能够自动处理系统中可识别程序的访问网络行为，不需要用户参与。可识别程序包括：可信程序、已知程序（包括微点识别的系统程序和正常应用软件程序）。

勾选“启用智能防火墙”后，只对非可识别程序的访问网络行为弹出报警框询问用户，可识别程序访问网络行为将直接放行，减少了用户自行判断的烦恼。默认设置开启此功能。若取消，则系统中任意进程访问网络时，微点主动防御软件都会弹出报警框询问用户。

## 5.2 防火墙

提供传统包过滤防火墙功能，可自定义协议、端口、本地地址、远端地址、处理操作等规则，实现对网络数据包的监控拦截设置。



图 23

## 1) 规则设置功能

- 防火墙默认规则包

微点主动防御软件提供了五个规则包供用户选择，用户可以根据实际使用环境选择不同的规则包，传统防火墙默认使用的规则包为：规则包（一）。为了确保用户安全，微点主动防御软件提供的五个默认规则包不允许进行任何更改。用户可以根据自己的需要，自行编辑定义新规则包，也可以采用另存方式，在提供的默认规则包的基础上编辑自己的防火墙规则策略。


- 规则包一：开放网络，不对进出数据包做任何限制。
- 规则包二：禁止网络，禁止任何数据包进出。
- 规则包三：开放本机连接共享，适用于局域网内部用户。
- 规则包四：普通用户规则。
- 规则包五：关闭本机连接共享，适用于使用互联网的用户。

- 防火墙规则包使用

- 新建规则包：在“规则包列表”中，单击右键菜单中的“新建”，打开的窗口中输入规则包名称及描述信息，单击“确定”，则新建一个空的规则包。
- 应用规则包：在“规则包列表”中，选择要应用的规则包，单击右键菜单中的“应用”，或者直接单击快捷应用列表的规则包，此时提示“设置成功”的对话框，表示应用新规则包成功。



图 24

- 导入规则包：在“规则包列表”中，单击右键菜单中的“导入”，导入防火墙规则包。
- 导出规则包：在“规则包列表”中，选择要导出的规则包，单击按钮将当前规则包导出到指定的磁盘目录，规则包的文件类型为.rpk。
- 另存规则包：在“规则包列表”中，选定规则包后，单击右键菜单中的“另存”则可将已存在的规则包重命名后作为一个新的规则包加到“规则包列表”中，当需要对默认规则包进行重新编辑修改时，可使用此设置。
- 修改规则包：在“规则包列表”中选中要更改的规则包后，双击或单击右键菜单中的“修改”，打开规则包的编辑窗口，可对规则包的各项规则进行修改。

**微点提醒：** 微点的默认规则包不允许进行编辑修改，用户可以采用“另存”规则包后，对其进行更改。

- 删除规则包：在“规则包列表”中选中自定义的规则包后，选择右键菜单中的“删除”，将选定的规则包从规则包列表中删除。
- 编辑防火墙规则包策略
 

双击“规则包列表”中的规则包名称，打开“编辑规则包”窗口进行编辑。
- 更改描述信息
 

单击“编辑规则包”窗口中的“描述”按钮，打开“规则包描述”对话框，修改描述信息。
- 新建规则
 

单击右键菜单中的“新建策略”在弹出的“地址规则”窗口中设定。

  - 【第一步】填写规则名称及其描述信息。
  - 【第二步】设置规则的条件：选择规则的数据包的协议类型：TCP、UDP、IGMP、ICMP、IP。
  - 【第三步】选择规则对哪个方向的数据包有效：发送、接收、双向。
  - 【第四步】设置端口和地址。
  - 【第五步】设置对规则的处理：拦截和放行。
    - 【拦截】 — 阻止该数据包进入您的计算机。
    - 【放行】 — 允许该数据包进入您的计算机。




■ **【第六步】** 设置对规则的动作：记日志和报警。

➢ **【记日志】** — 若勾选该项，则记录拦截或放行的数据包的信息到**【传统防火墙日志】**中。

➢ **【报警】** — 若勾选该项，则会记录拦截或放行的数据包进出您的计算机时的信息，详细信息请参阅第 7.2.3 **【传统防火墙信息】**。

● 导入规则策略

单击右键菜单中的“导入策略”，从微点主动防御软件提供的默认规则库中移入要导入的规则，单击按钮，按“确定”保存此设置，将规则导入到自定义规则列表中。

微点主动防御软件对应用程序访问不同地址和端口设置了两条特殊规则即：允许可识别程序通过（TCP）、允许可识别程序通过（UDP）。可识别程序是指：可信程序、已知程序、以及“程序访问网络策略”中允许访问网络的应用程序。为了减少用户对网络访问报警处理的参与，可识别程序的网络访问将被全部允许，不受后面其他规则对端口、协议及访问地址的限制。

**微点建议：在您创建自己的规则包时，建议您至少导入“允许可识别程序通过（TCP）”和“允许可识别程序通过（UDP）”两条规则。**

● 修改规则策略

单击右键菜单中的“修改策略”，对所选策略进行修改。

● 调整规则优先级

单击右键菜单中的“上移”将提高选中规则的优先级，单击“下移”将降级选中规则的优先级。

● 删除规则策略

选择要删除的规则策略后，单击右键菜单中“删除策略”，将所选策略删除。

● 保存规则包策略

设置完规则包策略后，单击“保存”按钮，保存对当前规则包的编辑修改。

● 取消对规则包策略的更改

单击“取消”按钮，则放弃对当前规则包所做的修改。

2) **恢复默认设置**

单击“恢复默认设置”按钮，则恢复到防火墙的初始设置。

3) **绑定 MAC 地址**

绑定 MAC 地址的功能，通过将 IP 地址与 MAC 地址绑定，防御局域网内的 arp 欺骗。单击“绑定 MAC 地址”

按钮，打开如下图：



图 25

- 启用 IP 与 MAC 地址的绑定

单击“刷新网关”和“查找所有主机”搜寻局域网内的其他机器的 IP 地址以及其对应的 MAC 地址的列表，单击中间的方向按钮，将其移动到左边的列表，勾选“启用绑定”，单击“应用”按钮，实现对左边列表中的 IP 与 MAC 地址的绑定。

您也可以在两边的列表中，单击右键菜单中的“添加”，手工添加要绑定的 IP 地址和 MAC 地址，进行绑定。或者单击右键菜单中的“修改”或“删除”，对列表中的信息进行更改和删除操作。

## 第6章. 报警处理

微点主动防御软件依据程序行为判断为主、特征判断为辅，自主发现有害程序，明确报出有害程序所属类型，并自动清除有害程序。报警处理是提供给用户的一种交互模式，微点主动防御软件实时监控系统，发现存在危害行为的有害程序，弹出警示信息窗口，提示用户发现有害程序，并由用户选择处理方式，详细设置请参阅第 4.1 【发现木马病毒后的处理方式】。

### 6.1 病毒报警

警示信息依据发现木马病毒的技术原理不同分为以下类别：

#### 1) 【已知木马/病毒报警】

- 原理 — 采用传统特征防御，通过病毒特征库检测已知木马、病毒。
- 处理 — 建议直接选择删除处理。

#### 2) 【未知木马/病毒报警】

- 原理 — 依据程序行为判断未知木马、病毒。

- 处理 —
  - **【删除】** — 将该程序及生成文件删除到**【隔离区】**，提取该程序的特征，下次直接采用特征防御。
  - **【不删除】** — 结束该程序的运行，不删除程序文件。如果该程序再次运行，将会再次报警。
  - **【不删除+添加为可信程序】** — 结束该程序的运行，并将该程序加入到**【可信程序】**。
- 3) **【网页挂马报警】**
  - 原理 — 结合浏览器的溢出行为与特征判断所浏览网页是否包含恶意代码。
  - 处理 — 单击确定。自动拦截恶意代码执行。
- 4) **【漏洞溢出攻击报警】**
  - 原理 — 防御黑客利用系统已知或零日漏洞远程攻击本地计算机。
  - 处理 — 单击确定。自动阻止远程溢出攻击。
- 5) **【网络入侵报警】**
  - 原理 — 自动提取远程网络攻击数据包的特征，阻止黑客下一次攻击。
  - 处理 — 建议勾选“下次不再显示”，单击确认。遇到同类攻击，自动后台阻止，不再提示。

## 6.2 其他报警

- 1) **【异常网络访问报警】**
  - 原理 — 应用程序未经许可的网络访问行为拦截。
  - 处理 —
    - **【放行】** — 允许该进程的本次网络访问行为，若再次访问网络，会再次弹出报警。
    - **【拒绝】** — 禁止该进程的本次网络访问行为，若再次访问网络，会再次弹出报警。
    - **【放行+本次的询问结果永远有效】** — 永远允许该进程访问网络，并添加允许策略到**【程序访问网络策略】**中。
    - **【拒绝+本次的询问结果永远有效】** — 永远禁止该进程访问网络，并添加禁止策略到**【程序访问网络策略】**中。
- 2) **【可疑程序报警】**
  - 原理 — 已超越正常软件行为，但还未满足木马、病毒行为程序的拦截。
  - 处理 — 建议选择阻止。
- 3) **【注册表保护报警】**

- 原理 — 在注册表修复里面已设置被保护的注册表项，被程序或人为修改的拦截。
  - 处理 — 建议选择阻止。阻止当前进程对注册表项的修改。
- 4) **【远程安装程序的报警】**
- 原理 — 来自其他计算机向本计算机系统远程安装程序行为拦截。
  - 处理 — 建议选择阻止。
    - **【阻止】** — 阻止远程安装程序的运行。
    - **【放行】** — 允许远程安装程序的运行。
- 5) **【未知病毒命名更新】**
- 原理 — 对于微点主动防御软件自动捕获的未知病毒，微点公司获取样本后将对该程序命名，并通过升级方式更新已知病毒特征库。升级后将自动对安全日志的相关记录进行更新。
  - 处理 — 单击确认即可。

## 第7章. 专家模式

微点主动防御软件为高级用户提供了详细了解与分析系统所有进程运行状态的工具，主要包括**【系统分析】**、**【网络分析】**和**【注册表分析】**三大分析工具，用户通过分析工具提供的信息，可以详细了解进程的运行状态、启动模式、程序生成时间，以及生成关系、进程与模块的关系、进程的网络访问等信息，用户可通过分析这些信息直观掌握当前系统中进程的运行状态，能够自行分析判断系统的安全性。专家模式如下图。



图 26

## 7.1 系统分析

【系统分析】提供了【进程综合信息】、【系统自启动信息】、【模块/进程】、【系统信息】四种进程分析工具，系统分析工具是对系统中当前所有进程的运行状况、程序及进程信息、进程启动模式、进程与模块的关系、进程网络连接状态等信息全面分析的工具，是用户学习系统知识的工具。

### 7.1.1 进程综合信息

【进程综合信息】对系统当前进程进行分类管理，显示进程的网络连接情况、端口信息、网络流量、以及每个进程的本地路径等详细信息，并显示相应进程所调用的模块信息。

通过查看【进程综合信息】用户可以了解系统当前进程的运行状况，并可自行分析判断系统中的可疑进程。

进程综合信息主要包含三个区域：①进程列表区、②进程详细信息区、③模块信息区，如下图：



图 27


- ①进程列表区是以树状索引结构根据进程的不同类别分类显示系统中当前运行的所有进程。
- ②进程详细信息区显示系统中当前运行进程的详细信息。
- ③模块信息区显示进程列表区中的进程所调用的模块的详细信息。



### 1) 进程分类

根据微点的程序识别将系统中的进程划分为四大类：其他软件、可信程序、Windows 系统软件、应用软件。

- 其他软件 — 微点主动防御软件不能准确判定为正常程序或有害程序的进程，这些进程包含用户安装的某些行业性软件、可疑进程。
- 可信程序 — 用户自己认可并添加到【可信程序】列表中的进程。
- Windows 系统软件 — 所有正在运行的 Windows 系统进程。
- 应用软件 — 显示当前系统中正在运行的应用软件的进程。根据软件的特点微点主动防御软件将其规划为八类：系统软件、网络软件、办公软件、编程软件、媒体软件、行业软件、游戏软件、安全软件。

### 2) 进程综合信息的描述

- 进程文字颜色描述
  - 黄色文字 — “其他软件”的进程信息。
  - 白色文字 — 正常软件的进程信息。
  - 白色高亮 — 被选中的进程信息。
- 网络端口图标描述
  -  — 表示端口正在连出。

-  — 表示端口正在连入。
-  — 表示端口处在监听状态。

### 3) 进程综合信息的操作

【进程综合信息】中提供了丰富的操作功能方便用户对系统中的进程进行查看、分析判断。

- 查看文件属性：将鼠标轻移到进程综合信息中的任意进程或模块的名称上，即可显示该进程或模块的文件自述、描述、产品名称、公司名称、文件版本，以及进程（或模块）启动/停止时间。
- 查看进程调用的模块信息：在“进程列表区”选择要查看的进程，单击该进程名称，在模块信息区显示该进程所调用模块信息，如下图显示进程 EXPLORER.EXE 所调用的模块信息。

模块名称	分类	全路径	程序说明
EXPLORER.EXE	Window...	C:\WINDOWS\EXPLORER.EXE	Microsoft Windows 7
EXPLORERFR...	Window...	C:\WINDOWS\SYSTEM32\EXPLORERFR...	Microsoft Windows 7
FRAMEDYNOS...	Window...	C:\WINDOWS\SYSTEM32\FRAMEDYNO...	Microsoft Windows 7
FXSAPI.DLL	Window...	C:\WINDOWS\SYSTEM32\FXSAPI.DLL	Microsoft Windows 7
FXSRESM.DLL	Window...	C:\WINDOWS\SYSTEM32\FXSRESM.DLL	Microsoft Windows 7

图 28

### 4) 字段栏右键操作

鼠标右键单击【进程综合信息】中的标签页字段栏，在弹出的列表中选择要显示的字段信息（如下图）。用户可以自己定制进程详细信息区所要显示的字段内容。



图 29

- 【程序说明~】— 描述进程的类别名。
- 【运行状态】— 进程当前状态。包含两种状态：进程启动日期—时间—运行、进程启动日期—时间—

停止。

- 【PID】— 进程号。
- 【路径】— 进程的绝对路径。
- 【进程命令行参数】— 显示执行当前进程的运行参数。
- 【PPID】— 父进程号。
- 【父进程全路径】— 父进程的绝对路径。
- 【流量比（不含本机内部流量(%)）】— 进程的总流量占本计算机总流量的百分比。
- 【本地 IP】— 本计算机的 IP 地址。
- 【远程 IP】— 远程计算机的 IP 地址。
- 【远程端口】— 连接的远程计算机的端口。
- 【协议】— 进程访问网络时所采用的协议，包含的协议：TCP、UDP、RAW。
- 【网络状态】— 包含连入、连出、监听三个状态。
- 【下载总流量 (Bytes)】— 显示进程的下载总流量。
- 【上传总流量 (Bytes)】— 显示进程的上传总流量。
- 【本机内部接收总流量 (Bytes)】— 显示进程循环地址的接收总流量。
- 【本机内部发送总流量 (Bytes)】— 显示进程循环地址的发送总流量。

#### 5) 查看进程状态信息

有两种查看方式：

- 方式一：通过定制标签页字段栏中的显示字段，在详细信息区中查看进程的状态信息。
- 方式二：双击“②进程详细信息区”中要查看的进程记录，显示进程状态信息。

#### 6) 右键操作

在①进程列表区，选择列表中的任意进程，单击右键，弹出如下图所示操作列表。



图 30

- 程序信息 — 显示从微点主动防御软件安装之后监控到的当前进程的所有信息，包括程序来源、生成的




文件、修改的注册表项。

- 进程信息 — 显示当前进程的状态，包含该进程本次运行时生成的文件和修改的注册表项。
- 流量图 — 动态显示所选进程的所有本地端口的网络流量情况。流量的操作方式请参看【网络分析】中的【流量图】。
- 结束进程/进程树 — 在右键菜单中选择“结束进程”或“结束进程树”，结束所选进程的运行。
- 查找目标 — 打开资源管理器，搜索并定位到所选进程或模块的路径。
- 添加到可信程序 — 在“其他软件”类别中，选择右键菜单中的“添加到可信程序”将选中的“其他软件”的进程，添加到可信程序中。
- 从可信程序移除 — 在“可信程序”类别中，选择右键菜单中的“从可信程序中移除”，将选中的进程从可信程序策略列表中删除。

## 7) 删除已退出的进程记录

在打开“进程综合信息”标签栏后，退出的进程，在进程综合信息中还会保留其记录，用户可根据需要将已退出的进程记录删除。

- 删除单个已退出进程记录 — 在进程列表中选中已退出进程，单击右键，选择“删除”，则可将该进程从进程列表中删除。

- 删除所有已退出进程记录 — 右键单击进程列表中“当前进程”，选择“删除所有已退出进程”



，则可将所有已退出的进程从“进程列表”中删除。

### 7.1.2 系统自启动信息

系统自启动信息是指那些未经用户执行，随 Windows 操作系统启动而自动加载的文件，有些自启动程序则是在后台运行，用户根本感觉不到什么。正因为这个特点，绝大多数恶意程序都利用自启动方式实现其危害的目的。微点主动防御软件的【系统自启动信息】模块可以作为用户分析系统中某进程是否为类似于木马或蠕虫等有害程序的判断依据之一。

在【系统自启动信息】中用户可查看自启动程序的相关信息，如下图。



图 31

【① 自启动项详细信息】— 详细显示系统自启动程序名称、启动方式、程序说明、全路径和启动信息；

【② 自启动项回收站】— 存储用户通过右键菜单删除的文件与自启动项，并可进行恢复、另存、上报、删除等管理操作。

### 1) 系统自启动信息颜色描述

- 墨绿色文字 — “其他软件”的自启动信息。
- 白色文字 — 已知程序的自启动信息。
- 红色文字 — 隐藏注册表或者隐藏文件的自启动信息。
- 灰色文字 — 文件已经不存在但注册表还在的自启动项。

### 2) 查看系统自启动信息的文件属性

将鼠标轻移到“系统自启动信息”中的任意自启动程序的名称上，即可显示该自启动程序的文件自述、描述、公司名称、文件版本号。

### 3) 右键菜单功能

- 刷新：重新检测并显示系统自启动信息。
- 隐藏已知的启动信息/显示所有启动信息
  - 隐藏已知的启动信息：仅显示归类为“其他软件”的自启动信息。
  - 显示所有的启动信息：显示当前【系统自启动信息】列表所有的自启动信息。

- 导出自启动项
  - 导出所有启动信息：将当前【系统自启动信息】列表中所有的自启动信息以 txt 文本方式导出到磁盘的指定目录。
  - 导出“其他软件”启动信息：将归类为“其他软件”的自启动信息以 txt 文本方式导出到磁盘的指定目录。
- 删除自启动项：对于归类为“其他软件”的自启动项，微点主动防御软件提供了右键删除的功能，可对其注册表项以及文件进行手工删除。
  - 仅删除自启动项：即将选定的自启动程序的注册表项删除到“自启动项回收站”中。
  - 删除文件与自启动项：将选定的文件以及其注册表项全部删除到“自启动项回收站”中。
- 查找目标：打开资源管理器搜索并定位到所选自启动项中涉及的程序文件的路径。

#### 4) 修改注册表键值

鼠标左键双击【系统自启动信息】详细信息区中的任意一项记录，可以直接打开注册表编辑器，并准确定位到该项记录的注册表键值，用户可以对该项记录的注册表键值做修改和删除操作。

**微点提示：对于不熟悉注册表修改的用户，我们强烈建议您不要对注册表做任何修改操作，以免因误操作造成系统瘫痪，由此所造成的损失由用户自行承担。**

### 7.1.3 模块/进程

【模块 / 进程】显示当前系统中已载入的所有模块以及调用这些模块的进程。

单击主功能【系统分析】中的【模块 / 进程】，打开【模块 / 进程】标签页，显示如下图：



图 32

### 1) 隐藏已知的/显示所有模块信息

- 隐藏已知的模块信息 — 只显示当前进程调用的“其他软件”的模块信息。
- 显示所有模块信息 — 显示当前系统中运行进程调用的所有模块信息。

### 2) 查找目标

打开资源管理器搜索并定位到所选模块的路径。

### 3) 查看调用模块的进程信息

在模块信息区，单击要查看的模块，在进程信息区可以看到当前正在调用该模块的所有进程的详细信息，如下图中显示的是正在调用 kernel32.dll 模块的所有进程的信息。

进程名称	分类	程序说明	全路径
LMS.EXE	系统软件	Intel	C:\PROGRAM FILES (X86)\I
ITUNESH... ..	媒体软件	iTunes	E:\PROGRAM FILES (X86)\I
FLASH.EXE	编程软件	HTML Help Workshop	C:\PROGRAM FILES (X86)\H
DAEMONU.EXE	系统软件	NVIDIA	C:\PROGRAM FILES (X86)\N
APPLEMOBIL...	媒体软件	iTunes	C:\PROGRAM FILES (X86)\C

图 33

### 4) 进程信息区的右键菜单

- 程序信息 — 查看所选进程的程序信息。
- 进程信息 — 查看所选进程的进程信息。
- 结束进程 — 结束所选进程的运行。
- 查找目标 — 打开资源管理器搜索并定位到所选进程的文件路径。

## 7.1.4 系统信息

在【系统分析】中，单击【系统信息】，在打开的【系统信息】可以查看和了解当前计算机的硬件信息以及操作系统的信息。

## 7.2 网络分析

微点主动防御软件提供的【网络分析】工具帮助用户监控和分析进程的网络访问信息和异常情况，提供【进程网络信息】、【IP 流量图】、【端口流量图】、【进程流量图】和【传统防火墙信息】五种网络分析工具。

### 7.2.1 进程网络信息

【进程网络信息】实时详细报告系统中所有正在运行进程的访问网络情况，提供 IP 地址、协议、本地端口、远端端口、监听状态以及网络流量信息，通过对这些信息的分析，用户可以判断当前运行的进程是否异常，是否有有害程序（如木马等）在运行，以便进一步采取措施对系统进行防护。

在【网络分析】子功能中，单击【进程网络信息】，查看进程的网络信息如下图。



进程名称	流量比率%	本地端口	远程IP	远程地址	远程
MPSVC2.exe	00	7100	127.0.0.1	本机地址	
MPSVC2.exe	00	7100			
MPSVC.exe	00	54014	127.0.0.1	本机地址	
MPSVC.exe	00	7400			
daemonu.exe	00	48000	127.0.0.1	本机地址	
daemonu.exe	00	2559			
ITUNESHelper.EXE	00	62233	127.0.0.1	本机地址	
ITUNESHelper.EXE	00	62232	127.0.0.1	本机地址	
ITUNESHelper.EXE	00	49161	127.0.0.1	本机地址	
svchost.exe	00	62234	239.255.255.250	IANA保留地址	
svchost.exe	00	62231	239.255.255.250	IANA保留地址	
svchost.exe	00	62230	239.255.255.250	IANA保留地址	
svchost.exe	00	62229	239.255.255.250	IANA保留地址	
svchost.exe	00	62228	239.255.255.250	IANA保留地址	

图 34

### 1) 网络状态背景颜色描述

- 绿色背景——将要退出的网络连接。
- 黄色背景——有流量的网络连接。
- 红色背景——新建的网络连接。

### 2) 查看网络进程的文件属性

将鼠标轻移到“进程网络信息”列表中的任意进程的名称上，即可显示该进程文件的文件自述、描述、产品名称、公司名称、文件版本，以及进程启动时间和本地端口打开时间。

### 3) 进程网络信息区右键菜单

- 程序信息 — 查看所选进程的程序信息。
- 进程信息 — 查看所选进程的进程信息。
- 流量图 — 查看所选进程的总流量以及其开启的端口流量。
- 结束进程/进程树 — 结束正在进行网络连接的进程的运行。
- 关闭该 tcp 连接 — 中断所选进程的当前的 tcp 连接。
- 查找目标 — 打开资源管理器搜索并定位到所选进程的文件路径。

## 7.2.2 流量图

微点主动防御软件提供了【IP 流量图】、【端口流量图】、【进程流量图】，直观显示系统中正在访问网络的进程的流量状况，通过流量图分析进程的流量情况，可判断是否有可疑进程在运行，再结合系统的其它分析工具（系

统分析) 来判断系统是否存在有害程序。

- 【IP 流量图】是以 IP 地址作为索引形式，以波形图的方式显示系统中所有（包括内部网、外部网）IP 地址的瞬时流量（流入和流出）情况。
- 【端口流量图】是以端口号作为索引形式，以波形图的方式显示系统中所有打开端口的流量情况。
- 【进程流量图】是以进程名称作为索引形式，以波形图的方式显示当前系统中正在运行的进程的流量情况。

### 7.2.3 防火墙信息

【防火墙信息】记录微点主动防御软件防火墙的报警信息，若系统中检测到需要记录报警信息的策略的数据包时，就会将该信息记录到防火墙信息中，提示用户进出数据包协议类型、本地地址及端口、方向、远程地址及端口。如下图。

序号	信息
100	协议类型:TCP 192.168.1.117:52051<=>123.125.104.228:80
101	协议类型:TCP 192.168.1.117:52234<=>60.2.251.193:80
102	协议类型:TCP 192.168.1.117:52051<=>123.125.104.228:80
103	协议类型:TCP 192.168.1.117:52051=>123.125.104.228:80
104	协议类型:TCP 192.168.1.117:52234<=>60.2.251.193:80
105	协议类型:TCP 192.168.1.117:52234=>60.2.251.193:80
106	协议类型:TCP 192.168.1.117:52234<=>60.2.251.193:80
107	协议类型:TCP 192.168.1.117:52234=>60.2.251.193:80
108	协议类型:TCP 192.168.1.117:52088<=>202.108.33.40:80
109	协议类型:TCP 192.168.1.117:52088=>202.108.33.40:80
110	协议类型:TCP 192.168.1.117:52088<=>202.108.6.122:80
111	协议类型:TCP 192.168.1.117:52088<=>202.108.33.40:80
112	协议类型:TCP 192.168.1.117:52088=>202.108.33.40:80
113	协议类型:TCP 192.168.1.117:52088<=>202.108.33.40:80

图 35

**微点提示：**微点主动防御软件的默认规则包不记录防火墙的报警信息。

## 7.3 注册表分析

微点主动防御软件提供的【注册表分析】工具主要为系统的一些重要注册表项提供保护功能，防止系统中一些重要的注册表项被恶意程序修改。

在【系统分析】中，选择【注册表分析】并单击【注册表保护】，打开如下图所示的标签页：



图 36

### 1) 刷新

单击“刷新”按钮，显示注册表保护里面注册表项的最新保护状态。

### 2) 取消保护

勾选列表中状态为“保护”的注册表项，单击“取消保护”按钮，此时注册表项的“保护状态”显示为“未保护”，则取消了当前注册表项的保护。

### 3) 保护

勾选要保护注册表项后，单击“保护”按钮，完成注册表项的保护，此时注册表项的“保护状态”显示为“保护”，对于设置为保护的注册表项，在被其他程序修改时，微点主动防御软件会立即弹出警示框阻止修改。

## 第8章. 服务与支持

### 8.1 生成技术支持信息

包含内容：操作系统的版本号、微点主动防御软件的具体版本信息、系统自启动信息、微点主动防御软件的日志信息（包含系统日志和安全日志）、当前运行的进程和模块信息。该报告文档中的文件采用文本文件类型（.txt），用户也可以打开查看。

导出方法：【微点主界面】>【帮助】>【生成技术支持信息】，然后单击“选择路径”设置导出文件的存储路径和文件名，默认存储路径为系统当前登录用户的桌面下，单击确定，则会自动导出一个压缩格式的文档（MPExInfo.zip）。

## 8.2 自助服务

登陆微点公司网站的客户服务中心 <http://service.micropoint.com.cn> 可以在常见问题和使用技巧根据问题的类型或关键字进行搜索查询，获取相关问题的解决方案。

## 8.3 在线问题反馈

登陆微点公司网站的电子邮局 <http://service.micropoint.com.cn/mail.php> 选择相应的问题类型，根据提示尽可能提供详细的相关问题的信息进行提交，微点公司会尽快以邮件的方式将结果回复至您的邮箱。

或者登陆微点社区 <http://community.micropoint.com.cn> 提交您的问题。

## 8.4 人工服务

技术服务热线：(010) 59798298-515

传真：(010) 88891696

邮件服务：support@micropoint.com.cn

公司地址：北京市海淀区蓝靛厂东路2号金源时代购物中心B区写字楼1608室



## 附录

### 附录一 常见问题

#### 1) 微点主动防御软件支持哪些操作系统？

解 答：支持简体中文/英文 Microsoft Windows 2000/XP/2003/2008/vista/7 32 位 (x86)、Microsoft Windows 7 64 位 (x64)、Microsoft Windows 2003 sp2 64 位 (x64)、Microsoft Windows 2008 64 位 (x64) 。

#### 2) 无法注册，提示“连接注册服务器失败...”

解 答： 出现这种问题的原因可能有三个：

- 是否正常连接网络？

如果不能上网，请检测网络连接。确认已正常连接网络后，再进行注册。

- 是否使用代理上网？

请尝试在微点软件的“升级设置”窗口设置好代理服务器，并测试代理通过后，再进行注册。

- 是否安装有其他安全软件或防火墙？

如果有，请尝试将微点的程序：MPMAIN.EXE、MPMON.EXE、MPSTART.EXE、MPSVC.EXE、MPSVC1.EXE、MPSVC2.EXE、MPUPDATE.EXE、DOWNLOAD.EXE 添加到其允许进程通讯的策略中或者监控排除列表中，再注册。若不清楚如何添加或添加后仍有无法注册，请尝试暂时关闭或卸载其他安全软件后再注册测试，或请直接联系微点客服。

如上述操作后，仍无法注册，请及时与微点客服联系处理。

#### 3) 一个序列号能否在多系统或者多台机器上注册使用

解 答：除非特别说明，微点主动防御软件同一个序列号只能在一个操作系统上注册使用。如果同时在多系统下注册使用同一序列号，则只有最后注册的那个系统的微点可以正常升级。

#### 4) 无法注册微点，提示“注册时使用的升级 id 不正确”

解 答：请仔细核对说明书上的升级 ID，避免因输入错误数字导致，如果仔细核对后仍有此提示请联系微点客服人员。

#### 5) 无法升级，提示“服务器繁忙或网络不通”

解 答：出现此问题的原因：

原因一： 没有连接网络。

解决办法：请正确连接网络后，再进行升级。

原因二：使用代理上网。

解决办法：在“升级设置”窗口设置代理服务器，并测试代理通过后，再进行注册升级。

原因三：系统中安装了其他安全软件或防火墙阻止了微点软件的升级。

解决办法：请将微点安装目录下的程序：MPSVS.exe、MPSVC1.exe、MPSVC2.exe、MPMon.exe、MPMain.exe、MPUpdate.exe、Download.exe 加入到防火墙允许程序通讯的策略中，然后再尝试升级，如仍有问题，请与微点客服联系。

原因四：微点的升级服务器繁忙。

解决办法：请选择其他时间升级，如仍有问题，请与微点客服联系。

## 6) 如何防范网页挂马？

解 答：三重防护功能：

微点主动防御软件最新版本加入了防范 ie 溢出代码攻击的防御功能，形成了多层次立体式防网页挂马的功能，为用户的上网安全提供了全面的防护功能。

第一层拦截：依据浏览器溢出行为查杀防御网页恶意代码（入口处拦截：拦截挂马网站）；

第二层拦截：特征码技术防杀已知木马病毒。

第三层拦截：主动防御技术防杀未知木马病毒。

## 7) 查看微点主动防御软件的当前版本号以及更新时间

解 答：可通过以下三种方法查看：

- 将鼠标移到任务栏中微点主动防御软件的图标上，即可显示微点主动防御软件的程序版本、特征版本以及最后一次更新时间。
- 打开微点主动防御软件的主界面，主界面底部的状态栏显示微点主动防御软件的程序版本号以及最后一次更新时间。
- 打开微点主动防御软件主界面，单击【帮助】->【关于】，显示微点主动防御软件的程序版本、特征版本以及最后一次更新时间。

## 8) 【常规】中自动处理、询问后处理、静默模式三种处理方式有何区别？

解 答：三种方式的区别：

“自动处理”是指微点主动防御软件在监控系统过程中，如果发现木马、病毒，自动拦截危害行为并删除到

隔离区中，同时弹出警示框告知用户。

“静默方式”是指微点主动防御软件在监控系统过程中，如果发现木马、病毒，自动拦截危害行为并删除到隔离区中，不弹出警示框提示用户。

“询问后处理”是指微点主动防御软件在监控系统过程中，如果发现木马、病毒，提示用户发现木马、病毒，并由用户选择处理方式，弹出的警示框会保留一定的时间，以使用户查看报警窗口的详细信息，做出处理。

#### 9) 微点主动防御软件过期后，能否继续使用？

解 答：不能使用。要想继续使用请续费或者购买新的正式版。

#### 10) 如何防范 U 盘病毒？

解 答：双重防范 U 盘病毒。

- 插入 U 盘自动检测：计算机接入 U 盘时，自动弹出警示框提示：“发现机器新增加一个可移动磁盘，是否需要扫描全盘？”，选择扫描后将立即对 U 盘进行病毒扫描检测。
- 主动防御行为监控判断：当对 U 盘自动检测未发现病毒时，微点软件仍然对 U 盘上所有程序和文件进行行为监控，实时分析程序行为，发现有程序试图产生病毒、木马行为时，主动拦截并通过警示框明确提示发现未知木马、病毒，用户确认后自动清除 U 盘病毒。

