

McAfee®

Total Protection

用户手册

目录

McAfee Total Protection	3
McAfee SecurityCenter.....	5
SecurityCenter 功能	6
使用 SecurityCenter	7
修复或忽略保护问题	15
使用警报	19
查看事件	25
McAfee VirusScan	27
VirusScan 功能.....	28
扫描计算机	29
处理扫描结果	33
扫描类型	36
使用其他防护	39
设置病毒防护	43
McAfee Personal Firewall	57
Personal Firewall 功能	58
启动防火墙	59
使用警报	61
管理信息警报	63
配置防火墙保护	65
管理程序和权限	75
管理计算机连接	83
管理系统服务	91
记录、监视和分析	97
了解 Internet 安全性	107
McAfee Anti-Spam	109
Anti-Spam 功能	111
配置垃圾邮件检测	113
过滤电子邮件	121
设置朋友	123
设置 Web 邮件帐户	127
处理过滤的电子邮件	131
配置网络钓鱼防护	133
McAfee Parental Controls	135
家长监控的功能	136
保护儿童	137
在 Web 上保护信息	153
保护密码	155
McAfee Backup and Restore	159
Backup and Restore 的功能	160
存档文件	161
处理已存档的文件	169

McAfee QuickClean	175
QuickClean 功能	176
清理计算机	177
对计算机进行碎片整理	180
计划任务	181
McAfee Shredder	187
Shredder 功能	188
清除文件、文件夹和磁盘	189
McAfee Network Manager	191
Network Manager 功能	192
了解 Network Manager 图标	193
设置托管网络	195
远程管理网络	201
监视您的网络	205
McAfee EasyNetwork	209
EasyNetwork 功能	210
设置 EasyNetwork	211
共享和发送文件	217
共享打印机	223
参考	226
 词汇表	 227
 关于 McAfee	 239
许可	239
版权	240
客户服务和技术支持	241
使用 McAfee Virtual Technician	241
支持和下载	242
 索引	 252

McAfee Total Protection

Total Protection 不仅是保护计算机的一款安全产品，还是一款全面的防御系统，在您在线工作或娱乐时，保护您和您家人的安全。您可以使用 Total Protection 保护计算机免受病毒、黑客和间谍软件的侵扰；监视 Internet 通讯是否有可疑活动；保护您家人的隐私；阻止有风险的网站等。

本章内容

McAfee SecurityCenter.....	5
McAfee VirusScan.....	27
McAfee Personal Firewall.....	57
McAfee Anti-Spam.....	109
McAfee Parental Controls.....	135
McAfee Backup and Restore	159
McAfee QuickClean.....	175
McAfee Shredder	187
McAfee Network Manager	191
McAfee EasyNetwork	209
参考	226
关于 McAfee.....	239
客户服务和技术支持.....	241

第 1 章

McAfee SecurityCenter

McAfee SecurityCenter 允许您监视计算机的安全状态，立即了解计算机的病毒、间谍软件、电子邮件和防火墙保护服务是否是最新的，并对可能的安全漏洞采取措施。它提供您所需的导航工具和控件以协调和管理所有计算机保护区域。

在开始配置和管理计算机的保护之前，请查看 SecurityCenter 界面，并确保您了解保护状态、保护类别和保护服务之间的差别。然后，更新 SecurityCenter 以确保可以从 McAfee 获得最新的保护。

在完成最初的配置任务后，可以使用 SecurityCenter 监视您计算机的保护状态。如果 SecurityCenter 检测到保护问题，它会提醒您，以便您可以根据严重性修复或忽略该问题。您还可以在事件日志中查看 SecurityCenter 事件，如病毒扫描配置更改。

注意： 在检测到重要和不重要的问题时，SecurityCenter 都会立即报告。如果您需要帮助来诊断保护问题，则可以运行 McAfee Virtual Technician。

本章内容

SecurityCenter 功能	6
使用 SecurityCenter	7
修复或忽略保护问题	15
使用警报	19
查看事件	25

SecurityCenter 功能

简化的保护状态

轻松查看计算机的保护状态、检查更新和修复保护问题。

自动更新和升级

SecurityCenter 会自动下载并安装程序的更新。一旦有新版本的 McAfee 程序推出，您的计算机就会在订购有效期间自动获得新版本，从而确保您始终获得最新的保护。

实时警报

安全警报会将紧急病毒发作和安全威胁通知给您。

使用 SecurityCenter

在开始使用 SecurityCenter 前, 请查看将用于管理计算机保护状态的组件和配置区域。有关此映像中所使用技术的详细信息, 请参阅了解保护状态 (第 8 页) 和了解保护类别 (第 9 页)。然后, 您可以查看 McAfee 帐户信息并验证订购的有效性。



本章内容

了解保护状态.....	8
了解保护类别.....	9
了解保护服务.....	10
管理您的订购.....	11
更新 SecurityCenter.....	13

了解保护状态

您计算机的保护状态显示在 SecurityCenter 的“主页”窗格上的保护状态区域。它表示您的计算机是否受到完全保护，可以抵御最新的安全威胁，以及是否受外部安全攻击、其他安全程序以及访问 Internet 程序之类的事件影响。

您计算机的保护状态可能是红色、黄色和绿色。

保护状态	说明
红色	<p>您的计算机未受保护。SecurityCenter 的“主页”窗格上的保护状态区域为红色，表示您未受保护。SecurityCenter 会至少报告一个重要安全问题。</p> <p>要获取完全保护，您必须修复每个保护类别中的所有重要安全问题（问题类别状态设置为“需要采取操作”时也是红色）。有关如何修复保护问题的信息，请参阅修复保护问题 (第 16 页)。</p>
黄色	<p>您的计算机受到部分保护。SecurityCenter 的“主页”窗格上的保护状态区域为黄色，表示您未受保护。SecurityCenter 会至少报告一个不重要的安全问题。</p> <p>要获得完全保护，则必须修复或忽略与每个保护类别关联的不重要的安全问题。有关如何修复或忽略保护问题的信息，请参阅修复或忽略保护问题 (第 15 页)。</p>
绿色	<p>您的计算机受到完全保护。SecurityCenter 的“主页”窗格上的保护状态区域为绿色，表示您受到保护。SecurityCenter 不会报告任何重要或不重要的安全问题。</p> <p>每个保护类别都会列出保护您计算机的服务。</p>

了解保护类别

SecurityCenter 的保护服务分为四个类别：计算机和文件、Internet 和网络、电子邮件和即时消息以及家长监控。这些类别有助于您浏览和配置保护计算机的安全服务。

您可以单击类别名称配置其保护服务，并查看这些服务检测到的任何安全问题。如果您的计算机保护状态为红色或黄色，则一个或多个类别会显示“需要采取操作”或“注意”消息，表示 SecurityCenter 检测到该类别的问题。有关保护状态的详细信息，请参阅了解保护状态（第 8 页）。

保护类别	说明
计算机和文件	“计算机和文件”类别允许配置以下保护服务： <ul style="list-style-type: none">▪ 病毒防护▪ 间谍软件防护▪ SystemGuard▪ Windows 保护▪ PC 健康
Internet 和网络	“Internet 和网络”类别允许配置以下保护服务： <ul style="list-style-type: none">▪ 防火墙保护▪ 网络钓鱼防护▪ 身份保护
电子邮件和即时消息	“电子邮件和即时消息”类别允许配置以下保护服务： <ul style="list-style-type: none">▪ 电子邮件病毒防护▪ 即时消息病毒防护▪ 电子邮件间谍软件防护▪ 即时消息间谍软件防护▪ 垃圾邮件防护
家长监控	“家长监控”类别允许配置以下保护服务： <ul style="list-style-type: none">▪ 内容阻止

了解保护服务

保护服务是可以进行配置以保护您计算机和文件的各种安全组件。保护服务直接与 McAfee 程序对应。例如，在安装 VirusScan 后，可以使用下列保护服务：病毒防护、间谍软件防护、SystemGuard 和脚本扫描。有关这些特定保护服务的详细信息，请参阅 VirusScan 帮助。

默认情况下，您在安装某个程序后，系统会启用与该程序关联的所有保护服务；不过，您可以随时禁用保护服务。例如，如果安装家长监控，则会启用“内容阻止”和“身份保护”。如果您不打算使用“内容阻止”保护服务，则可以将其完全禁用。您还可以在执行安装或维护任务时临时禁用保护服务。

管理您的订购

您所购买的每个 McAfee 保护产品都附带一个订购，该订购允许您在一段时间内在一定数量的计算机上使用该产品。订购期的长度因您购买的产品而异，但通常从您激活产品时开始。激活非常简单而且完全免费，您只需要拥有 Internet 连接即可，但是，激活却又非常重要，因为它使您能够定期接收自动产品更新，从而使您的计算机抵御最新的威胁。

激活通常在安装产品时发生，但是，如果您决定等到以后激活（例如，如果您没有 Internet 连接），则可以在 15 天之内激活。如果您未在 15 天内激活，则您的产品将不再接收关键更新或执行扫描。在您的订购即将到期时，我们还将定期（用屏幕上的消息）通知您。这样，您就可以通过提前续订您的保护或者通过在我们的网站上设置自动续订来避免保护中断。

如果您在 SecurityCenter 中看到一个提示您激活的链接，则说明您的订购尚未激活。要查看您的订购的到期日期，可以查看您的“帐户”页。

访问您的 McAfee 帐户

您可以轻松地从 SecurityCenter 访问 McAfee 帐户信息（您的“帐户”页）。

- 1 在“常见任务”下，单击“我的帐户”。
- 2 登录 McAfee 帐户。

激活您的产品

激活操作通常在您安装产品时发生。但是，如果您尚未激活，则会在 SecurityCenter 中看到一个提示您激活的链接。我们还将定期通知您。

- 在 SecurityCenter 的“主页”窗格上，在“SecurityCenter 信息”下，单击“请激活您的订购”。

提示：您可以从定期出现的警报中进行激活。

验证您的订购

您可以通过验证订购来确保它没有过期。

- 右键单击任务栏最右侧通知区域中的 SecurityCenter 图标 ，然后单击“验证订购”。

续订您的订购

在您的订购即将到期之前，您将在 SecurityCenter 中看到一个提示您续订的链接。我们还将定期用警报通知您订购即将过期。

- 在 SecurityCenter 的“主页”窗格上，在“SecurityCenter 信息”下，单击“续订”。

提示：您还可以从定期出现的通知消息中续订产品。或者，转至您的“帐户”页，在这里，可以续订您的产品或设置自动续订。

更新 SecurityCenter

SecurityCenter 会每隔四个小时检查和安装一次在线更新，从而确保注册的 McAfee 程序是最新的。在线更新可能会包括最新的病毒定义和黑客、垃圾邮件、间谍软件防护或隐私保护升级，这取决于您安装和激活的程序。如果要在默认的四个小时期限内检查更新，则可以随时更新。在 SecurityCenter 正在检查更新时，您可以执行其他任务。

您可以更改 SecurityCenter 检查和安装更新的方式，但并建议不要这样做。例如，您可以将 SecurityCenter 配置为下载更新但不安装，或在下载或安装更新之前通知您。您还可以禁用自动更新。

注意：如果您的 McAfee 产品是从光盘安装的，则必须在 15 天内激活该产品，否则您的产品将无法接收关键更新或执行扫描。

本章内容

检查更新.....	13
配置自动更新.....	13
禁用自动更新.....	14

检查更新

默认情况下，SecurityCenter 会在计算机连接到 Internet 后每四小时自动检查一次更新；不过，如果要在四小时内检查更新，则可以这样做。如果禁用了自动更新，则需要定期检查更新。

- 在 SecurityCenter 的“主页”窗格中，单击“更新”。

提示：您可以检查更新而无须启动 SecurityCenter，方法是右键单击任务栏最右侧通知区域中的 SecurityCenter 图标 ，然后单击“更新”。

配置自动更新

默认情况下，SecurityCenter 会在计算机连接到 Internet 后每四小时自动检查一次更新。如果要更改此默认行为，则可以将 SecurityCenter 配置为自动下载更新，然后在可以安装更新时通知您，或在下载更新前通知您。

注意：SecurityCenter 会使用警报在可以下载或安装更新时通知您。您可以在此警报中下载或安装更新，也可以推迟更新。在从警报中更新程序时，系统可能会提示您在下载和安装前验证订购。有关详细信息，请参阅使用警报（第 19 页）。

- 3 打开“SecurityCenter 配置”窗格。

如何实现？

1. 在“常见任务”下，单击“主页”。
 2. 在右侧窗格的“SecurityCenter 信息”下，单击“配置”。
- 4** 在“SecurityCenter 配置”窗格的“禁用自动更新”下，单击“开”，然后单击“高级”。
- 5** 单击以下任一按钮：
- 自动安装更新并在服务更新后通知我(建议)
 - 自动下载更新并在可以安装更新时通知我
 - 下载任何更新之前都通知我
- 6** 单击“确定”。

禁用自动更新

如果禁用自动更新，则您需要定期检测更新；否则，您的计算机不会获得最新的安全保护。有关手动检查更新的信息，请参阅检查更新（第 13 页）。

- 1** 打开“SecurityCenter 配置”窗格。

如何实现？

1. 在“常见任务”下，单击“主页”。
 2. 在右侧窗格的“SecurityCenter 信息”下，单击“配置”。
- 2** 在“SecurityCenter 配置”窗格的“已启用自动更新”下，单击“关”。
- 3** 在确认对话框中，单击“是”。

提示：您可以通过单击“开”按钮或清除“更新选项”窗格上的“禁用自动更新，我将手动检查更新”来启用自动更新。

修复或忽略保护问题

在检测到重要和不重要的问题时，SecurityCenter 会立即报告。重要保护问题需要立即采取操作，并且会更改保护状态（将颜色改为红色）。不重要的保护问题不需要立即采取操作，可能会（也可能不会）更改保护状态（取决于问题类型）。要获得绿色保护状态，您必须修复所有重要问题，修复或忽略所有不重要的问题。如果您需要帮助来诊断保护问题，则可以运行 McAfee Virtual Technician。有关 McAfee Virtual Technician 的详细信息，请参阅 McAfee Virtual Technician 帮助。

本章内容

修复保护问题	16
忽略保护问题	17

修复保护问题

大多数安全问题都可以自动修复；不过有些问题需要您采取操作。例如，如果禁用了防火墙保护，则 SecurityCenter 会自动启用它；不过，如果没有安装防火墙保护，则必须进行安装。下表介绍了一些在手动修复保护问题时可能采取的其他操作：

问题	操作
在过去的 30 天内，您计算机尚未进行完全扫描。	手动扫描计算机。有关详细信息，请参阅 VirusScan 帮助。
您的检测特征码文件 (DAT) 已过期。	手动更新保护。有关详细信息，请参阅 VirusScan 帮助。
某个程序尚未安装。	从 McAfee 网站或光盘安装此程序。
某个程序缺少组件。	从 McAfee 网站或光盘重新安装此程序。
某个程序未激活，而且无法受到完全保护。	在 McAfee 网站上激活此程序。
您的订购已过期。	在 McAfee 网站上检查帐户状态。有关详细信息，请参阅管理您的订购 (第 11 页)。

注意：通常，一个保护问题会影响多个保护类别。在此情况下，在一个类别中修复问题会将其从所有其他保护类别中清除。

自动修复保护问题

SecurityCenter 可以自动修复大多数保护问题。事件日志不会记录 SecurityCenter 自动修复保护问题时所做的配置更改。有关事件的详细信息，请参阅查看事件 (第 25 页)。

- 1 在“常见任务”下，单击“主页”。
- 2 在 SecurityCenter 的“主页”窗格的保护状态区域中，单击“修复”。

手动修复保护问题

如果在尝试自动修复一个或多个保护问题后这些问题依然存在，则可以手动修复问题。

- 1 在“常见任务”下，单击“主页”。
- 2 在 SecurityCenter 的“主页”窗格中，单击 SecurityCenter 所报告问题的保护类别。
- 3 单击问题描述后的链接。

忽略保护问题

如果 SecurityCenter 检测到不重要的问题，则可以修复或忽略此问题。其他不重要的问题（如未安装 Anti-Spam 或家长监控）会自动忽略。已忽略的问题不会显示在 SecurityCenter 的“主页”窗格上的保护类别信息区域中，除非计算机的保护状态为绿色。如果您忽略了某个问题，但稍后决定希望此问题显示在保护类别信息区域（即使计算机的保护状态不是绿色的），则可以显示已忽略的问题。

忽略保护问题

如果 SecurityCenter 检测到不重要的问题，而您并不打算修复，则可以将其忽略。忽略此问题会从 SecurityCenter 中的保护类别信息区域中将其删除。

- 1** 在“常见任务”下，单击“主页”。
- 2** 在 SecurityCenter 的“主页”窗格中，单击报告问题的保护类别。
- 3** 单击保护问题旁的“忽略”链接。

显示或隐藏忽略的问题

根据问题的严重性，您可以显示或隐藏忽略的保护问题。

- 1** 打开“警报选项”窗格。

如何实现？

1. 在“常见任务”下，单击“主页”。
 2. 在右侧窗格的“SecurityCenter 信息”下，单击“配置”。
 3. 在“警报”下，单击“高级”。
- 2** 在“SecurityCenter 配置”窗格上，单击“忽略的问题”。
 - 3** 在“忽略的问题”窗格上，执行以下操作：
 - 若要忽略问题，请选中其复选框。
 - 若要在保护类别信息区域报告问题，请清除其复选框。
 - 4** 单击“确定”。

提示：您还可以单击保护类别信息区域中已报告问题旁的“忽略”链接来忽略问题。

使用警报

警报是小型弹出式对话框，在发生某些 SecurityCenter 事件时会出现在屏幕的右下脚。警报会提供有关事件的详细信息，以及提供可能与事件关联的解决问题的建议和选项。有些警报还包含指向有关事件的其他信息的链接。使用这些链接可以启动 McAfee 的全球网站，或将信息发给 McAfee 来排除故障。

下面是三种类型的警报：红色警报、黄色警报和绿色警报。

警报类型	说明
红色	红色警报是要求您响应的重要通知。当 SecurityCenter 无法确定如何自动修复保护问题时，会产生红色警报。
黄色	黄色警报是不重要的通知，通常要求您进行响应。
绿色	绿色警报是不重要的通知，不要求您进行响应。绿色警报提供有关事件的基本信息。

因为警报在监视和管理警报状态时起着非常重要的作用，所以您无法禁用警报。不过，您可以控制是否显示某些类型的信息警报，以及配置某些其他警报选项（如 SecurityCenter 是否在出现警报时播放声音，或是否在启动时显示 McAfee 启动屏幕）。

本章内容

显示和隐藏信息警报.....	20
配置警报选项.....	22

显示和隐藏信息警报

信息警报会在发生对计算机安全没有威胁的事件时通知您。例如，如果设置了防火墙保护，则在默认情况下，会在对计算机上的程序授予 Internet 访问权限时出现信息警报。如果您不想显示特定类型的信息警报，则可以将其隐藏。如果您不希望显示任何信息警报，则可以隐藏所有警报。如果在计算机上以全屏模式玩游戏，还可以隐藏所有信息警报。在游戏结束并退出全屏幕模式后，SecurityCenter 会再次开始显示信息警报。

如果误隐藏了信息警报，则可以随时再次显示。默认情况下，SecurityCenter 会显示所有信息警报。

显示或隐藏信息警报

您可以将 SecurityCenter 配置为显示某些信息警报并隐藏其他的信息警报，也可以隐藏所有信息警报。

1 打开“警报选项”窗格。

如何实现？

1. 在“常见任务”下，单击“主页”。
2. 在右侧窗格的“SecurityCenter 信息”下，单击“配置”。
3. 在“警报”下，单击“高级”。

2 在“SecurityCenter 配置”窗格上，单击“信息警报”。

3 在“信息警报”窗格上，执行以下操作：

- 要显示信息警报，请清除其复选框。
- 若要隐藏信息警报，请选中其复选框。
- 要隐藏所有信息警报，请选中“不显示信息警报”复选框。

4 单击“确定”。

提示：您还可以选中警报本身的“不再显示此警报”复选框来隐藏某个信息警报。如果隐藏了此警报，您可以清除“信息警报”窗格上相应复选框来再次将其显示出来。

玩游戏时显示或隐藏信息警报

如果在计算机上以全屏模式玩游戏，可以隐藏信息警报。在游戏结束并退出全屏幕模式后，SecurityCenter 会再次开始显示信息警报。

1 打开“警报选项”窗格。

如何实现？

1. 在“常见任务”下，单击“主页”。
 2. 在右侧窗格的“SecurityCenter 信息”下，单击“配置”。
 3. 在“警报”下，单击“高级”。
- 2** 在“警报选项”窗格上，选中或清除“当检测到游戏模式时显示信息警报”复选框。
- 3** 单击“确定”。

配置警报选项

警报的外观和频率由 SecurityCenter 配置；不过，您可以调整某些基本的警报选项。例如，您可以在出现警报时播放声音，或在 Windows 启动时隐藏启动屏幕警报。您还可以隐藏在线社区中通知您有关病毒发作和其他安全威胁的警报。

出现警报时播放声音

如果您希望在出现警报时收到音频提示，则可以将 SecurityCenter 配置为在每次出现警报时播放声音。

1 打开“警报选项”窗格。

如何实现？

1. 在“常见任务”下，单击“主页”。
2. 在右侧窗格的“SecurityCenter 信息”下，单击“配置”。
3. 在“警报”下，单击“高级”。

2 在“警报选项”窗格的“声音”下，选中“出现警报时播放声音”复选框。

隐藏启动时的启动屏幕

默认情况下，McAfee 会在 Windows 启动时短暂显示启动屏幕，通知您 SecurityCenter 正在保护您的计算机。不过，如果不想显示启动屏幕，可以将其隐藏起来。

1 打开“警报选项”窗格。

如何实现？

1. 在“常见任务”下，单击“主页”。
2. 在右侧窗格的“SecurityCenter 信息”下，单击“配置”。
3. 在“警报”下，单击“高级”。

2 在“警报选项”窗格的“启动屏幕”下，清除“Windows 启动时显示 McAfee 启动屏幕”复选框。

提示：您可以选中“Windows 启动时显示 McAfee 启动屏幕”复选框，随时再次显示启动屏幕。

隐藏病毒发作警报

您可以隐藏在线社区中通知您有关病毒发作和其他安全威胁的警报。

1 打开“警报选项”窗格。

如何实现？

1. 在“常见任务”下，单击“主页”。
 2. 在右侧窗格的“SecurityCenter 信息”下，单击“配置”。
 3. 在“警报”下，单击“高级”。
- 2** 在“警报选项”窗格上，清除“当出现病毒或安全威胁时提醒我”复选框。

提示: 您可以选中“当出现病毒或安全威胁时提醒我”复选框随时显示病毒发作警报。

隐藏安全消息

您可以隐藏有关保护家庭网络上更多计算机的安全通知。这些消息提供有关您的订购的信息、可以用您的订购保护的计算机数以及如何扩展您的订购以保护更多的计算机。

- 1** 打开“警报选项”窗格。
如何实现？
 1. 在“常见任务”下，单击“主页”。
 2. 在右侧窗格的“SecurityCenter 信息”下，单击“配置”。
 3. 在“警报”下，单击“高级”。

2 在“警报选项”窗格上，清除“显示病毒安全公告和其他安全消息”复选框。

提示: 您可以通过选中“显示病毒安全公告和其他安全消息”复选框来随时显示这些安全消息。

查看事件

事件是在保护类别及其相关保护服务中发生操作或配置更改。不同的保护服务会记录不同类型的事件。例如，SecurityCenter 会在启用或禁用保护服务时记录事件；病毒防护会在每次检测到和删除病毒时记录事件；而防火墙保护会在每次阻止 Internet 连接尝试时记录事件。有关保护类别的详细信息，请参阅了解保护状态（第 9 页）。

您可以在解决配置问题和查看其他用户执行的操作时查看事件。许多家长都使用事件日志来监视其孩子在 Internet 上的行为。如果您只检查发生的最近 30 个事件，则可以查看最新事件。如果您要检查发生的所有事件的全面列表，可以查看所有事件。在您查看所有事件时，SecurityCenter 会启动事件日志，事件日志可以根据发生事件的保护类别来对事件分类。

本章内容

查看最新事件	25
查看所有事件	25

查看最新事件

如果您只检查发生的最近 30 个事件，则可以查看最新事件。

- 在“常见任务”下，单击“查看最新事件”。

查看所有事件

如果您要检查发生的所有事件的全面列表，可以查看所有事件。

- 1 在“常见任务”下，单击“查看最新事件”。
- 2 在“最新事件”窗格上，单击“查看日志”。
- 3 在事件日志的左窗格中，单击要查看的事件类型。

第 2 章

McAfee VirusScan

VirusScan 提供的高级检测和保护服务可以保护您和您的计算机免受最新安全威胁的侵扰，这些威胁有病毒、特洛伊木马程序、跟踪 Cookie、间谍软件、广告软件以及其他可能的有害程序。其保护范围可以扩展到桌面上的文件和文件夹之外，针对来自不同入口点（包括电子邮件、即时消息和 Web）的威胁。

有了 VirusScan，您的计算机将会得到及时和持续的保护（无需繁杂的管理）。当您工作、播放、浏览 Web 或检查电子邮件时，VirusScan 会在后台运行，实时监视、扫描和检测可能的损害。全面扫描会按计划定期运行，使用一组高级选项检查计算机。如果您愿意，可以使用 VirusScan 灵活地自定义此行为；如果您不愿意，您的计算机仍会受到保护。

正常使用计算机时，病毒、蠕虫和其他可能的威胁都可能会侵入您的计算机。如果发生此情况，VirusScan 会不仅将有关威胁通知给您，而且通常会进行处理，在发生任何损坏前清理或隔离感染的项目。有时需要进一步采取操作，不过这种情况很少见。在这些情况下，VirusScan 允许您决定所采取的操作（下次启动计算机时重新扫描，保留检测到的项目或删除检测到的项目）。

注意： 在检测到重要和不重要的问题时，SecurityCenter 都会立即报告。如果您需要帮助来诊断保护问题，则可以运行 McAfee Virtual Technician。

本章内容

VirusScan 功能	28
扫描计算机	29
处理扫描结果	33
扫描类型	36
使用其他防护	39
设置病毒防护	43

VirusScan 功能

全面病毒防护

保护您和您的计算机免受最新安全威胁的侵扰，这些威胁包括病毒、特洛伊木马程序、跟踪 Cookie、间谍软件、广告软件和其他可能有害的程序。其保护范围可以扩展到桌面上的文件和文件夹之外，抵御来自不同入口点（包括电子邮件、即时消息和 Web）的威胁。无需繁杂的管理。

资源感知扫描选项

如果您愿意，可以自定义扫描选项；如果您不愿意，您的计算机仍会受到保护。如果扫描速度很慢，则可以禁用此选项以使用最小计算机资源，但切记授予病毒防护的优先级要高于其他任务的优先级。

自动修复

如果 VirusScan 在运行扫描时检测到某个安全威胁，则它会尝试根据威胁类型来自动处理该威胁。通过这种方式，可以检测到并消除大多数威胁，而无须您的交互。VirusScan 也可能不会自行消除威胁，但这种情况很少见。在这些情况下，VirusScan 允许您决定所采取的操作（下次启动计算机时重新扫描，保留检测到的项目或删除检测到的项目）。

在全屏幕模式下暂停任务

在享受某些活动（如在计算机上观看电影、玩游戏，或进行占用整个计算机屏幕的活动）时，VirusScan 会暂停许多任务（如手动扫描）。

扫描计算机

即使在首次启动 SecurityCenter 之前，VirusScan 的实时病毒防护也会开始保护您的计算机免受可能有害病毒、特洛伊木马程序和其他安全威胁的侵扰。除非禁用实时病毒防护，否则 VirusScan 会使用您设置的实时扫描选项持续监视计算机中的病毒活动，每次您和您的计算机访问文件时扫描这些文件。为确保您的计算机能抵御最新的安全威胁，请将实时病毒防护打开，并建立一个计划以进行定期的全面手动扫描。有关设置扫描选项的详细信息，请参阅设置病毒防护（第 43 页）。

VirusScan 提供一组更详细的扫描选项供病毒防护使用，使您可以定期运行更广泛的扫描。您可以从 SecurityCenter 运行完全扫描、快速扫描、自定义扫描或计划的扫描。您还可以在工作时在 Windows 资源管理器中运行手动扫描。SecurityCenter 中扫描的优点是可以动态更改扫描选项。不过，从 Windows 资源管理器中进行扫描是一种为计算机提供安全保护的便捷方法。

无论是在 SecurityCenter 中还是在 Windows 资源管理器中运行扫描，都可以在扫描完成后查看扫描结果。您可以查看扫描结果，以确定 VirusScan 是否已检测到、修复了或隔离了病毒、特洛伊木马程序、间谍软件、广告软件、Cookie 和其他可能有害的程序。可以通过不同的方式来显示扫描结果。例如，您可以查看扫描结果的基本摘要或详细信息，如感染状态和类型。您还可以查看常规扫描和检测统计信息。

本章内容

扫描您的 PC.....	29
查看扫描结果.....	31

扫描您的 PC

VirusScan 提供一组完整的扫描选项供病毒防护使用，其中包括实时扫描（持续监视计算机中的病毒活动）、从 Windows 资源管理器运行手动扫描以及从 SecurityCenter 中运行完全扫描、快速扫描、自定义扫描或计划的扫描。

要...	执行此操作...
------	----------

要...	执行此操作...
启动“实时扫描”以持续监视计算机中的病毒活动，在您或您的计算机每次访问文件时都扫描文件	<p>1. 打开“计算机和文件配置”窗格。如何实现？</p> <ol style="list-style-type: none"> 1. 在左侧窗格上，单击“高级菜单”。 2. 单击“配置”。 3. 在“配置”窗格上，单击“计算机和文件”。 <p>2. 在“病毒防护”下，单击“开”。</p> <p>注意：实时扫描在默认情况下处于启用状态。</p>
启动“快速扫描”以快速检查您的计算机上是否有威胁	<ol style="list-style-type: none"> 1. 在“基本菜单”上单击“扫描”。 2. 在“扫描选项”窗格的“快速扫描”下，单击“启动”。
启动完全扫描以彻底检查您的计算机上是否有威胁	<ol style="list-style-type: none"> 1. 在“基本菜单”上单击“扫描”。 2. 在“扫描选项”窗格的“完全扫描”下，单击“启动”。
基于自己的设置启动自定义扫描。	<ol style="list-style-type: none"> 1. 在“基本菜单”上单击“扫描”。 2. 在“扫描选项”窗格的“请让我选择”下，单击“启动”。 3. 通过清除或选中以下选项来自定义扫描： <ul style="list-style-type: none"> 所有文件的全部威胁 未知病毒 将文件存档 间谍软件和潜在威胁 跟踪 Cookie 隐匿程序 4. 单击“开始”。
启动“手动扫描”以检查文件、文件夹或驱动器中是否有威胁	<ol style="list-style-type: none"> 1. 打开 Windows 资源管理器。 2. 右键单击文件、文件夹或驱动器，然后单击“扫描”。

要...	执行此操作...
启动“计划的扫描”以定期扫描您的计算机中是否有威胁	<p>如何实现？</p> <ol style="list-style-type: none"> 1. 在“常见任务”下，单击“主页”。 2. 在 SecurityCenter 的“主页”窗格上，单击“计算机和文件”。 3. 在“计算机和文件”信息区域中，单击“配置”。 4. 在“计算机和文件配置”窗格中，确保启用了病毒防护，然后单击“高级”。 5. 在“病毒防护”窗格中单击“计划的扫描”。 2. 选中“启用计划的扫描”。 3. 要用较小的处理器处理能力来进行常规扫描，请选中“使用最小的计算机资源进行扫描”。 4. 选择一天或多天。 5. 指定开始时间。 6. 单击“确定”。

扫描结果会显示在“扫描已完成”警报中。扫描结果包含扫描、检测、修复、隔离和删除的项目数。单击“查看扫描详细信息”以了解扫描结果的详细信息，或处理感染病毒的项目。

注意: 要了解有关扫描选项的更多信息，请参阅扫描类型 (第 36 页)。

查看扫描结果

在扫描完成后，您可以查看结果来确定扫描所找到的项目并分析计算机的当前保护状态。扫描结果可以确定 VirusScan 是否已检测到、修复了或隔离了病毒、特洛伊木马程序、间谍软件、广告软件、Cookie 和其他可能有害的程序。

在“基本菜单”和“高级菜单”上，单击“扫描”，然后执行以下操作：

要...	执行此操作...
查看警报中的扫描结果	查看“扫描已完成”警报中的扫描结果。

要...	执行此操作...
查看有关扫描结果的详细信息	单击“扫描已完成”中的“查看扫描详细信息”。
查看扫描结果的快速摘要	指向任务栏通知区域中的“扫描已完成”图标。
查看扫描和检测统计信息	双击任务栏通知区域中的“扫描已完成”图标。
查看有关检测到的项目、感染状态和类型的详细信息	1. 双击任务栏通知区域中的“扫描已完成”图标。 2. 单击“完全扫描”、“快速扫描”、“自定义扫描”或“手动扫描”窗格上的“详细信息”。
查看有关最近一次扫描的详细信息	在任务栏上的通知区域中双击“扫描已完成”图标，并在“完全扫描”、“快速扫描”、“自定义扫描”或“手动扫描”窗格上“您的扫描”下查看最近一次扫描的详细信息。

处理扫描结果

如果 VirusScan 在运行扫描时检测到某个安全威胁，则它会尝试根据威胁类型来自动处理该威胁。例如，如果 VirusScan 在计算机上检测到病毒、特洛伊木马程序或跟踪 Cookie，它会尝试清理感染病毒的文件。VirusScan 始终在尝试清除文件之前将其隔离。如果文件中存在威胁，则会将其隔离。

对于某些安全威胁，VirusScan 可能无法成功清理或隔离文件。在此情况下，VirusScan 会提示您处理威胁。您可以根据威胁类型采取不同的操作。例如，如果在某个文件中检测到病毒，但 VirusScan 无法成功清理或隔离文件，它会拒绝进一步访问该文件。如果检测到跟踪 Cookie，但 VirusScan 无法成功清理或隔离 Cookie，则可以确定是删除还是信任这些 Cookie。如果检测到可能有害的程序，则 VirusScan 不会采取任何自动操作；转而允许您确定是隔离还是信任该程序。

如果 VirusScan 隔离项目，则它会将其加密并在文件夹中隔离，防止文件、程序或 Cookie 损害您的计算机。您可以恢复或删除隔离的项目。在大多数情况下，您可以删除隔离的 Cookie 而不会影响您的系统；不过，如果 VirusScan 隔离了有用的程序，则可以考虑将其恢复。

本章内容

处理病毒和特洛伊木马程序.....	33
处理可能有害的程序.....	34
处理隔离的文件.....	34
处理隔离的程序和 Cookie	35

处理病毒和特洛伊木马程序

如果 VirusScan 在您的计算机上检测到病毒或特洛伊木马，它会尝试清理该文件。如果无法清理文件，则 VirusScan 会尝试将其隔离。如果隔离也失败，则拒绝对此文件进行访问（仅限实时扫描）。

1 打开“扫描结果”窗格。

如何实现？

1. 双击任务栏最右侧通知区域中的“扫描已完成”图标。
2. 在“扫描进度：手动扫描”窗格中，单击“查看结果”。

2 在扫描结果列表中，单击“病毒和特洛伊木马程序”。

注意：要处理 VirusScan 已隔离的文件，请参阅处理已隔离的文件（第 34 页）。

处理可能有害的程序

如果 VirusScan 在您的计算机上检测到可能有害的程序，您可以删除或信任此程序。如果您不熟悉该程序，我们建议您考虑将其删除。删除可能有害的程序不会从系统中实际删除该程序。相反，删除操作会隔离程序，防止程序损害计算机或文件。

1 打开“扫描结果”窗格。

如何实现？

1. 双击任务栏最右侧通知区域中的“扫描已完成”图标。

2. 在“扫描进度：手动扫描”窗格中，单击“查看结果”。

2 在扫描结果列表中，单击“可能有害的程序”。

3 选择可能有害的程序。

4 在“我想”下面，单击“删除”或“信任”。

5 确认您所选的选项。

处理隔离的文件

如果 VirusScan 隔离感染病毒的文件，则会将其加密，然后移到文件夹中，防止该文件损害您的计算机。然后，您可以恢复或删除隔离的文件。

1 打开“隔离的文件”窗格。

如何实现？

1. 在左侧窗格上，单击“高级菜单”。

2. 单击“还原”。

3. 单击“文件”。

2 选择隔离的文件。

3 执行下面某项操作：

- 若要修复感染病毒的文件并将其恢复到计算机上的最初位置，请单击“恢复”。
- 若要从计算机中删除感染病毒的文件，请单击“删除”。

4 单击“是”确认所选的选项。

提示：您可以同时恢复或删除多个文件。

处理隔离的程序和 Cookie

VirusScan 在隔离可能有害的程序或跟踪 Cookie 时，会将其加密，并移到受保护的文件夹，防止程序或 Cookie 损害您的计算机。然后，您可以恢复或删除隔离的项目。在大多数情况下，您可以删除隔离的项目而不会影响您的系统。

1 打开“隔离的程序”和“跟踪 Cookie”窗格。

如何实现？

1. 在左侧窗格上，单击“高级菜单”。
2. 单击“还原”。
3. 单击“程序和 Cookie”。

2 选择隔离的程序或 Cookie。

3 执行下面某项操作：

- 若要修复感染病毒的文件并将其恢复到计算机上的最初位置，请单击“恢复”。
- 若要从计算机中删除感染病毒的文件，请单击“删除”。

4 单击“是”确认此操作。

提示：您可以同时恢复或删除多个程序和 Cookie。

扫描类型

VirusScan 提供一组完整的扫描选项供病毒防护使用，其中包括实时扫描（持续监视 PC 中的威胁活动）；从 Windows 资源管理器中进行手动扫描；从 SecurityCenter 中运行完全扫描、快速扫描或自定义扫描的功能；或者自定义何时将发生计划的扫描。SecurityCenter 中扫描的优点是可以动态更改扫描选项。

实时扫描：

实时病毒防护会持续监视计算机中的病毒活动，每次您或您的计算机访问文件时都会扫描文件。为确保您的计算机能抵御最新的安全威胁，请将实时病毒防护打开，并建立一个计划以进行定期的全面手动扫描。

您可以为实时扫描设置默认选项，其中包括扫描未知病毒以及检查跟踪 Cookie 和网络驱动器中是否有威胁。您还可以利用缓冲区溢出防护，除非您使用的是 Windows Vista 64 位操作系统，否则该功能在默认情况下处于启用状态。要了解更多信息，请参阅设置实时扫描选项（第 44 页）。

快速扫描

使用快速扫描，可以检查计算机上的进程、关键 Windows 文件和其他可疑区域中是否有威胁活动。

完全扫描

使用完全扫描，可以彻底检查存在于您的 PC 中任何位置的病毒、间谍软件和其他安全威胁。

自定义扫描

使用自定义扫描，可以选择用自己的扫描设置来检查您的 PC 上是否有威胁活动。自定义扫描选项除了包括扫描未知病毒、间谍软件和隐匿程序，还包括检查所有文件、存档文件和 Cookie 中是否有威胁。

您可以为自定义扫描设置默认选项，其中包括扫描未知病毒、存档文件、间谍软件、潜在威胁、跟踪 Cookie 和隐匿程序。您还可以使用最少的计算机资源来进行扫描。要了解更多信息，请参阅设置自定义扫描选项（第 46 页）。

手动扫描

使用手动扫描，可以从 Windows 资源管理器中快速地实时检查文件、文件夹和驱动器中是否有威胁。

计划扫描

计划的扫描可以在一周的任何日期和时间对计算机上的病毒和其他威胁进行彻底的扫描。计划的扫描始终会使用默认扫描选项来检查整个计算机。默认情况下，VirusScan 会每周执行一次计划的扫描。如果您发现扫描速度很慢，则可以考虑禁用此选项来使用最小计算机资源，但切记授予病毒防护的优先级要高于其他任务的优先级。要了解更多信息，请参阅计划扫描 (第 48 页)。

注意：要了解如何启动适合您的最佳扫描选项，请参阅扫描您的 PC (第 29 页)

使用其他防护

除实时病毒防护外，VirusScan 还提供高级防护，抵御脚本、间谍软件和可能有害电子邮件和即时消息附件的侵扰。默认情况下，系统会打开脚本扫描、间谍软件、电子邮件和即时消息保护，从而保护您的计算机。

脚本扫描防护

脚本扫描防护会检测可能有害的脚本，并防止这些脚本在计算机或 Web 浏览器上运行。它会监视计算机中是否有可疑的脚本（如创建、复制或删除文件的脚本，或者打开 Windows 注册表的脚本）活动，并在任何损坏发生前提醒您。

间谍软件防护

间谍软件防护会检测间谍软件、广告软件和其他可能有害的程序。间谍软件是悄悄安装在您计算机上监视您行为的软件，它会收集个人信息，甚至通过安装其他软件或重定向浏览器活动来妨碍您对计算机的控制。

电子邮件保护

电子邮件保护会检测您发送的电子邮件和附件中的可疑活动。

即时消息保护

即时消息保护会检测您接收的即时消息附件中的可能安全威胁。它还会防止即时消息程序共享个人信息。

本章内容

启动脚本扫描防护.....	39
启动间谍软件防护.....	40
启动电子邮件保护.....	40
启动即时消息保护.....	41

启动脚本扫描防护

打开脚本扫描防护会检测可能有害的脚本，并防止这些脚本在计算机上运行。脚本扫描防护会在某个脚本尝试创建、复制或删除计算机上的文件，或者对 Windows 注册表进行更改时提醒您。

1 打开“计算机和文件配置”窗格。

如何实现？

1. 在左侧窗格上，单击“高级菜单”。
2. 单击“配置”。
3. 在“配置”窗格上，单击“计算机和文件”。

2 在“脚本扫描防护”下，单击“开”。

注意：您可以随时关闭脚本扫描防护，但这样做会使有害脚本利用计算机的漏洞。

启动间谍软件防护

打开间谍软件防护会检测和删除间谍软件、广告软件和其他可能有害的程序，这些程序会在您不知晓或未得您许可的情况下收集和传输信息。

1 打开“计算机和文件配置”窗格。

如何实现？

1. 在左侧窗格上，单击“高级菜单”。
2. 单击“配置”。
3. 在“配置”窗格上，单击“计算机和文件”。

2 在“间谍软件防护”下，单击“开”。

注意：您可以随时关闭间谍软件防护，但这样做会使可能有害的程序利用计算机的漏洞。

启动电子邮件保护

打开电子邮件保护会在入站 (POP3) 电子邮件消息和附件中检测蠕虫以及可能的威胁。

1 打开“电子邮件和即时消息配置”窗格。

如何实现？

1. 在左侧窗格上，单击“高级菜单”。
2. 单击“配置”。
3. 在“配置”窗格上，单击“电子邮件和即时消息”。

2 在“电子邮件保护”下，单击“开”。

注意：您可以随时关闭电子邮件保护，但这样做会使电子邮件威胁利用计算机的漏洞。

启动即时消息保护

打开即时消息保护会检测入站即时消息附件中可能包含的安全威胁。

1 打开“电子邮件和即时消息配置”窗格。

如何实现？

1. 在左侧窗格上，单击“高级菜单”。
2. 单击“配置”。
3. 在“配置”窗格上，单击“电子邮件和即时消息”。

2 在“即时消息保护”下，单击“开”。

注意：您可以随时关闭即时消息保护，但这样做会使可能有害的即时消息附件利用计算机的漏洞。

设置病毒防护

您可以为计划的扫描、自定义扫描和实时扫描设置不同的选项。例如，因为实时保护会持续监视您的计算机，所以您可以选择一些基本扫描选项，为手动、按需保护保留一组更全面的扫描选项。

您还可以确定希望 VirusScan 如何使用 SystemGuard 和可信列表，来监视和管理您 PC 上可能未经授权的更改或有害的更改。

SystemGuard 会监视、记录、报告和管理对 Windows 注册表或计算机上的重要系统文件进行的可能未经授权的更改。对注册表和文件进行未经授权的更改会损害您的计算机，危害其安全性并会损坏重要的系统文件。您可以使用可信列表来确定是信任还是删除用来检测文件或注册表更改 (SystemGuard)、程序或缓冲区溢出的规则。如果您信任此项目，并且指出您不想接收将来有关其活动的通知，则此项目会添加到信任列表中，而且 VirusScan 不再检测此项目或向您发送有关其活动的通知。

本章内容

设置实时扫描选项	44
设置自定义扫描选项	46
计划扫描	48
使用 SystemGuard 选项	49
使用可信列表	54

设置实时扫描选项

启动实时病毒防护后，VirusScan 会使用一组默认的选项扫描文件；不过，您可以更改默认选项来满足您的需要。

要更改实时扫描选项，您必须确定 VirusScan 扫描时检查的内容以及扫描的位置和文件类型。例如，您可以确定 VirusScan 是检查未知的病毒还是网站用于跟踪您行为的 Cookie，以及是扫描映射到您计算机的网络驱动器还是仅扫描本地驱动器。您还可以确定扫描文件的类型（所有文件，或仅限程序文件和文档，因为这是检测大多数病毒的位置）。

更改实时扫描选项后，您还必须确定在计算机上启用缓冲区溢出防护是否重要。缓冲区是临时存放计算机信息的部分内存。在可疑程序或进程存储在缓冲区中的信息量超过缓冲区容量时，会发生缓冲区溢出。如果发生缓冲区溢出，您的计算机易遭安全攻击。

设置实时扫描选项

您可以设置实时扫描选项来自定义 VirusScan 在实时扫描时查找的内容，以及扫描的位置和文件类型。这些选项包括扫描未知病毒，跟踪 Cookie 以及提供缓冲区溢出防护。您还可以配置实时扫描来检查映射到计算机的网络驱动器。

1 打开实时扫描窗格。

如何实现？

1. 在“常见任务”下，单击“主页”。
2. 在 SecurityCenter 的“主页”窗格上，单击“计算机和文件”。
3. 在“计算机和文件”信息区域中，单击“配置”。
4. 在“计算机和文件配置”窗格中，确保启用了病毒防护，然后单击“高级”。

2 指定实时扫描选项，然后单击“确定”。

要...	执行此操作...
检测未知病毒和已知病毒的新变种。	选择“扫描未知病毒”。
检测 Cookie	选择“扫描和删除跟踪 Cookie”。
在连接到网络的驱动器上检测病毒和其他可能的威胁。	选择“扫描网络驱动器”。
防止计算机出现缓冲区溢出	选择“启用缓冲区溢出防护”。

要...	执行此操作...
指定要扫描的文件类型	单击“所有文件（建议）”或“仅限程序文件和文档”。

停止实时病毒防护

您有时可能会暂时停止实时扫描（如更改某些扫描选项，或解决性能问题），但这种情况很少见。如果禁用了实时病毒防护，则您的计算机将不受保护，而 SecurityCenter 保护状态变为红色。有关保护状态的详细信息，请参阅 SecurityCenter 帮助中的“了解保护状态”。

您可以临时关闭实时病毒防护，然后指定继续保护的时间。您可以在计算机重新启动后的 15、30、45 或 60 分钟后自动恢复保护，也可以不恢复保护。

1 打开“计算机和文件配置”窗格。

如何实现？

1. 在左侧窗格上，单击“高级菜单”。
2. 单击“配置”。
3. 在“配置”窗格上，单击“计算机和文件”。

2 在“病毒防护”下，单击“关”。

3 在对话框中，选择恢复实时扫描的时间。

4 单击“确定”。

设置自定义扫描选项

自定义病毒防护允许您按需扫描文件。启动自定义扫描后，VirusScan 会使用一组更全面的扫描选项来检查计算机中是否有病毒和其他可能有害的项目。要更改自定义扫描选项，您必须确定 VirusScan 在扫描时所检查的内容。例如，您可以确定 VirusScan 是否查找未知病毒、可能有害的程序（如间谍软件或广告软件）、隐蔽程序和 Rootkit（可以授予对您计算机进行未经授权的访问）以及网站用于跟踪您行为的 Cookie。您还必须确定所检查的文件类型。例如，您可以确定 VirusScan 是检查所有文件还是仅检查程序文件和文档（因为这是大多数病毒所在的位置）。您还可以确定在扫描时是否包含存档文件（如 .zip 文件）。

默认情况下，VirusScan 会在每次运行自定义扫描时，检查您计算机上的所有驱动器和文件夹以及所有网络驱动器；不过，您可以更改默认位置来满足您的需要。例如，您可以只扫描重要的 PC 文件、桌面上的项目或 Program Files 文件夹中的项目。除非您要自行启动每个自定义扫描，否则可以设置定期扫描计划。计划的扫描始终会使用默认扫描选项来检查整个计算机。默认情况下，VirusScan 会每周执行一次计划的扫描。

如果您发现扫描速度很慢，则可以考虑禁用此选项来使用最小计算机资源，但切记授予病毒防护的优先级要高于其他任务的优先级。

注意：在享受某些活动（如在计算机上观看电影、玩游戏，或进行占用整个计算机屏幕的活动）时，VirusScan 会暂停许多任务，包括自动更新和自定义扫描。

设置自定义扫描选项

您可以设置自定义扫描选项来自定义 VirusScan 在自定义扫描时查找的内容，以及扫描的位置和文件类型。这些选项包括扫描未知病毒、文件存档、间谍软件和可能有害的程序、跟踪 Cookie、Rootkit 和隐蔽程序。您还可以设置自定义扫描位置来确定 VirusScan 在自定义扫描时查找病毒和其他有害项目的位置。您可以扫描计算机上的所有文件、文件夹和驱动器，也可以限定扫描特定的文件和驱动器。

1 打开“自定义扫描”窗格。

如何实现？

1. 在“常见任务”下，单击“主页”。
2. 在 SecurityCenter 的“主页”窗格上，单击“计算机和文件”。
3. 在“计算机和文件”信息区域中，单击“配置”。
4. 在“计算机和文件配置”窗格中，确保启用了病毒防护，然后单击“高级”。
5. 在“病毒防护”窗格中单击“手动扫描”。

2 指定自定义扫描选项，然后单击“确定”。

要...	执行此操作...
检测未知病毒和已知病毒的新变种。	选择“扫描未知病毒”。
检测和删除 .zip 和其他存档文件中的病毒	选择“扫描存档文件”。
检测间谍软件、广告软件和其他可能有害的程序	选择“扫描间谍软件和潜在威胁”。
检测 Cookie	选择“扫描和删除跟踪 Cookie”。
检查可以更改和利用现有 Windows 系统文件中漏洞的 Rootkit 和隐匿程序。	选择“扫描隐匿程序”。
使用较小的处理器处理能力进行扫描，同时让其他任务（如 Web 浏览或打开文档）拥有较高的优先级。	选择“使用最小的计算机资源进行扫描”。
指定要扫描的文件类型	单击“所有文件（建议）”或“仅限程序文件和文档”。

3. 单击“默认扫描位置”，选择要扫描的位置或清除要忽略的位置，然后单击“确定”：

要...	执行此操作...
扫描计算机上的所有文件和文件夹	选择“我的电脑”。
扫描计算机上特定的文件、文件夹和驱动器。	清除“我的电脑”复选框，然后选择一个或多个文件或驱动器。
扫描重要的系统文件	清除“我的电脑”复选框，然后选择“重要系统文件”复选框。

计划扫描

将扫描安排在一周的任何日期和时间对计算机上的病毒和其他威胁进行彻底的扫描。计划的扫描始终会使用默认扫描选项来检查整个计算机。默认情况下，VirusScan 会每周执行一次计划的扫描。如果您发现扫描速度很慢，则可以考虑禁用此选项来使用最小计算机资源，但切记授予病毒防护的优先级要高于其他任务的优先级。

安排扫描使用默认扫描选项来检查整个计算机中是否有病毒和其他威胁。默认情况下，VirusScan 会每周执行一次计划的扫描。

1 打开“计划的扫描”窗格。

如何实现？

1. 在“常见任务”下，单击“主页”。
2. 在 SecurityCenter 的“主页”窗格上，单击“计算机和文件”。
3. 在“计算机和文件”信息区域中，单击“配置”。
4. 在“计算机和文件配置”窗格中，确保启用了病毒防护，然后单击“高级”。
5. 在“病毒防护”窗格中单击“计划的扫描”。

2 选中“启用计划的扫描”。

3 要用较小的处理器处理能力来进行常规扫描，请选中“使用最小的计算机资源进行扫描”。

4 选择一天或多天。

5 指定开始时间。

6 单击“确定”。

提示：您可以单击“重置”来恢复默认的计划。

使用 SystemGuard 选项

SystemGuard 会监视、记录、报告和管理对 Windows 注册表或计算机上的重要系统文件进行的可能未经授权的更改。对注册表和文件进行未经授权的更改会损害您的计算机，危害其安全性并会损坏重要的系统文件。

计算机上的注册表和文件发生更改很常见，而且会定期发生。因为许多更改都是无害的，所以 SystemGuard 的默认设置配置为提供可靠的、智能的实时防护，抵御可能造成很大损害的未经授权的更改。例如，如果 SystemGuard 检测到不常见的更改并会造成可能的重大威胁，则系统会立即报告和记录此活动。系统也会记录很常见但仍会造成某些可能损害的更改。不过，默认情况下，系统会禁用对标准和低风险更改的监视。可以将 SystemGuard 技术配置为将其保护范围扩展到所需的任何环境。

下面是三种类型的 SystemGuard：程序 SystemGuard、Windows SystemGuard 和浏览器 SystemGuard。

程序 SystemGuard

程序 SystemGuard 会检测对计算机的注册表以及 Windows 的其他重要文件进行未经授权的更改。这些重要的注册表项和文件包括 ActiveX 安装、启动项目、Windows Shell 执行挂钩以及 Shell 服务对象延迟加载。通过对这些项目进行监视，Program SystemGuard 技术不仅可以阻止 Windows 启动时可自动启动的间谍软件和可能有害的程序，而且可以阻止可疑的 ActiveX 程序（从 Internet 下载）。

Windows SystemGuard

Windows SystemGuard 还会检测对您计算机的注册表以及 Windows 的其他重要文件进行未经授权的更改。这些重要的注册表项和文件包括上下文菜单处理程序、appInit DLLs 和 Windows Hosts 文件。通过监视这些项目，Windows SystemGuard 技术有助于防止计算机通过 Internet 发送和接收未经授权的信息或个人信息。它还帮助阻止可疑程序，这些程序会对您和您家人重要的程序的外观和行为进行有害的更改。

浏览器 SystemGuard

与程序和 Windows SystemGuard 类似，浏览器 SystemGuard 会检测对您计算机的注册表以及 Windows 的其他重要文件进行可能的未经授权的更改。不过，浏览器 SystemGuard 会监视对 Internet Explorer 加载项、Internet Explorer URL 和 Internet Explorer 安全区域等重要的注册表项和文件所进行的更改。通过监视这些项目，浏览器 SystemGuard 技术可以帮助防止未经授权的浏览器活动，如重定向到可疑网站、在您不知晓的情况下对浏览器设置和选项进行更改，以及信任可疑网站。

启用 SystemGuard 保护

启用 SystemGuard 保护可以检测计算机上可能未经授权的 Windows 注册表和文件更改，并提醒您。对注册表和文件进行未经授权的更改会损害您的计算机，危害其安全性并会损坏重要的系统文件。

1 打开“计算机和文件配置”窗格

如何实现？

1. 在左侧窗格上，单击“高级菜单”。
2. 单击“配置”。
3. 在“配置”窗格上，单击“计算机和文件”。

2 在“SystemGuard 保护”下，单击“开”。

注意：您可以单击“关”来禁用 SystemGuard 保护。

配置 SystemGuard 选项

使用“SystemGuard”窗格可以配置保护、记录和提醒选项，防止与 Windows 文件、程序和 Internet Explorer 关联的未经授权的注册表和文件更改。对注册表和文件进行未经授权的更改会损害您的计算机，危害其安全性并会损坏重要的系统文件。

1 打开“SystemGuard”窗格。

如何实现？

1. 在“常见任务”下，单击“主页”。
2. 在 SecurityCenter 的“主页”窗格上，单击“计算机和文件”。
3. 在“计算机和文件”信息区域中，单击“配置”。
4. 在“计算机和文件配置”窗格中，确保启用了 SystemGuard 保护，然后单击“高级”。

2 从列表中选择 SystemGuard 类型。

- 程序 SystemGuard
- Windows SystemGuard
- 浏览器 SystemGuard

3 在“我想”下，执行以下任一操作：

- 要检测、记录和报告与程序、Windows 和浏览器 SystemGuard 关联的未经授权的注册表和文件更改，请单击“显示警报”。
- 要检测和记录与程序、Windows 和浏览器 SystemGuard 关联的未经授权的注册表和文件更改，请单击“只记录更改”。
- 要禁用对与程序、Windows 和浏览器 SystemGuard 关联的未经授权的注册表和文件更改，请单击“禁用 SystemGuard”。

注意：有关 SystemGuard 类型的详细信息，请参阅关于 SystemGuard 类型 (第 51 页)。

关于 SystemGuard 类型

SystemGuard 会检测对您计算机的注册表以及 Windows 的其他重要文件进行可能未经授权的更改。下面是三种类型的 SystemGuard：程序 SystemGuard、Windows SystemGuard 和浏览器 SystemGuard

程序 SystemGuard

Program SystemGuard 技术不仅可以阻止 Windows 启动时启动的间谍软件和可能有害的程序，而且可以阻止可疑的 ActiveX 程序（从 Internet 下载的程序）。

SystemGuard	检测...
ActiveX 安装	对 ActiveX 安装进行未经授权的注册表更改，这些更改会损害您的计算机，危害其安全性并会损坏重要的系统文件。
启动项目	间谍软件、广告软件和其他可能有害的程序，这些程序可能对启动项目安装文件更改，从而在启动计算机时运行可疑程序。
Windows Shell 执行挂钩	间谍软件、广告软件和其他可能有害的程序，这些程序可能安装 Windows Shell 执行挂钩来阻止安全程序正常运行。
Shell 服务对象延迟加载	间谍软件、广告软件和其他可能有害的程序，这些程序可能对 Shell 服务对象延迟加载进行注册表更改，从而在启动计算机时运行有害文件。

Windows SystemGuard

Windows SystemGuard 技术有助于防止计算机通过 Internet 发送和接收未经授权的信息或个人信息。它还帮助阻止对您和您家人重要的程序的外观和行为进行可能有害的更改。

SystemGuard	检测...
上下文菜单处理程序	对 Windows 上下文菜单处理程序进行未经授权的注册表更改，这些更改可能会影响 Windows 菜单的外观和行为。使用上下文菜单可以对计算机执行操作，如右键单击文件。
AppInit DLLs	对 Windows AppInit DLLs 进行未经授权的注册表更改，这些更改可能会影响启动计算机时运行可能有害的文件。
Windows Hosts 文件	间谍软件、广告软件和其他可能有害的程序，这些程序可能对 Windows Hosts 文件进行未经授权的更改，使您的浏览器重定向到可疑网站并阻止软件更新。
Winlogon Shell	间谍软件、广告软件和其他可能有害的程序，这些程序可能对 Winlogon Shell 进行注册表更改，从而使其他程序替代 Windows Explorer。
Winlogon User Init	间谍软件、广告软件和其他可能有害的程序，这些程序可能对 Winlogon User Init 进行注册表更改，从而在您登录到 Windows 时运行可疑程序。
Windows 协议	间谍软件、广告软件和其他可能有害的程序，这些程序可能对 Windows Protocols 进行注册表更改，影响您的计算机在 Internet 上发送和接收信息的方式。
Winsock 分层服务提供者	间谍软件、广告软件和其他可能有害的程序，这些程序可能对 Winsock 分层服务提供者 (LSP) 安装注册表更改，以拦截和更改通过 Internet 发送和接收的信息。
Windows Shell Open Command	对 Windows Shell Open Commands 所进行的未经授权的更改，这些更改可能会使蠕虫和其他有害程序在计算机上运行。
共享任务计划程序	间谍软件、广告软件和其他可能有害的程序，这些程序可能对共享任务计划程序进行注册表和文件更改，从而在启动计算机时运行可能有害的文件。
Windows Messenger 服务	间谍软件、广告软件和其他可能有害的程序，这些程序可能对 Windows Messenger 服务进行注册表更改，使未经请求的广告和远程运行的程序在您计算机上运行。
Windows Win.ini 文件	间谍软件、广告软件和其他可能有害的程序，这些程序可能对 Win.ini 文件进行更改，从而在启动计算机时运行可疑程序。

浏览器 SystemGuard

浏览器 SystemGuard 技术可以帮助防止未经授权的浏览器活动，如重定向到可疑网站、在您不知晓的情况下对浏览器设置和选项进行更改，以及对可疑网站进行不必要的信任。

SystemGuard	检测...
浏览器辅助对象	间谍软件、广告软件和其他可能有害的程序，这些程序可能使用浏览器辅助对象跟踪 Web 浏览并显示未经请求的广告。
Internet Explorer 栏	对 Internet Explorer 栏程序（如“搜索”和“收藏夹”）进行未经授权的注册表更改，这些更改可能会影响 Internet Explorer 的外观和行为。
Internet Explorer 加载项	间谍软件、广告软件和其他可能有害的程序，这些程序可能安装 Internet Explorer 加载项来跟踪 Web 浏览并显示未经请求的广告。
Internet Explorer ShellBrowser	对 Internet Explorer Shell Browser 进行未经授权的注册表更改，这些更改可能会影响 Web 浏览器的外观和行为。
Internet Explorer WebBrowser	对 Internet Explorer Web 浏览器进行未经授权的注册表更改，这些更改可能会影响浏览器的外观和行为。
Internet Explorer URL 搜索挂钩	间谍软件、广告软件和其他可能有害的程序，这些程序可能对 Internet Explorer URL 搜索挂钩进行注册表更改，使浏览器在搜索 Web 时重定向到可疑的网站。
Internet Explorer URL	间谍软件、广告软件和其他可能有害的程序，这些程序可能对 Internet Explorer URL 进行注册表更改，从而影响浏览器设置。
Internet Explorer 限制	间谍软件、广告软件和其他可能有害的程序，这些程序可能对 Internet Explorer 限制进行注册表更改，从而影响浏览器设置和选项。
Internet Explorer 安全区域	间谍软件、广告软件和其他可能有害的程序，这些程序可能对 Internet Explorer 安全区域进行注册表更改，从而在启动计算机时运行可能有害的文件。
Internet Explorer 受信任的站点	间谍软件、广告软件和其他可能有害的程序，这些程序可能对 Internet Explorer 受信任的站点进行注册表更改，从而使浏览器信任可疑的网站。
Internet Explorer 策略	间谍软件、广告软件和其他可能有害的程序，这些程序可能对 Internet Explorer 策略进行注册表更改，从而影响浏览器的外观和行为。

使用可信列表

如果 VirusScan 检测到文件或注册表更改 (SystemGuard)、程序或缓冲区溢出，则会提示您信任或删除它。如果您信任此项目，并且指出您不想接收将来有关其活动的通知，则此项目会添加到信任列表中，而且 VirusScan 不再检测此项目或向您发送有关其活动的通知。如果已将某个项目添加到信任的列表，但决定要阻止其活动，则可以进行阻止。阻止操作会防止运行项目，或对您的计算机进行任何更改，而不会在每次尝试进行更改时通知您。您还可以从信任列表中删除项目。删除操作允许 VirusScan 再次检测项目活动。

管理可信列表

使用“可信列表”窗格可以信任或阻止以前已检测并信任的项目。您还可以从可信列表中删除项目，以便 VirusScan 再次对其进行检测。

1 打开“可信列表”窗格。

如何实现？

1. 在“常见任务”下，单击“主页”。
2. 在 SecurityCenter 的“主页”窗格上，单击“计算机和文件”。
3. 在“计算机和文件”信息区域中，单击“配置”。
4. 在“计算机和文件配置”窗格中，确保启用了病毒防护，然后单击“高级”。
5. 在“病毒防护”窗格中单击“可信列表”。

2 从下列信任列表类型中选择一个类型：

- 程序 SystemGuard
- Windows SystemGuard
- 浏览器 SystemGuard
- 可信的程序
- 可信的缓冲区溢出

3 在“我想”下，执行以下任一操作：

- 若要允许检测到的项目对计算机上的 Windows 注册表或重要系统文件进行更改而不通知您，请单击“信任”。
- 若要阻止检测到的项目对计算机上的 Windows 注册表或重要系统文件进行更改而不通知您，请单击“阻止”。
- 若要从可信列表中删除检测到的项目，请单击“删除”。

4 单击“确定”。

注意：有关可信列表类型的详细信息，请参阅关于可信列表类型 (第 55 页)。

关于可信列表类型

“可信列表”窗格中的 SystemGuard 表示, VirusScan 先前已检测未经授权的注册表和文件更改, 但您已从警报或“扫描结果”窗格中选择允许。您可以在“可信列表”窗格中管理的五种类型的信任列表类型: Program SystemGuard、Windows SystemGuard、浏览器 SystemGuard、可信的程序和可信的缓冲区溢出。

选项	说明
程序 SystemGuard	<p>“可信列表”窗格中的程序 SystemGuard 表示, VirusScan 先前已检测未经授权的注册表和文件更改, 但您已从警报或“扫描结果”窗格中选择允许。</p> <p>程序 SystemGuard 可以检测与 ActiveX 安装、启动项目、Windows Shell 执行挂钩、Shell 服务对象延迟加载相关的未经授权的注册表和文件更改。这些类型的未经授权的注册表和文件更改会损害您的计算机, 危害其安全性并会损坏重要的系统文件。</p>
Windows SystemGuard	<p>“可信列表”窗格中的 Windows SystemGuard 表示, VirusScan 先前已检测未经授权的注册表和文件更改, 但您已从警报或“扫描结果”窗格中选择允许。</p> <p>Windows SystemGuard 可以检测与上下文菜单处理程序、AppInit DLLs/Windows hosts 文件、Winlogon Shell、Winsock 分层服务提供者 (LSP) 等关联的未经授权的注册表和文件更改。这些类型的未经授权的注册表和文件更改可能会影响计算机通过 Internet 发送和接收信息的方式, 更改程序的外观和行为以及允许在计算机上运行可疑程序。</p>
浏览器 SystemGuard	<p>“可信列表”窗格中的浏览器 SystemGuard 表示, VirusScan 先前已检测未经授权的注册表和文件更改, 但您已从警报或“扫描结果”窗格中选择允许。</p> <p>浏览器 SystemGuard 可以检测与浏览器辅助对象、Internet Explorer 加载项、Internet Explorer URL、Internet Explorer 安全区域等相关的未经授权的注册表更改和其他有害行为。这些类型的未经授权的注册表更改可以产生有害的浏览器活动, 如重定向到可疑网站, 更改浏览器设置和选项以及信任可疑网站。</p>
可信的程序	可信程序是 VirusScan 先前检测到的可能有害的程序, 但您已从警报或“扫描结果”窗格中选择信任。

选项	说明
可信的缓冲区溢出	可信的缓冲区溢出表示，VirusScan 先前已检测到有害的程序，但您已从警报或“扫描结果”窗格中选择信任。 缓冲区溢出可能会损害计算机并损坏文件。在可疑程序或进程存储在缓冲区中的信息量超过缓冲区容量时，会发生缓冲区溢出。

第 3 章

McAfee Personal Firewall

Personal Firewall 可以为计算机和个人数据提供高级保护。它可以在您的计算机和 Internet 之间构筑一道屏障，悄无声息地监测 Internet 通讯是否存在可疑活动。

注意： 在检测到重要和不重要的问题时，SecurityCenter 都会立即报告。如果您需要帮助来诊断保护问题，则可以运行 McAfee Virtual Technician。

本章内容

Personal Firewall 功能.....	58
启动防火墙.....	59
使用警报.....	61
管理信息警报.....	63
配置防火墙保护.....	65
管理程序和权限.....	75
管理计算机连接.....	83
管理系统服务.....	91
记录、监视和分析.....	97
了解 Internet 安全性	107

Personal Firewall 功能

标准和自定义保护级别	使用防火墙的默认或可自定义保护设置防止入侵和可疑活动。
实时建议	动态接收建议，帮助您确定是否应允许程序访问 Internet，或是否应信任网络通讯。
对程序进行智能访问管理	通过警报和事件日志管理程序的 Internet 访问权限，以及配置特定程序的访问权限。
游戏保护	在玩全屏游戏期间，可以防止有关入侵尝试和可疑活动的警报分散您的注意力。
计算机启动保护	在 Windows® 启动后，保护您的计算机免受入侵尝试、有害程序以及网络通讯的侵扰。
系统服务端口控制	管理某些程序所需的打开和关闭的系统服务端口。
管理计算机连接	允许或阻止其他计算机与您计算机之间的远程连接。
HackerWatch 信息集成	通过 HackerWatch 网站跟踪全球黑客攻击和入侵模式，该网站还提供有关您计算机上程序的最新安全信息，以及提供全球安全事件和 Internet 端口统计信息。
锁定防火墙	立即阻止您的计算机与 Internet 之间的所有入站和出站通讯。
恢复防火墙	立即恢复防火墙的最初保护设置。
高级特洛伊木马程序检测	检测并阻止可能有恶意的应用程序（如特洛伊木马），以防个人数据发送到 Internet。
事件记录	跟踪最近的入站、出站和入侵事件。
监视 Internet 通讯	查看显示恶意攻击和通讯来源的世界地图。此外，该功能还会查找始发 IP 地址的所有者信息和地理数据。另外，它还分析入站和出站通讯，监视程序带宽使用情况和程序活动。
入侵防护	保护您的隐私免受可能的 Internet 威胁的侵扰。我们使用类似启发式的功能，通过阻止具有攻击症状或黑客攻击企图特征的项目来提供第三层保护。
高级通讯分析	查看入站和出站 Internet 通讯和程序连接，包括主动侦听打开连接的通讯和连接。此功能允许您了解易遭入侵的程序，并对这些程序采取措施。

启动防火墙

安装防火墙后，您的计算机便可以抵御入侵和有害网络通讯的侵扰。此外，您可以随时处理警报并管理已知和未知程序的入站和出站 Internet 访问权限。系统会自动启用“智能建议”和“自动”安全级别（选择此选项后可以允许程序具有仅出站 Internet 访问权限）。

虽然可以在“Internet 和网络配置”窗格中禁用防火墙，但您的计算机将无法抵御入侵和有害网络通讯的侵扰，并且无法有效管理入站和出站 Internet 连接。如果必须禁用防火墙保护，请将其临时禁用，而且只在有必要时才禁用。您还可以在“Internet 和网络配置”窗格中启用防火墙。

防火墙会自动禁用 Windows® 防火墙，并将自身设置为默认防火墙。

注意：要配置防火墙，请打开“Internet 和网络配置”窗格。

本章内容

启动防火墙保护.....	59
停止防火墙保护.....	59

启动防火墙保护

您可以启用防火墙以保护您的计算机免受入侵和有害网络通讯的侵扰，以及管理入站和出站 Internet 连接。

- 1 在“McAfee SecurityCenter”窗格上，单击“Internet 和网络”，然后单击“配置”。
- 2 在“Internet 和网络配置”窗格的“已禁用防火墙保护”下，单击“开”。

停止防火墙保护

如果您不想保护您的计算机免受入侵和有害网络通讯的侵扰，则可以禁用防火墙。如果禁用了防火墙，则不能管理入站或出站 Internet 连接。

- 1 在“McAfee SecurityCenter”窗格上，单击“Internet 和网络”，然后单击“配置”。
- 2 在“Internet 和网络配置”窗格的“已启用防火墙保护”下，单击“关”。

使用警报

防火墙使用一组警报来帮助您管理安全性。这些警报可以分为三种基本类型：

- 红色警报
- 黄色警报
- 绿色警报

警报还可以包含一些信息，帮助您确定如何处理警报或获取有关您计算机上运行程序的信息。

本章内容

关于警报	62
------------	----

关于警报

防火墙包含三种基本警报类型。有些警报包含的信息也可以帮助您了解或获得在您计算机上运行的程序的有关信息。

红色警报

当防火墙在计算机上检测到特洛伊木马程序时会显示红色警报，然后拦截特洛伊木马程序，并建议扫描其他威胁。特洛伊木马程序以合法程序的身份出现，但可能会破坏、损害您的计算机，并对您的计算机进行未经授权的访问。此警报会在每个安全级别出现。

黄色警报

最常见的警报类型是黄色警报，会将有关防火墙检测到的程序活动或网络事件的信息通知给您。发生此警报时，此警报会描述程序活动或网络事件，然后向您提供需要响应的一个或多个选项。例如，当安装防火墙的计算机连接到新网络时，会显示“新网络连接”警报。您可以指定要分配给这个新网络的信任级别，该信任级别随后将显示在“网络”列表中。如果“智能建议”处于启用状态，则会将已知程序自动添加到“程序权限”窗格中。

绿色警报

在大多数情况下，绿色警报提供有关事件的基本信息，且不需要响应。默认情况下，绿色警报处于禁用状态。

用户帮助

许多防火墙警报都包含其他信息来帮助您管理计算机的安全性，它包含以下各项：

- **了解有关此程序的更多信息：**连接到 McAfee 的全球安全网站，以获取防火墙已在您计算机上检测到的程序的有关信息。
- **通知 McAfee 有关此程序的信息：**将防火墙在计算机上检测到的有关未知文件的信息发送给 McAfee。
- **McAfee 推荐：**有关处理警报的建议。例如，警报可能建议您允许某个程序的访问权限。

管理信息警报

在某些事件期间（如玩全屏游戏时），如果防火墙检测到入侵尝试或可疑活动，则防火墙会允许您显示或隐藏信息警报。

本章内容

玩游戏时显示警报.....	63
隐藏信息警报.....	63

玩游戏时显示警报

在玩全屏游戏时，您可以允许防火墙在检测到入侵尝试或可疑活动时显示防火墙信息警报。

- 1 在“McAfee SecurityCenter”窗格上，单击“高级菜单”。
- 2 单击“配置”。
- 3 在“SecurityCenter 配置”窗格上，单击“警报”下的“高级”。
- 4 在“警报选项”窗格上，选中“当检测到游戏模式时显示信息警报”。
- 5 单击“确定”。

隐藏信息警报

您可以防止防火墙在检测到入侵尝试或可疑活动时显示防火墙信息警报。

- 1 在“McAfee SecurityCenter”窗格上，单击“高级菜单”。
- 2 单击“配置”。
- 3 在“SecurityCenter 配置”窗格上，单击“警报”下的“高级”。
- 4 在“SecurityCenter 配置”窗格上，单击“信息警报”。
- 5 在“信息警报”窗格上，执行以下任一操作：
 - 选择“不显示信息警报”以隐藏所有的信息警报。
 - 取消选择要隐藏的警报。
- 6 单击“确定”。

配置防火墙保护

防火墙提供一些方法来管理安全性以及定制您要响应安全事件和警报的方法。

首次安装防火墙后，您的计算机保护安全级别会设置为“自动”，而且允许程序具有仅出站 Internet 访问权限。不过，防火墙还提供了其他级别，范围从高度严格到高度宽松。

防火墙还使您有机会接收有关警报和程序的 Internet 访问权限的建议。

本章内容

管理防火墙安全级别.....	66
配置警报的“智能建议”.....	69
优化防火墙安全性.....	71
锁定和恢复防火墙.....	74

管理防火墙安全级别

防火墙的安全级别控制要管理和响应警报的程度。当它检测到有害网络通讯以及入站和出站 Internet 连接时会显示这些警报。默认情况下，防火墙的安全级别设置为“自动”，而且具有仅出站访问权限。

在设置“自动”安全级别且启用了“智能建议”后，黄色警报提供的选项可以允许或阻止需要入站访问权限的未知程序的访问。尽管绿色警报在默认情况下处于禁用状态，但是它们会在检测到已知程序后出现，而且会自动允许访问。允许访问权限会使程序创建出站连接并侦听未经请求的入站连接。

通常，安全级别越严格（如“隐匿”和“标准”），则所显示且必须由您处理的选项和警报数量就越多。

下表说明了防火墙的三个安全级别，依次为最严格的级别到最宽松的级别：

级别	说明
隐匿	阻止所有入站 Internet 连接（打开的端口除外），从而在 Internet 上隐藏您的计算机。防火墙会在新程序尝试进行出站 Internet 连接或接收入站连接请求时提示您。已阻止的程序和已添加的程序都会显示在“程序权限”窗格中。
标准	监视入站和出站连接，并在新程序尝试访问 Internet 时提示您。已阻止的程序和已添加的程序都会显示在“程序权限”窗格中。
自动	允许程序具有入站和出站（完全）访问权限或仅出站 Internet 访问权限。默认的安全级别为“自动”，选择此选项可以允许程序具有仅出站访问权限。 如果允许某个程序具有完全访问权限，则防火墙会自动信任此程序，并将其添加到“程序权限”窗格的允许程序列表中。 如果允许某个程序具有仅出站访问权限，则仅在该程序进行出站 Internet 连接时，防火墙才会自动信任此程序。入站连接不会自动被信任。

防火墙还允许在“恢复防火墙默认值”窗格中将安全级别立即重置为“自动”（并允许具有仅出站访问权限）。

将安全级别设置为“隐匿”

您可以将防火墙的安全级别设置为“隐匿”以阻止所有入站网络连接（打开的端口除外），从而在 Internet 上隐藏您的计算机。

- 1 在“McAfee SecurityCenter”窗格上，单击“Internet 和网络”，然后单击“配置”。
- 2 在“Internet 和网络配置”窗格的“已启用防火墙保护”下，单击“高级”。
- 3 在“安全级别”窗格上，移动滑块，直至“隐匿”显示为当前级别。
- 4 单击“确定”。

注意：在“隐匿”模式下，防火墙会在新程序请求出站 Internet 连接或接收入站连接请求时提醒您。

将安全级别设置为“标准”

您可以将安全级别设置为“标准”以监视入站和出站连接，并在新程序尝试访问 Internet 时提醒您。

- 1 在“McAfee SecurityCenter”窗格上，单击“Internet 和网络”，然后单击“配置”。
- 2 在“Internet 和网络配置”窗格的“已启用防火墙保护”下，单击“高级”。
- 3 在“安全级别”窗格上，移动滑块，直至“标准”显示为当前级别。
- 4 单击“确定”。

将安全级别设置为“自动”

您可以将防火墙的安全级别设置为“自动”以允许完全访问权限或仅出站网络访问权限。

- 1 在“McAfee SecurityCenter”窗格上，单击“Internet 和网络”，然后单击“配置”。
- 2 在“Internet 和网络配置”窗格的“已启用防火墙保护”下，单击“高级”。
- 3 在“安全级别”窗格上，移动滑块，直至“自动”显示为当前级别。
- 4 执行下面某项操作：
 - 要允许完全入站和出站网络访问权限，请选择“允许完全访问”。
 - 要允许仅出站网络访问权限，请选择“仅允许出站访问”。

5 单击“确定”。

注意: “仅允许出站访问”是默认选项。

配置警报的“智能建议”

您可以将防火墙配置为在任何程序尝试访问 Internet 时在警报中包含、排除或显示建议。启用“智能建议”有助于确定如何处理警报。

如果应用了“智能建议”（且安全级别设为“自动”，启用了仅出站访问权限），则防火墙会自动允许已知的程序，并阻止可能有危险的程序。

如果未应用“智能建议”，则防火墙既不会允许或阻止 Internet 访问，也不会在警报中提供建议。

如果将“智能建议”设为“显示”时，则出现的警报会提示您允许或阻止访问，而且防火墙会在警报中提供建议。

启用“智能建议”

您可以为防火墙启用“智能建议”以自动允许或阻止程序，以及在出现有关无法识别的和可能有危险的程序时提醒您。

- 1 在“McAfee SecurityCenter”窗格上，单击“Internet 和网络”，然后单击“配置”。
- 2 在“Internet 和网络配置”窗格的“已启用防火墙保护”下，单击“高级”。
- 3 在“安全级别”窗格的“智能建议”下，选择“应用智能建议”。
- 4 单击“确定”。

禁用“智能建议”

您可以为防火墙禁用“智能建议”以允许或阻止程序，以及在出现有关无法识别的和可能有危险的程序时提醒您。不过，这些警报不包含有关处理程序访问权限的任何建议。如果防火墙检测到新程序可疑或已知是可能的威胁，则它会自动阻止此程序访问 Internet。

- 1 在“McAfee SecurityCenter”窗格上，单击“Internet 和网络”，然后单击“配置”。
- 2 在“Internet 和网络配置”窗格的“已启用防火墙保护”下，单击“高级”。
- 3 在“安全级别”窗格的“智能建议”下，选择“不应用智能建议”。
- 4 单击“确定”。

显示智能建议

您可以显示“智能建议”，以便仅在警报中显示建议，从而使您可以确定允许或阻止无法识别和可能有危险的程序。

- 1** 在“McAfee SecurityCenter”窗格上，单击“Internet 和网络”，然后单击“配置”。
- 2** 在“Internet 和网络配置”窗格的“已启用防火墙保护”下，单击“高级”。
- 3** 在“安全级别”窗格的“智能建议”下，选择“显示智能建议”。
- 4** 单击“确定”。

优化防火墙安全性

有许多方法可以损害计算机的安全性。例如，某些程序可能会在 Windows® 启动时尝试连接到 Internet。此外，有经验的计算机用户也可以跟踪（或 ping）您的计算机，以确定它是否连接到网络上。而且，他们会使用 UDP 协议，以消息单元（数据报）形式向您的计算机发送信息。防火墙允许您阻止程序在 Windows 启动时访问 Internet，允许您阻止其他用户用来在网络上检测您的计算机的 ping 请求，允许您禁止其他用户以消息单元（数据报）形式向您的计算机发送信息，从而保护您的计算机免受这些类型的入侵。

标准安装设置包括自动检测最常见的入侵尝试，例如拒绝服务攻击或漏洞利用。使用标准安装设置会确保您能抵御这些攻击和扫描；不过，可以在“入侵检测”窗格上，禁用对一个或多个攻击或扫描进行自动检测。

启动过程中保护计算机

您可以在 Windows 启动时阻止以前启动时没有但现在需要 Internet 访问权限的新程序来保护您的计算机。防火墙会显示已请求访问 Internet 的程序的相关警报，您可以允许或阻止此访问。

- 1 在“McAfee SecurityCenter”窗格上，单击“Internet 和网络”，然后单击“配置”。
- 2 在“Internet 和网络配置”窗格的“已启用防火墙保护”下，单击“高级”。
- 3 在“安全级别”窗格的“安全设置”下，选择“在 Windows 启动时启用保护”。
- 4 单击“确定”。

注意：在启用启动时保护后，不记录已阻止的连接和入侵。

配置 ping 请求设置

您可以允许或阻止网络上其他计算机用户检测您的计算机。

- 1 在“McAfee SecurityCenter”窗格上，单击“Internet 和网络”，然后单击“配置”。
- 2 在“Internet 和网络配置”窗格的“已启用防火墙保护”下，单击“高级”。
- 3 在“安全级别”窗格的“安全设置”下，执行以下任一操作：
 - 选中“允许 ICMP ping 请求”以允许使用 ping 请求检测您的计算机是否在网络上。
 - 清除“允许 ICMP ping 请求”以禁止使用 ping 请求在网络上检测您的计算机。

4 单击“确定”。

配置 UDP 设置

您可以允许其他网络计算机用户使用 UDP 协议向您的计算机发送消息单元（数据报）。但是，只有当您同时关闭了系统服务端口以阻止此协议后，才能这样做。

- 1** 在“McAfee SecurityCenter”窗格上，单击“Internet 和网络”，然后单击“配置”。
- 2** 在“Internet 和网络配置”窗格的“已启用防火墙保护”下，单击“高级”。
- 3** 在“安全级别”窗格的“安全设置”下，执行以下任一操作：
 - 选择“启用 UDP 跟踪”可允许其他计算机用户向您的计算机发送消息单元（数据报）。
 - 清除“启用 UDP 跟踪”可禁止其他计算机用户向您的计算机发送消息单元（数据报）。
- 4** 单击“确定”。

配置入侵检测

您可以检测入侵尝试来保护计算机免遭攻击或未经授权的扫描。标准防火墙设置包括对最常见入侵尝试（如拒绝服务攻击或利用漏洞）的自动检测，不过，您可以禁用对一个或多个攻击或扫描的自动检测。

- 1** 在“McAfee SecurityCenter”窗格上，单击“Internet 和网络”，然后单击“配置”。
- 2** 在“Internet 和网络配置”窗格的“已启用防火墙保护”下，单击“高级”。
- 3** 在“防火墙”窗格上，单击“入侵检测”。
- 4** 在“检测入侵尝试”下，执行以下任一操作：
 - 选中名称以自动检测攻击或扫描。
 - 清除名称以禁用自动检测攻击或扫描。
- 5** 单击“确定”。

配置防火墙的“保护状态”设置

您可以将防火墙配置为忽略计算机上没有报告给 SecurityCenter 的特定问题。

- 1** 在“McAfee SecurityCenter”窗格的“SecurityCenter 信息”下，单击“配置”。
- 2** 在“SecurityCenter 配置”窗格的“保护状态”下，单击“高级”。
- 3** 在“忽略的问题”窗格中，选择下列一个或多个选项：
 - 已禁用防火墙保护。

- 防火墙服务没有运行。
- 您的计算机未安装防火墙保护。
- 已禁用您的 Windows 防火墙。
- 您的计算机未安装出站防火墙。

4 单击“确定”。

锁定和恢复防火墙

“锁定”会立即阻止所有入站和出站网络连接，包括对网站、电子邮件和安全更新的访问。“锁定”与断开计算机的网络电缆等效。可以使用此设置来阻止“系统服务”窗格上已打开的端口并帮助您隔离和解决计算机问题。

立即锁定防火墙

您可以立即锁定防火墙以阻止您的计算机和任何网络(包括 Internet)之间的所有网络通讯。

- 1 在“McAfee SecurityCenter”窗格的“常见任务”下，单击“锁定防火墙”。
- 2 在“锁定防火墙”窗格上，单击“启用‘锁定防火墙’”。
- 3 单击“是”进行确认。

提示: 您还可以右键单击任务栏最右侧通知区域中的 SecurityCenter 图标 ，依次单击“快速链接”、“锁定防火墙”来锁定防火墙。

立即解锁防火墙

您可以立即对防火墙解锁以允许您的计算机和任何网络（包括 Internet）之间的所有网络通讯。

- 1 在“McAfee SecurityCenter”窗格的“常见任务”下，单击“锁定防火墙”。
- 2 在“已启用锁定”窗格上，单击“禁用‘锁定防火墙’”。
- 3 单击“是”进行确认。

恢复防火墙设置

您可以快速将防火墙恢复到其最初的保护设置。这会将安全级别重置为“自动”，并允许仅出站网络访问权限，启用“智能建议”，恢复“程序权限”窗格中默认程序及其权限的列表，删除信任和禁止的 IP 地址，以及恢复系统服务、事件日志设置和入侵检测。

- 1 在“McAfee SecurityCenter”窗格上，单击“恢复防火墙默认值”。
- 2 在“恢复防火墙保护默认值”窗格上，单击“恢复默认值”。
- 3 单击“是”进行确认。
- 4 单击“确定”。

管理程序和权限

防火墙允许为需要入站和出站 Internet 访问权限的现有程序和新程序管理和创建访问权限。防火墙允许控制程序的完全或仅出站访问权限。您还可以阻止程序的访问权限。

本章内容

允许程序访问 Internet	76
允许程序具有仅出站访问权限	78
阻止程序的 Internet 访问权限	79
删除程序的访问权限	81
了解程序	82

允许程序访问 Internet

某些程序（如 Internet 浏览器）需要访问 Internet 才能正常工作。

防火墙允许使用“程序权限”页：

- 允许程序具有访问权限
- 允许程序具有仅出站访问权限
- 阻止程序访问

您还可以在“出站事件”和“最新事件”日志中允许程序具有完全和仅出站 Internet 访问权限。

允许程序具有完全访问权限

您可以允许计算机上现有的已阻止程序具有完全入站和出站 Internet 访问权限。

- 1 在“McAfee SecurityCenter”窗格上，单击“Internet 和网络”，然后单击“配置”。
- 2 在“Internet 和网络配置”窗格的“已启用防火墙保护”下，单击“高级”。
- 3 在“防火墙”窗格上，单击“程序权限”。
- 4 在“程序权限”下，选择权限为“已阻止”或“仅出站访问”的程序。
- 5 在“操作”下，单击“允许访问”。
- 6 单击“确定”。

允许新程序具有完全访问权限

您可以允许计算机上的新程序具有完全入站和出站 Internet 访问权限。

- 1 在“McAfee SecurityCenter”窗格上，单击“Internet 和网络”，然后单击“配置”。
- 2 在“Internet 和网络配置”窗格的“已启用防火墙保护”下，单击“高级”。
- 3 在“防火墙”窗格上，单击“程序权限”。
- 4 在“程序权限”下，单击“添加允许的程序”。
- 5 在“添加程序”对话框中，浏览并选择要添加的程序，然后单击“打开”。

注意：您可以像更改现有程序的权限一样更改新添加程序的权限，方法是先选择程序，然后单击“操作”下的“仅允许出站访问”或“阻止访问”。

从“最新事件”日志中允许完全访问权限

您可以允许“最近事件”日志中显示的现有已阻止程序具有完全入站和出站 Internet 访问权限。

- 1** 在“McAfee SecurityCenter”窗格上，单击“高级菜单”。
- 2** 单击“报告和日志”。
- 3** 在“最新事件”下，选择事件说明，然后单击“允许访问”。
- 4** 在“程序权限”对话框中，单击“是”确认。

相关主题

- 查看出站事件 (第 99 页)

从“出站事件”日志中允许完全访问权限

您可以允许“出站事件”日志中显示的现有已阻止程序具有完全入站和出站 Internet 访问权限。

- 1** 在“McAfee SecurityCenter”窗格上，单击“高级菜单”。
- 2** 单击“报告和日志”。
- 3** 在“最新事件”下，单击“查看日志”。
- 4** 单击“Internet 和网络”，然后单击“出站事件”。
- 5** 选择程序，然后在“我想”下，单击“允许访问”。
- 6** 在“程序权限”对话框中，单击“是”确认。

允许程序具有仅出站访问权限

计算机上的某些程序需要出站 Internet 访问权限。防火墙允许配置程序权限以允许仅出站 Internet 访问权限。

允许程序具有仅出站访问权限

您可以允许程序具有仅出站 Internet 访问权限。

- 1** 在“McAfee SecurityCenter”窗格上，单击“Internet 和网络”，然后单击“配置”。
- 2** 在“Internet 和网络配置”窗格的“已启用防火墙保护”下，单击“高级”。
- 3** 在“防火墙”窗格上，单击“程序权限”。
- 4** 在“程序权限”下，选择权限为“已阻止”或“完全访问”的程序。
- 5** 在“操作”下，单击“仅允许出站访问”。
- 6** 单击“确定”。

从“最新事件”日志中允许仅出站访问权限

您可以允许“最近事件”日志中显示的现有已阻止程序具有完全入站和出站 Internet 访问权限。

- 1** 在“McAfee SecurityCenter”窗格上，单击“高级菜单”。
- 2** 单击“报告和日志”。
- 3** 在“最新事件”下，选择事件说明，然后单击“仅允许出站访问”。
- 4** 在“程序权限”对话框中，单击“是”确认。

从“出站事件”日志允许仅出站访问权限

您可以允许“出站事件”日志中显示的现有已阻止程序具有仅出站 Internet 访问权限。

- 1** 在“McAfee SecurityCenter”窗格上，单击“高级菜单”。
- 2** 单击“报告和日志”。
- 3** 在“最新事件”下，单击“查看日志”。
- 4** 单击“Internet 和网络”，然后单击“出站事件”。
- 5** 选择程序，然后在“我想”下，单击“仅允许出站访问”。
- 6** 在“程序权限”对话框中，单击“是”确认。

阻止程序的 Internet 访问权限

防火墙允许阻止程序访问 Internet。确保对程序执行阻止操作将不会中断您的网络连接，或不会中断需要访问 Internet 才能正常工作的其他程序。

阻止程序具有访问权限

您可以阻止程序具有入站和出站 Internet 访问权限。

- 1 在“McAfee SecurityCenter”窗格上，单击“Internet 和网络”，然后单击“配置”。
- 2 在“Internet 和网络配置”窗格的“已启用防火墙保护”下，单击“高级”。
- 3 在“防火墙”窗格上，单击“程序权限”。
- 4 在“程序权限”下，选择权限为“完全访问”或“仅出站访问”的程序。
- 5 在“操作”下，单击“阻止访问”。
- 6 单击“确定”。

阻止新程序的访问权限

您可以阻止新程序具有入站和出站 Internet 访问权限。

- 1 在“McAfee SecurityCenter”窗格上，单击“Internet 和网络”，然后单击“配置”。
- 2 在“Internet 和网络配置”窗格的“已启用防火墙保护”下，单击“高级”。
- 3 在“防火墙”窗格上，单击“程序权限”。
- 4 在“程序权限”下，单击“添加阻止的程序”。
- 5 在“添加程序”对话框中，浏览并选择要添加的程序，然后单击“打开”。

注意：您可以更改新添加程序的权限，方法是先选择程序，然后单击“操作”下的“仅允许出站访问”或“允许访问”。

从“最新事件”日志阻止访问权限

您可以阻止“最新事件”日志中显示的程序具有入站和出站 Internet 访问权限。

- 1** 在“McAfee SecurityCenter”窗格上，单击“高级菜单”。
- 2** 单击“报告和日志”。
- 3** 在“最新事件”下，选择事件说明，然后单击“阻止访问”。
- 4** 在“程序权限”对话框中，单击“是”确认。

删除程序的访问权限

删除程序的权限之前，确保缺少此权限不会影响计算机的功能或网络链接。

删除程序权限

您可以删除程序的入站和出站 Internet 访问权限。

- 1** 在“McAfee SecurityCenter”窗格上，单击“Internet 和网络”，然后单击“配置”。
- 2** 在“Internet 和网络配置”窗格的“已启用防火墙保护”下，单击“高级”。
- 3** 在“防火墙”窗格上，单击“程序权限”。
- 4** 在“程序权限”下，选择程序。
- 5** 在“操作”下，单击“删除程序权限”。
- 6** 单击“确定”。

注意：防火墙会禁止通过使某些操作变灰以及将其禁用来修改某些程序。

了解程序

如果您不确定所要应用的程序权限，可以在 McAfee 的 HackerWatch 网站上获取有关程序的信息。

获取程序信息

您可以从 McAfee 的 HackerWatch 网站获取程序信息，以确定是允许还是阻止入站或出站 Internet 访问权限。

注意：确保已连接到 Internet，以便浏览器可以连接到 McAfee 的 HackerWatch 网站，此网站提供有关程序、Internet 访问要求和安全威胁的最新信息。

- 1** 在“McAfee SecurityCenter”窗格上，单击“Internet 和网络”，然后单击“配置”。
- 2** 在“Internet 和网络配置”窗格的“已启用防火墙保护”下，单击“高级”。
- 3** 在“防火墙”窗格上，单击“程序权限”。
- 4** 在“程序权限”下，选择程序。
- 5** 在“操作”下，单击“了解更多”。

从“出站事件”日志获取程序信息

在“出站事件”日志中，您可以从 McAfee 的 HackerWatch 网站获取程序信息，以确定允许或阻止入站和出站 Internet 访问权限的程序。

注意：确保已连接到 Internet，以便浏览器可以连接到 McAfee 的 HackerWatch 网站，此网站提供有关程序、Internet 访问要求和安全威胁的最新信息。

- 1** 在“McAfee SecurityCenter”窗格上，单击“高级菜单”。
- 2** 单击“报告和日志”。
- 3** 在“最新事件”下，然后单击“查看日志”。
- 4** 单击“Internet 和网络”，然后单击“出站事件”。
- 5** 选择 IP 地址，然后单击“了解更多”。

管理计算机连接

您可以根据与远程计算机相关联的 Internet 协议地址 (IP) 创建规则，将防火墙配置为管理与您计算机的特定远程连接。可以信任与信任 IP 地址相关联的计算机连接到您的计算机，而 IP 未知、可疑或不信任的计算机禁止连接到您的计算机。

当允许连接时，请确保您信任的计算机是安全的。如果您信任的计算机通过蠕虫或其他机制感染了病毒，您的计算机可能会易受感染。另外，McAfee 还建议您信任的计算机应受防火墙和最新防病毒程序的保护。防火墙并不记录来自“网络”列表中的受信任 IP 地址的通讯，也不为其生成事件警报。

可以禁止与未知、可疑或不信任 IP 相关联的计算机连接到您的计算机。

因为防火墙会禁止所有有害的通讯，所以通常不需要禁止 IP 地址。仅当您确信某个 Internet 连接会构成威胁时，才应禁止此 IP 地址。请确保您没有阻止重要的 IP 地址，例如，DNS 或 DHCP 服务器，或与 ISP 有关的其他服务器。

本章内容

关于计算机连接.....	84
禁止计算机连接.....	88

关于计算机连接

计算机连接是指在您的计算机与任何网络上的其他计算机之间所建立的连接。您可以在“网络”列表中添加、编辑和删除 IP 地址。这些 IP 地址与在连接到您的计算机时要为其分配信任级别的网络相关联：信任、标准和公用。

级别	说明
信任	防火墙允许来自某个 IP 的通讯通过任何端口到达您的计算机。防火墙不会过滤或分析与信任 IP 地址相关联的计算机和您计算机之间的活动。默认情况下，防火墙所找到的第一个专用网络会在“网络”列表中列为“信任”。本地网络或家庭网络中的一台或多台计算机就是“信任”网络的例子。
标准	在某个 IP 连接到您的计算机时，防火墙控制来自该 IP 的（而不是来自该网络中的任何其他计算机）的通讯，并根据“系统服务”列表中的规则允许或阻止它。防火墙记录通讯并根据标准 IP 地址生成事件警报。企业网络中的一台或多台计算机就是“标准”网络的一个例子。
公用	防火墙根据“系统服务”列表中的规则控制来自公用网络的通讯。咖啡馆、旅馆或机场中的 Internet 网络就是“公用”网络的一个例子。

当允许连接时，请确保您信任的计算机是安全的。如果您信任的计算机通过蠕虫或其他机制感染了病毒，您的计算机可能会易受感染。另外，McAfee 还建议您信任的计算机应受防火墙和最新防病毒程序的保护。

添加计算机连接

您可以添加信任、标准或公用的计算机连接及其关联的 IP 地址。

- 1 在“McAfee SecurityCenter”窗格上，单击“Internet 和网络”，然后单击“配置”。
- 2 在“Internet 和网络配置”窗格的“已启用防火墙保护”下，单击“高级”。
- 3 在“防火墙”窗格上，单击“网络”。
- 4 在“网络”窗格上，单击“添加”。
- 5 如果该计算机连接位于 IPv6 网络上，请选中“IPv6”复选框。
- 6 在“添加规则”下，执行以下任一操作：
 - 选择“单个”，然后在“IP 地址”框中输入 IP 地址。
 - 选择“范围”，然后在“自 IP 地址”和“至 IP 地址”框中，输入开始 IP 地址和结束 IP 地址。如果您的计算机连接位于 IPv6 网络上，请在“自 IP 地址”和“前缀长度”框中分别输入开始 IP 地址和前缀长度。

7 在“类型”下，执行以下任一操作：

- 选择“信任”可指定该计算机连接接受信任（例如，位于家庭网络中的计算机）。
- 选择“标准”可指定该计算机连接（而不是其所在网络中的其他计算机）受信任（例如，位于企业网络中的计算机）。
- 选择“公用”可指定该计算机连接是公用的（例如，位于网吧、旅馆或机场中的计算机）。

8 如果系统服务使用 Internet 连接共享 (ICS)，则可以添加下列 IP 地址范围：192.168.0.1 到 192.168.0.255。

9（可选）选中“规则过期时间”，然后输入实施此规则的天数。

10（可选）键入规则的说明。

11 单击“确定”。

注意：有关 Internet 连接共享 (ICS) 的详细信息，请参阅“配置新系统服务”。

从“入站事件”日志中添加计算机

您可以从“入站事件”日志中添加信任的或标准的计算机连接及其关联的 IP 地址。

1 在“McAfee SecurityCenter”窗格的“常见任务”窗格上下，单击“高级菜单”。

2 单击“报告和日志”。

3 在“最新事件”下，单击“查看日志”。

4 单击“Internet 和网络”，然后单击“入站事件”。

5 选择一个源 IP 地址，然后在“我想”下，执行以下任一操作：

- 单击“将此 IP 添加为‘信任’”，以便在“网络”列表中将该计算机添加为“信任”。
- 单击“将此 IP 添加为‘标准’”，以便在“网络”列表中将该计算机连接添加为“标准”。

6 单击“是”进行确认。

编辑计算机连接

您可以编辑信任、标准或公用的计算机连接及其关联的 IP 地址。

- 1 在“McAfee SecurityCenter”窗格上，单击“Internet 和网络”，然后单击“配置”。
- 2 在“Internet 和网络配置”窗格的“已启用防火墙保护”下，单击“高级”。
- 3 在“防火墙”窗格上，单击“网络”。
- 4 在“网络”窗格上，选择 IP 地址，然后单击“编辑”。
- 5 如果该计算机连接位于 IPv6 网络上，请选中“IPv6”复选框。
- 6 在“编辑规则”下，执行以下任一操作：
 - 选择“单个”，然后在“IP 地址”框中输入 IP 地址。
 - 选择“范围”，然后在“自 IP 地址”和“至 IP 地址”框中，输入开始 IP 地址和结束 IP 地址。如果您的计算机连接位于 IPv6 网络上，请在“自 IP 地址”和“前缀长度”框中分别输入开始 IP 地址和前缀长度。
- 7 在“类型”下，执行以下任一操作：
 - 选择“信任”可指定该计算机连接接受信任（例如，位于家庭网络中的计算机）。
 - 选择“标准”可指定该计算机连接（而不是其所在网络中的其他计算机）受信任（例如，位于企业网络中的计算机）。
 - 选择“公用”可指定该计算机连接是公用的（例如，位于网吧、旅馆或机场中的计算机）。
- 8 （可选）选中“规则过期时间”，并输入实施此规则的天数。
- 9 （可选）键入规则的说明。
- 10 单击“确定”。

注意：您不能编辑防火墙从信任专用网络中自动添加的默认计算机连接。

删除计算机连接

您可以删除信任、标准或公用的计算机连接及其关联的 IP 地址。

- 1** 在“McAfee SecurityCenter”窗格上，单击“Internet 和网络”，然后单击“配置”。
- 2** 在“Internet 和网络配置”窗格的“已启用防火墙保护”下，单击“高级”。
- 3** 在“防火墙”窗格上，单击“网络”。
- 4** 在“网络”窗格上，选择 IP 地址，然后单击“删除”。
- 5** 单击“是”进行确认。

禁止计算机连接

您可以在“禁止的 IP”窗格中添加、编辑和删除禁止的 IP 地址。

可以禁止与未知、可疑或不信任 IP 相关联的计算机连接到您的计算机。

因为防火墙会禁止所有有害的通讯，所以通常不需要禁止 IP 地址。仅当您确信某个 Internet 连接会构成威胁时，才应禁止此 IP 地址。请确保您没有阻止重要的 IP 地址，例如，DNS 或 DHCP 服务器，或与 ISP 有关的其他服务器。

添加禁止的计算机连接

您可以添加禁止的计算机连接及其关联的 IP 地址。

注意：确保您没有阻止重要的 IP 地址，例如，DNS 或 DHCP 服务器或与 ISP 有关的其他服务器。

- 1** 在“McAfee SecurityCenter”窗格上，单击“Internet 和网络”，然后单击“配置”。
- 2** 在“Internet 和网络配置”窗格的“已启用防火墙保护”下，单击“高级”。
- 3** 在“防火墙”窗格上，单击“禁止的 IP”。
- 4** 在“禁止的 IP”窗格上，单击“添加”。
- 5** 如果该计算机连接位于 IPv6 网络上，请选中“IPv6”复选框。
- 6** 在“添加规则”下，执行以下任一操作：
 - 选择“单个”，然后在“IP 地址”框中输入 IP 地址。
 - 选择“范围”，然后在“自 IP 地址”和“至 IP 地址”框中，输入开始 IP 地址和结束 IP 地址。如果您的计算机连接位于 IPv6 网络上，请在“自 IP 地址”和“前缀长度”框中分别输入开始 IP 地址和前缀长度。
- 7** (可选) 选中“规则过期时间”，然后输入实施此规则的天数。
- 8** (可选) 键入规则的说明。
- 9** 单击“确定”。
- 10** 单击“是”进行确认。

编辑禁止的计算机连接

您可以编辑禁止的计算机连接及其关联的 IP 地址。

- 1 在“McAfee SecurityCenter”窗格上，单击“Internet 和网络”，然后单击“配置”。
- 2 在“Internet 和网络配置”窗格的“已启用防火墙保护”下，单击“高级”。
- 3 在“防火墙”窗格上，单击“禁止的 IP”。
- 4 在“禁止的 IP”窗格上，单击“编辑”。
- 5 如果该计算机连接位于 IPv6 网络上，请选中“IPv6”复选框。
- 6 在“编辑规则”下，执行以下任一操作：
 - 选择“单个”，然后在“IP 地址”框中输入 IP 地址。
 - 选择“范围”，然后在“自 IP 地址”和“至 IP 地址”框中，输入开始 IP 地址和结束 IP 地址。如果您的计算机连接位于 IPv6 网络上，请在“自 IP 地址”和“前缀长度”框中分别输入开始 IP 地址和前缀长度。
- 7（可选）选中“规则过期时间”，然后输入实施此规则的天数。
- 8（可选）键入规则的说明。
- 9 单击“确定”。

删除禁止的计算机连接

您可以删除禁止的计算机连接及其关联的 IP 地址。

- 1 在“McAfee SecurityCenter”窗格上，单击“Internet 和网络”，然后单击“配置”。
- 2 在“Internet 和网络配置”窗格的“已启用防火墙保护”下，单击“高级”。
- 3 在“防火墙”窗格上，单击“禁止的 IP”。
- 4 在“禁止的 IP”窗格上，选择 IP 地址，然后单击“删除”。
- 5 单击“是”进行确认。

从“入站事件”日志禁止计算机

您可以从“入站事件”日志中禁止计算机连接及其关联的 IP 地址。该日志列出了所有 Internet 入站通讯的 IP 地址，可以使用该日志禁止可疑的或有害的 Internet 活动的源 IP 地址。

如果您希望阻止来自该 IP 地址的所有入站 Internet 通讯，则可以将该 IP 地址添加到“禁止的 IP”列表，而与您的“系统服务”端口是否已打开无关。

- 1 在“McAfee SecurityCenter”窗格的“常见任务”下，单击“高级菜单”。
- 2 单击“报告和日志”。
- 3 在“最新事件”下，单击“查看日志”。
- 4 单击“Internet 和网络”，然后单击“入站事件”。
- 5 选择源 IP 地址，然后在“我想”下单击“禁止此 IP”。
- 6 单击“是”进行确认。

从“入侵检测事件”日志中禁止计算机

您可以从“入侵检测事件”日志中禁止计算机连接及其关联的 IP 地址。

- 1 在“McAfee SecurityCenter”窗格的“常见任务”下，单击“高级菜单”。
- 2 单击“报告和日志”。
- 3 在“最新事件”下，单击“查看日志”。
- 4 单击“Internet 和网络”，然后单击“入侵检测事件”。
- 5 选择源 IP 地址，然后在“我想”下单击“禁止此 IP”。
- 6 单击“是”进行确认。

管理系统服务

某些程序(包括 Web 服务器和文件共享服务器程序)要能正常运行,必须通过指定的系统服务端口接受来自其他计算机的未经请求的连接。通常,防火墙会关闭这些系统服务端口,因为这些是系统中最容易受到攻击的端口。不过,要接受来自远程计算机的连接,必须打开系统服务端口。

本章内容

配置系统服务端口	92
----------------	----

配置系统服务端口

可以将系统服务端口配置为允许或阻止对计算机上服务的远程网络访问权限。对于在“网络”列表中列为“信任”、“标准”或“公用”的计算机，这些系统服务端口可以处于打开或关闭状态。

下面的列表显示常见的系统服务及其关联的端口：

- 常用的操作系统端口 5357
- 文件传输协议 (FTP) 端口 20-21
- 邮件服务器 (IMAP) 端口 143
- 邮件服务器 (POP3) 端口 110
- 邮件服务器 (SMTP) 端口 25
- Microsoft Directory Server (MSFT DS) 端口 445
- Microsoft SQL Server (MSFT SQL) 端口 1433
- 网络时间协议端口 123
- 远程桌面/远程协助/终端服务器 (RDP) 端口 3389
- 远程过程调用 (RPC) 端口 135
- 安全 Web 服务器 (HTTPS) 端口 443
- 通用即插即用 (UPNP) 端口 5000
- Web 服务器 (HTTP) 端口 80
- Windows 文件共享 (NETBIOS) 端口 137-139

还可以将系统服务端口配置为允许某台计算机与通过同一网络连接到它的其他计算机共享 Internet 连接。此连接（称为 Internet 连接共享 (ICS)）允许共享连接的计算机充当其他联网计算机连接到 Internet 的网关。

注意：如果您的计算机装有接受 Web 或 FTP 服务器连接的应用程序，共享连接的计算机可能需要打开关联的系统服务端口，并允许转发这些端口的入站连接。

允许访问现有的系统服务端口

您可以打开现有的端口来允许对计算机上的系统服务进行远程网络访问。

注意: 打开的系统服务端口会使计算机易遭 Internet 安全威胁的攻击，因此只有在必要时才打开端口。

- 1 在“McAfee SecurityCenter”窗格上，单击“Internet 和网络”，然后单击“配置”。
- 2 在“Internet 和网络配置”窗格的“已启用防火墙保护”下，单击“高级”。
- 3 在“防火墙”窗格上，单击“系统服务”。
- 4 在“打开系统服务端口”下，选择要打开其端口的系统服务。
- 5 单击“编辑”。
- 6 执行下面某项操作：
 - 要对于信任、标准或公用网络（例如，家庭网络、企业网络或 Internet 网络）上的任何计算机打开该端口，请选择“信任、标准和公用”。
 - 要对于标准网络（例如，企业网络）上的任何计算机打开该端口，请选择“标准(包括信任)”。
- 7 单击“确定”。

阻止访问现有的系统服务端口

您可以关闭现有的端口来阻止对您计算机上的系统服务进行远程网络访问。

- 1 在“McAfee SecurityCenter”窗格上，单击“Internet 和网络”，然后单击“配置”。
- 2 在“Internet 和网络配置”窗格的“已启用防火墙保护”下，单击“高级”。
- 3 在“防火墙”窗格上，单击“系统服务”。
- 4 在“打开系统服务端口”下，清除要关闭的系统服务端口旁边的复选框。
- 5 单击“确定”。

配置新系统服务端口

您可以在计算机上配置新网络服务端口，然后可以打开或关闭此端口来允许或阻止对计算机的远程访问。

- 1 在“McAfee SecurityCenter”窗格上，单击“Internet 和网络”，然后单击“配置”。
- 2 在“Internet 和网络配置”窗格的“已启用防火墙保护”下，单击“高级”。
- 3 在“防火墙”窗格上，单击“系统服务”。
- 4 单击“添加”。
- 5 在“系统服务”窗格的“添加系统服务规则”下，输入以下内容：
 - 系统服务名称
 - 系统服务类别
 - 本地 TCP/IP 端口
 - 本地 UDP 端口
- 6 执行下面某项操作：
 - 要对于信任、标准或公用网络（例如，家庭网络、企业网络或 Internet 网络）上的任何计算机打开该端口，请选择“信任、标准和公用”。
 - 要对于标准网络（例如，企业网络）上的任何计算机打开该端口，请选择“标准(包括信任)”。
- 7 如果您要将此端口活动信息发给共享 Internet 连接的其他 Windows 网络计算机，请选择“将此端口上的网络活动转发给使用 Internet 连接共享的网络计算机”。
- 8 （可选）描述新配置。
- 9 单击“确定”。

注意：如果您的计算机装有接受 Web 或 FTP 服务器连接的程序，共享连接的计算机可能需要打开关联的系统服务端口，并允许转发这些端口的入站连接。如果您使用 Internet 连接共享 (ICS)，还需要在“网络”列表中添加信任的计算机连接。有关详细信息，请参阅“添加计算机连接”。

修改系统服务端口

您可以修改有关现有系统服务端口的入站和出站网络访问信息。

注意: 如果输入的端口信息不正确，则系统服务失败。

- 1 在“McAfee SecurityCenter”窗格上，单击“Internet 和网络”，然后单击“配置”。
- 2 在“Internet 和网络配置”窗格的“已启用防火墙保护”下，单击“高级”。
- 3 在“防火墙”窗格上，单击“系统服务”。
- 4 单击所需系统服务旁边的复选框，然后单击“编辑”。
- 5 在“系统服务”窗格的“添加系统服务规则”下，修改以下内容：
 - 系统服务名称
 - 本地 TCP/IP 端口
 - 本地 UDP 端口
- 6 执行下面某项操作：
 - 要对于信任、标准或公用网络（例如，家庭网络、企业网络或 Internet 网络）上的任何计算机打开该端口，请选择“信任、标准和公用”。
 - 要对于标准网络（例如，企业网络）上的任何计算机打开该端口，请选择“标准(包括信任)”。
- 7 如果您要将此端口活动信息发给共享 Internet 连接的其他 Windows 网络计算机，请选择“将此端口上的网络活动转发给使用 Internet 连接共享的网络计算机”。
- 8 （可选）描述修改的配置。
- 9 单击“确定”。

删除系统服务端口

您可以从计算机中删除现有的系统服务端口。删除端口后，远程计算机便不能访问计算机上的网络服务。

- 1 在“McAfee SecurityCenter”窗格上，单击“Internet 和网络”，然后单击“配置”。
- 2 在“Internet 和网络配置”窗格的“已启用防火墙保护”下，单击“高级”。
- 3 在“防火墙”窗格上，单击“系统服务”。
- 4 选择系统服务，然后单击“删除”。
- 5 出现提示时，单击“是”确认。

记录、监视和分析

防火墙为 Internet 事件和通讯提供详细而易读的记录、监视和分析。了解 Internet 通讯和事件有助于管理 Internet 连接。

本章内容

事件记录.....	98
使用统计信息.....	100
跟踪 Internet 通讯	101
监视 Internet 通讯	104

事件记录

防火墙允许启用或禁用事件记录，以及启用后要记录哪些事件类型。使用事件记录可以查看最近的入站、出站事件以及入侵事件。

配置事件日志设置

您以指定和配置要记录的 Firewall 事件的类型。默认情况下，系统会对所有事件和活动启用事件记录。

- 1** 在“Internet 和网络配置”窗格的“已启用防火墙保护”下，单击“高级”。
- 2** 在“防火墙”窗格上，单击“事件日志设置”。
- 3** 如果尚未选择，请选择“启用事件记录”。
- 4** 在“启用事件记录”上，选中或清除想要（或不想）记录的事件类型。事件类型包括：
 - 阻止的程序
 - ICMP Ping
 - 来自禁止 IP 地址的通讯
 - 系统服务端口上的事件
 - 未知端口上的事件
 - 入侵检测 (IDS) 事件
- 5** 要防止记录特定的端口，请选中“下列端口上的事件不作记录”，然后输入逗号分隔的单个端口，或输入短横线分隔的端口范围。例如，137-139, 445, 400-5000。
- 6** 单击“确定”。

查看最新事件

如果已启用记录，则可以查看最新事件。“最新事件”窗格会显示事件的日期和说明。它会显示已明确阻止访问 Internet 的程序的活动。

- 在“高级菜单”的“常见任务”窗格下，单击“报告和日志”或“查看最新事件”。或者，在“基本菜单”的“常见任务”窗格下，单击“查看最新事件”。

查看入站事件

如果已启用记录，则可以查看入站事件。“入站事件”包括日期和时间、源 IP 地址、主机名以及信息和事件类型。

- 1** 确保启用了“高级菜单”。在“常见任务”窗格上，单击“报告和日志”。
- 2** 在“最新事件”下，单击“查看日志”。
- 3** 单击“Internet 和网络”，然后单击“入站事件”。

注意: 您可以从“入站事件”日志信任、禁止和跟踪 IP 地址。

查看出站事件

如果已启用记录，则可以查看出站事件。出站事件包括尝试出站访问的程序名称、事件的日期和时间，以及程序在计算机上的位置。

- 1** 在“常见任务”窗格上，单击“报告和日志”。
- 2** 在“最新事件”下，单击“查看日志”。
- 3** 单击“Internet 和网络”，然后单击“出站事件”。

注意: 您可以从“出站事件”日志允许程序具有完全和仅出站访问权限。您还可以查找有关程序的其他信息。

查看入侵检测事件

如果已启用记录，则可以查看入站入侵事件。入侵检测事件显示事件的日期和时间、源 IP、主机名以及事件类型

- 1** 在“常见任务”窗格上，单击“报告和日志”。
- 2** 在“最新事件”下，单击“查看日志”。
- 3** 单击“Internet 和网络”，然后单击“入侵检测事件”。

注意: 您可以从“入侵检测事件”日志禁止和跟踪 IP 地址。

使用统计信息

防火墙利用 McAfee 的 HackerWatch 安全网站提供有关全球 Internet 安全事件和端口活动的统计信息。

查看全球安全事件统计信息

HackerWatch 会跟踪全球 Internet 安全事件，可以在 SecurityCenter 中查看这些事件。跟踪的信息会列出过去 24 小时、7 天和 30 天向 HackerWatch 报告的事件。

- 1** 确保已启用了“高级菜单”，然后单击“工具”。
- 2** 在“工具”窗格上，单击“HackerWatch”。
- 3** 在“事件跟踪”下，查看安全事件统计信息。

查看全球 Internet 端口活动

HackerWatch 会跟踪全球 Internet 安全事件，可以在 SecurityCenter 中查看这些事件。显示的信息包括在过去 7 天向 HackerWatch 报告的最重要的事件端口。通常，会显示 HTTP、TCP 和 UDP 端口信息。

- 1** 确保已启用了“高级菜单”，然后单击“工具”。
- 2** 在“工具”窗格上，单击“HackerWatch”。
- 3** 查看“最近的端口活动”下最重要的事件端口事件。

跟踪 Internet 通讯

防火墙提供了一些跟踪 Internet 通讯的选项。使用这些选项可以跟踪网络计算机的位置，获取域和网络信息，以及从“入站事件”和“入侵检测事件”日志中跟踪计算机。

跟踪网络计算机的位置

您可以使用可视跟踪程序，利用正在连接到或试图连接到您计算机的计算机名称或 IP 地址，确定此计算机的位置。您也可以使用可视跟踪程序访问网络和注册信息。运行可视跟踪程序会显示一幅世界地图，显示从源计算机到您计算机传输数据时最可能采用的途径。

- 1** 确保已启用了“高级菜单”，然后单击“工具”。
- 2** 在“工具”窗格上，单击“可视跟踪程序”。
- 3** 键入计算机的 IP 地址，然后单击“跟踪”。
- 4** 在“可视跟踪程序”下，选择“分布视图”。

注意： 您无法跟踪环回、专用或无效的 IP 地址事件。

获取计算机注册信息

您可以使用可视跟踪程序从 SecurityCenter 获取计算机的注册信息。这些信息包括域名、注册人姓名与地址以及管理联系人。

- 1** 确保已启用了“高级菜单”，然后单击“工具”。
- 2** 在“工具”窗格上，单击“可视跟踪程序”。
- 3** 键入计算机的 IP 地址，然后单击“跟踪”。
- 4** 在“可视跟踪程序”下，选择“注册人视图”。

获取计算机网络信息

您可以使用可视跟踪程序从 SecurityCenter 获取计算机的网络信息。网络信息包括有关域所在网络的详细信息。

- 1** 确保已启用了“高级菜单”，然后单击“工具”。
- 2** 在“工具”窗格上，单击“可视跟踪程序”。
- 3** 键入计算机的 IP 地址，然后单击“跟踪”。
- 4** 在“可视跟踪程序”下，选择“网络视图”。

从“入站事件”日志跟踪计算机

在“入站事件”窗格中，可以跟踪“入站事件”日志中显示的 IP 地址。

- 1** 确保启用了“高级菜单”。在“常见任务”窗格上，单击“报告和日志”。
- 2** 在“最新事件”下，单击“查看日志”。
- 3** 单击“Internet 和网络”，然后单击“入站事件”。
- 4** 在“入站事件”窗格上，选择源 IP 地址，然后单击“跟踪此 IP”。
- 5** 在“可视跟踪程序”窗格上，单击以下任一项：
 - **分布图视图：** 使用所选 IP 地址确定计算机的位置。
 - **注册人视图：** 使用所选 IP 地址查找域信息。
 - **网络视图：** 使用所选 IP 地址查找网络信息。
- 6** 单击“完成”。

从“入侵检测事件”日志跟踪计算机

在“入侵检测事件”窗格中，可以跟踪“入侵检测事件”日志中显示的 IP 地址。

- 1** 在“常见任务”窗格上，单击“报告和日志”。
- 2** 在“最新事件”下，单击“查看日志”。
- 3** 单击“Internet 和网络”，然后单击“入侵检测事件”。在“入侵检测事件”窗格中，选择源 IP 地址，然后单击“跟踪此 IP”。
- 4** 在“可视跟踪程序”窗格上，单击以下任一项：
 - **分布图视图：** 使用所选 IP 地址确定计算机的位置。
 - **注册人视图：** 使用所选 IP 地址查找域信息。
 - **网络视图：** 使用所选 IP 地址查找网络信息。
- 5** 单击“完成”。

跟踪监视的 IP 地址

您可以跟踪被监视 IP 地址以获取地理视图，此视图显示从源计算机到您计算机传输数据时最可能采用的途径。此外，还可以获取有关 IP 地址的注册和网络信息。

- 1** 确保已启用了“高级菜单”，然后单击“工具”。
- 2** 在“工具”窗格上，单击“通讯流量监视器”。
- 3** 在“通讯流量监视器”下，单击“应用程序”。
- 4** 选择程序，然后选择程序名称下显示的 IP 地址。
- 5** 在“程序活动”下，单击“跟踪此 IP”。
- 6** 在“可视跟踪程序”下，您可以查看地图，它显示从源计算机到您计算机传输数据时最可能采用的途径。此外，还可以获取有关 IP 地址的注册和网络信息。

注意：要查看最新的统计信息，请单击“可视跟踪程序”下的“刷新”。

监视 Internet 通讯

防火墙提供一些监视 Internet 通讯的方法，包括：

- **流量分析图：**显示最近的入站和出站 Internet 通讯。
- **带宽使用率图：**显示过去 24 小时最活跃的程序使用带宽的百分比。
- **活动程序：**显示当前在您的计算机上使用最多网络连接的程序，以及这些程序访问的 IP。

关于流量分析图

“流量分析”图是 Internet 入站和出站通讯的数字和图形表示。而且，通讯流量监视器会显示您的计算机上使用最多网络连接的程序，以及这些程序访问的 IP。

在“流量分析”窗格中，可以查看最近的入站和出站 Internet 通讯以及当前、平均和最大传输率。您还可以查看通讯流量，包括自启动防火墙后的通讯量，以及本月和上个月的总通讯量。

“流量分析”窗格会显示您计算机中的实时 Internet 活动，包括您计算机上最近入站和出站 Internet 通讯流量和速率、连接速度以及在 Internet 上传输的总字节数。

绿色实线表示入站通讯的当前传输速率。绿色虚线表示入站通讯的平均传输速率。如果当前传输速率与平均传输速率相同，则不会在图形上显示虚线。用实线同时表示平均传输速率和当前传输速率。

红色实线表示出站通讯的当前传输速率。红色虚线表示出站通讯的平均传输速率。如果当前传输速率与平均传输速率相同，则不会在图形上显示虚线。用实线同时表示平均传输速率和当前传输速率。

分析入站和出站通讯

“流量分析”图是 Internet 入站和出站通讯的数字和图形表示。而且，通讯流量监视器会显示您的计算机上使用最多网络连接的程序，以及这些程序访问的 IP。

- 1 确保已启用了“高级菜单”，然后单击“工具”。
- 2 在“工具”窗格上，单击“通讯流量监视器”。
- 3 在“通讯流量监视器”下，单击“流量分析”。

提示：要查看最新的统计信息，请单击“流量分析”下的“刷新”。

监视程序带宽

您可以查看饼图，它会显示过去 24 小时您计算机上最活跃程序使用带宽的大致百分比。此饼图直观地表示了程序所使用的相对带宽量。

- 1 确保已启用了“高级菜单”，然后单击“工具”。
- 2 在“工具”窗格上，单击“通讯流量监视器”。
- 3 在“通讯流量监视器”下，单击“带宽使用率”。

提示: 要查看最新的统计信息，请单击“带宽使用率”下的“刷新”。

监视程序活动

您可以查看入站和出站程序活动，这会显示远程计算机连接和端口。

- 1 确保已启用了“高级菜单”，然后单击“工具”。
- 2 在“工具”窗格上，单击“通讯流量监视器”。
- 3 在“通讯流量监视器”下，单击“应用程序”。
- 4 您可以查看下列信息：
 - 程序活动图：选择程序以显示其活动图。
 - 倾听连接：选择程序名称下的倾听项目。
 - 计算机连接：选择程序名称、系统进程或服务下的 IP 地址。

注意: 要查看最新的统计信息，请单击“应用程序”下的“刷新”。

了解 Internet 安全性

防火墙利用 McAfee 的安全网站 (HackerWatch) 提供有关程序和全球 Internet 活动的最新信息。HackerWatch 还提供有关防火墙的 HTML 教程。

本章内容

启动 HackerWatch 教程.....	108
------------------------	-----

启动 HackerWatch 教程

要了解防火墙，可以从 SecurityCenter 访问 HackerWatch 教程。

- 1** 确保已启用了“高级菜单”，然后单击“工具”。
- 2** 在“工具”窗格上，单击“HackerWatch”。
- 3** 在“HackerWatch 资源”下，单击“查看教程”。

第 4 章

McAfee Anti-Spam

Anti-Spam（以前称为 SpamKiller）可以通过检查入站电子邮件，然后将其标为垃圾邮件（请求您购买商品的电子邮件）或网络钓鱼邮件（请求您将个人信息提供给可能的诈骗网站的电子邮件）来阻止未经请求的电子邮件进入您的收件箱。然后，Anti-Spam 会过滤垃圾电子邮件，并将其移到 McAfee Anti-Spam 文件夹。

如果朋友发给您的合法电子邮件有时显示为垃圾邮件，则可以通过将其电子邮件地址添加到 Anti-Spam 的朋友列表中，确保不会过滤此电子邮件。您还可以自定义检测垃圾邮件的方法。例如，您可以更严格地过滤邮件，指定在邮件中所查找的内容，以及创建自己的过滤器。

如果您尝试通过电子邮件中的链接访问可能的诈骗网站，Anti-Spam 也会为您提供保护。当您单击指向可能的欺诈网站的链接时，您会被重定向到网络钓鱼过滤器安全页。如果有不想过滤的网站，则可以将其添加到白名单（不过滤此列表中的网站）。

Anti-Spam 可以与许多电子邮件程序（如 Yahoo®、MSN®/Hotmail®、Windows® Mail 和 Live™ Mail、Microsoft® Outlook®、Outlook Express 和 Mozilla Thunderbird™）一起工作，以及使用各种电子邮件帐户（如 POP3、POP3 Webmail 和 MAPI (Microsoft Exchange Server)）。如果您使用浏览器读取电子邮件，则必须将您的 Web 邮件帐户添加到 Anti-Spam。所有其他帐户都会自动配置，您无须将其添加到 Anti-Spam。

在安装 Anti-Spam 之后，不必配置 Anti-Spam；但是，如果您是高级用户，则可能希望根据自己的喜好微调其高级垃圾邮件和网络钓鱼防护功能。

注意： 在检测到重要和不重要的问题时，SecurityCenter 都会立即报告。如果您需要帮助来诊断保护问题，则可以运行 McAfee Virtual Technician。

本章内容

Anti-Spam 功能	111
配置垃圾邮件检测	113
过滤电子邮件	121
设置朋友	123
设置 Web 邮件帐户	127
处理过滤的电子邮件	131
配置网络钓鱼防护	133

Anti-Spam 功能

垃圾邮件过滤

防止未经请求的电子邮件进入您的收件箱。Anti-Spam 的高级过滤器会自动针对您的所有电子邮件帐户进行更新。您还可以创建自定义过滤器以确保过滤所有垃圾邮件，并将垃圾邮件报告给 McAfee 以供分析。

网络钓鱼过滤

标识可能的网络钓鱼（欺诈）网站，这些网站会收集个人信息。

自定义垃圾邮件处理

将未经请求的电子邮件标记为垃圾邮件并将其移至您的 McAfee Anti-Spam 文件夹，或者将合法的电子邮件标记为非垃圾邮件并将其移至您的收件箱。

朋友

将您朋友的电子邮件地址导入朋友列表中，以便不对他们的电子邮件进行过滤。

配置垃圾邮件检测

Anti-Spam 允许自定义检测垃圾邮件的方式。您可以更严格地过滤邮件，指定在邮件中查找的内容，以及指定分析垃圾邮件时要查找的特定字符集。您还可以创建个人过滤器来精确确定 Anti-Spam 将哪些邮件标识为垃圾邮件。例如，如果没有过滤包含 `mortgage` 一词的未经请求的电子邮件，则您可以添加包含 `mortgage` 一词的过滤器。

如果您的电子邮件有问题，则可以将禁用垃圾邮件保护作为排除故障策略的一部分。

本章内容

设置过滤选项	114
使用个人过滤器	117
禁用垃圾邮件防护	119

设置过滤选项

如果您要更严格地过滤邮件，指定您要如何处理垃圾邮件，以及在分析垃圾邮件时查找特定的字符集，则应调整 Anti-Spam 过滤选项。

过滤级别

过滤级别确定过滤电子邮件的严格程度。例如，如果有垃圾邮件没有过滤，且过滤级别设置为“中”，则可以将其更改为“中高”或“高”。不过，如果过滤级别设置为“高”，只接受朋友列表中发件人发来的电子邮件：所有其他邮件都会过滤掉。

垃圾邮件处理

Anti-Spam 允许自定义各种垃圾邮件处理选项。例如，可以将垃圾邮件和网络钓鱼电子邮件放在特定的文件夹中，更改垃圾邮件和网络钓鱼电子邮件的主题行中所出现标记的名称，指定要过滤的最大大小，以及指定垃圾邮件规则的更新频率。

字符集

在分析垃圾邮件时，Anti-Spam 可能会查找特定的字符集。字符集用于表示一种语言，包括语言字母表、数字和其他符号。如果您收到希腊语垃圾邮件，则可以过滤包含希腊语字符集的所有邮件。

请注意不要过滤接收合法电子邮件所采用语言的字符集。例如，如果仅想过滤意大利语邮件，则可能会选择西欧语言，因为意大利语属于西欧语言。不过，如果您收到合法的英语电子邮件，则选择西欧语言还会过滤英语邮件以及西欧语言字符集中的所有其他语言的邮件。在此情况下，您无法只过滤意大利语邮件。

注意： 指定字符集过滤器是为高级用户设计的。

更改过滤级别

您可以更改要过滤电子邮件的严格程度。例如，如果过滤掉合法电子邮件，则可以降低过滤级别。

1 打开“垃圾邮件防护”窗格。

如何实现？

1. 在 SecurityCenter 的“主页”窗格上，单击“电子邮件和即时消息”。
 2. 在“电子邮件和即时消息”信息区域，单击“配置”。
 3. 在“电子邮件和即时消息配置”窗格的“垃圾邮件”防护下，单击“高级”。
- 2** 在“垃圾邮件防护”窗格上，单击“过滤选项”。
- 3** 在“指定垃圾邮件过滤级别”列表中，选择适当的级别，然后单击“确定”。

级别	说明
低	接受大多数电子邮件。
中低	只过滤明显的垃圾邮件。
中(建议)	在建议的级别过滤电子邮件。
中高	过滤与垃圾邮件类似的所有电子邮件。
高	只接受“朋友”列表中的发件人发来的邮件。

修改垃圾邮件的处理和标记方式

可以指定要用来存放垃圾邮件和网络钓鱼电子邮件的文件夹、更改出现在电子邮件主题行中的 [SPAM] 或 [PHISH] 标记，指定要过滤的最大大小，以及指定垃圾邮件规则的更新频率。

- 1** 打开“垃圾邮件防护”窗格。

如何实现？

1. 在 SecurityCenter 的“主页”窗格上，单击“电子邮件和即时消息”。
 2. 在“电子邮件和即时消息”信息区域，单击“配置”。
 3. 在“电子邮件和即时消息配置”窗格的“垃圾邮件”防护下，单击“高级”。
- 2** 在“垃圾邮件防护”窗格上，单击“过滤选项”。
- 3** 修改或选择下面的相应选项，然后单击“确定”。

要...	执行此操作...
指定要用来存放垃圾邮件和网络钓鱼电子邮件的位置	在“将垃圾电子邮件置于此文件夹中”列表中，选择一个文件夹。默认文件夹是 McAfee Anti-Spam。

要...	执行此操作...
更改垃圾电子邮件的主题行	在“以此方式标记垃圾电子邮件的主题”中，指定一个要添加到垃圾电子邮件主题行中的标记。默认标记是 [SPAM]。
更改网络钓鱼电子邮件的主题行	在“以此方式标记网络钓鱼电子邮件的主题”中，指定一个要添加到网络钓鱼电子邮件主题行中的标记。默认标记是 [PHISH]。
指定要过滤的最大电子邮件	在“指定要过滤的最大电子邮件大小(KB)”中，输入要过滤的电子邮件的最大大小。
更新垃圾邮件规则	选择“更新垃圾邮件规则(分钟)”，然后输入垃圾邮件规则的更新频率。建议的频率为 30 分钟。如果您的网络连接速度很快，则可以指定一个较高的频率（如 5 分钟）来获得更好的结果。
不更新垃圾邮件规则	选择“不更新垃圾邮件规则”。

应用字符集过滤器

注意： 高级用户可以过滤包含特定字符集中字符的邮件。

您可以过滤特定的语言字符集；不过，请不要过滤接收合法电子邮件所使用语言的字符集。

1 打开“垃圾邮件防护”窗格。

如何实现？

1. 在 SecurityCenter 的“主页”窗格上，单击“电子邮件和即时消息”。
 2. 在“电子邮件和即时消息”信息区域，单击“配置”。
 3. 在“电子邮件和即时消息配置”窗格的“垃圾邮件”防护下，单击“高级”。
- 2** 在“垃圾邮件防护”窗格上，单击“字符集”。
- 3** 选中要过滤的字符集旁的复选框。
- 4** 单击“确定”。

使用个人过滤器

个人过滤器指定是否根据特定的词语或短语来允许或阻止电子邮件。如果某封电子邮件中包含该过滤器设置为阻止的词语或短语，则该电子邮件将被标记为垃圾邮件，而且将保留在收件箱或移动到 McAfee Anti-Spam 文件夹中。有关处理垃圾邮件方法的详细信息，请参阅修改处理和标记邮件的方法 (第 115 页)。

Anti-Spam 具有一个可防止未经请求的电子邮件进入您的收件箱的高级过滤器；但是，如果您希望微调 Anti-Spam 将哪些电子邮件标记为垃圾邮件，则可以创建一个人过滤器。例如，如果添加包含 *mortgage* 一词的过滤器，Anti-Spam 会使用 *mortgage* 一词过滤邮件。请不要创建使用合法电子邮件中出现的常用词语的过滤器，因为这样会甚至会过滤非垃圾电子邮件。在创建过滤器后，如果发现此过滤器仍无法检测到某种垃圾邮件，则可以编辑此过滤器。例如，如果创建的过滤器在邮件主题中查找 *viagra* 一词，但您仍会收到包含 *viagra* 一词的邮件，这是因为这个词出现在邮件正文中，请将过滤器更改为查找邮件正文而不是邮件主题中的 *viagra*。

正则表达式 (RegEx) 是还可可在个人过滤器中使用的特殊字符和序列；不过，McAfee 仅建议高级用户使用正则表达式。如果您不熟悉正则表达式，或想了解正则表达式使用方法的详细信息，则可以在 Web 上搜索正则表达式（如访问 http://en.wikipedia.org/wiki/Regular_expression）。

添加个人过滤器

您还可以添加过滤器来精确确定 Anti-Spam 将哪些邮件标识为垃圾邮件。

1 打开“垃圾邮件防护”窗格。

如何实现？

1. 在 SecurityCenter 的“主页”窗格上，单击“电子邮件和即时消息”。
 2. 在“电子邮件和即时消息”信息区域，单击“配置”。
 3. 在“电子邮件和即时消息配置”窗格的“垃圾邮件”防护下，单击“高级”。
- 2** 在“垃圾邮件防护”窗格上，单击“个人过滤器”。
- 3** 单击“添加”。
- 4** 指定个人过滤器在电子邮件中查找的内容 (第 118 页)。
- 5** 单击“确定”。

编辑个人过滤器

编辑现有的过滤器以精确确定将哪些邮件标识为垃圾邮件。

- 1** 打开“垃圾邮件防护”窗格。

如何实现？

1. 在 SecurityCenter 的“主页”窗格上，单击“电子邮件和即时消息”。
2. 在“电子邮件和即时消息”信息区域，单击“配置”。
3. 在“电子邮件和即时消息配置”窗格的“垃圾邮件”防护下，单击“高级”。
- 2** 在“垃圾邮件防护”窗格上，单击“个人过滤器”。
- 3** 选择要编辑的过滤器，然后单击“编辑”。
- 4** 指定个人过滤器在电子邮件中查找的内容（第 118 页）。
- 5** 单击“确定”。

删除个人过滤器

您可以永久删除不想使用的过滤器。

- 1** 打开“垃圾邮件防护”窗格。

如何实现？

1. 在 SecurityCenter 的“主页”窗格上，单击“电子邮件和即时消息”。
2. 在“电子邮件和即时消息”信息区域，单击“配置”。
3. 在“电子邮件和即时消息配置”窗格的“垃圾邮件”防护下，单击“高级”。
- 2** 在“垃圾邮件防护”窗格上，单击“个人过滤器”。
- 3** 选择要删除的过滤器，然后单击“删除”。
- 4** 单击“确定”。

指定个人过滤器

下表说明个人过滤器在电子邮件中查找的内容。

要...	执行此操作...
指定要过滤的电子邮件部分	在“电子邮件部分”列表中，单击一个条目，以确定过滤器是否在邮件主题、正文、发件人、标题或收件人中查找词语或短语。
	在“电子邮件部分”列表中，单击一个条目，以确定过滤器是否查找包含（或不包含）指定词语或短语的电子邮件。

要...	执行此操作...
在过滤器中指定词语或短语	在“词语或短语”中，键入要在电子邮件中查找的内容。例如，如果指定“mortgage”，则会过滤包含此词语的全部电子邮件。
指定此过滤器使用正则表达式	选择“此过滤器使用正则表达式”。
选择是否根据过滤器中的词语或短语来阻止或允许电子邮件。	在“执行此操作”中，选择“阻止”或“允许”以阻止或允许包含过滤器中的词语或短语的电子邮件。

禁用垃圾邮件防护

您可以禁用垃圾邮件防护以防 Anti-Spam 过滤电子邮件。

- 1 在“高级菜单”上，单击“配置”。
- 2 在“配置”窗格上，单击“电子邮件和即时消息”。
- 3 在“已启用垃圾邮件防护”下，单击“关”。

提示：切记单击“已禁用垃圾邮件防护”下的“开”，以便可以抵御垃圾邮件。

过滤电子邮件

Anti-Spam 会检查入站电子邮件并将其分类为垃圾邮件（请求您购买商品的电子邮件）或网络钓鱼邮件（请求您将个人信息提供给可能的诈骗网站的电子邮件）。默认情况下，Anti-Spam 会将每封未经请求的电子邮件标记为垃圾邮件或网络钓鱼邮件（在邮件主题行中显示 [SPAM] 或 [PHISH]），并将此邮件移到 McAfee Anti-Spam 文件夹。

您可以在 Anti-Spam 工具栏将电子邮件标记为垃圾邮件或非垃圾邮件，更改垃圾邮件移到的位置，或更改主题行中显示的标记。

在遇到电子邮件程序问题时，作为故障排除策略的一部分，您还可以禁用 Anti-Spam 工具栏。

本章内容

在 Anti-Spam 工具栏中标记邮件	121
禁用 Anti-Spam 工具栏	121

在 Anti-Spam 工具栏中标记邮件

在将邮件标记为垃圾邮件时，系统会用 [SPAM] 或您所选的标记对邮件的主题进行标记，并将其保留在收件箱、McAfee Anti-Spam 文件夹（Outlook、Outlook Express、Windows Mail 和 Thunderbird）或 Junk 文件夹（Eudora®）中。如果将邮件标记为非垃圾邮件，则会删除邮件标记并将邮件移到收件箱中。

要在此程序中标记邮件...	请选择邮件，然后...
Outlook、Outlook Express 和 Windows Mail	单击“标记为垃圾邮件”或“标记为非垃圾邮件”。
Eudora	在“Anti-Spam”菜单上，单击“标记为垃圾邮件”或“标记为非垃圾邮件”。
Thunderbird	在“Anti-Spam”工具栏上，依次指向“M”、“标记为”，然后单击“垃圾邮件”或“非垃圾邮件”。

禁用 Anti-Spam 工具栏

如果使用 Outlook、Outlook Express、Windows Mail、Eudora 或 Thunderbird，则可以禁用 Anti-Spam 工具栏。

1 打开“垃圾邮件防护”窗格。

如何实现？

1. 在 SecurityCenter 的“主页”窗格上，单击“电子邮件和即时消息”。
 2. 在“电子邮件和即时消息”信息区域，单击“配置”。
 3. 在“电子邮件和即时消息配置”窗格的“垃圾邮件”防护下，单击“高级”。
- 2** 在“垃圾邮件防护”窗格上，单击“电子邮件工具栏”。
- 3** 清除要禁用的工具栏旁的复选框。
- 4** 单击“确定”。

提示：可以随时选中 Anti-Spam 工具栏的复选框来重新启用此工具栏。

设置朋友

由于 Anti-Spam 经过改进的过滤器能够识别和允许合法的电子邮件，因此，无论您是手动添加地址簿还是导入地址簿，都极少需要向朋友列表中添加朋友的电子邮件。但是，如果您仍添加朋友的电子邮件地址，那么，有人伪造它时，Anti-Spam 将允许来自该电子邮件地址的邮件进入您的收件箱。

如果您仍希望导入地址簿，那么，在地址簿发生更改时，您必须再次导入它们，因为 Anti-Spam 不会自动更新您的朋友列表。

您还可以手动更新 Anti-Spam 朋友列表，或如果要将域内的每个用户都添加到朋友列表，则可以添加整个域。例如，如果添加 company.com 域，则不会过滤该组织发来的任何电子邮件。

本章内容

导入地址簿	123
手动设置朋友	124

导入地址簿

如果您希望 Anti-Spam 将地址簿中的电子邮件地址添加到朋友列表中，则可以导入地址簿。

1 打开“垃圾邮件防护”窗格。

如何实现？

- 1 在 SecurityCenter 的“主页”窗格上，单击“电子邮件和即时消息”。
- 2 在“电子邮件和即时消息”信息区域，单击“配置”。
- 3 在“电子邮件和即时消息配置”窗格的“垃圾邮件”防护下，单击“高级”。

2 在“垃圾邮件防护”窗格上，单击“朋友”。

3 在“朋友”窗格上，单击“导入”。

4 在“选择要导入的地址簿”列表中选择要导入的地址簿类型。

5 单击“立即导入”。

手动设置朋友

您可以逐个编辑条目来手动更新朋友列表。例如，如果收到朋友发来的电子邮件而其地址不在地址簿中，则可以立即手动添加其电子邮件地址。达到此目的的最简单的方法是使用 Anti-Spam 工具栏。如果不使用 Anti-Spam 工具栏，则必须指定朋友的信息。

从 Anti-Spam 工具栏中添加朋友

如果使用 Outlook、Outlook Express、Windows Mail、EudoraTM 或 Thunderbird 电子邮件程序，则可以直接从 Anti-Spam 工具栏添加朋友。

要添加此程序中的朋友...	请选择邮件，然后...
Outlook、Outlook Express 和 Windows Mail	单击“添加朋友”。
Eudora	在“Anti-Spam”菜单上，单击“添加朋友”。
Thunderbird	在“Anti-Spam”工具栏上，依次指向“M”、“标记为”，然后单击“朋友”。

手动添加朋友

如果您不想直接从工具栏添加朋友，或在收到电子邮件后忘记添加，则仍可以将朋友添加到朋友列表。

1 打开“垃圾邮件防护”窗格。

如何实现？

1. 在 SecurityCenter 的“主页”窗格上，单击“电子邮件和即时消息”。
2. 在“电子邮件和即时消息”信息区域，单击“配置”。
3. 在“电子邮件和即时消息配置”窗格的“垃圾邮件”防护下，单击“高级”。

2 在“垃圾邮件防护”窗格上，单击“朋友”。

3 在“朋友”窗格上，单击“添加”。

4 在“名称”框中键入朋友的名称。

5 在“类型”列表中选择“单个电子邮件地址”。

6 在“电子邮件地址”框中键入电子邮件地址。

7 单击“确定”。

添加域

如果要将某个域中的每个用户都添加到朋友列表，则应添加整个域。例如，如果添加 company.com 域，则不会过滤该组织发来的任何电子邮件。

1 打开“垃圾邮件防护”窗格。

如何实现？

1. 在 SecurityCenter 的“主页”窗格上，单击“电子邮件和即时消息”。
2. 在“电子邮件和即时消息”信息区域，单击“配置”。
3. 在“电子邮件和即时消息配置”窗格的“垃圾邮件”防护下，单击“高级”。

2 在“垃圾邮件防护”窗格上，单击“朋友”。

3 在“朋友”窗格上，单击“添加”。

4 在“名称”框中键入组织或组的名称。

5 在“类型”列表中选择“整个域”

6 在“电子邮件地址”框中键入域名。

7 单击“确定”。

编辑朋友

如果朋友的信息发生变化，则可以更新朋友列表，以确保 Anti-Spam 不会将其邮件标记为垃圾邮件。

1 打开“垃圾邮件防护”窗格。

如何实现？

1. 在 SecurityCenter 的“主页”窗格上，单击“电子邮件和即时消息”。
2. 在“电子邮件和即时消息”信息区域，单击“配置”。
3. 在“电子邮件和即时消息配置”窗格的“垃圾邮件”防护下，单击“高级”。

2 在“垃圾邮件防护”窗格上，单击“朋友”。

3 选择要编辑的朋友，然后单击“编辑”。

4 在“名称”框中更改朋友的名称。

5 在“电子邮件地址”框中更改朋友的电子邮件地址。

6 单击“确定”。

编辑域

如果域的信息发生变化，则可以更新朋友列表，以确保 Anti-Spam 不会将该域发来的邮件标记为垃圾邮件。

1 打开“垃圾邮件防护”窗格。

如何实现？

1. 在 SecurityCenter 的“主页”窗格上，单击“电子邮件和即时消息”。

2. 在“电子邮件和即时消息”信息区域，单击“配置”。

3. 在“电子邮件和即时消息配置”窗格的“垃圾邮件”防护下，单击“高级”。

2 在“垃圾邮件防护”窗格上，单击“朋友”。

3 在“朋友”窗格上，单击“添加”。

4 在“名称”框中更改组织或组的名称。

5 在“类型”列表中选择“整个域”

6 在“电子邮件地址”框中更改域名。

7 单击“确定”。

删除朋友

如果朋友列表中的人员或域发给您垃圾邮件，则可以从 Anti-Spam 朋友列表中删除朋友，以便再次过滤其电子邮件。

1 打开“垃圾邮件防护”窗格。

如何实现？

1. 在 SecurityCenter 的“主页”窗格上，单击“电子邮件和即时消息”。

2. 在“电子邮件和即时消息”信息区域，单击“配置”。

3. 在“电子邮件和即时消息配置”窗格的“垃圾邮件”防护下，单击“高级”。

2 在“垃圾邮件防护”窗格上，单击“朋友”。

3 选择要删除的朋友，然后单击“删除”。

设置 Web 邮件帐户

如果您使用浏览器读取电子邮件，则必须配置 Anti-Spam 连接到您的帐户并过滤邮件。要将 Web 邮件帐户添加到 Anti-Spam，只需添加电子邮件提供商提供的帐户信息。

在添加 Web 邮件帐户后，您可以编辑帐户信息，并获取有关已过滤 Web 邮件的详细信息。如果您不再使用 Web 邮件帐户，或不想过滤此帐户，则可以将其删除。

Anti-Spam 可以与许多电子邮件程序（如 Yahoo!®、MSN®/Hotmail®、Windows® Mail 和 Live™ Mail、Microsoft® Outlook®、Outlook Express 和 Mozilla Thunderbird™）一起工作，以及使用各种电子邮件帐户（如 POP3、POP3 Webmail 和 MAPI (Microsoft Exchange Server)）。POP3 最常见的帐户类型，是 Internet 电子邮件的标准。如果您具有 POP3 帐户，Anti-Spam 会直接连接到电子邮件服务器，并在 Web 邮件帐户检索邮件之前进行过滤。POP3 Web 邮件、Yahoo!、MSN/Hotmail 和 Windows Mail 帐户都是基于 Web 的帐户。过滤 POP3 Web 邮件帐户与过滤 POP3 帐户类似。

本章内容

添加 Web 邮件帐户	127
编辑 Web 邮件帐户	128
删除 Web 邮件帐户	129
了解 Web 邮件帐户信息	129

添加 Web 邮件帐户

如果您要过滤 POP3（如 Yahoo）、MSN/Hotmail 或 Windows Mail（仅完全支持付费版本）Web 邮件帐户的垃圾邮件，请添加该帐户。

1 打开“垃圾邮件防护”窗格。

如何实现？

1. 在 SecurityCenter 的“主页”窗格上，单击“电子邮件和即时消息”。
 2. 在“电子邮件和即时消息”信息区域，单击“配置”。
 3. 在“电子邮件和即时消息配置”窗格的“垃圾邮件”防护下，单击“高级”。
- 2** 在“垃圾邮件防护”窗格上，单击“Web 邮件帐户”。
- 3** 在“Web 邮件帐户”窗格上，单击“添加”。
- 4** 指定帐户信息 (第 129 页)，然后单击“下一步”。
- 5** 在“检查选项”下，指定 Anti-Spam 检查帐户垃圾邮件的时间 (第 129 页)。
- 6** 如果使用拨号连接，请指定 Anti-Spam 连接到 Internet 的方式 (第 129 页)。
- 7** 单击“完成”。

编辑 Web 邮件帐户

如果帐户发生更改，则必须编辑 Web 安装信息。例如，如果更改密码或希望 Anti-Spam 更频繁地检查垃圾邮件，则应编辑 Web 邮件帐户。

- 1** 打开“垃圾邮件防护”窗格。
如何实现？
 1. 在 SecurityCenter 的“主页”窗格上，单击“电子邮件和即时消息”。
 2. 在“电子邮件和即时消息”信息区域，单击“配置”。
 3. 在“电子邮件和即时消息配置”窗格的“垃圾邮件”防护下，单击“高级”。

2 在“垃圾邮件防护”窗格上，单击“Web 邮件帐户”。

3 选择要修改的帐户，然后单击“编辑”。

4 指定帐户信息 (第 129 页)，然后单击“下一步”。

5 在“检查选项”下，指定 Anti-Spam 检查帐户垃圾邮件的时间 (第 129 页)。

6 如果使用拨号连接，请指定 Anti-Spam 连接到 Internet 的方式 (第 129 页)。

7 单击“完成”。

删除 Web 邮件帐户

如果不想过滤某个 Web 邮件帐户的垃圾邮件，请删除该帐户。例如，如果您的帐户无效或遇到问题，则可以在解决问题时删除帐户。

1 打开“垃圾邮件防护”窗格。

如何实现？

1. 在 SecurityCenter 的“主页”窗格上，单击“电子邮件和即时消息”。
2. 在“电子邮件和即时消息”信息区域，单击“配置”。
3. 在“电子邮件和即时消息配置”窗格的“垃圾邮件”防护下，单击“高级”。

2 在“垃圾邮件防护”窗格上，单击“Web 邮件帐户”。

3 选择要删除的帐户，然后单击“删除”。

了解 Web 邮件帐户信息

下表描述在添加或编辑 Web 邮件帐户时必须指定的信息。

帐户信息

信息	说明
说明	描述帐户，以供您参考。可以在此框中键入任何信息。
电子邮件地址	指定与此电子邮件帐户关联的电子邮件地址。
帐户类型	指定要添加的电子邮件帐户的类型(例如, POP3 Web 邮件或 MSN/Hotmail)。
服务器	指定此帐户所在的电子邮件服务器的名称。如果您不知道服务器名称，请参阅 Internet 服务提供商 (ISP) 提供的信息。
用户名	指定此电子邮件帐户的用户名。例如，如果电子邮件地址为 <i>username@hotmail.com</i> ，则用户名可能为 <i>username</i> 。
密码	指定此电子邮件帐户的密码。
确认密码	验证此电子邮件帐户的密码。

检查选项

选项	说明
检查频率为	Anti-Spam 会以您指定的时间间隔（分钟数）检查此帐户的垃圾邮件。时间间隔必须在 5 到 3600 分钟之间。
启动时检查	Anti-Spam 会在每次重新启动计算时检查帐户。

连接选项

选项	说明
从不进行拨号连接	Anti-Spam 不会自动进行拨号连接。您必须手动启动拨号连接。
无可用连接时拨号	如果 Internet 连接不可用，Anti-Spam 会尝试使用您指定的拨号连接进行连接。
始终拨指定连接	Anti-Spam 会尝试使用指定的拨号连接进行连接。如果您当前使用的拨号连接不是您指定的拨号连接，则会断开连接。
拔此连接	指定 Anti-Spam 用于连接到 Internet 的拨号连接。
过滤完成后保持连接状态	过滤完成后，计算机仍连接到 Internet。

处理过滤的电子邮件

有时，有些垃圾邮件可能检测不到。在发生这种情况后，您可以将垃圾邮件报告给 McAfee，McAfee 会分析此垃圾邮件来创建过滤器更新。

如果您使用的是 Web 邮件帐户，则可以查看、导出和删除已过滤的电子邮件。如果您无法确定是否过滤了合法邮件，或想了解过滤邮件的时间，则此功能很有用。

本章内容

将电子邮件报告给 McAfee.....	131
查看、导出或删除已过滤的 Web 邮件	132
查找已过滤 Web 邮件的事件。	132

将电子邮件报告给 McAfee

您可以在将电子邮件标记为垃圾邮件或非垃圾邮件时将它们报告给 McAfee，我们将对其进行分析以创建过滤器更新。

1 打开“垃圾邮件防护”窗格。

如何实现？

- 1 在 SecurityCenter 的“主页”窗格上，单击“电子邮件和即时消息”。
- 2 在“电子邮件和即时消息”信息区域，单击“配置”。
- 3 在“电子邮件和即时消息配置”窗格的“垃圾邮件”防护下，单击“高级”。
- 2 在“垃圾邮件防护”窗格上，单击“电子邮件工具栏”。
- 3 在“帮助改进 Anti-Spam”下，选中相应的复选框，然后单击“确定”。

要...	执行此操作...
每次将电子邮件标记为垃圾邮件时将其报告给 McAfee	选中“将电子邮件标记为垃圾邮件”。
每次将电子邮件标记为非垃圾邮件时将其报告给 McAfee	选中“将电子邮件标记为非垃圾邮件”。
在将电子邮件报告为非垃圾邮件时，将整个电子邮件(而不仅是标题)发送给 McAfee。	选中“发送整个电子邮件(不仅仅是标题)”。

注意: 当您将某个电子邮件报告为非垃圾邮件，并将整个电子邮件报告给 McAfee 时，该电子邮件不会进行加密。

查看、导出或删除已过滤的 Web 邮件

您可以查看、导出或删除已在 Web 邮件帐户中过滤的邮件。

- 1** 在“常见任务”下，单击“报告和日志”。
- 2** 在“报告和日志”窗格上，单击“已过滤的 Web 邮件”。
- 3** 选择邮件。
- 4** 在“我想”下，执行以下任一操作：
 - 单击“查看”以默认电子邮件程序查看邮件。
 - 单击“导出”以将邮件复制到您的计算机。
 - 单击“删除”以删除邮件。

查找已过滤 Web 邮件的事件。

您可以查看过滤电子邮件的日期和时间以及接收这些邮件的帐户。

- 1** 在“常见任务”下，单击“查看最新事件”。
- 2** 在“最新事件”窗格上，单击“查看日志”。
- 3** 在左侧窗格上，展开“电子邮件和即时消息”列表，然后单击“Web 邮件过滤事件”。
- 4** 选择要查看的日志。

配置网络钓鱼防护

Anti-Spam 会将未经请求的电子邮件分为垃圾邮件（请求您购买商品的电子邮件）或网络钓鱼邮件（请求您将个人信息提供给可能的诈骗网站的电子邮件）。网络钓鱼防护会防止您访问欺诈网站。如果您单击电子邮件中指向已知或可能欺诈网站的链接，则 Anti-Spam 会将您重定向到网络钓鱼过滤器安全页。

如果有您不想过滤的网站，则可以将其添加到网络钓鱼白名单中。您还可以编辑或删除白名单中的网站。您无须添加如 Google®、Yahoo 或 McAfee 之类的网站，因为这些网站不是欺诈网站。

注意：如果您安装了 SiteAdvisor，则您不会获得 Anti-Spam 网络钓鱼防护，因为 SiteAdvisor 已含有与 Anti-Spam 类似的网络钓鱼防护功能。

本章内容

将网站添加到白名单.....	133
编辑白名单中的站点.....	134
删除白名单中的网站.....	134
禁用网络钓鱼防护.....	134

将网站添加到白名单

如果有您不想过滤的网站，则可以将其添加到白名单中。

1 打开“网络钓鱼防护”窗格。

如何实现？

1. 在 SecurityCenter 的“主页”窗格中，单击“Internet 和网络”。
 2. 在“Internet 和网络”信息区域中，单击“配置”。
- 2** 在“网络钓鱼防护”窗格上，单击“高级”。
- 3** 在“白名单”下，单击“添加”。
- 4** 输入网站地址，然后单击“确定”。

编辑白名单中的站点

如果您已将某个网站添加到白名单且网站地址发生变化，则可以随时进行更新。

- 1** 打开“网络钓鱼防护”窗格。

如何实现？

1. 在 SecurityCenter 的“主页”窗格中，单击“Internet 和网络”。
2. 在“Internet 和网络”信息区域中，单击“配置”。
- 2** 在“网络钓鱼防护”窗格上，单击“高级”。
- 3** 在“白名单”下，选择要更新的网站，然后单击“编辑”。
- 4** 编辑网站地址，然后单击“确定”。

删除白名单中的网站

如果您要访问某个网站而将其添加到白名单中，但现在又希望过滤该网站，请从白名单中将其删除。

- 1** 打开“网络钓鱼防护”窗格。

如何实现？

1. 在 SecurityCenter 的“主页”窗格中，单击“Internet 和网络”。
2. 在“Internet 和网络”信息区域中，单击“配置”。
- 2** 在“网络钓鱼防护”窗格上，单击“高级”。
- 3** 在“白名单”下，选择要删除的网站，然后单击“删除”。

禁用网络钓鱼防护

如果您安装的网络钓鱼软件不是 McAfee 提供的，而且发生冲突，请禁用 Anti-Spam 网络钓鱼防护。

- 1** 在 SecurityCenter 的“主页”窗格中，单击“Internet 和网络”。
- 2** 在“Internet 和网络”信息区域中，单击“配置”。
- 3** 在“已启用网络钓鱼防护”下，单击“关”。

提示：完成操作后，请单击“已禁用网络钓鱼防护”下的“开”，这样便可以免受欺诈网站的侵扰。

第 5 章

McAfee Parental Controls

家长监控会为您、家人、个人文件和计算机提供高级保护。它会帮助您抵御在线身份信息窃取，阻止个人信息的传输，以及过滤可能不良的在线内容（包括图像）。它还允许您监视、控制和记录未经授权的 Web 浏览习惯，并为个人密码提供安全的存储区域。

开始使用家长监控之前，您应熟悉某些最常用的功能。家长监控帮助提供有关配置和使用这些功能的详细信息。

注意： 在检测到重要和不重要的问题时，SecurityCenter 都会立即报告。如果您需要帮助来诊断保护问题，则可以运行 McAfee Virtual Technician。

本章内容

家长监控的功能	136
保护儿童	137
在 Web 上保护信息	153
保护密码	155

家长监控的功能

家长监控

过滤可能不良的图像、启用适合年龄的搜索、配置用户的年龄（用于确定将阻止哪些内容）以及为 SecurityCenter 用户设置 Web 浏览时间限制（用户可以访问 Web 的日期和时间）。“家长监控”还会全面限制用户对特定网站的访问权限，并根据关联的关键字授予或阻止访问权限。

个人信息保护

阻止在 Web 上传输敏感信息或机密信息（如信用卡号、银行帐号、地址等）。

密码存储库

安全地存储您的个人密码，而不用担心其他用户（甚至管理员）访问它们。

保护儿童

如果儿童使用您的计算机，您可以使用家长监控来帮助每个儿童在浏览 Web 时可以查看的内容和执行的操作。例如，您可以启用或禁用适合年龄的搜索和图像过滤，选择内容评级组并设置 Web 浏览时间限制。

适合年龄的搜索可确保启用针对某些常见搜索引擎的安全过滤，以便将可能不良的项目自动排除在儿童的搜索结果之外；在儿童浏览 Web 时，图像过滤会阻止显示可能不良的图像；内容评级组会根据儿童的年龄组确定儿童可以访问的内容种类；而 Web 浏览时间限制会定义儿童可以访问 Web 的日期和时间。您还可以对所有儿童过滤（阻止或允许）某些网站。

注意：要将家长监控配置为保护儿童，您必须以 Windows 管理员身份登录计算机。如果您是从该 McAfee 产品的旧版本升级的，而且仍使用 McAfee 用户，则还必须确保您以 McAfee 管理员身份登录。

本章内容

使用关键字过滤网站.....	138
过滤网站.....	140
设置 Web 浏览时间限制.....	143
设置内容评级组.....	144
过滤可能不良的 Web 图像.....	145
启用适合年龄的搜索.....	146
配置用户.....	147

使用关键字过滤网站

关键字过滤允许您阻止非成人用户访问包含可能不良词语的网站。如果启用了关键字过滤，则系统会根据用户的内容评级组，使用默认的关键字列表和相应的规则针对用户对内容进行评级。用户只有属于某个组才能访问包含特定关键字的网站。例如，只有成人组的成员才能访问包含“色情”一词的网站，而只有儿童组（以及更高年龄组）的成员才能访问包含“毒品”一词的网站。

您还可以将自己的关键字添加到默认列表，并其与某些内容评级组关联起来。您添加的关键字规则会覆盖可能已与默认列表中匹配关键字相关的规则。

根据关键字阻止网站

如果您要阻止包含不良内容的网站，但并不知道具体的站点地址，则可以根据其关键字阻止网站。只需输入关键字，然后确定哪些内容评级组可以浏览包含此关键字的网站。

1 打开“家长监控”窗格。

如何实现？

1. 在 SecurityCenter 的“主页”窗格上，单击“家长监控”。
2. 在“家长监控”信息区域中，单击“配置”。
3. 在“家长监控配置”窗格上，确保启用了“家长监控”，然后单击“高级”。

2 在“家长监控”窗格上，单击“关键字”并确保启用了关键字过滤。

3 在“关键字列表”下的“查找”框键入关键字。

4 移动“最小年龄”滑块来指定最小年龄组。

此年龄组及更高年龄组中的用户可以浏览包含关键字的网站。

5 单击“确定”。

禁用关键字过滤

默认情况下会启用关键字过滤，即系统会根据用户的内容评级组，使用默认的关键字列表和相应的规则针对用户对内容进行评级。尽管您可以随时禁用关键字过滤，但 McAfee 建议不要这样做。

1 打开“家长监控”窗格。

如何实现？

1. 在 SecurityCenter 的“主页”窗格上，单击“家长监控”。
 2. 在“家长监控”信息区域中，单击“配置”。
 3. 在“家长监控配置”窗格上，确保启用了“家长监控”，然后单击“高级”。
- 2** 在“家长监控”窗格上，单击“关键字”。
- 3** 在“关键字”窗格上，单击“关”。
- 4** 单击“确定”。

过滤网站

您可以为除成人组中的用户外的所有用户过滤（阻止或允许）网站。在阻止某个网站后，可以防止儿童在浏览 Web 时访问此网站。如果儿童尝试访问已阻止的网站，则会显示一条消息，指出因为 McAfee 已阻止此网站，所以无法对其进行访问。

如果 McAfee 默认已阻止某个网站，但希望儿童访问此网站，则可以允许此网站。有关 McAfee 默认阻止的网站的详细信息，请参阅使用关键字过滤网站（第 138 页）。您还可以随时更新或删除已过滤的网站。

注意：属于成人组的用户（包括管理员）可以访问所有网站，即使已阻止这些网站也可以访问。要测试阻止的网站，您必须以非成人用户身份登录，但是，请记住，在完成测试之后清除 Web 浏览器的浏览历史记录。

删除已过滤的网站

如果不再对此已过滤的网站进行阻止或允许，则可以删除此网站。

1 打开“家长监控”窗格。

如何实现？

1. 在 SecurityCenter 的“主页”窗格上，单击“家长监控”。
2. 在“家长监控”信息区域中，单击“配置”。
3. 在“家长监控配置”窗格上，确保启用了“家长监控”，然后单击“高级”。

2 在“家长监控”窗格上，单击“已过滤的网站”。

3 在“已过滤的网站”窗格上，单击“已过滤的网站”列表中的条目，然后单击“删除”。

4 单击“确定”。

更新已过滤的网站

如果某个网站的地址发生变化，或在阻止或允许时输入不正确，则可以更新此网站的地址。

1 打开“家长监控”窗格。

如何实现？

1. 在 SecurityCenter 的“主页”窗格上，单击“家长监控”。
 2. 在“家长监控”信息区域中，单击“配置”。
 3. 在“家长监控配置”窗格上，确保启用了“家长监控”，然后单击“高级”。
- 2** 在“家长监控”窗格上，单击“已过滤的网站”。
- 3** 在“已过滤的网站”窗格上，单击“已过滤的网站”列表中的条目，在“http://”框中修改网站地址，然后单击“更新”。
- 4** 单击“确定”。

允许网站

允许某个网站可以确保没有对任何用户阻止此网站。如果您允许 McAfee 默认已阻止的网站，则可以覆盖默认设置。

- 1** 打开“家长监控”窗格。

如何实现？

1. 在 SecurityCenter 的“主页”窗格上，单击“家长监控”。
 2. 在“家长监控”信息区域中，单击“配置”。
 3. 在“家长监控配置”窗格上，确保启用了“家长监控”，然后单击“高级”。
- 2** 在“家长监控”窗格上，单击“已过滤的网站”。
- 3** 在“已过滤的网站”窗格上，在“http://”框中键入网站的地址，然后单击“允许”。
- 4** 单击“确定”。

提示：您可以允许以前阻止的网站，方法是单击“已过滤的网站”列表中的网站地址，然后单击“允许”。

阻止网站

在阻止某个网站后，可以防止儿童在浏览 Web 时访问此网站。如果儿童尝试访问已阻止的网站，则会显示一条消息，指出因为 McAfee 已阻止此网站，所以无法对其进行访问。

- 1** 打开“家长监控”窗格。

如何实现？

1. 在 SecurityCenter 的“主页”窗格上，单击“家长监控”。
 2. 在“家长监控”信息区域中，单击“配置”。
 3. 在“家长监控配置”窗格上，确保启用了“家长监控”，然后单击“高级”。
- 2** 在“家长监控”窗格上，单击“已过滤的网站”。
- 3** 在“已过滤的网站”窗格上，在“http://”框中键入网站的地址，然后单击“阻止”。
- 4** 单击“确定”。

提示：您可以阻止以前允许的网站，方法是单击“已过滤的网站”列表中的网站地址，然后单击“阻止”。

设置 Web 浏览时间限制

如果您要防止对 Internet 不负责任或过度的使用，则可以对儿童的 Web 浏览设置适当的时间限制。如果您将儿童限制在特定的时间浏览 Web，则您可以确信，即使您不在家，SecurityCenter 也会实施这些限制。

默认情况下，可以允许儿童全天候浏览 Web，不过，您可以将浏览 Web 的时间限制在特定的时间或日期，或完全禁止浏览 Web。如果儿童在禁止期间尝试浏览 Web，则 McAfee 会通知儿童，指出他们无法访问。如果您完全禁止浏览 Web，则儿童可以登录并使用计算机（包括使用其他 Internet 程序，如电子邮件、即时消息程序、ftp、游戏等），但无法浏览 Web。

设置 Web 浏览时间限制

您可以使用 Web 浏览时间限制网格限制儿童只能在特定的日期和时间浏览 Web。

1 打开“用户设置”窗格。

如何实现？

1. 在 SecurityCenter 的“主页”窗格上，单击“家长监控”。
 2. 在“家长监控”信息区域中，单击“配置”。
 3. 在“家长监控配置”窗格上，单击“高级”。
 4. 在“家长监控”窗格上，单击“用户设置”。
- 2** 在“用户设置”窗格中，单击用户名，然后单击“编辑”。
- 3** 在“编辑用户帐户”窗口的“Web 浏览时间限制”下，拖动鼠标以指定此用户不能浏览 Web 的日期和时间。
- 4** 单击“确定”。

设置内容评级组

用户可以属于以下任一内容评级组：

- 幼儿
- 儿童
- 青少年(较小)
- 青少年(较大)
- 成人

家长监控会根据用户所属的组对 Web 内容进行评级(阻止或允许)。您可以为家庭中的某些用户阻止或允许某些网站。例如，您可以为属于幼儿组的用户阻止 Web 内容，而为属于青少年(较小)组的用户允许此内容。如果您要更严格地为某个用户评级内容，则可以允许用户只查看“已过滤的网站”列表中允许的网站。有关详细信息，请参阅过滤网站(第 140 页)。

设置用户的内容评级组

默认情况下，新用户会添加到成人组，允许此用户访问所有 Web 内容。然后，您可以根据个人的年龄和成熟阶段调整用户的内容评级组。

1 打开“用户设置”窗格。

如何实现？

1. 在 SecurityCenter 的“主页”窗格上，单击“家长监控”。
 2. 在“家长监控”信息区域中，单击“配置”。
 3. 在“家长监控配置”窗格上，单击“高级”。
 4. 在“家长监控”窗格上，单击“用户设置”。
- 2 在“用户设置”窗格中，单击用户名，然后单击“编辑”。**
- 3 在“编辑用户帐户”窗口的“内容评级”下，单击要分配给用户的年龄组。**
- 要防止用户浏览“已过滤的网站”列表中阻止的任何网站，请选中“此用户只能访问‘允许的网站’列表中的站点”复选框。
- 4 单击“确定”。**

过滤可能不良的 Web 图像

根据用户的年龄或成熟阶段，您可以在用户浏览 Web 时过滤（阻止或允许）可能不良的图像。例如，您可以阻止儿童浏览 Web 时显示可能不良的图像，但允许其向家庭中的青少年（较大）和成人请求帮助。默认情况下，系统会对成人组中的所有成员禁用图像过滤，即这些用户在浏览 Web 时会看到可能不良的图像。有关设置用户年龄组的详细信息，请参阅设置内容评级组（第 144 页）。

过滤可能不良的 Web 图像

默认情况下，新用户会添加到成人组，而且禁用图像过滤。如果要阻止某个特定用户在浏览 Web 时显示可能的不良图像，则可以启用图像过滤。每个可能的不良 Web 图像会自动用静态 McAfee 图像代替。

1 打开“用户设置”窗格。

如何实现？

1. 在 SecurityCenter 的“主页”窗格上，单击“家长监控”。
 2. 在“家长监控”信息区域中，单击“配置”。
 3. 在“家长监控配置”窗格上，单击“高级”。
 4. 在“家长监控”窗格上，单击“用户设置”。
- 2 在“用户设置”窗格中，单击用户名，然后单击“编辑”。**
- 3 在“编辑用户帐户”窗口的“图像过滤”下，单击“开”。**
- 4 单击“确定”。**

启用适合年龄的搜索

某些常见的搜索引擎（如 Yahoo! 和 Google）提供“安全搜索”，这是一个搜索设置，能够防止可能不良的搜索结果出现在搜索引擎的搜索结果列表中。这些搜索引擎通常允许您选择安全搜索过滤的严格程度，而且还允许您或任何其他用户随时关闭它。

在家长监控中，通过“适合年龄的搜索”可以方便地确保在用户使用以下任一搜索引擎时，“安全搜索”始终对于用户处于打开状态：

- Google™
- MSN®
- Windows® Live Search
- Yahoo!®

如果您启用适合年龄的搜索，我们将确保搜索引擎的安全搜索过滤功能对于该用户处于打开状态并设置为其最严格的设置。而且，如果用户尝试（在搜索引擎的首选项或高级设置中）关闭该过滤功能，我们将自动打开它。

默认情况下，“适合年龄的搜索”对于除管理员和成人组成员以外的所有用户均处于启用状态。有关设置用户年龄组的详细信息，请参阅设置内容评级组（第 144 页）。

启用适合年龄的搜索

默认情况下，新用户会添加到成人组，而且“适合年龄的搜索”处于禁用状态。如果您希望确保针对成人用户打开某些常见搜索引擎所提供的安全搜索过滤，则可以启用“适合年龄的搜索”。

1 打开“用户设置”窗格。

如何实现？

1. 在 SecurityCenter 的“主页”窗格上，单击“家长监控”。
 2. 在“家长监控”信息区域中，单击“配置”。
 3. 在“家长监控配置”窗格上，单击“高级”。
 4. 在“家长监控”窗格上，单击“用户设置”。
- 2** 在“用户设置”窗格中，单击用户名，然后单击“编辑”。
- 3** 在“编辑用户帐户”窗口的“适合年龄的搜索”下，单击“开”。
- 4** 单击“确定”。

配置用户

要将家长监控配置为保护儿童，可以在 SecurityCenter 中为他们分配某些权限。这些权限确定了每个儿童可以在 Web 上查看的内容和执行的操作。

默认情况下，SecurityCenter 用户对应于计算机上已建立的 Windows 用户。不过，如果您已从使用 McAfee 用户的早期版本的 SecurityCenter 升级，则仍会保留 McAfee 用户及其权限。

注意：要配置用户，您必须以 Windows 管理员身份登录计算机。如果您是从该 McAfee 产品的旧版本升级的，而且仍使用 McAfee 用户，则还必须确保您以 McAfee 管理员身份登录。

本章内容

使用 McAfee 用户	148
使用 Windows 用户	151

使用 McAfee 用户

如果您从使用 McAfee 用户的早期版本的 SecurityCenter 升级，则仍会自动保留 McAfee 用户及其权限。您可以继续配置和管理 McAfee 用户，不过，McAfee 建议切换到 Windows 用户。在切换到 Windows 用户后，就无法重新切换到 McAfee 用户。

如果继续使用 McAfee 用户，则可以添加、编辑或删除用户，以及更改或检索 McAfee 管理员的密码。

检索 McAfee 管理员的密码

如果您忘记了管理员密码，可以取回该密码。

- 1 右键单击 SecurityCenter 图标 ，然后单击“切换用户”。
- 2 在“用户名”列表中，选择“管理员”，然后单击“忘记了密码？”。
- 3 在“您的答案”框中键入机密问题的答案。
- 4 单击“提交”。

更改 McAfee 管理员的密码

如果 McAfee 管理员密码不易记忆，或怀疑可能泄漏，则可以更改密码。

- 1 以管理员用户身份登录 SecurityCenter。
- 2 打开“用户设置”窗格。

如何实现？

1. 在“常见任务”下，单击“主页”。
2. 在 SecurityCenter 的“主页”窗格上，单击“家长监控”。
3. 在“家长监控”信息区域中，单击“配置”。
4. 在“家长监控配置”窗格上，单击“高级”。
- 3 在“用户设置”窗格的“McAfee 用户帐户”下，选择“管理员”，然后单击“编辑”。
- 4 在“编辑用户帐户”对话框的“新密码”框中键入新密码，然后在“重新输入密码”中重新键入此新密码。
- 5 单击“确定”。

删除 McAfee 用户

您可以随时删除 McAfee 用户。

删除 McAfee 用户：

- 1 以管理员用户身份登录 SecurityCenter。
- 2 打开“用户设置”窗格。

如何实现？

1. 在“常见任务”下，单击“主页”。
 2. 在 SecurityCenter 的“主页”窗格上，单击“家长监控”。
 3. 在“家长监控”信息区域中，单击“配置”。
 4. 在“家长监控配置”窗格上，单击“高级”。
- 3** 在“用户设置”窗格的“McAfee 用户帐户”下，选择用户名，然后单击“删除”。

编辑 McAfee 用户帐户的信息

您可以更改 McAfee 用户的密码、帐户类型或自动登录功能。

- 1** 以管理员用户身份登录 SecurityCenter。
- 2** 打开“用户设置”窗格。

如何实现？

1. 在“常见任务”下，单击“主页”。
 2. 在 SecurityCenter 的“主页”窗格上，单击“家长监控”。
 3. 在“家长监控”信息区域中，单击“配置”。
 4. 在“家长监控配置”窗格上，单击“高级”。
- 3** 在“用户设置”窗格中，单击用户名，然后单击“编辑”。
- 4** 按照屏幕上的说明编辑用户名的密码、帐户类型或“家长监控”保护。
- 5** 单击“确定”。

添加 McAfee 用户

在创建 McAfee 用户后，您可以为该用户配置“家长监控”保护。有关详细信息，请参阅家长监控帮助。

- 1** 以管理员用户身份登录 SecurityCenter。
- 2** 打开“用户设置”窗格。

如何实现？

1. 在“常见任务”下，单击“主页”。
 2. 在 SecurityCenter 的“主页”窗格上，单击“家长监控”。
 3. 在“家长监控”信息区域中，单击“配置”。
 4. 在“家长监控配置”窗格上，单击“高级”。
- 3** 在“用户设置”窗格上，单击“添加”。
- 4** 按照屏幕上的说明设置用户名、密码、帐户类型和“家长监控”保护。
- 5** 单击“创建”。

[切换到 Windows 用户](#)

为便于管理，McAfee 建议切换到 Windows 用户；不过，这样做之后，就无法重新切换到 McAfee 用户。

- 1** 打开“用户设置”窗格。

如何实现？

1. 在“常见任务”下，单击“主页”。
 2. 在 SecurityCenter 的“主页”窗格上，单击“家长监控”。
 3. 在“家长监控”信息区域中，单击“配置”。
 4. 在“家长监控配置”窗格上，单击“高级”。
- 2** 在“用户设置”窗格上，单击“切换”。
- 3** 配置操作。

使用 Windows 用户

默认情况下，SecurityCenter 用户对应于计算机上已建立的 Windows 用户。您可以在 Windows 中的“计算机管理”下添加用户、编辑用户帐户信息或删除用户。然后，可以在 SecurityCenter 中为这些用户设置“家长监控”保护。

如果从使用 McAfee 用户的早期版本的 SecurityCenter 升级，请参阅使用 McAfee 用户 (第 148 页)。

在 Web 上保护信息

您可以通过将个人信息添加到受保护的信息区域来防止个人信息(如姓名、地址、信用卡号和银行帐号)在 Web 上传输。

注意: 家长监控不会阻止安全网站(即使用 https:// 协议的网站, 如银行站点)所进行的个人信息传输。

本章内容

保护个人信息	154
--------------	-----

保护个人信息

通过阻止个人信息来防止个人信息（如姓名、地址、信用卡号和银行帐号）在 Web 上传输。如果 McAfee 检测到某些组件（如表单的字段或文件）中包含要通过 Web 发送的个人信息，则会发生以下情况：

- 如果您是管理员，则必须确认是否要发送信息。
- 如果您不是管理员，则会用星号 (*) 替换已阻止的部分。例如，如果恶意网站尝试将您的信用卡号发送给另一台计算机，则此号码本身会用星号代替。

保护个人信息

您可以阻止以下类型的个人信息：姓名、地址、邮政编码、社会保险号、电话号码、信用卡号、银行帐户、经纪人帐户和电话卡。如果要阻止不同类型的个人信息，可以将类型设置为“其他”。

1 打开“保护的信息”窗格。

如何实现？

1. 在“常见任务”下，单击“主页”。
 2. 在 SecurityCenter 的“主页”窗格中，单击“Internet 和网络”。
 3. 在“Internet 和网络”信息区域中，单击“配置”。
 4. 在“Internet 和网络配置”窗格中，确保启用了“个人信息”保护，然后单击“高级”。
- 2** 在“保护的信息”窗格上，单击“添加”。
- 3** 在列表中选择要阻止的信息类型。
- 4** 输入个人信息，然后单击“确定”。

保护密码

密码存储库是存放个人密码的安全存储区域。您可以利用它存储您的密码，不用担心其他用户（甚至管理员）访问它们。

本章内容

设置密码存储库.....	156
--------------	-----

设置密码存储库

在开始使用密码存储库之前，必须设置密码存储库的密码。只有知道此密码的用户才能访问密码存储库。如果忘记密码存储库密码，则可以重新设置此密码；不过，这会删除以前存储在密码存储库中的所有密码。

在设置密码存储库密码后，您可以添加、编辑或删除存储库中的密码。您还可以随时更改密码存储库密码。

重置密码存储库密码

如果忘记密码存储库密码，则可以重新设置此密码；不过，这会删除以前输入的所有密码。

1 打开“密码存储库”窗格。

如何实现？

1. 在“常见任务”下，单击“主页”。
2. 在 SecurityCenter 的“主页”窗格中，单击“Internet 和网络”。
3. 在“Internet 和网络”信息区域中，单击“配置”。
4. 在“Internet 和网络配置”窗格上，单击“密码存储库”下的“高级”。

2 单击“忘记了密码？”。

3 在“重置密码存储库”对话框的“密码”框中键入新密码，然后在“重新输入密码”中重新键入此新密码。

4 单击“重置”。

5 在“确认重置密码”对话框中，单击“是”。

更改您的密码存储库密码

您可以随时更改密码存储库密码。

1 打开“密码存储库”窗格。

如何实现？

1. 在“常见任务”下，单击“主页”。
 2. 在 SecurityCenter 的“主页”窗格中，单击“Internet 和网络”。
 3. 在“Internet 和网络”信息区域中，单击“配置”。
 4. 在“Internet 和网络配置”窗格上，单击“密码存储库”下的“高级”。
- 2** 在“密码存储库”窗格的“密码”框中键入当前密码，然后单击“打开”。
- 3** 在“管理密码存储库”窗格上，单击“更改密码”。
- 4** 在“选择密码”框中键入新密码，然后在“重新输入密码”框中重新键入此密码。
- 5** 单击“确定”。
- 6** 在“已更改密码存储库密码”对话框中，单击“确定”。

删除密码

您可以随时删除密码存储库中的密码。从存储库中删除密码后，将无法恢复密码。

- 1** 打开“密码存储库”窗格。
如何实现？
 1. 在“常见任务”下，单击“主页”。
 2. 在 SecurityCenter 的“主页”窗格中，单击“Internet 和网络”。
 3. 在“Internet 和网络”信息区域中，单击“配置”。
 4. 在“Internet 和网络配置”窗格上，单击“密码存储库”下的“高级”。

2 在“密码”框中键入密码存储库密码。

3 单击“打开”。

4 在“管理密码存储库”窗格中，单击密码条目，然后单击“删除”。

5 在“确认删除”对话框中，单击“是”。

修改密码

要确保密码存储库中的条目始终准确和可靠，必须在密码更改时更新这些条目。

- 1** 打开“密码存储库”窗格。

如何实现？

1. 在“常见任务”下，单击“主页”。
 2. 在 SecurityCenter 的“主页”窗格中，单击“Internet 和网络”。
 3. 在“Internet 和网络”信息区域中，单击“配置”。
 4. 在“Internet 和网络配置”窗格上，单击“密码存储库”下的“高级”。
- 2** 在“密码”框中键入密码存储库密码。
- 3** 单击“打开”。
- 4** 在“管理密码存储库”窗格中，单击密码条目，然后单击“编辑”。
- 5** 在“描述”框中修改密码的描述(如用于哪方面)，或在“密码”框中修改密码。
- 6** 单击“确定”。

添加密码

如果密码很难记住，则可以将其添加到密码存储库。密码存储库是一个安全位置，只能由了解密码存储库密码的用户访问。

- 1** 打开“密码存储库”窗格。
如何实现？
 1. 在“常见任务”下，单击“主页”。
 2. 在 SecurityCenter 的“主页”窗格中，单击“Internet 和网络”。
 3. 在“Internet 和网络”信息区域中，单击“配置”。
 4. 在“Internet 和网络配置”窗格上，单击“密码存储库”下的“高级”。

2 在“密码”框中键入密码存储库密码。

3 单击“打开”。

4 在“管理密码存储库”窗格上，单击“添加”。

5 在“描述”框中键入密码的描述(如用于哪方面)，然后在“密码”框中键入密码。

6 单击“确定”。

第 6 章

McAfee Backup and Restore

使用 McAfee® Backup and Restore 可以将文件存档至 CD、DVD、USB 驱动器、外部硬盘驱动器或网络驱动器，从而避免数据意外丢失。本地存档可以将个人数据存档（备份）到 CD、DVD、USB 驱动器、外部硬盘驱动器或网络驱动器。这便提供与您个人有关的记录、文档和其他资料的副本，以防意外丢失。

在开始使用 Backup and Restore 之前，您应熟悉某些最常用的功能。Backup and Restore 帮助会提供有关配置和使用这些功能的详细信息。在浏览程序的功能后，必须确保有足够的存档介质可用于本地存档。

注意： 在检测到重要和不重要的问题时，SecurityCenter 都会立即报告。如果您需要帮助来诊断保护问题，则可以运行 McAfee Virtual Technician。

本章内容

Backup and Restore 的功能.....	160
存档文件.....	161
处理已存档的文件.....	169

Backup and Restore 的功能

计划本地存档

通过将文件或文件夹存档到 CD、DVD、USB 驱动器、外部硬盘驱动器或网络驱动器来保护您的数据。在初次存档之后，系统会自动进行增量存档。

一次单击还原

如果误删除或损坏您计算机上的文件和文件夹，则可以通过所用的存档介质来还原最新存档的文件和文件夹。

压缩和加密

默认情况下，已存档的文件都会进行压缩，从而节省存档介质上的空间。作为额外的安全措施，系统会在默认情况下对存档进行加密。

存档文件

您可以使用 McAfee Backup and Restore 将计算机上的文件副本存档到 CD、DVD、USB 驱动器、外部硬盘驱动器或网络驱动器。以此种方式存档文件会在数据意外丢失或损坏时，轻松地获得信息。

在开始存档文件之前，必须选择默认的存档位置（CD、DVD、USB 驱动器、外部硬盘驱动器或网络驱动器）。McAfee 已预设了一些设置，例如要存档的文件夹和文件类型，不过您可以修改这些设置。

在设置本地存档选项后，您可以修改 Backup and Restore 运行完全存档或快速存档频率的默认设置。您可以随时运行手动存档。

本章内容

启用和禁用本地存档.....	162
设置存档选项.....	163
运行完全存档和快速存档.....	167

启用和禁用本地存档

第一次启动 Backup and Restore 时，可以根据您希望如何使用 Backup and Restore 来决定是否启用本地存档。一旦登录且开始使用 Backup and Restore，就可以随时启用或禁用本地存档。

如果您不希望将计算机上文件的副本存档到 CD、DVD、USB 驱动器、外部硬盘驱动器或网络驱动器，则可以禁用本地存档。

启用本地存档

如果您希望将计算机上文件的副本存档到 CD、DVD、USB 驱动器、外部硬盘驱动器或网络驱动器，则可以启用本地存档。

- 1** 在 SecurityCenter 中的“高级菜单”上，单击“配置”。
- 2** 在“配置”窗格上，单击“计算机和文件”。
- 3** 在“计算机和文件配置”窗格的“‘本地存档’处于禁用状态”下，单击“开”。

禁用本地存档

如果您不希望将计算机上文件的副本存档到 CD、DVD、USB 驱动器、外部硬盘驱动器或网络驱动器，则可以禁用本地存档。

- 1** 在 SecurityCenter 中的“高级菜单”上，单击“配置”。
- 2** 在“配置”窗格上，单击“计算机和文件”。
- 3** 在“计算机和文件配置”窗格的“‘本地存档’处于启用状态”下，单击“关”。

设置存档选项

在开始存档文件之前，必须设置某些本地存档选项。例如，必须设置监视位置和监视文件类型。监视位置是计算机上的文件夹，Backup and Restore 监视其是否有新文件或文件更改。监视文件类型是 Backup and Restore 在监视位置上存档的文件类型（如 .doc、.xls 等）。默认情况下，系统会存档以下文件类型；不过，您还可以存档其他文件类型。

- Microsoft® Word 文档 (.doc 和 .docx)
- Microsoft Excel® 电子表格 (.xls 和 .xlsx)
- Microsoft PowerPoint® 演示文稿 (.ppt 和 .pptx)
- Microsoft Project® 文件 (.mpp)
- Adobe® PDF 文件 (.pdf)
- 纯文本文件 (.txt)
- HTML 文件 (.html)
- 联合图像专家组文件 (.jpg 和 .jpeg)
- 标签图像格式文件 (.tif)
- MPEG Audio Stream III 文件 (.mp3)
- 视频文件 (.vdo)

注意：您不能存档以下文件类型：.ost 和 .pst。

您可以设置两种类型的监视位置：顶层文件夹及其子文件夹；仅限顶层文件夹。如果设置顶层文件夹及其子文件夹位置，Backup and Restore 会存档此文件夹及其子文件夹内的监视文件类型。如果设置顶层文件夹位置，Backup and Restore 仅存档此文件夹（不包含其子文件夹）中的监视文件类型。您还可以确定要从本地存档中排除的位置。默认情况下，Windows 桌面和“我的文档”位置设成顶层文件夹及其子文件夹监视位置。

在设置监视文件类型和位置之后，必须设置存档位置（即用于存储已存档数据的 CD、DVD、USB 驱动器、外部硬盘驱动器或网络驱动器）。您可以随时更改存档位置。

出于安全原因或大小问题，默认情况下会为已存档的文件启用加密或压缩。已加密的文件内容会从文本转换为代码，这样可以隐藏信息，不了解解密方法的人员将无法访问此信息。压缩文件会压缩成存储和传送所需空间最小的形式。虽然 McAfee 建议不要这样做，但您可以随时将其禁用。

在存档中包含位置

您可以设置两种用于存档的监视位置：顶层文件夹及其子文件夹；仅限顶层文件夹。如果设置顶层文件夹及其子文件夹位置，Backup and Restore 会监视文件夹及其子文件夹中的内容是否有更改。如果设置顶层文件夹位置，Backup and Restore 仅监视文件夹（不包含其子文件夹）的内容是否有更改。

1 打开“本地存档设置”对话框。

如何实现？

1. 单击“本地存档”选项卡。
2. 在左侧窗格中，单击“设置”。

2 单击“监视位置”。

3 执行下面某项操作：

- 要存档文件夹的内容（包括其子文件夹的内容），请单击“顶层存档文件夹和子文件夹”下的“添加文件夹”。
- 要存档文件夹的内容（但不包括其子文件夹的内容），请单击“顶层存档文件夹”下的“添加文件夹”。
- 要存档整个文件，请单击“顶层存档文件夹”下的“添加文件”。

4 在“浏览文件夹”（或“打开”）对话框中，导航到要监视的文件夹（或文件），然后单击“确定”。

5 单击“确定”。

提示：如果希望 Backup and Restore 监视尚未创建的文件夹，可以单击“浏览文件夹”对话框中的“创建新文件夹”，以添加文件夹并同时将其设置为监视位置。

设置存档文件类型

您可以指定在顶层文件夹及其子文件夹或顶层文件夹位置存档的文件类型。您可以从现有文件类型列表中选择，也可以将新类型添加到列表。

1 打开“本地存档设置”对话框。

如何实现？

1. 单击“本地存档”选项卡。
 2. 在左侧窗格中，单击“设置”。
- 2** 单击“文件类型”。
- 3** 展开文件类型列表，并选中要存档的文件类型旁的复选框。
- 4** 单击“确定”。

提示：要将新文件类型添加到“所选文件类型”列表，请在“将自定义文件类型添加到‘其他’”框中键入文件扩展名，单击“添加”，然后单击“确定”。新文件类型会自动变为监视文件类型。

从存档中排除位置

如果要禁止存档某个位置（文件夹）及其内容，可以从存档中排除此位置。

- 1** 打开“本地存档设置”对话框。
如何实现？
 1. 单击“本地存档”选项卡。
 2. 在左侧窗格中，单击“设置”。

2 单击“监视位置”。

3 单击“从备份中排除的文件夹”下的“添加文件夹”。

4 在“浏览文件夹”对话框中，导航到要排除的文件夹，进行选择，然后单击“确定”。

5 单击“确定”。

提示：如果希望 Backup and Restore 排除尚未创建的文件夹，则可以单击“浏览文件夹”对话框中的“创建新文件夹”，在添加文件夹的同时将其排除。

更改存档位置

在更改存档位置后，以前在其他位置存档的文件会作为“未存档”文件列出。

- 1** 打开“本地存档设置”对话框。
如何实现？
 1. 单击“本地存档”选项卡。
 2. 在左侧窗格中，单击“设置”。

2 单击“更改存档位置”。

3 在“存档位置”对话框中，执行以下任一操作：
 - 单击“选择 CD/DVD 刻录机”，单击“刻录机”列表中计算机的 CD 或 DVD 驱动器，然后单击“确定”。

- 单击“选择驱动器位置”，导航到 USB 驱动器、本地驱动器或外部硬盘驱动器，进行选择，然后单击“确定”。
 - 单击“选择网络位置”，导航到网络文件夹，选择文件夹，然后单击“确定”。
- 4** 验证“所选的存档位置”下的新存档位置，然后单击“确定”。
- 5** 在确认对话框中，单击“确定”。
- 6** 单击“确定”。

注意：当您更改存档位置时，以前存档的文件将在“状态”列中列为“未存档”。

禁用存档加密和压缩

加密已存档的文件会通过隐藏文件内容以使其不可读取来保护数据的机密性。压缩已存档的文件会有助于最大程度减少文件的大小。默认情况下，加密和压缩都会启用，不过，您可以随时禁用这些选项。

- 1** 打开“本地存档设置”对话框。

如何实现？

1. 单击“本地存档”选项卡。
 2. 在左侧窗格中，单击“设置”。
- 2** 单击“高级设置”。
- 3** 清除“启用加密功能以提高安全性”复选框。
- 4** 清除“启用压缩功能以减少存储空间”复选框。
- 5** 单击“确定”。

注意：McAfee 建议在存档文件时不要禁用加密和压缩。

运行完全存档和快速存档

您可以运行两种类型的存档：完全存档或快速存档。在运行完全存档时，会根据已设置的监视文件类型和位置对一组完整的数据进行存档。在运行快速存档时，会仅存档自上次完全存档或快速存档后已更改的受监视文件。

默认情况下，会安排 Backup and Restore 在每周一的上午 9:00 点对监视位置上的监视文件类型运行完全存档，而自上次完全存档或快速存档后每 48 小时运行一次快速存档。此计划会确保始终维护文件的最新存档。如果您不想每 48 小时存档一次，则可以调整计划以符合您的需要。

如果要按需存档监视位置的内容，则可以随时进行存档。例如，如果您修改了一个文件且要将其存档，但并未安排 Backup and Restore 在数小时后运行完全存档或快速存档，则可以手动存档文件。在手动存档文件时，为自动存档设置的间隔将会重置。

如果自动存档或手动存档在不适当的时间运行，还可以将其中断。例如，假设在您执行资源密集型任务时自动存档开始，那么您可以将其停止。在停止自动存档后，为自动存档设置的间隔将会重置。

计划自动存档

您可以设置完全存档和快速存档的频率，以确保数据始终得到保护。

1 打开“本地存档设置”对话框。

如何实现？

1. 单击“本地存档”选项卡。
2. 在左侧窗格中，单击“设置”。

2 单击“常规”。

3 要每日、每周或每月运行完全存档，请单击“完全存档频率”下的任一项：

- 日
- 周
- 月

4 选中要运行完全存档的日旁的复选框。

5 单击“于”列表中的值，以指定要运行完全存档的时间。

6 要以天或小时为基础运行快速存档，请单击“快速存档”下的任一项：

- 小时
- 天

- 7 在“快速存档频率”框中键入表示频率的数字。
- 8 单击“确定”。

注意: 您可以通过在“完全存档频率”下选择“手动”来禁用计划存档。

中断自动存档

Backup and Restore 会根据您定义的计划自动存档监视位置的文件和文件夹。但是，如果在自动存档正在进行时要将其中断，则可以随时将其中断。

- 1 在左侧窗格中，单击“停止存档”。
- 2 在确认对话框中，单击“是”。

注意: 只有在存档正在进行时，才会显示“停止存档”链接。

手动运行存档

尽管可以根据预先定义的计划运行自动存档，但也可以随时手动运行快速存档或完全存档。快速存档仅存档自上次完全存档或快速存档后已更改的文件。完全存档会存档所有监视位置上的监视文件类型。

- 1 单击“本地存档”选项卡。
- 2 执行下面某项操作：
 - 要运行快速存档，请单击左侧窗格中的“快速存档”。
 - 要运行完全存档，请单击左侧窗格中的“完全存档”。
- 3 在“开始存档”对话框中，检查您的存储空间和设置，然后单击“继续”。

处理已存档的文件

在存档一些文件后，可以使用 **Backup and Restore** 进行处理。已存档的文件会显示在传统的资源管理器视图中，您可以轻松查找它们。随着存档的增长，您可能要排序或搜索文件。您还可以直接在资源管理器视图中打开文件来检查内容，而无须检索文件。

如果文件的本地副本过期、丢失或损坏，则可以从存档中检索它们。**Backup and Restore** 还会提供管理本地存档和存储介质所需的信息。

本章内容

使用本地存档资源管理器.....	170
还原已存档的文件.....	172
管理存档.....	174

使用本地存档资源管理器

利用本地存档资源管理器可以查看和操纵已在本地存档的文件。您可以查看每个文件的名称、类型、位置、大小、状态（已存档、未存档或存档正在进行）和上次存档每个文件的日期。您还可以按任意条件排序文件。

如果存档很大，则通过搜索文件可以快速找到它。您可以搜索文件的全部或部分名称或路径，然后通过指定文件的大致大小和上次存档的大致日期来缩小搜索范围。

在找到文件后，可以直接在本地存档资源管理器中将其打开。Backup and Restore 会在其本机程序中打开文件，您无须离开本地存档资源管理器便可进行更改。此文件会保存到您计算机上的最初监视位置，并会根据已定义的存档计划自动存档。

排序已存档的文件

您可以按以下条件排序已存档的文件和文件夹：名称、文件类型、大小、状态（即已存档、未存档或存档正在进行）、上次存档文件的日期或计算机上的文件位置（路径）。

- 1** 单击“本地存档”选项卡。
- 2** 在右侧窗格中，单击列名。

搜索已存档的文件

如果存放已存档文件的库很大，则可以通过搜索此文件来快速找到它。您可以查找文件的所有或部分名称或路径，然后通过指定文件大致大小和上次存档的大致日期来缩小搜索范围。

- 1** 在屏幕顶部的“搜索”框中键入全部或部分文件名，然后按 Enter。
- 2** 在“全部或部分路径”框中，键入全部或部分路径。
- 3** 通过执行以下任一项，指定要搜索文件的大致大小：
 - 单击“小于 100 KB”、“小于 1 MB”或“大于 1 MB”。
 - 单击“大小(KB)”，然后从框中选择适当的大小值。
- 4** 通过指定以下任一项，指定上次存档文件的大致日期：
 - 单击“本周”、“本月”或“本年”。
 - 单击“指定日期”，在列表中单击“已存档”，然后从日期列表中单击适当的日期值。

5 单击“搜索”。

注意: 如果您不了解上次存档的大致大小或大致日期, 请单击“未知”。

打开已存档的文件

您可以在本地存档资源管理器中直接打开已存档的文件来检查其内容。

- 1** 单击“本地存档”选项卡。
- 2** 在右侧窗格中, 单击文件名, 然后单击“打开”。

提示: 您还可以通过双击文件名打开已存档的文件。

还原已存档的文件

如果受监视的文件已损坏、丢失或被错误删除，则可以从本地存档还原此文件的副本。出于此原因，请务必定期存档您的文件。您还可以从本地存档中还原较旧版本的文件。例如，如果您定期存档某个文件，但要将其还原到此文件的以前版本，则可以在存档位置查找此文件进行还原。如果存档位置是本地驱动器或网络驱动器，则可以浏览此文件。如果存档位置是外部硬盘驱动器或 USB 驱动器，则必须先将驱动器连接到计算机，然后才能浏览查找此文件。如果存档位置是 CD 或 DVD，则必须先将 CD 或 DVD 插入计算机，然后才能浏览查找此文件。

您还可以从另一台计算机还原已在某台计算机上存档的文件。例如，如果将一组文件存档到计算机 A 的外部硬盘驱动器，则可以在计算机 B 上还原这些文件。为此，必须在计算机 B 上安装 Backup and Restore 并连接上外部硬盘驱动器。然后，在 Backup and Restore 中浏览文件，这些文件即被添加到“缺少的文件”列表中以便于还原。

有关存档文件的详细信息，请参阅存档文件。如果您有意地从存档中删除某个受监视的文件，则还可以从“缺少的文件”列表中删除此条目。

从本地存档还原缺少的文件

使用 Backup and Restore 的本地存档可以恢复本地计算机上监视文件夹中缺少的数据。例如，如果将某个文件移出监视文件夹或将其删除，并且此文件已存档，则可以从本地存档将其还原。

- 1 单击“本地存档”选项卡。
- 2 在屏幕底部的“缺少的文件”选项卡上，选中您要还原的文件名称旁边的复选框。
- 3 单击“还原”。

提示：您可以单击“全部还原”来还原“缺少的文件”列表中的全部文件。

从本地存档还原较旧版本的文件

如果要还原较旧版本的已存档文件，则可以找到此文件并将其添加到“缺少的文件”列表中。然后，您可以像还原“缺少的文件”列表中的任何其他文件一样还原此文件。

- 1 单击“本地存档”选项卡。
- 2 在屏幕底部的“缺少的文件”选项卡上，单击“浏览”，然后找到存档的存储位置。

已存档的文件夹名称采用以下格式：cre ddmmmyy hh-mm-ss ***，其中 ddmmmyy 是存档文件的日期，hh-mm-ss 是存档文件的时间，

*** 是“Full”或“Inc”，这取决于是执行完全存档还是执行快速存档。

3 选择位置，然后单击“确定”。

所选位置包含的文件会显示在“缺少的文件”列表中，可以随时还原。有关详细信息，请参阅从本地存档还原缺少的文件(第 172 页)。

[从“缺少的文件”列表中删除文件](#)

如果将某个已存档的文件移到监视文件夹之外或将其删除，则它会自动显示在“缺少的文件”列表中。这便向您表明，已存档的文件和监视文件夹中包含的文件不一致。如果此文件是您有意移到监视文件夹之外或删除的，则可以从“缺少的文件”列表中删除此文件。

- 1** 单击“本地存档”选项卡。
- 2** 在屏幕底部的“缺少的文件”选项卡上，选中您要删除的文件名称旁边的复选框。
- 3** 单击“删除”。

提示：您可以单击“全部删除”来删除“缺少的文件”列表中的全部文件。

管理存档

您可以随时查看有关完全存档和快速存档的信息摘要。例如，您可以查看有关当前正在监视的数据量、已存档的数据量以及当前正在监视但尚未存档的数据量的信息。您还可以查看有关存档计划的信息，例如上次和下次存档的日期。

查看存档活动的摘要

您可以随时查看有关存档活动的信息。例如，您可以查看已存档文件的百分比、正在监视的数据大小、已存档的数据大小以及正在监视但尚未存档的数据大小。您还可以查看上次存档和下次存档发生的日期。

- 1** 单击“本地存档”选项卡。
- 2** 在屏幕的顶部，单击“帐户摘要”。

第 7 章

McAfee QuickClean

QuickClean 通过删除会在计算机上生成垃圾信息的文件来提高计算机的性能。它会清空回收站，删除临时文件、快捷方式、丢失的文件碎片、注册表文件、缓存文件、Cookie、浏览器历史记录文件、已发送和删除的电子邮件、最近使用的文件、Active-X 文件和系统还原点文件。QuickClean 还会使用 McAfee Shredder 组件安全且永久地删除可能包含敏感个人信息(如姓名和地址)的项目来保护您的隐私。有关清除文件的信息，请参阅 McAfee Shredder。

磁盘碎片整理程序可以整理计算机上的文件和文件夹，确保这些文件和文件夹在保存到计算机硬盘驱动器时不会分散(即碎片化)。定期对硬盘驱动器进行碎片整理，可以确保这些碎片化的文件和文件夹合并到一起，供以后快速检索。

如果不想手动维护计算机，则可以安排 QuickClean 和磁盘碎片整理程序以任一频率定期运行(作为独立的任务)。

注意： 在检测到重要和不重要的问题时，SecurityCenter 都会立即报告。如果您需要帮助来诊断保护问题，则可以运行 McAfee Virtual Technician。

本章内容

QuickClean 功能.....	176
清理计算机.....	177
对计算机进行碎片整理.....	180
计划任务.....	181

QuickClean 功能

文件清除程序

使用多种清除程序安全且高效地删除无用文件。通过删除这些文件，可以增加计算机硬盘驱动器上的空间，并提高其性能。

清理计算机

QuickClean 会删除在计算机上生成垃圾信息的文件。它会清空回收站，删除临时文件、快捷方式、丢失的文件碎片、注册表文件、缓存文件、Cookie、浏览器历史记录文件、已发送和删除的电子邮件、最近使用的文件、Active-X 文件和系统还原点文件。QuickClean 会删除这些项目，但不会影响其他重要信息。

您可以使用任一 QuickClean 的清除程序删除计算机中的无用文件。下表介绍 QuickClean 清除程序：

名称	功能
回收站清除程序	删除回收站中的文件。
临时文件清除程序	删除临时文件夹中存储的文件。
快捷方式清除程序	删除中断的快捷方式以及没有关联程序的快捷方式。
丢失的文件碎片清除程序	删除计算机中丢失的文件碎片。
注册表清除程序	删除计算机中不再存在的程序的 Windows® 注册表信息。 注册表是 Windows 存储其配置信息的数据库。注册表包含每个计算机用户的配置文件以及有关系统硬件、安装程序和属性设置的信息。Windows 运行时会持续引用此信息。
缓存清除程序	删除浏览网页时累积的缓存文件。这些文件通常以临时文件的形式存储在缓存文件夹中。 缓存文件夹是计算机上的临时存储区域。为提高 Web 浏览速度和效率，浏览器会在您下次查看某个网页时从其缓存（而不是从远程服务器）中检索该网页。
Cookie 清除程序	删除 Cookie。这些文件通常以临时文件的形式存储。 Cookie 是存储在个人浏览 Web 的计算机上且包含信息的小文件，通常包含用户名和当前日期和文件。网站主要使用 Cookie 来标识以前在站点注册或访问站点的用户；不过，Cookie 也可能被黑客的信息来源。
浏览器历史记录清除程序	删除 Web 浏览器历史记录。

名称	功能
Outlook Express 和 Outlook 电子邮件清除程序（已发送和删除的项目）	从 Outlook® 和 Outlook Express 中删除已发送和删除的电子邮件。
最近使用项的清除程序	删除使用以下任一程序生成的最近使用的文件： <ul style="list-style-type: none">▪ Adobe Acrobat®▪ Corel® WordPerfect® Office (Corel Office)▪ Jasc®▪ Lotus®▪ Microsoft® Office®▪ RealPlayer™▪ Windows History▪ Windows Media Player▪ WinRAR®▪ WinZip®
ActiveX 清除程序	删除 ActiveX 控件。 ActiveX 是程序或网页使用的软件组件，用于添加合并到程序或者网页且如同程序或网页正常部分的功能。大多数 ActiveX 控件是无害的；不过，某些控件可能会获取计算机中的信息。
系统还原点清除程序	删除计算机中旧的系统还原点(最近的还原点除外)。 系统还原点由 Windows 创建，用于标记对计算机所做的任何更改，以便在发生任何问题时，可以恢复到以前的状态。

本章内容

清理计算机..... 179

清理计算机

您可以使用任一 QuickClean 的清除程序删除计算机中的无用文件。完成后，可以在“QuickClean 摘要”下查看清理后回收的磁盘空间量、已删除的文件数量，以及上次 QuickClean 操作在计算机上运行的日期和时间。

- 1** 在“McAfee SecurityCenter”窗格的“常见任务”下，单击“维护计算机”。
- 2** 在“McAfee QuickClean”下，单击“开始”。
- 3** 执行下面任一操作：
 - 单击“下一步”接受列表中的默认清除程序。
 - 选择或清除适当的清除程序，然后单击“下一步”。如果选择最近使用项的清除程序，则可以单击“属性”以选择或清除最近使用列表中的程序创建的文件，然后单击“确定”。
 - 单击“恢复默认值”以恢复默认的清除程序，然后单击“下一步”。
- 4** 在执行分析后，单击“下一步”。
- 5** 单击“下一步”以确认文件删除。
- 6** 执行下面任一操作：
 - 单击“下一步”以接受默认值“否，我要使用标准 Windows 删除来删除文件”。
 - 单击“是，我要使用 Shredder 安全删除文件”，然后指定操作数量（最多 10 次），然后单击“下一步”。如果要删除大量信息，则清除文件是一个费时的过程。
- 7** 如果在清理期间有文件或项目被锁定，系统可能会提示您重新启动计算机。单击“确定”关闭该提示。
- 8** 单击“完成”。

注意： 使用 Shredder 删除的文件将无法恢复。有关清除文件的信息，请参阅 McAfee Shredder。

对计算机进行碎片整理

磁盘碎片整理程序可以整理计算机上的文件和文件夹，以便这些文件和文件夹在保存到计算机的硬盘驱动器时不会分散（即碎片化）。定期对硬盘驱动器进行碎片整理，可以确保这些碎片化的文件和文件夹合并到一起，供以后快速检索。

本章内容

对计算机进行碎片整理 180

对计算机进行碎片整理

您可以对计算机进行碎片整理，以提高文件和文件夹访问和检索的性能。

- 1** 在“McAfee SecurityCenter”窗格的“常见任务”下，单击“维护计算机”。
- 2** 在“磁盘碎片整理程序”下，单击“分析”。
- 3** 按照屏幕上的说明执行操作。

注意：有关磁盘碎片整理程序的详细信息，请参阅 Windows 帮助。

计划任务

任务计划程序会设置 QuickClean 或磁盘碎片整理程序在计算机上自动运行的频率。例如，您可以安排 QuickClean 任务在周日下午 9:00 点清空回收站，或安排磁盘碎片整理程序任务在每月的最后一天对计算机硬盘驱动器进行碎片整理。您可以随时创建、修改或删除任务。要运行计划的任务，您必须登录到计算机。如果任务因某种原因没有运行，则会在您再次登录后的五分钟重新计划该任务。

本章内容

计划 QuickClean 任务	181
修改 QuickClean 任务	182
删除 QuickClean 任务	183
计划磁盘碎片整理程序任务	183
修改磁盘碎片整理程序任务	184
删除磁盘碎片整理程序任务	184

计划 QuickClean 任务

您可以安排 QuickClean 任务使用一个或多个清除程序自动清理计算机。完成后，您可以在“QuickClean 摘要”下查看安排任务再次运行的日期和时间。

1 打开“任务计划程序”窗格。

如何实现？

- 1 在“McAfee SecurityCenter”的“常见任务”下，单击“维护计算机”。
 - 2 在“任务计划程序”下，单击“开始”。
- 2 在“选择要计划的操作”列表中，单击“McAfee QuickClean”。
- 3 在“任务名称”框中键入任务的名称，然后单击“创建”。
- 4 执行下面任一操作：
 - 单击“下一步”接受列表中的清除程序。
 - 选择或清除适当的清除程序，然后单击“下一步”。如果选择最近使用项的清除程序，则可以单击“属性”以选择或清除最近使用列表中的程序创建的文件，然后单击“确定”。
 - 单击“恢复默认值”以恢复默认的清除程序，然后单击“下一步”。

5 执行下面任一操作：

- 单击“计划”以接受默认值“否，我要使用标准 Windows 删除来删除文件”。
 - 单击“是，我要使用 Shredder 安全删除文件”，然后指定操作数量（最多 10 次），然后单击“计划”。
- 6** 在“计划”对话框中，选择希望任务运行的频率，然后单击“确定”。
- 7** 如果您对最近使用项的清除程序属性进行更改，系统可能会提示您重新启动计算机。请单击“确定”关闭该提示。
- 8** 单击“完成”。

注意： 使用 Shredder 删除的文件将无法恢复。有关清除文件的信息，请参阅 McAfee Shredder。

修改 QuickClean 任务

您可以修改计划的 QuickClean 任务，以更改该任务使用的清除程序或它在计算机上自动运行的频率。完成后，您可以在“QuickClean 摘要”下查看安排任务再次运行的日期和时间。

1 打开“任务计划程序”窗格。

如何实现？

1. 在“McAfee SecurityCenter”的“常见任务”下，单击“维护计算机”。
2. 在“任务计划程序”下，单击“开始”。
3. 在“选择要计划的操作”列表中，单击“McAfee QuickClean”。
4. 执行下面任一操作：
 - 单击“下一步”接受为此任务选定的清除程序。
 - 选择或清除适当的清除程序，然后单击“下一步”。如果选择最近使用项的清除程序，则可以单击“属性”以选择或清除最近使用列表中的程序创建的文件，然后单击“确定”。
 - 单击“恢复默认值”以恢复默认的清除程序，然后单击“下一步”。
5. 执行下面任一操作：
 - 单击“计划”以接受默认值“否，我要使用标准 Windows 删除来删除文件”。
 - 单击“是，我要使用 Shredder 安全删除文件”，然后指定操作数量（最多 10 次），然后单击“计划”。

- 6 在“计划”对话框中，选择希望任务运行的频率，然后单击“确定”。
- 7 如果您对最近使用项的清除程序属性进行更改，系统可能会提示您重新启动计算机。请单击“确定”关闭该提示。
- 8 单击“完成”。

注意：使用 Shredder 删除的文件将无法恢复。有关清除文件的信息，请参阅 McAfee Shredder。

删除 QuickClean 任务

如果不希望计划的 QuickClean 任务自动运行，可以删除此任务。

- 1 打开“任务计划程序”窗格。

如何实现？

1. 在“McAfee SecurityCenter”的“常见任务”下，单击“维护计算机”。
 2. 在“任务计划程序”下，单击“开始”。
- 2 在“选择要计划的操作”列表中，单击“McAfee QuickClean”。
 - 3 在“选择现有的任务”列表中选择任务。
 - 4 单击“删除”，然后单击“是”确认删除。
 - 5 单击“完成”。

计划磁盘碎片整理程序任务

您可以安排磁盘碎片整理程序任务来计划自动对计算机硬盘驱动器进行碎片整理的频率。整理完碎片后，您可以在“磁盘碎片整理程序”下查看安排任务再次运行的日期和时间。

- 1 打开“任务计划程序”窗格。

如何实现？

1. 在“McAfee SecurityCenter”的“常见任务”下，单击“维护计算机”。
 2. 在“任务计划程序”下，单击“开始”。
- 2 在“选择要计划的操作”列表中，单击“磁盘碎片整理程序”。
 - 3 在“任务名称”框中键入任务的名称，然后单击“创建”。
 - 4 执行下面任一操作：
 - 单击“计划”以接受默认的“即使可用空间很少，仍执行碎片整理”选项。

- 清除“即使可用空间很少，仍执行碎片整理”选项，然后单击“计划”。
- 5** 在“计划”对话框中，选择希望任务运行的频率，然后单击“确定”。
- 6** 单击“完成”。

修改磁盘碎片整理程序任务

您可以通过修改计划的磁盘碎片整理程序任务来更改它在计算机上自动运行的频率。完成后，可以在“磁盘碎片整理程序”下查看安排任务再次运行的日期和时间。

- 1** 打开“任务计划程序”窗格。

如何实现？

1. 在“McAfee SecurityCenter”的“常见任务”下，单击“维护计算机”。
2. 在“任务计划程序”下，单击“开始”。
- 2** 在“选择要计划的操作”列表中，单击“磁盘碎片整理程序”。
- 3** 在“选择现有的任务”列表中选择任务，然后单击“修改”。
- 4** 执行下面任一操作：
 - 单击“计划”以接受默认的“即使可用空间很少，仍执行碎片整理”选项。
 - 清除“即使可用空间很少，仍执行碎片整理”选项，然后单击“计划”。
- 5** 在“计划”对话框中，选择希望任务运行的频率，然后单击“确定”。
- 6** 单击“完成”。

删除磁盘碎片整理程序任务

如果不希望计划的磁盘碎片整理程序任务自动运行，可以删除此任务。

- 1** 打开“任务计划程序”窗格。

如何实现？

1. 在“McAfee SecurityCenter”的“常见任务”下，单击“维护计算机”。
 2. 在“任务计划程序”下，单击“开始”。
- 2** 在“选择要计划的操作”列表中，单击“磁盘碎片整理程序”。
- 3** 在“选择现有的任务”列表中选择任务。
- 4** 单击“删除”，然后单击“是”确认删除。
- 5** 单击“完成”。

第 8 章

McAfee Shredder

McAfee Shredder 可以永久删除（或清除）计算机硬盘驱动器中的项目。即使在您手动删除文件和文件夹，清空回收站，或删除 Temporary Internet Files 文件夹后，仍可以使用计算机分析工具恢复此信息。同样，因为某些程序会创建打开文件的临时隐藏副本，所以也可以恢复已删除的文件。Shredder 可以安全且永久地删除这些不需要的文件来保护您的隐私。切记，已清除的文件无法恢复。

注意： 在检测到重要和不重要的问题时，SecurityCenter 都会立即报告。如果您需要帮助来诊断保护问题，则可以运行 McAfee Virtual Technician。

本章内容

Shredder 功能	188
清除文件、文件夹和磁盘.....	189

Shredder 功能

永久删除文件和文件夹

删除计算机硬盘驱动器中的项目，这样便无法恢复与其相关的信息。Shredder 可以安全且永久地删除文件和文件夹、回收站和 Temporary Internet Files 文件夹中的项目以及计算机磁盘（如可重写光盘、外部硬盘驱动器和软盘）的整个内容，从而保护您的隐私。

清除文件、文件夹和磁盘

即使使用专门工具，Shredder 也会确保无法恢复回收站和 Temporary Internet Files 文件夹中已删除文件和文件夹所包含的信息。您可以使用 Shredder 指定要清除项目的次数（最多 10 次）。清除操作的次数越多，文件的安全删除级别就越高。

清除文件和文件夹

您可以清除计算机硬盘驱动器中的文件和文件夹，包括回收站和 Temporary Internet Files 文件夹中的项目。

1 打开“Shredder”。

如何实现？

- 1 在“McAfee SecurityCenter”窗格的“常见任务”下，单击“高级菜单”。
- 2 在左侧窗格中，单击“工具”。
- 3 单击“Shredder”。
- 2 在“清除文件和文件夹”窗格的“我想”下，单击“删除文件和文件夹”。
- 3 在“清除级别”下，单击以下任一清除级别：
 - **快速：** 清除选定项目一次。
 - **全面：** 清除选定项目 7 次。
 - **自定义：** 清除选定项目最多 10 次。
- 4 单击“下一步”。
- 5 执行下面任一操作：
 - 在“选择要清除的文件”列表中，单击“回收站内容”或“临时 Internet 文件”。
 - 单击“浏览”，导航到要清除的文件，选择此文件，然后单击“打开”。
- 6 单击“下一步”。
- 7 单击“开始”。
- 8 Shredder 完成后，单击“完成”。

注意：在 Shredder 完成任务前，请不要使用任何文件。

清除整个磁盘

您可以一次清除磁盘的整个内容。只能清除可以移动驱动器，如外部硬盘驱动器、可写光盘和软盘。

1 打开“Shredder”。

如何实现？

1. 在“McAfee SecurityCenter”窗格的“常见任务”下，单击“高级菜单”。
2. 在左侧窗格中，单击“工具”。
3. 单击“Shredder”。
- 2 在“清除文件和文件夹”窗格的“我想”下，单击“删除整个磁盘”。
- 3 在“清除级别”下，单击以下任一清除级别：
 - **快速：** 清除选定的驱动器一次。
 - **全面：** 清除选定驱动器 7 次。
 - **自定义：** 清除选定驱动器最多 10 次。
- 4 单击“下一步”。
- 5 在“选择磁盘”列表中，单击要清除的驱动器。
- 6 单击“下一步”，然后单击“是”以确认。
- 7 单击“开始”。
- 8 Shredder 完成后，单击“完成”。

注意：在 Shredder 完成任务前，请不要使用任何文件。

第 9 章

McAfee Network Manager

Network Manager 提供组成家庭网络的计算机和其他设备的图形视图。您可以使用 Network Manager 远程管理网络中每个托管计算机的保护状态，并在这些计算机上远程修复已报告的安全漏洞。如果您已经安装了 McAfee Total Protection，则 Network Manager 还可以监视您的网络中是否有入侵者（您无法识别或不信任的计算机或设备）尝试与其连接。

在使用 Network Manager 前，您可以熟悉某些功能。Network Manager 帮助提供有关配置和使用这些功能的详细信息。

注意： 在检测到重要和不重要的问题时，SecurityCenter 都会立即报告。如果您需要帮助来诊断保护问题，则可以运行 McAfee Virtual Technician。

本章内容

Network Manager 功能.....	192
了解 Network Manager 图标.....	193
设置托管网络.....	195
远程管理网络.....	201
监视您的网络.....	205

Network Manager 功能

图形网络图

查看组成家庭网络的计算机和设备的保护状态的图形概述。在更改网络（如添加计算机）时，网络图会识别这些更改。您可以刷新网络图，重命名网络，并显示或隐藏网络图的组件来自定义您的视图。您还可以查看网络图中任一设备的详细信息。

远程管理

管理组成家庭网络的计算机的保护状态。您可以邀请计算机加入托管网络，监视托管计算机的保护状态，并为网络上的远程计算机修复已知的安全漏洞。

网络监视

如果该功能可用的话，则会让 Network Manager 监视您的网络并在朋友或入侵者连接时通知您。只有当您购买了 McAfee Total Protection 之后，网络监视功能才可用。

了解 Network Manager 图标

下表介绍 Network Manager 网络图中最常用的图标。

图标	说明
	代表联机的托管计算机
	代表脱机的托管计算机
	代表已安装 SecurityCenter 的非托管计算机。
	代表脱机的非托管计算机
	代表没有安装 SecurityCenter 的联机计算机，或代表未知的网络设备
	代表没有安装 SecurityCenter 的脱机计算机，或代表脱机的未知网络设备
	表示已保护或已连接相应的项目
	表示相应的项目可能需要处理
	表示相应的项目需要立即处理
	代表无线家用路由器
	代表标准家用路由器
	代表连接后的 Internet
	代表断开连接后的 Internet

设置托管网络

要设置托管网络，请信任该网络（如果尚且不信任的话）并将成员（计算机）添加到该网络。在可以远程管理某台计算机或可以授予其权限以远程管理网络上的其他计算机之前，该计算机必须成为此网络的信任成员。具有管理权限的现有网络成员（计算机）可以将网络成员关系授予新计算机。

您可以查看与网络图上显示的任何项目关联的详细信息，甚至在对网络进行更改（如添加计算机）后也可以显示这些信息。

本章内容

使用网络图	196
加入托管网络	198

使用网络图

将计算机连接到网络时，Network Manager 会分析网络以确定是否有托管成员和非托管成员，路由器的属性是什么以及 Internet 状态。如果没有找到任何成员，则 Network Manager 会假定当前所连接的计算机是网络上的第一台计算机，并使此计算机成为具有管理权限的托管成员。默认情况下，网络名称包含连接到网络且安装了 SecurityCenter 安全软件的第一台计算机的名称；不过，您可以随时重命名网络。

在更改网络（如添加计算机）后，可以自定义网络图。例如，可以刷新网络图，重命名网络，并显示或隐藏网络图上的项目来自定义您的视图。您还可以查看与网络图中显示的任一项目相关联的详细信息。

访问网络图

网络图提供组成家庭网络的计算机和设备的图形表示。

- 在“基本菜单”或“高级菜单”上，单击“管理网络”。

注意：如果您尚未（使用 McAfee Personal Firewall）信任该网络，系统会在您首次访问网络图时信任该网络。

刷新网络图

您可以随时刷新网络图；例如，在其他计算机加入托管网络后刷新。

- 1 在“基本菜单”或“高级菜单”上，单击“管理网络”。
- 2 单击“我想”下的“刷新网络图”。

注意：只有当在网络图上的没有选择项目时，“刷新网络图”链接才可用。要清除项目，请单击所选项目，或单击网络图上的空白区域。

重命名网络

默认情况下，网络名称包含连接到网络且安装了 SecurityCenter 安全软件的第一台计算机的名称。如果您愿意使用其他名称，则可以更改此名称。

- 1 在“基本菜单”或“高级菜单”上，单击“管理网络”。
- 2 单击“我想”下的“重命名网络”。
- 3 在“网络名称”框中输入网络的名称。
- 4 单击“确定”。

注意：只有当在网络图上没有选择项目时，“重命名网络”链接才可用。要清除项目，请单击所选项目，或单击网络图上的空白区域。

显示或隐藏网络图中的项目

默认情况下，家庭网络中的所有计算机和设备都会显示在网络图中。不过，如果包含隐藏项目，您可以随时再次显示这些项目。只有非托管的项目才能隐藏；托管计算机无法隐藏。

要...	在“基本菜单”或“高级菜单”上，单击“管理网络”，然后执行以下操作...
隐藏网络图上的项目	单击网络图上的项目，然后单击“我想”下的“隐藏此项目”。在确认对话框中，单击“是”。
显示网络图中的隐藏项目	在“我想”下，单击“显示隐藏项目”。

查看项目的详细信息

如果您选择网络图上的任一组成部分，可以查看网络中任何项目的详细信息。此信息包含项目名称、其保护状态和管理该项目所需的其他信息。

- 1** 单击网络图上项目的图标。
- 2** 在“详细信息”下，查看有关项目的信息。

加入托管网络

在可以远程管理某台计算机或可以授予其权限以远程管理网络上的其他计算机之前，该计算机必须成为此网络的信任成员。具有管理权限的现有网络成员（计算机）可以将网络成员关系授予新计算机。为确保只有信任的计算机加入网络，授予权限的计算机和加入计算机的用户都必须互相进行身份验证。

在计算机加入网络时，系统会提示将其 McAfee 保护状态公开给网络上的其他计算机。如果计算机同意公开其保护状态，则它成为此网络的托管成员。如果计算机拒绝公开其保护状态，则它成为此网络的非托管成员。网络的非托管成员通常是要访问其他网络功能（如发送文件或共享打印机）的来宾计算机。

注意：在计算机加入网络后，如果您已安装了其他 McAfee 网络程序（如 EasyNetwork），这些程序也会将此计算机识别为托管计算机。分配给 Network Manager 中计算机的权限级别会应用于所有 McAfee 网络程序。有关在其他 McAfee 网络程序中来宾权限、完全权限或管理权限含义的详细信息，请参阅为此程序提供的文档。

加入托管网络

当您收到加入托管网络的邀请时，您可以接受或拒绝邀请。您还可以确定是否希望网络上的其他计算机管理此计算机的安全设置。

- 1 在“托管网络”对话框中，确保选中“允许此网络上的每台计算机管理安全设置”复选框。
- 2 单击“加入”。
在接受邀请后，会显示两个卡片。
- 3 确认卡片与邀请您加入托管网络的计算机上显示的卡片相同。
- 4 单击“确定”。

注意：如果邀请您加入托管网络的计算机显示的卡片与安全确认对话框中显示的卡片不同，则表明托管网络上有安全隐患。加入此网络可能会使您的计算机面临风险；因此，单击“托管网络”对话框中的“取消”。

邀请计算机加入此托管网络

如果已将计算机添加到托管网络或网络中存在其他非托管计算机，则可以邀请此计算机加入托管网络。只有网络上具有管理权限的计算机才能邀请其他计算机加入。发送邀请时，还可以指定要分配给加入计算机的权限级别。

- 1** 单击网络图上非托管计算机的图标。
- 2** 单击“我想”下的“管理此计算机”。
- 3** 在“邀请计算机加入此托管网络”对话框中，单击以下任一选项：
 - 单击“允许对托管网络程序的来宾访问权限”以允许计算机访问网络（您可以对家庭中的临时用户使用此选项）。
 - 单击“允许对托管网络程序的完全访问权限”以允许计算机访问网络。
 - 单击“允许对托管网络程序的管理访问权限”以允许计算机以管理权限访问网络。它还允许计算机将访问权限授予要加入托管网络的其他计算机。
- 4** 单击“确定”。
加入托管网络的邀请会发给此计算机。在计算机接受邀请后，会显示两个卡片。
- 5** 确认卡片与邀请您加入托管网络的计算机上显示的卡片相同。
- 6** 单击“授予访问权限”。

注意：如果邀请您加入托管网络的计算机显示的卡片与安全确认对话框中显示的卡片不同，则表明托管网络上有安全隐患。允许此计算机加入网络可能会使其他计算机面临风险；因此，单击安全确认对话框中的“拒绝访问”。

停止信任网络上的计算机

如果您误信任网络中的其他计算机，则可以停止信任它们。

- 单击“我想”下的“停止信任此网络上的计算机”。

注意: 如果您具有管理权限，并且网络上有其他托管计算机，则“停止信任此网络上的计算机”链接不可用。

远程管理网络

在设置托管网络后，您可以远程管理组成网络的计算机和设备。您可以管理计算机和设备的状态和权限级别，然后远程修复大多数安全漏洞。

本章内容

管理状态和权限.....	202
修复安全漏洞.....	204

管理状态和权限

托管网络包含托管成员和非托管成员。托管成员允许网络上的其他计算机管理其 McAfee 保护状态；而非托管成员则不会这样做。非托管成员通常是要访问其他网络功能（如发送文件或共享打印机）的来宾计算机。非托管计算机可以随时由网络上具有管理权限的其他托管计算机邀请成为托管计算机。同样，具有管理权限的托管计算机可以随时使另一个托管计算机不受管理。

托管计算机具有管理权限、完全权限或来宾权限。管理权限允许托管计算机管理网络上所有其他托管计算机的保护状态，并将其他计算机与网络的成员关系授予这些计算机。完全和来宾权限仅允许计算机访问网络。您可以随时修改计算机的权限级别。

因为托管网络可能还包含设备（如路由器），所以可以使用 Network Manager 管理这些设备。您还可以配置和修改网络图上设备的显示属性。

管理计算机的保护状态

如果网络上某台计算机的保护状态未受管理（此计算机不是网络成员，即为非托管成员），则可以要求管理它。

- 1** 单击网络图上非托管计算机的图标。
- 2** 单击“我想”下的“管理此计算机”。

停止管理计算机的保护状态

您可以停止管理网络中托管计算机的保护状态，不过，如果此后该计算机变为非托管计算机，您就不能远程管理其保护状态。

- 1** 单击网络图上托管计算机的图标。
- 2** 单击“我想”下的“停止管理此计算机”。
- 3** 在确认对话框中，单击“是”。

修改托管计算机的权限

您可以随时更改托管计算机的权限。此功能允许您修改可以管理网络上其他计算机的保护状态的计算机。

- 1** 单击网络图上托管计算机的图标。
- 2** 单击“我想”下的“修改此计算机的权限”。
- 3** 在修改权限对话框中，选中或清除复选框，以确定此计算机和托管网络中的其他计算机是否可以互相管理各自的保护状态。
- 4** 单击“确定”。

管理设备

您可以从网络图中访问设备的管理网页来管理设备。

- 1 单击网络图上的设备图标。
- 2 单击“我想”下的“管理此设备”。
此时会打开 Web 浏览器并显示设备的管理网页。
- 3 在 Web 浏览器中，提供您的登录信息并配置设备的安全设置。

注意：如果此设备是受 McAfee Wireless Network Security 保护的无线路由器或接入点，则必须使用 Wireless Network Security 配置设备的安全设置。

修改设备的显示属性

修改设备的显示属性时，可以更改网络图上设备的显示名称，并指定此设备是否是无线路由器。

- 1 单击网络图上的设备图标。
- 2 单击“我想”下的“修改设备属性”。
- 3 指定设备的显示名称，在“名称”框中键入名称。
- 4 要指定设备的类型，请单击“标准路由器”（如果不是无线路由器）或“无线路由器”（如果是无线路由器）。
- 5 单击“确定”。

修复安全漏洞

具有管理权限的托管计算机可以管理网络上其他托管计算机的 McAfee 保护状态，并远程修复报告的安全漏洞。例如，如果托管计算机的 McAfee 保护状态指出已禁用 VirusScan，则具有管理权限的其他托管计算机都可以远程启用 VirusScan。

远程修复安全漏洞时，Network Manager 会修复大多数报告的问题。不过，某些安全漏洞可能需要在本地计算机上进行手动干预。在此情况下，Network Manager 会修复可以远程修复的问题，然后提示您修复其余的问题，方法是登录到有漏洞计算机上的 SecurityCenter，然后按照提供的建议执行操作。在某些情况下，建议的解决方案是在远程计算机或网络上的计算机上安装最新版 SecurityCenter。

修复安全漏洞

您可以使用 Network Manager 在远程托管计算机上修复大多数安全漏洞。例如，如果在远程计算机上禁用了 VirusScan，则可以启用它。

- 1 单击网络图上项目的图标。
- 2 查看“详细信息”下项目的保护状态。
- 3 单击“我想”下的“修复安全漏洞”。
- 4 如果已修复安全问题，请单击“确定”。

注意：尽管 Network Manager 会自动修复大多数安全漏洞，但某些修复可能会要求您在有漏洞的计算机上打开 SecurityCenter，并按照提供的建议进行操作。

在远程计算机上安装 McAfee 安全软件

如果网络上的一台或多台计算机没有使用最新版 SecurityCenter，则无法远程管理其保护状态。如果要远程管理这些计算机，则必须转至每台计算机，并安装最新版 SecurityCenter。

- 1 请确保您按照要远程管理的计算机上的说明执行操作。
- 2 准备好 McAfee 登录信息，即第一次激活 McAfee 软件时使用的电子邮件地址和密码。
- 3 在浏览器中，访问 McAfee 网站，登录，然后单击“我的帐户”。
- 4 找到要安装的产品，单击它的“下载”按钮，然后按照屏幕上的说明执行操作。

提示：您还可以通过打开您的网络图并在“我想”下单击“保护我的 PC”，来了解如何在远程计算机上安装 McAfee 安全软件。

监视您的网络

如果您安装了 McAfee Total Protection, Network Manager 还会监视您的网络中是否有入侵者。每当有未知计算机或设备连接到您的网络时, 您就会获得相应的通知, 以便您可以确定该计算机或设备是朋友还是入侵者。朋友是您能够识别且信任的计算机或设备, 入侵者是指您无法识别或不信任的计算机或设备。如果您将某台计算机或设备标记为“朋友”, 您可以决定在该朋友每次连接到您的网络时, 您是否希望得到通知。如果您将某台计算机或设备标记为入侵者, 我们将在其每次连接时自动提醒您。

在安装或升级到该版本的 Total Protection 之后, 当您第一次连接到某个网络时, 我们会自动将每台计算机或设备标记为朋友, 以后, 当这些计算机或设备连接到该网络时, 我们将不会通知您。在三天之后, 我们会开始将连接到该网络的每台未知计算机或设备通知给您, 以便您能够对它们进行标记。

注意: 网络监视是 Network Manager 的一个功能, 它只能与 McAfee Total Protection 一起使用。有关 Total Protection 的详细信息, 请访问我们的网站。

本章内容

停止监视网络	205
重新启用网络监视通知	206
标记为入侵者	206
标记为朋友	207
停止检测新朋友	207

停止监视网络

如果您禁用了网络监视功能, 那么, 当入侵者连接到您的家庭网络或您连接到的任何其他网络时, 我们将不能再向您发出警报。

1 打开“Internet 和网络配置”窗格。

如何实现?

1. 在“常见任务”下, 单击“主页”。
2. 在 SecurityCenter 的“主页”窗格中, 单击“Internet 和网络”。
3. 在“Internet 和网络”信息区域中, 单击“配置”。

2 在“网络监视”下, 单击“关”。

重新启用网络监视通知

尽管您可以禁用网络监视通知，但是我们不建议您这样做。如果您禁用网络监视通知，那么，在未知计算机或入侵者连接到您的网络时，我们将不能再通知您。如果您无意中禁用了这些通知（例如，如果您在警报中选中“不再显示此警报”复选框），则可以随时重新启用它们。

1 打开“警报选项”窗格。

如何实现？

1. 在“常见任务”下，单击“主页”。
2. 在右侧窗格的“SecurityCenter 信息”下，单击“配置”。
3. 在“警报”下，单击“高级”。
4. 在“SecurityCenter 配置”窗格上，单击“信息警报”。
5. 在“信息警报”窗格中，确保以下复选框处于清除状态：
 - 在新 PC 或设备连接到网络时不显示警报
 - 在入侵者连接到网络时不显示警报
 - 对于我通常希望获得其相关通知的朋友不显示警报
 - 在检测到未知的 PC 或设备时不提醒我
 - 在 McAfee 完成对新朋友的检测时不向我发出警报
6. 单击“确定”。

标记为入侵者

如果您无法识别或不信任网络上的某台计算机或设备，则可以将其标记为入侵者。每当它连接到您的网络时，我们将自动向您发出警报。

1. 在“基本菜单”或“高级菜单”上，单击“管理网络”。
2. 在网络图上，单击某个项目。
3. 在“我想”下面，单击“标记为朋友或入侵者”。
4. 在该对话框中，单击“入侵者”。

标记为朋友

只有当您能够识别且信任网络上的某台计算机或设备时，才将它标记为朋友。如果您将某台计算机或设备标记为“朋友”，您还可以决定在它每次连接到您的网络时，您是否希望获得通知。

- 1** 在“基本菜单”或“高级菜单”上，单击“管理网络”。
- 2** 在网络图上，单击某个项目。
- 3** 在“我想”下面，单击“标记为朋友或入侵者”。
- 4** 在该对话框中，单击“朋友”。
- 5** 为了在该朋友每次连接到该网络时获得通知，请选中“在该计算机或设备连接到网络时通知我”复选框。

停止检测新朋友

在连接到装有此版本的 Total Protection 的网络之后的前三天，我们会将每台计算机或设备自动标记为您不希望获得其相关通知的朋友。在这三天内，您可以随时停止这个自动标记功能，但是您以后无法重新启动它。

- 1** 在“基本菜单”或“高级菜单”上，单击“管理网络”。
- 2** 单击“我想”下的“停止检测新朋友”。

第 10 章

McAfee EasyNetwork

EasyNetwork 允许您安全地共享文件，简化文件传输，以及在家庭网络中的计算机之间共享打印机。不过，网络中的计算机必须安装 EasyNetwork 才能访问其功能。

在使用 EasyNetwork 前，您可以熟悉某些功能。EasyNetwork 帮助提供有关配置和使用这些功能的详细信息。

注意： 在检测到重要和不重要的问题时，SecurityCenter 都会立即报告。如果您需要帮助来诊断保护问题，则可以运行 McAfee Virtual Technician。

本章内容

EasyNetwork 功能.....	210
设置 EasyNetwork	211
共享和发送文件.....	217
共享打印机.....	223

EasyNetwork 功能

EasyNetwork 提供以下功能。

文件共享

使用 EasyNetwork 可以轻松地与网络上的其他计算机共享文件。共享文件时，可以授予其他计算机对这些文件的只读访问权限。只有对托管网络具有完全或管理访问权限的计算机（成员）才能共享或访问其他成员共享的文件。

文件传输

您可以将文件发到对托管网络具有完全或管理访问权限的其他计算机（成员）。接收文件后，此文件会显示在 EasyNetwork 收件箱中。收件箱是一个临时存储位置，用于存储网络上的其他计算机发给您的所有文件。

自动共享打印机

在加入托管网络后，您可以将打印机的当前名称用作共享打印机名称，与其他成员共享连接到您计算机的任何本地打印机。它还会检测由网络上其他计算机共享的打印机，并允许您配置和使用这些打印机。

设置 EasyNetwork

在可以使用 EasyNetwork 之前，必须打开它并加入托管网络。在加入托管网络后，您可以共享、搜索并将文件发到网络上的其他计算机。您还可以共享打印机。如果您决定离开网络，则可以随时离开。

本章内容

打开 EasyNetwork.....	211
加入托管网络.....	212
离开托管网络.....	215

打开 EasyNetwork

可以从 Windows “开始” 菜单或通过双击桌面上的 EasyNetwork 图标来打开 EasyNetwork。

- 在“开始”菜单上，依次指向“程序”和“McAfee”，然后单击“McAfee EasyNetwork”。

提示：您还可以通过双击桌面上的 McAfee EasyNetwork 图标来打开 EasyNetwork。

加入托管网络

如果您所连接到的网络上的计算机都没有安装 SecurityCenter，则您可以成为此网络的成员，而且系统会提示标识是否信任此网络。作为加入网络的第一台计算机，您的计算机名称包含在网络名称中；不过，您可以随时重命名网络。

在计算机连接到网络时，它会将加入请求发给网络上的其他计算机。此网络上具有管理权限的任何计算机都可以授予此请求访问权限。授予方还可以确定加入网络的计算机的权限级别；例如，来宾权限（仅限文件传输）或完全权限/管理权限（文件传输和文件共享）。在 EasyNetwork 中，具有管理访问权限的计算机可以将访问权限授予其他计算机并管理权限（提升或降低计算机的权限）；具有完全访问权限的计算机不能执行这些管理任务。

注意：在计算机加入网络后，如果您已安装了其他 McAfee 网络程序（如 Network Manager），则这些程序也会将此计算机识别为托管计算机。分配给 EasyNetwork 中计算机的权限级别会应用于所有 McAfee 网络程序。有关在其他 McAfee 网络程序中来宾权限、完全权限或管理权限含义的详细信息，请参阅为此程序提供的文档。

加入网络

当计算机在安装 EasyNetwork 后首次连接到信任的网络时，会显示一条消息，询问是否加入托管网络。如果计算机同意加入，则会将请求发给网络上具有管理访问权限的所有其他计算机。在计算机可以共享打印机或文件，或发送网络上的文件副本之前，必须授予此请求访问权限。网络上的第一台计算机会自动授予管理权限。

- 1** 在“共享文件”窗口中，单击“加入此网络”。
当网络上的管理计算机准予您的请求时，会显示一条消息，询问是否允许此计算机和网络上的其他计算机互相管理对方的安全设置。
- 2** 要允许此计算机和网络上的其他计算机互相管理对方的安全设置，请单击“确定”；否则，请单击“取消”。
- 3** 确认授予权限的计算机显示安全确认对话框中所显示的图片，然后单击“确定”。

注意：如果邀请您加入托管网络的计算机显示的图片与安全确认对话框中显示的图片不同，则表明托管网络上有安全隐患。加入此网络可能会使您的计算机面临风险；因此，请单击安全确认对话框中的“取消”。

授予对网络的访问权限

在计算机请求加入托管网络时，系统会将一条消息发给网络上具有管理访问权限的其他计算机。进行响应的第一台计算机成为授予方。作为授予方，您负责决定授予此计算机哪种类型的访问权限：来宾、完全或管理权限。

- 1** 在警报中，单击相应的访问级别。
- 2** 在“邀请计算机加入此托管网络”对话框中，单击以下任一选项：
 - 单击“允许对托管网络程序的来宾访问权限”以允许计算机访问网络（您可以对家庭中的临时用户使用此选项）。
 - 单击“允许对托管网络程序的完全访问权限”以允许计算机访问网络。
 - 单击“允许对托管网络程序的管理访问权限”以允许计算机以管理权限访问网络。它还允许计算机将访问权限授予要加入托管网络的其他计算机。
- 3** 单击“确定”。
- 4** 确认计算机显示安全确认对话框中所显示的图片，然后单击“授予访问权限”。

注意：如果计算机显示的图片与安全确认对话框中显示的图片不同，则表明托管网络上有安全隐患。授予此计算机对网络的访问权限可能会使其他计算机面临风险；因此，请单击安全确认对话框中的“拒绝访问”。

重命名网络

默认情况下，网络名称包含加入网络的第一台计算机的名称；不过，您可以随时更改网络名称。重命名网络时，可以更改 EasyNetwork 中显示的网络描述。

- 1** 在“选项”菜单中，单击“配置”。
- 2** 在“配置”对话框的“网络名称”框中，键入网络名称。
- 3** 单击“确定”。

离开托管网络

如果您加入托管网络，然后决定不希望作为其成员，则可以离开网络。在离开托管网络后，您可以随时重新加入；不过，您必须再次被授予权限。有关加入的详细信息，请参阅加入托管网络（第 212 页）。

离开托管网络

您可以离开以前加入的托管网络。

- 1** 断开计算机与网络的连接。
- 2** 在 EasyNetwork 中的“工具”菜单上，单击“离开网络”。
- 3** 在“离开网络”对话框中，选择要离开的网络名称。
- 4** 单击“离开网络”。

共享和发送文件

使用 EasyNetwork 可以轻松地与网络中的其他计算机共享文件及互发文件。共享文件时，可以授予其他计算机对这些文件的只读访问权限。只有作为托管网络成员（具有完全或管理访问权限）的计算机才能共享或访问由其他成员计算机共享的文件。

注意：如果您共享大量文件，则您的计算机资源可能会受到影响。

本章内容

共享文件.....	218
将文件发给其他计算机.....	220

共享文件

只有作为托管网络成员（具有完全或管理访问权限）的计算机才能共享或访问由其他成员计算机共享的文件。如果共享文件夹，则会共享包含在此文件夹及其子文件夹中的所有文件；不过，不会自动共享后续添加到此文件夹中的文件。如果删除了共享文件或文件夹，则会从“共享文件”窗口中将其删除。您可以随时停止共享文件。

要访问共享文件，请直接从 EasyNetwork 中打开文件，或将其复制到您的计算机上，然后在您的计算机上打开文件。如果共享文件的列表很大，而且很难找到文件的位置，则可以搜索文件。

注意：使用 EasyNetwork 共享的文件无法在其他计算机上通过 Windows 资源管理器进行访问，因为 EasyNetwork 文件共享必须通过安全连接进行。

共享文件

共享文件后，对托管网络具有完全或管理访问权限的所有成员都可以使用此文件。

- 1 在 Windows 资源管理器中，确定要共享的文件的位置。
- 2 在 Windows 资源管理器中将文件从其位置拖到 EasyNetwork 的“共享文件”窗口中。

提示：您还可以单击“工具”菜单上的“共享文件”来共享文件。在“共享”对话框中，导航到存储要共享文件的文件夹，选择文件，然后单击“共享”。

停止共享文件

如果在托管网络中共享文件，则可以随时停止共享。停止共享文件后，托管网络的其他成员便不能访问此文件。

- 1 在“工具”菜单中，单击“停止共享文件”。
- 2 在“停止共享文件”对话框中，选择不再共享的文件。
- 3 单击“确定”。

复制共享文件

您可以复制共享文件，这样可以在文件不再共享后仍可使用此文件。您可以从托管网络的任何计算机中复制共享文件。

- 将文件从 EasyNetwork 中的“共享文件”窗口拖到 Windows 资源管理器中的某个位置，或拖到 Windows 桌面。

提示：您还可以复制共享文件，方法是在 EasyNetwork 中选择文件，然后单击“工具”菜单上的“复制到”。在“复制到文件夹”对话框中，导航到要复制文件的文件夹，然后单击“保存”。

搜索共享文件

您可以搜索已由您或任何其他网络成员共享的文件。在键入搜索条件后，EasyNetwork 会在“共享文件”窗口中显示相应的结果。

- 1** 在“共享文件”窗口中，单击“搜索”。
- 2** 单击“包含”列表中的相应选项（第 219 页）。
- 3** 在“文件名或路径名”列表中键入部分或全部文件名或路径。
- 4** 单击“类型”列表中相应的文件类型（第 219 页）。
- 5** 在“开始”和“结束”列表中，单击表示创建文件的日期范围的日期。

搜索标准

下表描述搜索共享文件时可以指定的搜索标准。

文件或路径的名称

包含	说明
包含全部词语	搜索包含您在“文件名或路径名”列表中以任何顺序指定的所有词语的文件名或路径名。
包含任一词语	搜索包含您在“文件名或路径名”列表中指定的任何词语的文件名或路径名。
包含准确的字符串	搜索包含您在“文件名或路径名”列表中指定的准确短语的文件名或路径名。

文件的类型

类型	说明
任一	搜索所有共享文件类型。
文档	搜索所有共享文档。
图像	搜索所有共享图像文件。
视频	搜索所有共享视频文件。
音频	搜索所有共享音频文件。
已压缩	搜索所有已压缩的文件（如 .zip 文件）。

将文件发给其他计算机

您可以将文件发给作为托管网络成员的其他计算机。EasyNetwork 在发送文件之前，会确认接收文件的计算机是否有足够的可用磁盘空间。

接收文件后，此文件会显示在 EasyNetwork 收件箱中。收件箱是一个临时存储位置，用于存储网络上的其他计算机发给您的文件。如果接收文件时打开了 EasyNetwork，则文件会立即显示在收件箱中；否则，会在任务栏右侧的通知区域显示一条消息。如果您不想接收通知消息（如这些消息会打断您的工作），则可以关闭此功能。如果收件箱中存在同名的文件，则会用数字后缀重命名新文件。在您接受文件（将其复制到您的计算机）之前，文件会留在收件箱中。

将文件发送到另一台计算机

您可以将文件发送到托管网络上的另一台计算机，而不共享此文件。接收计算机上的用户要查看此文件，必须将它保存到本地位置。有关详细信息，请参阅接受另一台计算机发来的文件（第 220 页）。

- 1 在 Windows 资源管理器中，确定要发送的文件的位置。
- 2 在 Windows 资源管理器中将文件从其位置拖到 EasyNetwork 的活动计算机图标。

提示：选择文件时按 CTRL 可以将多个文件发给计算机。您还可以单击“工具”菜单上的“发送”，选择文件，然后单击“发送”来发送文件。

接受另一台计算机发来的文件

如果托管网络上的其他计算机将文件发给您，则您必须将其保存到计算机上来接受此文件。如果文件发送到您计算机时 EasyNetwork 没有运行，则您会在任务栏右侧的通知区域中收到一条通知消息。单击此通知消息可以打开 EasyNetwork 并访问文件。

- 单击“已接收”，然后将文件从 EasyNetwork 收件箱拖到 Windows 资源管理器中的文件夹。

提示：您还可以接收其他计算机发来的文件，方法是选择 EasyNetwork 收件箱中的文件，然后单击“工具”菜单上的“接受”。在“接受到文件夹”对话框中，导航到要保存接收文件的文件夹，然后单击“保存”。

发送文件时接收通知

您可以在托管网络上的其他计算机向您发送文件时接收通知消息。如果 EasyNetwork 没有运行，则通知消息会出现在任务栏右侧的通知区域。

- 1** 在“选项”菜单中，单击“配置”。
- 2** 在“配置”对话框中，选中“其他计算机向我发送文件时通知我”复选框。
- 3** 单击“确定”。

共享打印机

在加入托管网络后，EasyNetwork 会共享连接到您计算机的本地打印机，并将打印机的名称用作共享打印机名称。EasyNetwork 还会检测由网络上其他计算机共享的打印机，并允许您配置和使用这些打印机。

如果您配置了打印机驱动程序以通过网络打印服务器（如无线 USB 打印服务器）进行打印，则 EasyNetwork 会将此打印机认为是本地打印机，并在网络上进行共享。您还可以随时停止共享打印机。

本章内容

使用共享打印机.....	224
--------------	-----

使用共享打印机

EasyNetwork 会检测网络上计算机共享的打印机。如果 EasyNetwork 检测到未连接到您计算机的远程打印机，则会在您首次打开 EasyNetwork 时，在“共享文件”窗口中显示“可用的网络打印机”链接。然后，您便可以安装可用打印机或卸载已连接到您计算机上的打印机。您还可以刷新打印机的列表以确保您可以查看最新的信息。

如果您尚未加入托管网络，但已连接到此网络，则可以在 Windows 打印机控制面板上访问共享打印机。

停止共享打印机

停止共享打印机后，各成员便无法使用此打印机。

- 1** 在“工具”菜单上，单击“打印机”。
- 2** 在“管理网络打印机”对话框中，单击您不再共享的打印机的名称。
- 3** 单击“不共享”。

安装可用的网络打印机

如果您是托管网络的成员，则可以访问共享的打印机；不过，您必须安装打印机使用的打印机驱动程序。如果打印机的所有者停止共享其打印机，则不能使用此打印机。

- 1** 在“工具”菜单上，单击“打印机”。
- 2** 在“可用的网络打印机”对话框中，单击打印机名称。
- 3** 单击“安装”。

参考

词汇表列出并定义 McAfee 产品中最常用的安全术语。

词汇表

8

802.11

一组通过无限网络传输数据的标准。802.11 通常称为 Wi-Fi。

802.11a

对 802.11 的扩展，使用 5 GHz 频段以最高 54 Mbps 传输数据。尽管此标准的传输速度超过 802.11b，但覆盖距离较短。

802.11b

对 802.11 的扩展，使用 2.4 GHz 频段以最高 11 Mbps 传输数据。尽管此标准的传输速度比 802.11b 慢，但覆盖距离较长。

802.1x

有线和无线网络上的身份验证标准。802.1x 通常与 802.11 无线网络结合使用。另请参阅身份验证 (第 236 页)。

A

ActiveX 控件

程序或网页使用的软件组件，用于添加如同程序或网页正常部分的功能。大多数 ActiveX 控件是无害的；不过，某些控件可能会获取计算机中的信息。

C

Cookie

由许多网站用来存储有关已访问网页的信息的小型文本文件，存储在浏览网站的用户的计算机上。Cookie 中可能包含登录或注册信息、购物车信息或用户喜好。网站主要使用 Cookie 来标识以前在网站注册或访问网站的用户；不过，Cookie 也可能是黑客的信息来源。

D

DAT

检测定义文件（又称为特征码文件），其中包含的定义用来标识、检测和修复病毒、特洛伊木马、间谍软件、广告软件和其他可能有害程序 (PUP)。

DNS

域名系统。将 IP 地址（如 11.2.3.44）转换为域名（如 www.mcafee.com）的数据库系统。

E

ESS

扩展服务集。构成一个子网的两个或多个网络。

I

IP 地址

Internet 协议地址。用来标识 TCP/IP 网络上计算机或设备的地址。IP 地址的格式是 32 位的数字地址，采用句点分隔的四个数字的形式表示。每个数字可以是 0 到 255（如 192.168.1.100）。

IP 伪造

伪造 IP 数据包中的 IP 地址。在许多类型的攻击（包括会话劫持）中都使用此地址。它还常用于伪造垃圾邮件的电子邮件标题，以使这些邮件无法正确跟踪。

L

LAN

局域网。一种涵盖相对较小区域（如一座建筑物）的计算机网络。LAN 上的计算机可以互相通信并共享资源，如打印机和文件。

launchpad

U3 接口组件，充当启动和管理 U3 USB 程序的起始点。

M

MAC 地址

媒体访问控制地址。分配给访问网络的物理设备（NIC，即网络接口卡）的唯一序列号。

MAPI

消息应用程序编程接口。Microsoft 接口规范，能使不同的消息和工作组程序（包括电子邮件、语音、语音邮件和传真）通过一个客户端（如 Exchange 客户端）来工作。

MSN

Microsoft 网络。由 Microsoft Corporation 提供的一组基于 Web 的服务，包括搜索引擎、电子邮件、即时消息和门户网站。

N

NIC

网络接口卡。插在膝上型计算机或其他设备上，并将设备连接到 LAN 的一个卡。

P

PCI 无线适配器卡

外部部件互连。插入计算机 PCI 扩展插槽的无线适配器卡。

POP3

邮局协议 3。电子邮件客户端程序和电子邮件服务器之间的接口。大多数家庭用户都有一个 POP3 电子邮件帐户，也称为标准电子邮件帐户。

PPPoE

以太网上的点对点协议。点对点协议 (PPP) 拨号协议与以太网一起进行数据传送的一种方法。

R

RADIUS

远程访问拨入用户服务。通常在远程访问环境中允许进行用户身份验证的协议。此协议最初定义为与拨入远程访问服务器一起使用，此协议现在用于各种身份验证环境中，包括 WLAN 用户共享密钥的 802.1x 身份验证。另请参阅共享密钥。

Rootkit

授予用户对计算机或计算机网络的管理员级访问权限的工具（程序）集合。Rootkit 可能包含间谍软件和其他可能有害的程序，这些程序可能会对您的计算机数据和个人信息带来额外的安全或隐私风险。

S

SMTP

简单邮件传输协议。它是将消息从网络上的一台计算机发送到另一台计算机所使用的 TCP/IP 协议。Internet 上使用此协议来传送电子邮件。

SSID

服务集标识符。标识 Wi-Fi (802.11) 网络的一种标记（密钥）。SSID 由网络管理员建立，而且必须由希望加入网络的用户提供。

SSL

安全套接字层。Netscape 为在 Internet 上传输专用文档而开发的协议。SSL 通过使用公钥加密在 SSL 连接上传输的数据来工作。需要 SSL 连接的 URL 都以 HTTPS 而不是以 HTTP 开头。

SystemGuard

McAfee 会检测对计算机未经授权的更改并在出现更改时提醒您。

T

TKIP

临时密钥完整性协议（读音为 tee-kip）。无线 LAN 的 802.11i 加密标准的一部分。TKIP 是下一代 WEP，用于保护 802.11 无线 LAN。TKIP 提供每数据包的密钥混和、消息完整性检查和密钥重建机制，从而修复 WEP 的缺陷。

U

U3

代表 You: Simplified, Smarter, Mobile, 即“您：简单、智能和移动”。一种直接从 USB 驱动器运行 Windows 2000 或 Windows XP 程序的平台。M-Systems 和 SanDisk 在 2004 年发明了 U3 方案，用户可以利用它在 Windows 上运行 U3 程序，而无须在计算机上安装或存储数据或设置。

URL

统一资源定位器。标准的 Internet 地址格式。

USB

通用串行总线。目前大多数计算机上符合行业标准的连接器，可连接多个设备（从键盘和鼠标到网络摄像头、扫描仪和打印机）。

USB 驱动器

插入计算机 USB 端口的小型内存驱动器。USB 驱动器就像一个小型磁盘驱动器，利用它可以轻松地将文件从一台计算机传输到另一台计算机。

USB 无线适配器卡

插入计算机 USB 端口的无线适配器卡。

V

VPN

虚拟专用网。通过主机网络（如 Internet）配置的专用通信网络。通过 VPN 连接进行的数据传输经过加密而且拥有强安全功能。

W

Web 邮件

基于 Web 的邮件。主要通过 Web 浏览器而不是通过基于计算机的客户端（如 Microsoft Outlook）访问的电子邮件服务。另请参阅电子邮件（第 232 页）。

WEP

有线等效加密。定义为 Wi-Fi (802.11) 标准一部分的加密和身份验证协议。最初的版本以 RC4 密码为基础，并有严重缺陷。WEP 会尝试对通过无线电波传输的数据进行加密来提供安全性，以便数据在从一个端点传输到另一个端点时获得保护。不过，已发现 WEP 并没有以前所认为的那样安全。

Wi-Fi

无线保真。Wi-Fi Alliance 提及任何类型的 802.11 网络时所使用的术语。

Wi-Fi Alliance

由主要的无线硬件和软件提供商组成的组织。Wi-Fi Alliance 的使命是认证所有基于 802.11 产品的互操作性，以及对于基于 802.11 的所有无线 LAN 产品的所有市场，将术语 Wi-Fi 推广为全球品牌名称。此组织的性质就像协会、测试实验室以及要提高行业增长的厂商的信息交流中心。

Wi-Fi Certified

由 Wi-Fi Alliance 测试和批准。Wi-Fi Certified 产品被认为是可互操作的，即使来自不同的制造商也是如此。使用具有 Wi-Fi Certified 产品的用户可以将任何品牌的接入点 (AP) 与同样经过认证的任何其他客户端硬件品牌一起使用。

WLAN

无线局域网。使用无线连接的局域网 (LAN)。WLAN 使用高频无线电波而不是有线线路在计算机之间进行通信。

WPA

Wi-Fi 保护访问。一种规范标准，可以极大增强现有的和将来的无线 LAN 系统的数据保护和访问控制级别。WPA 设计作为软件升级在现有的硬件上运行，WPA 从 802.11i 标准派生，并与其兼容。正确安装后，即会高度保证无线 LAN 用户的数据会受到保护，而且只有经授权的网络用户才能访问网络。

WPA-PSK

专为不需要强企业级安全性且无权访问身份验证服务器的家庭用户设计的专用 WPA 模式。在此模式下，家庭用户需要手动输入启动密码，以采用“预共享密钥”模式来激活 Wi-Fi 保护访问，并应定期更改每个无线计算机和接入点上的密码短语。另请参阅 WPA2-PSK (第 231 页) 和 TKIP (第 229 页)。

WPA2

WPA 安全标准的更新，它基于 802.11i 标准。

WPA2-PSK

与 WPA-PSK 类似的专用 WPA 模式，它基于 WPA2 标准。WPA2-PSK 的一种常见功能是，设备通常会同时支持多个加密模式（如 AES、TKIP），而旧设备通常一次仅支持一个加密模式（即所有客户端将必须使用相同的加密模式）。

汉字（拼音）

按需扫描

按计划检查选定的文件、应用程序或网络设备以查找威胁、漏洞或其他可能有害的代码。它可以立即执行、在将来计划的时间内执行，或者按计划的间隔定期执行。与按访问扫描进行比较。另请参阅漏洞。

白名单

被视为安全的网站或电子邮件地址的列表。白名单上的网站是指允许用户进行访问的网站。白名单上的电子邮件地址来自您要接收其邮件的可信来源。与黑名单 (第 233 页) 进行比较。

暴力攻击

黑客用来查找密码或密钥的方法，做法是尝试每个可能的字符组合，直到破解加密为止。

备份

创建重要文件的副本（通常在安全的联机服务器上）。与存档（第 232 页）进行比较。

标准电子邮件帐户

请参阅 POP3（第 228 页）。

病毒

一种在没有权限或用户不知情的情况下可自行复制并感染计算机的计算机程序。

拨号程序

一种软件，将 Internet 连接重定向到用户默认 ISP（Internet 服务提供商）以外的其他方，以便增加内容提供商、供应商或其他第三方的连接费用。

插件

一个用来为大型软件添加功能或对其进行增强的小型软件程序。例如，Web 浏览器利用插件可以访问和执行嵌在 HTML 文档中且浏览器通常无法识别其格式（如动画、视频和音频文件）的文件。

存档

在 CD、DVD、USB 驱动器、外部硬盘驱动器或网络驱动器上创建重要文件的副本。与备份（第 232 页）进行比较。

代理

计算机或其上运行的软件，它仅向外部站点提供单个网络地址，从而在网络和 Internet 之间构筑了一个屏障。代理代表所有内部计算机，从而在保护网络身份的同时仍提供对 Internet 的访问。另请参阅代理服务器（第 232 页）。

代理服务器

用于管理 Internet 与局域网（LAN）之间通讯的防火墙组件。代理服务器可通过提供经常请求的数据（如常用网页）来提高性能，以及过滤和丢弃所有者认为不适当的请求，如未经授权访问专用文件的请求。

带宽

固定时间段内可以传输的数据量（吞吐量）。

电子邮件

电子邮件。以电子形式通过计算机网络收发的邮件。另请参阅 Web 邮件（第 230 页）。

电子邮件客户端

在计算机上运行的用于收发电子邮件的程序（例如 Microsoft Outlook）。

端口

用来将数据传入和传出计算设备的硬件位置。个人计算机有各种类型的端口，其中包括用来连接磁盘驱动器、监视器和键盘的内部端口，以及用来连接调制解调器、打印机、鼠标和其他外围设备的外部端口。

恶意接入点

未授权的接入点。恶意接入点可能安装在安全的公司网络中，将网络访问权限授予未授权的各方。还可以创建恶意接入点来允许攻击者执行中间人攻击。

发布

使已备份的文件在 Internet 上公开使用的过程。您可以搜索 Backup and Restore 库来访问已发布的文件。

防火墙

专用于防止对专用网络或来自专用网络的未经授权访问的系统（硬件、软件或软硬兼具）。防火墙常用于防止未经授权的 Internet 用户访问连接到 Internet 的专用网络，特别是在内部网络中更是如此。进入或离开内部网的所有消息都会通过防火墙，防火墙会检查每条消息，并拦截不符合指定安全标准的消息。

服务器

接受来自其他计算机或程序的连接并返回适当响应的计算机或程序。例如，每次您收发电子邮件时，您的电子邮件程序会连接到电子邮件服务器。

隔离

强制隔离怀疑含有病毒、垃圾邮件、可疑内容或可能有害程序 (PUP) 的文件或文件夹，以便文件或文件夹无法打开或执行。

共享

允许电子邮件收件人在有限的时间段内访问所选备份文件。在共享文件后，您会将此文件的备份副本发给您指定的电子邮件收件人。收件人会收到一封由 Backup and Restore 发来的电子邮件，指出文件已共享。电子邮件还包含指向共享文件的链接。

共享密钥

在开始通信前，已在两个通信方之间共享的字符串或密钥（通常为密码）。它用于保护 RADIUS 消息的敏感部分。另请参阅 RADIUS (第 229 页)。

黑名单

在 Anti-Spam 中，您不希望接收其所发送邮件的电子邮件地址的列表，因为您认为这些邮件会是垃圾邮件。在防网络钓鱼中，这是被认为具有欺诈行为的网站列表。与白名单 (第 231 页) 进行比较。

缓冲区溢出

可疑程序或可疑进程尝试在计算机缓冲区（临时数据存储区）中存储的数据超过其所能存放的数据时，在操作系统或应用程序中发生的一种情况。缓冲区溢出会损坏内存或覆盖相邻缓冲区中的数据。

缓存

计算机上的临时存储区域，用来存储经常或最近访问的数据。例如，为提高 Web 浏览速度和效率，浏览器会在您下次查看某个网页时，从其缓存而不是从远程服务器中检索该网页。

回收站

垃圾箱的一种模拟形式，可以存放 Windows 中的已删除文件和文件夹。

集成网关

将接入点 (AP)、路由器和防火墙的功能合并在一起的一种设备。某些设备还包含增强的安全功能和桥接功能。

加密

一种对信息进行编码以便未授权的各方无法访问它的方法。在对数据编码之后，该过程使用“密钥”和数学算法。没有正确的密钥，就无法对加密信息进行解密。病毒有时使用加密功能来尝试逃避检测。

家庭网络

家庭中互相连接的两台或多台计算机，它们可以共享网络和 Internet 访问。另请参阅 LAN (第 228 页)。

监视位置

计算机上由 Backup and Restore 监视的文件夹。

监视文件类型

Backup and Restore 在监视位置备份或存档的文件类型（例如 .doc 和 .xls）。

脚本

可以自动执行（即没有用户交互）的命令列表。与程序不同，脚本通常以纯文本的形式存储，并在每次运行时进行编译。宏和批处理文件也称为脚本。

接入点 (AP)

一种网络设备（通常称为无线路由器），可以插入以太网集线器或交换机来扩展无线用户的实际服务范围。在无线用户持有移动设备漫游时，数据传输会从一个接入点切换到另一个接入点，从而保持连接性。

节点

连接到网络上的单台计算机。

拒绝服务 (DOS) 攻击

一种减缓或阻止网络上通讯的计算机、服务器或网络的攻击类型。当网络被许多额外的请求淹没，以至于常规通讯很缓慢或完全中断时，就是发生了这种攻击。拒绝服务攻击将大量假连接请求发送到其目标，使目标忽略合法请求。

可能有害的程序 (PUP)

可能有害的软件程序，无论用户是否同意下载它。它可能会修改装有它的计算机的安全性或隐私设置。PUP 可能（但不一定）包括间谍软件、广告软件和拨号程序，而且可能随用户所需的程序一起下载。

可信列表

您信任且不进行检测的项目的列表。如果您误信任某个项目（例如，可能有害的程序或注册表更改），或者您希望再次检测此项目，则必须将其从该列表中删除。

客户端

在个人计算机或工作站上运行并依赖服务器执行某些操作的程序。例如，电子邮件客户端是允许您收发电子邮件的应用程序。

快捷方式

只包含计算机上另一个文件位置的文件。

临时文件

操作系统或某个其他程序在内存或磁盘中创建的文件，在会话过程中会使用此文件，然后将其丢弃。

浏览器

用于查看 Internet 上网页的程序。常用的 Web 浏览器有 Microsoft Internet Explorer 和 Mozilla Firefox。

路由器

将数据包从一个网络转发到另一个网络的网络设备。路由器会读取每个传入的数据包，然后根据来源地址和目标地址以及当前通讯情况来决定如何转发该数据包。有时路由器也称为接入点 (AP)。

漫游

在不中断服务或不丢失连接的情况下，从一个接入点 (AP) 覆盖区域移到另一个接入点覆盖区域。

密码

访问计算机、程序或网站所使用的代码（通常由字母和数字组成）。

密码存储库

存放个人密码的安全存储区域。您可以利用它存储您的密码，不用担心其他用户（甚至管理员）访问它们。

密文

加密的文本。除非将密文转换为明文（即已解密），否则密文是不可读的。另请参阅加密（第 234 页）。

密钥

两台设备对通信进行身份验证所使用的一组字母和数字。两台设备都必须有密钥。另请参阅 WEP（第 230 页）、WPA（第 231 页）、WPA2（第 231 页）、WPA2-PSK（第 231 页）和 WPA-PSK（第 231 页）。

明文

没有加密的文本。另请参阅加密（第 234 页）。

内部网

通常位于组织内部的一种专用计算机网络，只能由授权用户进行访问。

内容评级组

家长控制中用户所属的年龄组。根据用户所属的内容评级组使内容可用或将其阻止。内容评级组包括：幼儿、儿童、青少年（较小）、青少年（较大）和成人。

热点

由 Wi-Fi (802.11) 接入点 (AP) 覆盖的地理界限。使用无线膝上型计算机进入热点的用户可以连接到 Internet，前提是该热点正在发送信标（即公告其存在），而且不需要身份验证。热点通常位于人口密集的地区，如机场。

蠕虫

通过在其他驱动器、系统或网络上创建其自身副本进行扩散的病毒。邮件散播蠕虫是要求用户干预传播（例如，打开附件或执行下载的文件）的蠕虫。当今的大部分电子邮件病毒都是蠕虫。自行传播的蠕虫不需要用户干预即可传播。Blaster 和 Sasser 就是自行传播的蠕虫。

扫台者

配备 Wi-Fi 计算机以及某种专用硬件或软件的人员，他们驾车在城市间穿梭以搜索 Wi-Fi (802.11) 网络。

身份验证

验证电子通信发送者的数字身份的过程。

实时扫描

在您或您的计算机访问文件和文件夹时，扫描其中是否有病毒和其他活动的过程。

事件

在计算机系统或程序中，可以由安全软件按照预定义的条件检测到的事件或事情。通常，事件触发操作，如发送通知或者在事件日志中添加条目。

弹出窗口

出现在计算机屏幕上其他窗口上的小窗口。Web 浏览器常使用弹出窗口显示广告。

特洛伊，特洛伊木马

一个不会进行复制但会损坏或威胁计算机安全的程序。通常，特洛伊木马是由别人通过电子邮件发给您的，它不会通过电子邮件自行发送。特洛伊木马也可能无意间从网站或通过对等网络下载。

同步

解决已备份文件与本地计算机上存储的文件之间的不一致问题。如果联机备份库中的文件版本比其他计算机上的文件版本新，您可以同步文件。

外部硬盘驱动器

位于计算机外的硬盘驱动器。

网络

组合成一个逻辑单元的一系列基于 IP 的系统（如路由器、交换机、服务器和防火墙）。例如，“财务网络”可能包括为财务部门提供服务的所有服务器、路由器和系统。另请参阅家庭网络（第 234 页）。

网络臭虫

可以将自身嵌入 HTML 页面的小型图形文件，使未经授权的来源在您的计算机上设置 Cookie。然后，这些 Cookie 可以将信息传输到未经授权的来源。网络臭虫还称为“Web 信标”、“像素标记”、“透明 GIF”或“不可见的 GIF”。

网络钓鱼

一种通过发送看上去源自受信任来源（如银行或合法公司）的伪造电子邮件，来欺诈性地获取个人信息（如密码、社会保险编号和信用卡详细信息）的方法。通常，网络钓鱼电子邮件会请求收件人单击电子邮件中的链接来验证或更新联系详细信息或信用卡信息。

网络驱动器

连接到网络上的服务器并由多个用户共享的磁盘驱动器或磁带驱动器。有时也将网络驱动器称为远程驱动器。

网络图

组成家庭网络的计算机和组件的图形表示。

文件碎片

分布在磁盘上的文件残余。添加或删除文件时会产生文件碎片，可能会降低计算机的性能。

无线适配器

在计算机或 PDA 上增加无线功能的设备。可以通过 USB 端口、PC 卡 (CardBus) 插槽、内存卡插槽或在内部插入 PCI 总线进行连接。

系统还原点

计算机内存或数据库的内容的快照（映像）。Windows 会定期及在发生重要系统事件（如安装程序或驱动程序）时创建还原点。您还可以随时创建和命名自己的还原点。

消息身份验证代码 (MAC)

用于对在两台计算机之间传送的消息进行加密的安全代码。如果计算机认为解密代码是有效的，则会接收消息。

协议

一组允许计算机或设备交换数据的规则。在分层网络构架（开放系统互连模型）中，每一层都有其各自的协议，指定如何在该层上进行通信。您的计算机或设备必须支持正确的协议，才能与其他计算机通信。另请参阅开放系统互连 (OSI)。

压缩

将文件压缩成存储或传送所需空间最小的形式的过程。

域

本地子网或 Internet 上站点的描述符。在局域网 (LAN) 中，域是由一个安全数据库控制的客户端和服务器计算机组成的子网。在 Internet 上，域是每个 Web 地址的一部分。例如，在 www.mcafee.com 中，mcafee 是域。

智能驱动器

请参阅 USB 驱动器(第 230 页)。

中间人攻击

拦截而且有可能修改双方之间消息的一种方法，通信双方的任一方都不知道其通信链路遭破坏。

注册表

Windows 用来存储有关每个计算机用户、系统硬件、已安装程序和属性设置的配置信息的数据。该数据库可拆分成多个设置了值的项。有害程序可能会更改注册表项的值，或者创建新的注册表项，以执行恶意代码。

字典攻击

一种暴力攻击类型，使用常用的词来尝试发现密码。

关于 McAfee

McAfee, Inc. 的总部设在加利福尼亚的 Santa Clara, 它在入侵防护和安全风险管理方面居于世界领先地位, 可以为世界各地的系统和网络提供前瞻性和成熟的安全解决方案及服务。McAfee 具有无可比拟的安全经验和勇于创新的精神, 可以帮助家庭用户、企业、公共部门和服务提供商有效阻止攻击、防止破坏以及持续跟踪和提高其安全性。

许可

致全体用户: 请仔细阅读与您所购买的许可相关的法律协议, 以了解使用许可软件的一般条款和条件。如果您不清楚所购买的许可属于哪一类, 请查看软件包装盒中或购买产品时单独提供的销售文档以及其他相关的许可授权或订单文档, 这些文档既可以是小册子、产品光盘上的文件, 也可以是软件包下载网站提供的文件。如果您不接受该协议规定的条款和条件, 请勿安装本软件。根据情况, 您可以将产品退回 McAfee, Inc. 或原购买处以获得全额退款。

版权

版权所有 © 2008 McAfee, Inc. 保留所有权利。未经 McAfee, Inc. 的书面许可，不得以任何形式或手段将本出版物的任何内容复制、传播、转录、存储于检索系统或翻译成任何语言。本文档包含的 McAfee 和其它商标是 McAfee, Inc. 和/或其子公司在美国和/或其它国家或地区的注册商标或商标。与安全内容相关的 McAfee 红色是 McAfee 品牌产品的特色。本文档中所有其它已注册和未注册商标以及受版权保护的材料均为其各自所有者专有。

商标归属

AVERT、EPO、EPOLICY ORCHESTRATOR、FLASHBOX、
FOUNDSTONE、GROUPSHIELD、HERCULES、INTRUSHIELD、
INTRUSION、INTELLIGENCE、LINUXSHIELD、MANAGED MAIL
PROTECTION、MAX (MCAFEE SECURITY ALLIANCE
EXCHANGE)、MCAFEE、MCAFEE.COM、NETSHIELD、
PORTALSHIELD、PREVENTSYS、PROTECTION-IN-DEPTH
STRATEGY、PROTECTIONPILOT、SECURE MESSAGING
SERVICE、SECURITY ALLIANCE、SITEADVISOR、THREATSCAN、
TOTAL PROTECTION、VIREX 和 VIRUSSCAN。

客户服务和技术支持

在检测到重要和不重要的问题时，SecurityCenter 会立即报告。重要保护问题需要立即采取操作，并且会更改保护状态（将颜色改为红色）。不重要的保护问题不需要立即采取操作，可能会（也可能不会）更改保护状态（取决于问题类型）。要获得绿色保护状态，您必须修复所有重要问题，修复或忽略所有不重要的问题。如果您需要帮助来诊断保护问题，则可以运行 McAfee Virtual Technician。有关 McAfee Virtual Technician 的详细信息，请参阅 McAfee Virtual Technician 帮助。

如果您已从 McAfee 之外的合作伙伴或提供商购买安全软件，请打开 Web 浏览器，然后访问 www.mcafeehelp.com。然后，在“Partner Links”（合作伙伴）链接下，选择您的合作伙伴或供应商来访问 McAfee Virtual Technician。

注意：要安装和运行 McAfee Virtual Technician，则必须以 Windows 管理员身份登录计算机。如果无法这样做，则 MVT 可能无法解决问题。有关以 Windows 管理员身份登录的信息，请参阅 Windows 帮助。在 Windows Vista™ 中，系统会在您运行 MVT 时提示您。在系统提示时，请单击“Accept”（接受）。Virtual Technician 无法与 Mozilla® Firefox 一起使用。

本章内容

使用 McAfee Virtual Technician.....	241
支持和下载.....	242

使用 McAfee Virtual Technician

Virtual Technician 就像一名技术支持代表人员，收集有关您的 SecurityCenter 程序的信息，从而可以帮助您解决计算机的保护问题。运行 Virtual Technician 时，它会进行检查以确保 SecurityCenter 程序在正常工作。如果发现问题，Virtual Technician 会进行修复，或向您提供有关这些问题的详细信息。完成后，Virtual Technician 会显示其分析结果，并允许寻求 McAfee 的其它技术支持（如果需要）。

为保持您计算机和文件的安全性和完整性，Virtual Technician 不会收集可识别您个人身份的信息。

注意：有关 Virtual Technician 的详细信息，请单击 Virtual Technician 中的“帮助”图标。

启动 Virtual Technician

Virtual Technician 会收集有关 SecurityCenter 程序的信息，以便可以帮助您解决保护问题。为保护您的隐私，此信息不包含可识别个人身份的信息。

- 1** 在“常见任务”下，单击“McAfee Virtual Technician”。
- 2** 请按照屏幕上的说明下载并运行 Virtual Technician。

支持和下载

请参阅下表来了解您所在国家或地区的 McAfee 支持和下载站点，包括《用户手册》。

支持和下载

国家/地区	McAfee 支援	McAfee 下载
澳大利亚	www.mcafeehelp.com	au.mcafee.com/root/downloads.asp
巴西	www.mcafeeajuda.com	br.mcafee.com/root/downloads.asp
加拿大 (英文)	www.mcafeehelp.com	ca.mcafee.com/root/downloads.asp
加拿大 (法文)	www.mcafeehelp.com	ca.mcafee.com/root/downloads.asp?langid=48
中国 (简体中文)	www.mcafeehelp.com	cn.mcafee.com/root/downloads.asp
捷克共和国	www.mcafeenapoveda.com	cz.mcafee.com/root/downloads.asp
丹麦	www.mcafeehjaelp.com	dk.mcafee.com/root/downloads.asp
芬兰	www.mcafeehelp.com	fi.mcafee.com/root/downloads.asp
法国	www.mcaafeaide.com	fr.mcafee.com/root/downloads.asp
德国	www.mcafeehilfe.com	de.mcafee.com/root/downloads.asp
希腊	www.mcafeehelp.com	el.mcafee.com/root/downloads.asp
匈牙利	www.mcafeehelp.com	hu.mcafee.com/root/downloads.asp
意大利	www.mcafeeaiuto.com	it.mcafee.com/root/downloads.asp

日本	www.mcafeehelp.jp	jp.mcafee.com/root/downloads.asp
韩国	www.mcafeehelp.com	kr.mcafee.com/root/downloads.asp
墨西哥	www.mcafeehelp.com	mx.mcafee.com/root/downloads.asp
挪威	www.mcafeehjelp.com	no.mcafee.com/root/downloads.asp
波兰	www.mcafeepomoc.com	pl.mcafee.com/root/downloads.asp
葡萄牙	www.mcafeeajuda.com	pt.mcafee.com/root/downloads.asp
俄罗斯	www.mcafeehelp.com	ru.mcafee.com/root/downloads.asp
斯洛伐克	www.mcafeehelp.com	sk.mcafee.com/root/downloads.asp
西班牙	www.mcafeeayuda.com	es.mcafee.com/root/downloads.asp
瑞典	www.mcafeehjalp.com	se.mcafee.com/root/downloads.asp
台湾	www.mcafeehelp.com	tw.mcafee.com/root/downloads.asp
土耳其	www.mcafeehelp.com	tr.mcafee.com/root/downloads.asp
英国	www.mcafeehelp.com	uk.mcafee.com/root/downloads.asp
美国	www.mcafeehelp.com	us.mcafee.com/root/downloads.asp

McAfee Total Protection 使用手册

国家/地区	McAfee 使用手册
澳大利亚	download.mcafee.com/products/manuals/en-au/MTP_userguide_2008.pdf
巴西	download.mcafee.com/products/manuals/pt-br/MTP_userguide_2008.pdf
加拿大 (英文)	download.mcafee.com/products/manuals/en-ca/MTP_userguide_2008.pdf
加拿大 (法文)	download.mcafee.com/products/manuals/fr-ca/MTP_userguide_2008.pdf
中国 (简体中文)	download.mcafee.com/products/manuals/zh-cn/MTP_userguide_2008.pdf
捷克共和国	download.mcafee.com/products/manuals/cz/MTP_userguide_2008.pdf

丹麦	download.mcafee.com/products/manuals/dk/MTP_userguide_2008.pdf
芬兰	download.mcafee.com/products/manuals/fi/MTP_userguide_2008.pdf
法国	download.mcafee.com/products/manuals/fr/MTP_userguide_2008.pdf
德国	download.mcafee.com/products/manuals/de/MTP_userguide_2008.pdf
希腊	download.mcafee.com/products/manuals/el/MTP_userguide_2008.pdf
匈牙利	download.mcafee.com/products/manuals/hu/MTP_userguide_2008.pdf
意大利	download.mcafee.com/products/manuals/it/MTP_userguide_2008.pdf
日本	download.mcafee.com/products/manuals/ja/MTP_userguide_2008.pdf
韩国	download.mcafee.com/products/manuals/ko/MTP_userguide_2008.pdf
墨西哥	download.mcafee.com/products/manuals/es-mx/MTP_userguide_2008.pdf
荷兰	download.mcafee.com/products/manuals/nl/MTP_userguide_2008.pdf
挪威	download.mcafee.com/products/manuals/no/MTP_userguide_2008.pdf
波兰	download.mcafee.com/products/manuals/pl/MTP_userguide_2008.pdf
葡萄牙	download.mcafee.com/products/manuals/pt/MTP_userguide_2008.pdf
俄罗斯	download.mcafee.com/products/manuals/ru/MTP_userguide_2008.pdf
斯洛伐克	download.mcafee.com/products/manuals/sk/MTP_userguide_2008.pdf
西班牙	download.mcafee.com/products/manuals/es/MTP_userguide_2008.pdf
瑞典	download.mcafee.com/products/manuals/sv/MTP_userguide_2008.pdf
台湾	download.mcafee.com/products/manuals/zh-tw/MTP_userguide_2008.pdf
土耳其	download.mcafee.com/products/manuals/tr/MTP_userguide_2008.pdf
英国	download.mcafee.com/products/manuals/en-uk/MTP_userguide_2008.pdf
美国	download.mcafee.com/products/manuals/en-us/MTP_userguide_2008.pdf

McAfee Internet Security 使用手册

国家/地区	McAfee 使用手册
澳大利亚	download.mcafee.com/products/manuals/en-au/MIS_userguide_2008.pdf
巴西	download.mcafee.com/products/manuals/pt-br/MIS_userguide_2008.pdf
加拿大 (英文)	download.mcafee.com/products/manuals/en-ca/MIS_userguide_2008.pdf
加拿大 (法文)	download.mcafee.com/products/manuals/fr-ca/MIS_userguide_2008.pdf
中国 (简体中文)	download.mcafee.com/products/manuals/zh-cn/MIS_userguide_2008.pdf
捷克共和国	download.mcafee.com/products/manuals/cz/MIS_userguide_2008.pdf
丹麦	download.mcafee.com/products/manuals/dk/MIS_userguide_2008.pdf
芬兰	download.mcafee.com/products/manuals/fi/MIS_userguide_2008.pdf
法国	download.mcafee.com/products/manuals/fr/MIS_userguide_2008.pdf
德国	download.mcafee.com/products/manuals/de/MIS_userguide_2008.pdf
希腊	download.mcafee.com/products/manuals/el/MIS_userguide_2008.pdf
匈牙利	download.mcafee.com/products/manuals/hu/MIS_userguide_2008.pdf
意大利	download.mcafee.com/products/manuals/it/MIS_userguide_2008.pdf
日本	download.mcafee.com/products/manuals/ja/MIS_userguide_2008.pdf
韩国	download.mcafee.com/products/manuals/ko/MIS_userguide_2008.pdf
墨西哥	download.mcafee.com/products/manuals/es-mx/MIS_userguide_2008.pdf
荷兰	download.mcafee.com/products/manuals/nl/MIS_userguide_2008.pdf
挪威	download.mcafee.com/products/manuals/no/MIS_userguide_2008.pdf
波兰	download.mcafee.com/products/manuals/pl/MIS_userguide_2008.pdf
葡萄牙	download.mcafee.com/products/manuals/pt/MIS_userguide_2008.pdf

俄罗斯	download.mcafee.com/products/manuals/ru/MIS_userguide_2008.pdf
斯洛伐克	download.mcafee.com/products/manuals/sk/MIS_userguide_2008.pdf
西班牙	download.mcafee.com/products/manuals/es/MIS_userguide_2008.pdf
瑞典	download.mcafee.com/products/manuals/sv/MIS_userguide_2008.pdf
台湾	download.mcafee.com/products/manuals/zh-tw/MIS_userguide_2008.pdf
土耳其	download.mcafee.com/products/manuals/tr/MIS_userguide_2008.pdf
英国	download.mcafee.com/products/manuals/en-uk/MIS_userguide_2008.pdf
美国	download.mcafee.com/products/manuals/en-us/MIS_userguide_2008.pdf

McAfee VirusScan Plus 使用手册

国家/地区	McAfee 使用手册
澳大利亚	download.mcafee.com/products/manuals/en-au/VSP_userguide_2008.pdf
巴西	download.mcafee.com/products/manuals/pt-br/VSP_userguide_2008.pdf
加拿大 (英文)	download.mcafee.com/products/manuals/en-ca/VSP_userguide_2008.pdf
加拿大 (法文)	download.mcafee.com/products/manuals/fr-ca/VSP_userguide_2008.pdf
中国 (简体中文)	download.mcafee.com/products/manuals/zh-cn/VSP_userguide_2008.pdf
捷克共和国	download.mcafee.com/products/manuals/cz/VSP_userguide_2008.pdf
丹麦	download.mcafee.com/products/manuals/dk/VSP_userguide_2008.pdf
芬兰	download.mcafee.com/products/manuals/fi/VSP_userguide_2008.pdf
法国	download.mcafee.com/products/manuals/fr/VSP_userguide_2008.pdf
德国	download.mcafee.com/products/manuals/de/VSP_userguide_2008.pdf
希腊	download.mcafee.com/products/manuals/el/VSP_userguide_2008.pdf
匈牙利	download.mcafee.com/products/manuals/hu/VSP_userguide_2008.pdf

意大利	download.mcafee.com/products/manuals/it/VSP_userguide_2008.pdf
日本	download.mcafee.com/products/manuals/ja/VSP_userguide_2008.pdf
韩国	download.mcafee.com/products/manuals/ko/VSP_userguide_2008.pdf
墨西哥	download.mcafee.com/products/manuals/es-mx/VSP_userguide_2008.pdf
荷兰	download.mcafee.com/products/manuals/nl/VSP_userguide_2008.pdf
挪威	download.mcafee.com/products/manuals/no/VSP_userguide_2008.pdf
波兰	download.mcafee.com/products/manuals/pl/VSP_userguide_2008.pdf
葡萄牙	download.mcafee.com/products/manuals/pt/VSP_userguide_2008.pdf
俄罗斯	download.mcafee.com/products/manuals/ru/VSP_userguide_2008.pdf
斯洛伐克	download.mcafee.com/products/manuals/sk/VSP_userguide_2008.pdf
西班牙	download.mcafee.com/products/manuals/es/VSP_userguide_2008.pdf
瑞典	download.mcafee.com/products/manuals/sv/VSP_userguide_2008.pdf
台湾	download.mcafee.com/products/manuals/zh-tw/VSP_userguide_2008.pdf
土耳其	download.mcafee.com/products/manuals/tr/VSP_userguide_2008.pdf
英国	download.mcafee.com/products/manuals/en-uk/VSP_userguide_2008.pdf
美国	download.mcafee.com/products/manuals/en-us/VSP_userguide_2008.pdf

McAfee VirusScan 使用手册

国家/地区	McAfee 使用手册
澳大利亚	download.mcafee.com/products/manuals/en-au/VS_userguide_2008.pdf
巴西	download.mcafee.com/products/manuals/pt-br/VS_userguide_2008.pdf
加拿大 (英文)	download.mcafee.com/products/manuals/en-ca/VS_userguide_2008.pdf
加拿大 (法文)	download.mcafee.com/products/manuals/fr-ca/VS_userguide_2008.pdf

中国 (简体中文)	download.mcafee.com/products/manuals/zh-cn/VS_userguide_2008.pdf
捷克共和国	download.mcafee.com/products/manuals/cz/VS_userguide_2008.pdf
丹麦	download.mcafee.com/products/manuals/dk/VS_userguide_2008.pdf
芬兰	download.mcafee.com/products/manuals/fi/VS_userguide_2008.pdf
法国	download.mcafee.com/products/manuals/fr/VS_userguide_2008.pdf
德国	download.mcafee.com/products/manuals/de/VS_userguide_2008.pdf
希腊	download.mcafee.com/products/manuals/el/VS_userguide_2008.pdf
匈牙利	download.mcafee.com/products/manuals/hu/VS_userguide_2008.pdf
意大利	download.mcafee.com/products/manuals/it/VS_userguide_2008.pdf
日本	download.mcafee.com/products/manuals/ja/VS_userguide_2008.pdf
韩国	download.mcafee.com/products/manuals/ko/VS_userguide_2008.pdf
墨西哥	download.mcafee.com/products/manuals/es-mx/VS_userguide_2008.pdf
荷兰	download.mcafee.com/products/manuals/nl/VS_userguide_2008.pdf
挪威	download.mcafee.com/products/manuals/no/VS_userguide_2008.pdf
波兰	download.mcafee.com/products/manuals/pl/VS_userguide_2008.pdf
葡萄牙	download.mcafee.com/products/manuals/pt/VS_userguide_2008.pdf
俄罗斯	download.mcafee.com/products/manuals/ru/VS_userguide_2008.pdf
斯洛伐克	download.mcafee.com/products/manuals/sk/VS_userguide_2008.pdf
西班牙	download.mcafee.com/products/manuals/es/VS_userguide_2008.pdf
瑞典	download.mcafee.com/products/manuals/sv/VS_userguide_2008.pdf
台湾	download.mcafee.com/products/manuals/zh-tw/VS_userguide_2008.pdf
土耳其	download.mcafee.com/products/manuals/tr/VS_userguide_2008.pdf
英国	download.mcafee.com/products/manuals/en-uk/VS_userguide_2008.pdf

美国	download.mcafee.com/products/manuals/en-us/VS_userguide_2008.pdf
----	--

请参阅下表来了解您所在国家或地区的 McAfee 威胁中心和病毒信息站点。

国家/地区	安全总部	病毒信息
澳大利亚	www.mcafee.com/us/threat_center	au.mcafee.com/virusInfo
巴西	www.mcafee.com/us/threat_center	br.mcafee.com/virusInfo
加拿大 (英文)	www.mcafee.com/us/threat_center	ca.mcafee.com/virusInfo
加拿大 (法文)	www.mcafee.com/us/threat_center	ca.mcafee.com/virusInfo
中国 (简体中文)	www.mcafee.com/us/threat_center	cn.mcafee.com/virusInfo
捷克共和国	www.mcafee.com/us/threat_center	cz.mcafee.com/virusInfo
丹麦	www.mcafee.com/us/threat_center	dk.mcafee.com/virusInfo
芬兰	www.mcafee.com/us/threat_center	fi.mcafee.com/virusInfo
法国	www.mcafee.com/us/threat_center	fr.mcafee.com/virusInfo
德国	www.mcafee.com/us/threat_center	de.mcafee.com/virusInfo
希腊	www.mcafee.com/us/threat_center	gr.mcafee.com/virusInfo
匈牙利	www.mcafee.com/us/threat_center	hu.mcafee.com/virusInfo
意大利	www.mcafee.com/us/threat_center	it.mcafee.com/virusInfo
日本	www.mcafee.com/us/threat_center	jp.mcafee.com/virusInfo
韩国	www.mcafee.com/us/threat_center	kr.mcafee.com/virusInfo
墨西哥	www.mcafee.com/us/threat_center	mx.mcafee.com/virusInfo
荷兰	www.mcafee.com/us/threat_center	nl.mcafee.com/virusInfo
挪威	www.mcafee.com/us/threat_center	no.mcafee.com/virusInfo
波兰	www.mcafee.com/us/threat_center	pl.mcafee.com/virusInfo
葡萄牙	www.mcafee.com/us/threat_center	pt.mcafee.com/virusInfo
俄罗斯	www.mcafee.com/us/threat_center	ru.mcafee.com/virusInfo
斯洛伐克	www.mcafee.com/us/threat_center	sk.mcafee.com/virusInfo
西班牙	www.mcafee.com/us/threat_center	es.mcafee.com/virusInfo
瑞典	www.mcafee.com/us/threat_center	se.mcafee.com/virusInfo

台湾	www.mcafee.com/us/threat_center	tw.mcafee.com/virusInfo
土耳其	www.mcafee.com/us/threat_center	tr.mcafee.com/virusInfo
英国	www.mcafee.com/us/threat_center	uk.mcafee.com/virusInfo
美国	www.mcafee.com/us/threat_center	us.mcafee.com/virusInfo

请参阅下表来了解您所在国家或地区的 HackerWatch 站点。

国家/地区	HackerWatch
澳大利亚	www.hackerwatch.org
巴西	www.hackerwatch.org/?lang=pt-br
加拿大 (英文)	www.hackerwatch.org
加拿大 (法文)	www.hackerwatch.org/?lang=fr-ca
中国 (简体中文)	www.hackerwatch.org/?lang=zh-cn
捷克共和国	www.hackerwatch.org/?lang=cs
丹麦	www.hackerwatch.org/?lang=da
芬兰	www.hackerwatch.org/?lang=fi
法国	www.hackerwatch.org/?lang=fr
德国	www.hackerwatch.org/?lang=de
希腊	www.hackerwatch.org/?lang=el
匈牙利	www.hackerwatch.org/?lang=hu
意大利	www.hackerwatch.org/?lang=it
日本	www.hackerwatch.org/?lang=jp
韩国	www.hackerwatch.org/?lang=ko
墨西哥	www.hackerwatch.org/?lang=es-mx
荷兰	www.hackerwatch.org/?lang=nl
挪威	www.hackerwatch.org/?lang=no
波兰	www.hackerwatch.org/?lang=pl
葡萄牙	www.hackerwatch.org/?lang=pt-pt
俄罗斯	www.hackerwatch.org/?lang=ru
斯洛伐克	www.hackerwatch.org/?lang=sk
西班牙	www.hackerwatch.org/?lang=es
瑞典	www.hackerwatch.org/?lang=sv
台湾	www.hackerwatch.org/?lang=zh-tw
土耳其	www.hackerwatch.org/?lang=tr

英国	www.hackerwatch.org
美国	www.hackerwatch.org

索引

8

- 802.11 227
- 802.11a 227
- 802.11b 227
- 802.1x 227

A

- ActiveX 控件 227
- Anti-Spam 功能 111
- 安装可用的网络打印机 224
- 按需扫描 231

B

- Backup and Restore 的功能 160
- 白名单 231, 233
- 版权 240
- 保护儿童 137
- 保护个人信息 154
- 保护密码 155
- 暴力攻击 232
- 备份 232
- 编辑 McAfee 用户帐户的信息 149
- 编辑 Web 邮件帐户 128
- 编辑白名单中的站点 134
- 编辑个人过滤器 118
- 编辑计算机连接 86
- 编辑禁止的计算机连接 89
- 编辑朋友 125
- 编辑域 126
- 标记为朋友 207
- 标记为入侵者 206
- 标准电子邮件帐户 232
- 病毒 232
- 拨号程序 232

C

- Cookie 227
- 参考 226
- 插件 232
- 查看、导出或删除已过滤的 Web 邮件
- 查看出站事件 77, 99
- 查看存档活动的摘要 174
- 查看全球 Internet 端口活动 100
- 查看全球安全事件统计信息 100
- 查看入侵检测事件 99

132

- 查看入站事件 99
- 查看扫描结果 31
- 查看事件 16, 25
- 查看所有事件 25
- 查看项目的详细信息 197
- 查看最新事件 25, 98
- 查找已过滤 Web 邮件的事件 132
- 重命名网络 196, 214
- 重新启用网络监视通知 206
- 重置密码存储库密码 156
- 出现警报时播放声音 22
- 处理病毒和特洛伊木马程序 33
- 处理隔离的程序和 Cookie 35
- 处理隔离的文件 33, 34
- 处理过滤的电子邮件 131
- 处理可能有害的程序 34
- 处理扫描结果 33
- 处理已存档的文件 169
- 从 Anti-Spam 工具栏中添加朋友 124
- 从本地存档还原较旧版本的文件 172
- 从本地存档还原缺少的文件 172, 173
- 从存档中排除位置 165
- 存档 232
- 存档文件 161

D

- DAT 227
- DNS 227
- 打开 EasyNetwork 211
- 打开已存档的文件 171
- 代理 232
- 代理服务器 232
- 带宽 232
- 导入地址簿 123
- 电子邮件 230, 232
- 电子邮件客户端 232
- 端口 233
- 对计算机进行碎片整理 180

E

- EasyNetwork 功能 210
- ESS 228
- 恶意接入点 233

F

- 发布 233
- 发送文件时接收通知 221

防火墙 233
 访问您的 McAfee 帐户 11
 访问网络图 196
 分析入站和出站通讯 104
 服务器 233
 复制共享文件 218

G

隔离 233
 根据关键字阻止网站 138
 跟踪 Internet 通讯 101
 跟踪监视的 IP 地址 103
 跟踪网络计算机的位置 101
 更改 McAfee 管理员的密码 148
 更改存档位置 165
 更改过滤级别 114
 更改您的密码存储库密码 156
 更新 SecurityCenter 13
 更新已过滤的网站 140
 共享 233
 共享打印机 223
 共享和发送文件 217
 共享密钥 233
 共享文件 218
 关于 McAfee 239
 关于 SystemGuard 类型 51
 关于警报 62
 关于计算机连接 84
 关于可信列表类型 54, 55
 关于流量分析图 104
 管理程序和权限 75
 管理存档 174
 管理防火墙安全级别 66
 管理计算机的保护状态 202
 管理计算机连接 83
 管理可信列表 54
 管理您的订购 11, 16
 管理设备 203
 管理系统服务 91
 管理信息警报 63
 管理状态和权限 202
 过滤电子邮件 121
 过滤可能不良的 Web 图像 145
 过滤网站 140, 144

H

黑名单 231, 233
 忽略保护问题 17
 还原已存档的文件 172
 缓冲区溢出 234
 缓存 234
 恢复防火墙设置 74
 回收站 234
 获取程序信息 82
 获取计算机网络信息 101
 获取计算机注册信息 101

I

IP 地址 228
 IP 伪造 228

J

激活您的产品 11
 集成网关 234
 计划 QuickClean 任务 181
 计划磁盘碎片整理程序任务 183
 计划任务 181
 计划扫描 37, 48
 计划自动存档 167
 记录、监视和分析 97
 加密 234, 236
 加入托管网络 198, 212, 215
 加入网络 212
 家长监控的功能 136
 家庭网络 234, 237
 监视 Internet 通讯 104
 监视程序带宽 105
 监视程序活动 105
 监视您的网络 205
 监视位置 234
 监视文件类型 234
 检查更新 13, 14
 检索 McAfee 管理员的密码 148
 将安全级别设置为 67
 将电子邮件报告给 McAfee 131
 将网站添加到白名单 133
 将文件发给其他计算机 220
 将文件发送到另一台计算机 220
 脚本 234
 接入点 (AP) 234
 接受另一台计算机发来的文件 220
 节点 234
 禁用 69
 禁用 Anti-Spam 工具栏 121
 禁用本地存档 162
 禁用存档加密和压缩 166
 禁用关键字过滤 138
 禁用垃圾邮件防护 119
 禁用网络钓鱼防护 134
 禁用自动更新 14
 禁止计算机连接 88
 拒绝服务 (DOS) 攻击 235

K

可能有害的程序 (PUP) 235
 可信列表 235
 客户端 235
 客户服务和技术支持 241
 快捷方式 235

L

LAN	228, 234
launchpad.....	228
离开托管网络	215
立即解锁防火墙	74
立即锁定防火墙	74
了解 Internet 安全性	107
了解 Network Manager 图标	193
了解 Web 邮件帐户信息	128, 129
了解保护服务	10
了解保护类别	7, 9, 25
了解保护状态	7, 8, 9
了解程序	82
临时文件	235
浏览器	235
路由器	235

M

MAC 地址	228
MAPI	228
McAfee Anti-Spam	109
McAfee Backup and Restore	159
McAfee EasyNetwork	209
McAfee Network Manager	191
McAfee Parental Controls	135
McAfee Personal Firewall	57
McAfee QuickClean	175
McAfee SecurityCenter	5
McAfee Shredder	187
McAfee Total Protection	3
McAfee VirusScan	27
MSN	228
漫游	235
密码	235
密码存储库	236
密文	236
密钥	236
明文	236

N

Network Manager 功能	192
NIC	228
内部网	236
内容评级组	236

P

PCI 无线适配器卡	228
Personal Firewall 功能	58
POP3	229, 232
PPPoE	229
排序已存档的文件	170
配置 ping 请求设置	71
配置 SystemGuard 选项	50
配置 UDP 设置	72
配置防火墙保护	65

配置警报的	69
配置警报选项	22
配置垃圾邮件检测	113
配置入侵检测	72
配置事件日志设置	98
配置网络钓鱼防护	133
配置系统服务端口	92
配置新服务端口	94
配置用户	147
配置自动更新	13

Q

QuickClean 功能	176
启动 HackerWatch 教程	108
启动 Virtual Technician	242
启动电子邮件保护	40
启动防火墙	59
启动防火墙保护	59
启动过程中保护计算机	71
启动即时消息保护	41
启动间谍软件防护	40
启动脚本扫描防护	39
启用	69
启用 SystemGuard 保护	50
启用本地存档	162
启用和禁用本地存档	162
启用适合年龄的搜索	146
切换到 Windows 用户	150
清除文件、文件夹和磁盘	189
清除文件和文件夹	189
清除整个磁盘	190
清理计算机	177, 179

R

RADIUS	229, 233
Rootkit	229
热点	236
蠕虫	236

S

SecurityCenter 功能	6
Shredder 功能	188
SMTP	229
SSID	229
SSL	229
SystemGuard	229
扫描计算机	29
扫描类型	31, 36
扫描您的 PC	29, 37
扫台者	236
删除 McAfee 用户	148
删除 QuickClean 任务	183
删除 Web 邮件帐户	129
删除白名单中的网站	134
删除程序的访问权限	81
删除程序权限	81

删除磁盘碎片整理程序任务 184
 删除个人过滤器 118
 删除计算机连接 87
 删除禁止的计算机连接 89
 删除密码 157
 删除朋友 126
 删除系统服务端口 95
 删除已过滤的网站 140
 配置防火墙的 72
 设置 EasyNetwork 211
 设置 Web 浏览时间限制 143
 设置 Web 邮件帐户 127
 设置病毒防护 29, 43
 设置存档文件类型 164
 设置存档选项 163
 设置过滤选项 114
 设置密码存储库 156
 设置内容评级组 144, 145, 146
 设置朋友 123
 设置实时扫描选项 36, 44
 设置托管网络 195
 设置用户的内容评级组 144
 设置自定义扫描选项 36, 46
 身份验证 227, 236
 实时扫描 236
 使用 McAfee Virtual Technician... 241
 使用 McAfee 用户 148, 151
 使用 SecurityCenter 7
 使用 SystemGuard 选项 49
 使用 Windows 用户 151
 使用本地存档资源管理器 170
 使用个人过滤器 117
 使用共享打印机 224
 使用关键字过滤网站 138, 140
 使用警报 13, 19, 61
 使用可信列表 54
 使用其他防护 39
 使用统计信息 100
 使用网络图 196
 事件 236
 事件记录 98
 手动设置朋友 124
 手动添加朋友 124
 手动修复保护问题 16
 手动运行存档 168
 授予对网络的访问权限 213
 刷新网络图 196
 搜索标准 219
 搜索共享文件 219
 搜索已存档的文件 170
 锁定和恢复防火墙 74

T

TKIP 229, 231
 弹出窗口 237
 特洛伊, 特洛伊木马 237
 添加 McAfee 用户 149

添加 Web 邮件帐户 127
 添加个人过滤器 117
 添加计算机连接 84
 添加禁止的计算机连接 88
 添加密码 158
 添加域 125
 停止防火墙保护 59
 停止共享打印机 224
 停止共享文件 218
 停止管理计算机的保护状态 202
 停止监视网络 205
 停止检测新朋友 207
 停止实时病毒防护 45
 停止信任网络上的计算机 200
 同步 237

U

U3 230
 URL 230
 USB 230
 USB 驱动器 230, 238
 USB 无线适配器卡 230

V

VirusScan 功能 28
 VPN 230

W

Web 邮件 230, 232
 WEP 230, 236
 Wi-Fi 230
 Wi-Fi Alliance 231
 Wi-Fi Certified 231
 WLAN 231
 WPA 231, 236
 WPA2 231, 236
 WPA2-PSK 236
 WPA2-PSK 231
 WPA-PSK 231, 236
 外部硬盘驱动器 237
 玩游戏时显示或隐藏信息警报 20
 玩游戏时显示警报 63
 网络 237
 网络臭虫 237
 网络钓鱼 237
 网络驱动器 237
 网络图 237
 文件碎片 237
 无线适配器 237

X

系统还原点 237
 显示和隐藏信息警报 20
 显示或隐藏忽略的问题 17
 显示或隐藏网络图中的项目 197

显示或隐藏信息警报	20
显示智能建议	70
消息身份验证代码 (MAC)	238
协议	238
修复安全漏洞	204
修复保护问题	8, 16
修复或忽略保护问题	8, 15
修改 QuickClean 任务	182
修改磁盘碎片整理程序任务	184
修改垃圾邮件的处理和标记方式	115, 117
修改密码	157
修改设备的显示属性	203
修改托管计算机的权限	202
修改系统服务端口	95
许可	240
续订您的订购	12

Y

压缩	238
验证您的订购	11
邀请计算机加入此托管网络	199
隐藏安全消息	23
隐藏病毒发作警报	22
隐藏启动时的启动屏幕	22
隐藏信息警报	63
应用字符集过滤器	116
优化防火墙安全性	71
域	238

远程管理网络	201
允许程序访问 Internet	76
允许程序具有仅出站访问权限	78
允许程序具有完全访问权限	76
允许访问现有的系统服务端口	93
允许网站	141
允许新程序具有完全访问权限	76
运行完全存档和快速存档	167

Z

在 Anti-Spam 工具栏中标记邮件	121
在 Web 上保护信息	153
在存档中包含位置	164
在远程计算机上安装 McAfee 安全软件	204
支持和下载	242
指定个人过滤器	117, 118
智能驱动器	238
中断自动存档	168
中间人攻击	238
注册表	238
字典攻击	238
自动修复保护问题	16
阻止程序的 Internet 访问权限	79
阻止程序具有访问权限	79
阻止访问现有的系统服务端口	93
阻止网站	141
阻止新程序的访问权限	79