McAfee®

Total Protection 2007

用户手册

目录

第 1 章

McAfee Total Protection

McAfee Total Protection Suite 会为您的身份信息、计算机和无线网络提供完整的防护，还提供重要文件的自动备份。McAfee 会始终打开、时刻更新和时刻防护，这样您在上网冲浪、购物、处理银行业务、使用电子邮件、收发即使消息时，可以享受安全无忧的 Internet 体验。McAfee 提供的令人信赖的防护功能会自动拦截威胁并阻止黑客，保持您的计算机不受感染和安全。使用 McAfee Network Manager 监视和修复所有家用计算机上的安全问题。使用 McAfee EasyNetwork，可以在网络上轻松共享文件和打印机。使用重新设计的 McAfee SecurityCenter，McAfee 还使您可以轻松查看安全状态，扫描病毒和间谍软件，并确保产品是最新的。另外，通过订购，您还会自动接收最新的软件和更新。

Total Protection 包含以下程序：

- SecurityCenter
- Privacy Service
- Shredder
- VirusScan
- Personal Firewall
- SpamKiller
- Data Backup
- Wireless Security
- Network Manager
- EasyNetwork
- SiteAdvisor

第 2 章

McAfee SecurityCenter

McAfee SecurityCenter 操作简便，McAfee 用户可以通过它启动、管理和配置已订购的安全产品。

SecurityCenter 还可以提供病毒警报、产品信息、支持以及订购信息，只需单击一次，即可访问在 McAfee 网站上提供的工具和新闻。

本章内容

功能

McAfee SecurityCenter 具有以下新功能及优点：

重新设计的保护状态

轻松查看计算机的安全状态、检查更新和修复可能的安全问题。

持续更新和升级

自动安装每日更新。如果有新版本的 McAfee 软件，则可在订购期间自动免费获得，确保您始终获得最新的保护。

实时警报

安全警报会将病毒发作和安全威胁通知给您，并提供用于消除和化解威胁以及了解威胁详细信息的选项。

便捷的保护

各种续订选项会将您的 McAfee 保护保持最新。

性能工具

删除不使用的文件，对使用的文件进行碎片整理，并使用系统还原以保持计算机发挥最佳性能。

真正的在线帮助

通过 Internet 聊天、电子邮件和电话获得 McAfee 的计算机安全专家提供的支持。

安全的冲浪保护

如果已安装 McAfee SiteAdvisor 浏览器插件，则它会通过对您访问的或出现在您的 Web 搜索结果中的网站评级，保护您免受间谍软件、垃圾邮件、病毒和在线诈骗的侵扰。您可以查看详细的安全评级，这些安全评级显示了针对网站的电子邮件活动、下载、在线成员以及干扰（如弹出窗口和第三方跟踪 Cookie）进行的测试方式。

第 3 章

使用 SecurityCenter

可以通过任务栏最右侧 Windows 通知区域中的 McAfee SecurityCenter 图标 或从 Windows 桌面运行 SecurityCenter。

打开 SecurityCenter 后，“主页”窗格将显示计算机的安全状态，并提供快速访问更新、扫描（如果已安装 McAfee VirusScan）以及其他常见任务的功能：

标题

帮助

查看程序帮助文件。

左栏

更新

更新您的产品以确保您的计算机免受最新的威胁。

扫描

如果已安装 McAfee VirusScan，则可以对计算机执行手动扫描。

常见任务

执行包括返回到“主页”窗格、查看最新事件、管理计算机网络（如果在对此网络具有管理功能的计算机上）以及维护计算机等常见任务。如果已安装 McAfee Data Backup，还可以备份数据。

已安装组件

查看正在保护您的计算机安全的安全服务。

主窗格

保护状态

在“我是否受到保护?”下，查看计算机的整体保护状态。在它下面，还可以按类别和类型查看状态详细分类。

SecurityCenter 信息

查看计算机上次更新时间、上次扫描时间（如果已安装 McAfee VirusScan）以及订购过期时间。

本章内容

了解 SecurityCenter 图标

SecurityCenter 图标显示在任务栏最右侧的 Windows 通知区域内。使用这些图标可以查看您的计算机是否已受完全保护、查看扫描过程的状态（如果已安装 McAfee VirusScan）、检查是否有更新、查看最新事件、维护计算机以及从 McAfee 网站获得支持。

打开 SecurityCenter 和使用其他功能

SecurityCenter 运行时，SecurityCenter M 图标 会显示在任务栏最右侧的 Windows 通知区域。

打开 SecurityCenter 或使用其他功能：

- 右键单击主 SecurityCenter 图标，然后单击以下任一选项：
  - 打开 SecurityCenter
  - 更新
  - 快速链接

    该子菜单包含指向“主页”、“查看最新事件”、“管理网络”、“维护计算机”以及“Data Backup”（如果已安装）的链接。
  - 验证订购

    （当至少有一个产品订购过期时，会出现此项目。）
  - 升级中心
  - 客户支持

检查保护状态

如果您的计算机未受完全保护，则保护状态图标 会显示在任务栏最右侧的 Windows 通知区域。根据保护状态的不同，此图标可能是红色，也可能是黄色。

检查保护状态：

- 单击保护状态图标打开 SecurityCenter 并修复所有问题。

检查更新状态

如果您正在检查是否有更新，则更新图标 会显示在任务栏最右侧的 Windows 通知区域。

检查更新状态：

- 指向更新图标以在工具提示中查看更新状态。

了解保护状态

计算机的整体安全保护状态显示在 SecurityCenter 中的“我是否受到保护?”下。

保护状态会通知您计算机是否已受完全保护以抵御最新的安全威胁，或者是否需要注意某些问题以及如何解决。当某个问题影响多个保护类别时，修复该问题可能会导致多个类别恢复到完全受保护状态。

影响保护状态的一些因素包括：外部安全威胁、计算机所安装的安全产品、访问 Internet 的产品，以及配置安全产品和 Internet 产品的方式。

默认情况下，如果未安装垃圾邮件防护或内容阻止功能，则会自动忽略非关键保护问题，而且不会在整体保护状态中对其进行跟踪。不过，如果在保护问题的后面出现“忽略”链接，则可以在确定无须对其进行修复的情况下，选择忽略该问题。

我是否受到保护？

在 SecurityCenter 中的“我是否受到保护?”下，查看计算机的整体保护状态：

- 如果计算机受完全保护（绿色），则显示“是”。
- 如果计算机受局部保护（黄色）或未受保护（红色），则显示“否”。

要自动解决大多数保护问题，请单击保护状态旁边的“修复”。不过，如果仍存在一个或多个问题并且需要您响应，请单击此问题后面的链接以采取建议的操作。

了解保护类别和类型

在 SecurityCenter 中的“我是否受到保护?”下，可以查看包含以下保护类别和类型的状态详细分类：

- 计算机和文件
- Internet 和网络
- 电子邮件和 IM
- 家长监控

在 SecurityCenter 中显示的保护类型取决于已安装的产品。例如，如果已安装 McAfee Data Backup 软件，则会显示“PC 健康”保护类型。

如果某一类别没有任何保护问题，则其状态显示为绿色。如果单击“绿色”类别，则会在右侧显示已启用的保护类型列表，后面还会显示已忽略的问题列表。如果没有任何问题，则会显示病毒安全公告而不显示任何问题。您还可以单击“配置”以更改此类别的选项。

如果类别内的所有保护类型的状态均显示为“绿色”，则此类别的状态显示为“绿色”。同样，如果所有保护类别的状态均显示为“绿色”，则整体保护状态将显示为“绿色”。

如果任何保护类别的状态显示为“黄色”或“红色”，则可以通过对其进行修复或忽略（这会将状态更改为“绿色”）来解决保护问题。

了解计算机和文件保护

“计算机和文件”保护类别包括以下保护类型：

- **病毒防护** -- 实时扫描保护会保护您的计算机免受病毒、蠕虫、特洛伊木马程序、可疑脚本、混合型病毒以及其他威胁的侵扰。当您或您的计算机访问文件时，它会自动扫描和尝试清除文件（包括 .exe 压缩文件、引导扇区、内存和重要文件）中的病毒。
- **间谍软件防护** -- 间谍软件防护可以快速检测、阻止和删除未经许可收集和传输您的隐私数据的间谍软件、广告软件和其他可能有害的程序。
- SystemGuard -- SystemGuard 会检测对计算机的更改并在出现更改时提醒您。然后，您可以查看这些更改并决定是否允许更改。
- **Windows 保护** -- Windows 保护会提供计算机上 Windows 更新的状态。如果已安装 McAfee VirusScan，则还可以使用缓冲区溢出保护。

影响“计算机和文件”保护的因素之一是外部病毒威胁。例如，当某种病毒发作时，您的防病毒软件能否保护计算机免遭破坏。此外，还包括一些其他因素，例如防病毒软件的配置、是否使用最新的检测签名文件持续更新您的软件，以保护计算机免受最新威胁。

打开“计算机和文件”配置窗格

如果在“计算机和文件”下面没有任何问题，则可以从信息窗格中打开该配置窗格。

打开“计算机和文件”配置窗格：

1. 在“主页”窗格中，单击“计算机和文件”。
2. 在右侧窗格中，单击“配置”。

了解“Internet 和网络”保护

“Internet 和网络”保护类别包括以下保护类型：

- **防火墙保护** -- 防火墙保护会防止您的计算机遭受入侵和有害网络通讯的干扰，并帮助您管理入站和出站 Internet 连接。
- **无线保护** -- 无线保护会防止您的家用无线网络遭受入侵和数据拦截。不过，如果您当前已连接到外部无线网络，则您具有的保护类型将取决于该网络的安全级别。
- **Web 浏览防护** -- Web 浏览防护会在您浏览 Internet 时，隐藏计算机上的广告、弹出窗口和 Web 错误。
- **网络钓鱼防护** -- 网络钓鱼防护会通过电子邮件和即时消息、弹出窗口以及其他来源中的超链接，帮助过滤收集个人信息的欺诈网站。
- **个人信息保护** -- 个人信息保护会阻止通过 Internet 发布敏感和机密信息。

打开“Internet 和网络”配置窗格

如果在“Internet 和网络”下面没有任何问题，则可以从信息窗格中打开该配置窗格。

打开“Internet 和网络”配置窗格：

1. 在“主页”窗格中，单击“Internet 和网络”。
2. 在右侧窗格中，单击“配置”。

了解“电子邮件和 IM”保护

“电子邮件和 IM”保护类别包括以下保护类型：

- **电子邮件保护** -- 电子邮件保护会自动扫描和尝试清除入站和出站电子邮件及附件中的病毒、间谍软件和潜在威胁。
- **垃圾邮件防护** -- 垃圾邮件防护会阻止有害的电子邮件进入您的收件箱。
- **即时消息保护** -- 即时消息 (IM) 保护会自动扫描和尝试清除入站即时消息附件中的病毒、间谍软件和潜在威胁。它还会阻止即时消息客户端通过 Internet 交换可能有害的内容或个人信息。
- **安全冲浪保护** -- 如果已安装 McAfee SiteAdvisor 浏览器插件，则它会通过对您访问的或出现在您的 Web 搜索结果中的网站评级，保护您免受间谍软件、垃圾邮件、病毒和在线诈骗的侵扰。您可以查看详细的安全评级，这些安全评级显示了针对网站的电子邮件活动、下载、在线成员以及干扰（例如弹出窗口和第三方跟踪 Cookie）进行的测试方式。

打开“电子邮件和 IM”配置窗格

如果在“电子邮件和 IM”下面没有任何问题，则可以从信息窗格中打开该配置窗格。

打开“电子邮件和 IM”配置窗格：

1 在“主页”窗格中，单击“电子邮件和 IM”。

2 在右侧窗格中，单击“配置”。

了解“家长监控”保护

“家长监控”保护类别包括以下保护类型：

- **家长监控** -- 内容阻止通过禁止访问可能有害的网站，阻止用户查看有害的 Internet 内容。用户的 Internet 活动和使用也可能会受到监控和限制。

打开“家长监控”配置窗格

如果在“家长监控”下面没有任何问题，则可以从信息窗格中打开该配置窗格。

打开“家长监控”配置窗格：

1. 在“主页”窗格中，单击“家长监控”。
2. 在右侧窗格中，单击“配置”。

修复保护问题

大多数保护问题都可以自动解决。不过，如果仍存在一个或多个问题，您必须手动解决。

自动修复保护问题

大多数保护问题都可以自动解决。

自动修复保护问题：

- 单击保护状态旁边的“修复”。

手动修复保护问题

如果一个或多个保护问题没有自动解决，请单击该问题后面的链接以采取建议的操作。

手动修复保护问题：

- 执行以下任一操作：
  - 如果在最近 30 天内尚未对计算机执行完全扫描，请单击主保护状态左侧的“扫描”以执行手动扫描。（如果已安装 McAfee VirusScan，则会出现此项目。）
  - 如果您的病毒签名 (DAT) 文件已过期，请单击主保护状态左侧的“更新”以更新保护文件。
  - 如果未安装某个程序，请单击“获得完全防护”以安装此程序。
  - 如果某个程序丢失部分组件，请重新安装此程序。
  - 如果必须注册程序才能获得完全保护，请单击“立即注册”进行注册。（如果一个或多个程序已过期，则会出现此项目。）
  - 如果某个程序已过期，请单击“立即验证我的订购状态”以检查您的帐户状态。（如果一个或多个程序已过期，则会出现此项目。）

查看 SecurityCenter 信息

在保护状态窗格的底部，“SecurityCenter 信息”提供了访问 SecurityCenter 选项的功能，并显示了上次更新、上次扫描（如果已安装 McAfee VirusScan）以及有关您的 McAfee 产品的订购过期信息。

打开 SecurityCenter 配置窗格

为方便起见，您可以从“主页”窗格中打开 SecurityCenter 配置窗格以更改选项。

打开 SecurityCenter 配置窗格：

- 在“SecurityCenter 信息”下面的“主页”窗格中，单击“配置”。

查看已安装的产品信息

您可以查看已安装的产品列表，其中显示了该产品的版本号以及上次更新的时间。

查看 McAfee 产品信息：

- 在“主页”窗格的“SecurityCenter 信息”下，单击“查看详细信息”以打开产品信息窗口。

使用高级菜单

首次打开 SecurityCenter 时，会在左侧栏显示“基本菜单”。如果您是高级用户，可以单击“高级菜单”以在其位置上打开更详细的命令菜单。为方便起见，您上次使用的菜单会在下次打开 SecurityCenter 时显示。

“高级菜单”包含以下项目：

- 主页
- 报告和日志（包括“最新事件”列表以及按类型列出的最近 30、60 和 90 天内的日志）
- 配置
- 恢复
- 工具

第 4 章

配置 SecurityCenter 选项

SecurityCenter 会显示计算机的整体安全保护状态，允许您创建 McAfee 用户帐户、自动安装最新的产品更新，以及自动发出警报和声音通知您有关流行病毒发作、安全威胁和产品更新的信息。

在“SecurityCenter 配置”窗格，您可以针对下列功能更改 SecurityCenter 选项：

- 保护状态
- 用户
- 自动更新
- 警报

本章内容

配置保护状态

计算机的整体安全保护状态显示在 SecurityCenter 中的“我是否受到保护?”下。

保护状态会通知您计算机是否已受完全保护以抵御最新的安全威胁，或者是否需要注意某些问题以及如何解决。

默认情况下，如果未安装垃圾邮件防护或内容阻止功能，则会自动忽略非关键保护问题，而且不会在整体保护状态中对其进行跟踪。不过，如果在保护问题的后面出现“忽略”链接，则可以在确定无须对其进行修复的情况下，选择忽略该问题。如果您决定以后修复以前忽略的问题，则可以将其包含在保护状态中进行跟踪。

配置忽略的问题

您可以将要跟踪的问题包含在计算机的整体保护状态中或将其从中排除。如果在保护问题的后面出现“忽略”链接，则可以在确定无须对其进行修复的情况下，选择忽略该问题。如果您决定以后修复以前忽略的问题，则可以将其包含在保护状态中进行跟踪。

配置忽略的问题：

1. 在“SecurityCenter 信息”下，单击“配置”。
2. 单击“保护状态”旁边的箭头以展开其窗格，然后单击“高级”。
3. 在“忽略的问题”窗格中执行以下任一操作：
   - 要将以前忽略的问题包含在保护状态中，请清除其复选框。
   - 要将问题从保护状态中排除，请选中其复选框。
4. 单击“确定”。

配置用户选项

如果您在运行需要用户权限的 McAfee 程序，则默认情况下，这些权限对应于此计算机上的 Windows 用户帐户。为更方便地管理这些程序的用户，您可以随时切换到使用 McAfee 用户帐户。

如果您切换到使用 McAfee 用户帐户，则会自动导入“家长监控”程序中所有现有的用户名和权限。不过，首次切换时，您必须创建管理员帐户。然后，您可以开始创建和配置其他 McAfee 用户帐户。

切换到 McAfee 用户帐户

默认情况下，您使用的是 Windows 用户帐户。不过，可以切换到 McAfee 用户帐户，而无须创建其他 Windows 用户帐户。

切换到 McAfee 用户帐户：

1. 在“SecurityCenter 信息”下，单击“配置”。
2. 单击“用户”旁边的箭头以展开其窗格，然后单击“高级”。
3. 要使用 McAfee 用户帐户，请单击“切换”。

如果您是首次切换到 McAfee 用户帐户，则必须创建管理员帐户 (第 25 页)。

创建管理员帐户

首次切换到使用 McAfee 用户时，会提示您创建管理员帐户。

创建管理员帐户：

1. 在“密码”框中键入密码，然后在“确认密码”框中重新键入此密码。
2. 在列表中选择密码恢复问题，然后在“答案”框中键入此机密问题的答案。
3. 单击“应用”。

   完成上述操作后，会使用“家长监控”程序（如果有）中现有的用户名和权限更新此窗格中的用户帐户类型。如果您是首次配置用户帐户，会显示“管理用户”窗格。

配置用户选项

如果您切换到使用 McAfee 用户帐户，则会自动导入“家长监控”程序中所有现有的用户名和权限。不过，首次切换时，您必须创建管理员帐户。然后，您可以开始创建和配置其他 McAfee 用户帐户。

配置用户选项：

1 在“SecurityCenter 信息”下面，单击“配置”。

2 单击“用户”旁边的箭头以展开其窗格，然后单击“高级”。

3 在“用户帐户”下，单击“添加”。

4 在“用户名”框中键入用户名。

5 在“密码”框中键入密码，然后在“确认密码”框中重新键入此密码。

6 如果需要该新用户在 SecurityCenter 启动时自动登录，请选中“启动用户”复选框。

7 在“用户帐户类型”下，选择该用户的帐户类型，然后单击“创建”。

注意：创建用户帐户后，必须在“家长监控”下为“受限用户”配置设置。

8 要编辑用户密码、自动登录或帐户类型，请在列表中选择用户名，然后单击“编辑”。

9 完成后，请单击“应用”。

取回管理员密码

如果您忘记了管理员密码，可以取回该密码。

取回管理员密码：

1 右键单击 SecurityCenter M 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 键入您创建管理员帐户时选择的机密问题的答案。

4 单击“提交”。

随即会显示您遗忘的管理员密码。

更改管理员密码

如果您认为管理员密码不易记忆，或者怀疑可能会泄漏，则可以更改该密码。

更改管理员密码：

1. 右键单击 SecurityCenter M 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“更改密码”。
3. 在“旧密码”框中键入当前密码。
4. 在“密码”框中键入新密码，然后在“确认密码”框中重新键入此密码。
5. 单击“确定”。

配置更新选项

连接到 Internet 后，SecurityCenter 每四小时自动检查一次所有 McAfee 服务的更新，并自动安装最新产品更新。不过，您可以随时使用任务栏最右侧通知区域中的 SecurityCenter 图标手动检查更新。

自动检查更新

连接到 Internet 后，SecurityCenter 每四个小时自动检查一次更新。不过，您可以将 SecurityCenter 配置为在下载或安装更新之前通知您。

自动检查更新：

1. 在“SecurityCenter 信息”下面，单击“配置”。
2. 单击“已启用自动更新”状态旁边的箭头以展开其窗格，然后单击“高级”。
3. 在“更新选项”窗格中选择以下任一选项：
   - 自动安装更新并在产品更新后通知我（建议） (第 29 页)
   - 自动下载更新并在可以安装更新时通知我 (第 29 页)
   - 下载任何更新之前都通知我 (第 30 页)
4. 单击“确定”。

注意：为了获得最大限度的保护，McAfee 建议使 SecurityCenter 执行自动检查并安装更新。不过，如果您只想手动更新安全服务，请禁用自动更新 (第 30 页)。

自动下载并安装更新

如果在 SecurityCenter“更新选项”中选中“自动安装更新并在服务更新后通知我(建议)”，SecurityCenter 将自动下载并安装更新。

自动下载更新

如果在“更新选项”中选中“自动下载更新并在可以开始安装更新时通知我”，SecurityCenter 将自动下载更新，并在安装准备就绪时发出通知。随后可以选择安装更新或推迟更新 (第 30 页)。

安装自动下载的更新：

1. 单击警报窗口中的“立即更新产品”，然后单击“确定”。

   如果出现提示，则必须先登录网站验证您的订购状态，然后才能进行下载。
2. 验证完订购状态后，请单击“更新”窗格中的“更新”以下载并安装更新。如果订购已过期，请单击警报窗口中的“续订”，并按照提示进行操作。

注意：在某些情况下，可能会提示您重新启动计算机以完成更新。在重新启动之前，请保存所有工作并关闭所有程序。

下载更新之前发出通知

如果在“更新选项”窗格中选中“下载任何更新之前都通知我”，SecurityCenter 将在下载任何更新之前发出通知。随后即可选择下载并安装安全服务更新以免遭受威胁的攻击。

下载并安装更新：

1 选择警报窗口中的“立即更新产品”，然后单击“确定”。

2 如果出现提示，请登录网站。

系统将自动下载更新。

3 安装完更新后，请单击警报窗口中的“确定”。

注意：在某些情况下，可能会提示您重新启动计算机以完成更新。在重新启动之前，请保存所有工作并关闭所有程序。

禁用自动更新

为了获得最大限度的保护，McAfee 建议使 SecurityCenter 执行自动检查并安装更新。不过，如果您只想手动更新安全服务，则可以禁用自动更新。

注意：必须记住每周至少手动检查更新 (第 31 页)一次。如果没有检查更新，则无法使用最新的安全更新来保护您的计算机。

禁用自动更新：

1 在“SecurityCenter 信息”下，单击“配置”。

2 单击“已启用自动更新”状态旁边的箭头以展开其窗格。

3 单击“关”。

4 单击“是”确认更改。

标题中的状态已更新。

如果在 7 天内没有手动检查更新，将会出现一条警报，提醒您检查更新。

推迟更新

当显示警报时，如果因太忙而无法更新安全服务，可以选择稍后提醒或者忽略警报。

推迟更新：

- 执行以下任一操作：
  - 选择警报窗口中的“稍后提醒我”，然后单击“确定”。
  - 选择“关闭此警报”，然后单击“确定”关闭警报窗口而不执行任何操作。

手动检查更新

连接到 Internet 时，SecurityCenter 每四小时自动检查一次更新，并安装最新产品更新。不过，您可以随时使用任务栏最右侧的 Windows 通知区域中的 SecurityCenter 图标手动检查更新。

注意：为了获得最大限度的保护，McAfee 建议使 SecurityCenter 执行自动检查并安装更新。不过，如果您只想手动更新安全服务，请禁用自动更新 (第 30 页)。

手动检查更新：

1. 确保计算机已连接到 Internet。
2. 右键单击任务栏最右侧的 Windows 通知区域中的 SecurityCenter M 图标  ，然后单击“更新”。

   在 SecurityCenter 正在检查更新时，您可以使用它执行其他任务。

   为方便起见，系统会在任务栏最右侧的 Windows 通知区域显示一个动画图标。在 SecurityCenter 完成执行后，此图标会自动消失。
3. 如果出现提示，请登录到网站验证您的订购状态。

注意：在某些情况下，可能会提示您重新启动计算机以完成更新。在重新启动之前，请保存所有工作并关闭所有程序。

配置警报选项

SecurityCenter 会自动发出警报和声音，通知您有关流行病毒发作、安全威胁以及产品更新的信息。不过，您可以将 SecurityCenter 配置为仅显示要求立即处理的警报。

配置警报选项

SecurityCenter 会自动发出警报和声音，通知您有关流行病毒发作、安全威胁以及产品更新的信息。不过，您可以将 SecurityCenter 配置为仅显示要求立即处理的警报。

配置警报选项：

1 在“SecurityCenter 信息”下面，单击“配置”。

2 单击“警报”旁边的箭头以展开其窗格，然后单击“高级”。

3 在“警报选项”窗格中选择以下任一选项：

- **当某一流行病毒发作或出现安全威胁时发出警报**
- **当检测到游戏模式时显示信息警报**
- **出现警报时播放声音**
- **在 Windows 启动时显示 McAfee 启动屏幕**

4 单击“确定”。

注意：要禁用将来警报自身发来的信息警报，请选中“不再显示此警报”复选框。您可以稍后在“信息警报”窗格中再次启用它们。

配置信息警报

信息警报会在发生不要求立即处理的事件时通知您。如果禁用将来警报自身发来的信息警报，则可以稍后在“信息警报”窗格中再次启用它们。

配置信息警报：

1 在“SecurityCenter 信息”下，单击“配置”。

2 单击“警报”旁边的箭头以展开其窗格，然后单击“高级”。

3 在“SecurityCenter 配置”下，单击“信息警报”。

4 清除“隐藏信息警报”复选框，然后在列表中清除要显示的警报的复选框。

5 单击“确定”。

第 5 章

执行常见任务

您可以执行常见任务，包括返回到“主页”窗格、查看最新事件、管理计算机网络（如果在对此网络具有管理功能的计算机上）以及维护计算机。如果已安装 McAfee Data Backup，还可以备份数据。

本章内容

执行常见任务

您可以执行常见任务，包括返回到“主页”窗格、查看最新事件、维护计算机、管理计算机网络（如果在对此网络具有管理功能的计算机上）以及备份数据（如果已安装 McAfee Data Backup）。

执行常见任务：

- 在“基本菜单”的“常见任务”下，执行以下任一操作：
  - 要返回到“主页”窗格，请单击“主页”。
  - 要查看通过安全软件检测到的最新事件，请单击“最新事件”。
  - 要删除不使用的文件、对数据进行碎片整理以及将计算机还原到以前的设置，请单击“维护计算机”。
  - 要管理计算机网络，请在对此网络有管理功能的计算机上单击“管理网络”。

    Network Manager 会监视网络上计算机的安全弱点，这样您可以轻松地识别网络安全问题。
  - 要创建文件的备份副本，请单击“Data Backup”（如果已安装 McAfee Data Backup）。

    自动备份会保存您指定位置上最重要的文件副本，并将文件加密并存储到 CD/DVD、USB、外部或网络驱动器上。

提示：为方便起见，您可以从其他两个位置执行常见任务（在“高级菜单”的“主页”下；在任务栏最右侧 SecurityCenter M 图标的“快速链接”菜单中）。您还可以在“高级菜单”上的“报告和日志”下面查看最新事件以及按类型列出的综合日志。

查看最新事件

最新事件是在计算机发生更改时记录的。计算机发生更改时的示例包括：启用或禁用保护类型时、删除威胁时或者阻止 Internet 连接尝试时。您可以查看最多 20 条最新事件及其详细信息。

有关其事件的详细信息，请参阅相关产品的帮助文件。

查看最新事件：

1. 右键单击主 SecurityCenter 图标，指向“快速链接”，然后单击“查看最新事件”。

   任何最新事件均会出现在列表中，其中显示了事件日期及简要说明。

2. 在“最新事件”下，选择某个事件以在“详细信息”窗格中查看其他信息。

   在“我想”下，会显示所有可执行的操作。

3. 要查看更全面的事件列表，请单击“查看日志”。

自动维护计算机

要释放宝贵的磁盘空间并优化计算机性能，您可以计划定期运行 QuickClean 或磁盘碎片整理程序任务。这些任务包括删除、清除文件和文件夹以及对文件和文件夹进行碎片整理。

自动维护计算机：

1. 右键单击主 SecurityCenter 图标，指向“快速链接”，然后单击“维护计算机”。
2. 在“任务计划程序”下，单击“开始”。
3. 在操作列表中，选择“QuickClean”或“磁盘碎片整理程序”。
4. 执行以下任一操作：
   - 要修改现有任务，请选择该任务，然后单击“修改”。按照屏幕上的说明执行操作。
   - 要创建新任务，请在“任务名称”框中输入名称，然后单击“创建”。按照屏幕上的说明执行操作。
   - 要删除任务，请选择该任务，然后单击“删除”。

5　在“任务摘要”下，查看上次运行任务的时间、下次运行任务的时间及其状态。

手动维护计算机

您可以执行手动维护任务以删除不使用的文件、对数据进行碎片整理或将计算机还原到以前的设置。

手动维护计算机：

- 执行以下任一操作：
  - 要使用 QuickClean，请右键单击主 SecurityCenter 图标，指向“快速链接”，然后依次单击“维护计算机”和“开始”。
  - 要使用磁盘碎片整理程序，请右键单击主 SecurityCenter 图标，指向“快速链接”，然后依次单击“维护计算机”和“分析”。
  - 要使用“系统还原”功能，请在“高级菜单”上单击“工具”，然后依次单击“系统还原”和“开始”。

删除不使用的文件和文件夹

使用 QuickClean 释放宝贵的磁盘空间并优化计算机性能。

删除不使用的文件和文件夹：

1. 右键单击主 SecurityCenter 图标，指向“快速链接”，然后单击“维护计算机”。
2. 在“QuickClean”下，单击“开始”。
3. 按照屏幕上的说明执行操作。

对文件和文件夹进行碎片整理

删除文件和文件夹以及添加新文件时，都会出现文件碎片。这些碎片会降低磁盘访问速度以及计算机的整体性能，尽管通常并不严重。

使用碎片整理功能可以将文件的某些部分重新写入到硬盘上的连续扇区，以增加磁盘访问和检索速度。

对文件和文件夹进行碎片整理：

1. 右键单击主 SecurityCenter 图标，指向“快速链接”，然后单击“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。

将计算机还原到以前的设置

还原点是指 Windows 定期保存的、发生重要事件（例如安装程序或驱动程序）时的计算机的“快照”。不过，您可以随时创建和命名自己的还原点。

使用还原点可以撤消对计算机有害的更改并使其恢复为以前的设置。

将计算机还原到以前的设置：

1. 在“高级菜单”上，依次单击“工具”和“系统还原”。
2. 在“系统还原”下，单击“开始”。
3. 按照屏幕上的说明执行操作。

管理网络

如果您的计算机具有网络管理功能，则可以使用 Network Manager 监视网络上计算机的安全漏洞，这样您可以轻松地识别安全问题。

如果计算机的保护状态在网络上未受到监视，则表明此计算机不属于该网络，或者是该网络中不受管理的成员。有关详细信息，请参阅 Network Manager 帮助文件。

管理网络：

1. 右键单击主 SecurityCenter 图标，指向“快速链接”，然后单击“管理网络”。
2. 单击网络图中代表此计算机的图标。
3. 在“我想”下面，单击“监视此计算机”。

了解有关病毒的更多信息

使用病毒信息库和病毒分布图执行以下操作：

- 了解有关最新病毒、电子邮件病毒恶作剧和其他威胁的详细信息。
- 获得免费的病毒删除工具，以帮助您修复计算机。
- 实时获取全球计算机感染的最新病毒分布情况一览图。

了解有关病毒的更多信息：

1. 在“高级菜单”上，依次单击“工具”和“病毒信息”。
2. 执行以下任一操作：
   - 使用免费的 McAfee 病毒信息库研究病毒。
   - 使用 McAfee 网站上的全球病毒分布图研究病毒。

第 6 章

McAfee QuickClean

在 Internet 上冲浪时，计算机会迅速累积大量垃圾文件。使用 QuickClean 可以保护隐私并删除不需要的 Internet 和电子邮件垃圾。QuickClean 能够识别并删除在网上冲浪时累积的文件，包括 Cookie、电子邮件、下载和历史记录（即包含您个人信息的数据）。它通过安全删除此敏感信息，即可保护您的隐私。

QuickClean 还会删除不需要的文件。指定要清除的文件，然后彻底删除垃圾文件而不会删除重要信息。

本章内容

了解 QuickClean 功能

本节介绍 QuickClean 功能。

功能

QuickClean 提供一组可以安全删除数字碎片的有效且易用的工具。您可以释放宝贵的驱动器空间并优化计算机的性能。

第 7 章

清理计算机

QuickClean 可以安全删除文件和文件夹。

浏览 Internet 时，浏览器会将每个 Internet 页面及其图像复制到磁盘上的缓存文件夹。如果您再次返回此页面，浏览器便可快速将其加载。如果重复访问相同的 Internet 页面，而且这些页面的内容不会频繁更改，则缓存文件很有用。不过，在大多数情况下，缓存文件没有用，可以将其删除。

可以使用以下清除程序删除多种项目。

- 回收站清除程序：清除 Windows 回收站。
- 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：删除断开的快捷方式和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。
- 缓存清除程序：删除浏览 Internet 时累积的缓存文件。此类型文件通常作为临时 Internet 文件存储。
- Cookie 清除程序：删除 Cookie。此类型文件通常作为临时 Internet 文件存储。
  Cookie 是 Web 浏览器在请求 Web 服务器时存储在您计算机上的小文件。在您每次浏览 Web 服务器的网页时，浏览器便会将 Cookie 重新发送到服务器。这些 Cookie 可以作为标记，Web 服务器利用它们跟踪您浏览的页面以及重新浏览这些页面的频率。
- 浏览器历史记录清除程序：删除浏览器历史记录。
- 已删除项目和已发送项目的 Outlook Express 和 Outlook 电子邮件清除程序：从已发送和已删除的 Outlook 文件夹中删除邮件。
- 最近使用项的清除程序：删除计算机上存储的最近使用的项目，例如 Microsoft Office 文档。
- ActiveX 和插件清除程序：删除 ActiveX 控件和插件。
  ActiveX 是一种用于在程序中实现控件的技术。ActiveX 控件可以将按钮添加到程序的界面。大多数控件是无害的；不过，有人可能会使用 ActiveX 技术来捕获您计算机的信息。
  插件是可以插入较大应用程序以提供附加功能的小软件程序。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的文件（如动画、视频和音频文件）。

- 系统还原点清除程序：删除计算机中旧的系统还原点。

本章内容

使用 QuickClean

本节介绍如何使用 QuickClean。

清理计算机

您可以删除无用的文件和文件夹，释放磁盘空间，使计算机更有效地运行。

清理计算机：

1. 在“高级菜单”上，单击“工具”。
2. 单击“维护计算机”，然后单击“McAfee QuickClean”下的“开始”。
3. 执行以下任一操作：
   - 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”。对于“最近使用项的清除程序”，可以单击“属性”以取消选中不希望清除其列表的程序。
   - 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”执行文件删除。您可以展开此列表以查看要清除的文件及其位置。
5. 单击“下一步”。
6. 执行以下任一操作：
   - 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。使用 Shredder 删除的文件将无法恢复。
7. 单击“完成”。
8. 在“QuickClean 摘要”下，查看已删除的注册表文件的数量，以及在执行磁盘和 Internet 清除后回收的磁盘空间量。

第 8 章

McAfee Shredder

即使清空回收站，也可以从计算机恢复已删除的文件。删除文件后，Windows 会将磁盘驱动器上的此空间标记为不再使用，但文件仍位于原位置。使用计算机分析工具，可以恢复纳税记录、工作简历或已删除的其他文档。Shredder 可以通过安全而永久删除不需要的文件来保护您的隐私。

要永久删除文件，必须用新文件反复覆盖现有的文件。Microsoft® Windows 不会安全地删除文件，因为每个文件操作都很慢。清除文档并不一定会防止恢复文档，因为某些程序会创建打开文档的临时隐藏副本。如果只清除在 Windows® 资源管理器中看到的文档，这些文档仍有临时副本。

注意：已清除的文件不会备份。您无法恢复 Shredder 已删除的文件。

本章内容

了解 Shredder 功能

本节介绍 Shredder 功能。

功能

Shredder 可以删除回收站内容、临时 Internet 文件、网站历史记录、文件、文件夹和磁盘。

第 9 章

使用 Shredder 删除不需要的文件

Shredder 会通过安全而永久地删除不需要的文件（如回收站内容、临时 Internet 文件和网站历史记录）来保护您的隐私。您可以选择要清除的文件和文件，或通过浏览查找这些文件和文件夹。

本章内容

使用 Shredder

本节介绍如何使用 Shredder。

清除文件、文件夹和磁盘

即使在清空回收站后，文件也可能会驻留在计算机上。不过，在清除文件后，您的数据将永久删除，黑客无法对其进行访问。

清除文件、文件夹和磁盘：

1. 在“高级菜单”上，依次单击“工具”和“Shredder”。
2. 执行以下任一操作：
   - 单击“删除文件和文件夹”以清除文件和文件夹。
   - 单击“删除整个磁盘”以清除磁盘。
3. 选择以下任一清除级别：
   - **快速**：清除所选项目 1 次。
   - **全面**：清除所选项目 7 次。
   - **自定义**：清除所选项目最多 10 次。更高的清除操作数会增加文件的安全删除级别。
4. 单击“下一步”。
5. 执行以下任一操作：
   - 如果要清除文件，请在“选择要清除的文件”列表中，单击“回收站内容”、“临时 Internet 文件”或“网站历史记录”。如果要清除磁盘，请单击磁盘。
   - 单击“浏览”，导航到要清除的文件，然后选择文件。
   - 在“选择要清除的文件”列表中，键入要清除文件的路径。
6. 单击“下一步”。
7. 单击“完成”以完成操作。
8. 单击“完成”。

第 10 章

McAfee Network Manager

McAfee® Network Manager 提供组成家庭网络的计算机和组件的图形视图。您可以使用 Network Manager 远程监视网络中每个托管计算机的保护状态，并在这些托管计算机上远程修复已报告的安全漏洞。

在开始使用 Network Manager 之前，您应熟悉某些最常用的功能。Network Manager 帮助会提供有关配置和使用这些功能的详细信息。

本章内容

功能

Network Manager 提供以下功能：

图形网络图

Network Manager 的网络图会提供组成家庭网络的计算机和组件的安全状态的图形概述。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。还可以查看与网络图中显示的任一组件关联的详细信息。

远程管理

使用 Network Manager 网络图可以管理组成家庭网络的计算机的安全状态。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，并从网络上的远程计算机修复已知的安全漏洞。

了解 Network Manager 图标

下表介绍 Network Manager 网络图中最常用的图标。

图标	描述
	表示联机的托管计算机
	表示脱机的托管计算机
	表示已安装 McAfee 2007 安全软件的非托管计算机
	表示脱机的非托管计算机
	表示没有安装 McAfee 2007 安全软件的联机计算机，或表示未知的网络设备
	表示没有安装 McAfee 2007 安全软件的脱机计算机，或表示脱机的未知网络设备
	表示已保护或已连接相应的项目
	表示相应的项目需要处理
	表示相应的项目需要处理且已断开连接
	表示无线家用路由器
	表示标准家用路由器
	表示连接后的 Internet
	表示断开连接后的 Internet

第 11 章

设置托管网络

通过使用网络图上的项目并将成员（计算机）添加到网络来设置托管网络。

本章内容

使用网络图

每次将计算机连接到网络，Network Manager 会分析网络的状态，以确定是否有任何成员（托管或非托管）、路由器属性和 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，并自动使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 McAfee 2007 安全软件的第一台计算机的工作组或域名；不过，您可以随时重命名网络。

在更改网络（如添加计算机）时，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的组件来自定义您的视图。还可以查看与网络图中显示的任一组件关联的详细信息。

访问网络图

您可以从常用任务的 SecurityCenter 列表中启动 Network Manager 来访问网络图。网络图提供组成家庭网络的计算机和组件的图形表示。

访问网络图：

- 在“基本菜单”或“高级菜单”上，单击“管理网络”。
  网络图随即会显示在右侧窗格中。

注意：首次访问网络图时，系统会提示您先信任网络上的其他计算机，然后才会显示网络图。

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。

刷新网络图：

1. 在“基本菜单”或“高级菜单”上，单击“管理网络”。
   网络图随即会显示在右侧窗格中。
2. 单击“我想”下的“刷新网络图”。

注意：只有在网络图上没有选择项目的情况下，“刷新网络图”链接才可用。要取消选中项目，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 McAfee 2007 安全软件的第一台计算机的工作组或域名。如果此名称不合适，您可以更改此名称。

重命名网络：

1. 在“基本菜单”或“高级菜单”上，单击“管理网络”。
   网络图随即会显示在右侧窗格中。
2. 单击“我想”下的“重命名网络”。
3. 在“重命名网络”框中键入网络的名称。
4. 单击“确定”。

注意：只有在网络图上没有选择项目的情况下，“重命名网络”链接才可用。要取消选中项目，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组件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”。

查看项目详细信息

通过选择网络图上的组件，可以查看网络中有关任何组件的详细信息。此信息包含组件名称、其保护状态和管理组件所需的其他信息。

查看项目的详细信息：

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

在可以远程管理计算机或可以授予它权限以远程管理网络上的其他计算机之前，它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（如共享文件或打印机）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 McAfee Wireless Network Security 或 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此计算机和网络上的其他计算机互相监视各自的安全设置（如计算机的病毒保护服务是否是最新的）。

加入托管网络：

1. 在邀请对话框中，选中“允许此计算机和其他计算机互相监视各自的安全设置”复选框，以允许托管网络上的其他计算机监视您计算机的安全设置。
2. 单击“加入”。
   在接受邀请后，会显示两个图片。
3. 确认图片与邀请您加入托管网络的计算机上显示的图片相同。
4. 单击“确认”。

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相同，则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，单击安全确认对话框中的“拒绝”。

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网络。发送邀请时，还可以指定要分配给加入计算机的权限级别。

邀请计算机加入此托管网络：

1 单击网络图上非托管计算机的图标。

2 单击“我想”下的“监视此计算机”。

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：

- **授予来宾访问权限**
  来宾访问权限允许计算机访问网络。
- **授予对所有托管网络应用程序的完全访问权限**
  完全访问权限（类似来宾访问权限）允许计算机访问网络。
- **授予对所有托管网络应用程序的管理访问权限**
  管理访问权限允许计算机使用管理权限访问网络。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“邀请”。
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，会显示两个图片。

5 确认图片与邀请您加入托管网络的计算机上显示的图片相同。

6 单击“授予访问权限”。

注意：如果您邀请加入托管网络的计算机所显示的图片与安全确认对话框中显示的图片不相同，则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

如果您错误同意信任网络上的其他计算机，则可以停止信任它们。

停止信任网络上的计算机：

- 单击“我想”下的“停止信任此网络上的计算机”。

注意：只有在其他托管计算机没有加入网络时，“停止信任此网络上的计算机”链接才可用。

第 12 章

远程管理网络

在设置托管网络后，可以使用 Network Manager 远程管理组成网络的计算机和组件。您可以监视计算机和组件的状态及权限级别，然后远程修复安全漏洞。

本章内容

监视状态和权限

托管网络包含两种类型的成员：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监视其 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（如共享文件或打印机）的来宾计算机。非托管计算机可以随时由网络上的其他托管计算机邀请成为托管计算机。同样，托管计算机可以随时成为非托管计算机。

托管计算机包含与其相关联的管理、完全或来宾权限。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。

因为托管网络还包含设备（如路由器），所以也可以使用 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。

监视计算机的保护状态

如果网络上的某台计算机的保护状态未受监视（由于计算机不是网络的成员或计算机是网络的非托管成员），则可以请求监视它。

监视计算机的保护状态：

1 单击网络图上非托管计算机的图标。

2 单击“我想”下的“监视此计算机”。

停止监视计算机的保护状态

您可以停止监视专用网络中托管计算机的保护状态。然后，计算机便成为非托管计算机。

停止监视计算机的保护状态：

1 单击网络图上托管计算机的图标。

2 单击“我想”下的“停止监视此计算机”。

3 在确认对话框中，单击“是”。

修改托管计算机的权限

您可以随时修改托管计算机的权限。此功能允许您调整可以监视网络上其他计算机的保护状态（安全设置）的计算机。

修改托管计算机的权限：

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监视各自的保护状态。
4. 单击“确定”。

管理设备

您可以访问 Network Manager 中设备的管理网页来管理设备。

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”。
   Web 浏览器会打开和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 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。

修改设备的显示属性：

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. 指定设备类型，单击以下任一项：
   - **路由器**
     这表示标准的家用路由器。
   - **无线路由器**
     这表示无线家用路由器。

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监视网络上其他托管计算机的 McAfee 保护状态，并远程修复任何报告的安全漏洞。例如，如果托管计算机的 McAfee 保护状态表示已禁用 VirusScan，则具有管理权限的其他托管计算机都可以通过远程启用 VirusScan 来“修复”此安全漏洞。

远程修复安全漏洞时，Network Manager 会自动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 会修复这些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，建议的修复方法是在远程计算机或网络上的计算机上安装 McAfee 2007 安全软件。

修复安全漏洞

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

修复安全漏洞：

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，某些修复可能会要求您在有漏洞的计算机上启动 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运行 McAfee 2007 安全软件，则无法远程监视其安全状态。如果要远程监视这些计算机，则必须转至每台计算机，并安装 McAfee 2007 安全软件。

在远程计算机上安装 McAfee 安全软件：

1. 在远程计算机上的浏览器中，转至 http://download.mcafee.com/us/。
2. 按照屏幕上的说明在计算机上安装 McAfee 2007 安全软件。

第 13 章

McAfee VirusScan

VirusScan 提供全面的、可靠的和最新的病毒和间谍软件防护。VirusScan 采用屡获大奖的 McAfee 扫描技术，可以抵御病毒、蠕虫、特洛伊木马程序、可疑脚本、Rootkit、缓冲区溢出、混合型病毒、间谍软件、可能有害的程序以及其他威胁的攻击。

本章内容

功能

本版本的 VirusScan 具有以下功能。

病毒防护

实时扫描会在您或您的计算机访问文件时扫描这些文件。

扫描

在硬盘驱动器、软盘以及个别文件和文件夹中搜索病毒和其他威胁。您还可以右键单击一个项目来扫描它。

间谍软件和广告软件检测

VirusScan 可以确定并删除危及隐私安全和降低计算机性能的间谍软件、广告软件和其他程序。

自动更新

自动更新会抵御最新的已知和未知的计算机威胁。

快速后台扫描

以无需干预的方式快速进行扫描，确定并销毁病毒、特洛伊木马程序、蠕虫、间谍软件、广告软件、拨号程序以及其他威胁，而且不会打断您的工作。

实时安全警报

安全警报会发出有关紧急病毒发作和安全威胁的通知，并提供用于消除和化解威胁以及了解威胁详细信息的选项。

在多个侵入点检测和清除病毒

VirusScan 会在计算机的关键侵入点监控和清除病毒，其中包括：电子邮件、即时消息附件和 Internet 下载。

监视电子邮件中的类蠕虫活动

WormStopper™ 会阻止特洛伊木马程序用电子邮件将蠕虫传送到其他计算机，并在未知的电子邮件程序将电子邮件发送到其他计算机之前提醒您。

监视脚本中的类蠕虫活动

ScriptStopper™ 会阻止未知的、有害的脚本在您计算机上运行。

McAfee X-ray for Windows

McAfee X-ray 会检测和封杀躲避 Windows 的 Rootkit 和其他程序。

缓冲区溢出保护

缓冲区溢出保护会防止出现缓冲区溢出。在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）中存储超过其限制的数据时，会发生缓冲区溢出，从而损害或覆盖相邻缓冲区中的有效数据。

McAfee SystemGuard

SystemGuard 会检查计算机上可能表示病毒、间谍软件或黑客活动的特定行为。

第 14 章

管理病毒防护

您可以管理实时病毒、间谍软件、SystemGuard 和脚本防护。例如，可以禁用扫描或指定要扫描的内容。

只有管理员权限的用户才能修改高级选项。

本章内容

使用病毒防护

启动病毒防护（实时扫描）后，它会持续监视计算机中的病毒活动。实时扫描会在您或您的计算机每次访问文件时对其进行扫描。在病毒防护检测到感染病毒的文件后，它会尝试清除或删除感染的文件。如果无法清除或删除文件，则会显示警报提示您采取进一步的措施。

相关主题

- 了解安全警报 (第 101 页)

禁用病毒防护

如果禁用病毒防护，则不会持续监视计算机中的病毒活动。如果必须停止病毒防护，确保您没有连接到 Internet。

注意：禁用病毒防护还禁用了实时间谍软件、电子邮件和即时消息防护。

禁用病毒防护：

1. 在“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“病毒防护”下，单击“关”。
4. 在“确认”对话框中，执行以下任一操作：
   - 要在指定的时间后重新启动病毒的防护，请选中“在此时间后重新启用实时扫描”复选框，然后从菜单中选择时间。
   - 要在指定的时间后禁止病毒防护重新启动，请清除“在此时间后重新启用病毒防护”复选框。
5. 单击“确定”。

如果已将实时防护配置为在 Windows 启动时启动，则计算机在重新启动后便会获得防护。

相关主题

- 配置实时防护 (第 74 页)

启用病毒防护

病毒防护会持续监视计算机中的病毒活动。

启用病毒防护：

1. 在“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“病毒防护”下，单击“开”。

配置实时防护

您可以修改实时病毒防护。例如，可以只扫描程序和文档，也可以在 Windows 启动时禁用实时扫描（建议不要禁用）。

配置实时防护

您可以修改实时病毒防护。例如，可以在 Windows 启动时只扫描程序和文档，也可以禁用实时扫描（不推荐）。

配置实时防护：

1 在“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“病毒防护”下，单击“高级”。

4 选中或清除以下复选框：

- **使用启发式技术扫描未知病毒**：将文件与已知病毒的签名进行比较，以检测未知病毒的特征。此选项是最彻底的扫描方法，但通常比正常扫描速度慢。
- **关机时扫描软盘驱动器**：关闭计算机时，扫描软盘驱动器。
- **扫描间谍软件和可能有害的程序**：检测和删除未经许可可能收集及传输数据的间谍软件、广告软件和其他程序。
- **扫描和删除跟踪 Cookie**：检测和删除未经许可可能收集及传输数据的 Cookie。用户访问网页时，Cookie 会标识用户。
- **扫描网络驱动器**：扫描连接到网络的驱动器。
- **启用缓冲区溢出防护**：如果检测到缓冲区溢出活动，它会阻止此活动并提醒您。
- **Windows 启动时启动实时扫描(建议)**：每次启动计算机时启用实时防护，即使关闭了某个会话的实时防护也是如此。

5 单击以下任一按钮：

- **所有文件(建议)**：扫描计算机使用的每种文件类型。使用此选项进行最全面的扫描。
- **仅限程序文件和文档**：只扫描程序文件和文档。

6 单击“确定”。

使用间谍软件防护

间谍软件防护会删除未经许可收集和传输数据的间谍软件、广告软件和其他可能有害的程序。

禁用间谍软件防护

如果禁用间谍软件防护，则不会检测未经许可收集和传输数据的可能有害的程序。

禁用间谍软件防护：

1 在“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“间谍软件防护”下，单击“关”。

启用间谍软件防护

间谍软件防护会删除未经许可收集和传输数据的间谍软件、广告软件和其他可能有害的程序。

启用间谍软件防护：

1 在“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“间谍软件防护”下，单击“开”。

使用 SystemGuard

SystemGuard 会检测对计算机的可能未授权的更改并在出现更改时提醒您。然后，您可以查看这些更改并决定是否允许更改。

SystemGuard 分类如下。

程序

程序 SystemGuard 会检测对启动文件、扩展名和配置文件的更改。

Windows

Windows SystemGuard 会检测对 Internet Explorer 设置（包括浏览器属性和安全设置）的更改。

浏览器

浏览器 SystemGuard 会检测对 Windows® 服务、证书和配置文件的更改。

禁用 SystemGuard

如果禁用 SystemGuard，则不会检测对计算机的可能未经授权的更改。

禁用全部 SystemGuard：

1 在“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“SystemGuard 保护”下，单击“关”。

启用 SystemGuard

SystemGuard 会检测对计算机的可能未授权的更改并在出现更改时提醒您。

启用 SystemGuard：

1 在“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“SystemGuard 保护”下，单击“开”。

配置 SystemGuard

您可以修改 SystemGuard。对于检测到的每个更改，可以确定是否提醒您并记录事件、只记录事件或禁用 SystemGuard。

配置 SystemGuard

您可以修改 SystemGuard。对于检测到的每个更改，可以确定是否提醒您并记录事件、只记录事件或禁用 SystemGuard。

配置 SystemGuard：

1. 在“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“SystemGuard 保护”下，单击“高级”。
4. 在 SystemGuard 列表中，单击某个类别以查看相关联的 SystemGuard 及其状态的列表。
5. 单击 SystemGuard 的名称。
6. 在“详细信息”下，查看有关 SystemGuard 的信息。
7. 在 “我想”下，执行以下任一操作：
   - 如果要在更改发生时提醒您并记录事件，请单击“显示警报”。
   - 如果不想在检测到更改时采取操作，请单击“只记录更改”。只会记录更改。
   - 单击“禁用此 SystemGuard”以关闭 SystemGuard。更改发生时不会提醒您且不记录事件。
8. 单击“确定”。

了解 SystemGuard

SystemGuard 会检测对计算机的可能未授权的更改并在出现更改时提醒您。然后，您可以查看这些更改并决定是否允许更改。

SystemGuard 分类如下。

程序

程序 SystemGuard 会检测对启动文件、扩展名和配置文件的更改。

Windows

Windows SystemGuard 会检测对 Internet Explorer 设置（包括浏览器属性和安全设置）的更改。

浏览器

浏览器 SystemGuard 会检测对 Windows® 服务、证书和配置文件的更改。

关于程序 SystemGuard

程序 SystemGuard 会检测以下项目。

ActiveX 安装

检测通过 Internet Explorer 下载的 ActiveX 程序。ActiveX 程序从网站下载后，存储在计算机的 C:\Windows\Downloaded Program Files 或 C:\Windows\Temp\Temporary Internet Files 中。这些程序也可以在注册表中通过 CLSID（花括号之间的一长串数字）引用。

Internet Explorer 使用许多合法的 ActiveX 程序。如果您无法确定 ActiveX 程序是否有害，可以删除它而不会损害计算机。如果以后需要此程序，Internet Explorer 会在下次您返回所需的网站时自动下载。

启动项目

监视对启动注册表项和文件夹的更改。Windows 注册表中的启动注册表项和“启动”菜单中的启动文件夹存储指向计算机上程序的路径。Windows 启动时会加载这些位置列出的程序。间谍软件或其他可能有害的程序通常会在 Windows 启动时尝试加载。

Windows Shell 执行挂钩

监视对 explorer.exe 中加载的程序列表所做的更改。Shell 执行挂钩是加载到 explorer.exe Windows Shell 的程序。Shell 执行挂钩程序接收计算机上运行的所有执行命令。在实际启动其他程序之前，加载到 explorer.exe Shell 中的任何程序都可以执行其他任务。间谍软件或其他可能有害的程序可能使用 Shell 执行挂钩阻止安全程序运行。

Shell 服务对象延迟加载

监视对 Shell 服务对象延迟加载中列出的文件的更改。计算机启动时，由 explorer.exe 加载这些文件。因为 explore.exe 是计算机的 Shell，所以它始终会启动，加载此关键字下的文件。这些文件最初会在启动过程加载，这一过程之前没有人为干预。

关于 Windows SystemGuard

Windows SystemGuard 会检测以下项目。

上下文菜单处理程序

防止对 Windows 上下文菜单进行未经授权的更改。利用这些菜单可以右键单击文件，然后执行与此文件有关的特定操作。

AppInit DLL

防止对 Windows AppInit.DLL 进行未经授权的更改或添加。AppInit_DLL 注册表值包含一个在加载 user32.dll 时加载的文件列表。AppInit_DLL 值中的文件是最初在 Windows 启动例程执行时加载的，因而会在人为干预之前，有害的 .DLL 可能会隐藏自身。

Windows Hosts 文件

监视对计算机 Hosts 文件的更改。Hosts 文件用于将某些域名重定向到特定的 IP 地址。例如，在访问 www.example.com 时，浏览器会检查 Hosts 文件，查看 example.com 的条目，并指向此域的 IP 地址。某些间谍软件程序会尝试更改 Hosts 文件，以将浏览器重定向到其他站点或禁止软件正常更新。

Winlogon Shell

监视 Winlogon Shell。此 Shell 在用户登录到 Windows 时加载。此 Shell 是用于管理 Windows 的主用户接口 (UI)，通常是 Windows 资源管理器 (explorer.exe)。不过，您可以轻松地更改 Windows Shell 以指向其他程序。如果发生这种情况，则用户每次登录时都会启动 Windows Shell 之外的程序。

Winlogon User Init

监视对 Windows 登录用户设置的更改。注册表项 HKLM\Software\Microsoft WindowsNT\CurrentVersion\Winlogon\Userinit 指定在用户登录到 Windows 后所启动的程序。此默认程序会恢复您用户名的配置文件、字体、颜色和其他设置。间谍软件和其他可能有害的程序可能会尝试将自身添加到此项来启动。

Windows 协议

监视对网络协议的更改。某些间谍软件或其他可能有害的程序会控制计算机发送和接收信息的特定方式。这可以通过 Windows 协议过滤器和处理程序来实现。

Winsock 分层服务提供者

监视分层服务提供者 (LSP)，它可以在网络上拦截您的数据，并对其进行更改或重定向。合法 LSP 包含家长监控软件、防火墙和其他安全程序。间谍软件可以使用 LSP 监视您的 Internet 活动和修改数据。为避免重新安装操作系统，请使用 McAfee 程序自动删除间谍软件和受损害的 LSP。

Windows Shell Open Command

防止对 Windows Shell (explore.exe) Open Command 的更改。Shell Open Command 允许每次运行某种类型的文件时运行特定的程序。例如，蠕虫可能试图在每次 .exe 应用程序运行时运行。

共享任务计划程序

监视 SharedTaskScheduler 注册表项，它包含 Windows 启动时运行程序的列表。某些间谍软件或其他可能有害的程序会修改此注册表项，并在未经您许可的情况下，将自身添加到此列表中。

Windows Messenger 服务

监视 Windows Messenger 服务，这是一个未公开的 Windows Messenger 功能，允许用户发送弹出消息。某些间谍软件或其他可能有害的程序试图启用此服务并发送未经请求的广告，还可以利用此服务的已知漏洞来远程运行代码。

Windows Win.ini 文件

win.ini 文件是一个文本文件，提供 Windows 启动时运行程序的列表。此文件含有加载这些程序的语法，用于支持旧版 Windows。大多数程序都不使用 win.ini 文件加载程序。不过，某些间谍软件或其他可能有害的程序会专门利用此语法，在 Windows 启动时加载自身。

关于浏览器 SystemGuard

浏览器 SystemGuard 会检测以下项目。

浏览器辅助对象

监视浏览器辅助对象 (BHO) 的添加。BHO 是用作 Internet Explorer 插件的程序。间谍软件和浏览器劫持程序经常使用 BHO 显示广告或跟踪您的浏览习惯。许多合法程序（如常见的搜索工具栏）也使用 BHO。

Internet Explorer 栏

监视对 Internet Explorer 栏程序列表的更改。浏览器栏是一个窗格，类似于 Internet Explorer (IE) 或 Windows 资源管理器中的“搜索”、“收藏夹”或“历史记录”窗格。

Internet Explorer 插件

防止间谍软件安装 Internet Explorer 插件。Internet Explorer 插件是在 Internet Explorer 启动时加载的软件加载项。间谍软件通常使用 Internet Explorer 插件显示广告或跟踪浏览习惯。合法插件会将功能添加到 Internet Explorer。

Internet Explorer ShellBrowser

监视对 Internet Explorer ShellBrowser 实例的更改。Internet Explorer ShellBrowser 包含有关 Internet Explorer 实例的信息和设置。如果更改了这些设置或添加了新 ShellBrowser，则此 ShellBrowser 可以完全控制 Internet Explorer，并添加工具栏、菜单和按钮等功能。

Internet Explorer WebBrowser

监视对 Internet Explorer WebBrowser 实例的更改。Internet Explorer WebBrowser 包含有关 Internet Explorer 实例的信息和设置。如果更改了这些设置或添加了新 WebBrowser，则此 WebBrowser 可以完全控制 Internet Explorer，并添加工具栏、菜单和按钮等功能。

Internet Explorer URL 搜索挂钩

监视对 Internet Explorer URL 搜索挂钩的更改。在浏览器的位置字段中键入地址而此地址中没有协议（如 http:// 或 ftp://）时，会使用 URL 搜索挂钩。如果输入此类地址，浏览器可能会使用 UrlSearchHook 搜索 Internet 以查找所输入的位置。

Internet Explorer URL

监视对 Internet Explorer 预置 URL 的更改。这会防止间谍软件或其他可能有害的程序未经许可便更改浏览器设置。

Internet Explorer 限制

监视 Internet Explorer 限制，计算机管理员利用它可以禁止用户更改 Internet Explorer 中的主页或其他选项。这些选项只有在管理员主动设置时才会出现。

Internet Explorer 安全区域

监视 Internet Explorer 安全区域。Internet Explorer 包含四个预先定义的安全区域：Internet、本地 Intranet、受信任的站点和受限制的站点。每个安全区域都有自己的安全设置，这些安全设置是预先定义的或自定义的。安全区域是某些间谍软件或其他可能有害程序的攻击目标，因为降低安全级别会使这些程序绕过安全警报且检测不到其行为。

Internet Explorer 受信任的站点

监视 Internet Explorer 受信任的站点。受信任的站点列表是您已信任的网站的目录。某些间谍软件或其他可能有害的程序会以此列表为攻击目标，因为它会提供一种方法，以在未经您许可的情况下信任可疑站点。

Internet Explorer 策略

监视 Internet Explorer 策略。这些设置通常由系统管理员更改，但可以被间谍软件所利用。这些更改可以防止设置不同的主页，也可以隐藏“工具”菜单的“Internet 选项”对话框中的选项卡。

使用脚本扫描

脚本可以创建、复制或删除文件。它还可以打开 Windows 注册表。

脚本扫描会自动阻止未知的、有害的脚本在您计算机上运行。

禁用脚本扫描

如果禁用脚本扫描，则不会检测可疑脚本的执行。

禁用脚本扫描：

1 在“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“脚本扫描防护”下，单击“关”。

启用脚本扫描

如果脚本执行导致创建、复制、删除文件或打开 Windows 注册表，则脚本扫描会提醒您。

启用脚本扫描：

1 在“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“脚本扫描防护”下，单击“开”。

使用电子邮件保护

电子邮件保护会检测和阻止包含病毒、特洛伊木马程序、蠕虫、间谍软件、广告软件和其他威胁的入站 (POP3) 和出站 (SMTP) 电子邮件及附件。

禁用电子邮件保护

如果禁用电子邮件保护，则不会检测入站 (POP3) 和出站 (SMTP) 电子邮件及附件中的可能威胁。

禁用电子邮件保护：

1 在“高级菜单”上，单击“配置”。

2 在“配置”窗格中，单击“电子邮件和 IM”。

3 在“电子邮件保护”下，单击“关”。

启用电子邮件保护

电子邮件会检测入站 (POP3) 和出站 (SMTP) 电子邮件消息和附件中的威胁。

启用电子邮件保护：

1 在“高级菜单”上，单击“配置”。

2 在“配置”窗格中，单击“电子邮件和 IM”。

3 在“电子邮件保护”下，单击“开”。

配置电子邮件保护

利用电子邮件保护选项可以扫描入站电子邮件、出站电子邮件和蠕虫。蠕虫会进行复制，从而消耗系统资源，降低性能或停止执行任务。蠕虫可以通过电子邮件发送自身副本。例如，它们可能会试图将电子邮件发给地址簿中的人员。

配置电子邮件保护

利用电子邮件保护选项可以扫描入站电子邮件、出站电子邮件和蠕虫。

配置电子邮件保护：

1. 在“高级菜单”上，单击“配置”。
2. 在“配置”窗格中，单击“电子邮件和 IM”。
3. 在“电子邮件保护”下，单击“高级”。
4. 选中或清除以下复选框：
   - **扫描入站电子邮件**：扫描入站 (POP3) 电子邮件中的可能威胁。
   - **扫描出站电子邮件**：扫描出站 (SMTP) 电子邮件中的可能威胁。
   - **启用 WormStopper**：WormStopper 会拦截电子邮件中的蠕虫。
5. 单击“确定”。

使用即时消息保护

即时消息保护会检测入站即时消息附件中的威胁。

禁用即时消息保护

如果禁用即时消息保护，则不会检测入站即时消息附件中的威胁。

禁用即时消息保护：

1 在“高级菜单”上，单击“配置”。

2 在“配置”窗格中，单击“电子邮件和 IM”。

3 在“即时消息保护”下，单击“关”。

启用即时消息保护

即时消息保护会检测入站即时消息附件中的威胁。

启用即时消息保护：

1 在“高级菜单”上，单击“配置”。

2 在“配置”窗格中，单击“电子邮件和 IM”。

3 在“即时消息保护”下，单击“开”。

第 15 章

手动扫描计算机

可以在硬盘驱动器、软盘以及个别文件和文件夹中搜索病毒和其他威胁。当 VirusScan 发现可疑的文件时，除非此文件是可能有害的程序，否则会尝试清除文件中的病毒。如果 VirusScan 无法清除文件中的病毒，您可以将此文件隔离或删除。

本章内容

手动扫描

您可以随时手动扫描。例如，如果刚安装了 VirusScan，则可以执行扫描，以确保您的计算机没有任何病毒或其他威胁。或者，如果您禁用了实时扫描，则可以执行扫描，以确保您的计算机仍受到安全保护。

使用手动扫描设置扫描

此类型的扫描使用您指定的手动扫描设置。VirusScan 可以扫描内部压缩文件（.zip、.cab 等），但会将压缩文件视作一个文件。此外，如果自上次扫描后删除过 Internet 临时文件，扫描的文件个数可能会发生变化。

使用手动扫描设置扫描：

1 在“基本菜单”上，单击“扫描”。完成扫描后，会出现一个摘要，说明扫描和检测到的项目数、清除的项目数以及上次扫描的时间。

2 单击“完成”。

相关主题

- 配置手动扫描 (第 92 页)

不使用手动扫描设置扫描

此类型的扫描不使用您指定的手动扫描设置。VirusScan 可以扫描内部压缩文件（.zip、.cab 等），但会将压缩文件视作一个文件。此外，如果自上次扫描后删除过 Internet 临时文件，扫描的文件个数可能会发生变化。

不使用手动扫描设置扫描：

1 在“高级菜单”上，单击“主页”。

2 在“主页”窗格中，单击“扫描”。

3 在“扫描位置”下，选中要扫描的文件、文件夹和驱动器旁的复选框。

4 在“选项”下，选中要扫描的文件类型旁的复选框。

5 单击“立即扫描”。完成扫描后，会出现一个摘要，说明扫描和检测到的项目数、清除的项目数以及上次扫描的时间。

6 单击“完成”。

注意：这些选项并不会保存。

在 Windows 资源管理器中扫描

您可以在 Windows 资源管理器中扫描所选文件、文件夹或驱动器中的病毒和其他威胁。

在 Windows 资源管理器中扫描文件：

1. 打开 Windows 资源管理器。
2. 右键单击要扫描的文件、文件夹或驱动器，然后单击“扫描”。所有默认选项即会选中以提供彻底的扫描。

配置手动扫描

执行手动扫描或计划的扫描时，可以指定要扫描的文件类型、扫描位置和运行扫描的时间。

配置要扫描的文件类型

可以配置要扫描的文件类型。

配置要扫描的文件类型：

1 在“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“病毒防护”下，单击“高级”。

4 在“病毒防护”窗格上，单击“手动扫描”。

5 选中或清除以下复选框：

- **使用启发式技术扫描未知病毒**：将文件与已知病毒的签名进行比较，以检测未知病毒的特征。此选项是最彻底的扫描方法，但通常比正常扫描速度慢。
- **扫描 .zip 和其他存档文件**：检测和删除 .zip 和其他存档文件中的病毒。有时，病毒编写者会将病毒植入 .zip 文件中，然后将该 .zip 文件嵌套在另一个 .zip 文件中，以期绕过防病毒扫描程序。
- **扫描间谍软件和可能有害的程序**：检测和删除未经许可可能收集及传输数据的间谍软件、广告软件和其他程序。
- **扫描和删除跟踪 Cookie**：检测和删除未经许可可能收集及传输数据的 Cookie。用户访问网页时，Cookie 会标识用户。
- **扫描 Rootkit 和其他隐匿程序**：检测和删除躲避 Windows 的任何 Rootkit 或其他程序。

6 单击以下任一按钮：

- **所有文件(建议)**：扫描计算机使用的每种文件类型。使用此选项进行最全面的扫描。
- **仅限程序文件和文档**：只扫描程序文件和文档。

7 单击“确定”。

配置要扫描的位置

可以配置对扫描位置进行手动扫描和计划的扫描。

配置扫描位置：

1 在“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“病毒防护”下，单击“高级”。

4 在“病毒防护”窗格上，单击“手动扫描”。

5 在“默认扫描位置”下，选中要扫描的文件、文件夹和驱动器。

要执行可能最全面的扫描，确保选中“重要文件”。

6 单击“确定”。

计划扫描

可以对扫描进行计划，以在指定的时间间隔全面检查计算机中的病毒和其他威胁。

计划扫描：

1 在“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“病毒防护”下，单击“高级”。

4 在“病毒防护”窗格上，单击“计划的扫描”。

5 确保选中“启用计划的扫描”。

6 选中执行扫描的一周的某天旁的复选框。

7 在开始时间列表中单击值来指定开始时间。

8 单击“确定”。

提示：要使用默认计划，请单击“重置”。

第 16 章

管理 VirusScan

您可以删除信任列表中的项目，管理隔离的程序、Cookie 和文件，查看事件和日志，以及向 McAfee 报告可疑活动。

本章内容

管理信任的列表

如果信任 SystemGuard、程序、缓冲区溢出或电子邮件程序，则此项目便会添加到信任列表中，这样不会再对其进行检测。

如果错误信任了某个程序，或希望对此程序进行检测，则必须从此列表将其删除。

管理信任的列表

如果信任 SystemGuard、程序、缓冲区溢出或电子邮件程序，则此项目便会添加到信任列表中，这样不会再对其进行检测。

如果错误信任了某个程序，或希望对此程序进行检测，则必须从此列表将其删除。

删除信任列表中的项目：

1. 在“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“病毒防护”下，单击“高级”。
4. 在“病毒防护”窗格上，单击“可信列表”。
5. 在此列表中，选择信任的 SystemGuard、程序、缓冲区溢出或电子邮件程序，以查看其项目及其信任状态。
6. 在“详细信息”下，查看有关此项目的信息。
7. 在“我想”下面，单击某个操作。
8. 单击“确定”。

管理隔离的程序、Cookie 和文件

可以恢复、删除隔离的程序、Cookie 和文件，也可以将其发送到 McAfee 以供分析。

恢复隔离的程序、Cookie 和文件

如有必要，可以恢复被隔离的程序、Cookie 和文件。

恢复隔离的程序、Cookie 和文件：

1. 在“高级菜单”上，单击“恢复”。
2. 在“恢复”窗格上，单击相应的“程序和 Cookie”或“文件”。
3. 选择要恢复的隔离程序、Cookie 或文件。
4. 有关被隔离病毒的详细信息，请在“详细信息”下单击其检测名称。随即会显示病毒信息库及病毒描述。
5. 在“我想”下面，单击“恢复”。

删除隔离的程序、Cookie 和文件

您可以删除被隔离的程序、Cookie 和文件。

删除隔离的程序、Cookie 和文件：

1. 在“高级菜单”上，单击“恢复”。
2. 在“恢复”窗格上，单击相应的“程序和 Cookie”或“文件”。
3. 选择要恢复的隔离程序、Cookie 或文件。
4. 有关被隔离病毒的详细信息，请在“详细信息”下单击其检测名称。随即会显示病毒信息库及病毒描述。
5. 在“我想”下面，单击“删除”。

将隔离的程序、Cookie 和文件发给 McAfee

可以将隔离的程序、Cookie 和文件发给 McAfee 以供分析。

注意：如果要发送的隔离文件超过最大大小，可以拒绝此文件。不过在大多数情况下，不会出现此种情况。

将隔离程序和文件发给 McAfee：

1. 在“高级菜单”上，单击“恢复”。
2. 在“恢复”窗格上，单击相应的“程序和 Cookie”或“文件”。
3. 选择要发给 McAfee 的隔离的程序、Cookie 或文件。
4. 有关被隔离病毒的详细信息，请在“详细信息”下单击其检测名称。随即会显示病毒信息库及病毒描述。
5. 在“我想”下面，单击“发给 McAfee”。

查看最新事件和日志

最新事件和日志会显示来自所有已安装 McAfee 产品的事件。

在“最新事件”下，可以查看计算机上发生的最近 30 个重要事件。您可以恢复已阻止的程序、重新启用实时扫描以及信任缓冲区溢出。

您还可以查看日志，日志记录了过去 30 天发生的每个事件。

查看事件

在“最新事件”下，可以查看计算机上发生的最近 30 个重要事件。您可以恢复已阻止的程序、重新启用实时扫描以及信任缓冲区溢出。

查看事件：

1 在“高级菜单”上，单击“报告和日志”。

2 在“报告和日志”窗格上，单击“最新事件”。

3 选择要查看的事件。

4 在“详细信息”下，查看有关事件的信息。

5 在“我想”下面，单击某个操作。

查看日志

日志会记录过去 30 天发生的每个事件。

查看日志：

1 在“高级菜单”上，单击“报告和日志”。

2 在“报告和日志”窗格上，单击“最新事件”。

3 在“最新事件”窗格上，单击“查看日志”。

4 选择要查看的日志类型，然后选择日志。

5 在“详细信息”下，查看有关日志的信息。

自动报告匿名信息

您可以将病毒、可能有害的程序和黑客跟踪信息以匿名方式发给 McAfee。此选项仅在安装过程中可用。

不会收集任何个人身份信息。

向 McAfee 报告

您可以将病毒、可能有害的程序和黑客跟踪信息发给 McAfee。此选项仅在安装过程中可用。

自动报告匿名信息：

1 在安装 VirusScan 过程中，接受默认的“提交匿名信息”。

2 单击“下一步”。

了解安全警报

如果实时扫描检测到威胁，则会显示警报。对于大多数病毒、特洛伊木马程序、脚本和蠕虫，实时扫描会自动尝试清除这些文件并提醒您。对于可能有害的程序和 SystemGuard，实时扫描会扫描检测文件或更改并提醒您。对于缓冲区溢出、跟踪 Cookie 和脚本活动，实时扫描会自动阻止此活动并提醒您。

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

然后，您可以选择如何管理检测到的文件、检测到的电子邮件、可疑脚本、可能的蠕虫、可能有害的程序、SystemGuard 或缓冲区溢出。

管理警报

McAfee 使用一组警报来帮助您管理您的安全。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

红色警报

红色警报要求您进行响应。在某些情况下，McAfee 无法确定如何对特定活动进行自动响应。此时，红色警报会介绍相关活动并提供一个或多个选项供您选择。

黄色警报

黄色警报是非关键性通知，通常要求您进行响应。黄色警报会介绍相关活动并提供一个或多个选项供您选择。

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。

配置警报选项

如果您先选择不再显示警报，稍后又改变主意，则可以返回并配置此警报再次显示。有关配置警报选项的信息，请参阅 SecurityCenter 文档。

第 17 章

其他帮助

本章介绍常见问题和故障排除方案。

本章内容

常见问题

本节提供常见问题的答案。

已检测到威胁，我该怎么办？

McAfee 通过警报帮助您管理安全性。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

然后，您可以选择如何管理检测到的文件、检测到的电子邮件、可疑脚本、可能的蠕虫、可能有害的程序、SystemGuard 或缓冲区溢出。

有关管理特定威胁的详细信息，请参阅病毒信息库，网址为：http://cn.mcafee.com/virusInfo/。

相关主题

- 了解安全警报 (第 101 页)

能否将 VirusScan 与 Netscape、Firefox 和 Opera 浏览器一起使用？

可以使用 Netscape、Firefox 和 Opera 作为默认 Internet 浏览器，但必须在计算机上安装 Microsoft® Internet Explorer 6.0 或更高版本。

是否需要连接到 Internet 以执行扫描？

您不必连接到 Internet 即可运行扫描，但为接收 McAfee 更新，一周至少连接到 Internet 一次。

VirusScan 是否扫描电子邮件附件？

如果启用了实时扫描和电子邮件保护，则当电子邮件到达时，即会扫描任何附件。

VirusScan 是否扫描压缩文件？

VirusScan 会扫描 .zip 文件和其他存档文件。

为什么会出现出站电子邮件扫描错误？

在扫描出站电子邮件时，可能会出现以下类型的错误：

- 协议错误。电子邮件服务器拒绝接收电子邮件。
  如果出现协议错误或系统错误，仍会继续处理此会话中的其余电子邮件并将其发送到服务器。
- 连接错误。与电子邮件服务器的连接中断。
  如果发生连接错误，请确保计算机已连接到 Internet，然后重新尝试发送电子邮件程序“已发送”项目列表中的邮件。
- 系统错误。发生了文件处理故障或其他系统错误。
- 加密的 SMTP 连接错误。检测到来自您电子邮件程序的加密 SMTP 连接。
  如果出现加密 SMTP 连接，则应在电子邮件程序中关闭加密 SMTP 连接，以确保能够扫描电子邮件。

如果在发送电子邮件时出现超时，请禁用出站电子邮件扫描，或关闭电子邮件程序中的加密 SMTP 连接。

相关主题

- 配置电子邮件保护 (第 86 页)

故障排除

本节对您可能遇到的一般问题提供帮助。

无法清除或删除病毒

对于某些病毒，必须手动清理计算机。尝试重新启动计算机，然后再次扫描。

如果计算机无法清除或删除病毒，请参阅病毒信息库，网址为：http://cn.mcafee.com/virusInfo/。

如果需要其他帮助，请通过 McAfee 网站咨询 McAfee 客户支持部门。

注意：无法从 CD-ROM、DVD 和有写保护的软盘清除病毒。

在重新启动后，仍有项目无法删除。

在某些情况下，扫描和删除项目后，需要重新启动计算机。

如果重新启动计算机后仍无法删除项目，请将文件提交给 McAfee。

注意：无法从 CD-ROM、DVD 和有写保护的软盘清除病毒。

相关主题

- 管理隔离的程序、Cookie 和文件 (第 97 页)

组件丢失或损坏

在某些情况下，可能无法正确安装 VirusScan：

- 计算机没有足够的磁盘空间或内存。确保计算机符合系统要求才能运行此软件。
- 未正确配置 Internet 浏览器。
- Internet 连接故障。请检查连接，否则，请稍后重新尝试连接。
- 缺少文件或安装失败。

最佳解决方案是先解决这些可能的问题，然后再重新安装 VirusScan。

第 18 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。

本章内容

功能

Personal Firewall 提供全面的入站和出站防火墙保护和自动信任已知的常规应用程序，并帮助拦截间谍软件、特洛伊木马程序和按键记录程序。Firewall 可使您能抵御黑客探测和攻击，监视 Internet 和网络活动，提醒您恶意事件或可疑事件，提供有关 Internet 通讯的详细信息，以及协助防御病毒。

标准和自定义保护级别

使用 Firewall 的默认保护设置防止入侵和可疑活动，或自定义 Firewall 来满足自己的安全需要。

实时建议

动态接收建议，帮助您确定是否应授予程序 Internet 访问权限，或是否应信任网络通信量。

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，或在 Firewall 的“程序权限”窗格中配置特定程序的访问权限。

游戏保护

在玩全屏游戏期间，防止有关入侵企图和可疑活动的警报分散您的注意力，可以配置 Firewall 在计算机游戏完成后再显示警报。

计算机启动保护

在 Windows 打开前，Firewall 会保护您的计算机免受入侵企图和有害程序以及网络通讯的侵扰。

系统服务端口控制

系统服务端口可以为您的计算机提供后门。Firewall 允许您创建和管理某些程序所需的打开的和关闭的系统服务端口。

管理计算机连接

信任和禁止连接到您计算机的远程连接和 IP 地址。

HackerWatch 信息集成

HackerWatch 是一个安全信息中心，它跟踪全局的黑客攻击和入侵模式，以及提供您计算机上有关程序的最新信息。您可以查看全局安全事件和 Internet 端口统计信息。

锁定 Firewall

立即阻止您的计算机和 Internet 之间的所有入站和出站 Internet 通讯。

恢复 Firewall

立即恢复 Firewall 的最初保护设置。如果 Personal Firewall 出现无法更正的有害行为，可以将 Firewall 恢复到其默认设置。

高级特洛伊木马程序检测

将程序连接管理与增强的数据库相结合，以检测并阻止可能有害的应用程序（如特洛伊木马程序）访问 Internet 和传播您的个人数据。

事件记录

指定是否要启用或禁用记录，以及启用后要记录哪些事件类型。事件记录允许查看最近的入站和出站事件。您还可以查看入侵检测事件。

监视 Internet 通讯

查看易于阅读的地图，它可以显示全球范围的恶意攻击和通讯的来源。此外，此地图还会查找始发 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

通过提供对可能 Internet 威胁的入侵防护来保护隐私。McAfee 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 Firewall

安装 Firewall 后，您的计算机便可以抵御入侵和有害网络通讯的损害。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。系统会自动启动“智能建议”和“标准”安全级别。

虽然可以在“Internet 和网络配置”窗格中禁用 Firewall，但您的计算机将无法抵御入侵和有害网络通讯的损害，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 Firewall。

Firewall 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 Firewall，请打开“Internet 和网络配置”窗格。

启动防火墙保护

启用防火墙保护会防止计算机免受入侵和有害网络通讯的干扰，帮助您管理入站和出站 Internet 连接。

启用防火墙保护：

1 在“McAfee SecurityCenter”窗格上，执行以下任一操作：
   - 单击“Internet 和网络”，然后单击“配置”。
   - 单击“高级菜单”，单击“主页”窗格上的“配置”，然后指向“Internet 和网络”。
2 在“Internet 和网络配置”窗格的“Firewall 防护”下，单击“开”。

停止防火墙保护

禁用防火墙保护会使您的计算机易遭入侵和有害网络通讯的损害。不启用防火墙保护，您不能管理入站和出站 Internet 连接。

禁用防火墙保护：

1 在“McAfee SecurityCenter”窗格上，执行以下任一操作：
   - 单击“Internet 和网络”，然后单击“配置”。
   - 单击“高级菜单”，单击“主页”窗格上的“配置”，然后指向“Internet 和网络”。

2　在“Internet 和网络配置”窗格的“Firewall 防护”下，单击“关”。

使用警报

Firewall 使用一组警报来帮助您管理安全性。这些警报可以分为 4 种基本类型。

- 阻止特洛伊木马程序警报
- 红色警报
- 黄色警报
- 绿色警报

警报还包含一些信息，帮助用户确定如何处理警报或获取有关其计算机上运行程序的信息。

关于警报

Firewall 包含四种基本警报类型。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。

阻止特洛伊木马程序警报

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。当 Firewall 在计算机上检测到特洛伊木马程序时，会显示特洛伊木马程序警报，拦截特洛伊木马程序，然后建议扫描其他威胁。此警报会在每个安全级别中出现，但不会在“开放”级别中出现，也不会在禁用“智能建议”时出现。

红色警报

最常见的警报类型是红色警报，通常需要您进行响应。因为 Firewall 在某些情况下无法自动确定对程序活动或网络事件采取的操作，所以警报会先说明相关程序活动或网络事件，接着会提供一个或多个您必须响应的选项。如果启用“智能建议”，则会将程序添加到“程序权限”窗格中。

下面是最常见的警报说明：

- **程序请求 Internet 访问权限**：Firewall 检测到有程序试图访问 Internet。
- **程序已修改**：Firewall 检测到某个程序已进行某种程度的更改，这可能是在线更新的结果。
- **已阻止程序**：Firewall 会阻止程序，因为它列在“程序权限”窗格上。

根据您的设置及程序活动或网络事件，下面是最常见的选项：

- **授予访问权限**：允许计算机上的程序访问 Internet。此规则会添加到“程序权限”页。
- **授予一次访问权限**：允许计算机上的程序临时访问 Internet。例如，安装新程序可能只需访问一次。
- **阻止访问**：禁止程序访问 Internet。
- **授予仅出站访问权限**：只允许 Internet 的出站连接。在设置“严格”和“隐匿”安全级别后，通常会显示此警报。
- **信任此网络**：允许来自网络的入站和出站通讯。此网络会添加到“可信的 IP 地址”区域。
- **此次不信任此网络**：阻止来自网络的入站和出站通讯。

黄色警报

黄色警报是非关键性通知，通知您 Firewall 检测到的网络事件。例如，首次运行 Firewall 或安装了 Firewall 的计算机连接到新网络时，都会显示“检测到新网络”警报。您可以选择信任或不信任此网络。如果信任此网络，Firewall 允许来自此网络上任何其他计算机的通讯，并将此网络添加到“可信的 IP 地址”。

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。在设置“标准”、“严格”、“隐匿”和“锁定”安全级别后，通常会显示绿色警报。绿色警报说明如下：

- **程序已修改**：通知您以前允许访问 Internet 的程序已修改。您可以选择阻止程序，但如果您不响应，此警报会从桌面消失，而程序继续进行访问。
- **已授予程序访问 Internet 的权限**：通知您已授予程序 Internet 访问权限。您可以选择阻止程序，但如果您不响应，此警报会消失，而程序继续访问 Internet。

用户帮助

许多 Firewall 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 Firewall 已在您计算机上检测到的程序的信息。
- **通知 McAfee 有关此程序的信息**：将 Firewall 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，警报可能建议授予某个程序访问权限。

管理信息警报

Firewall 允许在发生某些事件期间显示或隐藏信息警报。

玩游戏时显示警报

默认情况下，Firewall 会禁止在玩全屏游戏时显示信息警报。不过，您可以配置 Firewall，使其在您玩游戏期间检测到入侵企图或可疑活动时，显示信息警报。

在玩游戏期间显示警报：

1 在“常见任务”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”。

4 单击“高级”。

5 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”。

隐藏信息警报

信息警报会在发生不要求立即处理的事件时通知您。

隐藏信息警报：

1 在“常见任务”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”。

4 单击“高级”。

5 在“SecurityCenter 配置”窗格上，单击“信息警报”。

6 在“信息警报”窗格上，执行以下任一操作：

- 选中要隐藏的警报类型。
- 选中“隐藏信息警报”以隐藏所有的信息警报。

7 单击“确定”。

第 19 章

配置 Firewall 保护

Firewall 提供一些方法来管理安全性以及定制要响应安全事件和警报的方法。

首次安装 Firewall 后，保护级别会设置为“标准”安全性。对大多数人而言，此设置符合其所有安全需要。不过，Firewall 还提供了其他级别，范围从高度严格到高度宽松。

Firewall 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 Firewall 安全级别

您可以配置安全级别，以控制在 Firewall 检测到有害的网络通讯以及入站和出站 Internet 连接时，要管理和响应警报的程度。默认情况下，系统将启用“标准”安全级别。

如果设置“标准”安全级别并启用“智能建议”，则可以使用红色警报提供的选项，授予或阻止未知程序或已修改程序的访问权限。检测到已知的程序时，会显示绿色信息警报，并会自动授予访问权限。授予访问权限允许程序创建出站连接和侦听未经请求的入站连接。

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

Firewall 采用六种安全级别。从最严格的级别到最宽松的级别依次为：

- **锁定**：阻止所有 Internet 连接。
- **隐匿**：阻止所有入站 Internet 连接。
- **严格**：警报要求您对每个入站和出站 Internet 连接请求进行响应。
- **标准**：警报会在未知程序或新程序要求访问 Internet 时通知您。
- **信任**：将访问权限授予所有入站和出站 Internet 连接，并自动将其添加到“程序权限”窗格。
- **开放**：将访问权限授予所有入站和出站 Internet 连接。

Firewall 还允许从“恢复防火墙保护默认值”窗格中将安全级别重置为“标准”。

将安全级别设置为“锁定”

将防火墙的安全级别设置为“锁定”会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。此安全级别与取消 Internet 连接有相同的效果。可以使用此设置阻止在“系统服务”窗格上设置为打开的端口。在锁定期间，警报可能会继续提示您阻止程序。

将防火墙的安全级别设置为“锁定”：

1. 在“Internet 和网络配置”窗格上，单击“高级”。
2. 在“安全级别”窗格上，移动滑块，直至“锁定”显示为当前级别。
3. 单击“确定”。

将安全级别设置为“隐匿”

将防火墙的安全级别设置为“隐匿”会阻止所有入站网络连接（打开的端口除外）。此设置会完全隐藏您计算机在 Internet 上的踪迹。如果将安全级别设置为“隐匿”，则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醒您。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。

将防火墙的安全级别设置为“隐匿”：

1. 在“Internet 和网络配置”窗格上，单击“高级”。
2. 在“安全级别”窗格上，移动滑块，直至“隐匿”显示为当前级别。
3. 单击“确定”。

将安全级别设置为“严格”

如果将安全级别设置为“严格”，则 Firewall 会在新程序尝试进行出站 Internet 连接或接收入站连接请求时通知您。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。如果将安全级别设置为“严格”，程序只请求它当时需要的访问类型，如仅出站访问，您可以授予或阻止此访问权限。稍后，如果此程序既需要入站连接，又需要出站连接，则可以在“程序权限”窗格中授予此程序完全访问权限。

将防火墙的安全级别设置为“严格”：

1. 在“Internet 和网络配置”窗格上，单击“高级”。
2. 在“安全级别”窗格上，移动滑块，直至“严格”显示为当前级别。
3. 单击“确定”。

将安全级别设置为“标准”

“标准”级别是默认的和建议的安全级别。

如果将防火墙的安全级别设置为“标准”，则 Firewall 会监视入站和出站连接，并在新程序试图访问 Internet 时提醒您。阻止的程序和添加的程序都会显示在“程序权限”窗格中。

将防火墙的安全级别设置为“标准”：

1. 在“Internet 和网络配置”窗格上，单击“高级”。
2. 在“安全级别”窗格上，移动滑块，直至“标准”显示为当前级别。
3. 单击“确定”。

将安全级别设置为“信任”

将防火墙的安全级别设置为“信任”会允许所有入站和出站连接。在“信任”安全级别中，防火墙会自动为所有程序授予访问权限，并将其添加到“程序权限”窗格上允许的程序列表中。

将防火墙的安全级别设置为“信任”：

1. 在“Internet 和网络配置”窗格上，单击“高级”。
2. 在“安全级别”窗格上，移动滑块，直至“信任”显示为当前级别。
3. 单击“确定”。

配置警报的“智能建议”

您可以配置 Firewall 在警报中包含、排除或显示与尝试访问 Internet 的程序有关的建议。

启用“智能建议”有助于您确定如何处理警报。如果启用“智能建议”（且安全级别为“标准”），则 Firewall 自动授予或阻止已知程序的访问权限，并在检测到未知的和可能有危险的程序时，发出警报并建议采取操作。

如果禁用了“智能建议”，则 Firewall 既不会自动授予或阻止 Internet 访问权限，也不会建议采取操作。

如果将 Firewall 配置为只显示“智能建议”，警报会提示您授予或阻止访问权限，而不会建议采取操作。

启用“智能建议”

启用“智能建议”有助于确定如何处理警报。启用“智能建议”后，Firewall 会自动授予程序权限或阻止程序，并提醒您有关未能识别的和可能有危险的程序。

启用“智能建议”：

1. 在“Internet 和网络配置”窗格上，单击“高级”。
2. 在“安全级别”窗格的“智能建议”下，选择“启用智能建议”。
3. 单击“确定”。

禁用“智能建议”

如果禁用“智能建议”，则警报不会协助您处理警报和管理程序的访问权限。如果禁用“智能建议”，防火墙会继续授予程序权限和阻止程序，并提醒您有关未能识别的和可能有危险的程序。此外，如果它检测到新程序可疑或已知是可能的威胁，则 Firewall 会自动阻止此程序访问 Internet。

禁用“智能建议”：

1. 在“Internet 和网络配置”窗格上，单击“高级”。
2. 在“安全级别”窗格的“智能建议”下，选择“禁用智能建议”。
3. 单击“确定”。

仅显示“智能建议”

显示“智能建议”有助于确定如何处理与未识别的和可能有危险的程序有关的警报。如果将“智能建议”设置为“仅显示”，则会显示有关处理警报的信息，但与“启用智能建议”选项不同，它并不会自动应用显示的建议，并且不会自动授予或阻止程序的访问权限。警报会改为提供建议，以帮助您确定授予或阻止程序的访问权限。

仅显示“智能建议”：

1. 在“Internet 和网络配置”窗格上，单击“高级”。
2. 在“安全级别”窗格的“智能建议”下，选择“仅显示”。
3. 单击“确定”。

优化 Firewall 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® 启动前，尝试连接到 Internet。此外，有经验的计算机用户也可以 ping 您的计算机，以确定它是否连接到网络上。Firewall 支持启用引导时保护和阻止 ICMP ping 请求，从而抵御这两种类型的入侵。第一个设置会阻止程序在 Windows 启动时访问 Internet，而第二个设置会阻止 ping 请求，因为它会帮助其他用户检测您的计算机是否在网络上。

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

Firewall 可以在 Windows 启动时保护计算机。引导时保护会阻止以前尚未授予 Internet 访问权限，但需要访问 Internet 的所有新程序。启动 Firewall 后，它会针对在启动过程中已请求 Internet 访问权限的程序显示相关警报，您可以授予或阻止此访问权限。要使用此选项，不得将安全级别设置为“开放”或“锁定”。

启动过程中保护计算机：

1. 在“Internet 和网络配置”窗格上，单击“高级”。
2. 在“安全级别”窗格的“安全设置”下，选择“启用引导时保护”。
3. 单击“确定”。

注意：启用引导时保护后，不记录已阻止的连接和入侵。

配置 ping 请求设置

计算机用户可以使用 ping 工具（它会发送和接收 ICMP 回送请求消息）来确定指定的计算机是否已连接到网络上。您可以将 Firewall 配置为阻止或允许计算机用户 ping 您的计算机。

配置 ICMP ping 请求设置：

1. 在“Internet 和网络配置”窗格上，单击“高级”。
2. 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。

3 单击“确定”。

配置入侵检测

入侵检测 (IDS) 会监视入站数据包中是否存在可疑的数据传输或传输方法。IDS 分析通讯和数据包中是否有攻击者使用的特定通讯模式。例如，如果 Firewall 检测到 ICMP 数据包，它会将 ICMP 通讯与已知攻击模式进行比较，分析这些数据包是否存在可疑的通讯模式。Firewall 将数据包与签名数据库进行比较，如果来自恶意计算机的数据包可疑或有害，则会自动丢弃这些数据包，然后有选择地记录此事件。

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。

配置入侵检测：

1 在“Internet 和网络配置”窗格上，单击“高级”。

2 在“防火墙”窗格上，单击“入侵检测”。

3 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。

4 单击“确定”。

配置 Firewall 的“保护状态”设置

SecurityCenter 会跟踪整体计算机“保护状态”所含的问题。不过，您可以配置 Firewall 忽略计算机上可能影响“保护状态”的特定问题。您可以配置 SecurityCenter 在 Firewall 设置为“开放”安全级别时、Firewall 服务没有运行时以及在计算机上没有安装仅出站访问防火墙时，忽略这些问题。

配置 Firewall 的“保护状态”设置：

1. 在“常见任务”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”。
4. 单击“高级”。
5. 在“常见任务”窗格上，单击“高级菜单”。
6. 单击“配置”。
7. 在“SecurityCenter 配置”窗格上，单击“保护状态”。
8. 单击“高级”。
9. 在“忽略的问题”窗格中，选中以下一个或多个选项：
   - **防火墙已设置为“开放”安全级别。**
   - **防火墙服务没有运行。**
   - **您的计算机未安装出站防火墙。**
10. 单击“确定”。

锁定和恢复 Firewall

锁定功能在处理与计算机有关的紧急情况时很有用，该功能适用于需要阻止所有通讯以隔离并解决其计算机上问题的用户，或适用于那些不确定、但必须决定如何管理程序的 Internet 访问权限的用户。

立即锁定 Firewall

立即锁定 Firewall 会阻止您的计算机和 Internet 之间的所有入站和出站网络通讯。它会阻止所有远程连接访问您的计算机，并阻止您计算机上的所有程序访问 Internet。

立即锁定 Firewall 并阻止所有网络通讯：

1. 在启用了“基本菜单”或“高级菜单”的“主页”窗格或“常见任务”窗格上，单击“锁定防火墙”。
2. 在“锁定 Firewall”窗格上，单击“锁定”。
3. 在对话框上，单击“是”以确认您要立即阻止所有入站和出站通讯。

立即解锁 Firewall

立即锁定 Firewall 会阻止您的计算机和 Internet 之间的所有入站和出站网络通讯。它会阻止所有远程连接访问您的计算机，并阻止您计算机上的所有程序访问 Internet。在锁定 Firewall 后，可以对其进行解锁以允许网络通讯。

立即解锁 Firewall 并允许所有网络通讯：

1. 在启用了“基本菜单”或“高级菜单”的“主页”窗格或“常见任务”窗格上，单击“锁定防火墙”。
2. 在“已启用锁定”窗格上，单击“解锁”。
3. 在对话框上，单击“是”以确认您要解锁 Firewall 并允许网络通讯。

恢复 Firewall 设置

您可以快速将 Firewall 恢复到其最初的保护设置。这会将安全级别设置为“标准”，启用“智能建议”，重置信任的 IP 地址和禁止的 IP 地址，以及从“程序权限”窗格中删除全部程序。

将 Firewall 恢复到其最初的设置：

1. 在启用了“基本菜单”或“高级菜单”的“主页”窗格或“常见任务”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. 在“恢复防火墙保护默认值”对话框上，单击“是”以确认要将防火墙配置恢复到其最初的默认设置。

将安全级别设置为“开放”

将防火墙的安全级别设置为“开放”会允许防火墙为所有入站和出站网络连接授予访问权限。要为以前阻止的程序授予访问权限，请使用“程序权限”窗格。

将防火墙的安全级别设置为“开放”：

1. 在“Internet 和网络配置”窗格上，单击“高级”。
2. 在“安全级别”窗格上，移动滑块，直至“开放”显示为当前级别。
3. 单击“确定”。

注意：将防火墙安全级别设置为“开放”后，系统将继续阻止以前被阻止的程序。为防止出现此情况，可以将程序的规则改为“完全访问”。

第 20 章

管理程序和权限

Firewall 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。Firewall 允许授予程序完全访问权限或仅出站访问权限。您还可以阻止程序的访问权限。

本章内容

授予程序 Internet 访问权限

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

Firewall 允许使用“程序权限”页：

- 授予程序访问权限
- 授予程序仅出站访问权限
- 阻止程序的访问权限

您还可以在“出站事件”和“最新事件”日志中授予完全访问权限和仅出站访问权限。

授予程序完全访问权限

计算机上的许多程序都需要 Internet 的入站和出站访问权限。Personal Firewall 包括一个自动允许完全访问的程序列表，但您可以修改这些权限。

授予程序完全 Internet 访问权限：

1. 在“Internet 和网络配置”窗格上，单击“高级”。
2. 在“防火墙”窗格上，单击“程序权限”。
3. 在“程序权限”下，选择权限为“已阻止”或“仅出站访问”的程序。
4. 在“操作”下，单击“授予完全访问权限”。
5. 单击“确定”。

授予新程序完全访问权限

计算机上的许多程序都需要 Internet 的入站和出站访问权限。Firewall 包含了一个自动允许完全访问的程序列表，不过可以添加新程序并更改其权限。

授予新程序完全 Internet 访问权限：

1. 在“Internet 和网络配置”窗格上，单击“高级”。
2. 在“防火墙”窗格上，单击“程序权限”。
3. 在“程序权限”下，单击“添加允许的程序”。
4. 在“添加程序”对话框上，浏览并选择要添加的程序。
5. 单击“打开”。
6. 单击“确定”。

   新添加的程序随即会显示在“程序权限”下。

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“授予仅出站访问权限”或“阻止访问”。

从“最新事件”日志授予完全访问权限

计算机上的许多程序都需要 Internet 的入站和出站访问权限。您可以从“最新事件”日志中选择程序，然后授予它完全 Internet 访问权限。

从“最新事件”日志中授予程序完全访问权限：

1. 在“常见任务”窗格上，单击“报告和日志”。
2. 在“最新事件”下，选择事件说明，然后单击“授予完全访问权限”。
3. 在“程序权限”对话框上，单击“是”以确认您要授予程序完全访问权限。

相关主题

- 查看出站事件 (第 155 页)

从“出站事件”日志授予完全访问权限

计算机上的许多程序都需要 Internet 的入站和出站访问权限。可以从“出站事件”日志选择程序，然后授予它完全 Internet 访问权限。

从“出站事件”日志授予程序完全 Internet 访问权限：

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. 选择“Internet 和网络”，然后单击“出站事件”。
4. 在“出站事件”窗格中，选择源 IP 地址，然后单击“授予访问权限”。
5. 在“程序权限”对话框上，单击“是”以确认您要授予程序完全的 Internet 访问权限。

相关主题

- 查看出站事件 (第 155 页)

授予程序仅出站访问权限

计算机上的许多程序仅需要 Internet 的出站访问权限。Firewall 允许授予程序对 Internet 的仅出站访问权限。

授予程序仅出站访问权限

计算机上的许多程序都需要 Internet 的入站和出站访问权限。Personal Firewall 包括一个自动允许完全访问的程序列表，但您可以修改这些权限。

授予程序仅出站访问权限：

1 在“Internet 和网络配置”窗格上，单击“高级”。

2 在“防火墙”窗格上，单击“程序权限”。

3 在“程序权限”下，选择权限为“已阻止”或“完全访问”的程序。

4 在“操作”下，单击“授予仅出站访问权限”。

5 单击“确定”。

从“最新事件”日志授予仅出站访问权限

计算机上的许多程序都需要 Internet 的入站和出站访问权限。您可以从“最新事件”日志中选择程序，然后授予它仅出站 Internet 访问权限。

从“最新事件”日志中授予程序仅出站访问权限：

1 在“常见任务”窗格上，单击“报告和日志”。

2 在“最新事件”下，选择事件说明，然后单击“授予仅出站访问权限”。

3 在“程序权限”对话框上，单击“是”以确认您要授予程序仅出站访问权限。

相关主题

- 查看出站事件 (第 155 页)

从“出站事件”日志授予仅出站访问权限

计算机上的许多程序都需要 Internet 的入站和出站访问权限。可以从“出站事件”日志选择程序，然后授予它仅出站 Internet 访问权限。

从“出站事件”日志授予程序仅出站访问权限：

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. 选择“Internet 和网络”，然后单击“出站事件”。
4. 在“出站事件”窗格中，选择源 IP 地址，然后单击“授予仅出站访问权限”。
5. 在“程序权限”对话框上，单击“是”以确认您要授予程序仅出站访问权限。

相关主题

- 查看出站事件 (第 155 页)

阻止程序的 Internet 访问权限

Firewall 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。

阻止程序的访问权限

计算机上的许多程序都需要 Internet 的入站和出站访问权限。Personal Firewall 包括一个自动允许完全访问的程序列表，但您可以阻止这些权限。

阻止程序访问 Internet：

1. 在“Internet 和网络配置”窗格上，单击“高级”。
2. 在“防火墙”窗格上，单击“程序权限”。
3. 在“程序权限”下，选择权限为“完全访问”或“仅出站访问”的程序。
4. 在“操作”下，单击“阻止访问”。
5. 单击“确定”。

阻止新程序的访问权限

计算机上的许多程序都需要 Internet 的入站和出站访问权限。Personal Firewall 包含一个自动允许完全访问的程序列表，不过可以添加新程序，然后阻止其访问 Internet。

阻止新程序访问 Internet：

1. 在“Internet 和网络配置”窗格上，单击“高级”。
2. 在“防火墙”窗格下，单击“程序权限”。
3. 在“程序权限”下，单击“添加阻止的程序”。
4. 在“添加程序”对话框上，浏览并选择要添加的程序。
5. 单击“打开”。
6. 单击“确定”。

   新添加的程序随即会显示在“程序权限”下。

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“授予仅出站访问权限”或“授予完全访问权限”。

从“最新事件”日志阻止访问权限

计算机上的许多程序都需要 Internet 的入站和出站访问权限。不过，您还可以从“最新事件”日志中选择阻止程序访问 Internet。

从“最新事件”日志中阻止程序访问：

1 在“常见任务”窗格上，单击“报告和日志”。

2 在“最新事件”下，选择事件说明，然后单击“阻止访问”。

3 在“程序权限”对话框上，单击“是”以确认您要阻止此程序。

相关主题

- 查看出站事件 (第 155 页)

删除程序的访问权限

删除程序的程序权限之前，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

计算机上的许多程序都需要 Internet 的入站和出站访问权限。Firewall 包含一个自动允许完全访问的程序列表，不过可以删除已自动和手动添加的程序。

删除新程序的程序权限：

1. 在“Internet 和网络配置”窗格上，单击“高级”。
2. 在“防火墙”窗格上，单击“程序权限”。
3. 在“程序权限”下，选择程序。
4. 在“操作”下，单击“删除程序权限”。
5. 单击“确定”。

   此程序随即会从“程序权限”窗格中删除。

注意：Firewall 会禁止通过使操作变灰或禁用操作来修改某些程序。

了解程序

如果您不确定要应用的程序权限，可以在 McAfee 的 HackerWatch 网站上获取有关程序的信息，以帮助您进行决定。

获取程序信息

计算机上的许多程序都需要 Internet 的入站和出站访问权限。Personal Firewall 包含一个自动允许完全访问的程序列表，不过可以修改这些权限。

Firewall 可以帮助您决定是授予还是阻止程序的 Internet 访问权限。确保已连接到 Internet，以便浏览器可以成功连接到 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。

获取程序信息：

1. 在“Internet 和网络配置”窗格上，单击“高级”。
2. 在“防火墙”窗格上，单击“程序权限”。
3. 在“程序权限”下，选择程序。
4. 在“操作”下，单击“了解更多”。

从“出站事件”日志获取程序信息

Personal Firewall 允许您获取“出站事件”日志中显示的程序的有关信息。

在获取有关程序的信息之前，确保您可以连接到 Internet 和 Internet 浏览器。

从“出站事件”日志获取程序信息：

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. 选择“Internet 和网络”，然后单击“出站事件”。
4. 在“出站事件”窗格上，选择源 IP 地址，然后单击“了解更多”。

   您可以在 HackerWatch 网站上查看有关程序的信息。HackerWatch 提供有关程序、Internet 访问要求和安全威胁的最新信息。

相关主题

- 查看出站事件 (第 155 页)

第 21 章

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，Firewall 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。

以下列表显示了公共服务的标准端口。

- 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
- 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

本章内容

配置系统服务端口

要允许远程访问您计算机上的服务，必须指定要打开的服务和关联的端口。只选择您确信必须打开的服务和端口。需要打开端口的情况并不多见。

允许访问现有的系统服务端口

在“系统服务”窗格中，可以打开或关闭现有的端口，以允许或拒绝对您计算机上的服务进行远程访问。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。

访问系统服务端口：

1 在“Internet 和网络配置”窗格上，单击“高级”。

2 在“防火墙”窗格上，单击“系统服务”。

3 在“打开系统服务端口”下，选择要打开端口的系统服务。

4 单击“确定”。

阻止访问现有的系统服务端口

在“系统服务”窗格中，可以打开或关闭现有的端口，以允许或拒绝对您计算机上的服务进行远程访问。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。

阻止访问系统服务端口：

1 在“Internet 和网络配置”窗格上，单击“高级”。

2 在“防火墙”窗格下，单击“系统服务”。

3 在“打开系统服务端口”下，清除系统服务以关闭端口。

4 单击“确定”。

配置新系统服务端口

在“系统服务”窗格中，可以添加新系统服务端口，然后可以打开或关闭此端口，以允许或拒绝对您计算机上的网络服务的远程访问。打开的系统服务端口可以使计算机易遭 Internet 安全威胁的攻击，因此只有在必要时才打开端口。

创建和配置新系统服务端口：

1 在“Internet 和网络配置”窗格上，单击“高级”。

2 在“防火墙”窗格上，单击“系统服务”。

3 单击“添加”。

4 在“添加端口配置”下，指定以下各项：

- 程序名称

- 入站 TCP/IP 端口
- 出站 TCP/IP 端口
- 入站 UDP 端口
- 出站 UDP 端口

5 （可选）描述新配置。

6 单击“确定”。

新配置的系统服务端口随即会显示在“打开系统服务端口”下。

修改系统服务端口

打开的和关闭的端口会允许和拒绝访问您计算机上的网络服务。在“系统服务”窗格中，可以修改现有端口的入站和出站信息。如果输入的端口信息不正确，则系统服务失败。

修改系统服务端口：

1 在“Internet 和网络配置”窗格上，单击“高级”。

2 在“防火墙”窗格上，单击“系统服务”。

3 选择系统服务，然后单击“编辑”。

4 在“添加端口配置”下，指定以下各项：

- 程序名称
- 入站 TCP/IP 端口
- 出站 TCP/IP 端口
- 入站 UDP 端口
- 出站 UDP 端口

5 （可选）描述修改的配置。

6 单击“确定”。

已修改的配置系统服务端口随即会显示在“打开系统服务”下。

删除系统服务端口

打开的或关闭的端口会允许或拒绝访问您计算机上的网络服务。在“系统服务”窗格上，可以删除现有端口和关联的系统服务。在“系统服务”窗格中删除端口和系统服务后，远程计算机将无法访问您计算机上的网络服务。

删除系统服务端口：

1. 在“Internet 和网络配置”窗格上，单击“高级”。
2. 在“防火墙”窗格上，单击“系统服务”。
3. 选择系统服务，然后单击“删除”。
4. 在“系统服务”对话框上，单击“是”以确认您要删除系统服务。

   系统服务端口便不会再显示在“系统服务”窗格中。

第 22 章

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 Firewall 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。

允许连接时，确保您信任的计算机是安全的。如果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。Firewall 并不记录来自“可信的 IP 地址”列表中的 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 Firewall 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 连接会构成特定威胁时，才应禁止此 IP 地址。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。根据您的安全设置，Firewall 可以在检测到来自禁止计算机的事件时提醒您。

本章内容

信任计算机连接

您可以在“信任的 IP 和禁止的 IP”窗格的“可信的 IP 地址”下，添加、编辑和删除信任的 IP 地址。

在“信任的 IP 和禁止的 IP”窗格上的“可信的 IP 地址”列表中，可以允许来自特定计算机的所有通讯到达您的计算机。Firewall 不会记录来自“可信的 IP 地址”列表中显示的 IP 地址的通讯，也不为其生成事件警报。

Firewall 会信任在此列表中选中的任何 IP 地址，并始终允许信任 IP 地址通过任何端口发来的通讯流经防火墙。Firewall 不会记录来自信任 IP 地址的任何事件。Firewall 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。

允许连接时，确保您信任的计算机是安全的。如果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。

添加信任的计算机连接

您可以使用 Firewall 添加信任的计算机连接及其关联的 IP 地址。

在“信任的 IP 和禁止的 IP”窗格上的“可信的 IP 地址”列表中，可以允许来自特定计算机的所有通讯到达您的计算机。Firewall 不会记录来自“可信的 IP 地址”列表中显示的 IP 地址的通讯，也不为其生成事件警报。

与信任 IP 地址相关联的计算机可以始终连接到您的计算机。在添加、编辑或删除信任的 IP 地址之前，确保此地址是可以与之安全通信的地址，否则便将其删除。

添加信任的计算机连接：

1. 在“Internet 和网络配置”窗格上，单击“高级”。
2. 在“防火墙”窗格上，单击“信任的 IP 和禁止的 IP”。
3. 在“信任的 IP 和禁止的 IP”窗格上，选择“可信的 IP 地址”。
4. 单击“添加”。
5. 在“添加可信的 IP 地址规则”下，执行以下任一操作：
   - 选择“单个 IP 地址”，然后输入 IP 地址。
   - 选择“IP 地址范围”，然后在“自 IP 地址”和“至 IP 地址”中，输入开始 IP 地址和结束 IP 地址。

6　（可选）选中“规则过期时间”，然后输入实施此规则的天数。

7　（可选）键入规则的说明。

8　单击“确定”。

9　在“添加可信的 IP 地址规则”对话框中，单击“是”以确认您要添加信任的计算机连接。

新添加的 IP 地址随即会显示在“可信的 IP 地址”下。

从“入站事件”日志添加信任的计算机

您可以从“入站事件”日志添加信任的计算机连接及其关联的 IP 地址。

与信任 IP 地址相关联的计算机可以始终连接到您的计算机。在添加、编辑或删除信任的 IP 地址之前，确保此地址是可以与之安全通信的地址，否则便将其删除。

从“入站事件”日志添加信任的计算机连接：

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“信任此地址”。

5　在“添加可信的 IP 地址规则”对话框中，单击“是”以确认您要信任此 IP 地址。

新添加的 IP 地址随即会显示在“可信的 IP 地址”下。

相关主题

- 事件记录 (第 154 页)

编辑信任的计算机连接

您可以使用 Firewall 编辑信任的计算机连接及其关联的 IP 地址。

与信任 IP 地址相关联的计算机可以始终连接到您的计算机。在添加、编辑或删除信任的 IP 地址之前，确保此地址是可以与之安全通信的地址，否则便将其删除。

编辑信任的计算机连接：

1. 在“Internet 和网络配置”窗格上，单击“高级”。
2. 在“防火墙”窗格上，单击“信任的 IP 和禁止的 IP”。
3. 在“信任的 IP 和禁止的 IP”窗格上，选择“可信的 IP 地址”。
4. 选择 IP 地址，然后单击“编辑”。
5. 在“添加可信的 IP 地址规则”下，执行以下任一操作：
   - 选择“单个 IP 地址”，然后输入 IP 地址。
   - 选择“IP 地址范围”，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。
6. （可选）选中“规则过期时间”，然后输入实施此规则的天数。
7. （可选）键入规则的说明。
8. 单击“确定”。

   已修改的 IP 地址随即会显示在“可信的 IP 地址”下。

删除信任的计算机连接

您可以使用 Firewall 删除信任的计算机连接及其关联的 IP 地址。

与信任 IP 地址相关联的计算机可以始终连接到您的计算机。在添加、编辑或删除信任的 IP 地址之前，确保此地址是可以与之安全通信的地址，否则便将其删除。

删除信任的计算机连接：

1. 在“Internet 和网络配置”窗格上，单击“高级”。
2. 在“防火墙”窗格上，单击“信任的 IP 和禁止的 IP”。
3. 在“信任的 IP 和禁止的 IP”窗格上，选择“可信的 IP 地址”。
4. 选择 IP 地址，然后单击“删除”。
5. 在“信任的 IP 和禁止的 IP”对话框中，单击“是”，以确认您要删除“可信的 IP 地址”下的信任 IP 地址。

禁止计算机连接

您可以在“信任的 IP 和禁止的 IP”窗格的“禁止的 IP 地址”下，添加、编辑和删除信任的 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 Firewall 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 连接会构成特定威胁时，才应禁止此 IP 地址。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。根据您的安全设置，Firewall 可以在检测到来自禁止计算机的事件时提醒您。

添加禁止的计算机连接

您可以使用 Firewall 添加禁止的计算机连接及其关联的 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 Firewall 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 连接会构成特定威胁时，才应禁止此 IP 地址。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。根据您的安全设置，Firewall 可以在检测到来自禁止计算机的事件时提醒您。

添加禁止的计算机连接：

1. 在“Internet 和网络配置”窗格上，单击“高级”。
2. 在“防火墙”窗格上，单击“信任的 IP 和禁止的 IP”。
3. 在“信任的 IP 和禁止的 IP”窗格上，选择“禁止的 IP 地址”。
4. 单击“添加”。
5. 在“添加禁止的 IP 地址规则”下，执行以下任一操作：
   - 选择“单个 IP 地址”，然后输入 IP 地址。
   - 选择“IP 地址范围”，然后在“自 IP 地址”和“至 IP 地址”字段中，输入开始 IP 地址和结束 IP 地址。

6 （可选）选中“规则过期时间”，然后输入实施此规则的天数。

7 （可选）键入规则的说明。

8 单击“确定”。

9 在“添加禁止的 IP 地址规则”对话框上，单击“是”以确认您要添加禁止的计算机连接。

新添加的 IP 地址随即会显示在“禁止的 IP 地址”下。

编辑禁止的计算机连接

您可以使用 Firewall 编辑禁止的计算机连接及其关联的 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 Firewall 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 连接会构成特定威胁时，才应禁止此 IP 地址。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。根据您的安全设置，Firewall 可以在检测到来自禁止计算机的事件时提醒您。

编辑禁止的计算机连接：

1 在“Internet 和网络配置”窗格上，单击“高级”。

2 在“防火墙”窗格上，单击“信任的 IP 和禁止的 IP”。

3 在“信任的 IP 和禁止的 IP”窗格上，选择“禁止的 IP 地址”。

4 选择 IP 地址，然后单击“编辑”。

5 在“添加可信的 IP 地址规则”下，执行以下任一操作：

- 选择“单个 IP 地址”，然后键入 IP 地址。
- 选择“IP 地址范围”，然后在“自 IP 地址”和“至 IP 地址”字段中键入开始 IP 地址和结束 IP 地址。

6 （可选）选中“规则过期时间”，然后键入实施此规则的天数。

7 （可选）键入规则的说明。

单击“确定”。修改的 IP 地址随即会显示在“禁止的 IP 地址”下。

删除禁止的计算机连接

您可以使用 Firewall 删除禁止的计算机连接及其关联的 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 Firewall 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 连接会构成特定威胁时，才应禁止此 IP 地址。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。根据您的安全设置，Firewall 可以在检测到来自禁止计算机的事件时提醒您。

编辑禁止的计算机连接：

1. 在“Internet 和网络配置”窗格上，单击“高级”。
2. 在“防火墙”窗格上，单击“信任的 IP 和禁止的 IP”。
3. 在“信任的 IP 和禁止的 IP”窗格上，选择“禁止的 IP 地址”。
4. 选择 IP 地址，然后单击“删除”。
5. 在“信任的 IP 和禁止的 IP”对话框上，单击“是”以确认您要删除“禁止的 IP 地址”中的 IP 地址。

从“入站事件”日志禁止计算机

您可以从“入站事件”日志禁止计算机连接及其关联的 IP 地址。

“入站事件”日志中显示的 IP 地址都会被禁止。因此，除非计算机使用蓄意打开的端口，或除非计算机包含已授予 Internet 访问权限的程序，否则禁用地址不会增加额外的安全保护。

仅当一个或多个端口被蓄意打开，而且有理由相信必须阻止某个地址访问打开的端口时，才应将此 IP 地址添加到“禁止的 IP 地址”列表中。

“入站事件”页列出所有 Internet 入站通讯的 IP 地址，可以使用此页禁止可疑或有害 Internet 活动的源 IP 地址。

从“入站事件”日志禁止信任的计算机连接：

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”窗格中，选择源 IP 地址，然后单击“禁止此地址”。
5. 在“添加禁止的 IP 地址规则”对话框上，单击“是”以确认您要禁止此 IP 地址。

   新添加的 IP 地址随即会显示在“禁止的 IP 地址”下。

相关主题

- 事件记录 (第 154 页)

从“入侵检测事件”日志禁止计算机

您可以从“入侵检测事件”日志禁止计算机连接及其关联的 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 Firewall 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 连接会构成特定威胁时，才应禁止此 IP 地址。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。根据您的安全设置，Firewall 可以在检测到来自禁止计算机的事件时提醒您。

从“入侵检测事件”日志禁用计算机连接：

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”。
4. 在“入侵检测事件”窗格中，选择源 IP 地址，然后单击“禁止此地址”。
5. 在“添加禁止的 IP 地址规则”对话框上，单击“是”以确认您要禁止此 IP 地址。

   新添加的 IP 地址随即会显示在“禁止的 IP 地址”下。

相关主题

- 事件记录 (第 154 页)

第 23 章

记录、监视和分析

Firewall 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

Firewall 允许指定是否要启用或禁用记录，以及启用后要记录哪些事件类型。事件记录允许查看最近的入站和出站事件。您还可以查看入侵检测事件。

配置事件日志设置

要跟踪防火墙事件和活动，您可以指定和配置要查看事件的类型。

配置事件记录：

1 在“Internet 和网络配置”窗格上，单击“高级”。

2 在“防火墙”窗格上，单击“事件日志设置”。

3 在“事件日志设置”窗格上，执行以下任一操作：

- 选择“记录该事件”以启用事件记录。
- 选择“不记录该事件”以禁用事件记录。

4 在“事件日志设置”下，指定要记录的事件类型。事件类型包括：

- ICMP Ping
- 禁止的 IP 地址中的通讯
- 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。“最新事件”窗格只显示已明确阻止访问 Internet 的程序的活动。

查看 Firewall 的最新事件：

- 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，则可以查看和排序入站事件。

“入站事件”日志包括以下记录类别：

- 日期和时间
- 源 IP 地址
- 主机名
- 信息和事件类型

查看防火墙的入站事件：

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。

相关主题

- 从“入站事件”日志添加信任的计算机 (第 145 页)
- 从“入站事件”日志禁止计算机 (第 150 页)
- 从“入站事件”日志跟踪计算机 (第 159 页)

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。

查看防火墙的出站事件：

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. 选择“Internet 和网络”，然后单击“出站事件”。

注意：您可以从“出站事件”日志授予程序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。

相关主题

- 从“出站事件”日志授予完全访问权限 (第 132 页)
- 从“出站事件”日志授予仅出站访问权限 (第 134 页)
- 从“出站事件”日志获取程序信息 (第 138 页)

查看入侵检测事件

如果已启用记录，则可以查看入站事件。入侵检测事件显示事件的日期和时间、源 IP 以及主机名。日志还说明了事件类型。

查看入侵检测事件：

1 在“常见任务”窗格下，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。

相关主题

- 从“入侵检测事件”日志禁止计算机 (第 151 页)
- 从“入侵检测事件”日志跟踪计算机 (第 159 页)

使用统计信息

Firewall 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。

查看全球安全统计信息：

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“事件跟踪”下的安全事件统计信息。

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。

查看全球端口活动：

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

Firewall 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。

确定计算机的位置：

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“分布图视图”。

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。

获取计算机的域信息：

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“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。

获取计算机的网络信息：

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“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。

从“入站事件”日志跟踪计算机的 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“跟踪此地址”。
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”。

相关主题

- 跟踪 Internet 通讯 (第 158 页)
- 查看入站事件 (第 155 页)

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。

从“入侵检测事件”日志跟踪计算机的 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“跟踪此地址”。
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”。

相关主题

- 跟踪 Internet 通讯 (第 158 页)
- 记录、监视和分析 (第 153 页)

跟踪被监视 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 IP 地址的注册和网络信息。

监视程序带宽使用情况：

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“活动程序”。
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 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”。

相关主题

- 监视 Internet 通讯 (第 161 页)

监视 Internet 通讯

Firewall 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。此外，通讯流量监视器还显示当前使用您计算机上大部分网络连接的程序及其访问的 IP 地址。

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 Firewall 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。

相关主题

- 分析入站和出站通讯 (第 162 页)

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。此外，通讯流量监视器还显示当前使用您计算机上大部分网络连接的程序及其访问的 IP 地址。

分析入站和出站通讯：

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”。

相关主题

- 关于流量分析图 (第 161 页)

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。

监视程序带宽使用情况：

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。

监视程序带宽使用情况：

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“活动程序”。

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。
- 侦听连接：选择程序名称下的侦听项目。
- 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“活动程序”下的“刷新”。

第 24 章

了解 Internet 安全性

Firewall 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 Firewall 的 HTML 教程。

本章内容

启动 HackerWatch 教程

要了解 Firewall，可以从 SecurityCenter 访问 HackerWatch 教程。

启动 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 25 章

McAfee SpamKiller

SpamKiller 过滤垃圾邮件和网络钓鱼电子邮件，并提供以下项目。

用户选项

- 过滤多个电子邮件帐户
- 将联系人导入朋友列表
- 创建自定义过滤器并将垃圾邮件报告给 McAfee 以供分析
- 标记为垃圾邮件和标记为非垃圾邮件选项
- 多用户支持（Windows® XP 和 Vista™）

过滤

- 自动更新过滤器
- 创建自定义电子邮件过滤器
- 多层核心过滤引擎
- 网络钓鱼过滤器

本章内容

功能

此版本的 SpamKiller 提供以下功能。

过滤

高级过滤技术会增强用户的体验。

网络钓鱼

网络钓鱼功能会轻松确定和阻止可能的网络钓鱼网站。

安装

优化设置和配置。

界面

直观的用户界面，可以避免计算机受垃圾邮件的侵扰。

支持

免费的即时消息和电子邮件技术支持，可以轻松、便捷和实时提供客户服务。

垃圾邮件处理

处理垃圾电子邮件的可选设置。利用这些设置可以查看没有正确过滤的邮件。

支持的电子邮件程序

- 任何 POP3 电子邮件程序
- 对 Outlook® 2000 或更高版本提供 MAPI 支持
- 为使用 POP3 或付费版 MSN®/Hotmail® 的 Web 邮件提供过滤器支持

支持的电子邮件工具栏

- Outlook Express 6.0 或更高版本
- Outlook 2000、XP、2003 或 2007
- Eudora® 6.0 或更高版本
- Thunderbird™ 1.5 或更高版本

支持的网络钓鱼防护

任何 HTTP 兼容的 Web 浏览器，包括：

- Internet Explorer
- Firefox®
- Netscape®

第 26 章

管理 Web 邮件帐户

您可以添加 Web 邮件帐户来过滤垃圾邮件，编辑 Web 邮件帐户信息，或在不再想过滤 Web 邮件帐户时删除这些帐户。

您还可以管理 Web 邮件过滤。例如，可以对 Web 邮件帐户中的电子邮件禁用或启用过滤，管理已过滤的邮件和查看日志。

本章内容

添加 Web 邮件帐户

您可以添加以下类型的 Web 邮件帐户来过滤这些帐户的垃圾邮件。

- POP3 Web 邮件（如 Yahoo®）
- MSN/Hotmail（仅完全支持付费版本）

添加 POP3 或 MSN/Hotmail Web 邮件帐户

添加电子邮件帐户，过滤这些帐户的垃圾邮件。

添加 POP3 或 MSN/Hotmail Web 邮件帐户：

1. 在“高级菜单”上，单击“配置”。
2. 在“配置”窗格中，单击“电子邮件和 IM”。
3. 在“垃圾邮件防护”下，单击“高级”。
4. 在“垃圾邮件防护”窗格上，单击“Web 邮件帐户”。
5. 在“Web 邮件帐户”窗格上，单击“添加”。
6. 在以下框中指定 Web 邮件帐户信息：
   - **描述**：描述帐户。可以在此框中键入任何信息。
   - **电子邮件地址**：指定此帐户的电子邮件地址。
   - **帐户类型**：指定电子邮件帐户的类型。
   - **服务器**：指定此帐户的服务器名称。
   - **用户名**：指定此帐户的用户名
   - **密码**：指定用于访问此帐户的密码。
   - **确认密码**：确认密码。
7. 单击“下一步”。
8. 在“检查选项”下，选择以下任一选项，以确定 SpamKiller 检查帐户中垃圾邮件的时间：
   - 在“检查频率为”框中键入值。

     SpamKiller 会在指定的时间间隔（分钟数）检查此帐户。如果键入数字零，则 SpamKiller 只在连接时检查帐户。
   - 选中“启动时检查”复选框。

     SpamKiller 会在每次重新启动计算机时检查帐户。如果您有直接连接，请使用此选项。
9. 如果使用拨号连接，请选择“连接选项”下的任一选项来确定 SpamKiller 连接到 Internet 的方式：
   - 单击“从不进行拨号连接”。

     SpamKiller 不会自动进行拨号连接。必须手动启动拨号连接。

- 单击“无可用连接时拨号”。

  如果 Internet 连接不可用，SpamKiller 会尝试使用您指定的拨号连接进行连接。

- 单击“始终拨指定连接”。

  SpamKiller 会尝试使用指定的拨号连接进行连接。

- 单击“拨此连接”列表中的条目。

  此条目指定 SpamKiller 尝试连接到的拨号连接。

- 单击“过滤完成后保持连接状态”复选框。

  过滤完成后，计算机仍连接到 Internet。

10 单击“完成”。

修改 Web 邮件帐户

您可以启用或禁用 Web 电子邮件帐户，也可以编辑这些帐户的信息。例如，可以更改电子邮件地址、帐户描述、帐户类型、密码、SpamKiller 检查帐户中是否有垃圾邮件的频率，以及计算机连接到 Internet 的方式。

编辑 POP3 或 MSN/Hotmail Web 邮件帐户

您可以启用或禁用 Web 电子邮件帐户，也可以编辑这些帐户的信息。例如，可以更改电子邮件地址、帐户描述、服务器信息、SpamKiller 检查帐户中垃圾邮件的频率以及计算机连接到 Internet 的方式。

修改 POP3 或 MSN/Hotmail Web 邮件帐户：

1. 在“高级菜单”上，单击“配置”。
2. 在“配置”窗格中，单击“电子邮件和 IM”。
3. 在“垃圾邮件防护”下，单击“高级”。
4. 在“垃圾邮件防护”窗格上，单击“Web 邮件帐户”。
5. 选择要修改的帐户，然后单击“编辑”。
6. 编辑以下框中的帐户信息：
   - **描述**：描述帐户。可以在此框中键入任何信息。
   - **电子邮件地址**：指定此帐户的电子邮件地址。
   - **帐户类型**：指定电子邮件帐户的类型。
   - **服务器**：指定此帐户的服务器名称。
   - **用户名**：指定此帐户的用户名
   - **密码**：指定用于访问此帐户的密码。
   - **确认密码**：确认密码。
7. 单击“下一步”。
8. 在“检查选项”下，选择以下任一选项，以确定 SpamKiller 检查帐户中垃圾邮件的时间：
   - 在“检查频率为”框中键入值。

     SpamKiller 会在指定的时间间隔（分钟数）检查此帐户。如果键入数字零，则 SpamKiller 只在连接时检查帐户。
   - 选中“启动时检查”复选框。

     SpamKiller 会在每次重新启动计算机时检查帐户。如果您有直接连接，请使用此选项。

9 如果使用拨号连接，请选择“连接选项”下的任一选项来确定 SpamKiller 连接到 Internet 的方式：

- 单击“从不进行拨号连接”。

  SpamKiller 不会自动进行拨号连接。必须手动启动拨号连接。

- 单击“无可用连接时拨号”。

  如果 Internet 连接不可用，SpamKiller 会尝试使用您指定的拨号连接进行连接。

- 单击“始终拨指定连接”。

  SpamKiller 会尝试使用指定的拨号连接进行连接。

- 单击“拨此连接”列表中的条目。

  此条目指定 SpamKiller 尝试连接到的拨号连接。

- 单击“过滤完成后保持连接状态”复选框。

  过滤完成后，计算机仍连接到 Internet。

10 单击“完成”。

删除 Web 邮件帐户

您可以删除不再要过滤的 Web 邮件帐户。

删除 Web 邮件帐户

删除不再要过滤的电子邮件帐户。

删除 Web 邮件帐户：

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 IM”。

3 在“垃圾邮件防护”下，单击“高级”。

4 在“垃圾邮件防护”窗格上，单击“Web 邮件帐户”。

5 选择要删除的帐户，然后单击“删除”。

管理 Web 邮件过滤

您可以对 Web 邮件帐户中的电子邮件禁用或启用过滤，管理已过滤的邮件和查看日志。

禁用 Web 邮件过滤

您可以禁用 Web 邮件过滤，从而禁止过滤电子邮件。

禁用 Web 邮件过滤：

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 IM”。
3. 在“垃圾邮件防护”下，单击“高级”。
4. 在“垃圾邮件防护”窗格上，单击“Web 邮件帐户”。
5. 清除要禁用的帐户旁的复选框。
6. 单击“确定”。

启用 Web 邮件过滤

如果禁用了任何 Web 邮件帐户，可以再次启用这些帐户。

启用 Web 邮件过滤：

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 IM”。
3. 在“垃圾邮件防护”下，单击“高级”。
4. 在“垃圾邮件防护”窗格上，单击“Web 邮件帐户”。
5. 选中要启用的帐户旁的复选框。
6. 单击“确定”。

管理 Web 邮件帐户的已过滤邮件

您可以查看、复制或删除已在 Web 邮件帐户中过滤的邮件。

查看、复制或删除 Web 邮件帐户的已过滤邮件：

1. 在“高级菜单”上，单击“报告和日志”。
2. 在“报告和日志”窗格中，单击“已过滤的 Web 邮件”。
3. 在“已过滤的 Web 邮件”窗格中，选择要查看、复制或删除的邮件。
4. 在“我想”下，执行以下任一操作：
   - 单击“复制”以将邮件复制到剪贴板。

- 单击“删除”以删除邮件。

查看已过滤 Web 邮件的日志

您可以查看已过滤 Web 邮件的日志。例如，可以查看过滤电子邮件的时间以及接收它的帐户。

查看已过滤 Web 邮件的日志：

1. 在“高级菜单”上，单击“报告和日志”。
2. 在“报告和日志”上，单击“最新事件”。
3. 在“最新事件”窗格上，单击“查看日志”。
4. 在左侧窗格上，展开“电子邮件和 IM”列表，然后单击“Web 邮件过滤事件”。
5. 选择要查看的日志。
6. 在“详细信息”下，查看有关日志的信息。

第 27 章

管理朋友

为确保您收到朋友发来的全部邮件，请将其地址添加到朋友列表中。您还可以添加域、编辑或删除朋友以及安排对朋友列表进行自动更新的时间。

本章内容

了解如何管理朋友

本节介绍如何管理朋友。

在 SpamKiller 工具栏中手动添加朋友

为确保您收到朋友发来的全部邮件，请将其地址添加到朋友列表中。

如果使用 Outlook、Outlook Express、Windows Mail、Eudora 或 Thunderbird 电子邮件程序，则可以从 SpamKiller 工具栏添加朋友。

从 Outlook 添加朋友：

- 在电子邮件程序中，选择一封邮件，然后单击“添加朋友”。

从 Outlook Express、Windows Mail、Eudora 或 Thunderbird 添加朋友：

- 在电子邮件程序中，选择一封邮件。然后，在“SpamKiller”菜单中，单击“添加朋友”。

手动添加朋友

为确保您收到朋友发来的全部邮件，请将其地址添加到朋友列表中。您还可以添加域。

手动添加朋友：

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 IM”。
3. 在“垃圾邮件防护”下，单击“高级”。
4. 在“垃圾邮件防护”窗格上，单击“朋友”。
5. 在“朋友”窗格上，单击“添加”。
6. 在以下框中键入朋友的信息：
   - **姓名**：指定朋友的姓名。
   - **类型**：指定是要指定单个电子邮件地址，还是指定整个域。
   - **电子邮件地址**：指定朋友的电子邮件地址，或指定不想过滤的域。
7. 单击“确定”。

编辑朋友

如果有朋友的信息发生变化，则可以更新列表，以确保收到此朋友的全部邮件。

编辑朋友：

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 IM”。

3 在“垃圾邮件防护”下，单击“高级”。

4 在“垃圾邮件防护”窗格上，单击“朋友”。

5 选择要编辑的朋友，然后单击“编辑”。

6 在以下框中编辑朋友的信息：

- **姓名**：指定朋友的姓名。
- **类型**：指定是要编辑单个电子邮件地址，还是编辑整个域。
- **电子邮件地址**：指定朋友的电子邮件地址，或指定不想过滤的域。

7 单击“确定”。

删除朋友

如果要过滤朋友，则从此列表中删除朋友。

删除朋友：

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 IM”。

3 在“垃圾邮件防护”下，单击“高级”。

4 在“垃圾邮件防护”窗格上，单击“朋友”。

5 选择要删除的朋友，然后单击“删除”。

自动更新朋友

为确保收到朋友发来的所有邮件，可以从地址簿中手动导入其地址，或安排自动更新的时间。

手动导入地址簿

SpamKiller 可以导入地址簿并更新朋友。

手动导入地址簿：

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 IM”。
3. 在“垃圾邮件防护”下，单击“高级”。
4. 在“垃圾邮件防护”窗格上，单击“地址簿”。
5. 选择要导入的地址簿，然后单击“ 立即运行”。
6. 单击“确定”。

添加地址簿

为接收朋友发来的所有邮件，确保包含要导入的地址簿。

添加地址簿：

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 IM”。
3. 在“垃圾邮件防护”下，单击“高级”。
4. 在“垃圾邮件防护”窗格上，单击“地址簿”。
5. 在“地址簿”窗格上，单击“添加”。
6. 在“类型”列表中，单击要导入的地址簿的类型。
7. 如果适用，请在“来源”列表中选择地址簿来源。
8. 在“计划”列表中，单击“每天”、“每周”或“每月”，以确定 SpamKiller 检查地址簿中是否有新地址的时间。
9. 单击“确定”。

编辑地址簿

SpamKiller 可以按计划的时间间隔导入地址簿并更新朋友。您还可以编辑地址簿并更改其导入计划。

编辑地址簿：

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 IM”。
3. 在“垃圾邮件防护”下，单击“高级”。
4. 在“垃圾邮件防护”窗格上，单击“地址簿”。
5. 选择要编辑的地址簿，然后单击“编辑”。
6. 执行以下任一操作：
   - 在“类型”列表中，单击要导入的地址簿的类型。
   - 如果适用，请在“来源”列表中选择地址簿来源。
   - 在“计划”列表中，单击“每天”、“每周”或“每月”，以确定 SpamKiller 检查地址簿中是否有新地址的时间。
7. 单击“确定”。

删除地址簿

如果不再想从地址簿中自动导入地址，则可以删除地址簿。

从自动导入中删除地址簿：

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 IM”。
3. 在“垃圾邮件防护”下，单击“高级”。
4. 在“垃圾邮件防护”窗格上，单击“地址簿”。
5. 选择要删除的地址簿，然后单击“删除”。

第 28 章

修改过滤选项

过滤选项包括更改过滤级别、修改特殊过滤器、自定义处理邮件的方式、指定要过滤的字符集，以及将垃圾邮件报告给 McAfee。

本章内容

修改电子邮件过滤

您可以更改要过滤邮件的积极程度。如果过滤合法的电子邮件，则可以降低过滤级别。

您还可以启用或禁用特殊过滤器。例如，默认情况下，过滤主要包含图像的邮件。如果要接收这些邮件，可以禁用此过滤器。

更改电子邮件过滤级别

您可以更改要过滤邮件的积极程度。例如，如果过滤合法的电子邮件，则可以降低过滤级别。

更改电子邮件过滤级别：

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 IM”。

3 在“垃圾邮件防护”下，单击“高级”。

4 在“垃圾邮件防护”窗格上，单击“过滤选项”。

5 在“过滤选项”下，将滑块移到以下任一设置：

- **低**：接受大多数电子邮件。
- **中低**：只过滤明显的垃圾邮件。
- **中**：接受较多的电子邮件。
- **中高**：过滤与垃圾邮件类似的任何电子邮件。
- **高**：只接受“朋友”列表中的发件人发来的邮件。

6 单击“确定”。

修改特殊过滤器

您可以启用或禁用特殊过滤器。例如，默认情况下，过滤主要包含图像的邮件。如果要接收这些邮件，可以禁用此过滤器。

修改特殊过滤器：

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 IM”。

3 在“垃圾邮件防护”下，单击“高级”。

4 选择“过滤选项”。

5 在“特殊过滤器”下，启用或禁用以下任一复选框：

- **过滤包含隐藏文本的邮件**：隐藏文本用于避开检测。
- **过滤包含特定图文比率的邮件**：主要包含图像的邮件通常是垃圾邮件。

- **过滤故意包含 HTML 格式错误的邮件：**无效格式用于防止过滤器过滤垃圾邮件。
- **过滤的邮件不大于：**不过滤大于指定大小的邮件。您可以增加或减小邮件大小（有效范围为 0-250 KB）。

6 单击“确定”。

修改处理邮件的方式

您可以更改标记和处理邮件的方式。例如，可以更改垃圾邮件或网络钓鱼标记的名称，以及邮件保留在收件箱还是 SpamKiller 文件夹中。

修改处理邮件的方式

您可以更改标记和处理邮件的方式。例如，可以更改垃圾邮件或网络钓鱼标记的名称，以及邮件保留在收件箱还是 SpamKiller 文件夹中。

修改 SpamKiller 处理垃圾邮件的方式：

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 IM”。
3. 在“垃圾邮件防护”下，单击“高级”。
4. 在“垃圾邮件防护”窗格上，单击“处理”。
5. 执行以下任一操作：
   - 单击“标记为垃圾邮件并移至 SpamKiller 文件夹”。

     这是默认设置。将垃圾邮件移到 SpamKiller 文件夹。
   - 单击“标记为垃圾邮件并保存在收件箱中”。

     垃圾邮件仍留在收件箱中。
   - 在“将此可自定义标记添加到垃圾邮件的主题”框中键入自定义标记。

     您指定的标记会添加到垃圾邮件的电子邮件主题行。
   - 在“将此可自定义的标记添加到网络钓鱼邮件的主题”框中键入自定义标记。

     您指定的标记会添加到网络钓鱼邮件的电子邮件主题行。
6. 单击“确定”。

使用字符集过滤邮件

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。您可以过滤包含特定字符集的邮件。不过，请不要过滤接收合法电子邮件所采用语言的字符集。

例如，如果要过滤意大利语邮件，而接收合法的英语电子邮件，请不要选择西欧语言。选择西欧语言会过滤意大利语邮件，但也会过滤西欧语言字符集中的英语和其他语言的邮件。

使用字符集过滤邮件

您可以过滤包含特定字符集的邮件。不过，请不要过滤接收合法电子邮件所采用语言的字符集。

使用字符集过滤邮件：

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 IM”。
3. 在“垃圾邮件防护”下，单击“高级”。
4. 在“垃圾邮件防护”窗格上，单击“字符集”。
5. 选中要过滤的字符集旁的复选框。
6. 单击“确定”。

报告垃圾邮件消息

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。

报告垃圾邮件

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。

将垃圾邮件报告给 McAfee：

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 IM”。
3. 在“垃圾邮件防护”下，单击“高级”。
4. 在“垃圾邮件防护”窗格上，单击“向 McAfee 报告”。
5. 选中以下任一复选框：
   - **单击“标记为垃圾邮件”时启用报告**：每次将邮件标记为垃圾邮件时将其报告给 McAfee。
   - **单击“标记为非垃圾邮件”时启用报告**：每次将邮件标记为非垃圾邮件时将其报告给 McAfee。
   - **发送整个邮件（不只是标题）**：将邮件报告给 McAfee 时发送整个邮件，而不仅仅是标题。
6. 单击“确定”。

第 29 章

管理个人过滤器

过滤器指定 SpamKiller 在电子邮件中查找的内容。

SpamKiller 会使用许多过滤器；不过，您可以创建新过滤器或编辑现有的过滤器，以便精确确定将哪些邮件标识为垃圾邮件。例如，如果过滤器表达式包含“mortgage”，SpamKiller 会查找包含词语“mortgage”的邮件。

添加过滤器时，请仔细检查要过滤的短语。如果有短语可能在正常的电子邮件中使用，请不要使用此短语。

本章内容

了解如何管理个人过滤器

本节介绍如何管理个人过滤器。

添加个人过滤器

创建过滤器是可选择，这些过滤器会影响入站邮件。因此，请不要对可能显示在非垃圾邮件中的常用词语创建过滤器。

添加过滤器：

1. 在“高级菜单”上，单击“配置”。
2. 在“配置”窗格中，单击“电子邮件和 IM”。
3. 在“垃圾邮件防护”下，单击“高级”。
4. 在“垃圾邮件防护”窗格上，单击“个人过滤器”。
5. 单击“添加”。
6. 在“项目”列表中，单击一个条目，以确定过滤器是否在邮件主题、正文、标题或邮件发送人中查找词语或短语。
7. 在“条件”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）指定词语或短语的邮件。
8. 在“词语或短语”框中，键入要在邮件中查找的内容。例如，如果指定“mortgage”，则会过滤包含此词语的全部邮件。
9. 选中“此过滤器使用常规表达式(RegEx)”复选框，以指定在过滤器条件中使用的字符模式。要测试字符模式，请单击“测试”。
10. 单击“确定”。

编辑个人过滤器

过滤器指定 SpamKiller 在电子邮件中查找的内容。SpamKiller 会使用许多过滤器；不过，您可以创建新过滤器或编辑现有的过滤器，以便精确确定将哪些邮件标识为垃圾邮件。

添加过滤器：

1. 在“高级菜单”上，单击“配置”。
2. 在“配置”窗格中，单击“电子邮件和 IM”。
3. 在“垃圾邮件防护”下，单击“高级”。
4. 在“垃圾邮件防护”窗格上，单击“个人过滤器”。
5. 选择要编辑的过滤器，然后单击“编辑”。
6. 在“项目”列表中，单击一个条目，以确定过滤器是否在邮件主题、正文、标题或邮件发送人中查找词语或短语。
7. 在“条件”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）指定词语或短语的邮件。
8. 在“词语或短语”框中，键入要在邮件中查找的内容。例如，如果指定“mortgage”，则会过滤包含此词语的全部邮件。
9. 选中“此过滤器使用常规表达式(RegEx)”复选框，以指定在过滤器条件中使用的字符模式。要测试字符模式，请单击“测试”。
10. 单击“确定”。

删除个人过滤器

您可以删除不再想使用的过滤器。删除过滤器后，过滤器即会永久删除。

删除过滤器：

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 IM”。
3. 在“垃圾邮件防护”下，单击“高级”。
4. 在“垃圾邮件防护”窗格上，单击“个人过滤器”。
5. 选择要删除的过滤器，然后单击“删除”。
6. 单击“确定”。

使用常规表达式

常规表达式是在定义表达式时使用的特殊字符和序列。例如：

- 常规表达式 `[0-9]*\.[0-9]+`

  匹配给定非工程表示法的浮点数。常规表达式匹配“12.12”、“.1212”和“12.0”，但不匹配“12”和“12”。

- 常规表达式 `\D*[0-9]+\D*`

  匹配带有数字的所有词语：“SpamKi11er”和“V1AGRA”，但不匹配“SpamKiller”和“VIAGRA”。

使用常规表达式

常规表达式是在定义表达式时使用的特殊字符和序列。

\

将下个字符标记为特殊字符或文字。例如，“n”匹配字符“n”。“\n”匹配换行字符。序列“\\”匹配“\”，“\(”匹配“(”。

^

匹配输入内容的开头。

$

匹配输入内容的结尾。

*

匹配前面的字符零次或多次。例如，“zo*”匹配“z”或“zoo”。

+

匹配前面的字符一次或多次。例如，“zo+”匹配“zoo”，但不匹配“z”。

?

匹配前面的字符零次或一次。例如，“a?ve?”匹配“never”中的“ve”。

.

匹配换行字符外的任意一个字符。

（模式）

匹配模式并记住匹配项目。可以使用项目 [0]...[n] 从结果匹配集合中检索匹配的子字符串。要匹配括号字符 ( )，请使用“\(”或“\)”。

x|y

匹配 x 或 y。例如，“z|wood”匹配“z”或“wood”。“(z|w)oo”匹配“zoo”或“wood”。

{n}

n 是非负整数。准确匹配 n 次数。例如，“o{2}”不匹配“Bob”中的“o”，而匹配“foooood”中的前两个“o”。

{n,}

n 是非负整数。匹配至少 n 次数。例如，“o{2}”不匹配“Bob”中的“o”，而匹配“foooood”中的所有“o”。“o{1,}”等同于“o+”。“o{0,}”等同于“o*”。

{n,m}

m 和 n 都是非负整数。匹配至少 n 次，至多 m 次。例如，“o{1,3}”匹配“fooooood”中的前三个“o”。“o{0,1}”等同于“o?”。

[xyz]

字符集。匹配任一括住的字符。例如，“[abc]”匹配“plain”中的“a”。

[^xyz]

否定字符集。匹配未括住的任何字符。例如，“[^abc]”匹配“plain”中的“p”。

[a-z]

字符范围。匹配指定范围中的任何字符。例如，“[a-z]”匹配范围“a”到“z”和“A”到“Z”中的任何大小写字母字符。

[A-Z]

字符范围。匹配指定范围中的任何字符。例如，“[A-Z]”匹配范围“A”到“Z”和“a”到“z”中的任何大小写字母字符。

[^m-z]

否定范围字符。匹配指定范围中未包含的任何字符。例如，“[^m-z]”不匹配范围“m”到“z”中的任何字符。

\b

匹配词语的边界，即位于词语和空格之间的位置。例如，“er\b”匹配“never”中的“er”，但不匹配“verb”中的“er”。

\B

匹配非词语的边界。“ea*r\B”匹配“never early”中的“ear”。

\d

匹配数字字符。等同于 [0-9]。

\D

匹配非数字字符。等同于 [^0-9]。

\f

匹配走纸换页字符。

\n

匹配换行符。

\r

匹配回车符。

\s

匹配任何空白，包括空格、制表符、走纸换页等。等同于“[\f\n\r\t\v]”。

\S

匹配任何非空白字符。等同于“[^ \f\n\r\t\v]”。

\t

匹配制表符。

\v

匹配垂直制表符。

\w

匹配包含下划线的任何词语字符。等同于“[A-Za-z0-9_]”。

\W

匹配任何非词语字符。等同于“[^A-Za-z0-9_]”。

\num

匹配 num，其中 num 是正整数。重新引用到记住的匹配项。例如，“(.)\1”匹配两个连续的相同字符。\n 匹配 n，其中 n 是八进制转义值。八进制转义值必须是 1、2 或 3 个数字长。例如，“\11”和“\011”都匹配制表符。“\0011”等同于“\001”和“1”。八进制转义值不得超过 256。如果超过 256，则只有前两个数字组成表达式。允许在常规表达式中使用 ASCII 代码。

\xn

匹配 n，其中 n 是十六进制转义值。十六进制转义值必须正好是两个数字长。例如，“\x41”匹配“A”。“\x041”等同于“\x04”和“1”。允许在常规表达式中使用 ASCII 代码。

第 30 章

维护 SpamKiller

维护 SpamKiller 包括管理垃圾邮件防护和使用工具栏。

管理垃圾邮件防护时，可以禁用或启用过滤。

使用工具栏时，可以禁用或启用 SpamKiller 提供的电子邮件工具栏，并从工具栏中将邮件标记为垃圾邮件或非垃圾邮件。

本章内容

管理垃圾邮件防护

您可以禁用或启用电子邮件过滤。

禁用垃圾邮件防护会防止过滤电子邮件，或启用垃圾邮件防护来过滤电子邮件。

禁用垃圾邮件防护

您可以禁用垃圾邮件防护，从而禁止过滤电子邮件。

禁用过滤：

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 IM”。

3 在“垃圾邮件防护”下，单击“关”。

启用垃圾邮件防护

您可以启用垃圾邮件防护并过滤电子邮件。

启用过滤：

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 IM”。

3 在“垃圾邮件防护”下，单击“开”。

使用工具栏

您可以为支持的电子邮件客户端禁用或启用电子邮件工具栏。

如果使用 Outlook、Outlook Express、Windows Mail、Eudora 或 Thunderbird 电子邮件程序，则还可以从 SpamKiller 工具栏将邮件标记为垃圾邮件和非垃圾邮件。

禁用工具栏

您可以禁用支持电子邮件客户端的工具栏。

禁用工具栏：

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 IM”。
3. 在“垃圾邮件防护”下，单击“高级”。
4. 在“垃圾邮件防护”窗格上，单击“电子邮件工具栏”，并清除要禁用工具栏旁的复选框。
5. 单击“确定”。

启用工具栏

如果禁用了任何工具栏，则可以再次启用这些工具栏。

启用工具栏：

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 IM”。
3. 在“垃圾邮件防护”下，单击“高级”。
4. 在“垃圾邮件防护”窗格上，单击“电子邮件工具栏”，并选中要启用工具栏旁的复选框。
5. 单击“确定”。

在 SpamKiller 工具栏中将邮件标记为垃圾邮件或非垃圾邮件

如果使用 Outlook、Outlook Express、Windows Mail、Eudora 或 Thunderbird 电子邮件程序，则可以从 SpamKiller 工具栏将邮件标记为垃圾邮件和非垃圾邮件。

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进行标记，并将其留在收件箱中、SpamKiller 文件夹（Outlook、Outlook Express、Windows Mail 和 Thunderbird）或垃圾文件夹 (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。

在 Outlook 中将邮件标记为垃圾邮件或非垃圾邮件：

1 在电子邮件程序中，选择一封邮件。

2 在“SpamKiller”工具栏上，单击“标记为垃圾邮件”或“标记为非垃圾邮件”。

在 Outlook Express、Windows Mail、Eudora 或 Thunderbird 中将邮件标记为垃圾邮件或非垃圾邮件：

1 在电子邮件程序中，选择一封邮件。

2 在“SpamKiller”菜单上，单击“标记为垃圾邮件”或“标记为非垃圾邮件”。

第 31 章

配置网络钓鱼防护

系统会将未经请求的电子邮件归到垃圾邮件（请求您购买商品的垃圾邮件）或网络钓鱼（请求您将个人信息提供给已知的或可能的诈骗网站）类别中。

网络钓鱼过滤器会帮助您防护诈骗网站。如果浏览到已知或可能的诈骗网站，则系统会将您重定向到“网络钓鱼过滤器”页。

您可以禁用或启用网络钓鱼防护，或修改过滤选项。

本章内容

禁用或启用网络钓鱼防护

您可以禁用或启用网络钓鱼防护。例如，在要访问信任但被阻止的网站时禁用网络钓鱼防护。

禁用网络钓鱼防护

在要访问信任但被阻止的网站时禁用网络钓鱼防护。

禁用网络钓鱼防护：

1 在“高级菜单”上，单击“配置”。

2 在“配置”窗格中，单击“Internet 和网络”。

3 在“网络钓鱼”下，单击“关”。

启用网络钓鱼防护

启用网络钓鱼防护，以确保抵御网络钓鱼网站的侵扰。

启用网络钓鱼防护：

1 在“高级菜单”上，单击“配置”。

2 在“配置”窗格中，单击“Internet 和网络”。

3 在“网络钓鱼”下，单击“开”。

修改网络钓鱼过滤

McAfee 会采用两种方法确定网站是否是网络钓鱼网站：将浏览的网站与已知诈骗网站列表进行比较，或尝试确定您浏览的网站是否是诈骗网站。

修改网络钓鱼过滤

McAfee 会采用两种方法确定网站是否是网络钓鱼网站。如果需要完全防护，请选中这两个选项。

更改网络钓鱼选项：

1. 在“高级菜单”上，单击“配置”。
2. 在“配置”窗格中，单击“Internet 和网络”。
3. 在“网络钓鱼”下，单击“高级”。
4. 启用或禁用以下任一复选框：
   - **启用黑名单和白名单查找，以检测欺诈 Web 站点**：将浏览的网站与已知的诈骗网站进行比较。
   - **启用启发式技术以检测欺诈网站**：尝试确定您浏览的网站是否是诈骗网站。
5. 单击“确定”。

第 32 章

其他帮助

本章介绍常见问题。

本章内容

常见问题

本节提供常见问题的答案。

何谓 POP3、MSN/Hotmail 和 MAPI 帐户？

SpamKiller 专用于使用以下类型的电子邮件帐户：POP3、POP3 Web Mail、MSN/Hotmail 和 MAPI。这些帐户有些区别，这会影响 SpamKiller 执行过滤的方式。

POP3

这是最常见的帐户类型，是 Internet 电子邮件的标准。如果您使用 POP3 帐户，SpamKiller 会直接连接到服务器，并在电子邮件程序检索这些邮件之前过滤这些邮件。

POP3 Web 邮件

POP3 Web 邮件帐户基于 Web。过滤 POP3 Web 邮件帐户与过滤 POP3 帐户类似。

MSN/Hotmail

MSN/Hotmail 帐户基于 Web。过滤 MSN/Hotmail 帐户与过滤 POP3 帐户类似。

MAPI

MAPI 是 Microsoft 设计的系统，它支持许多消息类型，包括 Internet 电子邮件、传真和 Exchange Server 消息。出于此原因，MAPI 通常在运行 Microsoft® Exchange Server 的公司环境中使用。不过，许多人都使用 Microsoft Outlook 收发个人 Internet 电子邮件。
SpamKiller 可以访问 MAPI 帐户，但请注意：

- 通常，在您使用电子邮件程序检索邮件后，才执行过滤。
- SpamKiller 只过滤默认的收件箱和 Internet 电子邮件。

何谓网络钓鱼过滤器？

系统会将未经请求的电子邮件归到垃圾邮件（请求您购买商品的垃圾邮件）或网络钓鱼（请求您将个人信息提供给已知的或可能的诈骗网站）类别中。

网络钓鱼过滤器有助于避开列在黑名单中的网站（已确认的网络钓鱼或与欺诈有关的站点），或列在灰名单（包含某些危险内容或黑名单中站点的链接）中的网站。

如果浏览到已知或可能的诈骗网站，则会将您重定向到“网络钓鱼过滤器”页。

McAfee 为何使用 Cookie？

McAfee 网站使用称为 Cookie 的软件标记来识别再次访问网站的用户的身份。Cookie 是放在计算机硬盘上文件中的文本块。当您下次访问网站时，系统会使用 Cookie 来识别您的身份。

McAfee 使用 Cookie 执行以下操作：

- 管理您的订购权限和权利
- 将您识别为老用户，无需每次访问时都重新注册
- 帮助了解您的购买喜好，并根据您的需要自定义服务
- 提供您可能感兴趣的信息、产品和特别优惠

McAfee 还要求您提供名字，以便可以个性化您的 McAfee 网站体验。

如果用户将浏览器设置为拒绝 Cookie，McAfee 将无法为这些用户提供订购服务。McAfee 不会出售和出租收集到的信息，也不会与任何第三方共享此类信息。

McAfee 允许广告商在访问者的浏览器中设置 Cookie。McAfee 无权访问广告商 Cookie 中包含的信息。

第 33 章

McAfee Privacy Service

Privacy Service 会为您、家人、个人数据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，阻止个人身份信息的传输，以及过滤可能不良的在线内容（包括图像、广告、弹出窗口和 Web 错误）。它还提供高级家长监控，允许成人监视、控制和记录儿童的 Web 浏览习惯，以及为密码提供安全存储区域。

开始使用 Privacy Service 之前，您应熟悉某些最常用的功能。Privacy Service 帮助会提供有关配置和使用这些功能的详细信息。

本章内容

功能

Privacy Service 提供以下功能：

- Web 浏览防护
- 个人信息保护
- 家长监控
- 密码存储

Web 浏览防护

Web 浏览防护可以拦截您计算机上的广告、弹出窗口和 Web 错误。阻止广告和弹出窗口会防止在浏览器中显示大多数广告和弹出窗口。阻止 Web 错误会防止网站跟踪您的在线活动以及将信息发给未经授权的来源。它结合了广告、弹出窗口和 Web 错误阻止，加强了安全性并防止未经请求的内容干扰您的 Web 浏览。

个人信息保护

个人信息保护会阻止在 Internet 上传输敏感信息或机密信息（如信用卡号、银行帐号、地址等）。

家长监控

“家长监控”可以配置内容评级及 Internet 时间限制，前者限定用户可以查看的网站和内容，后者指定用户可以访问 Internet 的时段。“家长监控”还会全面限制用户对特定网站的访问权限，并根据年龄组和相关联的关键字授予或阻止访问权限。

密码存储

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 McAfee 管理员或系统管理员）访问它们。

第 34 章

设置家长监控

在添加用户后，可以为此用户设置家长监控。家长监控是定义用户内容评级组、Cookie 拦截级别和 Internet 时间限制的设置。内容评级组会根据用户的年龄组确定用户可以访问的 Internet 内容和网站的类型。Cookie 拦截级别确定是否允许网站读取用户登录时网站在计算机上设置的 Cookie。Internet 时间限制定义用户可以访问 Internet 的日期和时间。

您还可以设置某些适用于所有非成人用户的全局家长监控。例如，您可以阻止或允许某些网站，或在非成人用户浏览 Internet 时阻止显示可能的不良图像。您还可以为所有用户配置全局 Cookie 拦截设置。不过，如果个别用户的 Cookie 拦截级别与全局 Cookie 拦截级别设置不同，则全局设置优先。

注意：您必须是管理员才能设置家长监控。

本章内容

设置用户的内容评级组

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

系统会根据用户所属的组对内容评级（即可用或阻止）。例如，系统会为属于幼儿组的用户阻止某些网站，但属于年长青少年组的用户可以访问这些网站。属于成人组的用户可以访问所有内容。默认情况下，系统会将新用户自动添加到幼儿组，完全限制其对内容的访问。

作为管理员，您可以设置用户的内容评级组，然后根据这些组阻止或允许网站。如果要为用户更严格地评级内容，则还可以禁止用户浏览全局“允许的网站”列表中未包含的任何网站。有关详细信息，请参阅根据关键字阻止网站 (第 220 页)和允许网站 (第 221 页)。

设置用户的内容评级组

用户的内容评级组是一个年龄组，用于确定用户可访问的 Internet 内容和网站的类型。

设置用户的内容评级组：

1. 在“常见任务”下，单击“主页”。
2. 在“SecurityCenter 信息”下面，单击“配置”。
3. 在“SecurityCenter 配置”窗格上，单击“用户”下的“高级”。
4. 在“用户”窗格上，单击“家长监控”。
5. 在此列表中选择用户名。
6. 在“内容评级”下，单击要分配给用户的年龄组。
   然后，您可以根据每个年龄组对内容进行评级，从而禁止显示不适合某个年龄级别或成熟阶段的内容。
7. 要限制用户浏览全局“允许的网站”列表中没有包含的网站，请选中“限定此用户访问‘允许的网站’列表中的网站”复选框。
8. 单击“确定”。

设置用户的 Cookie 拦截级别

某些网站会在计算机上创建名为“Cookie”的小文件，用于监视个人首选项和浏览习惯。做为管理员，您可以将以下任一 Cookie 拦截级别分配给用户：

- 接受所有 Cookie
- 拒绝所有 Cookie
- 提示用户接受 Cookie

接受所有 Cookie 设置会允许网站在相应用户登录时读取这些网站在您计算机上设置的 Cookie。拒绝所有 Cookie 设置会防止网站读取 Cookie。提示用户接受 Cookie 设置会在每次网站试图在您计算机上设置 Cookie 时提示用户。然后，用户可以根据具体情况决定是否允许使用 Cookie。在用户确定接受或拒绝特定网站的 Cookie 后，系统不会就此网站再次向用户提示。

注意：某些网站需要启用 Cookie 才能工作正常。

设置用户的 Cookie 拦截级别

某些网站会在计算机上创建名为“Cookie”的小文件，用于监视个人首选项和浏览习惯。您可以为您计算机上的每个用户设置处理 Cookie 的方法。

设置用户的 Cookie 拦截级别：

1. 在“常见任务”下，单击“主页”。
2. 在“SecurityCenter 信息”下，单击“配置”。
3. 在“SecurityCenter 配置”窗格上，单击“用户”下的“高级”。
4. 在“用户”窗格上，单击“家长监控”。
5. 在此列表中选择用户名。
6. 在“Cookie 拦截功能”下，单击以下任一项目：
   - **接受所有 Cookie：**用户浏览的所有网站都可以读取其在计算机上设置的 Cookie。
   - **拒绝所有 Cookie：**用户浏览的任何网站都不会读取其在计算机上设置的 Cookie。
   - **提示用户接受 Cookie：**当用户尝试浏览网站时，会显示一条消息，提示用户允许或拒绝 Cookie。
7. 单击“确定”。

将网站添加到用户的接受 Cookie 列表中

如果将用户的 Cookie 拦截级别设置为提示提供网站的权限才能设置 Cookie，但始终要允许某些网站设置 Cookie 而不进行提示，可以将这些网站添加到用户的接受 Cookie 列表中。

将网站添加到用户的接受 Cookie 列表中：

1. 在“常见任务”下，单击“主页”。
2. 在“SecurityCenter 信息”下面，单击“配置”。
3. 在“SecurityCenter 配置”窗格上，单击“用户”下的“高级”。
4. 在“用户”窗格上，单击“家长监控”。
5. 在此列表中选择用户名。
6. 在“Cookie 拦截功能”下，单击“查看列表”。
7. 在“接受 Cookie 的网站”下的“http://”框中键入网站的地址，然后单击“添加”。
8. 单击“完成”。

修改用户的接受 Cookie 列表中的网站

如果网站的地址发生变化，或在您将其添加到用户的接受 Cookie 列表中时输入错误，则可以修改它。

修改用户的接受 Cookie 列表中的网站：

1. 在“常见任务”下，单击“主页”。
2. 在“SecurityCenter 信息”下面，单击“配置”。
3. 在“SecurityCenter 配置”窗格上，单击“用户”下的“高级”。
4. 在“用户”窗格上，单击“家长监控”。
5. 在此列表中选择用户名。
6. 在“Cookie 拦截功能”下，单击“查看列表”。
7. 在“接受 Cookie 的网站”下，单击“网站”列表中的条目，修改“http://”框中的网站地址，然后单击“更新”。
8. 单击“完成”。

删除用户的接受 Cookie 列表中的网站

如果错误地将网站添加到用户的接受 Cookie 列表，则可以删除它。

删除用户的接受 Cookie 列表中的网站：

1. 在“常见任务”下，单击“主页”。
2. 在“SecurityCenter 信息”下面，单击“配置”。
3. 在“SecurityCenter 配置”窗格上，单击“用户”下的“高级”。
4. 在“用户”窗格上，单击“家长监控”。
5. 在此列表中选择用户名。
6. 在“Cookie 拦截功能”下，单击“查看列表”。
7. 在“接受 Cookie 的网站”下，单击“网站”列表中的条目，然后单击“删除”。
8. 在“确认删除”对话框中，单击“是”。
9. 单击“完成”。

将网站添加到用户的接受 Cookie 列表中

如果将用户的 Cookie 拦截级别设置为提示提供网站的权限才能设置 Cookie，但始终要防止某些网站设置 Cookie 而不进行提示，可以将这些网站添加到用户的拒绝 Cookie 列表中。

将网站添加到用户的拒绝 Cookie 列表中：

1. 在“常见任务”下，单击“主页”。
2. 在“SecurityCenter 信息”下面，单击“配置”。
3. 在“SecurityCenter 配置”窗格上，单击“用户”下的“高级”。
4. 在“用户”窗格上，单击“家长监控”。
5. 在此列表中选择用户名。
6. 在“Cookie 拦截功能”下，单击“查看列表”。
7. 单击“拒绝 Cookie 的网站”。
8. 在“拒绝 Cookie 的网站”下的“http://”框中键入网站的地址，然后单击“添加”。
9. 单击“完成”。

修改用户的拒绝 Cookie 列表中的网站

如果网站的地址发生变化，或在您将其添加到用户的拒绝 Cookie 列表中时输入错误，则可以修改它。

修改用户的拒绝 Cookie 列表中的网站：

1. 在“常见任务”下，单击“主页”。
2. 在“SecurityCenter 信息”下面，单击“配置”。
3. 在“SecurityCenter 配置”窗格上，单击“用户”下的“高级”。
4. 在“用户”窗格上，单击“家长监控”。
5. 在此列表中选择用户名。
6. 在“Cookie 拦截功能”下，单击“查看列表”。
7. 单击“拒绝 Cookie 的网站”。
8. 在“拒绝 Cookie 的网站”下，单击“网站”列表中的条目，修改“http://”框中的网站地址，然后单击“更新”。
9. 单击“完成”。

删除用户的拒绝 Cookie 列表中的网站

如果错误地将网站添加到用户的拒绝 Cookie 列表，则可以删除它。

删除用户的拒绝 Cookie 列表中的网站：

1. 在“常见任务”下，单击“主页”。
2. 在“SecurityCenter 信息”下面，单击“配置”。
3. 在“SecurityCenter 配置”窗格上，单击“用户”下的“高级”。
4. 在“用户”窗格上，单击“家长监控”。
5. 在此列表中选择用户名。
6. 在“Cookie 拦截功能”下，单击“查看列表”。
7. 单击“拒绝 Cookie 的网站”。
8. 在“拒绝 Cookie 的网站”下，单击“网站”列表中的条目，然后单击“删除”。
9. 在“确认删除”对话框中，单击“是”。
10. 单击“完成”。

设置用户的 Internet 时间限制

作为管理员，您可以使用 Internet 时间限制网格指定用户是否及何时可以访问 Internet。您以授予用户无限制 Internet 使用、有限 Internet 使用或完全禁止 Internet 使用。

Internet 时间限制网格允许指定以三十分钟间隔为单位的时间限制。网格的绿色部分表示用户可以访问 Internet 的日期和时间。网格的红色部分表示拒绝访问的日期和时间。如果用户在禁止期间尝试访问 Internet，则 McAfee 会通知用户，指出他们无法访问。

如果完全禁止用户访问 Internet，则此用户可以登录并使用计算机，但不能访问 Internet。

设置用户的 Internet 时间限制

您可以使用 Internet 时间限制网格指定特定用户可以访问 Internet 的时间。网格的绿色部分表示用户可以访问 Internet 的日期和时间。网格的红色部分表示拒绝访问的日期和时间。

设置用户的 Internet 时间限制：

1. 在“常见任务”下，单击“主页”。
2. 在“SecurityCenter 信息”下面，单击“配置”。
3. 在“SecurityCenter 配置”窗格上，单击“用户”下的“高级”。
4. 在“用户”窗格上，单击“家长监控”。
5. 在此列表中选择用户名。
6. 在“Internet 时间限制”下，按下并拖动以指定此用户可以访问 Internet 的日期和时间。
7. 单击“确定”。

阻止网站

如果您是管理员并要阻止所有非成人用户访问特定的网站，则可以阻止此网站。在用户尝试访问已阻止的网站时，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。

属于成人年龄组的用户（包括管理员）可以访问所有网站，即使此网站位于“阻止的网站”列表中。要测试已阻止的网站，必须以非成人用户身份登录。

作为管理员，您还可以根据网站包含的关键字阻止网站。McAfee 维护一个关键字和相应规则的默认列表，此列表确定是否允许某个年龄组的用户浏览关键字存在的网站。启用关键字扫描后，则使用关键字的默认列表为用户评级内容。不过，您可以将自己的允许关键字添加到默认列表中，并将其与某些年龄组关联。您添加的关键字规则会覆盖可能与默认列表中匹配关键字相关联的规则。您可以查找现有的关键字或指定新关键字，以将其与某些年龄组关联。

阻止网站

如果要禁止所有非成人用户访问某个网站，则可以阻止此网站。如果有用户尝试访问此网站，则会显示一条消息，指出 McAfee 已阻止此网站。

阻止网站：

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，单击“配置”。
4. 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”。
5. 在“阻止的网站”窗格下的“http://”框中键入网站的地址，然后单击“添加”。
6. 单击“确定”。

修改阻止的网站

如果网站的地址发生变化，或在您将其添加到“阻止的网站”列表中时输入错误，则可以修改它。

修改阻止的网站：

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，单击“配置”。
4. 在“家长监控配置”窗格上，单击“高级”。
5. 在“阻止的网站”窗格上，单击“阻止的网站”列表中的条目，修改“http://”框中的网站地址，然后单击“更新”。
6. 单击“确定”。

删除阻止的网站

如果不再希望阻止某个网站，必须从“阻止的网站”列表中将其删除。

删除阻止的网站：

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，单击“配置”。
4. 在“家长监控配置”窗格上，单击“高级”。
5. 在“阻止的网站”窗格上，单击“阻止的网站”列表中的条目，然后单击“删除”。
6. 在“确认删除”对话框中，单击“是”。
7. 单击“确定”。

禁用关键字扫描

默认情况下启用关键字扫描，这表明使用 McAfee 的默认关键字列表为用户评级内容。尽管您可以随时禁用关键字扫描，但 McAfee 建议不要这样做。

禁用关键字扫描：

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，单击“配置”。

4 在“家长监控配置”窗格上，单击“高级”。

5 在“全局家长监控”窗格上，单击“关键字扫描”。

6 在“关键字扫描”窗格上，单击“关”。

7 单击“确定”。

根据关键字阻止网站

如果要根据网站的内容阻止网站，但不了解特定的站点地址，则可以根据其关键字来阻止网站。只需输入关键字，然后确定哪些年龄组可以和不可以浏览包含此关键字的网站。

根据关键字阻止网站：

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，单击“配置”。

4 在“家长监控配置”窗格上，单击“高级”。

5 在“全局家长监控”窗格上，单击“关键字扫描”，并确保启用了关键字扫描。

6 在“全局家长监控”窗格上，单击“关键字”。

7 在“查找”框中键入关键字。
系统将阻止包含这个单词的网站。

8 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。

9 单击“确定”。

允许网站

如果您是管理员，则可以允许所有用户访问特定的网站，覆盖任何默认设置及阻止的网站。

有关已阻止网站的信息，请参阅阻止网站 (第 218 页)。

允许网站

如果要确保没有为任何用户阻止某个网站，可以将此网站的地址添加到“允许的网站”列表中。在将网站添加到“允许的网站”列表中后，您会覆盖任何默认设置和已添加到“阻止的网站”列表中的网站。

允许网站：

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，单击“配置”。
4. 在“家长监控配置”窗格上，单击“高级”。
5. 在“全局家长监控”窗格上，单击“允许的网站”。
6. 在“允许的网站”窗格上的“http://”框中键入网站的地址，然后单击“添加”。
7. 单击“确定”。

提示：您可以禁止用户浏览“允许的网站”列表中未包含的任何网站。有关详细信息，请参阅设置用户的内容评级组 (第 212 页)。

修改允许的网站

如果网站的地址发生变化，或在您将其添加到“允许的网站”列表中时输入错误，则可以修改它。

修改允许的网站：

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，单击“配置”。
4. 在“家长监控配置”窗格上，单击“高级”。
5. 在“全局家长监控”窗格上，单击“允许的网站”。
6. 在“允许的网站”窗格上，单击“允许的网站”列表中的条目，修改“http://”框中的地址，然后单击“更新”。
7. 单击“确定”。

删除允许的网站

您可以随时删除允许的网站。根据您的设置，在删除“允许的网站”列表中的网站后，McAfee 用户可能无法再访问此网站。

删除允许的网站：

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，单击“配置”。
4. 在“家长监控配置”窗格上，单击“高级”。
5. 在“全局家长监控”窗格上，单击“允许的网站”。
6. 在“允许的网站”窗格上，单击“允许的网站”列表中的条目，然后单击“删除”。
7. 在“确认删除”对话框中，单击“是”。
8. 单击“确定”。

允许网站设置 Cookie

如果阻止所有网站读取其在计算机上设置的 Cookie，或配置某些用户在接受 Cookie 之前接收消息提示，然后发现某些网站不能正常运行，则可以允许这些网站读取其 Cookie。

有关 Cookie 和 Cookie 拦截级别的详细信息，请参阅设置用户的 Cookie 拦截级别 (第 213 页)。

允许网站设置 Cookie

如果阻止所有网站读取其在计算机上设置的 Cookie，或配置某些用户在接受 Cookie 之前接收消息提示，然后发现某些网站不能正常运行，则可以允许这些网站读取其 Cookie。

允许网站设置 Cookie：

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，单击“配置”。
4. 在“家长监控配置”窗格上，单击“高级”。
5. 在“全局家长监控”窗格上，单击“Cookie”。
6. 在“Cookie”窗格上的“http://”框中键入网站的地址，然后单击“添加”。
7. 单击“确定”。

修改接受的 Cookie 列表

如果网站的地址发生变化，或在您将其添加到“接受 Cookie”列表中时输入错误，则可以修改它。

修改 Cookie 列表：

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，单击“配置”。
4. 在“家长监控配置”窗格上，单击“高级”。
5. 在“全局家长监控”窗格上，单击“Cookie”。
6. 在“Cookie”窗格上，单击“接受 Cookie”列表中的条目，修改“http://”框中的地址，然后单击“更新”。
7. 单击“确定”。

禁止网站设置 Cookie

如果要禁止特定的网站读取它在您计算机上设置的 Cookie，可以将其从“接受 Cookie”列表中删除。

禁止网站设置 Cookie：

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，单击“配置”。
4. 在“家长监控配置”窗格上，单击“高级”。
5. 在“全局家长监控”窗格上，单击“Cookie”。
6. 在“Cookie”窗格上，单击“接受 Cookie”列表中的条目，然后单击“删除”。
7. 在“确认删除”对话框中，单击“是”。
8. 单击“确定”。

阻止可能不良的 Web 图像

通过在浏览 Internet 时阻止显示可能不良的图像，可以保护家庭成员。可以为所有用户阻止图像，也可以为除成人年龄组成员外的所有用户阻止图像。有关年龄组的详细信息，请参阅设置用户的内容评级组 (第 212 页)。

默认情况下，系统会为除成人年龄组的成员外的所有用户启用图像分析；不过，如果您是管理员，则可以随时禁用图像分析。

阻止可能不良的图像

默认情况下，McAfee 启用图像分析，它通过在浏览 Internet 时阻止可能不良的图像来保护您的家人。如果 McAfee 检测到可能不良的图像，它会用自定义图像替换此图像，指出已阻止最初的图像。如果要禁用图像分析，则您必须是管理员。

阻止可能不良的图像：

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，单击“配置”。
4. 在“家长监控配置”窗格上，单击“高级”。
5. 在“全局家长监控”窗格上，单击“图像分析”。
6. 在“图像分析”窗格上，执行以下任一操作：
   - 单击“所有用户”以为所有用户阻止可能不良的图像。
   - 单击“青少年和儿童”，为除成人年龄组成员外的所有用户阻止可能不良的图像。
7. 单击“确定”。

第 35 章

保护 Internet 的信息

使用 Privacy Service 可以在浏览 Internet 时保护家庭成员和个人信息。例如，如果您是管理员，则可以配置 McAfee 在用户浏览 Internet 时阻止广告、弹出窗口和 Web 错误。您还可以通过将个人信息添加到阻止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 Internet 上传输。

本章内容

阻止广告、弹出窗口和 Web 错误

如果您是管理员，则可以配置 McAfee 在用户浏览 Internet 时阻止广告、弹出窗口和 Web 错误。阻止广告和弹出窗口会防止在 Web 浏览器中显示大多数广告和弹出窗口。这有助于提高您浏览 Internet 时的速度和效率。阻止 Web 错误会防止网站跟踪您的在线活动以及将信息发给未经授权的来源。Web 错误（也称为 Web 信标、像素标记、透明 GIF 或不可见 GIF）是小型图像文件，可以将自身嵌在 HTML 页面中，并允许未经授权的来源在您计算机上设置 Cookie。然后，这些 Cookie 可以将信息传输到未经授权的来源。

默认情况下，系统会在您的计算机上阻止广告、弹出窗口和 Web 错误。如果您是管理员，则可以随时允许广告、弹出窗口或 Web 错误。

阻止广告

您可以在用户访问 Internet 时阻止显示广告。

阻止广告：

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，单击“配置”。
4. 在“Internet 和网络配置”窗格上，单击“Web 浏览防护”下的“高级”。
5. 在“广告、弹出窗口和 Web 错误阻止”窗格上，选中“在您浏览 Internet 时，阻止网页上显示的广告”复选框。
6. 单击“确定”。

阻止弹出窗口

您可以阻止弹出窗口在用户访问 Internet 时显示。

阻止弹出窗口：

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，单击“配置”。
4. 在“Internet 和网络配置”窗格上，单击“Web 浏览防护”下的“高级”。
5. 在“广告、弹出窗口和 Web 错误阻止”窗格上，选中“在您浏览 Internet 时，阻止显示弹出窗口”复选框。
6. 单击“确定”。

阻止 Web 错误

Web 错误（也称为 Web 信标、像素标记、透明 GIF 或不可见 GIF）是小型图像文件，可以将自身嵌在 HTML 页面中，并允许未经授权的来源在您计算机上设置 Cookie。然后，这些 Cookie 可以将信息传输到未经授权的来源。您可以通过阻止 Web 错误防止其加载到您的计算机上。

阻止 Web 错误：

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，单击“配置”。
4. 在“Internet 和网络配置”窗格上，单击“Web 浏览防护”下的“高级”。
5. 在“广告、弹出窗口和 Web 错误阻止”窗格上，选择“在此计算机上阻止 Web 错误”。
6. 单击“确定”。

阻止个人信息

通过将个人信息添加到阻止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 Internet 上传输。当 McAfee 在要发送的内容中检测个人身份信息时，会发生以下情况：

- 如果您是管理员，则会提示您确认是否要发送信息。
- 如果您不是管理员，则会用星号 (*) 替换已阻止的信息。例如，如果发送电子邮件 Lance Armstrong wins tour，且 Armstrong 设置为要阻止的个人信息，则发送的电子邮件是 Lance ********* wins tour。

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”。

阻止个人信息

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”。

阻止个人信息：

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，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”。
5. 在“已阻止的信息”窗格上，单击“添加”。
6. 在列表中选择要阻止的信息类型。
7. 输入个人信息，然后单击“确定”。
8. 在“个人信息保护”对话框中，单击“确定”。

第 36 章

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 McAfee 管理员或系统管理员）访问它们。

本章内容

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。只有了解此密码的用户能访问密码存储库。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。

将密码添加到密码存储库

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。

将密码添加到密码存储库：

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，单击“配置”。
4. 在“Internet 和网络配置”窗格上，单击“个人信息保护”下的“高级”。
5. 在“个人信息保护”窗格上，单击“密码存储库”。
6. 在“密码”框中键入密码存储库密码，然后在“确认密码”框中重新键入此密码。
7. 单击“打开”。
8. 在“密码存储库”窗格上，单击“添加”。
9. 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。
10. 单击“添加”，然后单击“确定”。

修改密码存储库中的密码

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。

修改密码存储库中的密码：

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，单击“配置”。

4 在“Internet 和网络配置”窗格上，单击“个人信息保护”下的“高级”。

5 在“个人信息保护”窗格上，单击“密码存储库”。

6 在“密码”框中键入密码存储库密码。

7 单击“打开”。

8 在“密码存储库”窗格中，单击密码条目，然后单击“编辑”。

9 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。

10 单击“添加”，然后单击“确定”。

删除密码存储库中的密码

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。

删除密码存储库中的密码：

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，单击“配置”。

4 在“Internet 和网络配置”窗格上，单击“个人信息保护”下的“高级”。

5 在“个人信息保护”窗格上，单击“密码存储库”。

6 在“密码”框中键入密码存储库密码。

7 单击“打开”。

8 在“密码存储库”窗格中，单击密码条目，然后单击“删除”。

9 在“确认删除”对话框中，单击“是”。

10 单击“确定”。

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。

重置密码存储库密码：

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”信息窗格，单击“配置”。
4. 在“Internet 和网络配置”窗格上，单击“个人信息保护”下的“高级”。
5. 在“个人信息保护”窗格上，单击“密码存储库”。
6. 在“重置密码存储库”下的“密码”框中键入新密码，然后在“确认密码”框中重新键入此密码。
7. 单击“重置”。
8. 在“确认重置密码”对话框中，单击“是”。

第 37 章

McAfee Data Backup

使用 Data Backup 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，可以避免数据意外丢失。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。

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

本章内容

功能

Data Backup 提供以下功能来保存和还原您的照片、音乐和其他重要文件。

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。初次存档之后，系统会自动进行增量存档。

一次单击还原

如果错误删除了或损坏了您计算机上的文件和文件夹，则可以从使用的存档介质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。

第 38 章

存档文件

您可以使用 McAfee Data Backup 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。

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 Data Backup 运行完全存档或快速存档的频率的默认设置。您可以随时运行手动存档。

本章内容

设置存档选项

开始存档数据之前，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，Data Backup 会监视其中是否存在新文件或文件更改。监视文件类型是在监视位置上 Data Backup 存档的文件类型（如 .doc、.xls 等）。默认情况下，Data Backup 会监视存储在监视位置上的所有文件类型。

您可以设置两种类型的监视位置：深层监视位置和浅层监视位置。如果设置深层监视位置，Data Backup 会存档此文件夹及其子文件夹内的监视文件类型。如果设置浅层监视位置，Data Backup 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 My Documents 位置设成深层监视位置。

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：深层监视位置和浅层监视位置。如果设置深层监视位置，Data Backup 会监视文件夹及其子文件夹中的内容是否有更改。如果设置浅层监视位置，Data Backup 仅监视此文件夹（不包含其子文件夹）的内容是否有更改。

在存档中包含位置：

1 单击“本地存档”选项卡。

2 在左侧窗格中，单击“设置”。

3 在“本地存档设置”对话框中，单击“监视位置”。

4 执行以下任一操作：

- 要存档文件夹的内容（包括其子文件夹的内容），请单击“深层监视位置”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“浅层监视位置”下的“添加文件夹”。

5 在“浏览文件夹”对话框中，导航到要监视的文件夹，然后单击“确定”。

6 单击“保存”。

提示：如果要 Data Backup 监视尚未创建的文件夹，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设置为监视位置。

设置存档文件类型

您可以指定在深层监视位置或浅层监视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。

设置存档文件类型：

1 单击“本地存档”选项卡。

2 在左侧窗格中，单击“设置”。

3 在“本地存档设置”对话框中，单击“文件类型”。

4 展开文件类型列表，并选中要存档的文件类型旁的复选框。

5 单击“保存”。

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，然后单击“添加”。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。

从存档中排除位置：

1 单击“本地存档”选项卡。

2 在左侧窗格中，单击“设置”。

3 在“本地存档设置”对话框中，单击“监视文件夹”。

4 单击“已排除监视的位置”下的“添加文件夹”。

5 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”。

6 单击“保存”。

提示：如果要 Data Backup 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

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。

更改存档位置：

1 单击“本地存档”选项卡。

2 在左侧窗格中，单击“设置”。

3 单击“更改存档位置”。

4 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”列表中的 CD 或 DVD 驱动器，然后单击“保存”。
- 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，进行选择，然后单击“确定”。

5 验证“所选的存档位置”下的新存档位置，然后单击“确定”。

6 在确认对话框中，单击“确定”。

7 单击“保存”。

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访问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。

禁用存档加密和压缩：

1 单击“本地存档”选项卡。

2 在左侧窗格中，单击“设置”。

3 在“本地存档设置”对话框中，单击“高级设置”。

4 清除“启用加密功能以提高安全性”复选框。

5 清除“启用压缩功能以减少存储空间”复选框。

6 单击“保存”。

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。运行完全存档时，会根据已设置的监视文件类型和位置对全部数据集进行存档。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，Data Backup 的计划是在每周一的上午 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 Data Backup 在数小时内运行完全存档或快速存档，则您可以手动存档该文件。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。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。

计划自动存档：

1. 单击“本地存档”选项卡。
2. 在左侧窗格中，单击“设置”。
3. 在“本地存档设置”对话框中，单击“常规”。
4. 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
5. 选择要运行完全存档的日旁的复选框。
6. 单击“于”列表中的值，以指定要运行完全存档的时间。
7. 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

8 在“快速存档频率”框中键入表示频率的数字。

9 单击“保存”。

中断自动存档

Data Backup 会根据您定义的计划自动存档监视位置上的文件。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。

中断自动存档：

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。

手动运行快速存档或完全存档：

1 单击“本地存档”选项卡。

2 要运行快速存档，请单击左侧窗格中的“快速存档”。

3 要运行完全存档，请单击左侧窗格中的“完全存档”。

4 在“准备开始存档”对话框中，检查您的存储空间和设置，然后单击“继续”。

第 39 章

处理已存档的文件

在文件存档后，可以使用 Data Backup 对其进行处理。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。您还可以在资源管理器视图中直接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。Data Backup 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

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。

找到文件后，可以在本地存档资源管理器中直接将其打开。Data Backup 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）。

排序已存档的文件：

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，则通过搜索此文件可以快速找到它。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。

搜索已存档的文件：

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“<100 KB”、“<1 MB”或“>1 MB”。
- 单击“大小(KB)”，然后从框中选择适当的大小值。

4 通过执行以下任一项，指定上次联机备份文件的大致日期：

- 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。

打开已存档的文件：

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 McAfee Data Backup 并连接上外部硬盘驱动器。然后，在 Data Backup 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 Data Backup 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。

从本地存档检索缺少的文件：

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。

从本地存档还原较旧版本的文件：

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 ddmmyy_hh-mm-ss_***，其中 ddmmyy 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。

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。

从“缺少的文件”列表中删除文件：

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。

查看备份活动的摘要：

1 单击“本地存档”选项卡。

2 在屏幕的顶部，单击“帐户摘要”。

第 40 章

McAfee Wireless Network Security

Wireless Network Security 通过易用而直观的一次单击界面，提供行业标准的自动防护，以防数据窃取、未经授权的网络访问和宽带的盗用。Wireless Network Security 会加密通过 Wi-Fi 发送的个人和隐私数据，并会阻止黑客访问您的无线网络。

Wireless Network Security 通过以下方法阻止黑客攻击您的无线网络：

- 阻止 Wi-Fi 网络的未经授权的连接
- 防止捕获通过 Wi-Fi 网络传输的数据
- 检测对 Wi-Fi 网络的连接尝试

Wireless Network Security 会将易用的功能（如即时网络锁定和将合法用户快速添加到网络的能力）与强大的安全功能（如自动密钥生成和计划密钥轮替）结合在一起。

本章内容

功能

Wireless Network Security 提供以下功能。

全天候防护

Wireless Network Security 会自动检测和保护您所连接到的任何有漏洞的无线网络。

直观界面

不用进行困难的决定或了解复杂的术语即可保护您的网络。

强自动加密

只允许您的朋友和家人访问您的网络，并在发送和接收数据时提供保护。

仅软件解决方案

Wireless Network Security 可以与标准的无线路由器或接入点以及安全软件一起使用。您无须购买额外的硬件。

自动密钥轮替

因为密钥会自动轮替，所以，即使最有决心的黑客也不能捕获您的信息。

添加网络用户

您可以轻松授予您的朋友和家人对您网络的访问权限。您可以通过无线方式或通过 USB 驱动器传输软件来添加用户。

直观的连接工具

无线连接工具既直观又提供丰富的信息，其中包含有关信号强度和安全状态的详细信息。

事件记录和警报

易于理解的报告和警报会向高级用户提供有关无线网络的更多信息。

暂停模式

临时暂停密钥轮替，这样特定的应用程序可以运行而不会中断。

与其他设备兼容

Wireless Network Security 会用大多数常用品牌的最新无线路由器或接入点模块自动更新，这些品牌有：Linksys®、NETGEAR®、D-Link®、Belkin®、TRENDnet® 和其他。

启动 Wireless Network Security

Wireless Network Security 在安装后会自动启用；您无须手动启动它。不过，您可以选择手动启用和禁用无线防护。

安装 Wireless Network Security 后，计算机会尝试建立指向无线路由器的连接。建立连接后，计算机会安排将密钥输入到无线路由器中。如果更改了默认密码，系统会提示您输入密码，这样 Wireless Network Security 便可以使用共享密钥和强安全模式配置无线路由器。您的计算机也使用相同的共享密钥和加密模式进行配置，以便建立安全的无线连接。

启动 Wireless Network Security

默认情况下启用 Wireless Network Security；不过，您可以手动启用和禁用无线防护。

启用无线防护可以防止黑客侵入您的无线网络并拦截数据。但是，如果连接到外部无线网络，则防护将随网络安全级别的不同而不同。

手动启用无线防护：

1 在“McAfee SecurityCenter”窗格上，执行以下任一操作：

- 单击“Internet 和网络”，然后单击“配置”。
- 单击“高级菜单”，单击“主页”窗格上的“配置”，然后指向“Internet 和网络”。

2 在“Internet 和网络配置”窗格的“无线防护”下，单击“开”。

注意：如果安装了兼容的无线适配器，则会自动启用 Wireless Network Security。

停止 Wireless Network Security

默认情况下启用 Wireless Network Security；不过，您可以手动启用和禁用无线防护。

禁用无线防护会使网络易遭入侵和数据拦截。

禁用无线防护：

1 在“McAfee SecurityCenter”窗格上，执行以下任一操作：

- 单击“Internet 和网络”，然后单击“配置”。

- 单击“高级菜单”，单击“主页”窗格上的“配置”，然后指向“Internet 和网络”。

2 在“Internet 和网络配置”窗格的“无线防护”下，单击“关”。

第 41 章

保护无线网络

Wireless Network Security 通过实现无线加密（根据不同的设备使用 WEP、WPA 或 WPA2）来保护您的网络。它会使用有效的密钥凭证自动安排客户端和无线路由器，这样无线路由器便会自动授权计算机进行连接。使用加密方法保护的无线网络会阻止未经授权的用户访问无线网络，并保护通过无线网络发送的数据。Wireless Network Security 通过以下方法实现这一点：

- 创建和分发较长、难于破解、随机和共享的密钥。
- 按计划轮替密钥
- 使用密钥配置每个无线设备

本章内容

设置受保护的无线网络

安装 Wireless Network Security 后，它会自动提示您保护连接到的不安全无线网络，或加入以前受保护的无线网络。

如果您未连接到无线网络，则 Wireless Network Security 会扫描受 McAfee 保护且信号较强的网络，并提示用户加入此网络。如果没有可用的受保护网络，则 Wireless Network Security 会扫描信号较强的不安全网络，发现此网络后，系统会提示您保护此网络。

除非无线网络已受 McAfee Wireless Network Security 保护，否则即使这些网络使用无线安全机制（如 WEP 和 WPA），McAfee 也会将这些无线网络视作“未受保护的网络”。

除非无线网络受 Wireless Network Security 的保护，否则即使此网络使用无线安全机制（如 WEP 和 WPA），McAfee 也会将此网络视作未受保护的网络。

关于访问类型

安装了 Wireless Network Security 的任何无线计算机都可以创建受保护的无线网络。保护路由器并创建受保护无线网络的第一台计算机会自动被授予对此网络的管理访问权限。具有管理访问权限的现有计算机可以授予稍后加入的计算机管理、完全或来宾访问权限。

具有管理和完全访问权限类型的计算机可以执行以下任务：

- 保护和删除路由器或接入点
- 轮替安全密钥
- 更改网络安全设置
- 修复网络
- 授予计算机对网络的访问权限
- 撤销对受保护无线网络的访问权限
- 更改计算机的管理级别

网络上具有来宾访问权限类型的计算机可以执行以下任务：

- 连接到网络
- 加入网络
- 修改特定于来宾计算机的设置

注意：计算机可以在一个无线网络上具有管理访问权限，而在另一个无线网络上具有来宾或完全访问权限。在网络上具有来宾或完全访问权限的计算机可以创建新网络。

相关主题

- 加入受保护的无线网络 (第 260 页)
- 授予计算机管理访问权限 (第 264 页)
- 撤销网络访问权限 (第 278 页)

创建受保护的无线网络

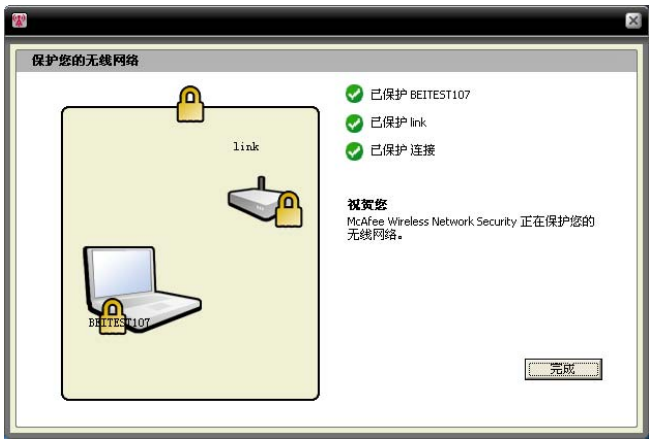
要创建受保护的无线网络，首先必须添加无线网络的无线路由器或接入点。

添加无线路由器或接入点：

1. 右键单击 Windows 通知区域中的 Wireless Network Security 图标。
2. 选择“查看工具”。
3. 在“保护工具”窗格的“保护无线路由器/接入点”下，单击“保护”。
4. 在“保护无线路由器/接入点”窗格上，选择要保护的无线网络，然后单击“保护”。

在 Wireless Network Security 尝试保护您的计算机、路由器和网络连接时，会显示“保护您的无线网络”窗格。

对所有这些组件的成功保护会完全保护您的无线网络。



5 单击“完成”。

注意：在保护网络后，会显示“下一步”对话框，提醒您在每个无线计算机上安装 Wireless Network Security，从而使这些计算机加入网络。

如果以前为路由器或接入点手动配置了预共享密钥，并在尝试保护路由器或接入点时没有连接到网络，则还必须在“WEP 密钥”框中输入密钥，然后单击“连接”。如果您以前更改了无线路由器的管理用户名或密码，则系统会提示您输入此信息，然后才能保护路由器或接入点。

相关主题

- 保护其他无线设备 (第 265 页)
- 将计算机添加到受保护的无线网络 (第 267 页)

加入受保护的无线网络

受保护的网络会防止黑客拦截通过网络传输的数据以及连接到您的网络。在授权计算机可以访问受保护的无线网络之前，必须先加入网络。

在计算机请求加入托管网络时，会将一条消息发给网络上具有管理权限的其他计算机。作为管理员，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。

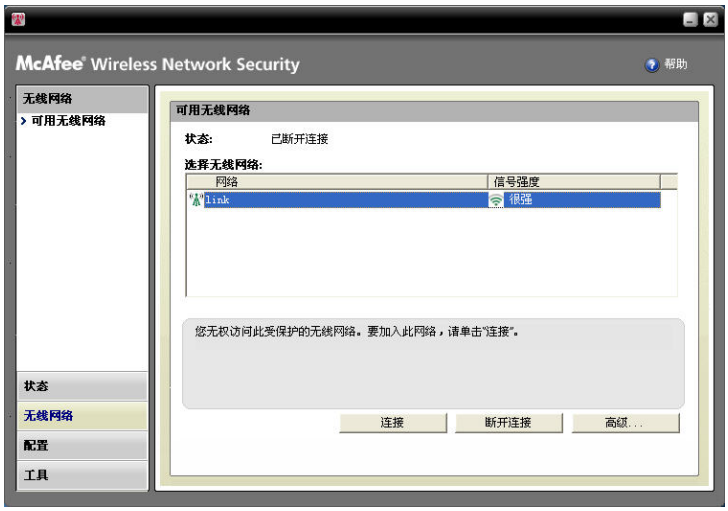
在可以加入受保护的网络之前，必须安装 Wireless Network Security，然后连接到受保护的无线网络。受保护无线网络上具有管理权限的现有网络用户必须允许您加入。在加入网络后，重新连接时无须重新加入。授予方和加入方必须具有有效的无线连接。授予方必须是连接到网络的管理员计算机。

加入受保护的无线网络：

1 在受保护的计算机上，右键单击 Windows 通知区域中的 Wireless Network Security 图标。

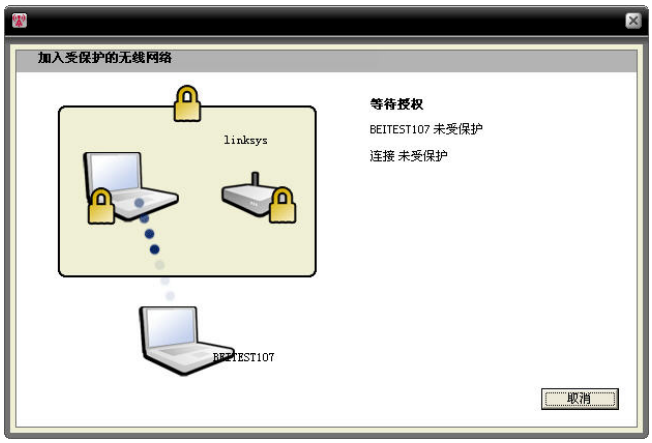
2 选择“查看无线网络”。

3 在“可用无线网络”窗格上，选择网络，然后单击“连接”。



4 在“加入受保护的无线网络”对话框上，单击“是”加入网络。

在 Wireless Network Security 尝试请求权限以加入网络时，会在尝试加入网络的计算机上显示“加入受保护的无线网络”窗格。



5 在管理员计算机上显示“加入网络”窗格，可以在此授予来宾、完全或管理访问权限。

在“加入网络”对话框上，选择以下任一选项：

授予来宾访问权限	允许计算机使用 McAfee EasyNetwork 将文件发给无线网络上的其他计算机，但不与这些计算机共享文件。
授予对所有托管网络应用程序的完全访问权限	允许计算机使用 McAfee EasyNetwork 发送和共享文件。
授予对所有托管网络应用程序的管理访问权限：	允许计算机使用 McAfee EasyNetwork 发送和共享文件，将访问权限授予其他计算机，以及调整无线网络上其他计算机的访问权限级别。

6 单击“授予访问权限”。

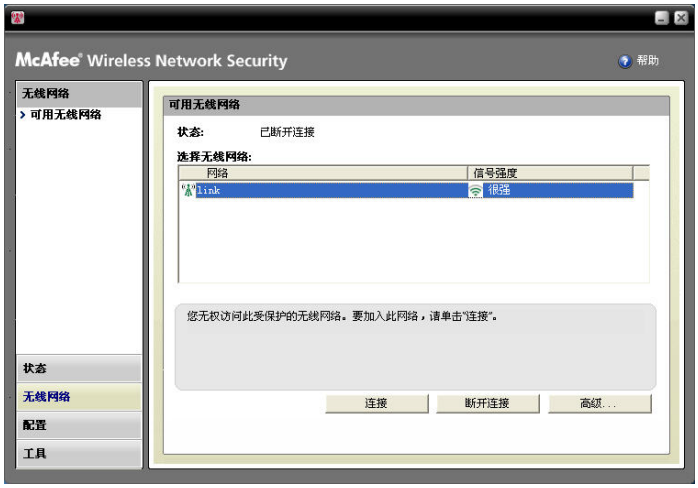
7 确认“授予网络访问权限”窗格上显示的卡与尝试加入无线网络计算机上显示的卡相同。如果卡匹配，请单击“授予访问权限”。

如果计算机没有显示相同的图片，则会出现可能的安全隐患。授予此计算机访问网络的权限会使您的计算机面临风险。要禁止计算机访问无线网络，请单击“拒绝访问”。

8 “授予网络访问权限”窗格会确认新计算机受 Wireless Network Security 的保护。要监视其他计算机的安全设置以及其他计算机监视的安全设置，请选择“允许此计算机与此网络上的其他计算机互相监视各自的安全设置”。

9 单击“完成”。

10 “可用无线网络”窗格会显示您已连接到受保护的无线网络。



相关主题

- 将计算机添加到受保护的无线网络 (第 267 页)

连接到受保护的无线网络

如果您已加入受保护的无线网络，但稍后断开连接且没有撤销访问权限，则可以随时重新连接而无须重新加入。

连接到受保护的无线网络:

1 右键单击 Windows 通知区域中的 Wireless Network Security 图标。

2 选择“查看无线网络”。

3 在“可用无线网络”窗格上，选择网络，然后单击“连接”。

授予计算机管理访问权限

具有管理权限的计算机可以保护无线路由器、更改安全模式并授予新计算机访问此受保护无线网络的权限。

配置管理访问权限：

1 右键单击 Windows 通知区域中的 Wireless Network Security 图标。

2 选择“查看配置”。

3 在“配置”窗格上，单击“管理设置”。

4 在“无线管理选项”窗格上，选择“是”或“否”，以允许或禁用管理访问权限。

5 单击“应用”。

相关主题

- 关于访问类型 (第 257 页)
- 撤销网络访问权限 (第 278 页)

保护其他无线设备

Wireless Network Security 允许将一个或多个无线打印机、打印服务器或游戏控制台添加到网络。

添加无线打印机、打印服务器或游戏控制台：

1. 右键单击 Windows 通知区域中的 Wireless Network Security 图标。
2. 选择“查看工具”。
3. 在“保护工具”窗格的“保护非接入点设备”下，单击“保护”。
4. 在“保护无线设备”窗格上，选择无线网络，然后单击“保护”。
5. “已保护非接入点设备”警报会确认已将设备添加到网络。

连接到禁用广播 SSID 的网络

您可以连接到禁用广播 SSID 的无线网络。路由器禁用广播 SSID 后，不会显示在“可用无线网络”窗格上。

McAfee 建议不要使用 Wireless Network Security 保护已禁用广播 SSID 的无线路由器。

连接到禁用广播 SSID 的无线网络：

1. 右键单击 Windows 通知区域中的 Wireless Network Security 图标。
2. 选择“查看无线网络”。
3. 在“可用无线网络”窗格上，单击“高级”。
4. 在“无线网络”窗格上，单击“添加”。
5. 在“添加无线网络”窗格上，指定以下设置，然后单击“确定”：

设置	描述
网络	网络的名称。如果在修改网络，则无法更改此名称。
安全设置	未受保护网络的安全。注意，如果无线适配器不支持所选的模式，则无法进行连接。安全模式包括：已禁用、开放 WEP、共享 WEP、自动 WEP、WPA-PSK 和 WPA2-PSK。
加密模式	与所选安全模式相关联的加密。加密模式包括：WEP、TKIP、AES 和 TKIP+AES。

注意：McAfee 建议不要使用 Wireless Network Security 保护已禁用广播 SSID 的无线路由器。如果必须使用此功能，只能在禁用广播 SSID 后使用。

将计算机添加到受保护的无线网络

您可以使用可移动设备（如 USB 闪存驱动器和可写 CD）或 Windows Connect Now 技术将计算机添加到受保护的无线网络。

使用可移动设备添加计算机

Wireless Network Security 允许使用 USB 闪存驱动器或可写 CD，将其他计算机添加到没有运行 Wireless Network Security 的受保护的无线网络。

添加计算机：

1. 右键单击 Windows 通知区域中的 Wireless Network Security 图标。
2. 选择“查看工具”。
3. 在“保护工具”窗格的“保护计算机”下，单击“保护”。
4. 在“保护其他计算机”窗格上，选择“将 Wireless Network Security 复制到可移动设备，如 USB Key 设备”。

5. 选择要复制 Wireless Network Security 的 CD 驱动器或 USB 闪存驱动器的位置。
6. 单击“复制”。
7. 在将所有文件复制到 CD 或 USB 闪存驱动器后，将可移动设备插入要保护的计算机。如果程序不会自动启动，请在 Windows 资源管理器中浏览可移动媒体的内容，然后单击“Install.exe”。
8. 按照屏幕上的说明执行操作。

注意：您还可以使用 Windows Connect Now 技术将计算机连接到受保护的无线网络。

相关主题

- 使用 Windows Connect Now 技术添加计算机 (第 268 页)

使用 Windows Connect Now 技术添加计算机

Wireless Network Security 允许使用 Windows Connect Now 技术将其他计算机添加到未运行 Wireless Network Security 的网络。

使用 Windows Connect Now 技术添加计算机：

1. 右键单击 Windows 通知区域中的 Wireless Network Security 图标。
2. 选择“查看工具”。
3. 在“保护工具”窗格的“保护计算机”下，单击“保护”。
4. 在“保护其他计算机”窗格上，选择“创建 Windows Connect Now 磁盘”
5. 选择要复制 Windows Connect Now 信息的位置。
6. 单击“复制”。
7. 将 Windows Connect Now 磁盘插入要保护的计算机
8. 如果磁盘没有自动启动，请执行以下操作：
   - 安装 Wireless Connect Now 技术：在 Windows 任务栏中，单击“开始”，然后单击“控制面板”。如果使用控制面板的分类视图，请单击“网络和 Internet 连接”，然后单击“无线网络安装向导”。如果使用控制面板的经典视图，请单击“无线网络安装向导”。按照屏幕上的说明执行操作。
   - 在 Windows 连接磁盘上打开“setupSNK.exe”，并将密钥复制并粘贴到无线网络选择客户端。

注意：如果使用 Windows 连接技术连接到无线网络，请暂停密钥轮替，否则网络连接将失败。连接失败原因是，密钥轮替创建的新密钥与 Windows Connect Now 技术所使用的密钥不同。

您还可以使用可移动设备（如可写 CD 或 USB 闪存驱动器）将计算机添加到受保护的无线网络。

相关主题

- 使用可移动设备添加计算机 (第 267 页)

第 42 章

管理无线网络

Wireless Network Security 提供一组完整的管理工具帮助您管理和维护无线网络。

本章内容

管理无线网络

在您连接到受保护的无线网络时，系统会加密发送和接收的信息。黑客无法解密通过受保护网络传输的数据，并且无法连接到您的网络。Wireless Network Security 提供许多工具，帮助您管理网络以防将来的入侵。

关于 Wireless Network Security 图标

Wireless Network Security 显示一些图标，用于表示各种网络连接类型和信号强度。

网络连接图标

下表介绍 Wireless Network Security 在“无线网络状态”窗格以及“保护工具”和“可用无线网络”窗格中最常使用的图标。图标表示各种网络连接和安全状态。

图标	状态窗格	保护窗格
	计算机连接到所选受保护无线网络。	设备由 Wireless Network Security 保护。
	计算机可以访问受保护的无线网络，但当前并未连接。	设备使用 WEP 或 WPA 安全。
	计算机以前是受保护无线网络的成员，但在计算机断开与网络的连接后被撤销了访问权限。	设备禁用了 Wireless Network Security。

信号强度图标

下表介绍 Wireless Network Security 最常用的表示各网络信号强度的图标。

图标	描述
	信号强度非常强
	信号强度很强
	信号强度强
	信号强度低

相关主题

- 查看网络的信号强度 (第 301 页)
- 查看当前受保护的计算机数 (第 307 页)
- 查看网络安全模式 (第 299 页)

列出首选网络

Wireless Network Security 允许指定首选无线网络。这样便可以指定计算机自动连接到的网络顺序。Wireless Network Security 会尝试连接到列表中显示的第一个网络。

此功能很有用，例如，如果在朋友的区域中，要自动连接到其无线网络可以使用此功能。您可以将其他网络上移到列表顶部。

列出首选的网络：

1. 右键单击 Windows 通知区域中的 Wireless Network Security 图标。
2. 选择“查看无线网络”。
3. 在“可用无线网络”窗格上，单击“高级”。
4. 选择要调整顺序的网络，然后单击“上移”或“下移”。

5. 单击“确定”。

相关主题

- 删除首选的无线网络 (第 272 页)

删除首选的无线网络

您可以使用 Wireless Network Security 删除首选的网络。

此功能很有用，例如，删除列表中的过时网络可以使用此功能。

删除首选的网络：

1 右键单击 Windows 通知区域中的 Wireless Network Security 图标。

2 选择“查看无线网络”。

3 在“可用无线网络”窗格上，单击“高级”。

4 在“无线网络”窗格上，选择网络，然后单击“删除”。

5 单击“确定”。

相关主题

- 列出首选网络 (第 271 页)

重命名受保护的无线网络

您可以使用 Wireless Network Security 重命名现有的受保护无线网络。

如果网络的名称与邻居使用的网络名称相似或相同，或如果要创建更易区分的唯一网络名称，则重命名网络很有用。

可能需要手动重新连接已连接到受保护无线网络的计算机，并在更改名称后通知您。

在重命名网络后，会在“保护无线路由器/接入点”窗格中显示新名称。

通知受保护的无线网络名称：

1. 右键单击 Windows 通知区域中的 Wireless Network Security 图标。
2. 选择“查看配置”。
3. 在“网络安全”窗格的“受保护的无线网络名称”框中键入新名称。
4. 单击“应用”。

   在 Wireless Network Security 更改受保护无线网络的名称时，会显示“更新网络安全设置”对话框。根据计算机的设置和信号强度，网络名称会在一分钟内得到更改。

注意：作为安全措施，McAfee 建议重命名路由器或接入点的默认 SSID。尽管 Wireless Network Security 支持默认的 SSID（如“linksys”、“belkin54g”或“NETGEAR”），但重命名 SSID 会抵御恶意接入点的威胁。

配置警报设置

Wireless Network Security 允许将警报设置配置为在某些事件发生时显示警报，例如新计算机连接到您的网络时。

配置警报行为：

1. 右键单击 Windows 通知区域中的 Wireless Network Security 图标。
2. 选择“查看配置”。
3. 单击“警报设置”。
4. 选中或清除以下一个或多个事件，然后单击“应用”：

警报设置	描述
轮替受保护的无线网络的安全密钥	在手动或自动轮替安全密钥后，会显示“已轮替安全密钥”警报。轮替密钥会保护您的网络，防止黑客尝试拦截数据或连接到您的网络。
其他受保护的计算机连接到此网络或断开与此网络的连接	在计算机连接到受保护的无线网络或从此网络断开连接后，会显示“计算机已连接”警报或“计算机已断开连接”警报。已连接计算机上的数据会立即受到保护，防止入侵和数据拦截。
授予其他计算机访问受保护的无线网络的权限	在管理员计算机允许其他计算机加入受保护的无线网络后，会显示“已授予计算机网络访问权限”警报。授予计算机对受保护网络的访问权限会防止黑客尝试拦截您的数据。
暂停或继续受保护的无线网络的密钥轮替	在手动暂停或继续密钥轮替后，会显示“已暂停密钥轮替”警报或“已继续密钥轮替”警报。密钥轮替会保护您的网络，防止黑客尝试拦截数据或连接到您的网络。
撤销所有断开连接的计算机的访问权限	在撤销未连接到网络的计算机的访问权限后，显示“已撤销访问权限”警报。断开连接的计算机必须重新加入网络。
将路由器添加到受保护的无线网络或将其从该网络中删除	在无线路由器或接入点添加到受保护的无线网络或从此网络删除后，会显示“路由器/接入点已添加到网络”警报或“已取消保护路由器/接入点”警报。
更改受保护的无线路由器的登录信息	在 Wireless Network Security 管理员更改路由器或接入点的用户名或密码后，会显示“已更改路由器/接入点登录”警报。
更改受保护的无线网络的名称或安全设置	在重命名受保护的无线网络或调整其安全设置后，会显示“已更改网络设置”警报或“已重命名网络”警报。
修复受保护的无线网络的设置	在修复网络的无线路由器或接入点的设置后，会显示“已修复网络”警报。

注意：要选中或清除所有警报设置，请单击“全选”或“全部清除”。要重置 Wireless Network Security 的警报设置，请单击“恢复默认值”。

相关主题

- 自动轮替密钥 (第 288 页)
- 加入受保护的无线网络 (第 260 页)
- 连接到受保护的无线网络 (第 263 页)
- 断开与受保护无线网络的连接 (第 277 页)
- 暂停自动密钥轮替 (第 291 页)
- 撤销网络访问权限 (第 278 页)
- 删除无线路由器或接入点 (第 276 页)
- 更改无线设备的凭证 (第 285 页)
- 重命名受保护的无线网络 (第 272 页)
- 修复网络安全设置 (第 286 页)

显示连接通知

您可以将 Wireless Network Security 配置为在计算机连接到无线网络时通知您。

连接到无线网络时显示通知：

1. 右键单击 Windows 通知区域中的 Wireless Network Security 图标。
2. 选择“查看配置”。
3. 单击“其他设置”。
4. 选择“连接到无线网络后显示通知消息”。
5. 单击“应用”。

相关主题

- 连接到受保护的无线网络 (第 263 页)

删除无线路由器或接入点

Wireless Network Security 可以从受保护的无线网络中删除一个或多个路由器或接入点。

删除无线路由器或接入点：

1. 右键单击 Windows 通知区域中的 Wireless Network Security 图标。
2. 选择“查看工具”。
3. 在“保护工具”窗格的“取消保护设备”下，单击“取消保护”。
4. 在“取消保护无线路由器/接入点”窗格上，选择要从受保护的无线网络中删除的无线路由器或接入点，然后单击“取消保护”。

5. 在“已取消保护无线路由器/接入点”对话框上单击“确定”，以确认已从网络中删除了无线路由器或接入点。

相关主题

- 创建受保护的无线网络 (第 258 页)

断开与受保护无线网络的连接

Wireless Network Security 允许计算机断开与网络的连接。

此功能很有用，例如，在计算机连接到与您网络名称相同的网络时可以使用此功能。您可以断开与网络的连接，然后重新连接到您的网络。

在您意外连接到错误的网络（由于其他接入点的信号强度很强或无线电干扰）时，此功能也非常有用。

断开与受保护无线网络的连接：

1. 右键单击 Windows 通知区域中的 Wireless Network Security 图标。
2. 选择“查看无线网络”。
3. 在“可用无线网络”窗格上，选择网络，然后单击“断开连接”。

相关主题

- 撤销网络访问权限 (第 278 页)
- 离开受保护的无线网络 (第 279 页)

撤销网络访问权限

Wireless Network Security 可以撤销未连接到网络的计算机的访问权限。系统会建立新的安全密钥轮替计划：未连接的计算机将失去对受保护无线网络的访问权限，但可以通过重新加入网络来获取此访问权限。系统将保留已连接计算机的访问权限。

例如，在访问者计算机断开连接后，可以使用 Wireless Network Security 撤销此计算机的访问权限。另外，成人可以采用对 Internet 访问权限家长监控的形式，撤销儿童使用的计算机的访问权限。还可以撤销意外授予某台计算机的访问权限。

撤销受保护网络中所有断开连接的计算机的访问权限：

1. 右键单击 Windows 通知区域中的 Wireless Network Security 图标。
2. 选择“查看工具”。
3. 在“工具”窗格上，单击“维护工具”。
4. 在“维护工具”窗格的“撤销访问权限”下，单击“撤销”。
5. 在“撤销访问权限”窗格上，单击“撤销”。
6. 在“Wireless Network Security”对话框中单击“确定”。

相关主题

- 断开与受保护无线网络的连接 (第 277 页)
- 离开受保护的无线网络 (第 279 页)

离开受保护的无线网络

您可以使用 Wireless Network Security 取消对受保护网络的访问权限。

离开网络：

1. 右键单击 Windows 通知区域中的 Wireless Network Security 图标。
2. 选择“查看配置”。
3. 在“配置”窗格上，单击“其他设置”。
4. 在“其他设置”窗格的“受保护的网络访问”下，选择要离开的网络，然后单击“离开网络”。
5. 在“断开与网络的连接”窗格上，单击“是”离开网络。

注意：离开网络后，其他用户必须在您重新加入网络之前，授予您对受保护网络的访问权限。

相关主题

- 断开与受保护无线网络的连接 (第 277 页)
- 撤销网络访问权限 (第 278 页)

第 43 章

管理无线网络安全

Wireless Network Security 提供一组完整的工具帮助您管理无线网络的安全功能。

本章内容

配置安全设置

在连接到受保护的无线网络之后，Wireless Network Security 会自动保护您的网络；不过，您可以随时配置其他安全设置。

配置安全模式

您可以指定受保护无线网络的安全模式。安全模式定义计算机与路由器或接入点之间的加密方式。

在保护网络时，系统会自动配置 WEP。不过，McAfee 建议将安全模式改为 WPA2 或 WPA-PSK AES。Wireless Network Security 最初会使用 WEP，因为所有路由器和无线网络适配器都支持此模式。但是，大多数新路由器和无线网络适配器都采用 WPA 模式，此模式会更安全。

更改受保护无线网络的安全模式：

1. 右键单击 Windows 通知区域中的 Wireless Network Security 图标。
2. 选择“查看配置”。
3. 在“网络安全”窗格上，选择要在“安全模式”框中实现的安全类型，然后单击“应用”。

下表介绍可用的安全模式：

强度	模式	描述
最弱	WEP	有线等效加密 (WEP) 是 IEEE 802.11 无线网络标准的一部分，用于保护 IEEE 802.11 无线网络。WEP 所提供的安全级别可以防止单纯的窥探行为，但通常没有 WPA-PSK 加密安全。尽管 Wireless Network Security 提供强（难于猜测且较长）密钥，但 McAfee 建议使用 WPA 安全模式。
平均	WPA-PSK TKIP	Wi-Fi 保护访问 (WPA) 是较旧版的 802.11i 安全标准。TKIP 专用于 WPA 以增强 WEP。TKIP 提供报文完整性、重建密钥机制和根据数据包的密钥混和功能
强	WPA-PSK AES	此安全模式将 WPA 和 AES 模式结合在一起。高级加密标准 (AES) 是数据块加密，由美国政府采用的一种加密标准。
较强	WPA2-PSK AES	此安全模式将 WPA 和 AES 模式结合在一起。WPA2 是批准 802.11i 安全标准的下一个进展。WPA2 使用计数器模式密码块链报文认证码协议 (CCMP)，它是一个比 TKIP 更安全、更稳定的解决方案。这是使用者所能获得的最强安全模式。
最强	WPA2-PSK TKIP+AES	此安全模式将 WPA2、AES 以及 WPA-PSK TKIP 模式结合在一起。它有较大的灵活性，这样旧无线适配器和新无线适配器都可以连接。

注意：安全模式改变后，可能需要手动重新连接。

相关主题

- 修复网络安全设置 (第 286 页)
- 查看网络安全模式 (第 299 页)

配置网络安全设置

您可以修改 Wireless Network Security 保护的网络的网络属性。此功能很有用，例如，将安全机制从 WEP 升级到 WPA 可以使用此功能。

McAfee 建议如果有警报建议修改网络安全设置，则可以这样做。

配置未受保护的网络属性：

1 右键单击 Windows 通知区域中的 Wireless Network Security 图标。

2 选择“查看无线网络”。

3 在“可用无线网络”窗格上，单击“高级”。

4 在“无线网络”窗格上，单击“属性”。

5 在“无线网络属性”窗格上，修改以下设置，然后单击“确定”：

设置	描述
网络	网络的名称。如果在修改网络，则无法更改此名称。
安全设置	受保护网络的安全。注意，如果无线适配器不支持所选的模式，则无法进行连接。安全模式包括：已禁用、开放 WEP、共享 WEP、自动 WEP、WPA-PSK 和 WPA2-PSK。
加密模式	与所选安全模式相关联的加密。加密模式包括：WEP、TKIP、AES 和 TKIP+AES。

更改无线设备的凭证

您可以在受保护无线路由器或接入点上更改设备的用户名或密码。设备的列表会显示在“受保护的无线网络设备”下。

McAfee 建议更改您的凭证，因为一个制造商制造的大多数无线设备都采用相同的登录凭证。更改登录凭证有助于防止他人访问您的无线路由器或接入点，以及更改其设置。

更改受保护无线网络设备的用户名或密码：

1. 右键单击 Windows 通知区域中的 Wireless Network Security 图标。
2. 选择“查看配置”。
3. 在“网络安全”窗格的“受保护的无线网络设备”下，选择无线网络路由器或接入点，然后单击“更改用户名或密码”。

4. 在输入登录信息后，在“Wireless Network Security”对话框上单击“确定”。

   新用户名和密码随即会显示在“受保护的无线网络设备”下。

注意：有些路由器不支持用户名，因此用户名将不会显示在“受保护的无线网络设备”下。

修复网络安全设置

如果在进行安全设置和配置时遇到问题，则可以使用 Wireless Network Security 修复路由器或接入点设置。

修复安全设置：

1. 右键单击 Windows 通知区域中的 Wireless Network Security 图标。
2. 选择“查看工具”。
3. 在“工具”窗格上，单击“维护工具”。
4. 在“修复网络安全设置”下，单击“修复”。
5. 在“修复网络安全设置”窗格上，单击“修复”。

   随即会显示 Wireless Network Security 警报，指出此网络是已修复还是尚未修复。

注意：如果网络修复尝试没有成功，请使用电缆连接到网络，然后重试。如果更改了路由器或接入点密码，则必须重新输入要连接的密码。

管理网络密钥

Wireless Network Security 会使用随机密钥生成器生成较长且难于破解的随机强密钥。使用 WEP，密钥会转换为 26 位的十六进制值（产生 104 位熵，即强度，128 位 WEP 支持的最大长度），而使用 WPA，密钥是 63 个字符的 ASCII 字符串。每个字符包含 64 个可能值（6 位），产生 384 位的熵，这超出了 256 位的 WAP 密钥长度。

管理网络密钥时，可以为非保护接入点以纯文本或星号的形式显示密钥，丢弃非保护接入点的保存密钥，启用或禁用密钥轮替，更改密钥轮替频率，手动轮替密钥以及暂停密钥轮替。

自动轮替密钥后，因为密钥会一直变化，所以黑客工具无法捕获您的信息。

不过，如果连接到 Wireless Network Security 不支持的无线设备（如将无线手持计算机连接到网络），则必须记下密钥，停止密钥轮替，然后在设备上输入密钥。

查看当前密钥

使用 Wireless Network Security 可以快速访问无线安全信息，包括受保护无线网络的当前密钥。

查看当前密钥：

1. 右键单击 Windows 通知区域中的 Wireless Network Security 图标。
2. 选择“查看状态”。
3. 在“无线网络状态”窗格的“受保护的无线网络”窗格下，单击“当前密钥”。

   为您网络配置的密钥随即会显示在“密钥配置”对话框中。

相关主题

- 查看密钥轮替的数量 (第 304 页)

自动轮替密钥

默认情况下启用自动密钥轮替，不过，如果暂停密钥轮替，则具有管理访问权限的计算机可以稍后重新启用它。

您可以配置 Wireless Network Security 自动轮替受保护无线网络的安全密钥。

Wireless Network Security 会自动生成无数个强密钥序列，可以通过网络对其进行同步。使用新安全密钥配置重新引导无线路由器时，系统会暂时中断无线连接，但网络用户通常不会察觉。

如果没有计算机连接到网络，则会在第一次连接时发生密钥轮替。

启用自动密钥轮替：

1. 右键单击 Windows 通知区域中的 Wireless Network Security 图标。
2. 选择“查看配置”。
3. 在“网络安全”窗格上，单击“启用自动密钥轮替”。

   您还可以在“无线网络状态”窗格上继续密钥轮替。
4. 单击“应用”。

注意：默认情况下，密钥会每三小时自动轮替一次，但可以调整密钥轮替频率来满足您的安全要求。

相关主题

- 调整密钥轮替频率 (第 289 页)
- 继续密钥轮替 (第 289 页)
- 查看密钥轮替的数量 (第 304 页)

继续密钥轮替

尽管默认情况下系统会启用自动密钥轮替，但具有管理访问权限的计算机可以在暂停密钥轮替后继续密钥轮替。

继续密钥轮替：

1. 右键单击 Windows 通知区域中的 Wireless Network Security 图标。
2. 选择“查看状态”。
3. 在“无线网络状态”窗格上，单击“继续密钥轮替”。

   “已开始进行密钥轮替”警报和“已轮替安全密钥”警报会确认密钥轮替开始且已成功轮替。

相关主题

- 自动轮替密钥 (第 288 页)
- 暂停自动密钥轮替 (第 291 页)
- 查看密钥轮替的数量 (第 304 页)

调整密钥轮替频率

如果配置 Wireless Network Security 自动轮替受保护无线网络的安全密钥，则可以调整密钥轮替发生时间段，范围从每十五分钟到每十五天。

McAfee 建议每天轮替一次安全密钥。

调整自动密钥轮替频率：

1. 右键单击 Windows 通知区域中的 Wireless Network Security 图标。
2. 选择“查看配置”。
3. 在“网络安全”窗格上，确认启用了自动密钥轮替，然后将“频率”滑块移到以下任一设置：
   - **每 15 分钟**
   - **每 30 分钟**
   - **每 1 小时**
   - **每 3 个小时**
   - **每 12 个小时**
   - **每 1 天**
   - **每 7 天**
   - **每 15 天**

4 单击“应用”。

注意：在设置密钥轮替频率前，务必启用自动密钥轮替。

相关主题

- 启用自动密钥轮替 (第 288 页)
- 查看密钥轮替的数量 (第 304 页)

暂停自动密钥轮替

连接到无线网络的任何计算机都可以暂停密钥轮替。您可以暂停密钥轮替以执行以下操作：

- 允许没有安装 Wireless Network Security 的来宾访问网络。
- 允许非 Windows 系统（如 Macintosh、Linux 或 TiVo）获取访问权限。停止密钥轮替后，记下密钥，然后将其输入到新设备中。
- 允许某些程序（如联机游戏）的无线连接（未因密钥轮替而中断）。
- 您应尽可能继续自动轮替密钥，以确保网络会完全抵御黑客的侵扰。

查看当前密钥：

1. 右键单击 Windows 通知区域中的 Wireless Network Security 图标。
2. 选择“查看状态”。
3. 在“无线网络状态”窗格的“受保护的无线网络”窗格下，单击“当前密钥”。记下“密钥配置”对话框中显示的密钥。没有安装 Wireless Network Security 的其他计算机可以使用此密钥连接到受保护的无线网络。
4. 在“密钥配置”对话框上，单击“暂停密钥轮替”。
5. 在“已暂停密钥轮替”对话框上，单击“确定”继续工作。

警告：如果没有暂停密钥轮替，则手动连接到网络的不支持的无线设备会在密钥轮替时断开连接。

您可以创建 Windows Connect Now 磁盘，然后使用文本文件将密钥复制并粘贴到其他计算机和设备。

相关主题

- 启用自动密钥轮替 (第 288 页)
- 使用 Windows Connect Now 技术添加计算机 (第 268 页)
- 继续密钥轮替 (第 289 页)
- 自动轮替密钥 (第 288 页)
- 查看密钥轮替的数量 (第 304 页)

手动轮替网络密钥

Wireless Network Security 允许手动轮替网络密钥，甚至在启用了自动密钥轮替的情况下进行手动轮替。

手动轮替网络密钥：

1. 右键单击 Windows 通知区域中的 Wireless Network Security 图标。
2. 选择“查看工具”。
3. 在“工具”窗格上，单击“维护工具”。
4. 在“维护工具”页的“手动轮替安全密钥”下，单击“轮替”。

   随即会显示“已开始进行密钥轮替”警报，并确认密钥轮替已开始。在轮替安全密钥后，会显示“已轮替安全密钥”警报，确认已成功进行了密钥轮替。

注意：为便于管理安全密钥，您可以在“网络安全”窗格上自动启用密钥轮替。

如果没有计算机连接到无线网络，则计算机在第一次连接时会自动发生密钥轮替。

相关主题

- 启用自动密钥轮替 (第 288 页)
- 调整密钥轮替频率 (第 289 页)
- 查看密钥轮替的数量 (第 304 页)

以星号显示密钥

默认情况下，密钥会显示为星号，但可以配置 Wireless Network Security 在 Wireless Network Security 没有保护的网络上以纯文本形式显示密钥。

Wireless Network Security 保护的网络会以纯文本形式显示密钥。

以星号显示密钥：

1. 右键单击 Windows 通知区域中的 Wireless Network Security 图标。
2. 选择“查看配置”。
3. 单击“其他设置”。
4. 清除“以纯文本显示密钥”框。
5. 单击“应用”。

相关主题

- 以纯文本显示密钥 (第 294 页)

以纯文本显示密钥

默认情况下，密钥会显示为星号，但可以配置 Wireless Network Security 在 Wireless Network Security 没有保护的网络上以纯文本形式显示密钥。

Wireless Network Security 保护的网络会以纯文本形式显示密钥。

以纯文本显示密钥：

1 右键单击 Windows 通知区域中的 Wireless Network Security 图标。

2 选择“查看配置”。

3 单击“其他设置”。

4 选中“以纯文本显示密钥”框。

5 单击“应用”。

相关主题

- 以星号显示密钥 (第 293 页)

删除网络密钥

Wireless Network Security 会自动保存 WEP 和 WPA 预共享密钥，您可以随时将其删除。

删除所有网络密钥：

1. 右键单击 Windows 通知区域中的 Wireless Network Security 图标。
2. 选择“查看配置”。
3. 在“配置”窗格上，单击“其他设置”。
4. 在“其他设置”窗格的“WEP 和 WPA 预共享密钥”下，单击“删除密钥”。
5. 如果要删除所有存储的 WEP 和 WPA 预共享密钥，请在“清除密钥”对话框上，单击“是”。

警告：永久删除密钥会将其从计算机中移除。删除网络密钥后，必须输入正确的密钥才能连接到 WEP 和 WPA 网络。

第 44 章

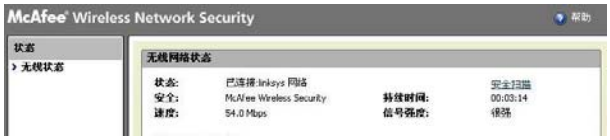
监视无线网络

Wireless Network Security 允许监视无线网络和受保护计算机的状态。

本章内容

监视无线网络连接

在“无线网络状态”窗格上，可以查看网络连接的状态、安全模式、速度、持续时间、信号强度以及安全报告。



下表介绍无线网络连接的状态指示器。

状态	描述	信息
状态	显示计算机是否连接到网络以及连接到哪个网络	查看连接状态 (第 299 页)
安全	显示要连接到的网络的安全模式。如果受到 Wireless Network Security 保护，则会显示 Wireless Network Security。	查看网络安全模式 (第 300 页)
速度	显示计算机连接到网络的速度。	查看网络连接速度 (第 300 页)
持续时间	显示计算机已连接到网络的时间段。	查看网络连接的持续时间 (第 300 页)
信号强度	显示网络的相对信号强度。	查看网络的信号强度 (第 302 页)
安全扫描	单击“安全扫描”显示安全信息，如无线安全漏洞、性能问题和无线网络的状态。	查看在线安全报告 (第 302 页)

相关主题

- 关于 Wireless Network Security 图标 (第 270 页)

查看连接状态

您可以使用“无线网络状态”窗格查看网络连接的状态，确认是否连接到网络或断开与网络的连接。

查看无线连接状态：

1 右键单击 Windows 通知区域中的 Wireless Network Security 图标。

2 选择“查看状态”。

连接到受保护无线网络的计算机以及每台计算机连接的时间和日期，均显示在“无线网络状态”窗格上的“计算机”下。

相关主题

- 监视无线网络连接 (第 298 页)
- 查看网络安全模式 (第 300 页)
- 查看网络连接速度 (第 300 页)
- 查看网络连接的持续时间 (第 300 页)
- 查看网络的信号强度 (第 302 页)
- 查看在线安全报告 (第 302 页)

查看网络安全模式

您可以使用“无线网络状态”窗格查看网络连接的安全模式。

查看网络安全模式：

1 右键单击 Windows 通知区域中的 Wireless Network Security 图标。

2 选择“查看状态”。

安全模式显示在“无线网络状态”窗格上的“安全”框中。

如果 Wireless Network Security 保护您的无线网络，则会显示 Wireless Network Security。

相关主题

- 监视无线网络连接 (第 298 页)
- 查看连接状态 (第 299 页)
- 查看网络连接速度 (第 300 页)
- 查看网络连接的持续时间 (第 300 页)
- 查看网络的信号强度 (第 302 页)
- 查看在线安全报告 (第 302 页)

查看网络连接速度

您可以使用 Wireless Network Status 窗格查看计算机连接到网络的速度。

查看网络连接速度：

1 右键单击 Windows 通知区域中的 Wireless Network Security 图标。

2 选择“查看状态”。

连接速度显示在“无线网络状态”窗格上的“速度”框中。

相关主题

- 监视无线网络连接 (第 298 页)
- 查看连接状态 (第 299 页)
- 查看网络安全模式 (第 300 页)
- 查看网络连接的持续时间 (第 300 页)
- 查看网络的信号强度 (第 302 页)
- 查看在线安全报告 (第 302 页)

查看网络连接的持续时间

您可以使用 Wireless Network Status 窗格查看已连接到网络的时间长度。

查看连接到网络的持续时间：

1 右键单击 Windows 通知区域中的 Wireless Network Security 图标。

2 选择“查看状态”。

计算机连接到无线网络的时间长度显示在“持续时间”框中。

相关主题

- 监视无线网络连接 (第 298 页)
- 查看连接状态 (第 299 页)
- 查看网络安全模式 (第 300 页)
- 查看网络连接速度 (第 300 页)
- 查看网络的信号强度 (第 302 页)
- 查看在线安全报告 (第 302 页)

查看网络的信号强度

您可以使用“无线网络状态”窗格查看网络的信号强度。

查看信号强度：

1 右键单击 Windows 通知区域中的 Wireless Network Security 图标。

2 选择“查看状态”。

信号质量显示在“信号强度”框中。

相关主题

- 监视无线网络连接 (第 298 页)
- 查看连接状态 (第 299 页)
- 查看网络安全模式 (第 300 页)
- 查看网络连接速度 (第 300 页)
- 查看网络连接的持续时间 (第 300 页)
- 查看在线安全报告 (第 302 页)

查看在线安全报告

您可以使用 Wireless Network Status 窗格查看有关无线连接的报告，了解它是否安全。

McAfee Wi-FiScan 网页显示有关无线安全漏洞的信息、性能问题、有关无线连接的信息、建议的安全解决方案，并指出连接是否安全。

在查看安全报告前，确保具有 Internet 连接。

查看有关网络的在线安全报告：

1. 右键单击 Windows 通知区域中的 Wireless Network Security 图标。
2. 选择“查看状态”。
3. 在“无线网络状态”窗格上，单击“安全扫描”。

   在浏览器打开后，您必须下载和安装 ActiveX 组件。根据浏览器的配置，浏览器可能会拦截控件。允许浏览器下载组件，然后运行它以开始扫描。根据 Internet 的连接速度，扫描可能会需要一段时间。

注意：有关下载 ActiveX 组件的信息，请参阅浏览器的文档。

McAfee 的 Wi-FiScan 支持 Internet Explorer 5.5 和更高版本。

相关主题

- 监视无线网络连接 (第 298 页)
- 查看连接状态 (第 299 页)
- 查看网络安全模式 (第 300 页)
- 查看网络连接速度 (第 300 页)
- 查看网络连接的持续时间 (第 300 页)
- 查看网络的信号强度 (第 302 页)

监视受保护的无线网络

Wireless Network Security 允许在“无线网络状态”窗格上查看连接、密钥轮替和受保护计算机的数量。您还可以查看网络事件、当前密钥和当前受保护的计算机。

下表介绍受保护无线网络连接的状态指示器。

状态	描述	信息
当天密钥轮替数	在受保护无线网络上显示每日密钥轮替数。	查看密钥轮替的数量 (第 304 页)
当天连接数	显示指向受保护网络的每日连接数。	查看每日连接数 (第 305 页)
本月保护的计算机数	显示本月受保护的计算机数。	查看每月受保护的计算机数 (第 305 页)
网络事件	单击“网络事件”显示网络、连接和密钥轮替事件。	查看受保护的无线网络事件 (第 305 页)
计算机	显示连接到受保护无线网络的计算机数和每台计算机连接到此网络的时间。	查看当前受保护的计算机数 (第 307 页)

查看密钥轮替的数量

Wireless Network Security 允许查看受保护网络上发生的每日密钥轮替数，以及上次发生密钥轮替的时间。

查看每日密钥轮替的数量：

1 右键单击 Windows 通知区域中的 Wireless Network Security 图标。

2 选择“查看状态”。

连接总数和最近密钥轮替总数会显示在“无线网络状态”窗格上“受保护的无线网络”下的“当天密钥轮替数”字段中。

相关主题

- 监视受保护的无线网络 (第 303 页)
- 查看每日连接数 (第 305 页)
- 查看每月受保护的计算机数 (第 305 页)
- 查看受保护的无线网络事件 (第 305 页)
- 查看当前受保护的计算机数 (第 307 页)
- 管理网络密钥 (第 287 页)
- 自动轮替密钥 (第 288 页)
- 手动轮替网络密钥 (第 292 页)

查看每日连接数

Wireless Network Security 允许查看受保护无线网络的每日连接数。

查看受保护无线网络的连接数：

1 右键单击 Windows 通知区域中的 Wireless Network Security 图标。

2 选择“查看状态”。

连接总数显示在“无线网络状态”窗格上“受保护的无线网络”下的“当天连接数”框中。

相关主题

- 监视受保护的无线网络 (第 303 页)
- 查看每月受保护的计算机数 (第 305 页)
- 查看受保护的无线网络事件 (第 305 页)
- 查看当前受保护的计算机数 (第 307 页)

查看每月受保护的计算机数

Wireless Network Security 允许查看当月受保护的计算机数。

查看当月受保护的计算机数：

1. 右键单击 Windows 通知区域中的 Wireless Network Security 图标。
2. 选择“查看状态”。
3. 当月受保护的计算机数显示在“无线网络状态”窗格上“受保护的无线网络”下的“本月保护的计算机数”框中。

相关主题

- 监视受保护的无线网络 (第 303 页)
- 查看密钥轮替的数量 (第 304 页)
- 查看每日连接数 (第 305 页)
- 查看受保护的无线网络事件 (第 305 页)
- 查看当前受保护的计算机数 (第 307 页)

查看受保护的无线网络事件

Wireless Network Security 记录无线网络上的事件，如轮替安全密钥的时间、其他计算机连接到 McAfee 保护的网络的时间以及其他计算机加入 McAfee 保护的网络的时间。

Wireless Network Security 允许查看介绍网络上发生事件的报告。您可以指定要显示的事件类型，而且可以根据日期、事件或计算机对事件信息进行排序。

查看网络事件：

1 右键单击 Windows 通知区域中的 Wireless Network Security 图标。

2 执行以下任一操作：

要...	执行此操作...
查看“无线网络状态”窗格中的网络事件	1. 选择“查看状态”。 2. 在“无线网络状态”窗格的“受保护的无线网络”下，单击“网络事件”。
查看“无线网络状态”窗格中的网络事件	1. 单击“查看工具”。 2. 在“工具”窗格上，单击“维护工具”。 3. 在“维护工具”窗格的“查看事件日志”下，单击“查看”。

3 选择以下一个或多个要显示的事件：

- **网络事件**：显示有关网络活动（如无线路由器或接入点的保护）的信息。
- **连接事件**：显示有关网络连接的信息，如连接到网络的计算机的日期和时间。
- **密钥轮替事件**：显示安全密钥轮替的日期和时间有关的信息。

4 单击“关闭”。

相关主题

- 监视受保护的无线网络 (第 303 页)
- 查看密钥轮替的数量 (第 304 页)
- 查看每日连接数 (第 304 页)
- 查看每日连接数 (第 305 页)
- 查看当前受保护的计算机数 (第 307 页)

查看当前受保护的计算机数

您可以查看连接到受保护无线网络的计算机数和每台计算机上次连接到此网络的时间。

查看连接到受保护网络的计算机：

1. 右键单击 Windows 通知区域中的 Wireless Network Security 图标。
2. 选择“查看状态”。
3. 连接到受保护网络的计算机以及每台计算机最近连接的时间和日期均显示在“无线网络状态”窗格上的“计算机”下。

相关主题

- 监视受保护的无线网络 (第 303 页)
- 查看密钥轮替的数量 (第 304 页)
- 查看每日连接数 (第 304 页)
- 查看每月受保护的计算机数 (第 305 页)
- 查看受保护的无线网络事件 (第 305 页)

第 45 章

故障排除

在使用 Wireless Security 和第三方设备时，可以对问题进行故障排除，这些问题有：

- 安装问题
- 无法保护或配置网络
- 无法将计算机连接到网络
- 无法连接到网络或 Internet
- 其他问题

本章内容

安装 Wireless Network Security

您可以对以下安装问题进行故障排除。

- 将此软件安装到哪些计算机上
- 未检测到无线适配器
- 多个无线适配器
- 无法在无线计算机上下载，因为网络已受到安全保护

将此软件安装到哪些计算机上

在网络中的每台计算机上安装 Wireless Network Security（与其他 McAfee 程序不同，您可以在多台计算机上安装此软件）。遵守购买软件的许可协议。在某些情况下，可能需要购买其他许可。

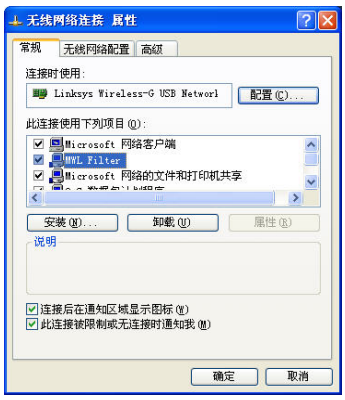
您可以（但并非必须）将此软件安装在没有安装无线适配器的计算机上，但此软件在这些计算机上是不活动的，因为这些计算机不需要无线防护。

Windows XP 或 Windows 2000 当前支持 Wireless Network Security。

未检测到兼容的无线适配器

如果安装和启用无线适配器后未检测到它，请重新启动计算机。如果在重新启动计算机后仍未检测到适配器，请执行以下步骤。

1. 启动 Windows 的“无线网络连接属性”对话框。
2. 使用 Windows 的经典“开始”菜单，查看并单击“开始”，指向“设置”，然后选择“网络连接”。
3. 单击“无线网络连接”图标。
4. 在“无线网络连接状态”对话框上，单击“属性”。
5. 在“无线网络连接属性”窗格上，清除“MWL 过滤器”，然后重新选中它。



6 单击“确定”。

如果这并不能解决问题，请运行 Wi-Fi Scan 进行验证。如果 Wi-Fi Scan 可以运行，则支持适配器。如果 Wi-Fi Scan 不运行，请更新适配器的驱动程序（使用 Windows Update 或访问制造商的网站）或购买新设备。

相关主题

- 查看在线安全报告 (第 302 页)

多个无线适配器

如果显示的错误表明您已安装了多个无线适配器，则必须禁用或拔下任一适配器。Wireless Home Network Security 只使用一个无线适配器。

在安全网络上下载失败

如果有安装 CD，请从 CD 中将 Wireless Network Security 安装到所有无线计算机上。

如果在将软件安装到所有其他无线计算机上之前，将其安装在一台无线计算机上并保护了您的网络，则可以执行以下操作。

- 取消网络保护。然后，下载软件并将其安装到所有无线计算机上。再次保护网络。
- 查看网络密钥。然后，在无线计算机上输入密钥以连接到网络。下载和安装软件，然后从此无线计算机加入网络。
- 将可执行文件下载到已连接到网络的计算机上，然后将其保存到 USB 闪存驱动器或将其写入 CD，以便在其他计算机上安装它。
- 运行 Windows Connect Now 技术。

相关主题

- 删除无线路由器或接入点 (第 276 页)
- 查看当前密钥 (第 287 页)
- 使用可移动设备添加计算机 (第 267 页)
- 使用 Windows Connect Now 技术添加计算机 (第 268 页)

保护或配置网络

您可以在保护或配置网络时对以下问题进行故障排除。

- 不支持的路由器或接入点
- 更新路由器或接入点防火墙
- 重复的管理员错误
- 网络显示不安全
- 无法修复

不支持的路由器或接入点

如果显示的错误表明可能不支持无线路由器或接入点，则 Wireless Network Security 无法配置设备，因为无法识别或找到设备。

通过请求更新，验证您使用最新版 Wireless Network Security（McAfee 会持续为新路由器和接入点提供支持）。如果路由器或接入点显示在支持路由器的列表中，并且仍收到此错误，则您会遇到计算机与路由器或接入点之间的通讯错误。

相关主题

- 支持的无线路由器 http://www.mcafee.com/router

更新路由器或接入点防火墙

如果显示的错误表明不支持无线路由器或接入点的固件修订，则系统会支持您的设备，但不支持设备的固件修订。通过请求更新，验证您使用最新版 Wireless Network Security（McAfee 会持续为新固件修订提供支持）。

如果您使用最新版 Wireless Network Security，请参考制造商的网站或咨询支持组织来了解路由器或接入点的信息，并安装支持路由器列表中列出的固件版本。

相关主题

- 支持的无线路由器 http://www.mcafee.com/router

重复的管理员错误

在配置路由器或接入点后，必须注销管理界面。在某些情况下，如果没有注销，则路由器或接入点的行为就像其他计算机仍在配置它一样，并且会显示错误消息。

如果无法注销，请拔下路由器或接入点的电源，然后重新插上电源。

密钥轮替失败

密钥轮替失败，原因是：

- 路由器或接入点的登录信息已经发生变化。
- 路由器或接入点的固件版本已改为不支持的版本。
- 路由器或接入点不可用。确保打开了路由器或接入点，并且已将其连接到网络。
- 重复的管理员错误。
- 对于某些无线路由器，如果其他计算机手动登录到无线路由器的 Web 界面，则 McAfee 客户端也可能无法访问管理界面来轮替密钥。

相关主题

- 更改无线设备的凭证 (第 285 页)
- 自动轮替密钥 (第 288 页)

无法修复路由器或接入点

如果修复失败，请尝试执行以下操作。注意每个步骤都是独立的。

- 使用电缆连接到网络，然后再次尝试重新修复。
- 拔下路由器或接入点的电源，再次插上电源，然后重试连接。
- 将无线路由器或接入点重置为其默认设置并修复它。执行此操作会将无线设置重置为其最初的设置。然后，重置 Internet 连接设置。
- 使用高级选项，从所有计算机上离开网络，将无线路由器或接入点重置为其默认设置，然后保护它。此操作会将无线设置重置为其最初的设置。然后，重置 Internet 连接设置。

相关主题

- 修复网络安全设置 (第 286 页)

网络显示未受保护

如果网络显示不安全，则网络未受保护。您必须保护网络才能保护它的安全。注意，Wireless Network Security 只有在使用兼容的路由器或接入点才能正常工作。

相关主题

- 创建受保护的无线网络 (第 258 页)
- 支持的无线路由器 http://www.mcafee.com/router

将计算机连接到网络

您可以在将计算机连接到网络时对以下问题进行故障排除。

- 等待授权
- 授予未知计算机访问权限

等待授权

如果您要尝试加入受保护的网络，而且您的计算机仍保持在等待授权模式，请验证以下各项。

- 已连接到网络的无线计算机已打开并已连接到网络。
- 有人存在，以在此计算机显示时，将访问权限授予给它。
- 计算机位于各计算机的无线范围内。

如果在对网络已具有访问权限的计算机上没有显示“授予访问权限”，请尝试从另一台计算机授予访问权限。

如果其他计算机不可用，请从对网络已具有访问权限的计算机上取消对网络的保护，然后从对网络没有访问权限的计算机上保护网络。然后，从最初保护网络的计算机上加入网络。

您还可以使用“保护其他计算机”功能。

相关主题

- 加入受保护的无线网络 (第 260 页)
- 离开受保护的无线网络 (第 279 页)
- 删除无线路由器或接入点 (第 276 页)
- 将计算机添加到受保护的无线网络 (第 267 页)

授予未知计算机访问权限

如果从未知计算机收到授予访问权限的请求，请在验证其合法性之前拒绝此请求。有人可能要非法访问您的网络。

连接到 Internet 和网络

在计算机连接到网络或 Internet 时，可以对以下问题进行故障排除。

- 错误的 Internet 连接
- 连接暂时停止
- 设备（并非您的计算机）丢失连接
- 提示输入 WEP、WPA 或 WPA2 密钥
- 无法连接
- 更新无线适配器
- 信号强度弱
- Windows 无法配置无线连接
- Windows 显示无连接

无法连接到 Internet

如果无法连接，请尝试使用电缆访问网络，然后连接到 Internet。如果仍无法连接，请验证以下各项：

- 调制解调器打开
- PPPoE 设置正确
- DSL 或电缆线有效

无线干扰也可能引发连接问题，如速度和信号强度。请尝试采用以下方法修复问题：

- 更改无绳电话的频道
- 消除可能的干扰来源
- 更改无线路由器、接入点或计算机的位置
- 更改路由器或接入点频道。对北美洲和南美洲，建议使用频道 1、4、7 和 11。对其他国家，建议使用频道 1、4、7 和 13。默认情况下，许多路由器都设置为频道 6
- 确保路由器和无线适配器（特别是无线 USB 适配器）不要靠墙
- 确保 USB 无线适配器不在无线接入点/路由器的旁边。
- 将路由器放置在远离墙和金属的位置

连接中断

如果连接出现短暂中断（如在玩在线游戏时），则可能是密钥轮替引起的。为防止出现此问题，可以暂停密钥轮替。

McAfee 建议应尽可能继续自动轮替密钥，以确保网络会完全抵御黑客的侵扰。

相关主题

- 自动轮替密钥 (第 288 页)
- 继续密钥轮替 (第 289 页)
- 暂停自动密钥轮替 (第 291 页)
- 手动轮替网络密钥 (第 292 页)

设备丢失连接

如果在使用 Wireless Network Security 时某些设备丢失了连接，请尝试使用以下方法修复问题：

- 暂停密钥轮替
- 更新无线适配器的驱动程序
- 禁用适配器客户端管理器

相关主题

- 暂停自动密钥轮替 (第 291 页)

提示输入 WEP、WPA 或 WPA2 密钥

如果必须输入 WEP、WPA 或 WPA2 密钥才能连接到受保护的无线网络，则可能没有在计算机上安装软件。

为正常运行，必须在网络中的每台无线计算机上安装 Wireless Network Security。

相关主题

- 启动 Wireless Network Security (第 253 页)
- 将计算机添加到受保护的无线网络 (第 267 页)

无法连接到无线路由器

如果无法连接，请尝试以下操作。注意每个步骤都是独立的。

- 如果未连接到受保护的网络，请验证您具有正确的密钥并再次输入它。
- 拔下无线适配器并重新插入，或禁用无线适配器并再次启用它。
- 关闭路由器或接入点，再次打开它，然后尝试连接。
- 确保您的无线路由器或接入点处于连接状态，然后修复安全设置。
- 重新启动计算机。
- 更新无线适配器或购买新无线适配器。例如，您的网络可能会使用 WPA-PSK TKIP 安全，而您的无线适配器可能不支持网络的安全模式（网络会显示 WEP，即使设置为 WPA 也是如此）。
- 如果在升级无线路由器或接入点后无法连接，则可以将其升级到不支持的版本。确保支持路由器或接入点。如果不支持，请将其降级到支持的版本，或等待，直到 Wireless Security 更新可用为止。

相关主题

- 修复网络安全设置 (第 286 页)
- 更新无线适配器 (第 317 页)

更新无线适配器

您可能需要更新无线适配器才能使用 Wireless Network Security。

更新适配器：

1. 在桌面上单击“开始”，指向“设置”，然后选择“控制面板”。
2. 双击“系统”图标。随即出现“系统属性”对话框。
3. 选择“硬件”选项卡，然后单击“设备管理器”。
4. 在“设备管理器”列表中，双击适配器。
5. 选择“驱动程序”选项卡，并注意您使用的驱动程序。
6. 访问适配器制造商的网站查找更新。驱动程序通常位于“支持”或“下载”部分。如果使用 miniPCI 卡，请导航到计算机的制造商，而不是导航到此卡的制造商。
7. 如果驱动程序更新可用，请按照网站上的说明进行下载。
8. 返回到“驱动程序”选项卡，然后单击“更新驱动程序”。随即会显示 Windows 向导。
9. 要安装驱动程序，请按照网站上的说明执行操作。

信号强度弱

如果连接断开或很慢，则可能是信号强度不太强。要增加信号强度，请尝试以下方法：

- 确保金属物体（如炉子、管道或大型设备）没有阻挡无线设备。无线信号无法穿透这些物体。
- 如果信号必须穿过墙壁，确保信号不是以很小的角度穿过，信号穿过墙壁所费的时间越长，信号就越弱
- 如果无线路由器或接入点有多个天线，请尝试将这两个天线调整为彼此垂直（一个竖直，一个水平，两者呈 90 度角）。
- 某些制造商会采用高增益天线。定向天线提供的范围更宽，而全向天线提供的功能最多。有关安装天线的信息，请参阅制造商的安装说明。

如果以上措施无效，请将接入点添加到靠近要连接到的计算机的网络。如果您将第二个接入点配置了相同的网络名称 (SSID) 和不同的频道，则适配器将自动查找最强的信号，然后通过响应的接入点进行连接。

相关主题

- 信号强度图标 (第 270 页)
- 查看网络的信号强度 (第 301 页)

Windows 不支持无线连接

如果显示的 Windows 错误消息指出无法配置您的无线连接，则可以忽略它。使用 Wireless Network Security 连接到无线网络并对其进行配置。

在 Windows 的“无线网络连接属性”对话框的“无线网络”选项卡下，确保清除“使用 Windows 配置无线网络设置”框。

Wireless Network Security 允许：

- 安装在运行 Windows 2000 计算机的适配器连接到 WPA 网络，即使不支持此卡的客户端管理器也是如此。
- 运行 Windows XP 的计算机上的适配器连接到 WPA2 网络，而无须查找和安装 Win XP SP2 紧急修复程序
- 运行 Windows XP SP1 的计算机上适配器连接到 WPA 和 WPA2 网络，而无须查找和安装紧急修复程序，Windows XP SP1 不支持此程序。

Windows 显示无连接

如果您已连接，但 Windows Network 图标显示 X（无连接），请将其忽略。您的连接正常。

其他问题

您可以对以下问题进行故障排除。

- 使用其他程序时网络名称不同
- 配置无线路由器或接入点时的问题
- 重新放置计算机
- 选择其他安全模式
- 升级操作系统后软件无法正常工作

使用其他程序时网络名称不同

如果通过其他程序查看时，网络名称不同（如名称包含 _SafeAaf），这是一种正常的现象。

Wireless Network Security 在网络受到保护时，会使用代码标记网络。

配置无线路由器或接入点

如果配置路由器或接入点，或在网络上添加多个路由器时出错，请验证所有路由器和接入点的 IP 地址是否都不同。

如果无线路由器或接入点的名称显示在“保护无线路由器或接入点”对话框中，则会在配置时出错：验证路由器或接入点受到支持。

如果已配置了路由器或接入点，但它们似乎不在正确的网络中（如您看不到连接到 LAN 的其他计算机），则验证您已配置了相应的路由器或接入点，而不是邻居的路由器或接入点。请拔下路由器或接入点的电源，并确保连接断开。如果配置了错误的路由器或接入点，则取消保护它，然后保护正确的路由器或接入点。

如果无法配置或添加路由器或接入点，则系统支持它，则您执行的某些更改可能会阻止正确配置。

- 按照制造商的说明将路由器或接入点配置为 DHCP，或配置正确的 IP 地址。在某些情况下，制造商提供配置工具。
- 将路由器或接入点重置为出厂设置，然后再次尝试修复网络。您可能已更改了路由器或接入点上的管理端口，或关闭了无线管理。确保您正在使用默认的配置，并启用了无线配置。其他可能的原因有禁用了 http 管理。在此情况下，确保启用了 http 管理。确保使用端口 80 进行管理。
- 如果无线路由器或接入点没有显示在要保护或要连接到的无线路由器或接入点的列表中，请启用广播 SSID，并确保您可以在 Wireless Network Security 的可用无线网络列表中看到您的路由器或接入点。
- 如果断开连接，或无法建立连接，则可能启用了 MAC 过滤功能。禁用 MAC 过滤。

- 如果在与网络具有无线连接的两台计算机之间无法执行网络操作（如共享文件或打印到共享打印机），则确保您没有启用接入点隔离。接入点隔离会防止无线计算机通过网络互相连接。
- 如果使用 McAfee Personal Firewall 之外的防火墙程序，请确保信任了子网。

相关主题

- 支持的无线路由器 http://www.mcafee.com/router

重新放置计算机

如果替换掉保护网络的计算机，并且没有任何计算机具有访问权限（您无法访问网络），请将无线路由器或接入点重置为其出厂默认值并再次保护您的网络。

选择其他安全模式

如果显示的错误表明无线适配器不支持所选的安全模式，则必须选择其他安全模式。

- 所有适配器都支持 WEP。
- 支持 WPA 的大多数适配器都可以实现 WPA-PSK TKIP 和 WPA-PSK AES 安全模式。
- 支持 WPA2 的适配器可以实现 WPA 安全模式以及 WPA2-PSK TKIP、WPA2-PSK AES 和 WPA2-PSK TKIP/AES。

相关主题

- 配置安全设置 (第 282 页)
- 查看网络安全模式 (第 299 页)

升级操作系统后，软件无法正常运行

如果在升级操作系统后 Wireless Network Security 无法运行，请先删除此程序，然后再重新安装。

第 46 章

McAfee EasyNetwork

McAfee® EasyNetwork 支持在家庭网络的各计算机之间安全共享文件、简化文件传输以及自动共享打印机。

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

本章内容

功能

EasyNetwork 提供以下功能。

文件共享

使用 EasyNetwork 可以轻松将您计算机上的文件与网络中的其他计算机共享。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的计算机（即具有完全或管理访问权限）才能共享或访问其他成员计算机共享的文件。

文件传输

您可以将文件发给作为托管网络成员的其他计算机。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，存储网络上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，EasyNetwork 通过将打印机的当前名称用作共享打印机名称，自动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。

第 47 章

设置 EasyNetwork

在可以使用 EasyNetwork 功能之前，必须启动此程序并加入托管网络。在加入托管网络之后，您可以决定随时离开网络。

本章内容

启动 EasyNetwork

默认情况下，在安装 EasyNetwork 后，系统会提示您立即启动它；不过，您也可以稍后启动 EasyNetwork。

启动 EasyNetwork

默认情况下，在安装 EasyNetwork 后，系统会提示立即启动它；不过，您也可以稍后启动 EasyNetwork。

启动 EasyNetwork：

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

提示：如果您同意在安装过程中创建桌面图标和快速启动图标，则还可以通过双击桌面上的 McAfee EasyNetwork 图标，或单击任务栏右侧通知区域的 McAfee EasyNetwork 图标来启动 EasyNetwork。

加入托管网络

安装 SecurityCenter 后，网络代理会添加到计算机并在后台运行。在 EasyNetwork 中，网络代理负责检测有效的网络连接、检测要共享的本地打印机和监视网络状态。

如果在您当前连接到的网络上没有运行网络代理的其他计算机，则您会自动成为此网络的成员，而且系统会提示您确定此网络是专用网络还是公共网络。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。

当有计算机连接到此网络时，加入请求会发给当前位于此网络上的所有其他计算机。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。授予方也可以确定当前加入网络的计算机的权限级别；例如，来宾（只有文件传输功能）或完全/管理（文件传输和文件共享功能）。在 EasyNetwork 中，具有管理访问权限的计算机可以授予其他计算机访问权限并管理权限（即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。在允许计算机加入前，还会执行安全检查。

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（例如 McAfee Wireless Network Security 或 Network Manager），这些程序也会将此计算机识别为托管计算机。分配给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，会显示一条消息提示，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。如果此计算机是网络上的第一台计算机，则会自动授予对此网络的管理权限。

加入网络：

1. 在“共享文件”窗口中，单击“是，立即加入网络”。
   在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“是”；否则，请单击“否”。
3. 确保授予权限的计算机显示当前显示在安全确认对话框中的图片，然后单击“确认”。

注意：如果授予权限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，单击安全确认对话框中的“拒绝”。

授予对网络的访问权限

在计算机请求加入托管网络时，会将一条消息发给网络上具有管理权限的其他计算机。响应此消息的第一台计算机便成为授予方。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。

授予对网络的访问权限：

1. 在警报中，选中以下任一复选框：
   - **授予来宾访问权限**：允许用户将文件发往其他计算机，但不允许共享文件。
   - **授予对所有托管网络应用程序的完全访问权限**：允许用户发送和共享文件。
   - **授予对所有托管网络应用程序的管理访问权限**：允许用户发送和共享文件，授予其他计算机访问权限，以及调整其他计算机的权限级别。

2　单击“授予访问权限”。

3　确保计算机显示当前显示在安全确认对话框中的图片，然后单击“确认”。

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，则托管网络上有安全隐患。授予此计算机网络访问权限可能会使您的计算机面临风险；因此，单击安全确认对话框中的“拒绝”。

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。

重命名网络：

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

如果加入托管网络，然后决定不再作为其成员，则可以离开网络。在放弃您的成员资格后，您可以随时重新加入；不过，您必须被授予权限才能加入，然后再次执行安全检查。有关详细信息，请参阅加入托管网络 (第 325 页)。

离开托管网络

您可以离开以前加入的托管网络。

离开托管网络：

1 在“工具”菜单上，单击“离开网络”。

2 在“离开网络”对话框中，选择要离开的网络名称。

3 单击“离开网络”。

第 48 章

共享和发送文件

使用 EasyNetwork 可以轻松与网络中的其他计算机共享和发送文件。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的计算机（即具有完全或管理访问权限）才能共享或访问其他成员计算机共享的文件。

本章内容

共享文件

使用 EasyNetwork 可以轻松将您计算机上的文件与网络中的其他计算机共享。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的计算机（即具有完全或管理访问权限）才能共享或访问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，则它会自动从“共享文件”窗口中删除。您可以随时停止共享文件。

可以通过两种方法访问共享文件：直接在 EasyNetwork 中打开文件，或将文件复制到计算机上的位置，然后打开此文件。如果共享文件的列表很长，则可以搜索要访问的共享文件。

注意：使用 EasyNetwork 共享的文件无法在其他计算机上使用 Windows 资源管理器进行访问。EasyNetwork 文件共享是通过安全连接进行的。

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其他成员都可以使用此文件。

共享文件：

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：您还可以通过单击“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不能再访问此文件。

停止共享文件：

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，选择不再希望共享的文件。
3. 单击“不共享”。

复制共享文件

您可以将共享文件从托管网络上的任一计算机复制到您的计算机。然后，如果此计算机停止共享文件，则您仍可以使用其副本。

复制文件：

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

提示：您还可以复制共享文件，方法是选择 EasyNetwork 中的文件，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”窗口中自动显示相应的结果。

搜索共享文件：

1. 在“共享文件”窗口中，单击“搜索”。
2. 在“包含”列表中单击以下任一选项：
   - **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。
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. 在“类型”列表中单击以下任一文件类型：
   - **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。
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。

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，存储网络上其他计算机发给您的所有文件。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 Windows 任务栏右侧的通知区域显示一条消息。如果不想接收通知消息，则可以将其关闭。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。在接受文件（即将其复制到您计算机上的位置）之前，这些文件会保存在收件箱中。

将文件发送到另一台计算机

您可以将文件直接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可以查看文件之前，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 334 页)。

将文件发送到另一台计算机：

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。您还可以通过单击“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，则您必须接受此文件（通过将其保存到计算机上的文件夹）。如果文件发给您的计算机时，您没有打开 EasyNetwork 或位于前台，则会在任务栏的右侧的通知区域收到通知消息。单击此通知消息打开 EasyNetwork 并访问文件。

接收其他计算机发来的文件：

- 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。如果当前没有打开 EasyNetwork 或不在桌面的前台，则会在 Windows 任务栏右侧的通知区域显示一条通知消息。

发送文件时接收通知：

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”。

第 49 章

共享打印机

在加入托管网络后，EasyNetwork 会自动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。

本章内容

使用共享打印机

在加入托管网络后，EasyNetwork 通过将打印机的当前名称用作共享打印机名称，自动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。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，EasyNetwork 会将此打印机认为是本地打印机，并自动在网络上进行共享。您可以随时停止共享打印机。

EasyNetwork 还会检测由网络上的其他计算机共享的打印机。如果它检测到尚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。这样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。您还可以刷新在网络上检测到的打印机列表。

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

停止共享打印机

您可以随时停止共享打印机。已安装此打印机的成员将不能再使用此打印机进行打印。

停止共享打印机：

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

作为托管网络的成员，您可以访问在网络上共享的打印机。为此，必须安装打印机使用的打印机驱动程序。如果在安装打印机驱动程序后，打印机的所有者停止共享打印机，则无法再打印到此打印机。

安装可用的网络打印机：

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”。

第 50 章

参考

术语词汇表列出并定义了 McAfee 产品中最常用的安全术语。

“关于 McAfee”提供有关 McAfee Corporation 的合法信息。

词汇表

8

802.11

适用于无线 LAN 技术的一组 IEEE 标准。802.11 指定了无线客户端和基站之间或两个无线客户端之间的无线接口。802.11 的几个规范包括：802.11a，使用 5Ghz 频段，联网速率最高为 54 Mbps 的标准；802.11b，使用 2.4 Ghz 频段，联网速率最高为 11 Mbps 的标准；802.11g，使用 2.4 Ghz 频段，联网速率最高为 54 Mbps 的标准；以及 802.11i，适用于所有无线以太网的一套安全标准。

802.11a

对 802.11 的扩展，适用于无线 LAN，使用 5GHz 频段以最高 54 Mbps 发送数据。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，适用于无线 LAN，使用 2.4 GHz 频段提供 11 Mbps 传输速率。802.11b 当前被视作无线标准。

802.11g

对 802.11 的扩展，适用于无线 LAN，使用 2.4 GHz 频段提供最高 54 Mbps 传输速率。

802.1x

Wireless Home Network Security 不支持此标准。有线和无线网络上的 IEEE 身份验证标准，但最主要与 802.11 无线网络结合使用。此标准在客户端和身份验证服务器之间提供强大的互相身份验证功能。此外，802.1x 还可以根据每个用户、每个会话提供动态的 WEP 密钥，这便消除了静态 WEP 带来的管理负担和安全风险。

C

cookie

万维网上 Web 服务器存储在客户端系统上的数据块。在用户返回到同一网站时，浏览器会将 Cookie 的副本重新发送到服务器。Cookie 用于标识用户，指示服务器发送自定义版本的请求网页，提交用户的帐户信息以及其他管理用途。

网站利用 Cookie 可以记住您的身份、跟踪访问网站的人数、访问时间以及所浏览的网页。Cookie 还有助于公司个性化您的网站。许多网站都要求提供用户名和密码才能访问某些网页，并会将 Cookie 发到您的计算机上，使您不必每次进行登录。不过，Cookie 也可被用来进行恶意活动。在线广告公司通常会使用 Cookie 确定您经常访问的站点，然后将广告发布到您喜爱的网站。在允许接收来自某个站点的 Cookie 时，确保您信任此网站。

尽管 Cookie 是合法公司的信息来源，但也可能是黑客的信息来源。许多包含在线商店的网站都会将信用卡和其他个人信息存储在 Cookie 中，以方便客户购物。但是，有一些安全问题会使黑客访问客户计算机上存储的 Cookie 中的信息。

D

DNS

域名系统 (Domain Name System) 的首字母缩写。一种层次结构系统，Internet 上的主机都具有域名地址（如 bluestem.prairienet.org）和 IP 地址（如 192.17.3.4）。域名地址由用户使用，而且会自动转换为数据包路由软件所使用的数字 IP 地址。DNS 名称由顶层域（如 .com、.org 和 .net）、第二层域（企业、组织或个人的站点名称）以及可能的一个或多个子域（第二层域中的服务器）组成。另请参阅 DNS 服务器和 IP 地址。

DNS 服务器

域名系统 (Domain Name System) 服务器的简称。它是一台回应域名系统 (DNS) 查询的计算机。DNS 服务器保留主机计算机及其对应 IP 地址的数据库。例如，如果显示为名称 apex.com，则 DNS 服务器将返回假设公司 Apex 的 IP 地址。也称为：名称服务器。另请参阅 DNS 和 IP 地址。

E

ESS（扩展服务集）

构成一个子网的两个或多个网络的集合。

I

Internet

Internet 由大量互连的网络组成，这些网络使用 TCP/IP 协议来查找和传输数据。Internet 是从最初将大学和学院的计算机相链接而逐步发展起来的（20 世纪 60 年代末和 70 年代初），这一计划是由美国国防部资助的，并将其命名为 ARPANET。现在的 Internet 是一个包括近 100,000 个独立网络的全球性网络。

IP 地址

Internet 协议地址或 IP 地址是一个唯一号码，它包含由圆点分隔的四个部分（如 63.227.89.66）。Internet 上的每台计算机（包括最大的服务器和通过手机进行通讯的膝上型计算机）都有唯一的 IP 号码。并非每台计算机都有域名，但是每台计算机都会有 IP。

下面列出一些不常用的 IP 地址类型：

- 无法路由的 IP 地址：又称“专用 IP 空间”。这些 IP 地址无法在 Internet 上使用。专用 IP 的范围是 10.x.x.x、172.16.x.x - 172.31.x.x 和 192.168.x.x。
- 环回 IP 地址：环回地址用于测试目的。发送到该 IP 地址块的通讯将立即返回给生成数据包的设备。它绝不会脱离设备，主要用于硬件和软件测试。环回 IP 的范围是 127.x.x.x。

空 IP 地址：这是无效的地址。如果出现此地址，则表明通讯中包含空 IP 地址。这显然不正常，它通常表明发送者蓄意隐藏通讯来源。除非收到数据包的应用程序了解数据包内容并且知道其中包含该应用程序的特定指令，否则发送者将无法收到任何答复。所有以 0 开头的地址 (0.x.x.x) 都是空地址。例如，0.0.0.0 即为空 IP 地址。

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）

覆盖范围相对较小的计算机网络。大多数 LAN 都在一个建筑物或在一组建筑物内。不过，可以通过电话和无线电波将一个 LAN 连接到任何距离外的其他 LAN。以此方式连接的 LAN 系统称为广域网 (WAN)。大多数 LAN 一般通过集线器或交换机连接工作站和个人计算机。LAN 中的每个节点（单个计算机）都有自己的可以执行程序的 CPU，但它还可以访问 LAN 上任何位置的数据和设备（如打印机）。这表明许多用户都可以共享昂贵的设备，例如激光打印机及数据。用户还可以使用 LAN 互相通信，例如发送电子邮件和加入聊天。

M

MAC 地址（媒体访问控制地址）

分配给访问网络的物理设备的低层地址。

MAC（媒体访问控制或消息验证者代码）

对于前者，请参阅 MAC 地址。后者是一个用于标识给定消息（如 RADIUS）的代码。此代码通常是消息内容的强加密散列表，其中包括唯一值，可确保重新执行保护。

MAPI 帐户

消息应用程序编程接口 (Messaging Application Programming Interface) 的首字母缩写。Microsoft 接口规范，能使不同的消息和工作组应用程序（包括电子邮件、语音邮件和传真）通过一个客户端（如 Exchange 客户端）来工作。出于此原因，MAPI 通常在公司使用 Microsoft® Exchange Server 的公司环境中使用。不过，许多人都使用 Microsoft 的 Outlook 收发个人 Internet 电子邮件。

MSN 帐户

Microsoft 网络（Microsoft Network）的首字母缩写。在线服务和 Internet 门户。这是基于 Web 的帐户。

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

将桌面计算机连接到网络。此卡插入计算机内部的 PCI 扩展插槽。

POP3 帐户

邮局协议 3（Post Office Protocol 3）的首字母缩写。大多数家庭用户都使用此类型的帐户。这是 TCP/IP 网络上最常用的邮局协议标准的最新版本。也称为标准电子邮件帐户。

PPPoE

以太网上的点对点协议。许多 DSL 提供商都使用 PPPoE，PPPoE 支持在 PPP 中广泛使用的协议层和身份验证，允许在以太网通常的多点体系结构中建立点对点连接。

R

RADIUS（远程访问拨入用户服务）

通常在远程访问环境中提供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。

S

SMTP 服务器

简单邮件传输协议（Simple Mail Transfer Protocol）的首字母缩写。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）

无线 LAN 子系统中设备的网络名称。这是添加到每个 WLAN 数据包报头的 32 个字符的字符串的纯文本。SSID 区分各 WLAN，因此，网络的所有用户都必须提供相同的 SSID 才能访问给定的接入点。SSID 会禁止没有 SSID 的任何客户端设备进行访问。不过，默认情况下，接入点 (AP) 会在其信标中广播其 SSID。即使关闭 SSID 广播，黑客也可以通过监听检测 SSID。

SSL（安全套接层）

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。Netscape Navigator 和 Internet Explorer 都使用并支持 SSL，许多网站使用此协议获取用户机密信息，如信用卡号。根据约定，需要 SSL 连接的 URL 都以 https: 而不是 http: 开头。

SystemGuard

SystemGuard 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）

克服 WEP 安全中固有弱点，特别是密钥重用问题的快速解决方法。每隔 10,000 个数据包，TKIP 便会更改一次临时密钥，提供可大大增强网络安全的动态分布式方法。TKIP（安全性）进程以客户端和接入点 (AP) 之间共享的 128 位临时密钥开头。TKIP 将临时密钥与（客户端计算机的）MAC 地址结合在一起，然后会添加相对较大的 16 个八位位组初始化向量来生成加密数据的密钥。此过程确保每个站使用不同的密钥流来加密数据。TKIP 使用 RC4 执行加密。WEP 还使用 RC4。

U

URL

统一资源定位器。这是标准的 Internet 地址格式。

USB 无线适配器卡

提供可扩展的即插即用的序列接口。此接口为外部设备（如键盘、鼠标、游戏杆、打印机、扫描仪、存储设备和视频会议相机）提供标准的、低成本的无线连接。

V

VPN（虚拟专用网）

使用公共线路重新结合节点来构建网络。例如，有许多系统都可以将 Internet 用作传输数据的媒介来创建网络。这些系统会使用加密和其他安全机制，以确保只有授权用户才能访问网络，而且数据不会被拦截。

W

Web 错误

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。Web 错误还称为 Web 信标、像素标记、透明 GIF 或不可见的 GIF。

WEP（有线等效加密）

定义为 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 Alliance

由主要的无线设备和软件提供商组成的组织，其使命是 (1) 认证所有基于 802.11 产品的互操作性，以及 (2) 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互操作能力和行业增长的厂商的信息交流中心。

尽管可以将所有 802.11a/b/g 产品称为 Wi-Fi，但只有通过 Wi-Fi Alliance 测试的产品才能将其产品称为 Wi-Fi Certified（注册商标）。通过认证的产品必须在其包装上印有 Wi-Fi Certified 字样的标识图章，并指出使用的无线电频段。此组织以前称为 Ethernet Compatibility Alliance (WECA)，在 2002 年 10 月更名，以便更好地反映其要建立的 Wi-Fi 品牌。

Wi-Fi Certified

Wi-Fi Alliance 测试和批准为 Wi-Fi Certified（注册商标）的任何产品都被证明为可互操作的，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。不过，通常使用相同无线电频率（如对 802.11b 或 11g 使用 2.4GHz，对 802.11a 使用 5GHz）的 Wi-Fi 产品都可以与任何其他产品（即使没有 Wi-Fi Certified）一起使用。

Wi-Fi（无线保真）

通常指任何类型的 802.11 网络（802.11b、802.11a、双频等）时使用。Wi-Fi Alliance 使用此术语。

WLAN（无线局域网）

另请参阅 LAN。使用无线媒介进行连接的局域网。WLAN 使用高频无线电波而不是有线线路在节点之间进行通信。

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 IEEE 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 和 TKIP。

WPA2

另请参阅 WPA。WPA2 是 WPA 安全标准的更新，它基于 802.11i IEEE 标准。

WPA2-PSK

另请参阅 WPA-PSK 和 WPA2。WPA2-PSK 与 WPA-PSK 类似，基于 WPA2 标准。WPA2-PSK 的一种常见功能是，设备通常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）

白名单

允许访问的网站列表，因为这些网站不是诈骗网站。

暴力攻击

也称为暴力破解，应用程序通过穷尽操作（使用暴力）而不是使用智能策略对加密数据（如密码）进行解码所使用的试错法。就像罪犯尝试各种可能组合破坏保险箱一样，暴力破解应用程序会按顺序尝试各种合法字符的可能组合。暴力破解尽管非常耗时，但被认为是一种可靠的方法。

备份

在安全的联机服务器上创建监视文件的副本。

标题

标题是在邮件的整个生存周期中添加到邮件部分的信息。标题会通知 Internet 软件传送邮件的方式、发送邮件回复的位置，电子邮件的唯一标识符以及其他管理信息。标题字段的示例有：收件人、发件人、抄送、日期、主题、邮件 ID 和已接收。

标准电子邮件帐户

大多数家庭用户都使用此类型的帐户。另请参阅 POP3 帐户。

存档

在 CD、DVD、USB 驱动器、外部硬盘驱动器或网络驱动器本地创建监视文件的副本。

存档

在 CD、DVD、USB 驱动器、外部硬盘驱动器或网络驱动器本地创建监视文件的副本。

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。通过充当代表所有内部计算机的中间计算机，代理可以保护网络身份，同时仍能提供对 Internet 的访问。另请参阅“代理服务器”。

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。代理服务器可以通过提供频繁请求的数据（如常用网页）来提高性能，可以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

固定时间内传输的数据量。对于数字设备，带宽的单位通常用每秒位数 (bps) 或每秒字节数表示。对于模拟设备，带宽用每秒周期数，即赫兹 (Hz) 表示。

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。McAfee 会拦截浏览器加载网页时自动加载的弹出窗口。McAfee 不会拦截单击链接后加载的弹出窗口。

电子邮件

电子邮件，即通过 Internet 或在公司 LAN 或 WAN 内发送的邮件。现在，越来越普遍地通过 EXE（可执行）文件或 VBS（Visual Basic 脚本）文件形式的电子邮件附件来传输病毒和特洛伊木马程序。

电子邮件客户端

电子邮件帐户。例如，Microsoft Outlook 或 Eudora。

端口

信息进入/离开计算机的位置，例如，传统的模拟调制解调器连接到串行端口。TCP/IP 通讯中使用的端口号是虚拟值，用于将通讯分隔为应用程序特定的流。端口将被分配给标准协议，如 SMTP 或 HTTP，以使程序了解尝试在哪个端口上建立连接。TCP 数据包的目标端口表示正在查找的应用程序或服务器。

恶意接入点

公司没有授权操作的接入点。问题在于，恶意接入点通常不遵守无线 LAN (WLAN) 安全策略。恶意接入点允许从实际控制的设备外通过打开的不安全接口访问公司网络。

在受到正确保护的 WLAN 中，恶意接入点比恶意用户更具有破坏性。如果有效的身份验证机制发挥作用，则尝试访问 WLAN 的未经授权的用户将不会成功获取有价值的公司资源。不过，如果员工或黑客插入恶意接入点，则会产生严重问题。在公司网络中配备了 802.11 的任何人，恶意接入点几乎都允许其访问。这样，他们就非常接近关键业务资源。

发布

在 Internet 上公开可用的已备份文件。

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的访问。防火墙可以通过硬件和软件实现，也可以结合软件和硬件来实现。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，并会阻止不符合指定安全条件的消息。防火墙被认为是保护隐私信息的第一道防线。要获得更高的安全性，可以对数据进行加密。

服务器

为其他计算机上运行的软件提供特定服务的计算机或软件。您的 ISP 的“邮件服务器”是一个软件，用于处理所有 ISP 用户的全部入站和出站邮件。LAN 上的服务器是构成网络上主要节点的硬件。它也可以包含软件，用于为相连的所有客户端计算机提供特定服务、数据或其他功能。

隔离

检测到可疑文件时，会将其隔离。然后，可以采取适当的措施。

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的一种操作。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 Data Backup 发来的电子邮件，指出此文件已共享。电子邮件还包含指向共享文件的链接。

共享密钥

另请参阅 RADIUS。保护 RADIUS 消息的机密部分。此共享密钥是验证者和身份验证服务器之间以某种安全方式共享的密码。

关键字

为已备份的文件指定的词语，用于与指定了相同关键字的其他文件建立关系或联系。为文件指定关键字会使您轻松搜索已发布到 Internet 上的文件。

黑名单

视为有恶意的网站列表。如果网站从事诈骗活动或利用浏览器漏洞将可能有害的程序发给用户，则会将此网站放入黑名单。

还原

从联机备份库或存档中获取文件的副本。

缓冲区溢出

在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）中存储超过其限制的数据时，会发生缓冲区溢出，从而损害或覆盖相邻缓冲区中的有效数据。

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。某些设备可能还包含增强的安全功能和桥接功能。

加密

将数据从文本转换为代码的过程，此过程会隐藏信息，不了解解密方法的人员将无法访问此信息。

家长监控

配置内容评级（限定用户可以查看的网站和内容）及 Internet 时间限制（指定用户可以访问 Internet 的时段）的设置。“家长监控”还会全面限制用户对特定网站的访问权限，并根据年龄组和相关联的关键字授予或阻止访问权限。

监视位置

Data Backup 监视的计算机上的文件夹。

监视文件类型

Data Backup 在监视位置备份或存档的文件类型（如 .doc、.xls 等）。

脚本

脚本可以创建、复制或删除文件。它们还可以打开 Windows 注册表。

接入点 (AP)

一种网络设备，允许 802.11 客户端连接到局域网 (LAN)。接入点为无线用户扩展了服务的实际范围。有时也将其称为无线路由器。

节点

连接到网络上的单台计算机。

拒绝服务

在 Internet 上，拒绝服务 (DoS) 攻击是用户或组织无法使用通常所需资源服务的事件。通常，失去服务是无法使用特定的网络服务（如电子邮件），或临时丢失所有网络连接和服务。例如，在最坏情况下，数百万人访问网站可能偶尔会使网站临时停止工作。拒绝服务攻击还可能会损坏计算机系统上的程序和文件。尽管拒绝服务攻击通常都是有意为之且带有恶意，但有时可能会意外发生拒绝服务攻击。拒绝服务攻击是破坏计算机系统安全的一种类型，但通常不会导致信息遭窃或其他安全损失。不过，这些攻击可能会给目标人员或目标公司带来大量的时间和经济损失。

可能有害的程序

可能有害的程序包括间谍软件、广告软件和其他未经许可收集和传输数据的程序。

客户端

在个人计算机或工作站上运行，并依赖服务器才能执行某些操作的应用程序。例如，电子邮件客户端是允许您收发电子邮件的应用程序。

库

存放 McAfee Data Backup 用户发布的文件的联机存储区。库是 Internet 上的网站，可以访问 Internet 的任何人都能对其进行访问。

快速存档

仅存档自上次完全存档或快速存档后已更改的监视文件。

联机备份库

备份监视文件后存储这些文件的联机服务器上的位置。

浏览器

使用超文本传输协议 (HTTP) 向 Internet 上的 Web 服务器发出请求的客户端程序。Web 浏览器以图形方式为浏览器用户显示内容。

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。路由器会根据内部路由表读取每个入站数据包并决定如何转发它。要将出站数据包发往路由器上的哪个接口，可能由源地址、目标地址以及当前通讯情况（如负载、线路损失及不良线路）的组合来决定。有时也将其称为接入点 (AP)。

漫游

在不中断服务或丢失连接的情况下，从一个接入点覆盖区域移到另一个接入点覆盖区域的能力。

密码

用于获取对计算机、给定程序或网站访问权限的代码（通常为字母数字形式）。

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 McAfee 管理员或系统管理员）访问它们。

密文

已加密的数据。除非使用密钥将密文转换为明文（已解密），否则密文是不可读的。

密钥

两台设备验证通信时所使用的一组字母和/或数字。两台设备都必须有密钥。另请参阅 WEP、WPA、WPA2、WPA-PSK 和 WPA2- PSK。

明文

没有加密的任何消息。

内部网

一种专用网络，通常位于组织内部，其功能与 Internet 非常类似。现在，允许校园外的学生或办公室外的员工使用独立计算机访问内部网是很常见的。防火墙、登录过程和密码都可以提供安全保护。

内容评级组

用户所属的年龄组。根据用户所属的内容评级组对内容进行评级（即使其可用或将其阻止）。内容评级组包括：幼儿、儿童、青少年（较小）、青少年（较大）和成人。

浅层监视位置

计算机上的文件夹，Data Backup 监视其是否有更改。如果设置浅层监视位置，Data Backup 会备份此文件夹（但不包含其子文件夹）内的监视文件类型。

热点

特定的地理位置，接入点 (AP) 在此通过无线网络将公共无线宽带网络服务提供给移动访问者。热点一般都位于人流密集的地方，如机场、火车站、图书馆、码头、会议展览中心和医院。热点的访问距离通常很短。

蠕虫

“蠕虫”是一种驻留在有效内存中的自我复制病毒，并且可通过电子邮件发送自身的副本。蠕虫会自我复制并消耗系统资源，从而降低性能或停止任务。

扫台者

配备有膝上型计算机、特殊软件和其他临时性硬件的闯入者，他们驾车在城市、市郊和商业区穿梭，以便拦截无线 LAN 通信。

身份验证

通常根据用户名和密码确定个人的过程。身份验证会确保此个人是所声称的个人，但不会关注个人的访问权限。

深层监视位置

计算机上的文件夹（和所有子文件夹），Data Backup 监视其是否有更改。如果设置深层监视位置，Data Backup 会备份此文件夹及其子文件夹内的监视文件类型。

实时扫描

在您和您的计算机访问文件时，扫描文件中是否有病毒和其他活动。

事件

来自 0.0.0.0 的事件

如果您看到来自 IP 地址 0.0.0.0 的事件，可能有两个原因。第一个（最常见）的原因是，计算机不知何故收到错误格式的数据包。Internet 并不总是百分之百可靠，有时也会出现错误的数据包。因为 Firewall 在 TCP/IP 验证数据包之前检测这些数据包，所以可能会报告有关这些数据包的事件。

另外一种情况是，源 IP 地址是“伪造”的或是虚假的。伪造的数据包可能表明有人正在扫描以查找特洛伊木马程序，并且碰巧在尝试扫描您的计算机。重要的是要记住，Firewall 会阻止这种企图。

来自 127.0.0.1 的事件

有时，事件会列出源 IP 为 127.0.0.1。要特别注意，此 IP 是特殊的 IP，又称环回地址。

不论您正在使用哪台计算机，127.0.0.1 始终指向您的本地计算机。因为计算机名称 localhost 始终解析为 IP 地址 127.0.0.1，所以此地址也称为 localhost。这是否意味着您的计算机正在尝试攻击自身？或是某种特洛伊木马程序或间谍软件将接管您的计算机？不太可能。很多合法程序都使用环回地址在组件间进行通讯。例如，许多个人邮件或 Web 服务器都可以通过采用 http://localhost/ 之类形式进行访问的 Web 界面来配置。

不过，Firewall 允许来自这些程序的通讯，因此，如果出现来自 127.0.0.1 的事件，很可能意味着源 IP 地址是伪造的或是虚假的。伪造的数据包通常表明有人正在扫描特洛伊木马程序。重要的是要记住，Firewall 会阻止这种企图。很明显，报告来自 127.0.0.1 的事件没什么作用，因此没必要这样做。

尽管如此，有些程序（如 Netscape 6.2 和更高版本）要求将 127.0.0.1 添加到“可信的 IP 地址”列表中。这些程序的组件之间以一种 Firewall 无法判定其通讯是否是本地的方式进行通讯。

以 Netscape 6.2 为例，如果不信任 127.0.0.1，您将无法使用好友名单。因此，如果出现来自 127.0.0.1 的通讯，并且计算机上的所有程序均正常运行，则可以放心地阻止该通讯。不过，如果某个程序（如 Netscape）出现问题，请将 127.0.0.1 添加到 Firewall 的“可信的 IP 地址”列表中，然后了解是否已经解决问题。

如果将 127.0.0.1 添加到“可信的 IP 地址”列表中可以解决问题，则需要考虑所进行的选择：如果信任 127.0.0.1，程序将正常运行，但是您更容易受到欺骗攻击。如果不信任此地址，程序将无法正常运行，但您的计算机能够抵御此类恶意通讯。

来自 LAN 计算机的事件

对于大多数公司的 LAN 设置，您可以信任 LAN 上的全部计算机。

来自专用 IP 地址的事件

采用 192.168.xxx.xxx、10.xxx.xxx.xxx 和 172.16.0.0 - 172.31.255.255 格式的 IP 地址称为无法路由的地址或专用 IP 地址。这些 IP 地址绝不会脱离您的网络，因此，大多数情况下可以信任这些地址。

192.168 块用于 Microsoft Internet 连接共享 (ICS)。如果使用 ICS，并且出现来自此 IP 块的事件，则可能需要将 IP 地址 192.168.255.255 添加到“可信的 IP 地址”列表中。此操作将信任整个 192.168.xxx.xxx 块。

如果没有使用专用网络，但出现来自该 IP 范围的事件，则源 IP 地址可能是伪造的或是虚假的。伪造的数据包通常表明有人正在扫描以查找特洛伊木马程序。重要的是要记住，Firewall 会阻止这种企图。

因为专用 IP 地址与 Internet 上的 IP 地址是分开的，所以报告这些事件没有任何效果。

特洛伊木马程序

特洛伊木马程序是一种经过伪装的程序。因为特洛伊木马程序不能对自身进行复制，所以不是病毒，但它与其他病毒一样具有破坏性。

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。同步功能会用联机备份库中的文件版本更新您计算机上的文件副本。

图像分析

阻止显示可能的不良图像。阻止成人组成员外的所有用户访问图像。

托管网络

包含以下两种类型成员的家庭网络：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监视其 McAfee 保护状态；而非托管成员则不会这样做。

外部硬盘驱动器

位于计算机机箱外的硬盘驱动器。

完全存档

根据已设置的监视文件类型和位置存档全部数据集。

网络

通过连接两台或多台计算机，即可建立一个网络。

网络钓鱼

发音与 fishing 相同，是一种窃取宝贵信息（如信用卡、社会保险编号、用户 ID 和密码）的诈骗手法。表面看似正式的电子邮件，假装可能的受害人的 ISP、银行或零售机构发给可能的受害人。电子邮件可以发给所选列表或任何列表中的人员，期望其中一些收件人实际上刚好拥有真实组织的帐户。

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

在 Network Manager 中，组成家庭网络的计算机和组件的图形表示。

无线适配器

包含电路，可使计算机或其他设备与无线路由器（连接到无线网络）通讯。无线适配器可以内置到硬件设备的主电路中，也可以作为单独的部件，通过适当的端口插入设备。

协议

两台设备之间传输数据的协定格式。从用户点角度来看，他们对协议唯一感兴趣的方面是，如果要与其他计算机通信，其计算机或设备必须支持正确的协议。协议可采用硬件实现，也可以采用软件实现。

压缩

将数据（文件）压缩成某种形式的过程，采用此形式可以最大程度减少存储和传送所需的空间。

域

在层次结构 server.organization.type 中标识地址的所有者的网络连接的地址。例如，www.whitehouse.gov 标识位于白宫的 Web 服务器，它属于美国政府。

中间人攻击

攻击者会拦截公钥交换中的消息，然后重新传输这些消息，用它们自己的公钥替换请求的公钥，这样原来的两方会仍看起来像是相互直接通信。攻击者使用一种程序，此程序会使客户端以为它是服务器，而使服务器以为它是客户端。攻击可以用于仅获取对消息的访问权限，也允许攻击者修改消息，然后重新传输。此术语来源于这样一种球类游戏：许多人尝试互相掷球，而一个人位于中间，试图抓住球。

字典攻击

这些攻击会试用列表中的许多单词，以便确定某人的密码。攻击者不会手动尝试所有组合，而是使用工具来自动尝试，以确定某人的密码。

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。

版权

索引

C

D

E

F

G

H

J

K

L

M

N

P

Q

R

S

T

W

X

Y

Z