McAfee®

VirusScan® Plus 2008

AntiVirus, Firewall & AntiSpyware

用户手册

目录

简介 3

McAfee SecurityCenter....5
SecurityCenter 功能....6
使用 SecurityCenter....7
更新 SecurityCenter....11
修复或忽略保护问题....13
使用警报....17
查看事件....23
McAfee VirusScan....25
VirusScan 功能....26
启动实时病毒防护....27
启动附加防护....29
设置病毒防护....33
扫描计算机....49
处理扫描结果....51
McAfee Personal Firewall....55
Personal Firewall 功能....56
启动 Firewall....59
使用警报....61
管理信息警报....63
配置 Firewall 保护....65
管理程序和权限....75
管理系统服务....83
管理计算机连接....89
记录、监视和分析....97
了解 Internet 安全性....107
McAfee QuickClean....109
QuickClean 功能....110
清理计算机....111
对计算机进行碎片整理....114
计划任务....115
McAfee Shredder....121
Shredder 功能....122
清除文件、文件夹和磁盘....123
McAfee Network Manager....125
Network Manager 功能....126
了解 Network Manager 图标....127
设置托管网络....129
远程管理网络....135
McAfee EasyNetwork....139
EasyNetwork 功能....140
设置 EasyNetwork....141

共享和发送文件 147
共享打印机 153
参考.....155

词汇表 156

关于 McAfee 169

版权 169
许可 170
客户服务和技术支持.....171
使用 McAfee Virtual Technician 172
支持和下载 173

索引 181

第 1 章

简介

McAfee VirusScan Plus 提供主动型 PC 安全功能以避开恶意攻击，能在您安心上网浏览、搜索和下载文件的同时保护您重要的资产。通过使用 McAfee SiteAdvisor 的 Web 安全评级，可帮助您避开不安全的网站。此服务通过组合防病毒、防间谍软件和防火墙技术，可抵御各种混合攻击。McAfee 的安全服务会持续不断地将最新软件传递给您，使您的保护功能永不过时。现在您可以为家中的多台 PC 轻松添加和管理安全性。而且，经改善的性能还能在不干扰您的前提下提供保护。

本章内容

McAfee SecurityCenter....5
McAfee VirusScan....25
McAfee Personal Firewall....55
McAfee QuickClean....109
McAfee Shredder....121
McAfee Network Manager....125
McAfee EasyNetwork....139
参考....155
关于 McAfee....169
客户服务和技术支持....171

第 2 章

McAfee SecurityCenter

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

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

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

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

本章内容

SecurityCenter 功能.....6
使用 SecurityCenter.....7
更新 SecurityCenter.....11
修复或忽略保护问题.....13
使用警报.....17
查看事件.....23

SecurityCenter 功能

SecurityCenter 提供以下功能：

简化的保护状态

轻松查看计算机的保护状态、检查更新和修复可能的保护问题。

自动更新和升级

自动下载和安装注册程序的更新。如果注册的 McAfee 程序有新版本，则可在订购有效期间免费获得，确保您始终获得最新的保护。

实时警报

安全警报会将紧急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。

第 3 章

使用 SecurityCenter

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

本章内容

了解保护状态.....8
了解保护类别.....9
了解保护服务.....9
管理 McAfee 帐户.....10

了解保护状态

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

您计算机的保护状态可能是红色、黄色和绿色。

保护状态	说明
红色	您的计算机未受保护。SecurityCenter 的“主页”窗格上的保护状态区域为红色，表示您未受保护。SecurityCenter 会至少报告一个重要安全问题。 要获取完全保护，您必须修复每个保护类别中的所有重要安全问题（问题类别状态设置为“需要采取操作”时也是红色）。有关如何修复保护问题的信息，请参阅修复保护问题 (第 14 页)。
黄色	您的计算机受到部分保护。SecurityCenter 的“主页”窗格上的保护状态区域为黄色，表示您未受保护。SecurityCenter 会至少报告一个不重要的安全问题。 要获得完全保护，则必须修复或忽略与每个保护类别关联的不重要的安全问题。有关如何修复或忽略保护问题的信息，请参阅修复或忽略保护问题 (第 13 页)。
绿色	您的计算机受到完全保护。SecurityCenter 的“主页”窗格上的保护状态区域为绿色，表示您受到保护。SecurityCenter 不会报告任何重要或不重要的安全问题。 每个保护类别都会列出保护您计算机的服务。

了解保护类别

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

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

保护类别	说明
计算机和文件	“计算机和文件”类别允许配置以下保护服务： ▪ 病毒防护 ▪ 可能有害的程序防护 ▪ 系统监视器 ▪ Windows 保护
Internet 和网络	“Internet 和网络”类别允许配置以下保护服务： ▪ 防火墙保护 ▪ 身份保护
电子邮件和 IM	“电子邮件和 IM”类别允许配置以下保护服务： ▪ 电子邮件保护 ▪ 垃圾邮件防护
家长监控	“家长监控”类别允许配置以下保护服务： ▪ 内容阻止

了解保护服务

保护服务是可以进行配置以保护您计算机的核心 SecurityCenter 组件。保护服务直接与 McAfee 程序对应。例如，在安装 VirusScan 后，可以使用下列保护服务：Virus 防护、可能有害的程序防护、系统监视器和 Windows 保护。有关这些特定保护服务的详细信息，请参阅 VirusScan 帮助。

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

管理 McAfee 帐户

您可以轻松访问和查看帐户信息并验证您的最新订购状态来从 SecurityCenter 中管理 McAfee 帐户。

注意：如果您从光盘安装 McAfee 程序，则必须在 McAfee 网站注册来创建或更新 McAfee 帐户。只有在注册后，您才有权定期自动执行程序更新。

管理 McAfee 帐户

您可以轻松地从 SecurityCenter 访问 McAfee 帐户信息（我的帐户）。

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

验证您的订购

您可以通过验证订购来确保它没有过期。

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

第 4 章

更新 SecurityCenter

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

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

注意：如果从光盘安装 McAfee 程序，则您无法接收这些程序的定期自动更新，除非您在 McAfee 网站上注册。

本章内容

检查更新.....11
配置自动更新.....12
禁用自动更新.....12

检查更新

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

- 在 SecurityCenter 的“主页”窗格中，单击“更新”。

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

配置自动更新

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

注意：SecurityCenter 会使用警报在可以下载或安装更新时通知您。您可以在此警报中下载或安装更新，也可以推迟更新。在从警报中更新程序时，系统可能会提示您在下载和安装前验证订购。有关详细信息，请参阅使用警报 (第 17 页)。

1 打开“SecurityCenter 配置”窗格。

如何实现？

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

2 在“SecurityCenter 配置”窗格的“禁用自动更新”下，单击“开”，然后单击“高级”。

3 单击以下任一按钮：

- **自动安装更新并在服务更新后通知我（建议）**
- **自动下载更新并在可以安装更新时通知我**
- **下载任何更新之前都通知我**

4 单击“确定”。

禁用自动更新

如果禁用自动更新，则您需要定期检测更新；否则，您的计算机不会获得最新的安全保护。有关手动检查更新的信息，请参阅检查更新 (第 11 页)。

1 打开“SecurityCenter 配置”窗格。

如何实现？

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

2 在“SecurityCenter 配置”窗格的“已启用自动更新”下，单击“关”。

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

第 5 章

修复或忽略保护问题

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

本章内容

修复保护问题.....14
忽略保护问题.....15

修复保护问题

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

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

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

自动修复保护问题

SecurityCenter 可以自动修复大多数保护问题。事件日志不会记录 SecurityCenter 自动修复保护问题时所做的配置更改。有关事件的详细信息，请参阅查看事件 (第 23 页)。

1 在“常见任务”下，单击“主页”。

2 在 SecurityCenter 的“主页”窗格的保护状态区域中，单击“修复”。

手动修复保护问题

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

1 在“常见任务”下，单击“主页”。

2 在 SecurityCenter 的“主页”窗格中，单击 SecurityCenter 所报告问题的保护类别。

3 单击问题描述后的链接。

忽略保护问题

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

忽略保护问题

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

1 在“常见任务”下，单击“主页”。

2 在 SecurityCenter 的“主页”窗格中，单击报告问题的保护类别。

3 单击保护问题旁的“忽略”链接。

显示或隐藏忽略的问题

根据问题的严重性，您可以显示或隐藏忽略的保护问题。

1 打开“警报选项”窗格。

如何实现？

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

2 在“SecurityCenter 配置”窗格上，单击“忽略的问题”。

3 在“忽略的问题”窗格上，执行以下操作：

- 若要忽略问题，请选中其复选框。
- 若要在保护类别信息区域报告问题，请清除其复选框。

4 单击“确定”。

提示：您还可以单击保护类别信息区域中已报告问题旁的“忽略”链接来忽略问题。

第 6 章

使用警报

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

下面是三种类型的警报：红色警报、黄色警报和绿色警报。

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

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

本章内容

显示和隐藏信息警报.....18
配置警报选项.....20

显示和隐藏信息警报

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

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

显示或隐藏信息警报

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

1 打开“警报选项”窗格。

如何实现？

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

2 在“SecurityCenter 配置”窗格上，单击“信息警报”。

3 在“信息警报”窗格上，执行以下操作：

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

4 单击“确定”。

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

玩游戏时显示或隐藏信息警报

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

1 打开“警报选项”窗格。

如何实现？

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

2 在“警报选项”窗格上，选中或清除“当检测到游戏模式时显示信息警报”复选框。

3 单击“确定”。

配置警报选项

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

出现警报时播放声音

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

1 打开“警报选项”窗格。

如何实现？

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

2 在“警报选项”窗格的“声音”下，选中“出现警报时播放声音”复选框。

隐藏启动时的启动屏幕

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

1 打开“警报选项”窗格。

如何实现？

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

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

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

隐藏病毒发作警报

您可以隐藏在线社区中通知您有关病毒发作和其他安全威胁的警报。

1 打开“警报选项”窗格。

如何实现？

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

2 在“警报选项”窗格上，清除“当出现病毒或安全威胁时提醒我”复选框。

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

第 7 章

查看事件

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

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

本章内容

查看最新事件.....23
查看所有事件.....23

查看最新事件

如果您只检查发生的最近 30 个事件，则可以查看最新事件。

- 在“常见任务”下，单击“查看最新事件”。

查看所有事件

如果您要检查发生的所有事件的全面列表，可以查看所有事件。

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

第 8 章

McAfee VirusScan

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

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

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

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

本章内容

VirusScan 功能 26
开始实时病毒防护 27
启动附加防护 29
设置病毒防护 33
扫描计算机 49
处理扫描结果 51

VirusScan 功能

VirusScan 提供以下功能。

全面病毒防护

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

资源感知扫描选项

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

自动修复

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

在全屏幕模式下暂停任务

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

启动实时病毒防护

VirusScan 提供两种类型的病毒防护：实时和手动。实时病毒防护会持续监视计算机中的病毒活动，每次您或您的计算机访问文件时都会扫描文件。手动病毒防护允许您按需扫描文件。为确保您的计算机能抵御最新的安全威胁，请将实时病毒防护打开，并建立一个计划以进行定期的全面手动扫描。默认情况下，VirusScan 会每周执行计划扫描一次。有关实时扫描和手动扫描的详细信息，请参阅扫描计算机 (第 49 页)。

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

启动实时病毒防护

默认情况下，系统会打开实时病毒防护，保护您的计算机免受病毒、特洛伊木马程序和其他安全威胁的侵扰。如果您关闭实时病毒防护，则必须再次将其打开，以便始终受到保护。

1 打开“计算机和文件配置”窗格。

如何实现？

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

2 在“病毒防护”下，单击“开”。

停止实时病毒防护

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

1 打开“计算机和文件配置”窗格。

如何实现？

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

2 在“病毒防护”下，单击“关”。

3 在对话框中，选择恢复实时扫描的时间。

4 单击“确定”。

第 9 章

启动附加防护

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

脚本扫描防护

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

间谍软件防护

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

电子邮件保护

电子邮件保护会检测您收发的电子邮件和附件中的可疑活动。

即时消息保护

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

本章内容

启动脚本扫描防护.....30
启动间谍软件防护.....30
启动电子邮件保护.....30
启动即时消息保护.....31

启动脚本扫描防护

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

1 打开“计算机和文件配置”窗格。

如何实现？

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

2 在“脚本扫描防护”下，单击“开”。

注意：您可以随时关闭脚本扫描防护，但这样做会使有害脚本利用计算机的漏洞。

启动间谍软件防护

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

1 打开“计算机和文件配置”窗格。

如何实现？

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

2 在“脚本扫描防护”下，单击“开”。

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

启动电子邮件保护

关闭电子邮件保护会在出站 (SMTP) 和入站 (POP3) 电子邮件消息和附件中检测蠕虫以及可能的威胁。

1 打开“电子邮件和 IM 配置”窗格。

如何实现？

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

2 在“电子邮件保护”下，单击“开”。

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

启动即时消息保护

打开即时消息保护会检测入站即时消息附件中可能包含的安全威胁。

1 打开“电子邮件和 IM 配置”窗格。

如何实现？

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

2 在“即时消息保护”下，单击“开”。

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

第 10 章

设置病毒防护

VirusScan 提供两种类型的病毒防护：实时和手动。实时病毒防护扫描会在您或您的计算机每次访问文件时对其进行扫描。手动病毒防护允许您按需扫描文件。您可以为每个类型的保护设置不同选项。例如，因为实时保护会持续监视您的计算机，所以您可以选择一些基本扫描选项，为手动、按需保护保留一组更全面的扫描选项。

本章内容

设置实时扫描选项.....34
设置手动扫描选项.....36
使用 SystemGuard 选项.....40
使用可信列表.....46

设置实时扫描选项

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

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

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

设置实时扫描选项

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

1 打开实时扫描窗格。

如何实现？

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

2 指定实时扫描选项，然后单击“确定”。

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

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

设置手动扫描选项

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

默认情况下，VirusScan 会在每次运行手动扫描时检查计算机上的所有驱动器和文件夹；不过，您可以更改默认位置来满足您的需要。例如，您可以只扫描重要的系统文件、桌面上的项目或程序文件夹中的项目。除非您要自行启动每个手动扫描，否则可以设置定期扫描计划。计划扫描始终会使用默认扫描选项来检查整个计算机。默认情况下，VirusScan 会每周执行一次计划的扫描。

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

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

设置手动扫描选项

您可以设置手动扫描选项来自定义 VirusScan 在手动扫描时查找的内容，以及扫描的位置和文件类型。这些选项包括扫描未知病毒、文件存档、间谍软件和可能有害的程序、跟踪 Cookie、Rootkit 和隐匿程序。

1 打开“手动扫描”窗格。

如何实现？

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

2 指定手动扫描选项，然后单击“确定”。

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

设置手动扫描位置

您可以设置手动扫描位置来确定 VirusScan 在手动扫描时查找病毒和其他有害项目的位置。您可以扫描计算机上的所有文件、文件夹和驱动器，也可以限定扫描特定的文件和驱动器。

1 打开“手动扫描”窗格。

如何实现？

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

2 单击“默认扫描位置”。

3 指定手动扫描位置，然后单击“确定”。

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

计划扫描

计划扫描可以一周的任何时间和日期对计算机上的病毒和其他威胁进行彻底的扫描。计划的扫描始终会使用默认扫描选项来检查整个计算机。默认情况下，VirusScan 会每周执行一次计划的扫描。如果您发现扫描速度很慢，则可以考虑禁用此选项来使用最小计算机资源，但切记授予病毒防护的优先级要高于其他任务的优先级。

1 打开“计划的扫描”窗格。

如何实现？

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

2 选中“启用计划的扫描”。

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

4 选择一天或多天。

5 指定开始时间。

6 单击“确定”。

提示：您可以单击“重置”来恢复默认的计划。

使用 SystemGuard 选项

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

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

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

程序 SystemGuard

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

Windows SystemGuard

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

浏览 SystemGuard

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

启用 SystemGuard 保护

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

1 打开“计算机和文件配置”窗格

如何实现？

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

2 在“SystemGuard 保护”下，单击“开”。

注意：您可以单击“关”来禁用 SystemGuard 保护。

配置 SystemGuard 选项

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

1 打开“SystemGuard”窗格。

如何实现？

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

2 从列表中选择 SystemGuard 类型。

- **程序 SystemGuard**

- Windows SystemGuard
- 浏览 SystemGuard

3 在“我想”下，执行以下任一操作：

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

注意：有关 SystemGuard 类型的详细信息，请参阅关于 SystemGuard 类型 (第 42 页)。

关于 SystemGuard 类型

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

程序 SystemGuard

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

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

Windows SystemGuard

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

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

SystemGuard	检测...
Windows Win.ini 文件	间谍软件、广告软件和其他可能有害的程序，这些程序可能对 Win.ini 文件进行更改，从而在启动计算机时运行可疑程序。

浏览器 SystemGuard

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

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

SystemGuard	检测...
Internet Explorer 受信任的站点	间谍软件、广告软件和其他可能有害的程序，这些程序可能对 Internet Explorer 受信任的站点进行注册表更改，从而使浏览器信任可疑的网站。
Internet Explorer 策略	间谍软件、广告软件和其他可能有害的程序，这些程序可能对 Internet Explorer 策略进行注册表更改，从而影响浏览器的外观和行为。

使用可信列表

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

管理可信列表

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

1 打开“可信列表”窗格。

如何实现？

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

2 从下列信任列表类型中选择一个类型：

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

3 在“我想”下，执行以下任一操作：

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

4 单击“确定”。

注意：有关可信列表类型的详细信息，请参阅关于可信列表类型 (第 47 页)。

关于可信列表类型

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

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

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

第 11 章

扫描计算机

首次启动 SecurityCenter 时，VirusScan 的实时病毒防护会开始保护您的计算机免受可能有害病毒、特洛伊木马程序和其他安全威胁的侵扰。除非禁用实时病毒防护，否则 VirusScan 会使用您设置的实时扫描选项持续监视计算机中的病毒活动，每次您和您的计算机访问文件时扫描这些文件。为确保您的计算机能抵御最新的安全威胁，请将实时病毒防护打开，并建立一个计划以进行定期的全面手动扫描。有关设置实时和手动扫描选项的详细信息，请参阅设置病毒防护 (第 33 页)。

VirusScan 提供一组详细的扫描选项供手动病毒防护使用，使您可以定期运行更广泛的扫描。您可以从 SecurityCenter 中运行手动扫描，根据设置的计划扫描特定的位置。不过，您还可以在工作时直接在 Windows 资源管理器中运行手动扫描。SecurityCenter 中扫描的优点是可以动态更改扫描选项。不过，从 Windows Explorer 中进行扫描是一种为计算机提供安全保护的便捷方法。

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

本章内容

扫描计算机.....49
查看扫描结果.....50

扫描计算机

您可以从 SecurityCenter 中的“高级”或“基本”菜单运行手动扫描。如果从“高级”菜单中运行扫描，则可以在扫描前确认手动扫描选项。如果从“基本”菜单中运行扫描，则 VirusScan 会使用现有的扫描选项立即开始扫描。您还可以使用现有扫描选项在 Windows 资源管理器中运行扫描。

- 执行下面某项操作：

  在 SecurityCenter 中扫描

要...	执行此操作...
使用现有设置扫描	在“基本”菜单上单击“扫描”。
使用已更改的设置进行扫描	在“高级”菜单上单击“扫描”，选择要扫描的位置，选择扫描选项，然后单击“立即扫描”。

在 Windows 资源管理器中扫描

1. 打开 Windows 资源管理器。
2. 右键单击文件、文件夹或驱动器，然后单击“扫描”。

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

查看扫描结果

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

- 在“基本”菜单和“高级”菜单上，单击“扫描”，然后执行以下操作：

要...	执行此操作...
查看警报中的扫描结果	查看“扫描已完成”警报中的扫描结果。
查看有关扫描结果的详细信息	单击查看“扫描已完成”中的“查看扫描详细信息”。
查看扫描结果的快速摘要	指向任务栏通知区域中的“扫描已完成”图标。
查看扫描和检测统计信息	双击任务栏通知区域中的“扫描已完成”图标。
查看有关检测到的项目、感染状态和类型的详细信息。	双击任务栏通知区域中的“扫描已完成”图标，然后在“扫描进度”中单击“查看结果”。“手动扫描”窗格。

第 12 章

处理扫描结果

在运行实时或手动扫描时，如果 VirusScan 检测到安全威胁，它会尝试根据威胁类型自动处理威胁。例如，如果 VirusScan 在计算机上检测到病毒、特洛伊木马程序或跟踪 Cookie，它会尝试清理感染病毒的文件。如果无法清理文件，则 VirusScan 会将其隔离。

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

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

本章内容

处理病毒和特洛伊木马程序.....51
处理可能有害的程序.....52
处理隔离的文件.....52
处理隔离的程序和 Cookie.....53

处理病毒和特洛伊木马程序

在实时扫描或手动扫描时，如果 VirusScan 在计算机的文件中检测到病毒或特洛伊木马程序，则会尝试将其清理。如果无法清理文件，则 VirusScan 会尝试将其隔离。如果隔离也失败，则拒绝对此文件进行访问（仅限实时扫描）。

1 打开“扫描结果”窗格。

如何实现？

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

2 在扫描结果列表中，单击“病毒和特洛伊木马程序”。

注意：要处理 VirusScan 已隔离的文件，请参阅处理隔离的文件 (第 52 页)。

处理可能有害的程序

在实时扫描或手动扫描时，如果 VirusScan 在计算机上检测到可能有害的程序，则可以删除或信任此程序。删除可能有害的程序不会从系统中实际删除该程序。相反，删除操作会隔离程序，防止程序损害计算机或文件。

1 打开“扫描结果”窗格。

如何实现？

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

2 在扫描结果列表中，单击“可能有害的程序”。

3 选择可能有害的程序。

4 在“我想”下面，单击“删除”或“信任”。

5 确认您所选的选项。

处理隔离的文件

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

1 打开“隔离的文件”窗格。

如何实现？

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

2 选择隔离的文件。

3 执行下面某项操作：

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

4 单击“是”确认所选的选项。

提示：您可以同时恢复或删除多个文件。

处理隔离的程序和 Cookie

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

1 打开“隔离的程序”和“跟踪 Cookie”窗格。

如何实现？

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

2 选择隔离的程序或 Cookie。

3 执行下面某项操作：

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

4 单击“是”确认此操作。

提示：您可以同时恢复或删除多个程序和 Cookie。

第 13 章

McAfee Personal Firewall

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

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

本章内容

Personal Firewall 功能.....56
启动 Firewall.....59
使用警报.....61
管理信息警报.....63
配置 Firewall 保护.....65
管理程序和权限.....75
管理系统服务.....83
管理计算机连接.....89
记录、监视和分析.....97
了解 Internet 安全性.....107

Personal Firewall 功能

Personal Firewall 提供以下功能。

标准和自定义保护级别

使用 Firewall 的默认或可自定义保护设置防止入侵和可疑活动。

实时建议

动态接收建议，帮助您确定是否应授予程序 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，或为特定程序配置访问权限。

游戏保护

在玩全屏游戏期间，可以防止有关入侵尝试和可疑活动的警报分散您的注意力。

计算机启动保护

在 Windows® 启动后，Firewall 会保护您的计算机免受入侵尝试和有害程序以及网络通讯的侵扰。

系统服务端口控制

管理某些程序所需的打开和关闭的系统服务端口。

管理计算机连接

允许或阻止其他计算机与您计算机之间的远程连接。

HackerWatch 信息集成

通过 HackerWatch 网站跟踪全局黑客攻击和入侵模式，该网站还提供有关您计算机上程序的当前安全信息，以及提供全局安全事件和 Internet 端口统计信息。

锁定 Firewall

立即阻止您的计算机与 Internet 之间的所有入站和出站通讯。

恢复 Firewall

立即恢复 Firewall 的最初保护设置。

高级特洛伊木马程序检测

检测并阻止可能有恶意的应用程序（如特洛伊木马），以防个人信息传播到 Internet。

事件记录

跟踪最近的入站、出站和入侵事件。

监视 Internet 通讯

查看显示恶意攻击和通讯来源的世界地图。此外，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

保护您的隐私免受可能的 Internet 威胁。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。

第 14 章

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。系统会自动启用“智能建议”和“信任”安全级别（选择此选项可以允许程序仅出站 Internet 访问权限）。

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® Firewall 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。

本章内容

启动防火墙保护.....59
停止防火墙保护.....60

启动防火墙保护

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

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

停止防火墙保护

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

1 在“McAfee SecurityCenter”窗格上，单击“Internet 和网络”，然后单击“配置”。

2 在“Internet 和网络配置”窗格的“已启用防火墙保护”下，单击“关”。

第 15 章

使用警报

Firewall 使用一组警报来帮助您管理安全性。这些警报可以分为三种基本类型：

- 红色警报
- 黄色警报
- 绿色警报

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

本章内容

关于警报.....62

关于警报

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

红色警报

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

黄色警报

最常见的警报类型是黄色警报，将有关 Firewall 检测到的程序活动或网络事件的信息通知给您。发生此警报时，此警报会描述程序活动或网络事件，然后向您提供需要响应的一个或多个选项。例如，当安装 Firewall 的计算机连接到新网络时，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”。如果启用“智能建议”，则会将程序添加到“程序权限”窗格中。

绿色警报

在大多数情况下，绿色警报提供有关事件的基本信息，且不需要响应。默认情况下会禁用绿色警报，通常会在设置“标准”、“信任”、“严格”和“隐匿”安全级别后显示。

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，警报可能建议您允许某个程序的访问权限。

第 16 章

管理信息警报

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

本章内容

玩游戏时显示警报.....63
隐藏信息警报.....63

玩游戏时显示警报

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

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

隐藏信息警报

您可以防止 Firewall 在检测到入侵尝试或可疑活动时显示 Firewall 信息警报。

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

第 17 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，您的计算机保护安全级别会设置为“信任”，而且允许程序仅出站 Internet 访问。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 66
配置警报的“智能建议” 69
优化 Firewall 安全性 71
锁定和恢复 Firewall 73

管理 Firewall 安全级别

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

在设置“信任”安全级别且启用了“智能建议”后，黄色警报提供的选项可以允许或阻止需要入站访问权限的未知程序的访问。检测到已知的程序时，会显示绿色信息警报，并会自动允许访问权限。允许访问权限会使程序创建出站连接并侦听未经请求的入站连接。

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

下表说明了 Firewall 的六个安全级别，依次为最严格的级别到最宽松的级别：

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

Firewall 还允许在“恢复防火墙保护默认值”窗格中将安全级别立即重置为“信任”（并允许仅出站访问权限）。

将安全级别设置为“锁定”

您可以将 Firewall 的安全级别设置为“锁定”以阻止所有入站和出站网络连接。

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

将安全级别设置为“隐匿”

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

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

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

将安全级别设置为“严格”

如果将 Firewall 安全级别设置为“严格”，以在新程序尝试进行出站 Internet 连接或接收入站连接请求时接收警报。

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

注意：在“严格”模式下，程序只请求它当时需要的访问类型，如仅出站访问，您可以允许或阻止此访问权限。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”窗格中允许此程序具有完全访问权限。

将安全级别设置为“标准”

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

1 在“McAfee SecurityCenter”窗格上，单击“Internet 和网络”，然后单击“配置”。

2 在“Internet 和网络配置”窗格的“已启用防火墙保护”下，单击“高级”。

3 在“安全级别”窗格上，移动滑块，直至“标准”显示为当前级别。

4 单击“确定”。

将安全级别设置为“信任”

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

1 在“McAfee SecurityCenter”窗格上，单击“Internet 和网络”，然后单击“配置”。

2 在“Internet 和网络配置”窗格的“已启用防火墙保护”下，单击“高级”。

3 在“安全级别”窗格上，移动滑块，直至“信任”显示为当前级别。

4 执行下面某项操作：

- 要允许完全入站和出站网络访问权限，请选择“允许完全访问”。
- 要允许仅出站网络访问权限，请选择“仅允许出站访问”。

5 单击“确定”。

注意：“仅允许出站访问”是默认选项。

将安全级别设置为“开放”

您可以将 Firewall 的安全级别设置为“打开”以允许所有入站和出站网络连接。

1 在“McAfee SecurityCenter”窗格上，单击“Internet 和网络”，然后单击“配置”。

2 在“Internet 和网络配置”窗格的“已启用防火墙保护”下，单击“高级”。

3 在“安全级别”窗格上，移动滑块，直至“开放”显示为当前级别。

4 单击“确定”。

配置警报的“智能建议”

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

如果启用了“智能建议”（且安全级别设为“信任”，启用了仅出站访问权限），则 Firewall 会自动允许或阻止已知的程序，并在检测到可能有危险的程序时，在警报中显示建议。

如果禁用“智能建议”，则 Firewall 既不会允许或阻止 Internet 访问，也不会在警报中建议采用某个操作计划。

如果将“智能建议”设为“仅显示”时，则出现的警报会提示您允许或阻止访问，而且会在警报中建议您采取某个操作计划。

启用“智能建议”

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

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

禁用“智能建议”

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

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

仅显示“智能建议”

您可以显示警报的“智能建议”，使其只提供操作计划建议，以便您可以确定允许或阻止无法识别的和可能有危险的程序。

1. 在“McAfee SecurityCenter”窗格上，单击“Internet 和网络”，然后单击“配置”。
2. 在“Internet 和网络配置”窗格的“已启用防火墙保护”下，单击“高级”。
3. 在“安全级别”窗格的“智能建议”下，选择“仅显示”。
4. 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跟踪（或 ping）您的计算机，以确定它是否连接到网络上。Firewall 支持启用启动时保护和阻止 ping 请求，从而防止两种类型的入侵。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

您可以在 Windows 启动时阻止以前启动时没有但现在需要 Internet 访问权限的新程序来保护您的计算机。Firewall 会显示已请求访问 Internet 的程序的相关警报，您可以允许或阻止此访问。要使用此选项，不得将安全级别设置为“开放”或“锁定”。

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

注意：启用启动时保护后，不记录已阻止的连接和入侵。

配置 ping 请求设置

您可以允许或阻止网络上其他计算机用户检测您的计算机。

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

配置入侵检测

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

1 在“McAfee SecurityCenter”窗格上，单击“Internet 和网络”，然后单击“配置”。

2 在“Internet 和网络配置”窗格的“已启用防火墙保护”下，单击“高级”。

3 在“Firewall”窗格上，单击“入侵检测”。

4 在“检测入侵尝试”下，执行以下任一操作：

- 选中名称以自动检测攻击或扫描。
- 清除名称以禁用自动检测攻击或扫描。

5 单击“确定”。

配置 Firewall 的“保护状态”设置

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

1 在“McAfee SecurityCenter”窗格的“SecurityCenter 信息”下，单击“配置”。

2 在“SecurityCenter 配置”窗格的“保护状态”下，单击“高级”。

3 在“忽略的问题”窗格中，选择下列一个或多个选项：

- **已禁用防火墙保护。**
- **防火墙已设置为“开放”安全级别。**
- **防火墙服务没有运行。**
- **您的计算机未安装防火墙保护。**
- **已禁用您的 Windows 防火墙。**
- **您的计算机未安装出站防火墙。**

4 单击“确定”。

锁定和恢复 Firewall

“锁定”功能会立即阻止所有入站和出站网络通讯，帮助您隔离和解决计算机上的问题。

立即锁定 Firewall

您可以立即锁定 Firewall 以阻止您的计算机和 Internet 之间的所有网路通讯。

1. 在“McAfee SecurityCenter”窗格的“常见任务”下，单击“锁定 Firewall”。
2. 在“锁定 Firewall”窗格上，单击“锁定”。
3. 单击“是”进行确认。

提示：您还可以右键单击任务栏右侧通知区域的 SecurityCenter 图标，依次单击“快速链接”、“锁定 Firewall”来锁定 Firewall。

立即解锁 Firewall

您可以立即对 Firewall 解锁以允许您的计算机和 Internet 之间的所有网路通讯。

1. 在“McAfee SecurityCenter”窗格的“常见任务”下，单击“锁定 Firewall”。
2. 在“已启用锁定”窗格上，单击“解锁”。
3. 单击“是”进行确认。

恢复 Firewall 设置

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

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

提示：您还可以右键单击任务栏右侧通知区域的 SecurityCenter 图标，依次单击“快速链接”、“恢复防火墙默认值”来恢复 Firewall 的默认设置。

第 18 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 允许控制程序的完全或仅出站访问权限。您还可以阻止程序的访问权限。

本章内容

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

允许程序访问 Internet

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

Firewall 允许使用“程序权限”页：

- 允许程序具有访问权限
- 允许程序具有仅出站访问权限
- 阻止程序访问

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

允许程序具有完全访问权限

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

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

允许新程序具有完全访问权限

您可以允许计算机上的新程序具有完全入站和出站 Internet 访问权限。

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

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

从“最新事件”日志中允许完全访问权限

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

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

相关主题

- 查看出站事件 (第 99 页)

从“出站事件”日志中允许完全访问权限

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

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

允许程序具有仅出站访问权限

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

允许程序具有仅出站访问权限

您可以允许程序具有仅出站 Internet 访问权限。

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

从“最新事件”日志中允许仅出站访问权限

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

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

从“出站事件”日志允许仅出站访问权限

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

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

阻止程序的 Internet 访问权限

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。

阻止程序具有访问权限

您可以阻止程序具有入站和出站 Internet 访问权限。

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

阻止新程序的访问权限

您可以阻止新程序具有入站和出站 Internet 访问权限。

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

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

从“最新事件”日志阻止访问权限

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

1 在“McAfee SecurityCenter”窗格上，单击“高级菜单”。

2 单击“报告和日志”。

3 在“最新事件”下，选择事件说明，然后单击“阻止访问”。

4 在“程序权限”对话框中，单击“是”确认。

删除程序的访问权限

删除程序的权限之前，确保缺少此权限不会影响计算机的功能或网络链接。

删除程序权限

您可以删除程序的入站和出站 Internet 访问权限。

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

注意：Firewall 会禁止通过使某些操作变灰以及将其禁用来修改某些程序。

了解程序

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

获取程序信息

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

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

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

从“出站事件”日志获取程序信息

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

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

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

第 19 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。

本章内容

配置系统服务端口.....84

配置系统服务端口

可以将系统服务端口配置为允许或阻止对计算机上服务的远程网络访问权限。

下面的列表显示常见的系统服务及其关联的端口：

- 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
- 网络时间协议端口 123
- 远程桌面/远程协助/终端服务器 (RDP) 端口 3389
- 远程过程调用 (RPC) 端口 135
- 安全 Web 服务器 (HTTPS) 端口 443
- 通用即插即用 (UPNP) 端口 5000
- Web 服务器 (HTTP) 端口 80
- Windows 文件共享 (NETBIOS) 端口 137-139

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

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

允许访问现有的系统服务端口

您可以打开现有的端口来允许对计算机上的网络服务进行远程访问。

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

1. 在“McAfee SecurityCenter”窗格上，单击“Internet 和网络”，然后单击“配置”。
2. 在“Internet 和网络配置”窗格的“已启用防火墙保护”下，单击“高级”。
3. 在“Firewall”窗格上，单击“系统服务”。
4. 在“打开系统服务端口”下，选择要打开其端口的系统服务。
5. 单击“确定”。

阻止访问现有的系统服务端口

您可以关闭现有的端口来阻止计算机上的网络服务进行远程访问。

1. 在“McAfee SecurityCenter”窗格上，单击“Internet 和网络”，然后单击“配置”。
2. 在“Internet 和网络配置”窗格的“已启用防火墙保护”下，单击“高级”。
3. 在“Firewall”窗格上，单击“系统服务”。
4. 在“打开系统服务端口”下，清除要关闭其端口的系统服务。
5. 单击“确定”。

配置新服务端口

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

1. 在“McAfee SecurityCenter”窗格上，单击“Internet 和网络”，然后单击“配置”。
2. 在“Internet 和网络配置”窗格的“已启用防火墙保护”下，单击“高级”。
3. 在“Firewall”窗格上，单击“系统服务”。
4. 单击“添加”。
5. 在“系统服务”窗格的“端口和系统服务”下，输入以下内容：
   - 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

6 如果您要将此端口活动信息发给共享 Internet 连接的其他联网 Windows 计算机，请选择“将此端口上的网络活动转发给使用 Internet 连接共享的网络用户”。

7 （可选）描述新配置。

8 单击“确定”。

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

修改系统服务端口

您可以修改有关现有系统服务端口的入站和出站网络访问信息。

注意：如果输入的端口信息不正确，则系统服务失败。

1 在“McAfee SecurityCenter”窗格上，单击“Internet 和网络”，然后单击“配置”。

2 在“Internet 和网络配置”窗格的“已启用防火墙保护”下，单击“高级”。

3 在“Firewall”窗格上，单击“系统服务”。

4 选择系统服务，然后单击“编辑”。

5 在“系统服务”窗格的“端口和系统服务”下，输入以下内容：

- 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

6 如果您要将此端口活动信息发给共享 Internet 连接的其他联网 Windows 计算机，请选择“将此端口上的网络活动转发给使用 Internet 连接共享的网络用户”。

7 （可选）描述修改的配置。

8 单击“确定”。

删除系统服务端口

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

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

第 20 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.....90
禁止计算机连接.....93

信任计算机连接

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

在“信任的和禁止的 IP”窗格上的“信任的 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“信任的 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 不会过滤或分析与信任 IP 地址相关联的计算机和您计算机之间的活动。默认情况下，“信任的 IP 地址”会列出 Firewall 找到的第一个专用网络。

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

您可以添加信任的计算机连接及其关联的 IP 地址。

1. 在“McAfee SecurityCenter”窗格上，单击“Internet 和网络”，然后单击“配置”。
2. 在“Internet 和网络配置”窗格的“已启用防火墙保护”下，单击“高级”。
3. 在“Firewall”窗格上，单击“信任的和禁止的 IP”。
4. 在“信任的和禁止的 IP”窗格上，选择“信任的 IP 地址”，然后单击“添加”。
5. 在“添加信任的 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 如果系统服务使用 Internet 连接共享 (ICS)，则可以添加下列 IP 地址范围：192.168.0.1 到 192.168.0.255。

7 （可选）选中“规则过期时间”，然后输入实施此规则的天数。

8 （可选）键入规则的说明。

9 单击“确定”。

10 在“信任的和禁止的 IP”对话框中，单击“是”确认。

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

从“入站事件”日志添加信任的计算机

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。

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

2 单击“报告和日志”。

3 在“最新事件”下，单击“查看日志”。

4 单击“Internet 和网络”，然后单击“入站事件”。

5 选择源 IP 地址，然后在“我想”下单击“信任此地址”。

6 单击“是”进行确认。

编辑信任的计算机连接

您可以编辑信任的计算机连接及其关联的 IP 地址。

1 在“McAfee SecurityCenter”窗格上，单击“Internet 和网络”，然后单击“配置”。

2 在“Internet 和网络配置”窗格的“已启用防火墙保护”下，单击“高级”。

3 在“Firewall”窗格上，单击“信任的和禁止的 IP”。

4 在“信任的和禁止的 IP”窗格上，选择“信任的 IP 地址”。

5 选择 IP 地址，然后单击“编辑”。

6 在“编辑信任的 IP 地址”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。

7 （可选）选中“规则过期时间”，并输入实施此规则的天数。

8 （可选）键入规则的说明。

9 单击“确定”。

注意：您不能编辑 Firewall 从信任专用网络中自动添加的默认计算机连接。

删除信任的计算机连接

您可以删除信任的计算机连接及其关联的 IP 地址。

1 在“McAfee SecurityCenter”窗格上，单击“Internet 和网络”，然后单击“配置”。

2 在“Internet 和网络配置”窗格的“已启用防火墙保护”下，单击“高级”。

3 在“Firewall”窗格上，单击“信任的和禁止的 IP”。

4 在“信任的和禁止的 IP”窗格上，选择“信任的 IP 地址”。

5 选择 IP 地址，然后单击“删除”。

6 在“信任的和禁止的 IP”对话框中，单击“是”确认。

禁止计算机连接

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

可以禁止与未知、可疑或不信任 IP 相关联的计算机连接到您的计算机。

因为 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

您可以添加禁止的计算机连接及其关联的 IP 地址。

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

1. 在“McAfee SecurityCenter”窗格上，单击“Internet 和网络”，然后单击“配置”。
2. 在“Internet 和网络配置”窗格的“已启用防火墙保护”下，单击“高级”。
3. 在“Firewall”窗格上，单击“信任的和禁止的 IP”。
4. 在“信任的和禁止的 IP”窗格上，选择“禁止的 IP 地址”，然后单击“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”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”。
9. 在“信任的和禁止的 IP”对话框中，单击“是”确认。

编辑禁止的计算机连接

您可以编辑禁止的计算机连接及其关联的 IP 地址。

1 在“McAfee SecurityCenter”窗格上，单击“Internet 和网络”，然后单击“配置”。

2 在“Internet 和网络配置”窗格的“已启用防火墙保护”下，单击“高级”。

3 在“Firewall”窗格上，单击“信任的和禁止的 IP”。

4 在“信任的和禁止的 IP”窗格上，选择“禁止的 IP 地址”，然后单击“编辑”。

5 在“编辑禁止的 IP 地址”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”。

删除禁止的计算机连接

您可以删除禁止的计算机连接及其关联的 IP 地址。

1 在“McAfee SecurityCenter”窗格上，单击“Internet 和网络”，然后单击“配置”。

2 在“Internet 和网络配置”窗格的“已启用防火墙保护”下，单击“高级”。

3 在“Firewall”窗格上，单击“信任的和禁止的 IP”。

4 在“信任的和禁止的 IP”窗格上，选择“禁止的 IP 地址”。

5 选择 IP 地址，然后单击“删除”。

6 在“信任的和禁止的 IP”对话框中，单击“是”确认。

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包含已允许访问 Internet 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，而且确信必须阻止某个地址访问打开的端口时，才应该将该 IP 地址添加到“禁止的 IP 地址”列表中。

“入站事件”页面列出了所有 Internet 入站通讯的 IP 地址，可以使用该页面禁止可疑的或有害的 Internet 活动的源 IP 地址。

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

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。

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

第 21 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.....98
使用统计信息.....100
跟踪 Internet 通讯.....101
监视 Internet 通讯.....104

事件记录

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

配置事件日志设置

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

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

查看最新事件

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

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

查看入站事件

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

1 确保启用了“高级”菜单。在“常见任务”窗格上，单击“报告和日志”。

2 在“最新事件”下，单击“查看日志”。

3 单击“Internet 和网络”，然后单击“入站事件”。

注意：您可以从“入站事件”日志信任、禁止和跟踪 IP 地址。

查看出站事件

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

1 在“常见任务”窗格上，单击“报告和日志”。

2 在“最新事件”下，单击“查看日志”。

3 单击“Internet 和网络”，然后单击“出站事件”。

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

查看入侵检测事件

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

1 在“常见任务”窗格上，单击“报告和日志”。

2 在“最新事件”下，单击“查看日志”。

3 单击“Internet 和网络”，然后单击“入侵检测事件”。

注意：您可以从“入侵检测事件”日志禁止和跟踪 IP 地址。

使用统计信息

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。

1 确保已启用了“高级菜单”，然后单击“工具”。

2 在“工具”窗格上，单击“HackerWatch”。

3 在“事件跟踪”下，查看安全事件统计信息。

查看全球 Internet 端口活动

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

1 确保已启用了“高级菜单”，然后单击“工具”。

2 在“工具”窗格上，单击“HackerWatch”。

3 查看“最近的端口活动”下最重要的事件端口事件。

跟踪 Internet 通讯

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。

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“地图视图”。

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。

1 确保已启用了“高级菜单”，然后单击“工具”。

2 在“工具”窗格上，单击“可视跟踪程序”。

3 键入计算机的 IP 地址，然后单击“跟踪”。

4 在“可视跟踪程序”下，选择“注册人视图”。

获取计算机网络信息

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

1 确保已启用了“高级菜单”，然后单击“工具”。

2 在“工具”窗格上，单击“可视跟踪程序”。

3 键入计算机的 IP 地址，然后单击“跟踪”。

4 在“可视跟踪程序”下，选择“网络视图”。

从“入站事件”日志跟踪计算机

在“入站事件”窗格中，可以跟踪“入站事件”日志中显示的 IP 地址。

1 确保启用了“高级”菜单。在“常见任务”窗格上，单击“报告和日志”。

2 在“最新事件”下，单击“查看日志”。

3 单击“Internet 和网络”，然后单击“入站事件”。

4 在“入站事件”窗格上，选择源 IP 地址，然后单击“跟踪此地址”。

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”。

从“入侵检测事件”日志跟踪计算机

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

1 在“常见任务”窗格上，单击“报告和日志”。

2 在“最新事件”下，单击“查看日志”。

3 单击“Internet 和网络”，然后单击“入侵检测事件”。在“入侵检测事件”窗格中，选择源 IP 地址，然后单击“跟踪此地址”。

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”。

跟踪监视的 IP 地址

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

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

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。

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。

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

提示：要查看最新的统计信息，请单击“流量分析”下的“刷新”。

监视程序带宽

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

1 确保已启用了“高级菜单”，然后单击“工具”。

2 在“工具”窗格上，单击“通讯流量监视器”。

3 在“通讯流量监视器”下，单击“带宽使用率”。

提示：要查看最新的统计信息，请单击“带宽使用率”下的“刷新”。

监视程序活动

您可以查看入站和出站程序活动，这会显示远程计算机连接和端口。

1 确保已启用了“高级菜单”，然后单击“工具”。

2 在“工具”窗格上，单击“通讯流量监视器”。

3 在“通讯流量监视器”下，单击“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 22 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.....108

启动 HackerWatch 教程

要了解 Firewall，可以从 SecurityCenter 访问 HackerWatch 教程。

1 确保已启用了“高级菜单”，然后单击“工具”。

2 在“工具”窗格上，单击“HackerWatch”。

3 在“HackerWatch 资源”下，单击“查看教程”。

第 23 章

McAfee QuickClean

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

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

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

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

本章内容

QuickClean 功能.....110
清理计算机.....111
对计算机进行碎片整理.....114
计划任务.....115

QuickClean 功能

QuickClean 提供许多清除程序，可以安全且有效地删除无用文件。通过删除这些文件，可以增加计算机硬盘驱动器上的空间，并提高其性能。

清理计算机

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

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

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

名称	功能
Outlook Express 和 Outlook 电子邮件清除程序（已发送和删除的项目）	从 Outlook® 和 Outlook Express 中删除已发送和删除的电子邮件。
最近使用项的清除程序	删除使用以下任一程序生成的最近使用的文件： ▪ Adobe Acrobat® ▪ Corel®WordPerfect®Office (Corel Office) ▪ Jasc® ▪ Lotus® ▪ Microsoft®Office® ▪ RealPlayer™ ▪ Windows History ▪ Windows Media Player ▪ WinRAR® ▪ WinZip®
ActiveX 清除程序	删除 ActiveX 控件。 ActiveX 是程序或网页使用的软件组件，用于添加合并到程序或者网页且如同程序或网页正常部分的功能。大多数 ActiveX 控件是无害的；不过，某些控件可能会获取计算机中的信息。
系统还原点清除程序	删除计算机中旧的系统还原点（最近的还原点除外）。 系统还原点由 Windows 创建，用于标记对计算机所做的任何更改，以便在发生任何问题时，可以恢复到以前的状态。

清理计算机

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

1 在“McAfee SecurityCenter”窗格的“常见任务”下，单击“维护计算机”。

2 在“McAfee QuickClean”下，单击“开始”。

3 执行下面任一操作：

- 单击“下一步”接受列表中的默认清除程序。
- 选择或清除适当的清除程序，然后单击“下一步”。如果选择最近使用项的清除程序，则可以单击“属性”以选择或清除最近使用列表中的程序创建的文件，然后单击“确定”。

- 单击“恢复默认值”以恢复默认的清除程序，然后单击“下一步”。

4 在执行分析后，单击“下一步”。

5 单击“下一步”以确认文件删除。

6 执行下面任一操作：

- 单击“下一步”以接受默认值“否，我要使用标准 Windows 删除来删除文件”。
- 单击“是，我要使用 Shredder 安全删除我的文件”，然后指定操作数量（最多 10 次），然后单击“下一步”。如果要删除大量信息，则清除文件是一个费时的过程。

7 如果在清理期间有文件或项目被锁定，系统可能会提示您重新启动计算机。单击“确定”关闭该提示。

8 单击“完成”。

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

对计算机进行碎片整理

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

对计算机进行碎片整理

您可以对计算机进行碎片整理，以提高文件和文件夹访问和检索的性能。

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

注意：有关磁盘碎片整理程序的详细信息，请参阅 Windows 帮助。

计划任务

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

计划 QuickClean 任务

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

1 打开“任务计划程序”窗格。

如何实现？

1. 在“McAfee SecurityCenter”的“常见任务”下，单击“维护计算机”。
2. 在“任务计划程序”下，单击“开始”。

2 在“选择要计划的操作”列表中，单击“McAfee QuickClean”。

3 在“任务名称”框中键入任务的名称，然后单击“创建”。

4 执行下面任一操作：

- 单击“下一步”接受列表中的清除程序。
- 选择或清除适当的清除程序，然后单击“下一步”。如果选择最近使用项的清除程序，则可以单击“属性”以选择或清除最近使用列表中的程序创建的文件，然后单击“确定”。
- 单击“恢复默认值”以恢复默认的清除程序，然后单击“下一步”。

5 执行下面任一操作：

- 单击“计划”以接受默认值“否，我要使用标准 Windows 删除来删除文件”。
- 单击“是，我要使用 Shredder 安全删除我的文件”，然后指定操作数量（最多 10 次），然后单击“计划”。

6 在“计划”对话框中，选择希望任务运行的频率，然后单击“确定”。

7 如果您对最近使用项的清除程序属性进行更改，系统可能会提示您重新启动计算机。请单击“确定”关闭该提示。

8 单击“完成”。

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

修改 QuickClean 任务

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

1 打开“任务计划程序”窗格。

如何实现？

1. 在“McAfee SecurityCenter”的“常见任务”下，单击“维护计算机”。
2. 在“任务计划程序”下，单击“开始”。

2 在“选择要计划的操作”列表中，单击“McAfee QuickClean”。

3 在“选择现有的任务”列表中选择任务，然后单击“修改”。

4 执行下面任一操作：

- 单击“下一步”接受为此任务选定的清除程序。
- 选择或清除适当的清除程序，然后单击“下一步”。如果选择最近使用项的清除程序，则可以单击“属性”以选择或清除最近使用列表中的程序创建的文件，然后单击“确定”。
- 单击“恢复默认值”以恢复默认的清除程序，然后单击“下一步”。

5 执行下面任一操作：

- 单击“计划”以接受默认值“否，我要使用标准 Windows 删除来删除文件”。
- 单击“是，我要使用 Shredder 安全删除我的文件”，然后指定操作数量（最多 10 次），然后单击“计划”。

6 在“计划”对话框中，选择希望任务运行的频率，然后单击“确定”。

7 如果您对最近使用项的清除程序属性进行更改，系统可能会提示您重新启动计算机。请单击“确定”关闭该提示。

8 单击“完成”。

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

删除 QuickClean 任务

如果不希望计划的 QuickClean 任务自动运行，可以删除此任务。

1 打开“任务计划程序”窗格。

如何实现？

1. 在“McAfee SecurityCenter”的“常见任务”下，单击“维护计算机”。
2. 在“任务计划程序”下，单击“开始”。

2 在“选择要计划的操作”列表中，单击“McAfee QuickClean”。

3 在“选择现有的任务”列表中选择任务。

4 单击“删除”，然后单击“是”确认删除。

5 单击“完成”。

计划磁盘碎片整理程序任务

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

1 打开“任务计划程序”窗格。

如何实现？

1. 在“McAfee SecurityCenter”的“常见任务”下，单击“维护计算机”。
2. 在“任务计划程序”下，单击“开始”。

2 在“选择要计划的操作”列表中，单击“磁盘碎片整理程序”。

3 在“任务名称”框中键入任务的名称，然后单击“创建”。

4 执行下面任一操作：

- 单击“计划”以接受默认的“即使可用空间很少，仍执行碎片整理”选项。

- 清除“即使可用空间很少，仍执行碎片整理”选项，然后单击“计划”。

5 在“计划”对话框中，选择希望任务运行的频率，然后单击“确定”。

6 单击“完成”。

修改磁盘碎片整理程序任务

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

1 打开“任务计划程序”窗格。

如何实现？

1. 在“McAfee SecurityCenter”的“常见任务”下，单击“维护计算机”。
2. 在“任务计划程序”下，单击“开始”。

2 在“选择要计划的操作”列表中，单击“磁盘碎片整理程序”。

3 在“选择现有的任务”列表中选择任务，然后单击“修改”。

4 执行下面任一操作：

- 单击“计划”以接受默认的“即使可用空间很少，仍执行碎片整理”选项。
- 清除“即使可用空间很少，仍执行碎片整理”选项，然后单击“计划”。

5 在“计划”对话框中，选择希望任务运行的频率，然后单击“确定”。

6 单击“完成”。

删除磁盘碎片整理程序任务

如果不希望计划的磁盘碎片整理程序任务自动运行，可以删除此任务。

1 打开“任务计划程序”窗格。

如何实现？

1. 在“McAfee SecurityCenter”的“常见任务”下，单击“维护计算机”。
2. 在“任务计划程序”下，单击“开始”。

2 在“选择要计划的操作”列表中，单击“磁盘碎片整理程序”。

3 在“选择现有的任务”列表中选择任务。

4 单击“删除”，然后单击“是”确认删除。

5 单击“完成”。

第 24 章

McAfee Shredder

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

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

本章内容

Shredder 功能 122
清除文件、文件夹和磁盘.....123

Shredder 功能

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

清除文件、文件夹和磁盘

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

清除文件和文件夹

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

1. 打开“Shredder”。

   如何实现？

   1. 在“McAfee SecurityCenter”窗格的“常见任务”下，单击“高级菜单”。
   2. 在左侧窗格中，单击“工具”。
   3. 单击“Shredder”。

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

注意：在 Shredder 完成任务前，请不要使用任何文件。

清除整个磁盘

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

1 打开“Shredder”。

如何实现？

1. 在“McAfee SecurityCenter”窗格的“常见任务”下，单击“高级菜单”。
2. 在左侧窗格中，单击“工具”。
3. 单击“Shredder”。

2 在“清除文件和文件夹”窗格的“我想”下，单击“删除整个磁盘”。

3 在“清除级别”下，单击以下任一清除级别：

- **快速**：清除选定的驱动器一次。
- **全面**：清除选定驱动器 7 次。
- **自定义**：清除选定驱动器最多 10 次。

4 单击“下一步”。

5 在“选择磁盘”列表中，单击要清除的驱动器。

6 单击“下一步”，然后单击“是”以确认。

7 单击“开始”。

8 Shredder 完成后，单击“完成”。

注意：在 Shredder 完成任务前，请不要使用任何文件。

第 25 章

McAfee Network Manager

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，并在这些计算机上远程修复已报告的安全漏洞。

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

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

本章内容

Network Manager 功能.....126
了解 Network Manager 图标.....127
设置托管网络.....129
远程管理网络.....135

Network Manager 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保护状态的图形概述。在更改网络（如添加计算机）时，网络图会识别这些更改。您可以刷新网络图，重命名网络，并显示或隐藏网络图的组件来自定义您的视图。您还可以查看网络图中任一组件的详细信息。

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

第 26 章

设置托管网络

要设置托管网络，请使用网络图上的项目并将成员（计算机）添加到网络。在可以远程管理某台计算机或可以授予其权限以远程管理网络上的其他计算机之前，该计算机必须成为此网络的信任成员。具有管理权限的现有网络成员（计算机）可以将网络成员关系授予新计算机。

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

本章内容

使用网络图.....130
加入托管网络.....132

使用网络图

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

在更改网络（如添加计算机）后，可以自定义网络图。例如，可以刷新网络图，重命名网络，并显示或隐藏网络图的组件来自定义您的视图。您还可以查看与网络图中显示的任一组件相关联的详细信息。

访问网络图

网络图提供组成家庭网络的计算机和组件的图形表示。

- 在“基本”菜单或“高级”菜单上，单击“管理网络”。

注意：首次访问网络图时，系统会提示您信任网络上的其 他计算机。

刷新网络图

您可以随时刷新网络图；例如，在其他计算机加入托管网络后刷新。

1. 在“基本”菜单或“高级”菜单上，单击“管理网络”。
2. 单击“我想”下的“刷新网络图”。

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

重命名网络

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

1. 在“基本”菜单或“高级”菜单上，单击“管理网络”。
2. 单击“我想”下的“重命名网络”。
3. 在“网络名称”框中输入网络的名称。
4. 单击“确定”。

注意：只有网络图上的没有选择项目的情况下，“重命名网络”链接才可用。要清除项目，请单击所选项目，或单击网络图上的空白区域。

显示或隐藏网络图中的项目

默认情况下，家庭网络中的所有计算机和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”。

查看项目的详细信息

如果您选择网络图上的任一组成部分，可以查看网络中有关该组成部分的详细信息。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。

1 单击网络图上项目的图标。

2 在“详细信息”下，查看有关项目的信息。

加入托管网络

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

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

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

加入托管网络

当您收到加入托管网络的邀请时，您可以接受或拒绝邀请。您还可以确定是否希望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）。

1. 在“托管网络”对话框中，确保选中“允许此网络上的每台计算机监视安全设置”复选框。
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“确定”。

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

邀请计算机加入此托管网络

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

1. 单击网络图上非托管计算机的图标。
2. 单击“我想”下的“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：
   - 单击“允许对托管网络程序的来宾访问权限”以允许计算机访问网络（您可以对家庭中的临时用户使用此选项）。
   - 单击“允许对托管网络程序的完全访问权限”以允许计算机访问网络。
   - 单击“允许对托管网络程序的管理访问权限”以允许计算机以管理权限访问网络。它还允许计算机将访问权限授予要加入托管网络的其他计算机。
4. 单击“确定”。
   加入托管网络的邀请会发给此计算机。在计算机接受邀请后，会显示两个图片。
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：如果邀请您加入托管网络的计算机显示的图片与安全确认对话框中显示的图片不同，则表明托管网络上有安全隐患。允许此计算机加入网络可能会使其他计算机面临风险；因此，单击安全确认对话框中的“拒绝访问”。

停止信任网络上的计算机

如果您误信任网络中的其他计算机，则可以停止信任它们。

- 单击“我想”下的“停止信任此网络上的计算机”。

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

第 27 章

远程管理网络

在设置托管网络后，您可以远程管理组成网络的计算机和组件。您可以监视计算机和组成部分的状态和权限级别，然后远程修复大多数安全漏洞。

本章内容

监视状态和权限.....136
修复安全漏洞.....138

监视状态和权限

托管网络包含托管成员和非托管成员。托管成员允许网络上的其他计算机监视其 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（如发送文件或共享打印机）的来宾计算机。非托管计算机可以随时由网络上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。

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

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

监视计算机的保护状态

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

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

您可以停止监视网络中托管计算机的保护状态，不过，如果此后该计算机变为非托管计算机，您就不能远程监视其保护状态。

1 单击网络图上托管计算机的图标。

2 单击“我想”下的“停止监视此计算机”。

3 在确认对话框中，单击“是”。

修改托管计算机的权限

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

1 单击网络图上托管计算机的图标。

2 单击“我想”下的“修改此计算机的权限”。

3 在修改权限对话框中，选中或清除复选框，以确定此计算机和托管网络中的其他计算机是否可以互相监视各自的保护状态。

4 单击“确定”。

管理设备

您可以在 Network Manager 中访问设备的管理网页来管理设备。

1 单击网络图上的设备图标。

2 单击“我想”下的“管理此设备”。
此时会打开 Web 浏览器并显示设备的管理网页。

3 在 Web 浏览器中，提供您的登录信息并配置设备的安全设置。

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

修改设备的显示属性

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

1 单击网络图上的设备图标。

2 单击“我想”下的“修改设备属性”。

3 指定设备的显示名称，在“名称”框中键入名称。

4 要指定设备的类型，请单击“标准路由器”（如果不是无线路由器）或“无线路由器”（如果是无线路由器）。

5 单击“确定”。

修复安全漏洞

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

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

修复安全漏洞

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

1 单击网络图上项目的图标。

2 查看“详细信息”下项目的保护状态。

3 单击“我想”下的“修复安全漏洞”。

4 如果已修复安全问题，请单击“确定”。

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

在远程计算机上安装 McAfee 安全软件

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

1 在要安装安全软件的计算机上打开 SecurityCenter。

2 在“常见任务”下，单击“我的帐户”。

3 使用电子邮件地址和密码登录，这是您首次安装安全软件时注册所使用的电子邮件和密码。

4 选择相应的产品，单击“下载/安装”图标，然后按照屏幕上的说明执行操作。

第 28 章

McAfee EasyNetwork

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

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

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

本章内容

EasyNetwork 功能 140
设置 EasyNetwork 141
共享和发送文件 147
共享打印机 153

EasyNetwork 功能

EasyNetwork 提供以下功能。

文件共享

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

文件传输

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

自动共享打印机

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

第 29 章

设置 EasyNetwork

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

本章内容

打开 EasyNetwork 141
加入托管网络 142
离开托管网络 145

打开 EasyNetwork

默认情况下，在安装 EasyNetwork 后系统会提示您打开它；不过，您也可以稍后打开 EasyNetwork。

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

提示：如果在安装过程中创建了桌面图标和快速启动图标，则还可以通过双击桌面上或任务栏右侧通知区域的 McAfee EasyNetwork 图标来打开 EasyNetwork。

加入托管网络

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

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

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

加入网络

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

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

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

授予对网络的访问权限

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

1 在警报中，单击相应的访问级别。

2 在“邀请计算机加入此托管网络”对话框中，单击以下任一选项：

- 单击“允许对托管网络程序的来宾访问权限”以允许计算机访问网络（您可以对家庭中的临时用户使用此选项）。
- 单击“允许对托管网络程序的完全访问权限”以允许计算机访问网络。
- 单击“允许对托管网络程序的管理访问权限”以允许计算机以管理权限访问网络。它还允许计算机将访问权限授予要加入托管网络的其他计算机。

3 单击“确定”。

4 确认计算机显示安全确认对话框中所显示的图片，然后单击“授予访问权限”。

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

重命名网络

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

1 在“选项”菜单中，单击“配置”。

2 在“配置”对话框的“网络名称”框中，键入网络名称。

3 单击“确定”。

离开托管网络

如果您加入托管网络，然后决定不希望作为其成员，则可以离开网络。在离开托管网络后，您可以随时重新加入；不过，您必须再次被授予权限。有关加入的详细信息，请参阅加入托管网络 (第 142 页)。

离开托管网络

您可以离开以前加入的托管网络。

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 30 章

共享和发送文件

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

注意：如果您共享大量文件，则您的计算机资源可能会受到影响。

本章内容

共享文件.....148
将文件发给其他计算机.....150

共享文件

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

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

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

共享文件

共享文件后，对托管网络具有完全或管理访问权限的所有成员都可以使用此文件。

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

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

停止共享文件

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

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

复制共享文件

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

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

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

搜索共享文件

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

1 在“共享文件”窗口中，单击“搜索”。

2 单击“包含”列表中的相应选项 (第 149 页)。

3 在“文件名或路径名”列表中键入部分或全部文件名或路径。

4 单击“类型”列表中相应的文件类型 (第 149 页)。

5 在“开始”和“结束”列表中，单击表示创建文件的日期范围的日期。

搜索标准

下表描述搜索共享文件时可以指定的搜索标准。

文件或路径的名称

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

文件的类型

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

将文件发给其他计算机

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

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

将文件发送到另一台计算机

您可以将文件发送到托管网络上的另一台计算机，而不共享此文件。接收计算机上的用户要查看此文件，必须将它保存到本地位置。有关详细信息，请参阅接受另一台计算机发来的文件 (第 150 页)。

1 在 Windows 资源管理器中，确定要发送的文件的位置。

2 在 Windows 资源管理器中将文件从其位置拖到 EasyNetwork 的活动计算机图标。

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

接受另一台计算机发来的文件

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

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

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

发送文件时接收通知

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

1 在“选项”菜单中，单击“配置”。

2 在“配置”对话框中，选中“其他计算机向我发送文件时通知我”复选框。

3 单击“确定”。

第 31 章

共享打印机

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

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

本章内容

使用共享打印机.....154

使用共享打印机

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

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

停止共享打印机

停止共享打印机后，各成员便无法使用此打印机。

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

安装可用的网络打印机

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

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

参考

词汇表列出并定义 McAfee 产品中最常用的安全术语。

词汇表

8

802.11

一组通过无限网络传输数据的 IEEE 标准。802.11 通常称为 Wi-Fi。

802.11a

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

802.11b

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

802.1x

有线和无线网络上的 IEEE 身份验证标准。802.1x 通常与 802.11 无线网络结合使用。

A

ActiveX 控件

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

C

Cookie

存储在个人浏览 Web 的计算机上且包含信息的小文件，通常包含用户名和当前日期和文件。网站主要使用 Cookie 来标识以前在站点注册或访问站点的用户；不过，Cookie 也可能是攻击者的信息来源。

D

DAT

（数据特征码文件）包含特征码的文件，在检测计算机或 USB 驱动器上的病毒、特洛伊木马程序、间谍软件、广告软件和其他可能有害的程序时会使用特征码。

DNS

（域名系统）将主机名或域名转换为 IP 地址的一种系统。在 Web 上，可以使用 DNS 将易于理解的 Web 地址（如 www.myhostname.com）转换为 IP 地址（如 111.2.3.44），从而可以检索到网站。如果没有 DNS，则必须在 Web 浏览器中键入 IP 地址。

DNS 服务器

（域名系统服务器）返回与主机名或域名关联的 IP 地址的计算机。另请参阅 DNS。

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

TCP/IP 网络上计算机或设备的标识符。使用 TCP/IP 协议的网络会根据目标的 IP 地址路由消息。IP 地址的格式是 32 位的数字地址，采用句点分隔的四个数字的形式表示。每个数字可以是 0 到 255（如 192.168.1.100）。

IP 伪造

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

L

LAN

（局域网）涵盖很小区域（如一座建筑物）的一种计算机网络。LAN 上的计算机可以互相通信并共享资源，如打印机和文件。

launchpad

U3 接口组件，充当启动和管理 U3 USB 程序的起始点。

M

MAC 地址

（媒体访问控制地址）分配给访问网络的物理设备的唯一序列号。

MAPI

（消息应用程序编程接口）Microsoft 接口规范，能使不同的消息和工作组应用程序（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。

MSN

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

N

NIC

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

P

PCI 无线适配器卡

（外部部件互连）插入计算机内部 PCI 扩展插槽的无线适配器卡。

POP3

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

PPPoE

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

R

RADIUS

（远程访问拨入用户服务）通常在远程访问环境中允许用户身份验证的一种协议。RADIUS 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。

Rootkit

授予用户对计算机或计算机网络的管理员级访问权限的工具（程序）集合。Rootkit 可能包含间谍软件和其他可能有害的程序，这些程序可能会对您的计算机数据和个人信息带来额外的安全或隐私风险。

S

SMTP

（简单邮件传输协议）将消息从网络上的一台计算机发送到另一台计算机所使用的 TCP/IP 协议。Internet 上使用此协议来传送电子邮件。

SSID

（服务集标识符）标识 Wi-Fi (802.11) 网络的一种标记（密钥）。SSID 由网络管理员建立，而且必须由希望加入网络的用户提供。

SSL

（安全套接层）Netscape 为在 Internet 上传输专用文档而制定的一种协议。SSL 通过使用公钥加密在 SSL 连接上传输的数据来工作。需要 SSL 连接的 URL 都以 https: 而不是 http: 开头。

SystemGuard

McAfee 会检测对计算机未经授权的更改并在出现更改时提醒您。

T

TKIP

（临时密钥完整性协议）解决 WEP 安全中的弱点，特别是密钥重用问题的协议。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。

U

U3

（代表 You: Simplified, Smarter, Mobile，即“您：简单、智能和移动”）一种直接从 USB 驱动器运行 Windows 2000 或 Windows XP 程序的平台。M-Systems 和 SanDisk 在 2004 年发明了 U3 方案，用户可以利用它在 Windows 上运行 U3 程序，而无须在计算机上安装或存储数据或设置。

URL

（统一资源定位器）标准的 Internet 地址格式。

USB

（通用串行总线）允许将外设（如键盘、游戏杆和打印机）连接到计算机的标准串行计算机接口。

USB 驱动器

插入计算机 USB 端口的小型内存驱动器。USB 驱动器就像一个小型磁盘驱动器，利用它可以轻松地将文件从一台计算机传输到另一台计算机。

USB 无线适配器卡

插入计算机 USB 插槽的无线适配器卡。

V

VPN

（虚拟专用网）在公共网络内配置的专用网络，从而利用公共网络中的管理功能。企业使用 VPN 可以创建跨多个地理区域的广域网 (WAN)，提供分支办公室的站点对站点连接，或允许移动用户拨入其公司的 LAN。

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。

Web 邮件

通过 Internet 以电子方式收发的邮件。另请参阅“电子邮件”。

WEP

（有线等效加密）定义为 Wi-Fi (802.11) 标准一部分的加密和身份验证协议。最初的版本以 RC4 密码为基础，并有严重缺陷。WEP 会尝试对通过无线电波传输的数据进行加密来提供安全性，以便数据在从一个端点传输到另一个端点时获得保护。不过，已发现 WEP 并没有以前所认为的那样安全。

Wi-Fi

（无线保真）Wi-Fi Alliance 提及任何类型的 802.11 网络时所使用的术语。

Wi-Fi Alliance

由主要的无线硬件和软件提供商组成的组织。Wi-Fi Alliance 的使命是认证所有基于 802.11 产品的互操作性，以及对于基于 802.11 的所有无线 LAN 产品的所有市场，将术语 Wi-Fi 推广为全球品牌名称。此组织的性质就像协会、测试实验室以及要提高行业增长的厂商的信息交流中心。

Wi-Fi Certified

由 Wi-Fi Alliance 测试和批准。Wi-Fi Certified 产品被认为是可互操作的，即使来自不同的制造商也是如此。使用具有 Wi-Fi Certified 产品的用户可以将任何品牌的接入点 (AP) 与同样经过认证的任何其他客户端硬件品牌一起使用。

WLAN

（无线局域网）使用无线连接的局域网 (LAN)。WLAN 使用高频无线电波而不是有线线路在计算机之间进行通信。

WPA

（Wi-Fi 保护访问）一种规范标准，可以极大增强现有的和将来的无线 LAN 系统的数据保护和访问控制级别。WPA 设计作为软件升级在现有的硬件上运行，WPA 从 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

WPA 安全标准的更新，它基于 802.11i IEEE 标准。

WPA2-PSK

与 WPA-PSK 类似的专用 WPA 模式，它基于 WPA2 标准。WPA2-PSK 的一种常见功能是，设备通常会同时支持多个加密模式（如 AES、TKIP），而旧设备通常一次仅支持一个加密模式（即所有客户端将必须使用相同的加密模式）。

汉字（拼音）

按需扫描

在请求时启动的扫描（即启动操作时）。与实时扫描不同，按需扫描不会自动启动。

白名单

允许用户访问的网站列表，因为这些网站不是诈骗网站。

暴力攻击

通过穷尽操作（使用暴力）而不是使用智能策略对加密数据（如果密码）进行解码所使用的方法。暴力破解尽管非常耗时，但被认为是一种可靠的方法。暴力攻击也称为暴力破解。

备份

在安全的联机服务器上创建重要文件的副本。

标准电子邮件帐户

请参阅 POP3。

病毒

可能更改文件或数据的自我复制程序。从表面上看，这些程序通常来自可信的发送人或包含无害内容。

拨号程序

帮助您建立 Internet 连接的软件。如果拨号程序遭恶意使用，它可能会将 Internet 连接重定向到除默认 Internet 服务提供商 (ISP) 之外的其他人，而您并不知道需要支付额外的费用。

插件

与较大程序一起来提供附加功能的小型软件程序。例如，Web 浏览器利用插件可以访问和执行嵌在 HTML 文档中且浏览器通常无法识别其格式（如动画、视频和音频文件）的文件。

存档

在 CD、DVD、USB 驱动器、外部硬盘驱动器或网络驱动器上创建重要文件的副本。

代理

计算机或其上运行的软件，它仅向外部站点提供单个网络地址，从而在网络和 Internet 之间构筑了一个屏障。代理代表所有内部计算机，从而在保护网络身份的同时仍提供对 Internet 的访问。另请参阅“代理服务器”。

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。

电子邮件

（电子邮件）以电子形式通过计算机网络收发的邮件。另请参阅 Webmail。

电子邮件客户端

在计算机上运行的用于收发电子邮件的程序（如 Microsoft Outlook）。

端口

信息进出计算机的位置。例如，传统的模拟调制解调器连接到串行端口。

恶意接入点

未授权的接入点。恶意接入点可能安装在安全的公司网络中，将网络访问权限授予未授权的各方。还可以创建恶意接入点来允许攻击者执行中间人攻击。

发布

在 Internet 上公开可用的已备份文件。您可以搜索 Data Backup 库来访问已发布的文件。

防火墙

专用于防止对专用网络或来自专用网络的未经授权访问的系统（硬件、软件或软硬兼具）。防火墙常用于防止未经授权的 Internet 用户访问连接到 Internet 的专用网络，特别是在内部网络中更是如此。进入或离开内部网的所有消息都会通过防火墙，防火墙会检查每条消息，并拦截不符合指定安全标准的消息。

服务器

从其他计算机或程序接受连接并返回适当响应的计算机或程序。例如，每次您收发电子邮件时，您的电子邮件程序会连接到电子邮件服务器。

隔离

进行隔离。例如，在 VirusScan 中，会在检测到可疑文件后进行隔离，以防对您的计算机和文件造成损害。

共享

允许电子邮件收件人在有限的时间段内访问所选备份文件。在共享文件后，您会将此文件的备份副本发给您指定的电子邮件收件人。收件人会收到一封 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

在开始通信前，已在两个通信方之间共享的字符串或密钥（通常为密码）。共享密钥用于保护 RADIUS 消息的敏感部分。

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

在防网络钓鱼中，认为具有欺诈行为的网站列表。

还原

从联机备份库或存档中获取文件的副本。

缓冲区溢出

可疑程序或可疑进程尝试在计算机缓冲区（临时数据存储区）中存储的数据超过其所能存放的数据时发生的一种情况。缓冲区溢出会损坏或覆盖相邻缓冲区中的数据。

缓存

计算机上的临时存储区。例如，为提高 Web 浏览速度和效率，浏览器会在您下次查看某个网页时从其缓存（而不是从远程服务器）中检索该网页。

回收站

垃圾箱的一种模拟形式，可以存放 Windows 中的已删除文件和文件夹。

集成网关

将接入点 (AP)、路由器和防火墙的功能合并在一起的一种设备。某些设备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。加密数据还称为密文。

家长监控

帮助控制儿童在浏览 Web 时可以查看的内容和执行的操作的设置。要设置家长监控，您可以启用或禁用图像过滤，选择内容评级组并设置 Web 浏览时间限制。

家庭网络

家庭中互相连接的两台或多台计算机，它们可以共享网络和 Internet 访问。另请参阅 LAN。

监视位置

Data Backup 所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

可以自动执行（即没有用户交互）的命令列表。与程序不同，脚本通常以纯文本的形式存储，并在每次运行时进行编译。宏和批处理文件也称为脚本。

接入点

一种网络设备（通常称为无线路由器），可以插入以太网集线器或交换机来扩展无线用户的实际服务范围。在无线用户持有移动设备漫游时，数据传输会从一个接入点 (AP) 切换到另一个接入点，从而保持连接性。

节点

连接到网络上的单台计算机。

拒绝服务

减缓或阻止网络上通讯的攻击类型。当网络被许多额外的请求淹没以至于常规通讯很缓慢或完全中断，则会发生拒绝服务攻击（DoS 攻击）。拒绝服务攻击通常不会发生信息窃取或产生其他安全漏洞。

可能有害的程序 (PUP)

未经允许收集并传送个人信息的程序（如间谍软件和广告软件）。

可信列表

包含您信任且不进行检测的项目。如果您误信任某个项目（如可能有害的程序或注册表更改），或要再次检测此项目，则必须从此列表中将其删除。

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

存储您已备份和发布的文件的在线存储区域。Data Backup 库是 Internet 上的网站，可以访问 Internet 的任何人都能对其进行访问。

快捷方式

只包含计算机上另一个文件位置的文件。

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。另请参阅“完全存档”。

联机备份库

备份文件后存储这些文件的联机服务器上的位置。

临时文件

操作系统或某个其他程序在内存或磁盘中创建的文件，在会话过程中会使用此文件，然后将其丢弃。

浏览器

用于查看 Internet 上网页的程序。常用的 Web 浏览器有 Microsoft Internet Explorer 和 Mozilla Firefox。

路由器

将数据包从一个网络转发到另一个网络的网络设备。路由器会按照内部路由表读取每个传入的数据包，然后根据来源地址和目标地址的组合以及当前通讯情况（如负载、线路损失以及不良线路）来决定如何转发数据包。有时将路由器也称为接入点 (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。

密码

访问计算机、程序或网站所使用的代码（通常由字母和数字组成）。

密码存储库

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

密文

加密的文本。除非将密文转换为明文（即已解密），否则密文是不可读的。

密钥

两台设备对通信进行身份验证所使用的一组字母和数字。两台设备都必须有密钥。另请参阅 WEP、WPA、WPA2、WPA-PSK 和 WPA2- PSK。

明文

没有加密的文本。另请参阅“加密”。

内部网

通常位于组织内部的一种专用计算机网络，只能由授权用户进行访问。

内容评级组

家长控制中用户所属的年龄组。根据用户所属的内容评级组使内容可用或将其阻止。内容评级组包括：幼儿、儿童、青少年（较小）、青少年（较大）和成人。

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

由 Wi-Fi (802.11) 接入点 (AP) 覆盖的地理界限。使用无线膝上型计算机进入热点的用户可以连接到 Internet，前提是该热点正在发送信标（即公告其存在），而且不需要身份验证。热点通常位于人口密集的地区，如机场。

蠕虫

一种可在当前内存中进行自我复制的病毒，并且可能会通过电子邮件发送自身的副本。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。

扫台者

配备 Wi-Fi 计算机以及某种专用硬件或软件的人员，他们驾车在城市间穿梭以搜索 Wi-Fi (802.11) 网络。

身份验证

通常按用户名和密码确定个人的过程。

深层监视位置

计算机上的文件夹，Data Backup 监视其是否有更改。如果设置深层监视位置，则 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

在您或您的计算机访问文件和文件夹时，扫描其中是否有病毒和其他活动。

事件

由用户、设备或计算机本身启动且可以触发响应的操作。McAfee 会在事件日志中记录事件。

弹出窗口

出现在计算机屏幕上其他窗口上的小窗口。Web 浏览器常使用弹出窗口显示广告。

特洛伊木马程序

以合法程序的身份出现，但可能会损坏重要文件，降低性能，并允许对计算机进行未经授权的访问的程序。

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。

图像过滤

一个家长监控选项，可以阻止显示可能不良的 Web 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

位于计算机外的硬盘驱动器。

完全存档

根据已设置的文件类型和位置存档全部数据集。另请参阅“快速存档”。

网络

接入点及其关联用户的集合，等同于 ESS。

网络钓鱼

一种 Internet 诈骗手法，专门获取未知用户的重要信息（如信用卡、身份证号、用户 ID 和密码）来进行诈骗活动。

网络驱动器

连接到网络上的服务器并由多个用户共享的磁盘驱动器或磁带驱动器。有时也将网络驱动器称为远程驱动器。

网络图

组成家庭网络的计算机和组件的图形表示。

文件碎片

分布在磁盘上的文件残余。添加或删除文件时会产生文件碎片，可能会降低计算机的性能。

无线适配器

在计算机或 PDA 上增加无线功能的设备。可以通过 USB 端口、PC 卡 (CardBus) 插槽、内存卡插槽或在内部插入 PCI 总线进行连接。

系统还原点

计算机内存或数据库的内容的快照（映像）。Windows 会定期及在发生重要事件（如安装程序或驱动程序）时创建还原点。您还可以随时创建和命名自己的还原点。

消息身份验证代码 (MAC)

用于对在两台计算机之间传送的消息进行加密的安全代码。如果计算机认为解密代码是有效的，则会接收消息。

协议

在两台设备之间传输数据的格式（硬件或软件）。如果要与其他计算机通信，您的计算机或设备必须支持正确的协议。

压缩

将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输所需的空间。

域

本地子网或 Internet 上的站点描述符。

在局域网 (LAN) 中，域是由一个安全数据库控制的客户端和服务器计算机组成的子网。在此环境中，域可以提高性能。在 Internet 上，域是每个 Web 地址的一部分（如在 www.abc.com 中，abc 是域）。

智能驱动器

请参阅 USB 驱动器。

中间人攻击

拦截而且有可能修改双方之间消息的一种方法，通信双方的任一方都不知道其通信了链路遭破坏。

注册表

Windows 存储器其配置信息的数据库。注册表包含每个计算机用户的配置文件以及有关系统硬件、安装程序和属性设置的信息。Windows 运行时会持续引用此信息。

字典攻击

一种暴力攻击类型，使用常用的词来尝试发现密码。

关于 McAfee

McAfee, Inc. 的总部设在加利福尼亚的 Santa Clara，它在入侵防护和安全风险管理方面居于世界领先地位，可以为世界各地的系统和网络提供前瞻性和成熟的安全解决方案及服务。McAfee 具有无可比拟的安全经验和勇于创新的精神，可以帮助家庭用户、企业、公共部门和服务提供商有效阻止攻击、防止破坏以及持续跟踪和提高其安全性。

版权

许可

致全体用户：请仔细阅读与您所购买的许可相关的法律协议，以了解使用许可软件的一般条款和条件。如果您不清楚所购买的许可属于哪一类，请查看软件包装盒中或购买产品时单独提供的销售文档以及其他相关的许可授权或订单文档，这些文档既可以是小册子、产品光盘上的文件，也可以是软件包下载网站提供的文件。如果您不接受该协议规定的所有条款和条件，请勿安装本软件。根据情况，您可以将产品退回 McAfee, Inc. 或原购买处以获得全额退款。

第 32 章

客户服务和技术支持

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

如果您已从 McAfee 之外的合作伙伴或提供商购买安全软件，请打开 Web 浏览器，然后访问 www.mcafeehelp.com。然后，在“Partner Links”（合作伙伴）链接下，选择您的合作伙伴或供应商来访问 McAfee Virtual Technician。

注意：要安装和运行 McAfee Virtual Technician，则必须以 Windows 管理员身份登录计算机。如果无法这样做，则 MVT 可能无法解决问题。有关以 Windows 管理员身份登录的信息，请参阅 Windows 帮助。在 Windows Vista™ 中，系统会在您运行 MVT 时提示您。在系统提示时，请单击“Accept”（接受）。Virtual Technician 无法与 Mozilla® Firefox 一起使用。

本章内容

使用 McAfee Virtual Technician.....172
支持和下载.....173

使用 McAfee Virtual Technician

Virtual Technician 就像一名技术支持代表人员，收集有关您的 SecurityCenter 程序的信息，从而可以帮助您解决计算机的保护问题。运行 Virtual Technician 时，它会进行检查以确保 SecurityCenter 程序在正常工作。如果发现问题，Virtual Technician 会进行修复，或向您提供有关这些问题的详细信息。完成后，Virtual Technician 会显示其分析结果，并允许寻求 McAfee 的其他技术支持（如果需要）。

为保持您计算机和文件的安全性和完整性，Virtual Technician 不会收集可识别您个人身份的信息。

注意：有关 Virtual Technician 的详细信息，请单击 Virtual Technician 中的“帮助”图标。

启动 Virtual Technician

Virtual Technician 会收集有关 SecurityCenter 程序的信息，以便可以帮助您解决保护问题。为保护您的隐私，此信息不包含可识别个人身份的信息。

1. 在“常见任务”下，单击“McAfee Virtual Technician”。
2. 按照屏幕上的说明下载和运行 Virtual Technician。

支持和下载

请参阅下表来了解您所在国家/地区的 McAfee 支持和下载站点，包括《用户手册》。

支持和下载

国家/地区	McAfee 支持	McAfee 下载
澳大利亚	www.mcafeehelp.com	au.mcafee.com/root/downloads.asp
巴西	www.mcafeeajuda.com	br.mcafee.com/root/downloads.asp
加拿大（英语）	www.mcafeehelp.com	ca.mcafee.com/root/downloads.asp
加拿大（法语）	www.mcafeehelp.com	ca.mcafee.com/root/downloads.asp
中国（中国）	www.mcafeehelp.com	cn.mcafee.com/root/downloads.asp
中国（台湾）	www.mcafeehelp.com	tw.mcafee.com/root/downloads.asp
捷克	www.mcafeenapoveda.com	cz.mcafee.com/root/downloads.asp
丹麦	www.mcafeehjaelp.com	dk.mcafee.com/root/downloads.asp
芬兰	www.mcafeehelp.com	fi.mcafee.com/root/downloads.asp
法国	www.mcafeeaide.com	fr.mcafee.com/root/downloads.asp
德国	www.mcafeehilfe.com	de.mcafee.com/root/downloads.asp
英国	www.mcafeehelp.com	uk.mcafee.com/root/downloads.asp
意大利	www.mcafeeaiuto.com	it.mcafee.com/root/downloads.asp
日本	www.mcafeehelp.jp	jp.mcafee.com/root/downloads.asp
韩国	www.mcafeehelp.com	kr.mcafee.com/root/downloads.asp
墨西哥	www.mcafeehelp.com	mx.mcafee.com/root/downloads.asp
挪威	www.mcafeehjelp.com	no.mcafee.com/root/downloads.asp
波兰	www.mcafeepomoc.com	pl.mcafee.com/root/downloads.asp

葡萄牙	www.mcafeeajuda.com	pt.mcafee.com/root/downloads.asp
西班牙	www.mcafeeayuda.com	es.mcafee.com/root/downloads.asp
瑞典	www.mcafeehjalp.com	se.mcafee.com/root/downloads.asp
土耳其	www.mcafeehelp.com	tr.mcafee.com/root/downloads.asp
美国	www.mcafeehelp.com	us.mcafee.com/root/downloads.asp

McAfee Total Protection 用户手册

国家/地区	McAfee 用户手册
澳大利亚	download.mcafee.com/products/manuals/en-au/MTP_userguide_2008.pdf
巴西	download.mcafee.com/products/manuals/pt-br/MTP_userguide_2008.pdf
加拿大（英语）	download.mcafee.com/products/manuals/en-ca/MTP_userguide_2008.pdf
加拿大（法语）	download.mcafee.com/products/manuals/fr-ca/MTP_userguide_2008.pdf
中国（中国）	download.mcafee.com/products/manuals/zh-cn/MTP_userguide_2008.pdf
中国（台湾）	download.mcafee.com/products/manuals/zh-tw/MTP_userguide_2008.pdf
捷克	download.mcafee.com/products/manuals/cz/MTP_userguide_2008.pdf
丹麦	download.mcafee.com/products/manuals/dk/MTP_userguide_2008.pdf
芬兰	download.mcafee.com/products/manuals/fi/MTP_userguide_2008.pdf
法国	download.mcafee.com/products/manuals/fr/MTP_userguide_2008.pdf
德国	download.mcafee.com/products/manuals/de/MTP_userguide_2008.pdf
英国	download.mcafee.com/products/manuals/en-uk/MTP_userguide_2008.pdf
荷兰	download.mcafee.com/products/manuals/nl/MTP_userguide_2008.pdf
意大利	download.mcafee.com/products/manuals/it/MTP_userguide_2008.pdf
日本	download.mcafee.com/products/manuals/ja/MTP_userguide_2008.pdf

韩国	download.mcafee.com/products/manuals/ko/MTP_userguide_2008.pdf
墨西哥	download.mcafee.com/products/manuals/es-mx/MTP_userguide_2008.pdf
挪威	download.mcafee.com/products/manuals/no/MTP_userguide_2008.pdf
波兰	download.mcafee.com/products/manuals/pl/MTP_userguide_2008.pdf
葡萄牙	download.mcafee.com/products/manuals/pt/MTP_userguide_2008.pdf
西班牙	download.mcafee.com/products/manuals/es/MTP_userguide_2008.pdf
瑞典	download.mcafee.com/products/manuals/sv/MTP_userguide_2008.pdf
土耳其	download.mcafee.com/products/manuals/tr/MTP_userguide_2008.pdf
美国	download.mcafee.com/products/manuals/en-us/MTP_userguide_2008.pdf

McAfee Internet Security 用户手册

国家/地区	McAfee 用户手册
澳大利亚	download.mcafee.com/products/manuals/en-au/MIS_userguide_2008.pdf
巴西	download.mcafee.com/products/manuals/pt-br/MIS_userguide_2008.pdf
加拿大（英语）	download.mcafee.com/products/manuals/en-ca/MIS_userguide_2008.pdf
加拿大（法语）	download.mcafee.com/products/manuals/fr-ca/MIS_userguide_2008.pdf
中国（中国）	download.mcafee.com/products/manuals/zh-cn/MIS_userguide_2008.pdf
中国（台湾）	download.mcafee.com/products/manuals/zh-tw/MIS_userguide_2008.pdf
捷克	download.mcafee.com/products/manuals/cz/MIS_userguide_2008.pdf
丹麦	download.mcafee.com/products/manuals/dk/MIS_userguide_2008.pdf
芬兰	download.mcafee.com/products/manuals/fi/MIS_userguide_2008.pdf
法国	download.mcafee.com/products/manuals/fr/MIS_userguide_2008.pdf
德国	download.mcafee.com/products/manuals/de/MIS_userguide_2008.pdf

英国	download.mcafee.com/products/manuals/en-uk/MIS_userguide_2008.pdf
荷兰	download.mcafee.com/products/manuals/nl/MIS_userguide_2008.pdf
意大利	download.mcafee.com/products/manuals/it/MIS_userguide_2008.pdf
日本	download.mcafee.com/products/manuals/ja/MIS_userguide_2008.pdf
韩国	download.mcafee.com/products/manuals/ko/MIS_userguide_2008.pdf
墨西哥	download.mcafee.com/products/manuals/es-mx/MIS_userguide_2008.pdf
挪威	download.mcafee.com/products/manuals/no/MIS_userguide_2008.pdf
波兰	download.mcafee.com/products/manuals/pl/MIS_userguide_2008.pdf
葡萄牙	download.mcafee.com/products/manuals/pt/MIS_userguide_2008.pdf
西班牙	download.mcafee.com/products/manuals/es/MIS_userguide_2008.pdf
瑞典	download.mcafee.com/products/manuals/sv/MIS_userguide_2008.pdf
土耳其	download.mcafee.com/products/manuals/tr/MIS_userguide_2008.pdf
美国	download.mcafee.com/products/manuals/en-us/MIS_userguide_2008.pdf

McAfee VirusScan Plus 用户手册

国家/地区	McAfee 用户手册
澳大利亚	download.mcafee.com/products/manuals/en-au/VSP_userguide_2008.pdf
巴西	download.mcafee.com/products/manuals/pt-br/VSP_userguide_2008.pdf
加拿大（英语）	download.mcafee.com/products/manuals/en-ca/VSP_userguide_2008.pdf
加拿大（法语）	download.mcafee.com/products/manuals/fr-ca/VSP_userguide_2008.pdf
中国（中国）	download.mcafee.com/products/manuals/zh-cn/VSP_userguide_2008.pdf
中国（台湾）	download.mcafee.com/products/manuals/zh-tw/VSP_userguide_2008.pdf
捷克	download.mcafee.com/products/manuals/cz/VSP_userguide_2008.pdf

丹麦	download.mcafee.com/products/manuals/dk/VSP_userguide_2008.pdf
芬兰	download.mcafee.com/products/manuals/fi/VSP_userguide_2008.pdf
法国	download.mcafee.com/products/manuals/fr/VSP_userguide_2008.pdf
德国	download.mcafee.com/products/manuals/de/VSP_userguide_2008.pdf
英国	download.mcafee.com/products/manuals/en-uk/VSP_userguide_2008.pdf
荷兰	download.mcafee.com/products/manuals/nl/VSP_userguide_2008.pdf
意大利	download.mcafee.com/products/manuals/it/VSP_userguide_2008.pdf
日本	download.mcafee.com/products/manuals/ja/VSP_userguide_2008.pdf
韩国	download.mcafee.com/products/manuals/ko/VSP_userguide_2008.pdf
墨西哥	download.mcafee.com/products/manuals/es-mx/VSP_userguide_2008.pdf
挪威	download.mcafee.com/products/manuals/no/VSP_userguide_2008.pdf
波兰	download.mcafee.com/products/manuals/pl/VSP_userguide_2008.pdf
葡萄牙	download.mcafee.com/products/manuals/pt/VSP_userguide_2008.pdf
西班牙	download.mcafee.com/products/manuals/es/VSP_userguide_2008.pdf
瑞典	download.mcafee.com/products/manuals/sv/VSP_userguide_2008.pdf
土耳其	download.mcafee.com/products/manuals/tr/VSP_userguide_2008.pdf
美国	download.mcafee.com/products/manuals/en-us/VSP_userguide_2008.pdf

McAfee VirusScan 用户手册

国家/地区	McAfee 用户手册
澳大利亚	download.mcafee.com/products/manuals/en-au/VS_userguide_2008.pdf
巴西	download.mcafee.com/products/manuals/pt-br/VS_userguide_2008.pdf
加拿大（英语）	download.mcafee.com/products/manuals/en-ca/VS_userguide_2008.pdf

加拿大（法语）	download.mcafee.com/products/manuals/fr-ca/VS_userguide_2008.pdf
中国（中国）	download.mcafee.com/products/manuals/zh-cn/VS_userguide_2008.pdf
中国（台湾）	download.mcafee.com/products/manuals/zh-tw/VS_userguide_2008.pdf
捷克	download.mcafee.com/products/manuals/cz/VS_userguide_2008.pdf
丹麦	download.mcafee.com/products/manuals/dk/VS_userguide_2008.pdf
芬兰	download.mcafee.com/products/manuals/fi/VS_userguide_2008.pdf
法国	download.mcafee.com/products/manuals/fr/VS_userguide_2008.pdf
德国	download.mcafee.com/products/manuals/de/VS_userguide_2008.pdf
英国	download.mcafee.com/products/manuals/en-uk/VS_userguide_2008.pdf
荷兰	download.mcafee.com/products/manuals/nl/VS_userguide_2008.pdf
意大利	download.mcafee.com/products/manuals/it/VS_userguide_2008.pdf
日本	download.mcafee.com/products/manuals/ja/VS_userguide_2008.pdf
韩国	download.mcafee.com/products/manuals/ko/VS_userguide_2008.pdf
墨西哥	download.mcafee.com/products/manuals/es-mx/VS_userguide_2008.pdf
挪威	download.mcafee.com/products/manuals/no/VS_userguide_2008.pdf
波兰	download.mcafee.com/products/manuals/pl/VS_userguide_2008.pdf
葡萄牙	download.mcafee.com/products/manuals/pt/VS_userguide_2008.pdf
西班牙	download.mcafee.com/products/manuals/es/VS_userguide_2008.pdf
瑞典	download.mcafee.com/products/manuals/sv/VS_userguide_2008.pdf
土耳其	download.mcafee.com/products/manuals/tr/VS_userguide_2008.pdf
美国	download.mcafee.com/products/manuals/en-us/VS_userguide_2008.pdf

请参阅下表来了解您所在国家/地区的 McAfee 威胁中心和病毒信息站点。

国家/地区	安全总部	病毒信息
澳大利亚	www.mcafee.com/us/threat_center	au.mcafee.com/virusInfo
巴西	www.mcafee.com/us/threat_center	br.mcafee.com/virusInfo
加拿大（英语）	www.mcafee.com/us/threat_center	ca.mcafee.com/virusInfo
加拿大（法语）	www.mcafee.com/us/threat_center	ca.mcafee.com/virusInfo
中国（中国）	www.mcafee.com/us/threat_center	cn.mcafee.com/virusInfo
中国（台湾）	www.mcafee.com/us/threat_center	tw.mcafee.com/virusInfo
捷克	www.mcafee.com/us/threat_center	cz.mcafee.com/virusInfo
丹麦	www.mcafee.com/us/threat_center	dk.mcafee.com/virusInfo
芬兰	www.mcafee.com/us/threat_center	fi.mcafee.com/virusInfo
法国	www.mcafee.com/us/threat_center	fr.mcafee.com/virusInfo
德国	www.mcafee.com/us/threat_center	de.mcafee.com/virusInfo
英国	www.mcafee.com/us/threat_center	uk.mcafee.com/virusInfo
荷兰	www.mcafee.com/us/threat_center	nl.mcafee.com/virusInfo
意大利	www.mcafee.com/us/threat_center	it.mcafee.com/virusInfo
日本	www.mcafee.com/us/threat_center	jp.mcafee.com/virusInfo
韩国	www.mcafee.com/us/threat_center	kr.mcafee.com/virusInfo
墨西哥	www.mcafee.com/us/threat_center	mx.mcafee.com/virusInfo
挪威	www.mcafee.com/us/threat_center	no.mcafee.com/virusInfo
波兰	www.mcafee.com/us/threat_center	pl.mcafee.com/virusInfo
葡萄牙	www.mcafee.com/us/threat_center	pt.mcafee.com/virusInfo
西班牙	www.mcafee.com/us/threat_center	es.mcafee.com/virusInfo
瑞典	www.mcafee.com/us/threat_center	se.mcafee.com/virusInfo
土耳其	www.mcafee.com/us/threat_center	tr.mcafee.com/virusInfo
美国	www.mcafee.com/us/threat_center	us.mcafee.com/virusInfo

请参阅下表来了解您所在国家/地区的 HackerWatch 站点。

国家/地区	HackerWatch
澳大利亚	www.hackerwatch.org
巴西	www.hackerwatch.org/?lang=pt-br
加拿大（英语）	www.hackerwatch.org
加拿大（法语）	www.hackerwatch.org/?lang=fr-ca
中国（中国）	www.hackerwatch.org/?lang=zh-cn
中国（台湾）	www.hackerwatch.org/?lang=zh-tw
捷克	www.hackerwatch.org/?lang=cs
丹麦	www.hackerwatch.org/?lang=da
芬兰	www.hackerwatch.org/?lang=fi
法国	www.hackerwatch.org/?lang=fr
德国	www.hackerwatch.org/?lang=de
英国	www.hackerwatch.org
荷兰	www.hackerwatch.org/?lang=nl
意大利	www.hackerwatch.org/?lang=it
日本	www.hackerwatch.org/?lang=jp
韩国	www.hackerwatch.org/?lang=ko
墨西哥	www.hackerwatch.org/?lang=es-mx
挪威	www.hackerwatch.org/?lang=no
波兰	www.hackerwatch.org/?lang=pl
葡萄牙	www.hackerwatch.org/?lang=pt-pt
西班牙	www.hackerwatch.org/?lang=es
瑞典	www.hackerwatch.org/?lang=sv
土耳其	www.hackerwatch.org/?lang=tr
美国	www.hackerwatch.org

索引

8

802.11 156
802.11a 156
802.11b 156
802.1x 156

A

ActiveX 控件 156
安装可用的网络打印机 154
按需扫描 161

B

Cookie 156
白名单 161
版权 169
暴力攻击 161
备份 161
编辑禁止的计算机连接 94
编辑信任的计算机连接 91
标准电子邮件帐户 161
病毒 161
拨号程序 161

C

参考 155
插件 161
查看出站事件 77, 99
查看全球 Internet 端口活动 100
查看全球安全事件统计信息 100
查看入侵检测事件 99
查看入站事件 99
查看扫描结果 50
查看事件 14, 23
查看所有事件 23
查看项目的详细信息 131
查看最新事件 23, 98
重命名网络 130, 144
出现警报时播放声音 20
处理病毒和特洛伊木马程序 51
处理隔离的程序和 Cookie 53
处理隔离的文件 52
处理可能有害的程序 52
处理扫描结果 51
存档 161

D

DAT 156
DNS 服务器 156
DNS 156
打开 EasyNetwork 141
代理 161
代理服务器 161
带宽 161
电子邮件 162
电子邮件客户端 162
端口 162
对计算机进行碎片整理 114

E

EasyNetwork 功能 140
ESS 157
恶意接入点 162

F

发布 162
发送文件时接收通知 151
防火墙 162
访问网络图 130
分析入站和出站通讯 104
服务器 162
复制共享文件 148

G

隔离 162
跟踪 Internet 通讯 101
跟踪监视的 IP 地址 103
跟踪网络计算机的位置 101
更新 SecurityCenter 11
共享 162
共享打印机 153
共享和发送文件 147
共享密钥 162
共享文件 148

关键字 162
关于 McAfee 169
关于 SystemGuard 类型 42
关于警报 62
关于可信列表类型 47
关于流量分析图 104
管理 Firewall 安全级别 66
管理 McAfee 帐户 10
管理程序和权限 75
管理计算机连接 89
管理可信列表 46
管理设备 137
管理系统服务 83
管理信息警报 63

H

黑名单 163
忽略保护问题 15
还原 163
缓冲区溢出 163
缓存 163
恢复 Firewall 设置 73
回收站 163
获取程序信息 82
获取计算机网络信息 101
获取计算机注册信息 101

I

Internet 157
IP 地址 157
IP 伪造 157

J

集成网关 163
计划 QuickClean 任务 115
计划磁盘碎片整理程序任务 117
计划任务 115
计划扫描 38
记录、监视和分析 97
加密 163
加入托管网络 132, 142, 145
加入网络 142
家长监控 163
家庭网络 163
监视 Internet 通讯 104
监视程序带宽 105
监视程序活动 105
监视计算机的保护状态 136
监视位置 163
监视文件类型 163
监视状态和权限 136
检查更新 11, 12
简介 3
将安全级别设置为 67, 68
将文件发给其他计算机 150
将文件发送到另一台计算机 150
脚本 163
接入点 164
接受另一台计算机发来的文件 150
节点 164
仅显示 70
禁用 69
禁用自动更新 12
禁止计算机连接 93
拒绝服务 164

K

可能有害的程序 (PUP) 164
可信列表 164
客户端 164
客户服务和技术支持 171
库 164
快捷方式 164
快速存档 164

L

LAN 157
launchpad 157
离开托管网络 145
立即解锁 Firewall 73
立即锁定 Firewall 73
联机备份库 164
了解 Internet 安全性 107
了解 Network Manager 图标 127
了解保护服务 9
了解保护类别 7, 9, 23
了解保护状态 7, 8, 9
了解程序 82
临时文件 164
浏览器 164
路由器 165

M

MAC 地址 157
MAPI 157
McAfee EasyNetwork 139

McAfee Network Manager....125
McAfee Personal Firewall....55
McAfee QuickClean....109
McAfee SecurityCenter....5
McAfee Shredder....121
McAfee VirusScan....25
MSN....157
漫游....165
密码....165
密码存储库....165
密文....165
密钥....165
明文....165

N

Network Manager 功能....126
NIC....157
内部网....165
内容评级组....165

P

PCI 无线适配器卡....158
Personal Firewall 功能....56
POP3....158
PPPoE....158
配置 Firewall 保护....65
配置 Firewall 的....72
配置 ping 请求设置....71
配置 SystemGuard 选项....41
配置警报的....69
配置警报选项....20
配置入侵检测....72
配置事件日志设置....98
配置系统服务端口....84
配置新服务端口....85
配置自动更新....12

Q

QuickClean 功能....110
启动 Firewall....59
启动 HackerWatch 教程....108
启动 Virtual Technician....172
启动电子邮件保护....30
启动防火墙保护....59
启动附加防护....29
启动过程中保护计算机....71
启动即时消息保护....31
启动间谍软件防护....30
启动脚本扫描防护....30
启动实时病毒防护....27
启用 SystemGuard 保护....41
启用....69
浅层监视位置....165
清除文件、文件夹和磁盘....123
清除文件和文件夹....123
清除整个磁盘....124
清理计算机....111, 112

R

RADIUS....158
Rootkit....158
热点....165
蠕虫....165

S

SecurityCenter 功能....6
Shredder 功能....122
SMTP....158
SSID....158
SSL....158
SystemGuard....158
扫描计算机....27, 49
扫台者....166
删除 QuickClean 任务....117
删除程序的访问权限....81
删除程序权限....81
删除磁盘碎片整理程序任务....118
删除禁止的计算机连接....94
删除系统服务端口....87
删除信任的计算机连接....92
设置 EasyNetwork....141
设置病毒防护....33, 49
设置实时扫描选项....34
设置手动扫描位置....37
设置手动扫描选项....36
设置托管网络....129
身份验证....166
深层监视位置....166
实时扫描....166
使用 McAfee Virtual Technician....172
使用 SecurityCenter....7
使用 SystemGuard 选项....40
使用共享打印机....154
使用警报....12, 17, 61
使用可信列表....46
使用统计信息....100
使用网络图....130

事件 166
事件记录 98
手动修复保护问题 14
授予对网络的访问权限 143
刷新网络图 130
搜索标准 149
搜索共享文件 149
锁定和恢复 Firewall 73

T

TKIP 159
弹出窗口 166
特洛伊木马程序 166
添加禁止的计算机连接 93
添加信任的计算机连接 90
停止防火墙保护 60
停止共享打印机 154
停止共享文件 148
停止监视计算机的保护状态 136
停止实时病毒防护 27
停止信任网络上的计算机 134
同步 166
图像过滤 166
托管网络 166

U

U3 159
URL 159
USB 驱动器 159
USB 无线适配器卡 159
USB 159

V

VirusScan 功能 26
VPN 159

W

Web 错误 159
Web 邮件 159
WEP 160
Wi-Fi Alliance 160
Wi-Fi Certified 160
Wi-Fi 160
WLAN 160
WPA 160
WPA2 160
WPA2-PSK 160
WPA-PSK 160
外部硬盘驱动器 166
完全存档 166
玩游戏时显示或隐藏信息警报 18
玩游戏时显示警报 63
网络 166
网络钓鱼 167
网络驱动器 167
网络图 167
文件碎片 167
无线适配器 167

X

显示和隐藏信息警报 18
显示或隐藏忽略的问题 15
显示或隐藏网络图中的项目 131
显示或隐藏信息警报 18
消息身份验证代码 (MAC) 167
协议 167
信任计算机连接 90
修复安全漏洞 138
修复保护问题 8, 14
修复或忽略保护问题 8, 13
修改 QuickClean 任务 116
修改磁盘碎片整理程序任务 118
修改设备的显示属性 137
修改托管计算机的权限 136
修改系统服务端口 86
许可 170
系统还原点 167

Y

压缩 167
验证您的订购 10
邀请计算机加入此托管网络 133
隐藏病毒发作警报 20
隐藏启动时的启动屏幕 20
隐藏信息警报 63
优化 Firewall 安全性 71
域 167
远程管理网络 135
允许程序访问 Internet 76
允许程序具有仅出站访问权限 78
允许程序具有完全访问权限 76
允许访问现有的系统服务端口 85
允许新程序具有完全访问权限 76

Z

在远程计算机上安装 McAfee 安全软件 138
支持和下载 173

智能驱动器.....167
中间人攻击.....168
注册表.....168
字典攻击.....168
自动修复保护问题.....14
阻止程序的 Internet 访问权限.....79
阻止程序具有访问权限.....79
阻止访问现有的系统服务端口.....85
阻止新程序的访问权限.....79