

Norton™ AntiVirus Plus
Norton™ 360
Norton™ 360 with LifeLock™
Norton™ 360 for Gamers

用戶手冊



Norton™ 360 with LifeLock™ 用户手册

本手册介绍的软件基于授权许可协议提供，且只能在遵守协议条款的前提下使用。

Copyright © 2021 NortonLifeLock Inc. © 2021 年 NortonLifeLock Inc. 版权所有。All rights reserved. 保留所有权利。

本文档中介绍的产品根据限制其使用、复制、分发和反编译/反向工程的授权许可协议分发。未经 NortonLifeLock Inc. 及其特许人（如果存在）事先书面授权，不得通过任何方式、以任何形式复制本文档的任何部分。

本文档按“现状”提供，对于所有明示或暗示的条款、陈述和保证，包括任何适销性、针对特定用途的适用性或无侵害知识产权的暗示保证，均不提供任何担保，除非此类免责声明的范围在法律上视为无效。NORTONLIFELOCK INC. 不对任何与提供或使用本文档相关的伴随或后果性损害负责。本文档所含信息如有更改，恕不另行通知。

根据 FAR 12.212 中的定义，授权许可的软件和文档被视为“商业计算机软件”，受 FAR 第 52.227-19 节“Commercial Computer Software - Restricted Rights”（商业计算机软件受限权利）和 DFARS 第 227.7202 节“Commercial Computer Software and Commercial Computer Software Documentation”（商业计算机软件或商业计算机软件文档）中的适用规定，以及所有后续法规中规定的权利的制约，无论是由诺顿LifeLock 在本地交付还是以托管服务的形式交付，概莫能外。美国政府仅可根据本协议的条款对授权许可的软件和文档进行使用、修改、发布复制、执行、显示或披露。

NortonLifeLock Inc.
60 East Rio Salado Parkway,
Suite 1000,
Tempe, AZ 85281

<https://www.nortonlifelock.com>

目录

第 1 章	欢迎使用 Norton LifeLock	5
	Norton 360 的系统要求	5
	访问 Norton 帐户	7
第 2 章	设置防护	9
	设置设备安全	9
	设置 Norton Password Manager	10
	设置云备份	15
	设置 LifeLock Identity Theft Protection	15
	暗网监控（由 LifeLock 提供支持）**	17
	设置安全 VPN	17
	设置家长控制	18
	使用 Norton Safe Web 保护银行信息	22
第 3 章	管理设备安全	23
	设备存在风险时要采取的操作	23
	运行 LiveUpdate	24
	查看或修复 Norton 检测到的设备安全风险	24
	处理隔离的风险或威胁	25
	使用 Norton 优化和提高计算机性能	27
	运行 Norton 扫描以检查 PC 上的威胁	30
	创建自己的自定义 Norton 扫描	33
	调度 Norton 扫描	34
	查看 Norton SONAR 检测到的实时威胁	35
	从 Norton 自动防护、SONAR 和下载智能分析扫描中排除文件和 文件夹	36
	从 Norton 扫描中排除具有低风险特征的文件	37
	打开或关闭自动任务	38
	运行自定义任务	38
	调度安全与性能扫描	39
	配置数据保护器以阻止影响您计算机的恶意进程	40
	设置 Norton 以删除在企图进行网络钓鱼时可利用的脚本	43
	详细了解 Norton 脚本控制	46
	保护您的设备免受漏洞利用、黑客和零日攻击的威胁	48

打开或关闭 Norton 防火墙	49
自定义程序规则以更改程序的访问设置	50
更改防火墙规则的顺序	50
暂时关闭通信规则	51
允许阻止的程序访问 Internet	52
关闭防火墙阻止通知	53
详细了解“入侵防护”排除列表	54
打开浏览器主动防护	54
设置 Norton 防火墙以停止或启动阻止攻击时向您发出通知	55
关闭或打开 AutoBlock	56
取消阻止 Norton 自动阻止功能已阻止的电脑	57
将设备添加到“设备信任”	57
关闭或打开“下载智能分析”	58
关闭或打开垃圾邮件过滤	59
定义 Norton 产品的 Internet 使用量	60
关闭或打开“网络流量感测”	61
设置 Norton 以监控应用程序并阻止恶意网站访问您的计算机	61
开始使用诺顿云备份	63
在备份集中添加或排除文件和文件夹	64
查看或更改 Norton 包括在备份中的默认文件类型或文件扩展 名	65
从 Norton 备份集还原图片、音乐或其他重要文件	66
从云备份中删除备份集和文件	67
自定义 Norton 产品设置	68
自定义“实时防护”设置	68
详细了解“扫描和风险”设置	70
详细了解入侵和浏览器主动防护设置	72
设置 Norton 以允许您远程管理受保护的设备	73
保护 Norton 设备安全设置免受未经授权的访问	73
设置在 Norton 设备安全中搜索信息的快捷键	74
使用 Game Optimizer 优化您计算机的游戏体验	74
详细了解 Game Optimizer	76
手动将游戏添加到“已优化游戏”列表中	77
第 4 章 查找其他解决方案	78
在 Windows 上卸载设备安全	78
免责声明	78

欢迎使用 Norton LifeLock

本章节包括下列主题：

- [Norton 360 的系统要求](#)
- [访问 Norton 帐户](#)

Norton 360 的系统要求

仅限 Norton 设备安全授权

- Norton AntiVirus™ Plus 涵盖一台 PC 或 Mac

设备安全和 Norton Secure VPN 授权

支持在 Windows、Mac、Android 和 iOS 上运行的设备

- Norton™ 360 Standard 涵盖一台设备
- Norton™ 360 Deluxe 最多可涵盖 5 台设备
- Norton™ 360 Premium 最多可涵盖 10 台设备
- Norton™ 360 with LifeLock Select 最多可涵盖 5 台设备
- Norton™ 360 with LifeLock Advantage 最多可涵盖 10 台设备
- Norton™ 360 with LifeLock Ultimate Plus 涵盖无限台设备（存在一定限制*）
- Norton™ 360 for Gamers 最多可涵盖 3 台设备

注意：并非所有地区或所有合作伙伴都可以使用上述所有诺顿LifeLock 防护产品。

设备安全性

注意：并非所有平台都提供所有功能。

注意：Mac 操作系统当前不支持家长控制、云备份和 SafeCam。

Windows™ 操作系统

- ◆ ■ Microsoft Windows® 10（所有版本）
 - S 模式的 Microsoft Windows® 10（32 位或 64 位或 ARM32）1803 版和更高版本
 - Microsoft Windows® 8/8.1（所有版本）
某些保护功能无法在 Windows 8 开始屏幕浏览器中使用。
 - Microsoft Windows® 7（32 位和 64 位）（带 Service Pack 1 (SP 1) 或更高版本）

注意：Norton AntiVirus Plus 在 S 模式的 Windows 10 上不受支持。

Norton Crypto 的设备要求

Norton Crypto 需要以下硬件规格才能运行。

- Microsoft Windows® 10/8/7*（64 位）
*Microsoft Windows 7 with Service Pack 1 (SP 1) 或更高版本
- 显卡 - Nvidia/AMD 卡，至少 6 GB 内存

注意：Norton Crypto 在 Windows 10 S 模式上不受支持。

Mac® 操作系统

- ◆ Mac OS X 10.10.x 或更高版本，并装有 Norton 产品版本 8.0 或更高版本。

注意：Mac 操作系统当前不支持 Norton Family 家长控制和云备份。

Android™ 操作系统

- ◆ Android 6.0 或更高版本

必须安装有 Google Play 应用程序。

自动扫描 Google Play 上的应用程序在 Android 4.1 或更高版本上受支持，但 Samsung 设备除外。运行 Android 4.2 或更高版本的 Samsung 设备受支持。对于更早版本的 Android，必须使用 Google Play 的“共享”功能在 Google Play 上扫描应用程序。

iOS 操作系统

- ◆ 运行当前版本和之前两个版本的 Apple iOS 的 iPhone 或 iPad

Norton™ Secure VPN 的系统要求

适用于 Windows™ PC、Mac®、iOS 和 Android™ 设备：

Norton Secure VPN 与 PC、Mac、Android 智能手机和平板电脑、iPad 以及 iPhone 兼容。Norton Secure VPN 可在指定数量的设备上使用 - 在订购期限内无限制使用。

Windows™ 操作系统

- ◆
 - Microsoft Windows® 10 (Windows 10 S 以外的全部版本)
 - Microsoft Windows® 8/8.1 (所有版本)
 - Microsoft Windows® 7 (32 位和 64 位) (带 Service Pack 1 (SP 1) 或更高版本)

150 MB 可用硬盘空间。

Mac® 操作系统

- ◆ 当前和前两个版本的 Mac OS。

300 MB 可用硬盘空间。

Android™ 操作系统

- ◆ Android 6.0 或更高版本
必须安装有 Google Play 应用程序。

iOS 操作系统

- ◆ 运行当前版本和之前两个版本的 Apple iOS 的 iPhone 或 iPad

访问 Norton 帐户

在购买或安装您的 Norton 产品时创建将帐户。您可以管理您的订购、查找您的产品密钥、激活订购续订或从您的帐户访问其他服务。

访问您的帐户

- 1 转到 my.Norton.com，并单击“登录”。
如果您没有 Norton 帐户，请单击“创建新帐户”，然后完成注册过程。
- 2 键入您的用户名或电子邮件地址和密码，然后单击“登录”。
- 3 如果忘记密码，请单击“忘记密码？”，然后按照屏幕上的说明找回丢失的密码。

无法访问您的帐户？

- ◆ ■ **我的帐户已注册到旧电子邮件地址：** 如果无法访问您的旧电子邮件，请联系[客户服务和支持](#)以获取帮助。
- **我的帐户被暂时锁定：** 如果看到一条消息，提示您由于失败登录尝试次数过多而暂时锁定了您的帐户，建议您等待一小时，然后再次尝试登录。
- **我在使用双重身份验证时遇到问题：** 要设置双重身份验证以及解决常见的双重身份验证问题，请阅读[常见问题解答：针对帐户的双重身份验证](#)。

是否需要更多帮助？

- [修复 Norton 中显示的错误订购日期](#)
- [在不小心购买了多个 Norton 订购时解决重复收费](#)

设置防护

本章节包括下列主题：

- 设置设备安全
- 设置 Norton Password Manager
- 设置云备份
- 设置 LifeLock Identity Theft Protection
- 设置安全 VPN
- 设置家长控制
- 使用 Norton Safe Web 保护银行信息

设置设备安全

要保护您的设备，必须安装 Norton 设备安全。可以在 Windows 台式机和笔记本电脑、Mac 计算机以及在 Android 和 iOS 上运行的移动设备上安装设备安全。

下载并安装设备安全

- 1 从每台计算机、笔记本电脑和智能手机，打开浏览器并输入以下 URL：
<https://norton.com/setup>
- 2 登录诺顿LifeLock 帐户。

- 3 在“Norton 安装”窗口中，单击“同意并下载”。



- 4 单击屏幕上箭头所指区域并按照屏幕上的说明进行操作。
系统将自动下载、安装并激活您的服务。

注意： 如果下载未完成，或者下载服务时看到任何错误，可重新开始下载。

设置 Norton Password Manager

安装 Device Security 之后，会提示您添加浏览器扩展。为了使功能发挥作用，您需要在 Internet Explorer、Firefox 和 Chrome 浏览器中添加扩展。

您必须启用 Norton 浏览器扩展，才能访问所有特定于浏览器的功能。Norton 浏览器扩展包括：

Norton Safe Web

一种安全的搜索体验，可帮助您冲浪、搜索以及安全地在线购物。它会分析您访问的网站，并检测是否存在任何病毒、间谍软件、恶意软件或其他威胁。

Norton Safe Search

一种安全的搜索引擎，使用 Ask.com 和 Yahoo! 生成搜索结果。Norton Safe Search 基于站点安全状态和 Norton 评级对搜索结果进行排名。

Norton 主页

使用 Norton Safe Search 功能增强用户 Web 搜索体验的网站。该网页将针对生成的每个搜索结果提供站点安全状态和 Norton 评级。

Norton Password Manager

可以存储所有敏感信息（如登录信息、个人信息和财务信息）的安全位置。您可以使用该信息登录到网站，自动填写在线表单和在线付款。

Internet Explorer

在 Internet Explorer 中添加 Norton 浏览器扩展

- 1 初次安装 Norton 后，启动新 Internet Explorer 会话时，“浏览器主动防护”页面将自动在新的窗口中打开。
- 2 在“浏览器主动防护”页面中，单击“**Norton Security 工具栏**”的“启用”选项。
- 3 在显示的扩展弹出窗口中，单击“添加扩展”。
- 4 启用 Norton Security 工具栏后，您可以为浏览器启用 Norton Safe Search 扩展、Norton 主页扩展和 Norton Password Manager 扩展。

您可以使用“单击以添加”选项并按照屏幕上的说明来启用这些功能。

- 5 如果您未安装这些扩展中的任何一项，则一周后启动 Internet Explorer 时，会显示“**Internet Explorer 防护警报**”通知。

单击“立即安装”并按照屏幕上的说明来安装这些扩展。

注意： 如果要在稍后启用 Norton 扩展，请单击“以后再提醒我”。如果您不希望显示通知警报，请单击“不要再询问”。

Google Chrome

在 Google Chrome 中添加 Norton 浏览器扩展

注意： 必须拥有最新版本的 Norton 360 才能安装 Google Chrome 的浏览器扩展。如果没有最新版本，请在您的 Norton 产品中运行 LiveUpdate。我们为 Google Chrome 浏览器提供了以下扩展：

- Norton Safe Web
- Norton Password Manager
- Norton Safe Search
- Norton 主页

您可以按照以下说明安装 Chrome 的浏览器扩展。

- 1 初次安装 Device Security 后，启动新 Google Chrome 会话时，将自动在新的窗口中打开“浏览器主动防护”页面。

也可以通过单击“**Internet 安全性**”列中的“立即设置”选项启动“浏览器主动防护”页面。

- 2 在“浏览器主动防护”页面中，单击 **Norton Safe Web** 的“单击以添加”选项。

- 3 在显示的扩展弹出窗口中，单击“添加扩展”。
- 4 启用 Norton Safe Web 后，您可以为浏览器启用 Norton Safe Search、Norton 主页和 Norton Password Manager 扩展。您可以使用“单击以添加”选项并按照屏幕上的说明来启用这些扩展。

要在 Google Chrome 中启用所有 Norton 扩展，请单击“免费添加所有 Norton 扩展”，然后按照屏幕上的说明执行操作。

 - 如果您未安装 Norton Safe Web 扩展，则一周后启动 Google Chrome 时，会显示“Chrome 防护已删除”警报通知。
 - 如果您未安装这些扩展中的任何一项，则一周后启动 Google Chrome 时，会显示“Google Chrome 防护警报”通知。
- 5 单击“立即安装”并按照屏幕上的说明来安装这些扩展。

注意：如果要在稍后启用 Norton 扩展，请单击“以后再提醒我”。如果不希望显示此通知警报，请单击“不要再询问”。

Mozilla Firefox

在 Mozilla Firefox 中添加 Norton 浏览器功能

注意：必须拥有最新版本的 Norton 360 才能安装 Mozilla Firefox 的基于 Web 的独立浏览器扩展。如果没有最新版本，请在您的 Norton 产品中运行 LiveUpdate。我们为 Firefox 浏览器提供了以下扩展：

- Norton Safe Web
- Norton Safe Search
- Norton 主页
- Norton Password Manager

您可以按照以下说明安装或升级 Firefox 浏览器扩展。

- 1 初次安装 Device Security 后，启动新 Mozilla Firefox 会话时，将自动在新的窗口/选项卡中打开“浏览器主动防护”页面。

如果已升级 Norton Device Security，请单击“浏览器主动防护”警报窗口中的“确定”显示扩展页面。

注意：也可以通过单击“Internet 安全性”列中的“立即设置”选项启动“浏览器主动防护”页面。

- 2 在“浏览器主动防护”页面中，单击 **Norton Safe Web** 的“启用”选项。
- 3 在显示的扩展弹出窗口中，单击“允许”。

启用 Norton Safe Web 后，您可以为浏览器启用 Norton Safe Search、Norton 主页和 Norton Password Manager 功能。您可以使用“启用”选项并按照屏幕上的说明来启用这些功能。

要在 Firefox 中启用所有 Norton 扩展，请单击“免费添加所有 Norton 扩展”，然后按照屏幕上的说明执行操作。

如果您未安装这些扩展，则一周后启动 Firefox 时，会显示“Firefox 防护警报”通知警报。如果要在稍后启用 Norton 扩展，请单击“以后再提醒我”。如果您不希望显示通知警报，请单击“不要再询问”。如果选择“稍后提醒我”，Firefox 会在一周后显示防护警报通知。您可以单击通知中的“立即安装”选项，然后按照屏幕上的说明安装扩展。

Microsoft Edge

在 Microsoft Edge 中添加 Norton 浏览器扩展

注意：Norton Password Manager 为独立扩展，不需要在 Microsoft Edge 浏览器中安装 Norton 产品。此扩展仅与运行 Windows 10 Creators Update（创意者更新）及更高版本的计算机兼容。

- 1 启动 Microsoft Edge 浏览器。
 - 2 在右上角，单击“更多”按钮，然后选择“扩展”。
 - 3 在“扩展”窗口中，单击“从应用商店获取扩展”。
 - 4 在“商店”窗口的搜索框中键入 **Norton**，然后单击结果中的 **Norton Password Manager**。
 - 5 单击“安装”。
- 安装扩展后，单击“启动”。
- 6 在“你有一个新扩展”弹出窗口中，单击“启用”。

- 7 要在地址栏中显示 Norton Password Manager 图标，请单击浏览器右上角的“更多”按钮，然后单击“扩展”。
- 8 在“扩展”窗口中，选择 **Norton Password Manager**。
- 9 在 **Norton Password Manager** 窗口的“在地址栏旁边显示按钮”下，将滑块移动到“打开”位置。

基于 Chromium 的 Microsoft Edge 的浏览器扩展

Microsoft 已基于 Chromium 开源项目启动了新版本的 Microsoft Edge。Norton 为 Microsoft Edge 商店的此新浏览器版本提供了以下浏览器扩展。

- Norton Password Manager - 帮助您提供您需要的工具，让您更安全地在线创建、存储和管理密码、信用卡以及其他敏感信息
- Norton Safe Web - 使您在浏览 Web 时免遭在线威胁。

这些扩展适用于 Windows 和 Mac 平台。

在 Microsoft Edge 中添加 Norton Safe Web 扩展

- 1 启动 Microsoft Edge 浏览器。
- 2 从“Microsoft Edge 加载项”页面启动 [Norton Safe Web 扩展](#)。

注意：可以依次单击设置图标和“扩展”，检查是否已安装 Norton Password Manager 扩展。在“扩展”页面上，移动 Norton Safe Web 滑块以启用扩展。

- 3 在“Norton Safe Web 加载项”页面中，单击“获取”。
- 4 在“将 **Norton Safe Web** 添加到 **Microsoft Edge**”通知弹出窗口中，单击“添加扩展”安装 Norton Safe Web 扩展。

在 Microsoft Edge 中添加 Norton Password Manager 扩展

- 1 启动 Microsoft Edge 浏览器。
- 2 从“Microsoft Edge 加载项”页面启动 [Norton Password Manager 扩展](#)。

注意：可以依次单击设置图标和“扩展”，检查是否已安装 Norton Password Manager 扩展。在“扩展”页面上，移动 Norton Password Manager 滑块以启用扩展。

- 3 在“Norton Password Manager 加载项”页面中，单击“获取”。
- 4 在“将 Norton Password Manager 添加到 Microsoft Edge”通知中，单击“添加扩展”安装 Norton Password Manager 扩展。

设置云备份

云备份是一种预防性措施，可防止出现勒索软件、恶意软件或 PC 遇到重大硬件问题导致数据丢失的情况。您的订购将提供特定量的诺顿云备份空间。可用的云存储量取决于您购买的订购。

注意：诺顿云备份功能仅适用于 Windows。

首次运行备份之前，必须激活云备份。

注意：要使用云备份，必须将“防火墙设置”窗口中的“网络流量感测”选项设置为“无限制”。

激活“云备份”

- 1 启动 Norton。
- 2 在“我的 Norton”窗口中，单击“云备份”旁边的“设置”。
- 3 在出现的窗口中，单击“激活备份”。
- 4 出现登录提示时，键入诺顿LifeLock 帐户电子邮件地址和密码，然后单击“登录”。
- 5 单击“完成”。

设置 LifeLock Identity Theft Protection

随着 LifeLock 和 Norton 合力于一家公司，我们现在可帮助保护您的身份。

您可以将以下个人信息添加到 LifeLock 以进行监控†：

- 驾照
- 身份证号、出生日期、母亲的婚前姓氏
- 5 个保险 ID
- 5 个地址
- 5 个电话号码

- 10 个银行帐户
- 10 个信用卡*

可以添加更多的信息以进行监控，例如更多的电话号码、电子邮件地址或帐户。

当某人使用您的身份时，LifeLock 身份警报系统会向您发出警报†。可能有人在试图以您的名义获得手机帐户或汽车贷款。

注意：LifeLock Identity Theft Protection 不为企业提供保护。我们的技术和服务旨在帮助保护有身份证号和其他个人身份信息的个人，而企业没有这些信息。

*可以添加大多数信用卡，如 Visa、MasterCard、American Express 和 Discover。遗憾的是，目前还不支持其他类型的卡，如零售店卡或礼品卡。

没有人能阻止所有身份盗用或网络犯罪。

†LifeLock 不会监控任何企业的任何交易。

设置 LifeLock Identity Theft Protection

- 1 启动 Norton。
- 2 在“我的 Norton”窗口中，单击 **Identity Theft Protection** 旁边的“设置”。
- 3 在“LifeLock 会员登录”页面上，单击“使用 Norton 登录”。
- 4 输入帐户凭据并登录。
- 5 按照屏幕上的说明操作。

在 Android 上安装 LifeLock for Norton 360 应用程序

- 1 在 Android 设备上，启动 **Play Store** 应用程序，然后搜索 **LifeLock Identity Theft Protection**。
- 2 在 Play Store 中找到该应用程序页面后，点击“安装”，然后点击“接受”。
- 3 安装完成后打开应用程序，并使用您的帐户凭据登录。

在 iOS 上安装 LifeLock for Norton 360 应用程序

- 1 在 iOS 设备上，启动 **App Store** 应用程序，然后搜索 **LifeLock Identity Theft Protection**。
- 2 在 App Store 中找到该应用程序页面后，点击“获取”，然后点击“安装”。
- 3 安装完成后打开应用程序，并使用您的帐户凭据登录。

暗网监控（由 LifeLock 提供支持）**

什么是暗网监控？

我们可监控您的个人信息**在不易发现的暗网和论坛中的使用。当我们在暗网上检测到您的信息时，会您发出通知。

为何如此重要？

身份窃贼可能会在不易发现的暗网和论坛上出售您的个人信息。

您应采取哪些措施？

如果您在通知中发现您的任何信息，请参考下面的步骤。

- **借记卡/信用卡泄漏：**如果卡已注销，则不需要采取任何措施。如果帐户正常，请联系您的信用卡/借记卡公司，并申请新卡。密切关注您的帐单。
- **电子邮件泄漏：**更改您当前的电子邮件密码。如果您的任何帐户都使用此密码，也请更改这些帐户。如果问题持续存在，您可能需要开立一个新的电子邮件帐户。切记，每 30 天更换一次密码有助于保证您帐户的安全。
- **身份证号泄漏：**我们建议您在三家征信机构中的一家设置欺诈警报，以进一步保护您的身份。
- **姓名/地址/电话号码泄漏：**幸运的是，在这种情况下，潜在破坏性更强的信息（如您的身份证号）没有被分享。但是，由于会泄漏一些个人信息，我们建议密切关注您的信用报告中是否存在任何差异。

我们将继续监控暗网以监测是否存在您的个人信息**。如果检测到您的信息，我们将发送另一封电子邮件。

注意： 没有人能阻止所有身份盗用。

**Norton 360 中的暗网监控功能计划默认只监控您的电子邮件地址。请登录门户查看是否可以添加其他信息以便进行监控。

设置安全 VPN

公共 Wi-Fi 随处可用：机场、咖啡厅、商场和酒店。免费“热点”分布之广且非常便利，人们往往会不假思索地建立连接。但阅读电子邮件，检查银行帐户或执行需要登录的任何活动时，使用公共 Wi-Fi 则充满危险。如果使用公共 Wi-Fi，您的在线活动可能受到监控。网络罪犯可能会窃取您的个人信息，如用户名、密码、位置、聊天数据、电子邮件或帐号。

Secure VPN 可帮助您使用公共无线连接时确保您的连接安全。它可创建虚拟专用网络 (VPN)，对您的敏感数据进行加密。

Secure VPN 通过以下方式在您使用公共 Wi-Fi 发送和接收数据时提供保护：

- 添加银行级加密以在您使用公共 Wi-Fi 热点时保护您的连接。

- 支持匿名浏览 Web 以保护您的网络隐私。
- 可在任何地方访问您喜欢的应用程序和内容，就像在家一样。
- 使用不跟踪或存储您活动的无日志虚拟专用网络加密您的数据。
- Norton LifeLock（消费者在线安全领导者）提供一流的客户支持。

注意：并非所有订购都提供 Secure VPN 功能。

请按照以下说明设置 Secure VPN。

设置 Secure VPN

- 1 启动 Norton。
- 2 在“我的 Norton”窗口中，单击“安全 VPN”旁边的“设置”。
- 3 在出现的网页中，单击“登录”。
- 4 输入帐户凭据并登录。
- 5 如果出现下载提示，请单击“下载”。
- 6 按照屏幕上的说明操作。

单击此处，加入 [Norton 社区](#)，与其他桌面用户进行讨论。

设置家长控制

现在，可以设置家长控制，以帮助孩子安全上网。只需三步即可完成设置，过程非常简单。

家长控制提供用于保护您家人上网时远离 Internet 危险和不当内容所需的资源。它甚至可以帮助您阻止孩子在线传递保密信息。

登录诺顿LifeLock 帐户

- 1 启动 Norton。
- 2 在“我的 Norton”窗口中，单击“家长控制”旁边的“设置”。
- 3 如果系统提示您登录，请输入帐户凭据并登录。
- 4 在显示的页面中，单击 **Family** 选项卡。
- 5 阅读“服务条款”，然后单击“同意并继续”设置您的家人。
- 6 按照屏幕上的说明操作。

在帐户中添加孩子

添加每个孩子时，家长控制会应用基于孩子年龄预定义的家规。您可以随时自定义家规，以便家规更适应孩子的成熟度。

注意：最多可将 15 名孩子添加到帐户。可随时将孩子添加到 Norton Family 帐户，或从其中删除孩子。

- 1 在“孩子姓名”框中，键入孩子的姓名。

注意：姓名不得包含特殊字符，例如 &、# 或 \$。

- 2 选择孩子的出生年份。
根据孩子的年龄应用不同的家规。
- 3 选择“选择头像”或“上传照片”为孩子设置个人档案图片。

注意：在您完成第一个孩子的设置之后，可以向帐户中添加更多孩子。

- 4 单击“下一步”。

在孩子的设备上安装 Norton Family

在您孩子使用的每台设备上安装 Norton Family。如果您未使用孩子的设备，请单击“否”通过电子邮件发送下载链接。在要安装 Norton Family 的设备上打开此电子邮件。

在 Windows 上安装 Norton Family

- 1 在“您的孩子使用此设备吗？”，单击“是”，然后单击“下一步”。
- 2 单击或运行已下载的安装程序文件。
- 3 Norton 下载管理器将自动在设备上安装 Norton Family。
- 4 阅读用户授权许可协议，然后单击“同意并安装”。
此设备将自动与您的帐户关联在一起。
- 5 单击“继续”。
- 6 在“分配设备”窗口中，单击您要向其分配该设备的孩子旁边的“编辑”。
- 7 单击“登录身份”，然后选择孩子用于登录到此设备的帐户。如果孩子使用多个用户帐户，请在所有这些用户帐户上选择孩子。
- 8 单击“保存” > “确定”。

在 Android 上安装 Norton Family 应用程序

- 1 在“安装 Norton Family”窗口，点击“是”，然后点击“继续”。
- 2 点击“下载 Norton Family 应用程序”。

- 3 如果系统提示，请使用 **Play Store** 完成操作。
- 4 点击“安装”，并按照屏幕上的说明操作。
- 5 打开 **Norton Family** 家长控制应用程序。
- 6 阅读“**Norton 授权许可协议**”，然后点击“**同意并继续**”>“**开始**”。
- 7 单击“**登录**”，并输入您的帐户凭据。
- 8 点击“**孩子**”进入孩子模式，然后点击“**继续**”。
孩子模式允许您添加孩子并为此设备分配家规。
- 9 要添加孩子，请点击“**添加孩子**”，并在“**个人档案**”窗口中输入孩子的详细信息。
通过点击头像图像，为孩子的档案选择一个头像。您可以从图库中选择一个图像或拍摄快照供孩子的档案使用。
- 10 点击“**继续**”，然后点击“**保存**”。
Norton Family 已根据您孩子的出生年份设置默认家规。点击“**家规**”可查看已分配给孩子的家规。
- 11 选择要将此设备分配给的孩子，并提供一个有助于您识别此设备的名称，然后点击“**完成**”。
- 12 如果出现提示，请启用“**应用程序使用情况**”和“**可访问性**”选项。
- 13 在出现的警报中，点击“**激活**”，以设备管理员的身份设置 **Norton Family**。

在 iOS 上安装 Norton Family 应用程序

- 1 在“**安装 Norton Family**”窗口，点击“**是**”，然后点击“**继续**”。
- 2 点击“**下载 Norton Family 应用程序**”。
- 3 点击并安装 **Norton Family** 应用程序。
- 4 点击“**打开**”。
- 5 点击“**确定**”以允许 **Norton Family** 向您发送通知。
- 6 阅读“**Norton 授权许可协议**”和“**隐私政策**”，然后点击“**同意并继续**”。
- 7 使用帐户凭据登录。
- 8 在“**添加孩子**”屏幕上，输入孩子的详细信息，然后点击“**添加**”。
要添加另一个孩子，请点击“**添加新的孩子**”，在“**添加孩子**”窗口中，输入孩子的详细信息，然后点击“**添加**”。
通过点击头像图像，为孩子的档案选择一个头像。您可以从图库中选择一个图像或拍摄快照供孩子的档案使用。

- 9 选择要向其分配此设备的孩子，并提供一个可帮助您识别此设备的名称。
- 10 点击“分配”。
- 11 点击“安装”，然后按照屏幕上的说明安装配置文件。
必需安装配置文件，即时锁定和其他功能才可在孩子的设备上运行。
- 12 按照屏幕上的说明设置限制条件。

在家长设备上安装 Norton Family

设置完成后，必须在您的设备上下载并安装以下移动应用程序：

- Android 设备：安装“**Norton Family 家长控制**”应用程序
- iOS 设备：安装“**家长版 Norton Family**”应用程序

在 Android 上下载并安装 Norton Family 家长控制应用程序

- 1 打开 Play Store 应用程序，然后搜索“**Norton Family 家长控制**”。
- 2 选择“**Norton Family 家长控制应用程序**”，然后点击“安装”。
- 3 安装应用程序后将其打开。
- 4 阅读“**Norton 授权许可协议**”和其他策略，然后点击“继续”。
- 5 使用帐户凭据登录。
- 6 点击“**家长设备**”。如果您与孩子共用设备，请在将设备交给孩子之前切换至“**孩子模式**”。

在 iOS 上下载并安装家长版 Norton Family 应用程序

- 1 打开 App Store 应用程序，然后搜索“**家长版 Norton Family**”。
- 2 选择“**家长版 Norton Family**”，然后点击“获取”。
- 3 安装应用程序后将其打开。

- 4 阅读“Norton 授权许可协议”和其他策略，然后点击“继续”。
- 5 使用帐户凭据登录。

与家人进行讨论

与家人沟通是确保家庭上网安全的关键。因此，您可以主动与孩子展开讨论，解释为何必须负责任地使用 Internet。

使用 Norton Safe Web 保护银行信息

当您通过银行网站进行交易时，Norton Safe Web 的银行保护功能可以提供更高的安全性。使用 Google Chrome、Mozilla Firefox 或 Microsoft Edge 浏览器访问银行网站时，您将收到安装或启用 Norton Safe Web 扩展的通知。单击通知中的“安装”或“启用”，并按照屏幕上的说明安装或启用 Norton Safe Web 扩展。

您可以单击通知中的“不要再显示”或转至“设置”窗口关闭“银行保护通知”警报。

关闭或打开“银行保护通知”

- 1 启动 Norton。
看到“我的 Norton”窗口时，单击“设备安全性”旁边的“打开”。
- 2 在 Norton 产品主窗口中，单击“设置”。
- 3 在“设置”窗口中，单击“防火墙”。
- 4 在“入侵和浏览器主动防护”选项卡上的“银行保护通知”行中，将“打开/关闭”滑块移到“关闭”或“打开”。
- 5 在“设置”窗口中，单击“应用”，然后单击“关闭”。

管理设备安全

本章节包括下列主题：

- [设备存在风险时要采取的操作](#)
- [使用 Norton 优化和提高计算机性能](#)
- [运行 Norton 扫描以检查 PC 上的威胁](#)
- [保护您的设备免受漏洞利用、黑客和零日攻击的威胁](#)
- [设置 Norton 以监控应用程序并阻止恶意网站访问您的计算机](#)
- [开始使用诺顿云备份](#)
- [自定义 Norton 产品设置](#)
- [使用 Game Optimizer 优化您计算机的游戏体验](#)

设备存在风险时要采取的操作

在 Norton 主窗口中，“安全性”、“Internet 安全性”、“备份”和“性能”磁贴的颜色表示每个类别的状态，如下所示：

- **绿色：**您具有保护。
- **橙色：**您需要注意您的计算机安全。
- **红色：**您的计算机存在风险。

注意：备份类别仅适用于高级版、专业版和 Norton 360 订购。

Norton 自动修复降低防护或系统性能的大多数问题，并在主窗口中显示“受保护”状态。Norton 将需要您注意的问题显示为“存在风险”或“注意”状态。

响应“注意”和“存在风险”状态指示器

- 1 启动 Norton。
看到“我的 Norton”窗口时，单击“设备安全”旁边的“打开”。
- 2 在 Norton 主窗口中，单击指示“存在风险”或“注意”类别的红色或橙色磁贴。
- 3 单击“立即修复”并按照屏幕上的说明进行操作。

如果仍然存在问题，单击“帮助”>“获取支持”运行诊断工具。

如果您认为您的计算机已受到严重感染，也可以尝试使用 [Norton Rescue Tools](#)。

运行 LiveUpdate

诺顿LifeLock 建议您在以下情况下定期运行 LiveUpdate 更新：

- 如果您已关闭“自动 LiveUpdate 更新”选项
- 如果计算机长时间未连接到 Internet

注意：要运行 LiveUpdate 更新，您需要具有有效的订购和 Internet 连接。

手动运行 LiveUpdate

- 1 启动 Norton。
看到“我的 Norton”窗口时，单击“设备安全性”旁边的“打开”。
- 2 在 Norton 产品主窗口中，双击“安全”，然后单击 **LiveUpdate**。
- 3 成功完成 LiveUpdate 后，在 **Norton LiveUpdate** 窗口中，单击“确定”。

查看或修复 Norton 检测到的设备安全风险

Norton 检测到安全风险时，除非需要您提供输入以了解您要如何解决风险，否则会自动删除该风险。如果您确实需要提供输入，则 Norton 会显示“检测到威胁”警报或“安全风险”警报以及如何应对安全风险的建议。

查看在扫描期间自动解决的风险

- 1 启动 Norton。
看到“我的 Norton”窗口时，单击“设备安全”旁边的“打开”。
- 2 在 Norton 主窗口中，双击“安全性”，然后单击“历史记录”。
- 3 在“安全历史记录”窗口的“显示”下拉列表中，选择“已解决的安全风险”。
- 4 选择列表中的风险，然后在“详细信息”窗格中查看采取的操作。

修复在扫描期间检测到的未解决的风险

在某些情况下，Norton 不会自动解决风险，但会向您建议应执行的操作以解决风险。

修复在扫描期间检测到的未解决的风险

- 1 启动 Norton。
看到“我的 Norton”窗口时，单击“设备安全”旁边的“打开”。
- 2 在 Norton 主窗口中，双击“安全性”，然后单击“历史记录”。
- 3 在“安全历史记录”窗口的“显示”下拉列表中，选择“未解决的安全风险”。
- 4 如果显示未解决的风险，请选择列表中的风险。
- 5 请遵循“详细信息”窗格中的“建议操作”。

注意：有时，在 Norton 消除安全风险之后，您可能需要重新启动计算机。如果 Norton 提示您重新启动计算机，应先保存所有打开的文件，然后再重新启动计算机。

注意：如果认为您的系统受到感染，请运行 Norton Power Eraser。Norton Power Eraser 是一个功能强大的恶意软件删除工具，可清除难以删除的安全风险。有关详细信息，请参见第 30 页的[“运行 Norton 扫描以检查 PC 上的威胁”](#)。

处理隔离的风险或威胁

隔离的项目与计算机的其他项目相隔离，因此它们无法进行传播或感染您的计算机。如果您认为某个项目已受到感染，但未被 Norton 识别为风险，您可以手动隔离该项目。如果您认为某个项目的风险较低，也可以从隔离区还原该项目。Norton 不修复您还原的项目。但是，Norton 可在后续扫描期间对还原的项目进行杀毒。

还原隔离区中的项目

- 1 启动 Norton。
看到“我的 Norton”窗口时，单击“设备安全”旁边的“打开”。
- 2 在 Norton 主窗口中，双击“安全性”，然后单击“历史记录”。
- 3 在“安全历史记录”窗口的“显示”下拉列表中，选择“隔离”类别。
- 4 选择要管理的项目。
- 5 在“详细信息”窗格中，单击“选项”。

在为项目选择某个操作之前，您可以使用“更多选项”链接查看有关该项目的更多详细信息。该链接将打开包含有关风险的更多信息的“文件智能分析”窗口。

- 6 在“检测到威胁”窗口中，选择下列选项之一：

- **还原**：将项目返回到计算机上的原始位置。此选项仅可用于手动隔离的项目。
- **还原并排除此文件**：将项目返回到其原始位置而不修复它，并在将来的扫描中不检测该项目。此选项仅适用于检测到的病毒和非病毒威胁。
- **从历史记录中删除**：从“安全历史记录”日志中删除所选项目。

7 如果选择还原，在“隔离区还原”窗口中，单击“是”。

8 在“浏览文件夹”对话框中，选择要还原文件的文件夹或驱动器，然后单击“确定”。

还原被错误识别为安全风险的文件

默认情况下，Norton 会从您的计算机中删除安全风险并将其隔离。如果您认为某个文件被误删除，可以将该文件从隔离区还原至其原始位置并将其排除在未来的扫描范围以外。

还原隔离区中的文件

注意：只有确信程序安全时，才能从 Norton 扫描中排除该程序。例如，如果其他程序要依赖于某安全风险程序才能运行，您可能会决定将该风险程序保留在计算机上。

1 启动 Norton。

看到“我的 Norton”窗口时，单击“设备安全”旁边的“打开”。

2 在 Norton 主窗口中，单击“安全性”，然后单击“历史记录”。

3 在“安全历史记录”窗口的“显示”下拉菜单下，选择“隔离区”。

4 选择要还原的文件。

5 在“详细信息”窗格中，单击“选项”。

6 在“检测到威胁”窗口中，单击“还原并排除此文件”。

7 在“隔离区还原”窗口中，单击“是”。

8 在“浏览文件夹”对话框中，选择要还原文件的文件夹或驱动器，然后单击“确定”。

提交项目以供 Norton 评估

提交您认为存在安全风险的文件，从而提高 Norton 产品的有效性。Norton 安全响应中心会分析文件，如果文件有风险，则将其添加到将来的防护定义中。

注意：提交的内容中从不包括个人身份信息。

- 1 启动 Norton。
看到“我的 Norton”窗口时，单击“设备安全”旁边的“打开”。
- 2 在 Norton 主窗口中，双击“安全性”，然后单击“历史记录”。
- 3 在“安全历史记录”窗口的“显示”下拉列表中，选择“隔离”类别。
- 4 选择要管理的项目。
- 5 在“详细信息”窗格中，单击“选项”。
在为项目选择某个操作之前，您可以使用“更多选项”链接查看有关该项目的更多详细信息。该链接将打开包含有关风险的更多信息的“文件智能分析”窗口。
- 6 在“检测到威胁”窗口中，单击“提交给诺顿LifeLock”。
- 7 在出现的屏幕中，单击“确定”。

手动隔离项目

- 1 启动 Norton。
看到“我的 Norton”窗口时，单击“设备安全”旁边的“打开”。
- 2 在 Norton 主窗口中，双击“安全性”，然后单击“历史记录”。
- 3 在“安全历史记录”窗口的“显示”下拉列表中，选择“隔离”类别。
- 4 单击“添加到隔离区”。
- 5 在“手动隔离”窗口中，添加要隔离的文件，然后输入描述以供参考。

注意：如果隔离与任何正在运行的进程关联的文件，则这些进程将终止。因此，在将文件添加到隔离区之前，请关闭所有打开的文件和正在运行的进程。

使用 Norton 优化和提高计算机性能

我们非常清楚计算机速度缓慢有多让人沮丧，一个简单的任务似乎永远完不成。一些用户感受到他们的计算机在安装 Norton 之后性能下降。但是实际上 Norton 已进行精简，可在不牺牲性能的情况下提供世界一流的防护。

此外，Norton 还提供了性能管理和优化工具，可以更快地完成日常任务，从而提升了计算机的速度。

加快我的计算机启动速度

许多应用程序配置为在您启动计算机时启动。这也包括了您从不使用、很少使用或者从不知道自己已经安装的程序。在启动计算机时，启动的程序越多，用时越长。您可以使用“**Norton 启动管理器**”禁用或延迟程序的启动，从而让您的启动速度更快。

禁用或延迟启动项

- 1 启动 Norton。
看到“我的 Norton”窗口时，单击“设备安全”旁边的“打开”。
- 2 在 Norton 主窗口中，双击“性能”，然后单击“启动管理器”。
- 3 在“启动管理器”窗口中，执行以下操作：
 - 在“打开/关闭”列中，取消选中您不使用的程序，防止它们在计算机启动时启动。
 - 在“延迟启动”列中，选择您仅希望在启动完成后加载的程序。
- 4 单击“应用”，然后单击“关闭”。

提高程序和文件加载的速度

“优化磁盘”工具可以重新排列随着时间推移分散在计算机中的文件碎片。该工具提高了计算机性能，使您的工作更高效。

运行优化磁盘

- 1 启动 Norton。
看到“我的 Norton”窗口时，单击“设备安全”旁边的“打开”。
- 2 在 Norton 主窗口中，双击“性能”，然后单击“优化磁盘”。
- 3 完成后，单击“关闭”。

删除使计算机运行缓慢的临时文件和文件夹

您每次浏览或下载文件时，计算机都会存储临时文件。即使您不需要保留这些文件，这些文件仍然会随时间累积，导致计算机速度下降。文件清理工具可以消除这些碎片，让计算机运行速度更快。

删除临时文件和文件夹

- 1 启动 Norton。
看到“我的 Norton”窗口时，单击“设备安全”旁边的“打开”。
- 2 在 Norton 主窗口中，双击“性能”，然后单击“文件清理”。
- 3 完成后，单击“关闭”。

优化引导卷

引导卷优化通过将文件碎片重新排列在相邻和连续的簇中来最大限度地增加可用空间。当硬盘的驱动器头在一个位置访问所有文件数据时，将文件读取到内存中的速度会更快。

优化引导卷

- 1 启动 Norton。
看到“我的 Norton”窗口时，单击“设备安全”旁边的“打开”。
- 2 在 Norton 主窗口中，双击“性能”，然后单击“图表”。
- 3 在“图表”窗口中的安全状态图顶部，单击“优化”。

提升我在玩游戏或看电影时的性能

您是否曾经遇到过在玩游戏或看电影到了最紧张的时候，安全软件开始运行，导致屏幕冻结？您可以设置“全屏检测”工具，以便在运行不应中断的程序时进行检测。此时 Norton 将等待，直至该应用程序完成，然后再运行后台任务来为您提供防护。

请确保启用了“全屏检测”

- 1 启动 Norton。
看到“我的 Norton”窗口时，单击“设备安全”旁边的“打开”。
- 2 在 Norton 主窗口中，单击“设置”。
- 3 在“设置”窗口中，单击“管理设置”。
- 4 在“静默模式设置”下的“全屏检测”行中，将开关移到“打开”位置。
- 5 单击“应用”，然后单击“关闭”。

在我使用偏好的应用程序时阻止中断

如果您认为 Norton 降低了您偏好程序的速度，可以使用“安静模式”设置，阻止 Norton 在您使用这些程序时运行。此时 Norton 将等待，直至这些应用程序完成，然后再启动后台任务来为您提供防护。

在“安静模式”下运行我偏好的应用程序

- 1 启动 Norton。
看到“我的 Norton”窗口时，单击“设备安全”旁边的“打开”。
- 2 在 Norton 主窗口中，单击“设置”。
- 3 在“设置”窗口中，单击“管理设置”。
- 4 在“静默模式设置”下的“用户指定程序”行中，单击“配置”。
- 5 在“安静模式程序”窗口中，单击“添加”。
- 6 在“添加程序”对话框中，导航到您的程序。
- 7 选择该文件，单击“打开”，然后单击“确定”。

显示占用资源并拖慢速度的程序

Norton 可监视您的计算机，并在有程序或进程似乎使用了不正常数量的资源时向您发出警报。如果您没有使用这些程序，就可以关闭它们来提升性能。

确定占用资源的进程

- 1 启动 Norton。
看到“我的 Norton”窗口时，单击“设备安全”旁边的“打开”。
- 2 在 Norton 主窗口中，双击“性能”，然后单击“图表”。
- 3 在“图表”窗口的左窗格中，单击“使用率”。
- 4 执行下列操作之一：
 - 要查看 CPU 图，请单击 **CPU** 选项卡。
 - 要查看内存图，请单击“内存”选项卡。
- 5 单击图上的任一时间点以获取资源消耗性进程的列表。
单击进程的名称以在“文件智能分析”窗口中获取有关该进程的更多信息。

运行 Norton 扫描以检查 PC 上的威胁

Norton 会自动更新病毒定义，并定期扫描 PC 以查找一系列威胁。如果您已离线，或者怀疑感染了病毒，则可以手动运行以下扫描：

- **快速扫描**，可分析计算机中最容易受到威胁的区域。
- **全面系统扫描**，可分析整个系统，包括相比于快速扫描检查项更安全的应用程序、文件和运行中进程。

- 自定义扫描，可分析您怀疑存在风险的单个文件、文件夹或驱动器。

注意：安装 Norton 后，首次扫描可能需要一小时或更长时间来分析整个系统。

运行快速扫描、全面系统扫描或自定义扫描

- 1 启动 Norton。

看到“我的 Norton”窗口时，单击“设备安全”旁边的“打开”。

- 2 在 Norton 主窗口中，双击“安全性”，然后单击“扫描”。

- 3 在“扫描”窗口的“扫描和任务”旁边，选择以下项之一：

- “快速扫描” > “开始”
- “全面系统扫描” > “开始”
- “自定义扫描” > “开始”，然后单击“驱动器扫描”、“文件夹扫描”或“文件扫描”旁边的“运行”以导航到要扫描的组件。

- 4 在“结果摘要”窗口中，单击“完成”。

如果有需要注意的项目，请在“检测到的威胁”窗口中查看风险。

全面系统扫描

“全面系统扫描”可对计算机进行彻底扫描以删除病毒和其他安全威胁。它会检查所有引导记录、文件和用户可访问的正在运行的进程。这会对您的电脑进行彻底的扫描，因而需要较长时间。

注意：当您使用管理员权限运行全面系统扫描时，所扫描的文件数要多于不使用管理员权限运行时所扫描的文件数。

运行全面系统扫描

- 1 启动 Norton。

看到“我的 Norton”窗口时，单击“设备安全”旁边的“打开”。

- 2 在 Norton 主窗口中，双击“安全性”，然后单击“扫描”。

- 3 在“扫描”窗口中的“扫描和任务”下，单击“全面系统扫描”。
- 4 单击“开始”。

自定义扫描

有时，可能希望扫描某个特定文件、可移动驱动器、任何计算机驱动器、计算机上的任何文件夹或文件。例如，当您使用可移动介质但怀疑可能存在病毒时，可以扫描该特定磁盘。另外，如果您在电子邮件中收到一个压缩文件，但怀疑存在病毒，可以扫描该单个元素。

扫描单个元素

- 1 启动 Norton。
 - 看到“我的 Norton”窗口时，单击“设备安全”旁边的“打开”。
- 2 在 Norton 主窗口中，双击“安全性”，然后单击“扫描”。
- 3 在“扫描”窗口中的“扫描和任务”下，单击“自定义扫描”。
- 4 单击“开始”。
- 5 在“扫描”窗口中，执行下列操作之一：
 - 要扫描特定驱动器，请单击“驱动器扫描”旁边的“运行”，选择要扫描的驱动器，然后单击“扫描”。
 - 要扫描特定文件夹，请单击“文件夹扫描”旁边的“运行”，选择要扫描的文件夹，然后单击“扫描”。
 - 要扫描特定文件，请单击“文件扫描”旁边的“运行”，选择要扫描的文件，然后单击“添加”。您也可以按 **Ctrl** 并选择多个文件进行扫描。
- 6 在“结果摘要”窗口中，单击“完成”。
 - 如果有任何项目需要注意，则进行查看并采取建议的操作。

Norton Power Eraser 扫描

Norton Power Eraser 是一个功能强大的恶意软件删除工具，可帮助清理难以删除的安全风险。Norton Power Eraser 使用主动的技术，而不是正常的扫描过程；有时存在这样的风险：Norton Power Eraser 会将合法程序标记为要删除。使用 Norton Power Eraser 删除任何文件之前，请仔细查看扫描结果。

下载 Norton Power Eraser 并运行扫描 (Windows 10/8/7)

- 1 下载 [Norton Power Eraser](#)。
- 2 按 **Ctrl + J** 键可在浏览器中打开“下载”窗口，然后双击 **NPE.exe** 文件即可。
 - 如果出现“用户帐户控制”窗口提示，请单击“是”或“继续”。

- 3 阅读授权许可协议，然后单击“同意”。
如果已接受授权许可协议，则系统不会再次提示您。
Norton Power Eraser 会检查并自动下载可用的新版本。
- 4 在 Norton Power Eraser 窗口中，选择“全面系统扫描”，然后单击“立即运行”。
- 5 如果要包括 Rootkit 扫描，请单击“设置”，在“扫描和日志设置”下，切换至“包括 Rootkit 扫描 (需要重新启动电脑)”选项，然后单击“应用”。
- 6 系统提示重新启动电脑时，单击“重新启动”。
等待扫描完成。按照屏幕上的说明操作。

下载 Norton Power Eraser 并行扫描 (Windows XP/Vista)

- 1 下载 [Norton Power Eraser](#)。
- 2 按 **Ctrl + J** 键可在浏览器中打开“下载”窗口，然后双击 **NPE.exe** 文件即可。
如果出现“用户帐户控制”窗口提示，请单击“是”或“继续”。
- 3 阅读授权许可协议，然后单击“接受”。
Norton Power Eraser 会检查并提示下载可用的新版本。
- 4 在 **Norton Power Eraser** 窗口中，单击“扫描风险”图标。
- 5 默认情况下，Norton Power Eraser 会执行 Rootkit 扫描，并要求重新启动系统。系统提示重新启动电脑时，单击“重新启动”。
如果不想包括 Rootkit 扫描，请转至“设置”，然后取消选中“包括 Rootkit 扫描 (需要重新启动电脑)”选项。
- 6 等待扫描完成。按照屏幕上的说明操作。

创建自己的自定义 Norton 扫描

虽然默认的 Norton 自动扫描设置非常适合大多数用户，但是有些用户可能希望自定义选项，以便按他们选择的计划扫描特定的驱动器、文件夹或文件。

创建自定义扫描

- 1 启动 Norton。
看到“我的 Norton”窗口时，单击“设备安全”旁边的“打开”。
- 2 在 Norton 主窗口中，双击“安全性”，然后单击“扫描”。
- 3 在“扫描”窗口中的“扫描和任务”下，单击“自定义扫描”，然后单击“开始”。
- 4 在“扫描”窗口中，单击“创建扫描”。

- 5 在“新建扫描”窗口中的“扫描名称”旁边，键入自定义扫描的名称并添加设置，如下所示：
 - 在“扫描项目”选项卡上，单击“添加驱动器”、“添加文件夹”或“添加文件”以导航到要包括在扫描中的组件。
 - 在“调度扫描”选项卡上的“您希望扫描何时运行”下，选择时间间隔，然后选择时间安排选项。

在“运行扫描”下，从选项中进行选择。对于大多数用户，最好选中所有框。这可确保扫描仅在您未使用计算机或者您未使用电池供电时运行，而且可防止在扫描期间计算机进入睡眠状态。
 - 在“扫描选项”选项卡上，移动开关以自定义扫描期间压缩文件或低风险威胁的行为。
- 6 单击“保存”。

编辑或删除 Norton 自定义扫描

可以编辑您创建的自定义扫描，重命名扫描、添加或删除文件或者更改计划。如果您不再需要运行扫描，则可以将其删除。

编辑或删除自定义扫描

- 1 启动 Norton。

看到“我的 Norton”窗口时，单击“设备安全”旁边的“打开”。
- 2 在 Norton 主窗口中，双击“安全性”，然后单击“扫描”。
- 3 在“扫描”窗口中的“扫描和任务”下，单击“自定义扫描”，然后单击“开始”。
- 4 在“扫描”窗口的“编辑扫描”列中，在要修改的自定义扫描旁边，执行以下操作之一：
 - 单击编辑图标，然后在“编辑扫描”窗口中，移动开关以打开或关闭扫描选项。对于大多数用户，默认设置效果良好。单击“使用默认值”以删除自定义设置。
 - 单击垃圾桶图标，然后单击“是”以确认要删除自定义扫描。
- 5 单击“保存”。

调度 Norton 扫描

Norton 会检测到您离开计算机的情况，然后自动运行扫描以确保定期监控系统中的威胁。您也可以调度自己的快速扫描、全面系统扫描或自定义扫描，使其按您选择的时间运行。

调度 Norton 快速扫描、全面系统扫描或自定义扫描

- 1 启动 Norton。
看到“我的 Norton”窗口时，单击“设备安全”旁边的“打开”。
- 2 在 Norton 主窗口中，双击“安全性”，然后单击“扫描”。
- 3 在“扫描”窗口中的“扫描和任务”下，单击“自定义扫描”。
- 4 单击“开始”。
- 5 在“扫描”窗口的“编辑扫描”列中，单击快速扫描、全面系统扫描或您之前创建的自定义扫描旁边的编辑图标。
- 6 在“编辑扫描”窗口的“扫描日程表”选项卡上：
 - 在“您希望扫描何时运行”下，选择时间间隔，然后选择时间安排选项。
 - 在“运行扫描”下，从选项中进行选择。对于大多数用户，最好选中所有框。这可确保扫描仅在您未使用计算机或者您未使用电池供电时运行，而且可防止在扫描期间计算机进入睡眠状态。
- 7 单击“下一步”。
- 8 在“扫描选项”窗口中，单击“保存”。

查看 Norton SONAR 检测到的实时威胁

SONAR 提供实时威胁防护并主动检测未知安全风险。SONAR 根据应用程序的行为识别新出现的威胁，比基于特征的传统型威胁检测方法速度更快。它有助于抵御恶意代码，即使尚未通过 LiveUpdate 提供病毒定义。

注意：SONAR 防护应时刻保持打开状态。如果关闭“自动防护”，也会禁用“SONAR 防护”，从而您的计算机将无法抵御新出现的威胁。

查看 SONAR 检测到的风险

- 1 启动 Norton。
看到“我的 Norton”窗口时，单击“设备安全”旁边的“打开”。
- 2 在 Norton 主窗口中，双击“安全性”，然后单击“历史记录”。
- 3 在“安全历史记录”窗口的下拉列表中，选择“SONAR 活动”。

- 4 在列表中选择一個風險（如果顯示風險）。
- 5 請遵循“詳細信息”窗格中的“建議操作”。

此類別還列出修改您的電腦配置或設置的所有活動。此類別的“更多詳細信息”選項提供了有關此活動影響的資源的詳細信息。

確保 SONAR 防護已打開

- 1 啟動 Norton。
看到“我的 Norton”窗口時，单击“设备安全”旁边的“打开”。
- 2 在 Norton 主窗口中，单击“设置”。
- 3 在“设置”窗口中，单击“防病毒”。
- 4 在“自动防护”选项卡的“实时防护”下，将“SONAR 防护”开关移到“打开”。
- 5 单击“应用”。
- 6 在“设置”窗口中，单击“关闭”。

从 Norton 自动防护、SONAR 和下载智能分析扫描中排除文件和文件夹

您可以將 Norton 配置為從自動防護掃描以及 SONAR 掃描中排除某些程序。您可以使用“掃描排除”窗口和“實時排除”窗口將病毒以及其他高風險的安全威脅從掃描中排除。當您將某一文件或文件夾添加到排除列表中時，Norton 在掃描安全風險時會忽略該文件或文件夾。

要從下載智能分析中排除文件，必須選擇一個文件夾並將文件下載到所選文件夾。例如，當您將不安全的可執行文件下載到此文件夾時，Norton 允許您下載該文件且不會將其從計算機中刪除。必須專門為下載智能分析排除文件創建一個新的文件夾。

注意：從 Norton 掃描中排除文件會降低計算機的防護級別，應只在有特定需要時使用。僅當您確信項目沒有受到感染時才排除這些項目。

從掃描中排除高風險安全威脅

- 1 啟動 Norton。
看到“我的 Norton”窗口時，单击“设备安全”旁边的“打开”。
- 2 在 Norton 主窗口中，单击“设置”。
- 3 在“设置”窗口中，单击“防病毒”。
- 4 在“防病毒”設置窗口中，单击“掃描和風險”選項卡。
- 5 在“排除/低風險”下，執行以下操作之一：

- 在“要从扫描排除的项目”行中，单击“配置”。
 - 在“要从自动防护、脚本控制、SONAR 和下载智能分析检测排除的项目”行中，单击“配置”。
- 6 在出现的窗口中，单击“添加文件夹”或“添加文件”。
- 您可以指定排除本地驱动器、文件夹、文件组、单个文件或网络驱动器。但是，Norton 不支持排除网络上的文件。如果向排除列表添加网络驱动器，请确保驱动器连接到您的计算机。
- 7 在“添加项目”对话框中，单击浏览图标。
 - 8 在出现的对话框中，选择要从扫描中排除的项目。
- 添加文件夹时，可以指定是包括还是排除子文件夹。
- 9 单击“确定”。
 - 10 在“添加项目”对话框中，单击“确定”。
 - 11 在出现的窗口中，单击“应用”，然后单击“确定”。

从 Norton 扫描中排除具有低风险特征的文件

Norton 特征排除允许您选择要从 Norton 扫描中排除的特定的已知安全风险。例如，如果某合法应用程序（如免费游戏）依赖于另一个程序（如广告软件）来运行，则您可能会决定保留该广告软件，即使它会让您面临风险。您还可能会决定在以后的扫描中不接收有关该风险程序的通知。

注意：排除会降低对您的保护，因此，仅当您具有特定需要且完全了解从 Norton 扫描中排除已知威胁的潜在风险时才应使用。

将低风险特征添加到“特征排除”

- 1 启动 Norton。
- 看到“我的 Norton”窗口时，单击“设备安全”旁边的“打开”。
- 2 在 Norton 主窗口中，单击“设置”。
 - 3 在“设置”窗口中，单击“防病毒”。
 - 4 在“防病毒”设置窗口中，单击“扫描和风险”选项卡。
 - 5 在“排除/低风险”下的“从所有检测排除的特征”行中，单击“配置”。
 - 6 在“特征排除”窗口中，单击“添加”。

- 7 在“安全风险”窗口中，单击要排除的安全风险，然后单击“添加”。
- 8 在“特征排除”窗口中，单击“应用”，然后单击“确定”。

打开或关闭自动任务

Norton 会运行自动任务，因为它以静默方式工作来保护您的计算机。这些自动任务包括病毒扫描、监控 Internet 连接、下载防护更新以及其他重要任务。当您的计算机打开时，将在后台运行这些活动。

如果有任何项目需要您注意，Norton 会显示一条消息，包含当前状态的信息或提示您执行某些操作。如果您未看到任何消息，则说明计算机处于保护状态。

您也可以随时打开 Norton 以快速查看计算机的状态或查看防护详细信息。

当后台活动正在进行时，Norton 会在位于任务栏最右侧的通知区域发出一条消息来通知您。您可以在下次打开 Norton 主窗口时看到最新活动的结果。

打开或关闭自动任务

- 1 启动 Norton。
看到“我的 Norton”窗口时，单击“设备安全”旁边的“打开”。
- 2 在 Norton 主窗口中，单击“设置”。
- 3 在“设置”窗口中，单击“任务调度”。
- 4 在“任务调度”窗口中的“自动任务”选项卡上，执行下列操作：
 - 选中要自动运行的功能。
选中“任务”复选框可一次性选中所有功能。
 - 取消选中不希望自动运行的功能。
取消选中“任务”复选框可一次性取消选中所有功能。
- 5 单击“应用”，然后单击“关闭”。

运行自定义任务

Norton 会自动检查系统并选择最佳设置来保持系统的安全。但是，您可以运行某些特定任务。可以使用“自定义任务”窗口中提供的选项来选择要运行的特定任务。

您可以选择自己的任务组合来执行一次性扫描。可以运行 LiveUpdate、备份数据、清除浏览历史记录、通过清理磁盘杂乱文件释放磁盘空间以及优化磁盘。

运行自定义任务

- 1 启动 Norton。
看到“我的 Norton”窗口时，单击“设备安全”旁边的“打开”。
- 2 在 Norton 主窗口中，双击“安全性”，然后单击“扫描”。
- 3 在“扫描”窗口中的“扫描和任务”下，单击“自定义任务”，然后单击“开始”。
- 4 在“自定义任务”窗口中，选中要运行的任务。
要选择所有任务，请选中“任务”。
- 5 单击“开始”。

调度安全与性能扫描

使用“任务调度”设置可让 Norton 自动检查系统中的安全与性能问题。您可以指定需要 Norton 执行这些检查的时间和频率。

您可以选择以下安全和性能扫描调度选项：

自动 (推荐)	<p>只要您的 PC 处于闲置状态，即会检查 PC 是否存在安全与性能问题。</p> <p>此设置可提供最强防护。</p>
每周	<p>每周检查 PC 一次或多次，以确定是否存在安全与性能问题。</p> <p>您可以选择在一周中的某几天和一天中的某个时间来执行扫描。</p>
每月	<p>每月检查一次 PC，以确定是否存在安全与性能问题。</p> <p>您可以选择在一个月中的某一天和一天中的某个时间来执行扫描。</p>
手动调度	<p>对您的 PC 不执行安全或性能调度扫描。</p> <p>如果选择此选项，则应定期对您的 PC 执行安全与性能手动扫描以获得保护。</p>

在计算机闲置时执行重要操作可以最大程度地提高计算机的性能。调度每周或每月扫描并选中“仅在空闲时间运行”选项时，Norton 将在计算机空闲时进行扫描。诺顿 LifeLock 建议您选中“仅在空闲时间运行”以提高计算机的性能。

调度安全与性能扫描

- 1 启动 Norton。

看到“我的 Norton”窗口时，单击“设备安全”旁边的“打开”。

- 2 在 Norton 主窗口中，单击“设置”。

- 3 在“设置”窗口中，单击“任务调度”。

- 4 在“调度”选项卡上，从“调度”下选择一个选项。

如果单击“每周”或“每月”，则必须选择运行自动任务的时间和日期。您还可以指定自动任务仅在 PC 闲置时运行。

- 5 单击“应用”，然后单击“关闭”。

配置数据保护器以阻止影响您计算机的恶意进程

数据保护器可保护您的计算机免受恶意进程的攻击，这些进程会破坏您的计算机、损坏和/或窃取您的数据并将恶意威胁传播到其他正常进程。可使用 Norton 信誉技术将进程标识为安全、恶意或未知。根据您的情况，在进行扫描和保护时，可添加更多文件夹和/或扩展名，也可以排除进程。

警告： 关闭此功能会降低对计算机的保护。因此，我们建议您始终将此功能保持打开状态。不过，如果您希望将其关闭，可暂时关闭，但确保重新将其打开。

关闭或打开数据保护器

- 1 启动 Norton。

看到“我的 Norton”窗口时，单击“设备安全”旁边的“打开”。

- 2 在 Norton 产品主窗口中，单击“设置”>“防病毒”。

- 3 在“防病毒”窗口中，单击“数据保护器”选项卡。

- 4 在“数据保护器”行中，将“打开/关闭”开关移到“打开”或“关闭”。

- 5 在“显示通知”行中，执行下列操作之一：

- 将开关移到“打开”以在每次数据保护器阻止威胁时发出通知。
- 将开关移到“关闭”以禁止显示通知。但是，可以在“安全历史记录”窗口中查看已阻止威胁的详细信息。
要访问“安全历史记录”窗口，请在 Norton 主窗口中双击“安全性”，然后单击“历史记录”>“数据保护器”。

- 6 单击“应用”。
- 7 如果出现提示，请选择在您希望将数据保护器功能关闭之前的持续时间，然后单击“确定”。

添加或编辑受数据保护器保护的文件夹

- 1 启动 Norton。
看到“我的 Norton”窗口时，单击“设备安全”旁边的“打开”。
- 2 在 Norton 产品主窗口中，单击“设置”>“防病毒”。
- 3 在“防病毒”窗口中，单击“数据保护器”选项卡。
- 4 在“数据保护器”行中，将“打开/关闭”开关移到“打开”。
- 5 要添加或编辑文件夹，请执行以下操作：
 - 在“受保护的文件夹”旁边，单击“配置”。
 - 在“受保护的文件夹”窗口中，执行以下操作：
 - 要包括新项目，请单击“添加”。
 - 要更改现有项目，请选择该项目，然后单击“编辑”对其进行修改。

注意：无法编辑预设文件夹。

- 在“添加项目”或“编辑项目”窗口中，浏览并选择文件夹。
 - 单击对应的复选框以包括子文件夹。
 - 单击“确定”。
- 6 单击“应用”，然后单击“确定”。

添加受数据保护器保护的扩展名

- 1 启动 Norton。
看到“我的 Norton”窗口时，单击“设备安全”旁边的“打开”。
- 2 在 Norton 产品主窗口中，单击“设置”>“防病毒”。
- 3 在“防病毒”窗口中，单击“数据保护器”选项卡。
- 4 在“数据保护器”行中，将“打开/关闭”开关移到“打开”。
- 5 要添加扩展名，请执行以下操作：
 - 在“受保护的文件类型”旁边，单击“配置”。

- 在“受保护的文件夹”窗口中，单击“添加”。
- 在“添加项目”窗口中，键入要保护的扩展。例如，如果要保护可执行文件，请在框中键入 .exe。位于计算机上任何位置的所有扩展名为 .exe 的文件都将受到保护。
- 单击“确定”。

6 单击“应用”，然后单击“确定”。

从数据保护器中删除文件夹或扩展名

- 1 启动 Norton。
看到“我的 Norton”窗口时，单击“设备安全”旁边的“打开”。
- 2 在 Norton 产品主窗口中，单击“设置”>“防病毒”。
- 3 在“防病毒”窗口中，单击“数据保护器”选项卡。
- 4 在“数据保护器”行中，将“打开/关闭”开关移到“打开”。
- 5 在“受保护的文件夹”或“受保护的文件夹类型”旁边，单击“配置”。
- 6 在“受保护的文件夹”或“受保护的文件夹类型”窗口中，选择要删除的项目。

注意：无法删除预设文件夹或扩展名。

- 7 单击“删除”。
- 8 单击“应用”，然后单击“确定”。

在数据保护器排除项中添加或删除进程

- 1 启动 Norton。
看到“我的 Norton”窗口时，单击“设备安全”旁边的“打开”。
- 2 在 Norton 产品主窗口中，单击“设置”>“防病毒”。
- 3 在“防病毒”窗口中，单击“数据保护器”选项卡。
- 4 在“数据保护器”行中，将“打开/关闭”开关移到“打开”。
- 5 在“进程排除项”行中，单击“配置”，然后执行以下操作：
 - 要添加进程作为数据保护器排除项，请单击“添加”，然后选择该进程。
 - 要从数据保护器排除项中删除进程，请单击该进程，然后单击“删除”。
- 6 单击“应用”，然后单击“确定”。

设置 Norton 以删除在企图进行网络钓鱼时可利用的脚本

脚本控制有助于保护您免受作为网络钓鱼电子邮件附件下载或接收的恶意软件的攻击。默认情况下，它可从文件中删除不常见脚本并清理文件^{**}。但是，您可以使用脚本还原原始文件，并配置希望 Norton 如何处理具有嵌入式脚本的文档。

注意： **对于 Chrome、Edge 和 Internet Explorer 浏览器，Windows 10 RS2 及更高版本都支持此功能。

此外，如果 Norton 检测到带有嵌入式脚本的任何不常见行为，它将阻止带有嵌入式脚本的程序运行该脚本。但是，可以配置希望 Norton 如何处理带有嵌入式脚本的程序。

脚本用于使文档具有动态性和交互性。虽然脚本的主要目的是改进文档体验，但网络罪犯可能会利用脚本在您的计算机上暗中安装恶意软件。通常，脚本对文档的功能并不重要，许多软件程序会默认将其禁用。

如果确信某些特定文件不包含恶意内容，则可以设置 Norton 以将这些文件从脚本控制中排除。有关详细信息，请参见第 36 页的“[从 Norton 自动防护、SONAR 和下载智能分析扫描中排除文件和文件夹](#)”。可以通过替换已清理的文件来还原原始文件。只有在确信文件不包含任何恶意内容时，才应排除这些文件。

脚本控制基于文件行为来识别潜在威胁。如果 Norton 在打开具有嵌入式脚本的文档或程序时检测到任何潜在的危险活动，则会阻止应用程序运行该脚本。在打开具有嵌入式脚本的文档或程序时，您可以配置希望 Norton 处理这些脚本的方式。

还原原始文件

- 1 启动 Norton。
看到“我的 Norton”窗口时，在“设备安全”行中，单击“打开”。
- 2 在 Norton 主窗口中，双击“安全性”，然后单击“历史记录”。
- 3 在“安全历史记录”窗口的“显示”下拉列表中，选择“脚本控制”。
- 4 在“脚本控制”视图中，选择要还原的项目。
- 5 在右窗格的“详细信息”下，单击“还原”。
- 6 在“脚本控制还原”窗口中，单击“是”。

- 7 在出现的提示中，选择“是”。
- 8 在“安全历史记录”窗口中，单击“关闭”。

打开或关闭脚本控制

- 1 启动 Norton。
看到“我的 Norton”窗口时，在“设备安全”行中，单击“打开”。
- 2 在 Norton 主窗口中，单击“设置”。
- 3 在“设置”窗口中，单击“防病毒”。
- 4 在“防病毒”设置窗口中，单击“脚本控制”选项卡。
- 5 在“下载文档时删除脚本”行中，将“打开/关闭”开关移至“打开”或“关闭”，然后单击“应用”。

如果关闭脚本控制，请执行下列操作：

- 在“安全请求”窗口中的“选择持续时间”下拉列表中，选择要关闭该选项的持续时间，然后单击“确定”。
- 6 在“打开文档时阻止脚本”行中，将“打开/关闭”开关移至“打开”或“关闭”，然后单击“应用”。

如果关闭脚本控制，请执行下列操作：

- 在“安全请求”窗口中的“选择持续时间”下拉列表中，选择要关闭该选项的持续时间，然后单击“确定”。
- 7 在“设置”窗口中，单击“关闭”。

永久删除所有脚本控制项目

- 1 启动 Norton。
看到“我的 Norton”窗口时，在“设备安全”行中，单击“打开”。
- 2 在 Norton 主窗口中，单击“设置”。
- 3 在“安全历史记录”窗口的“显示”下拉列表中，选择“脚本控制”。
- 4 在“脚本控制”视图中，单击“清除条目”。
- 5 在“清除条目”窗口中，单击“是”。

- 6 在确认对话框中，单击“是”。
- 7 在“安全历史记录”窗口中，单击“关闭”。

配置 Norton 应如何处理具有嵌入式脚本的文档和程序

- 1 启动 Norton。
看到“我的 Norton”窗口时，在“设备安全”行中，单击“打开”。
- 2 在 Norton 主窗口中，单击“设置”。
- 3 在“设置”窗口中，单击“防病毒”。
- 4 在“防病毒”设置窗口中，单击“脚本控制”选项卡。
- 5 在 **Microsoft Office** 行中的“打开文档时阻止脚本”下，单击“配置”。
- 6 在“**Microsoft Office 首选项**”窗口的“操作”下，选择您希望 Norton 针对每个应用程序执行的操作。

相关的选项有：

- 阻止
- 允许
- 询问我

您可以为每个应用程序选择不同的操作。

- 7 在出现的确认窗口中，单击“确定”。
- 8 在“**Microsoft Office 首选项**”窗口中，单击“应用”，然后单击“确定”。
- 9 在“**Adobe 文档**”行中，选择希望 Norton 针对 PDF 文档执行的操作。
- 10 在“阻止具有不常见行为的脚本”行中，选择希望 Norton 对带有嵌入式脚本的程序执行的操作。

相关的选项有：

- 阻止
- 允许

- 询问我

- 11 在“设置”窗口中，单击“应用”，然后单击“关闭”。

详细了解 Norton 脚本控制

脚本用于使文档具有动态性和交互性。此外，还可以通过自动执行某些任务来添加功能。脚本可以包括 ActiveX 控件、加载项、数据连接、宏、链接对象链接和嵌入式 OLE 文件、颜色主题文件等。

脚本控制有助于保护您免受作为网络钓鱼电子邮件附件下载或接收的恶意软件的攻击。

默认情况下，它可从文件中删除不安全脚本并清理文件。但是，您可以使用脚本还原原始文件，并配置希望 Norton 如何处理具有嵌入式脚本的文档。

以下各部分可帮助您配置脚本控制设置。

使用嵌入式脚本还原原始文件

可以通过替换已清理的文件来还原原始文件。只有在确信文件不包含任何恶意内容时，才应还原原始文件。

- 1 启动 Norton。
 - 看到“我的 Norton”窗口时，在“设备安全”行中，单击“打开”。
- 2 在 Norton 主窗口中，双击“安全性”，然后单击“历史记录”。
- 3 在“安全历史记录”窗口的“显示”下拉列表中，选择“脚本控制”。
- 4 在“脚本控制”视图中，选择要还原的活动内容项目。
- 5 在右窗格的“详细信息”下，单击“还原”。
- 6 在“脚本控制还原”窗口中，单击“是”。
- 7 在出现的提示中，选择“是”。
- 8 在“安全历史记录”窗口中，单击“关闭”。

配置 Norton 以处理带有嵌入式脚本的文档和程序

- 1 启动 Norton。
 - 看到“我的 Norton”窗口时，在“设备安全”行中，单击“打开”。
- 2 在 Norton 主窗口中，单击“设置”。
- 3 在“设置”窗口中，单击“防病毒”。
- 4 在“防病毒”设置窗口中，单击“脚本控制”选项卡。
- 5 在 Microsoft Office 行中的“打开文档时阻止脚本”下，单击“配置”。

- 在“**Microsoft Office 首选项**”窗口的“操作”下，选择您希望 Norton 针对每个应用程序执行的操作。

相关的选项有：

- 阻止
- 允许
- 询问我

您可以为每个应用程序选择不同的操作。

- 在出现的确认窗口中，单击“确定”。
- 在“**Microsoft Office 首选项**”窗口中，单击“应用”，然后单击“确定”。
- 在“**Adobe 文档**”行中，选择希望 Norton 针对 PDF 文档执行的操作。
- 在“阻止具有不常见行为的脚本”行中，选择希望 Norton 对带有嵌入式脚本的程序执行的操作。

相关的选项有：

- 阻止
- 允许
- 询问我

- 在“设置”窗口中，单击“应用”，然后单击“关闭”。

关闭脚本控制

注意：关闭脚本控制会削弱防护力度，仅当存在某种特定需求时才应执行此操作。脚本控制通过删除脚本和清理文档增加了一层安全保护。诺顿LifeLock 建议您始终打开脚本控制，因为它可以提供额外的安全保护。

- 启动 Norton。
看到“我的 Norton”窗口时，在“设备安全”行中，单击“打开”。
- 在 Norton 主窗口中，单击“设置”。
- 在“设置”窗口中，单击“防病毒”。
- 在“防病毒”设置窗口中，单击“脚本控制”选项卡。
- 在“下载文档时删除脚本”行中，将“打开/关闭”开关移至“关闭”。
- 在“打开文档时阻止脚本”行中，将“打开/关闭”开关移至“关闭”。

- 7 在“设置”窗口中，单击“应用”。
- 8 在“安全请求”窗口中的“选择持续时间”下拉列表中，选择要关闭该功能的持续时间，然后单击“确定”。
- 9 在“设置”窗口中，单击“关闭”。

保护您的设备免受漏洞利用、黑客和零日攻击的威胁

零日漏洞利用是一种技术，黑客会借助该技术利用程序中的漏洞在您的计算机中执行恶意操作。除了减慢计算机运行速度或致使程序运行失败之外，这些漏洞利用还会将您的个人数据或保密信息公开给黑客。

Norton 产品中的“漏洞利用防护”功能可保护容易受到漏洞利用攻击的应用程序和文件。默认情况下，Norton 的“漏洞利用防护”功能处于打开状态，会通过关闭易受攻击的程序阻止对这些程序的攻击。Norton 会在关闭程序时发送“攻击已阻止”通知并提供指向攻击相关信息的链接。

关闭或打开“漏洞利用防护”

注意：如果关闭“漏洞利用防护”，您的计算机将易受零日漏洞利用和其他漏洞利用的攻击。

- 1 启动 Norton。
看到“我的 Norton”窗口时，单击“设备安全性”旁边的“打开”。
- 2 在 Norton 主窗口中，单击“设置”。
- 3 在“设置”窗口中，单击“漏洞利用防护”。
- 4 在“漏洞利用防护”行中，将“打开/关闭”开关移到“关闭”或“打开”。
- 5 在“设置”窗口中，单击“应用”，然后单击“关闭”。

漏洞利用防护技术

Norton 利用主动漏洞利用防护技术保护您的计算机免遭最新的零日攻击。可以从“设置”窗口中打开或关闭各项技术。默认情况下，所有技术均处于打开状态。

注意：Norton 建议将各项漏洞利用防护技术保持为打开状态，以最大限度地抵御漏洞利用。

漏洞利用防护技术包括：

- **Java 进程防护**
防止远程黑客通过 Java 进程使用恶意代码，仅允许可信 Java 进程运行。

- **结构化异常处理程序覆盖保护**
 抵御结构化异常处理漏洞利用，这种漏洞利用可使用攻击者控制的地址覆盖异常处理程序的指针，进而危及应用程序。
- **堆栈透视检测**
 阻止以下漏洞利用攻击：通过攻击者控制的内存更改堆栈指针，执行其利用返回导向编程 (ROP) 技术编写的攻击代码。
- **数据执行防护强制执行**
 阻止攻击者从您计算机的堆栈或堆内存执行恶意代码。
- **内存布局随机化强制执行**
 强制动态加载的应用程序 DLL 或模块始终加载到随机位置，以保护它们免受攻击。
- **Heap Spray 防护**
 保护常用作攻击目标的内存位置，漏洞利用或攻击者常在这些位置使用 Heap Spray 攻击技术分配 shellcode。
- **内存布局随机化增强**
 分配应用程序的关键内存位置时改进操作系统的 ASLR（地址空间布局随机化）行为。这可使攻击者难以预测这些内存位置。
- **空页面保护**
 预分配空内存位置，这将有助于防止对空指针解除引用漏洞的攻击。
- **远程 DLL 注入检测**
 防止远程黑客通过外部网络（如公用 IP 地址或域）插入恶意可执行代码。
- **“堆栈执行防护”、“可疑 API 调用检测”和“堆负载检测”技术**可保护您的计算机，使其免遭可绕过地址空间布局随机化和数据执行防护漏洞利用缓解技术的返回导向编程 (ROP) 攻击。

打开或关闭 Norton 防火墙

智能防火墙可监视您的计算机与 Internet 上其他计算机之间的通信，它还可以保护您的计算机，使其不会出现常见的安全问题。如果关闭智能防火墙，您的计算机就无法防御 Internet 威胁和安全风险。

如果您需要关闭智能防火墙，只可将其关闭指定持续时间，之后它会自动重新打开。

打开或关闭 Norton 防火墙

- 1 启动 Norton。
 看到“我的 Norton”窗口时，单击“设备安全”旁边的“打开”。
- 2 在 Norton 主窗口中，单击“设置”。
- 3 在“设置”窗口中，单击“防火墙”。

- 4 在“常规设置”选项卡上的“智能防火墙”行中，将“打开/关闭”开关移到“关闭”或“打开”。
- 5 单击“应用”。
- 6 如果出现提示，请选择在您希望将“防火墙”功能关闭之前的持续时间，然后单击“确定”。

从 Windows 通知区域禁用或启用 Norton 防火墙

- 1 在任务栏上的通知区域中，右键单击 Norton 图标，然后单击“禁用智能防火墙”或“启用智能防火墙”。
- 2 如果出现提示，请选择在您希望将“防火墙”功能关闭之前的持续时间，然后单击“确定”。

自定义程序规则以更改程序的访问设置

在使用 Norton 一段时间之后，您可能需要更改某些程序的访问设置。

自定义“程序规则”

- 1 启动 Norton。
 看到“我的 Norton”窗口时，单击“设备安全”旁边的“打开”。
- 2 在 Norton 主窗口中，单击“设置”。
- 3 在“设置”窗口中，单击“防火墙”。
- 4 在“程序控制”选项卡上的“程序”列中，选择要更改的程序。
- 5 在要更改的程序旁边的下拉列表中，选择希望此程序所具备的访问级别。相关的选项有：

允许	允许此程序的所有访问尝试。
阻止	拒绝此程序的所有访问尝试。
自定义	创建控制该程序访问 Internet 的方式的规则。

- 6 单击“应用”。

更改防火墙规则的顺序

防火墙规则的每个列表都是自上而下进行处理的。您可以通过更改防火墙规则的顺序来调整处理它们的方式。

注意：除非您是高级用户，否则不要更改默认通信规则的顺序。更改默认通信规则的顺序会影响防火墙功能并降低您的计算机的安全性。

更改通信规则的顺序

- 1 启动 Norton。
看到“我的 Norton”窗口时，单击“设备安全”旁边的“打开”。
- 2 在 Norton 主窗口中，单击“设置”。
- 3 在“设置”窗口中，单击“防火墙”。
- 4 在“通信规则”选项卡上，选择要移动的规则。
- 5 执行下列操作之一：
 - 要将此规则向上移动一个位置，请单击“上移”。
 - 要将此规则向下移动一个位置，请单击“下移”。
- 6 移动规则后，单击“应用”。

更改程序规则的顺序

- 1 启动 Norton。
看到“我的 Norton”窗口时，单击“设备安全”旁边的“打开”。
- 2 在 Norton 主窗口中，单击“设置”。
- 3 在“设置”窗口中，单击“防火墙”。
- 4 在“程序控制”选项卡上，选择包含要移动的规则的程序。
- 5 单击“修改”。
- 6 在“规则”窗口中，选择要移动的规则。
- 7 执行下列操作之一：
 - 要将此规则向上移动一个位置，请单击“上移”。
 - 要将此规则向下移动一个位置，请单击“下移”。
- 8 移动规则后，单击“确定”。
- 9 在“防火墙”设置窗口中，单击“应用”。

暂时关闭通信规则

如果想要允许对某计算机或程序进行特定访问，可以暂时关闭通信规则。使用需要更改的程序或计算机后，请务必重新打开该规则。

注意：您无法关闭此列表中显示的某些默认防火墙规则。通过使用“查看”选项，您只能查看这些规则的设置。

暂时关闭通信规则

- 1 启动 Norton。
看到“我的 Norton”窗口时，单击“设备安全”旁边的“打开”。
- 2 在 Norton 主窗口中，单击“设置”。
- 3 在“设置”窗口中，单击“防火墙”。
- 4 在“通信规则”选项卡上，取消选中要关闭的规则旁边的框。
- 5 单击“应用”。

允许阻止的程序访问 Internet

默认情况下，智能防火墙会阻止某些程序访问 Internet。此类程序可能包括某些流媒体程序、网络游戏或老板提供的自定义业务应用程序。如果您知道该程序的 Internet 活动不会对您的安全造成威胁，则可以取消阻止该程序的 Internet 访问。

允许阻止的程序访问 Internet

- 1 启动 Norton。
看到“我的 Norton”窗口时，单击“设备安全”旁边的“打开”。
- 2 在 Norton 主窗口中，单击“设置”。
- 3 在“设置”窗口中，单击“防火墙”。
- 4 在“程序控制”选项卡上，选择要允许访问 Internet 的程序。
- 5 在程序条目对应的“访问”下拉列表中，单击“允许”。
- 6 单击“应用”。

默认情况下，Norton 防火墙自动为首次运行且启用了 Web 的程序配置 Internet 访问设置。当程序首次尝试访问 Internet 时，“自动程序控制”会为其创建规则。

但是，Norton 允许您手动为您的程序配置 Internet 访问设置。

为程序配置 Internet 访问设置

关闭自动程序控制

- 1 启动 Norton。
看到“我的 Norton”窗口时，单击“设备安全”旁边的“打开”。
- 2 在 Norton 主窗口中，单击“设置”。
- 3 在“设置”窗口中，单击“防火墙”。
- 4 在“防火墙”设置窗口中，单击“高级程序控制”。
- 5 在“自动程序控制”行，将“打开/关闭”开关移动到“关闭”。
- 6 在确认窗口中，单击“是”。
- 7 在“设置”窗口中，单击“应用”，然后单击“关闭”。

为程序配置 Internet 访问设置

- 1 启动程序。
当程序尝试访问 Internet 时，Norton 会通过显示防火墙警报来提示您。
- 2 在“防火墙警报”窗口中的“选项”下拉列表中，选择操作。
您可以允许、阻止或手动创建程序规则。
- 3 单击“确定”。

关闭防火墙阻止通知

打开“自动程序控制”时，智能防火墙会自动阻止恶意应用程序以及信誉低的应用程序连接到 Internet 或与网络上的其他计算机通信。

当智能防火墙阻止应用程序连接到网络时，Norton 会通知您。如果您不想看见此通知，可以使用“高级程序控制”将其关闭。

关闭防火墙阻止通知

- 1 启动 Norton。
看到“我的 Norton”窗口时，单击“设备安全”旁边的“打开”。
- 2 在 Norton 主窗口中，单击“设置”。
- 3 在“设置”窗口中，单击“防火墙”。
- 4 在“高级程序控制”选项卡上，将“显示防火墙阻止通知”开关移动到“关闭”。

详细了解“入侵防护”排除列表

如果您确定网络上的某个设备是安全的，则可以将该设备的信任级别更改为“完全信任”。可以使用“网络设置”下的“设备信任”配置设备的信任级别。您可以从“入侵防护”扫描中排除这些受信任设备。从“入侵防护”扫描中排除“完全信任”设备可以节省扫描时间，并且提高电脑的网络速度。当排除一个设置为“完全信任”的设备时，Norton 产品不会扫描从该设备收到的任何信息。系统会将从“入侵防护”扫描中排除的“完全信任”设备添加到“入侵防护”排除列表中。

如果发现从“入侵防护”扫描中排除的任一设备受到感染，可以清除已保存的排除列表。清除排除列表时，Norton 产品会从排除列表中删除所有 IPS 排除的设备。

可以在以下情况下清除已保存的排除列表：

- 从“入侵防护”扫描中排除的任何设备受到感染。
- 从“入侵防护”扫描中排除的任何设备试图感染您的计算机。
- 您的家用网络受到感染。

从“入侵防护”排除列表中删除所有设备

- 1 启动 Norton。
看到“我的 Norton”窗口时，单击“设备安全”旁边的“打开”。
- 2 在 Norton 主窗口中，单击“设置”。
- 3 在“设置”窗口中，单击“防火墙”。
- 4 单击“入侵和浏览器主动防护”选项卡。
- 5 在“入侵防护”下的“排除列表”行中，单击“清除”。
- 6 在确认对话框中，单击“是”。
- 7 在“设置”窗口中，单击“关闭”。

打开浏览器主动防护

恶意网站会检测并利用浏览器的漏洞来下载恶意软件。打开“浏览器主动防护”后，Norton 会在恶意软件可以发动攻击之前就加以阻止。它可帮助保护您的敏感信息并阻止攻击者访问您的计算机。

默认情况下，“浏览器主动防护”处于打开状态。让“浏览器主动防护”处于打开状态，确保抵御恶意网站的威胁。

注意：“浏览器主动防护”功能适用于 Google Chrome、Microsoft Internet Explorer、Mozilla Firefox 和 Microsoft Edge 浏览器。

如何打开“浏览器主动防护”？

为保护您的浏览器免受恶意网站的攻击，默认情况下会打开“浏览器主动防护”功能。但是，如果您出于某种原因将其关闭，也可以重新打开。

打开“浏览器主动防护”

- 1 启动 Norton。
看到“我的 Norton”窗口时，单击“设备安全”旁边的“打开”。
- 2 在 Norton 产品主窗口中，单击“设置”。
- 3 在“设置”窗口中，单击“防火墙”或“网络”。
- 4 单击“入侵和浏览器主动防护”选项卡。
- 5 在“浏览器主动防护”行中，将“打开/关闭”开关移到“打开”。
- 6 单击“应用”。
- 7 在“设置”窗口中，单击“关闭”。

设置 Norton 防火墙以停止或启动阻止攻击时向您发出通知

您可以选择是否要在 Norton 入侵防护阻止可疑的攻击时接收通知。

如果选择不接收通知，仍然可以在安全历史记录中查看 Norton 阻止的攻击。

关闭或打开入侵防护通知

- 1 启动 Norton。
看到“我的 Norton”窗口时，单击“设备安全”旁边的“打开”。
- 2 在 Norton 主窗口中，单击“设置”。
- 3 在“设置”窗口中，单击“防火墙”或“网络”。
- 4 单击“入侵和浏览器主动防护”选项卡。
- 5 在“入侵防护”下的“通知”行中，将“打开/关闭”开关移到“关闭”或“打开”。
- 6 在“设置”窗口中，单击“应用”，然后单击“关闭”。

关闭或打开个别入侵防护通知

- 1 启动 Norton。
看到“我的 Norton”窗口时，单击“设备安全”旁边的“打开”。
- 2 在 Norton 主窗口中，单击“设置”。
- 3 在“设置”窗口中，单击“防火墙”或“网络”。
- 4 单击“入侵和浏览器主动防护”选项卡。
- 5 在“入侵防护”下的“入侵特征”行中，单击“配置”。
- 6 在“入侵特征”窗口中，选中或取消选中对应于每个特征的“通知我”。
- 7 单击“确定”。
- 8 在“入侵特征”窗口中，单击“应用”，然后单击“确定”。
- 9 在“设置”窗口中，单击“关闭”。

关闭或打开 AutoBlock

Norton 自动阻止功能会阻止您网络中的设备与试图对该设备发起漏洞利用攻击的任何其他计算机之间的所有通信。由于可能会包括非恶意通信，因此自动阻止功能在检测到威胁后仅在有限的时间内阻止连接。您可以指定希望 Norton 产品阻止攻击计算机连接的时间段。默认情况下，Norton 产品会阻止您的计算机与攻击计算机进行通信长达 30 分钟。

如果自动阻止功能阻止了您要访问的一台或多台计算机，您可以关闭该功能。

关闭或打开 AutoBlock

- 1 启动 Norton。
看到“我的 Norton”窗口时，单击“设备安全”旁边的“打开”。
- 2 在 Norton 主窗口中，单击“设置”。
- 3 在“设置”窗口中，单击“防火墙”或“网络”。
- 4 单击“入侵和浏览器主动防护”选项卡。
- 5 在“入侵防护”下的“入侵自动阻止”行中，单击“配置”。
- 6 在“入侵自动阻止”窗口中的“自动阻止”下，执行下列操作之一：
 - 要关闭“入侵自动阻止”，请单击“关闭”。
 - 要打开“入侵自动阻止”，请单击“打开（推荐）”，然后在“自动阻止攻击计算机的时间”下拉列表中，选择您希望自动阻止保持打开的时间。

- 7 在“入侵自动阻止”窗口中，单击“确定”。
- 8 在“设置”窗口中，单击“关闭”。

取消阻止 Norton 自动阻止功能已阻止的电脑

如果 Norton 防火墙阻止您确定为安全的计算机的网络通信，您可以通过在 Norton 防火墙设置中从自动阻止列表删除该计算机，恢复该计算机的连接。

取消阻止已自动阻止的计算机

- 1 启动 Norton。
看到“我的 Norton”窗口时，单击“设备安全”旁边的“打开”。
- 2 在 Norton 主窗口中，单击“设置”。
- 3 在“设置”窗口中，单击“防火墙”或“网络”。
- 4 单击“入侵和浏览器主动防护”选项卡。
- 5 在“入侵防护”下的“入侵自动阻止”行中，单击“配置”。
- 6 在“入侵自动阻止”窗口中的“自动阻止当前所阻止的计算机”下，选择该计算机的 IP 地址。
- 7 在“操作”列下，从下拉列表中选择“取消禁止”。
- 8 在“入侵自动阻止”窗口中，单击“确定”。
- 9 在“设置”窗口中，单击“关闭”。

将设备添加到“设备信任”

您可以手动向“设备信任”添加设备。可以通过指定以下内容来添加设备：

- 设备的名称或说明
- 设备的 IP 地址或物理地址

注意：如果信任不在您的网络上的设备，您的计算机会面临潜在的安全风险。

将设备添加到“设备信任”

- 1 启动 Norton。
看到“我的 Norton”窗口时，单击“设备安全”旁边的“打开”。
- 2 在 Norton 主窗口中，单击“设置”。

- 3 在“设置”窗口中，单击“防火墙”。
- 4 在“常规设置”选项卡上的“设备信任”行中，单击“配置”。
- 5 在“设备信任”窗口中，单击“添加”。
- 6 在“添加设备”窗口的“名称”框中，键入要添加到网络中的设备的名称。
 设备名称的最大长度不应超过 15 个字符。
- 7 在“IP 或物理地址”框中，键入要添加到“设备信任”中的设备的 IP 地址或物理地址。
 可以在“IP 或物理地址”框中使用以下格式：

IPv4 地址	172.16.0.0
IPv6 地址	fe80::12ac:fe44:192a:14cc
物理地址	11-22-c3-5a-fe-a4
可解析的主机	ftp.myfiles.com

直到从网络中实际找到设备，才验证您提供的地址。

- 8 从“信任级别”下拉菜单中选择一个选项。相关的选项有：

完全信任	将设备添加到“完全信任”列表中。 对于“完全信任”设备，仅监视其中的已知攻击和感染。仅当您确信设备绝对安全时，才应选择此设置。
受限制	将设备添加到“受限制”列表中。 受限设备无法访问您的计算机。

- 9 如果您希望将此设备从“入侵防护”扫描中排除，请选中“从 IPS 扫描中排除”。
- 10 单击“添加设备”。

关闭或打开“下载智能分析”

“下载智能分析”可帮助您的计算机防御您可能在使用受支持的浏览器下载后运行或执行的任何不安全文件。默认情况下，“下载智能分析”选项处于打开状态。在这种情况下，“下载智能分析”会通知您有关下载的任何可执行文件的信誉级别。“下载智能分析”提供的信誉详细信息指示安装下载的文件是否安全。

有时您可能希望关闭“下载智能分析”。例如，如果您希望下载不安全的文件。在这种情况下，您必须关闭“下载智能分析”，以便 Norton 产品允许您下载该文件，并且不会从计算机中删除它。

您可以使用“下载智能分析”选项关闭或打开“下载智能分析”。

关闭或打开“下载智能分析”

- 1 启动 Norton。
看到“我的 Norton”窗口时，单击“设备安全”旁边的“打开”。
- 2 在 Norton 产品主窗口中，单击“设置”。
- 3 在“设置”窗口中，单击“防火墙”或“网络”。
- 4 单击“入侵和浏览器主动防护”选项卡。
- 5 在“下载智能分析”行中，将“打开/关闭”开关移到“关闭”或“打开”。
- 6 单击“应用”。
- 7 如果出现提示，请选择在您希望将“下载智能分析”功能关闭之前的持续时间，然后单击“确定”。
- 8 在“设置”窗口中，单击“关闭”。

关闭或打开垃圾邮件过滤

随着电子邮件使用量的日益增加，很多用户都会收到大量不需要和未经请求的商业电子邮件（称为垃圾邮件）。垃圾邮件不仅使识别有效电子邮件变得困难，而且一些垃圾邮件还包含不良信息和图像。

要控制这些垃圾邮件，您可以使用垃圾邮件过滤。默认情况下，垃圾邮件防护保持活动状态。如果您由于任何原因想要禁用它，则可以从程序本身中将其关闭。

注意：关闭 Norton AntiSpam 会增加收到未经请求的电子邮件的风险。

关闭或打开垃圾邮件过滤

- 1 启动 Norton。
看到“我的 Norton”窗口时，单击“设备安全性”旁边的“打开”。
- 2 在 Norton 产品主窗口中，单击“设置”。
- 3 在“设置”窗口中，单击“反垃圾邮件”。

- 4 在“过滤器”选项卡的“反垃圾邮件”行中，将“打开/关闭”开关移到“关闭”或“打开”。
- 5 如果关闭垃圾邮件过滤，请执行下列操作：
 - 在“安全请求”窗口中的“选择持续时间”下拉列表中，选择要关闭垃圾邮件过滤的持续时间。
- 6 单击“应用”。
- 7 单击“确定”。
- 8 在“设置”窗口中，单击“关闭”。

定义 Norton 产品的 Internet 使用量

“网络流量感测”允许您控制 Norton 使用的带宽。默认情况下，“网络流量感测”处于打开状态，并设置为“自动”。在 Windows 7 或更早版本中，默认设置为“无限制”。如果 Internet 连接速度缓慢，您可以减少 Norton 使用的带宽。还可以通过更改“网络流量感测”设置来为计算机使用的所有网络连接设置通信策略。

定义 Norton 产品的 Internet 使用量

- 1 启动 Norton。

看到“我的 Norton”窗口时，单击“设备安全”旁边的“打开”。
- 2 在 Norton 主窗口中，单击“设置”。
- 3 在“设置”窗口中，单击“防火墙”。
- 4 在“常规设置”选项卡上的“网络流量感测”行中，单击“配置”。如果“配置”选项已禁用，请将“打开/关闭”开关移到“打开”。
- 5 在“网络流量感测”设置窗口的“策略”列下，单击要为其设置策略的网络连接旁边的下拉列表。
- 6 选择下列各项之一：
 - “自动”允许 Norton 根据 Windows 流量感测策略接收全部产品和病毒定义更新。

注意：只有 Windows 8 或更高版本才会提供“自动”选项。

- “无限制”允许 Norton 使用所需的网络带宽接收全部产品和病毒定义更新。如果使用 Windows 7 或更早版本，则默认策略为“无限制”。

- “经济”仅允许 Norton 访问 Internet 来接收关键产品更新和病毒定义。如果您的 Internet 连接有限制，则“经济”可确保您抵御严重安全威胁。
 - “无通信”阻止 Norton 连接到 Internet。如果选择此策略，Norton 将无法接收关键病毒定义和程序更新，这会导致计算机遭受潜在危险和病毒攻击。
- 7 单击“应用”，然后单击“确定”。
 - 8 在“设置”窗口中，单击“关闭”。

关闭或打开“网络流量感测”

可以设置策略来限制 Norton 的 Internet 使用量。如果不想限制 Norton 产品的 Internet 使用量，可以关闭“网络流量感测”。

如果您认为 Norton 占用了过多的网络带宽，则可以打开“网络流量感测”。然后，可以设置策略来限制 Norton 的 Internet 使用量。Norton 产品根据您在“网络流量感测”设置窗口中设置的策略连接到 Internet。默认情况下，“网络流量感测”处于打开状态。

关闭或打开“网络流量感测”

- 1 启动 Norton。
看到“我的 Norton”窗口时，单击“设备安全”旁边的“打开”。
- 2 在 Norton 主窗口中，单击“设置”。
- 3 在“设置”窗口中，单击“防火墙”。
如果您安装了 Norton AntiVirus，请单击“网络”。
- 4 在“常规设置”选项卡上的“网络流量感测”行中，将“打开/关闭”开关移到“关闭”或“打开”。
- 5 在“设置”窗口中，单击“应用”，然后单击“关闭”。

设置 Norton 以监控应用程序并阻止恶意网站访问您的计算机

当您安装或打开任何免费软件或共享软件应用程序时，一些恶意网站可能会尝试以未经授权的方式访问您的设备信息。恶意网站会检测并利用漏洞下载恶意软件，比如可将您的设备信息泄露给网络罪犯的 **crypto mining** 恶意软件。

当“应用程序 URL 监控”处于打开状态时，Norton 会监控您的计算机上安装的所有应用程序并阻止恶意网站访问您的计算机。Norton 在阻止某个恶意网站时会向您发送警报，而且您可以通过“安全历史记录”窗口查看有关攻击的信息。

注意：“应用程序 URL 监控”不监控浏览器应用程序。为防止您的浏览器应用程序遭受恶意网站攻击，您需要添加 Norton 浏览器扩展。

打开“应用程序 URL 监控”以阻止恶意网站

默认情况下，“应用程序 URL 监控”处于打开状态。让“应用程序 URL 监控”处于打开状态，确保抵御恶意网站的威胁。

- 1 启动 Norton。
看到“我的 Norton”窗口时，单击“设备安全”旁边的“打开”。
- 2 在 Norton 主窗口中，单击“设置”。
- 3 在“设置”窗口中，单击“防火墙”或“网络”。
- 4 单击“入侵和浏览器主动防护”选项卡。
- 5 在“入侵防护”下的“应用程序 URL 监控”行中，将“打开/关闭”开关移动到“打开”。

从监控中排除 URL 或域

“入侵防护”功能使用一个包含大量攻击特征的列表来检测和阻止可疑的网站。在某些情况下，良性网站会被识为可疑活动，因为它们具有类似的攻击特征。如果您收到有关可能攻击的通知，但是您知道触发通知的网站或域是安全的，则可以从监控中排除该特征。

从警报通知中排除 URL 或域

- 1 出现警报通知时，单击“查看详细信息”。
- 2 在“安全历史记录 - 高级详细信息”窗口中，单击“取消阻止 URL”。

使用您的 Norton 排除 URL 或域

- 1 启动 Norton。
看到“我的 Norton”窗口时，单击“设备安全”旁边的“打开”。
- 2 在 Norton 主窗口中，单击“设置”。
- 3 在“设置”窗口中，单击“防火墙”或“网络”。
- 4 单击“入侵和浏览器主动防护”选项卡。
- 5 在“入侵防护”下的“应用程序 URL 监控排除”行中，单击“配置”。
- 6 单击“添加”按钮并输入要从监控中排除的 URL 或域名。
- 7 如果要编辑或删除 URL 或域，请执行以下操作：
 - 从列表中选择要删除的 URL 或域，然后单击“编辑”按钮。修改 URL 或域名。

- 选择要删除的 URL 或域，然后单击“删除”按钮。

查看有关被阻止 URL 的信息

查看警报通知中的信息

- 1 出现警报通知时，单击“查看详细信息”。
- 2 在“安全历史记录 - 高级详细信息”窗口中，可以查看有关被阻止 URL 的更多详细信息。

在“安全历史记录”窗口中查看信息

- 1 启动 Norton。
看到“我的 Norton”窗口时，单击“设备安全”旁边的“打开”。
- 2 在 Norton 产品主窗口中，双击“安全”，然后单击“历史记录”。
- 3 在“安全历史记录”窗口的“显示”下拉列表中，选择“入侵防护”。
- 4 单击某行可查看该项目的详细信息。
- 5 双击行或单击“更多选项”打开“安全历史记录高级详细信息”以查看有关活动的更多详细信息并在需要时对活动执行操作。

开始使用诺顿云备份

云备份负责存储和保护重要的文件和文档，作为一种预防性措施，可防止硬盘驱动器故障、设备被盗甚至勒索软件引起的数据丢失。

注意：诺顿云备份只能在 Windows 上使用。

在运行诺顿云备份之前，请创建一个用于指定要备份的文件的备份集。此外，您还可以指定文件的备份位置以及备份的运行时间。您可以使用诺顿云备份将文件备份到云，也可以备份到自己的外部驱动器。

注意：首次运行备份时，Norton 可能需要一些时间来检查并复制计算机上的所有文件。如果 Internet 连接速度较慢，则此过程可能需要更长时间。

如果备份目标是本地备份，则 Norton 不会自动备份文件。备份到本地存储设备需要您的干预。

创建备份集

- 1 启动 Norton。
看到“我的 Norton”窗口时，单击“设备安全”旁边的“打开”。
- 2 在 Norton 主窗口中，双击“备份”，然后单击“备份集”。

- 3 在“备份设置”窗口中，单击“创建新集”。
- 4 在出现的窗口中，键入备份集的名称，然后单击“确定”。
- 5 在“内容”选项卡中的“文件类型”下，打开要备份的一个或多个文件类别。
- 6 在“位置”选项卡中的“目标”列中，选择“安全云存储”。
如果尚未激活云备份，请单击“免费激活”链接，然后按照说明进行操作。
- 7 在“时间”选项卡上，使用“调度”列表选择最符合需求的备份计划。
- 8 单击“保存设置”。

运行诺顿云备份

注意：首次运行备份时，Norton 可能会提示您输入帐户凭据进行身份验证。

- 1 启动 Norton。
看到“我的 Norton”窗口时，单击“设备安全”旁边的“打开”。
- 2 在 Norton 主窗口中，双击“备份”，然后单击“运行备份”。
- 3 在“运行备份”窗口中，按照屏幕上的说明操作。
- 4 单击“关闭”。

注意：如果备份未完成，Norton 会建议可能的原因，如存储容量不足或速度限制。运行备份时始终检查是否连接到 Internet，以及是否连接并打开了存储设备。

在备份集中添加或排除文件和文件夹

Norton 支持将不同的文件类型（如图片、音乐或视频文件）备份到备份集。可以指定包含备份集中通常所含文件类型的文件或文件夹，然后从备份中将其排除。

也可以添加或删除通常为默认文件类型一部分的文件扩展名。有关详细信息，请参见第 65 页的“查看或更改 Norton 包括在备份中的默认文件类型或文件扩展名”。

在备份集中添加或排除文件和文件夹

- 1 启动 Norton。
看到“我的 Norton”窗口时，单击“设备安全”旁边的“打开”。
- 2 在 Norton 主窗口中，双击“备份”，然后单击“备份集”。
- 3 在“备份设置”窗口中的“备份集”下拉列表中，选择要配置的备份集。

- 4 在“内容”选项卡上，单击“添加或排除文件或文件夹”。
- 5 在出现的窗口中，执行以下操作：
 - 要将文件添加到备份集中，请单击“包含文件”，然后导航到要添加的文件。
 - 要将文件夹添加到备份集中，请单击“包含文件夹”，然后导航到要添加的文件夹。
 - 要从备份集中删除文件，请单击“排除文件”，然后导航到要删除的文件。
 - 要从备份集中删除文件夹，请单击“排除文件夹”，然后导航到要删除的文件夹。
- 6 在“备份设置”窗口中，单击“保存设置”。

注意：也可以右键单击文件或文件夹，然后从快捷菜单中选择 **Norton Security** > “添加到备份/从备份中排除”。

仅在配置备份并关闭了“备份设置”和“还原文件”窗口后，“添加到备份”和“从备份中排除”选项才会出现在快捷菜单中。

查看或更改 Norton 包括在备份中的默认文件类型或文件扩展名

默认情况下，Norton 备份在运行备份之前查找属于特定文件类型（如图片、音乐或视频）的文件。默认文件类型可确保，在创建备份集并运行备份后，会立即自动备份大多数用户认为重要的数据。如果要在备份中包括或排除数据，则可以更改备份文件类型默认值或者每种文件类型中包括的扩展名。

查看或更改包括在备份中的默认文件类型或文件扩展名

- 1 启动 Norton。
 - 看到“我的 Norton”窗口时，单击“设备安全”旁边的“打开”。
- 2 在 Norton 主窗口中，双击“备份”，然后单击“备份集”。
- 3 在“备份设置”窗口中的“备份集”下拉列表中，选择要配置的备份集。
- 4 在“内容”选项卡上，选中“编辑文件类型”以更改图片、音乐、视频文件类型和其他文件类型中包括的扩展名。
- 5 在“文件类型”下，单击文件类型旁边的“配置”。
- 6 在出现的窗口中，执行以下操作，然后单击“保存”。
 - 要删除文件扩展名，请在列表中选择文件扩展名，然后单击“删除”。
 - 要将其他扩展名添加到列表中，请单击“新增”。
- 7 在“备份设置”窗口中，单击“保存设置”。

从 Norton 备份集还原图片、音乐或其他重要文件

如果您是勒索软件或其他恶意软件的受害者，或者遇到无法恢复的硬件问题，则可以轻松还原 Norton 备份数据。您可以选择还原整个备份集或备份集中的特定文件。您还可以确定还原备份文件的位置。

注意：根据配置的备份集进行还原。如果还原到新设备，Norton 可能不会根据旧设备的所需文件夹结构还原文件。

还原 Norton 备份文件或整个备份集

- 1 启动 Norton。
看到“我的 Norton”窗口时，单击“设备安全”旁边的“打开”。
- 2 在 Norton 主窗口中，双击“备份”，然后单击“还原文件”。
- 3 在“还原文件”窗口中的“还原源位置”下，单击“查看全部”。
单击备份集，然后单击“确定”。
- 4 在“还原文件”窗口中的“文件”下，单击“浏览文件和文件夹”。
选择要还原的文件，然后单击“确定”。
- 5 在“还原文件”窗口中的“还原目标位置”下，单击“原始位置”。
如果不希望还原到原始位置，请单击“更改”并按照说明操作。
- 6 单击“还原文件”，然后单击“关闭”。

从云备份下载文件

- 1 转到 <https://my.Norton.com>。
- 2 单击“登录”。
- 3 输入诺顿LifeLock 帐户电子邮件地址和密码，然后单击“登录”。
- 4 在“我的 Norton”页面中的“云备份”磁贴中，单击“查看备份集”。
- 5 选择包含要下载的文件备份集。
- 6 导航到要下载的文件。
如果知道文件名，则可以使用搜索功能来搜索特定文件。
使用“过滤器”选项可以过滤出图片和文档。
- 7 将鼠标指针移到文件名上，然后单击“下载”。

从云备份中删除备份集和文件

如果不再需要某个备份集，可将其删除。如果只有一个备份集，则无法删除该备份集。不过，您可以先创建新的备份集，然后再删除旧备份集。

注意：有时，后端服务中断或服务器维护会阻止您删除备份数据。在此类情况下，请尝试稍后删除。要确定服务是否中断，请查看 [Norton 服务状态](#) 页面。

删除某个备份集后，该备份集中所包含文件的备份详细信息也会发生更改。例如，图标将重叠并且文件属性中的“备份”选项卡不再显示。

如果您想释放安全云存储上的一些空间，则删除备份集尤其有用。

注意：要从云备份中删除某个备份集，必须将“防火墙设置”窗口中的“网络流量感测”选项设置为“无限制”。

有关详细信息，请参见第 60 页的[“定义 Norton 产品的 Internet 使用量”](#)。

删除备份集

- 1 启动 Norton。
 - 看到“我的 Norton”窗口时，单击“设备安全”旁边的“打开”。
- 2 在 Norton 主窗口中，双击“备份”，然后单击“备份集”。
- 3 在“备份设置”窗口的“备份集”下拉列表中，选择要删除的备份集。
- 4 单击“删除”。
- 5 在“删除备份集”窗口中，执行以下操作之一：
 - 要删除当前备份集，请选择“删除备份集”。
 - 要删除当前备份集并清除已备份的文件，请选择“删除备份集和文件”。
- 6 单击“是”。

从帐户中删除备份集

- 1 登录您的帐户。
- 2 在“我的 Norton”页面中的“云备份”下，单击“查看备份集”。

此时将显示正在使用的现有备份集。

- 3 要删除备份集，请单击要删除的备份集的垃圾桶图标。
- 4 在“删除备份集”确认窗口中，单击“删除”。
单击“取消”可显示备份页面而不删除备份集。

自定义 Norton 产品设置

在“设置”窗口中，您可以打开或关闭以下“快速控制”服务：

- 静默模式
- 备份
- 备份状态覆盖
- 自动 LiveUpdate 更新
- 智能防火墙
- Norton 篡改防护

除“静默模式”外，应将所有其他服务保持打开状态。

打开或关闭“快速控制”服务

- 1 启动 Norton。
看到“我的 Norton”窗口时，单击“设备安全性”旁边的“打开”。
- 2 在 Norton 主窗口中，单击“设置”。
- 3 在“设置”窗口中的“快速控制”下，执行下列操作之一：
 - 要打开某项服务，请选中它所对应的复选框。
 - 要关闭某项服务，请取消选中它所对应的复选框。
如果显示警报或消息，请从下拉菜单中选择持续时间，然后单击“确定”。

自定义“实时防护”设置

“实时防护”可检查计算机上的未知安全风险并让您确定对所发现风险采取的操作。

注意：建议大多数用户使用默认设置。如果要暂时关闭功能，请尽快重新打开。如果要自动删除低风险项目，请配置“SONAR 高级模式”。自动防护会在每次您运行计算机上的程序时检查病毒和其他安全风险。使“自动防护”始终处于打开状态。

设置“自动防护”以扫描可移动介质

在您访问可移动介质时检查引导型病毒。对可移动介质进行引导型病毒扫描后，如果该介质未重新插入或格式化，就不会再次进行扫描。如果仍怀疑可移动介质感染了引导型病毒，请确保打开“自动防护”以重新扫描该可移动介质。然后，插入该可移动介质，并从“我的电脑”打开它以便“自动防护”重新对其进行扫描。也可以进行手动扫描，以验证可移动介质是否受到感染。

自定义“自动防护”设置

- 1 启动 Norton。
看到“我的 Norton”窗口时，单击“设备安全”旁边的“打开”。
- 2 在 Norton 主窗口中，单击“设置”。
- 3 在“设置”窗口中，单击“防病毒”。
- 4 在“可移动介质扫描”下，将滑块设置为“打开”。

设置 SONAR 以自动删除威胁

SONAR 在您的计算机上提供实时威胁防护并主动检测未知安全风险。SONAR 基于应用程序的行为来识别新出现的威胁。您可以配置 SONAR 如何使用“SONAR 高级模式”设置删除威胁。

设置 SONAR 以自动删除威胁

- 1 启动 Norton。
看到“我的 Norton”窗口时，单击“设备安全”旁边的“打开”。
- 2 在 Norton 主窗口中，单击“设置”。
- 3 在“设置”窗口中，单击“防病毒”。
- 4 在“自动删除风险”下，将滑块设置为“始终”。
- 5 在“在我离开时删除风险”下，将滑块设置为“始终”。
- 6 单击“应用”。

设置“自动防护”以从 Norton 扫描中排除已知的正常文件

如果认为 Norton 将有效应用程序标识为安全风险，可以从 Norton 扫描中排除该文件。

从 Norton 扫描中排除文件

- 1 启动 Norton。
看到“我的 Norton”窗口时，单击“设备安全”旁边的“打开”。
- 2 在 Norton 主窗口中，单击“设置”。

- 3 在“设置”窗口中，单击“防病毒”。
- 4 在“防病毒”设置窗口中，单击“扫描和风险”选项卡。
- 5 在“排除/低风险”下，执行以下操作之一：
 - 在“要从扫描排除的项目”行中，单击“配置”。
 - 在“要从自动防护、SONAR 和下载智能分析检测排除的项目”行中，单击“配置”。
- 6 在出现的窗口中，单击“添加文件夹”或“添加文件”。
- 7 在“添加项目”对话框中，单击浏览图标。在出现的对话框中，选择要从扫描中排除的项目。
- 8 单击“确定”。

详细了解“扫描和风险”设置

“扫描和风险”设置允许您自定义 Norton 在计算机上执行的扫描。您可以根据计算机上文件的数字签名和信任级别来配置扫描。您可以定义 Norton 在扫描电子邮件时应如何操作。

可以使用以下“扫描和风险”设置：

计算机扫描

您可以运行不同类型的扫描，以检测和阻止计算机上的任何病毒感染。这些扫描包括快速扫描、全面系统扫描和自定义扫描。您可以使用各种“计算机扫描”选项来自定义 Norton 在计算机上执行的扫描。您还可以指定对压缩文件进行的扫描。

使用“计算机扫描”选项，您还可以指定扫描操作检测 Rootkit、其他隐藏项目、跟踪 Cookie 和未知安全威胁。相关的选项有：

- **压缩文件扫描**
扫描并修复压缩文件中包含的文件。
打开此功能时，Norton 会扫描并检测压缩文件中包含的文件中的病毒和其他安全风险，并会删除压缩文件。
- **Rootkit 和隐藏项目扫描**
扫描可能隐藏在电脑上的 Rootkit 和其他安全风险。
- **网络驱动器扫描**
扫描连接到您计算机的网络驱动器。
在“全面系统扫描”和“自定义扫描”过程中，Norton 会执行“网络驱动器扫描”。默认情况下，“网络驱动器扫描”选项处于打开状态。如果关闭此选项，Norton 将不会扫描网络驱动器。
- **启发式防护**

扫描电脑，以抵御未知安全威胁。

Norton 使用启发式技术检查文件的可疑特征以将该文件分类为受感染的文件。它将文件的特征与已知受感染的文件进行比较。如果该文件具有足够的可疑特征，则 Norton 将该文件识别为包含威胁的受感染的文件。

- **跟踪 Cookie 扫描**

扫描程序可能放在您的电脑上以跟踪您的计算活动的小文件。

- **全面系统扫描**

全面系统扫描可彻底检查整台电脑以查找病毒、间谍软件和其他安全漏洞。可以使用“配置”选项调度全面系统扫描。

受保护的端口

“受保护的端口”设置保护电子邮件程序的 POP3 和 SMTP 端口。

您可以使用该选项为电子邮件防护手动配置 POP3 和 SMTP 电子邮件端口。如果您的 Internet 服务提供商 (ISP) 为电子邮件程序提供的 SMTP 和 POP3 端口号与默认的 SMTP 和 POP3 端口号不同，则必须对 Norton 进行配置以保护这些端口。

电子邮件防病毒扫描

电子邮件防病毒扫描可保护您免遭通过电子邮件附件发送或接收的威胁的侵害。

您可以使用“电子邮件防病毒扫描”选项来定义 Norton 在扫描电子邮件时应如何操作。根据您的选择的选项，Norton 会自动扫描您发送或接收的电子邮件。

排除/低风险

“排除”选项指定从 Norton 扫描中排除的项目，如文件夹、文件和驱动器。扫描、签名和低风险项目是一些可从扫描中排除的项目。

“排除”选项还允许您选择希望 Norton 检测的风险类别。相关的选项有：

- **低风险**

用于管理在电脑上找到的低风险项目。

您可以指定希望 Norton 响应低风险项目的方式。

- **要从扫描排除的项目**

用于确定要从风险扫描中排除的磁盘、文件夹或文件。

您可以在已排除项目列表中添加新排除项目或编辑已添加的项目，还可以从已排除项目列表中删除项目。

- **要从自动防护、SONAR 和下载智能分析检测排除的项目**

用于确定要从自动防护和 SONAR 扫描中排除的磁盘、文件夹或文件。

您可以添加需要排除的新项目或修改已经排除的项目。还可以从已排除项目列表中删除项目。

- **从所有检测排除的特征**

可让您按名称选择已知风险，以及从已排除项目列表中删除风险名称。您还可以基于性能、隐私、清除状态和隐藏影响查看风险影响。

- **清除扫描期间排除的文件 ID**

允许您删除从扫描排除的文件的信誉信息。

可使用“全部清除”选项清除从扫描排除的文件的信誉信息。

注意：排除会降低防护级别，应只在有特定需要时使用。

详细了解入侵和浏览器主动防护设置

“入侵防护”扫描进出电脑的所有网络通信，并将此信息与一组攻击特征进行比较。攻击特征包含的信息可用于确定攻击者对已知操作系统或程序漏洞的利用企图。“入侵防护”可保护电脑不受最常见 Internet 攻击的侵害。

如果信息符合某个攻击特征，“入侵防护”会自动丢弃该数据包，并断开与发送该数据的电脑的连接。此操作保护您的电脑免受任何形式的影响。

“入侵防护”功能需要使用一个包含大量攻击特征的列表来检测和阻止可疑的网络活动。Norton 产品会自动运行 LiveUpdate 以使攻击特征列表处于最新状态。如果不使用自动 LiveUpdate 更新，则应每周运行一次 LiveUpdate。

Norton 产品还提供浏览器主动防护功能以确保您的浏览器免遭恶意程序的攻击。

注意：“浏览器主动防护”功能适用于 Google Chrome、Microsoft Internet Explorer、Mozilla Firefox 和 Microsoft Edge 浏览器。

随着 Internet 使用率的增长，浏览器有可能受到恶意网站的攻击。这些网站可检测并利用浏览器的漏洞，从而在您不知情或未经您同意的情况下将恶意软件程序下载到您的系统。这些恶意软件程序也称为“偷渡式下载”。Norton 产品可保护您的浏览器，避免遇到来自恶意网站的偷渡式下载。

“入侵和浏览器主动防护”设置还包括“下载智能分析”选项，可保护您的电脑免受所下载的任何不安全文件的侵害。“下载智能分析”提供了有关您使用浏览器下载的任何可执行文件的信誉级别的信息。“下载智能分析”仅支持使用 HTTPS 协议、Internet Explorer 6.0 浏览器或更高版本、Edge 40.15063 浏览器或更高版本、Chrome 10.0 浏览器或更高版本以及 Firefox 3.6 浏览器或更高版本进行下载。“下载智能分析”提供的信誉详细信息指示安装下载的文件是否安全。您可以使用这些详细信息来决定是否要安装可执行文件。

设置 Norton 以允许您远程管理受保护的设备

Norton “远程管理” 将设备的运行状况和其他信息发送到适用于 Windows 的 Norton Studio 应用程序。可以使用此应用程序远程查看、管理或浏览 Norton 产品，以及修复设备的一些防护问题。默认情况下，“远程管理” 处于关闭状态。

打开“远程管理”

- 1 启动 Norton。
看到“我的 Norton” 窗口时，单击“设备安全” 旁边的“打开”。
- 2 在 Norton 产品主窗口中，单击“设置”。
- 3 在“设置” 窗口中，单击“管理设置”。
- 4 在“远程管理” 行中，将开关移到“打开”。
- 5 单击“应用”，然后单击“关闭”。

保护 Norton 设备安全设置免受未经授权的访问

要防止对 Norton 设备安全设置进行未经授权的更改，请打开“设置密码保护” 和“Norton 篡改防护”。

- “设置密码保护” 用于设置查看或更改设备安全设置的密码。
- “Norton 篡改防护” 检查未知或可疑应用程序对设置进行的修改。

打开或关闭“设置密码保护” 和“Norton 篡改防护”

- 1 启动 Norton。
看到“我的 Norton” 窗口时，单击“设备安全” 旁边的“打开”。
- 2 在 Norton 产品主窗口中，单击“设置”。
- 3 在“设置” 窗口中，单击“管理设置”。
- 4 在“产品安全性” 下：
 - 在“设置密码保护” 行中，将开关移到“打开” 或“关闭”。
 - 在“Norton 篡改防护” 行中，将开关移到“打开” 或“关闭”。
如果出现提示，则选择希望该功能关闭多长时间，然后单击“确定”。
- 5 单击“应用”。
- 6 如果看到“设置密码” 窗口，则键入密码并确认。每次关闭和打开此功能时都需要设置密码。

- 7 单击“确定”。
- 8 在“设置”窗口中，单击“关闭”。

根据 Norton 设置密码保护设置的密码丢失或忘记时重置

必须重新安装 Norton 才能访问设置以及设置新密码。

设置在 Norton 设备安全中搜索信息的快捷键

使用 Norton 设备安全应用程序中的搜索图标进行搜索时，可以在线查找 Norton 功能和支持信息以及常规主题。可以使用默认的键盘快捷键 **Ctrl + F** 更快地启动搜索，也可以设置快捷键。

设置搜索快捷键

- 1 启动 Norton。
 - 看到“我的 Norton”窗口时，单击“设备安全”旁边的“打开”。
- 2 在 Norton 产品主窗口中，单击“设置”。
- 3 在“设置”窗口中，单击“管理设置”。
- 4 在“搜索快捷键”行中，将开关移到“打开”。
- 5 单击箭头，然后选择要分配给产品内搜索的键。
- 6 执行下列操作之一：
 - 要使快捷键仅在 Norton 产品具有焦点时有效，则取消选中“全局”选项。
 - 要使快捷键在 Norton 产品没有焦点时也有效，则选中“全局”选项。
- 7 单击“应用”，然后单击“关闭”。

使用 Game Optimizer 优化您计算机的游戏体验

Game Optimizer¹ 是用于多核 CPU PC 的专利技术。它可以减少性能中断，同时仍保证计算机的安全，从而提供身临其境的游戏体验。通过将不必要的应用程序隔离到单个 CPU 核心，它可以将其余的 CPU 分配给游戏。

注意：计算机处理器必须至少具有 4 个核心，Game Optimizer 才能正常运行。

Game Optimizer 通过以下方式增强您的游戏体验：

- 优化 CPU 性能以实现更流畅的游戏体验
- 将不必要的应用程序隔离到单个 CPU 核心，以便将其余 CPU 分配给游戏，以提高性能
- 自动检测游戏²

- 可添加或选择不想优化的游戏
- 增加每秒帧数 (FPS) 并减少延迟
- 将 CPU 专用于实现最佳游戏性能，无需关闭病毒防护
- 通过将 CPU 核心专用于游戏来减少随机 CPU 峰值（这可能减慢游戏速度）

有关更多信息，请参见请参见第 76 页的“详细了解 Game Optimizer”。

注意：保护计算机免受病毒和其他安全威胁侵害的所有重要诺顿防护功能都在后台运行，不会中断您的游戏体验。

配置 Game Optimizer 以获得最佳游戏体验

- 1 启动 Norton。
- 2 在“我的 Norton”窗口的中心窗格，单击闪电图标。
- 3 在“游戏控制板”中，单击“管理优化”。
- 4 在 **Game Optimizer** 窗口中，配置以下设置：
 - **限制用户进程的资源使用率：**打开此选项可以限制所有用户启动的进程的 CPU 使用率。
 - **限制系统进程的资源使用率：**打开此选项可以限制所有操作系统启动的进程的 CPU 使用率。
 - **自动将电源计划设置为最大性能：**打开此选项可切换到 Windows 上的高性能电源计划设置。Game Optimizer 会创建自定义 Windows 电源计划设置，以实现游戏性能最大化。仅在进行游戏会话时才能使用此电源计划。游戏会话结束后，电源计划默认恢复为原始设置。
Norton 建议使此选项保持打开状态，以获得更好的游戏体验。
 - **已优化游戏：**列出由 Game Optimizer 优化的游戏。

默认情况下，Game Optimizer 处于打开状态。如果不希望 Game Optimizer 增强您的游戏体验，则可以将其关闭。Norton 建议使此功能保持打开状态，以获得更好的游戏体验。

关闭或打开 Game Optimizer

- 1 启动 Norton。
- 2 在“我的 Norton”窗口的左窗格中，滑动 **Game Optimizer** 开关以启用或禁用该功能。

¹Game Optimizer 仅在具有四个或更多核心处理器的 Windows（不包括 Windows 10 S 模式和运行 ARM 处理器的 Windows）上可用。

²如果用户手动添加游戏，或者先前已检测到该游戏，则会自动检测那些基于全屏检测模式、具有高 CPU 使用率并且使用游戏启动程序的游戏。截至 2021 年 4 月，目前监控的游戏启动程序包括：Bethesda、Blizzard、Epic、ID、Origin、Rockstar、Steam 和 Uplay。

详细了解 Game Optimizer

Game Optimizer¹ 是用于多核 CPU PC 的专利技术。它可以减少性能中断，同时仍保证计算机的安全，从而提供身临其境的游戏体验。通过将不必要的应用程序隔离到单个 CPU 核心，它可以将其余的 CPU 分配给游戏。

Game Optimizer 通过以下方式增强您的游戏体验：

- 优化 CPU 性能以实现更流畅的游戏体验
- 将不必要的应用程序隔离到单个 CPU 核心，以便将其余 CPU 分配给游戏，以提高性能
- 自动检测游戏²
- 可添加或选择不想优化的游戏
- 增加每秒帧数 (FPS) 并减少延迟
- 将 CPU 专用于实现最佳游戏性能，无需关闭病毒防护
- 通过将 CPU 核心专用于游戏来减少随机 CPU 峰值（这可能减慢游戏速度）

注意：计算机处理器必须至少具有 4 个核心，Game Optimizer 才能正常运行。

工作原理

启动游戏应用程序时，Game Optimizer 会开始进行优化，直到退出游戏为止。在游戏会话处于活动状态时，如果退出全屏模式，优化将暂停。例如，如果按 **Alt + Tab** 访问任何其他正在运行的程序，则它会退出游戏优化并删除限制。但是，返回到游戏时，它会继续进行游戏优化，并且受限制的程序无法访问 CPU 使用率。

尽可能减少后台活动还可确保计算机具备较高性能，非常适合游戏。结束游戏会话后，Norton 360 for Gamers 会恢复所有暂停的活动以在后台运行。

保护计算机免受病毒和其他安全威胁侵害的所有重要诺顿防护功能都在后台运行，不会中断您的游戏体验。

检查 Game Optimizer 状态

可在任务栏的通知区域中验证 Game Optimizer 的状态。启用 Game Optimizer 后，通知区域中的 Norton 产品图标显示绿色闪电图标。关闭 Game Optimizer 后，颜色变为灰色。

“游戏控制板”显示 Game Optimizer 状态、最近玩过的游戏的优化状态以及对 Game Optimizer 设置的访问权限。可以使用切换开关启用或禁用最近玩过的游戏的优化。

注意：Game Optimizer 功能仅适用于 Norton 360 for Gamers。

¹Game Optimizer 仅在具有四个或更多核心处理器的 Windows（不包括 Windows 10 S 模式和运行 ARM 处理器的 Windows）上可用。

²如果用户手动添加游戏，或者先前已检测到该游戏，则会自动检测那些基于全屏检测模式、具有高 CPU 使用率并且使用游戏启动程序的游戏。截至 2021 年 4 月，目前监控的游戏启动程序包括：Bethesda、Blizzard、Epic、ID、Origin、Rockstar、Steam 和 Uplay。

手动将游戏添加到“已优化游戏”列表中

Game Optimizer¹ 是用于多核 CPU PC 的专利技术。它可以减少性能中断，同时仍保证计算机的安全，从而提供身临其境的游戏体验。通过将不必要的应用程序隔离到单个 CPU 核心，它可以将其余的 CPU 分配给游戏。它会自动检查已知游戏的内部列表以检测游戏应用程序。^{1,2} 但是，如果它未自动检测到特定游戏，则可以手动将该游戏添加到“已优化游戏”列表中。

此外，如果不希望 Norton 360 for Gamers 增强这些游戏的性能，也可以从“已优化游戏”列表中将其删除。

注意：从“已优化游戏”列表中删除特定游戏后，将不再对该游戏进行优化，并且可能会影响您使用该游戏的游戏体验。

将游戏添加到“已优化游戏”列表中

- 1 启动 Norton。
- 2 在“我的 Norton”窗口的中心窗格，单击闪电图标。
- 3 在“游戏控制板”中，单击“管理优化”。
- 4 在 **Game Optimizer** 窗口中，单击“已优化游戏”旁边的“添加”。
- 5 导航并选择希望 Norton 优化的游戏程序。

从“已优化游戏”列表中删除游戏

- 1 启动 Norton。
- 2 在“我的 Norton”窗口的中心窗格，单击闪电图标。
- 3 在“游戏控制板”中，单击“管理优化”。
- 4 在 **Game Optimizer** 窗口的“已优化游戏”下，禁用要删除的游戏程序旁边的开关。

¹Game Optimizer 仅在具有四个或更多核心处理器的 Windows（不包括 Windows 10 S 模式和运行 ARM 处理器的 Windows）上可用。

²如果用户手动添加游戏，或者先前已检测到该游戏，则会自动检测那些基于全屏检测模式、具有高 CPU 使用率并且使用游戏启动程序的游戏。截至 2021 年 4 月，目前监控的游戏启动程序包括：Bethesda、Blizzard、Epic、ID、Origin、Rockstar、Steam 和 Uplay。

查找其他解决方案

本章节包括下列主题：

- [在 Windows 上卸载设备安全](#)
- [免责声明](#)

在 Windows 上卸载设备安全

要从计算机中卸载设备安全应用程序，请按照以下说明操作。

从 Windows 卸载设备安全

- 1 按 **Windows + R** 组合键以打开“运行”对话框。
- 2 键入 `appwiz.cpl`，然后按 **Enter** 键。
- 3 在当前已安装程序列表中，选择您的 Norton 产品，然后单击“卸载/更改”。
- 4 按照屏幕上的说明操作。

只有在重新启动计算机后才会完全卸载 Device Security。

免责声明

Copyright © 2021 NortonLifeLock Inc. © 2021 年 NortonLifeLock Inc. 版权所有。All rights reserved. 保留所有权利。诺顿 LifeLock、诺顿LifeLock 标志、打勾标志、Norton、LifeLock 以及锁头人型标志，均为 NortonLifeLock Inc. 或其子公司在美国及其他国家或地区的商标或注册商标。Firefox 是 Mozilla Foundation 的商标。Google Chrome 和 Android 是 Google, LLC 的商标。Mac、iPhone 和 iPad 是 Apple Inc. 的商标。Microsoft 和 Windows 徽标是 Microsoft Corporation 在美国和/或其他某些国家/地区的商标。通过 Google 创建和共享的作品复制或修改 Android Robot，并根据 Creative Commons 3.0 Attribution 许可证中所述的条款进行使用。其他名称可能为其各自所有者的商标，特此声明。