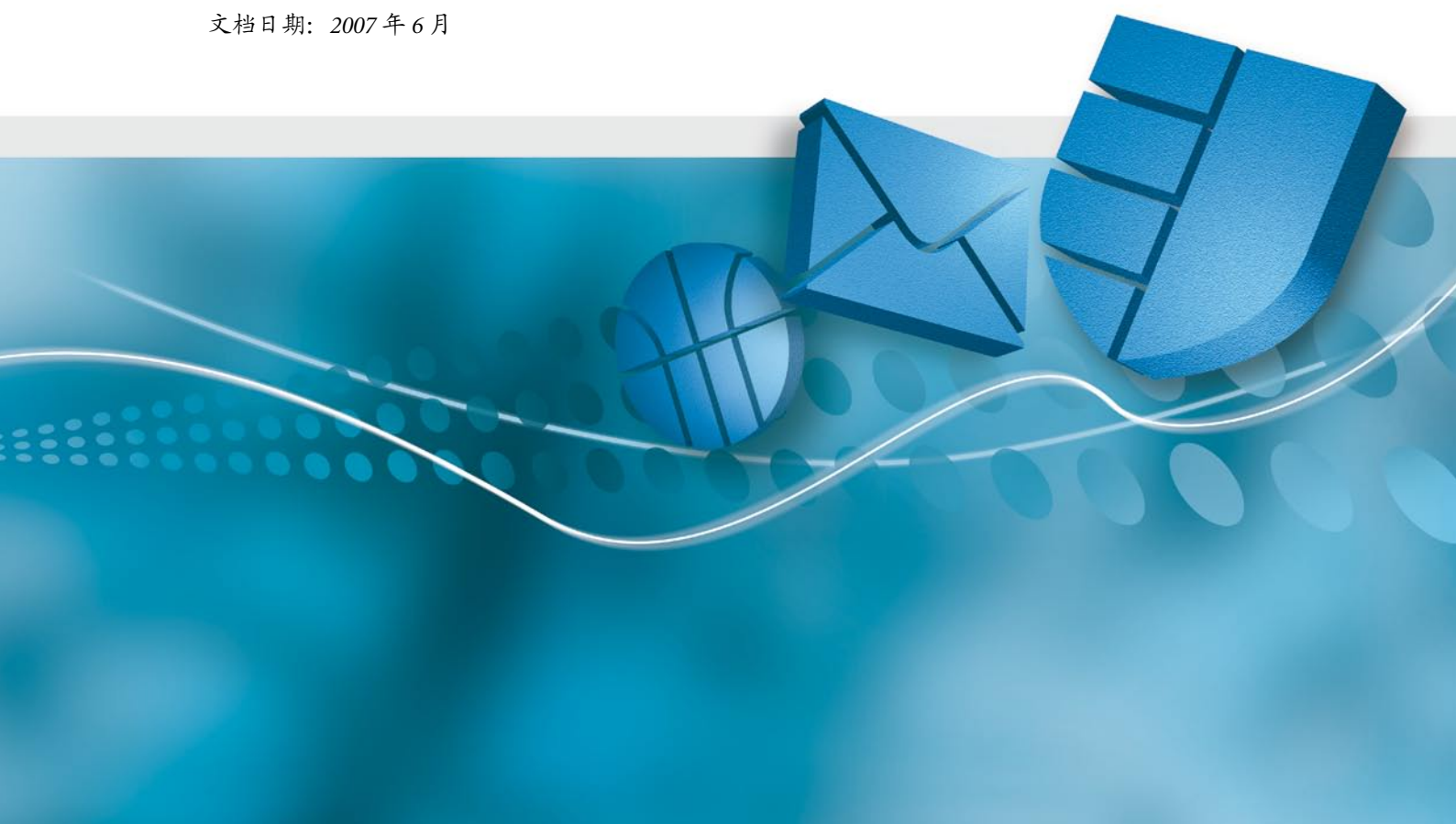


SOPHOS

Sophos Anti-Virus for Windows 版本 7 用户手册

供 Windows 2000 及以后的计算机使用

文档日期: 2007 年 6 月



目录

1	关于 Sophos Anti-Virus	4
2	检查本计算机是否受到扫描保护	9
3	即时扫描各种项目	10
4	扫描单个项目	14
5	限制访问权限	15
6	为多用户更改设置	16
7	配置扫描	17
8	配置运行时行为分析	25
9	配置警报	26
10	日志记录	29
11	更新	31
12	进行清除	36
13	管理隔离项目	41
14	批准使用项目	50
15	排疑解难	52
	索引	60

1 关于 Sophos Anti-Virus

什么是 Sophos Anti-Virus?

Sophos Anti-Virus 是一种软件，用于检测和处置您的计算机或网络中的

- 安全隐患：病毒，蠕虫，特洛伊木马，间谍软件，可疑文件，可疑行为，以及广告软件/PUA (可能不想安装的应用程序)。
- 受控程序。

特别地，它能够

- 扫描您的计算机或网络中的安全隐患和受控程序；
- 检查您访问的每个文件是否是安全隐患或受控程序；
- 在发现安全隐患或受控程序时，向您发出警报；
- 清除被感染的项目；
- 中止可疑行为；
- 阻止广告软件 / 可能不想安装的应用程序在计算机上运行；
- 清除计算机上的广告软件 / 可能不想安装的应用程序；
- 保存活动日志记录；
- 保持更新以检测最新的安全隐患。

Sophos Anti-Virus 可以安装在运行 Windows 2000 或以后的计算机上。

Sophos Anti-Virus 中整合了管理控制台，从而使网络系统管理员可以统一管理安装在各工作站上的 Sophos Anti-Virus。Sophos Anti-Virus 中还整合了网络安全解决方案 Cisco® 网络准入控制 (NAC)，这样在对主机做网络准入策略校验时，就可以使网络管理员提供 Sophos Anti-Virus 的状态。欲知更多信息，请参考管理控制台的帮助文件和 *Sophos Anti-Virus Cisco NAC 整合指南*。

使用 Sophos Anti-Virus 的方法有两种：

- 通过 Sophos Anti-Virus 窗口。

- 通过 Sophos Anti-Virus 系统托盘图标。

Sophos Anti-Virus 可以执行

- 读写扫描
- 即时扫描
- 单击右键扫描
- 运行时行为分析

Sophos Anti-Virus 窗口

要开启 **Sophos Anti-Virus** 窗口，右击 Sophos Anti-Virus 系统托盘图标，显示菜单。



选择 打开 **Sophos Anti-Virus**。窗口的组成部分，描述如下：



工具栏

包括获取帮助，以及在 **Sophos Anti-Virus** 窗口中，右手边的窗

格板里的各功能之间往返的按钮。

状态

包括读写扫描的状态，隔离区中的项目数，Sophos Anti-Virus 最近一次更新的时间，以及产品版本号。

帮助和信息

使您能够联系 Sophos 技术支持，使用 Sophos Anti-Virus 中的帮助，以及获取安全隐患和受控程序的信息。要查看您计算机上安装的 Sophos Anti-Virus 的版本的详情，请单击 [查看产品信息](#)。

活动摘要

在您运行一次扫描时出现，包括所发现的所有项目的相关信息。

主页

在您打开 **Sophos Anti-Virus** 窗口时，显示在右手边的窗格板中。它包括功能列表和 可用的扫描 列表。在您使用 **Sophos Anti-Virus** 窗口时，右手边窗格板中的内容可能会变化。您可以单击 [主页](#) 按钮返回到主页。

功能列表显示在主页的顶端。它使您能够

- [扫描您的计算机](#)
- [设置扫描](#)
- [管理隔离项目](#)
- [配置 Sophos Anti-Virus](#)

可用的扫描 列表列示已经设置的扫描。从这里，您可以运行，编辑或删除每一个扫描，以及查看摘要，了解最近一次扫描的情况。

Sophos Anti-Virus 系统托盘图标


Sophos Anti-Virus 系统托盘图标会总是显示出来，即使 **Sophos**

Anti-Virus 窗口是关闭的。







如果您将鼠标指针移到图标上，工具提示会显示最近一次更新 Sophos Anti-Virus 的时间。

如果您右击该图标，会弹出一个菜单。从菜单中，您可以

- 更新 Sophos Anti-Virus
- 配置更新
- 检查更新进程
- 开启 **Sophos Anti-Virus** 窗口


 您需要成为 SophosAdministrator 组的成员，才能配置更新。

根据读写扫描是否激活，Sophos Anti-Virus 是否已更新，以及 Sophos Anti-Virus 上一次是否更新成功，该图标的外观会有所不同。

图标外观	释意
	蓝色的盾牌说明读写扫描处于激活状态。Sophos Anti-Virus 上一次的更新成功。
	如果在蓝色的盾牌上出现上下移动的绿色条，这说明 Sophos Anti-Virus 正在进行更新。读写扫描处于激活状态。
	如果在蓝色的盾牌上出现红色的圈和在其中有个白色的叉，这说明更新失败了。读写扫描处于激活状态。
	灰色的盾牌说明读写扫描处于没有激活状态。Sophos Anti-Virus 上一次的更新成功。
	如果在灰色的盾牌上出现上下移动的绿色条，这说明 Sophos Anti-Virus 正在进行更新。读写扫描处于没有激活状态。
	如果在灰色的盾牌上出现红色的圈，以及在其中有个白色的叉，这说明更新失败了。读写扫描处于没有激活状态。


要了解，如果在系统托盘图标上出现红色的圈，以及在其中有个白色的叉，或者，该图标呈灰白显示时，应该怎么办？请参看 [系统托盘图标上出现白色的叉_或_系统托盘图标呈灰白显示。](#)

什么是读写扫描？

 读写扫描 介入对文件的读写，从而保证只能读写那些没有对您的计算机构成安全隐患，或者已批准使用的文件。


欲了解更多有关读写扫描的信息，请参见 [检查计算机是否受到保护](#) 以及 [配置扫描](#)。

什么是即时扫描？

 即时扫描 是对整个计算机，或对计算机的某些部分所进行的扫描，您可以随时随地运行即时扫描，也可以计划安排在某一时间运行它。


欲了解更多有关即时扫描的信息，请参见 [即时扫描各种项目](#) 以及 [配置扫描](#)。

什么是单击右键扫描？

 单击右键扫描 是对在 Windows 资源管理器中，或者在桌面上，选择的项目所进行的扫描，您可以在所选择的项目上单击右键，并在弹出的菜单中选择 **用 Sophos Anti-Virus 扫描**。

欲了解更多有关单击右键扫描的信息，请参见 [扫描单个项目](#) 以及 [配置扫描](#)。

什么是运行时行为分析？


 运行时行为分析由可疑行为检测和缓冲区溢出检测组成。可疑行为检测，是对运行在计算机上的所有程序进行动态分析，检测和阻断看起来有不良意图的运行活动。

欲了解更多有关运行时行为分析的信息，请参见 [检测可疑行为和缓冲区溢出](#)。

2 检查本计算机是否受到扫描保护

检查扫描保护是否开启


计算机受到读写扫描的保护。

 读写扫描介入对文件的读写，从而保证只能读写那些没有对您的计算机构成安全隐患，或者已批准使用的文件。

当读写扫描处于激活状态时，一个蓝色的盾牌会显示在系统托盘中。





当读写扫描处于未激活状态时，该盾牌是灰色的。

 读写扫描的状态，同时也显示在 **Sophos Anti-Virus** 窗口中的状态显示区中。

如果您的计算机是在网络中的，那么读写扫描可能已经被配置了。不过，如果您想要更改这些设置，请参见 [配置扫描](#)。

为计算机开启或关闭扫描保护

 如果您关闭扫描保护，Sophos Anti-Virus 就不会在读取文件时进行安全隐患扫描。

 您需要成为 SophosAdministrator 组的成员，才能为计算机开启或关闭扫描保护。

1. 在配置菜单中，单击读写扫描。
2. 在本计算机的读写扫描设置对话框，单击扫描标签。

要为计算机开启读写扫描，勾选在本计算机上启用读写扫描，然后，单击确定。Sophos Anti-Virus 系统托盘图标会变

成蓝色。

要为计算机 **关闭** 读写扫描，取消勾选 **在本计算机上启用读写扫描**，然后，单击 **确定**。Sophos Anti-Virus 系统托盘图标会变成灰色。

Sophos Anti-Virus 窗口中的 **状态** 显示区会相应更新。



即使您重新启动计算机，Sophos Anti-Virus 还是会将您在此所作的设置保留。如果您已经将读写扫描关闭，那么，读写扫描将一直保持 **未激活** 状态，直到它被重新开启。



如果您关闭了读写扫描，您仍然可以在计算机上运行即时扫描。

3 即时扫描各种项目

什么是即时扫描？



即时扫描 是对整个计算机，或对计算机的某些部分所进行的扫描，您可以随时随地运行即时扫描，也可以计划安排在某一时间运行它。

扫描我的电脑


要扫描计算机上的所有固定硬盘，包括其引导扇区，请按以下说明做。

在 **Sophos Anti-Virus** 窗口的 主页 中，单击 扫描我的电脑。

这时会有一个扫描进程对话框出现，同时 **活动摘要** 会出现在 **Sophos Anti-Virus** 窗口中。

如果发现了安全隐患或受控程序，单击 **更多信息**，并参见 **管理隔离项目**。


要停止扫描，单击 **停止扫描**。

 扫描我的电脑 功能并不扫描存储在 Windows 计算机上的 Macintosh 文件。如果您想要 Sophos Anti-Virus 扫描可执行的 Macintosh 文件,您必须 设置一个自定义的即时扫描,并为该扫描启动扫描_Macintosh_文件选项。


有关设置,计划,运行和配置一次扫描的更多信息,请参见本节的剩余部分,以及 [配置扫描](#)。

设置扫描

1. 在 文件 菜单,单击 [新扫描](#),显示扫描设置页。
2. 在 扫描名称 文本框中,输入扫描的名称。
3. 在 扫描项目 面板中,选择您想要扫描的驱动器和文件夹。勾选各驱动器或文件左边的勾选框,可以进行选择。要了解出现在勾选框中的各种图标的含义,请参见 [扫描项目的示意图标](#)。


 在显示不可用的驱动器或文件夹(因为它们是离线的,或者已被删除)时,会有删除线。如果它们被取消了勾选,或者,如果更改了对它们的父驱动器或父文件夹的选择,它们会被从 扫描项目 窗格板中删除。

4. 要进一步配置选项,单击 [配置本扫描](#)。(请参见 [配置扫描](#) 获取更多信息。)
5. 要计划本扫描,单击 [计划本扫描](#)。(请参见 [计划一次扫描获取更多的信息](#)。)


 您不能够手动运行一个您已经计划了的扫描。计划了的扫描会显示在 可用的扫描 列表中,并带有一个时钟图标。

6. 单击 [存盘](#) 保存本扫描,或者,单击 [存盘并启动](#),保存并运行该扫描。

计划扫描

 您需要成为 **Sophos Administrator** 组的成员，才能安排计划扫描，或者，查看和编辑其它用户创建的计划扫描。

要计划一次您正在设置或者编辑的扫描，请按以下说明做：

 您不能够手动运行一个您已经计划了的扫描。计划了的扫描会显示在 可用的扫描 列表中，并带有一个时钟图标。

1. 在 **Sophos Anti-Virus** 窗口，右手边的窗格板中，单击 计划本扫描。

2. 在 计划扫描 对话框中，选择 启用计划。

选择扫描应该运行的时间。

单击 添加 可添加时间。

如果需要，选择时间，然后分别单击 删除 或 编辑，可以删除或编辑该时间。


3. 输入 用户名 和 密码。密码不能为空。

该计划扫描将依据该用户的访问权限运行。

运行扫描

要运行一次已经设置的扫描，请按以下说明做：

在 **Sophos Anti-Virus** 窗口的主页中，在可用的扫描 列表中，选择您想要运行的扫描。单击 启动。

 您不能够手动运行一个您已经计划了的扫描。计划了的扫描会显示在 可用的扫描 列表中，并带有一个时钟图标。

这时会有一个扫描进程对话框出现，同时 活动摘要 会出现在 **Sophos Anti-Virus** 窗口中。

如果发现了安全隐患或受控程序，单击 更多信息，并参见 管理隔离项目。


要停止扫描，单击 停止扫描。

有关设置,计划和配置一次扫描的更多信息,请参见本节的剩余部分,以及 [配置扫描](#)。


编辑扫描

要编辑一次已经设置的扫描,请按以下说明做:

1. 在 **Sophos Anti-Virus** 窗口的 主页 中,在 可用的扫描 列表中,选择您想要编辑的扫描。单击 **编辑** 显示该扫描的设置页面。
2. 要重新命名本扫描,在 **扫描名称** 文本框中,输入本扫描的名称。
3. 要更改扫描的项目,在 **扫描项目** 面板中,勾选或者取消勾选您想扫描或者不想扫描的驱动器和文件夹。勾选各驱动器或文件左边的勾选框,可以进行选择。要了解出现在勾选框中的各种图标的含义,请参见 [扫描项目的示意图标](#)。

 在显示不可用的驱动器或文件夹(因为它们是离线的,或者已被删除)时,会有删除线。如果它们被取消了勾选,或者,如果更改了对它们的父驱动器或父文件夹的选择,它们会被从 **扫描项目** 窗格板中删除。

4. 要进一步配置选项,单击 **配置本扫描**。(请参见 [配置扫描](#) 获取更多信息。)
5. 要计划本扫描,单击 **计划本扫描**。(请参见 [计划一次扫描](#) 获取更多的信息。)

 您不能够手动运行一个您已经计划的扫描。计划的扫描会显示在 **可用的扫描** 列表中,并带有一个时钟图标。

6. 单击 **存盘** 保存本扫描,或者,单击 **存盘并启动**,保存并运行该扫描。

要删除某个扫描,请在 **Sophos Anti-Virus** 窗口的 主页 中,在 可用扫描 列表里,选择您想要删除的扫描。单击 **删除**,然后,单击 **是** 确认删除。

扫描项目的示意图标


在扫描项目窗格板中,各种不同的图标会出现在每个项目(驱动器或文件夹)的勾选框中,图标的不同取决于要扫描的项目。对这些图标的说明如下。

图标	释意
<input type="checkbox"/>	该项目及其所有子项目都没有被选择为扫描对象。
<input checked="" type="checkbox"/>	该项目及其所有子项目都已被选择为扫描对象。
<input checked="" type="checkbox"/>	部分地被选择的项目:该项目本身没有被选择,但是,该项目的一些子项目被选择进行扫描。
<input checked="" type="checkbox"/>	该项目及其所有子项目会被从特定的扫描中排除。
<input checked="" type="checkbox"/>	部分地排除的项目:该项目本身被选择,但是,该项目的一些子项目被从该特定的扫描中排除。
<input checked="" type="checkbox"/>	该项目及其所有子项目都已被从所有即时扫描中排除,因为已经设定了一个即时扫描的排除列表。

4 扫描单个项目

扫描单个项目

您可以用单击右键扫描对单个项目实行扫描。

 单击右键扫描 是对在 Windows 资源管理器中, 或者在桌面上, 选择的项目所进行的扫描, 您可以在所选择的项目上单击右键, 并在弹出的菜单中选择 用 **Sophos Anti-Virus** 扫描。

1. 打开 Windows 资源管理器。要打开 Windows 资源管理器, 请在任务栏中, 单击 开始 | 程序 | 附件 | **Windows** 资源管理器。
2. 选择您想要扫描的文件, 文件夹和 / 或磁盘驱动器。
3. 右击该选择, 弹出菜单, 然后选择 用 **Sophos Anti-Virus** 扫描。

这时会显示一个扫描进程对话框。

如果发现了安全隐患或受控程序, 单击 更多信息, 并参见 [管理隔离项目](#)。

要停止扫描, 单击 停止扫描。

有关配置扫描的信息, 请参见 [配置扫描](#)。

5 限制访问权限

用户类型

Sophos Anti-Virus 会限制某些类型的用户, 对本软件的特定部分的访问。该安全措施是基于已经在本计算机中设置的 Windows 的用户组。在安装 Sophos Anti-Virus 时, 根据其所属的 Windows 用户组, 每一个用户都会被指派给其中一个 Sophos 用户组, 具体说明如下。

- Windows Administrators 组中的成员会被指派给 SophosAdministrator 组
- Windows Power Users 组中的成员会被指派给 SophosPowerUser 组
- Windows Users 组中的成员会被指派给 SophosUser 组

任何没有被指派给任一 Sophos 用户组的用户, 以及 Guest 用

户,只能够执行

- 读写扫描
- 从单击右键菜单中运行的扫描

SophosUser 组中的成员可以执行上述功能,以及

- 进入 Sophos Anti-Virus 窗口
- 设置和运行即时扫描
- 配置从单击右键菜单中运行的扫描
- 具备限定的权限管理隔离项目

SophosPowerUser 组中的成员,具有与 SophosUser 组中的成员相同的权限,此外,还在隔离区管理器中具有更多的权限,以及访问批准管理器的权限。

SophosAdministrator 组中的成员,可以使用和配置 Sophos Anti-Virus 的任何部分。

更改 Sophos 用户组的成员身份

要更改 Sophos 用户组的成员身份,您必须按以下说明做。(必要时请参考您的 Windows 技术文档)。

1. 使用 Windows 将用户从一个 Sophos 用户组移到另一个 Sophos 用户组中。
2. 当该用户再次登录 Windows 时,他们因该发现其访问权限已相应地改变。

6 为多用户更改设置

为所有计算机更改设置

要在网络中统一配置工作站上的 Sophos Anti-Virus,请参见管理控制台帮助文件。

为计算机上的所有用户更改设置

要为计算机上的所有用户配置 Sophos Anti-Virus，请使用 **配置** 菜单。从配置菜单中，您可以配置以下设置。

- 读写扫描
- 即时扫描文件扩展名和排除文件
- 运行时行为分析
- 应用程序控制
- 用户使用隔离区管理器的权限
- 已批准的广告软件 / 可能不想安装的应用程序，以及可疑项目的列表
- 消息发送
- 日志记录
- 更新

您需要成为 SophosAdministrator 组的成员，才能更改这些设置。

7 配置扫描

打开扫描设置对话框


针对三种扫描类型的扫描设置，分别在三种不同的对话框中。

要打开 **读写扫描** 设置对话框，在 **配置** 菜单中，单击 **读写扫描**。

要打开 **读写扫描** 设置对话框，在 **Sophos Anti-Virus** 窗口的主页中的 **可用的扫描** 列表中，选择您想要编辑的扫描。单击 **编辑**。在扫描设置页中，单击 **配置本扫描**。

要打开 **单击右键扫描** 设置对话框，在 **配置** 菜单中，单击 **单击右键扫描**。

更改要扫描的文件类型

 如果使用了管理控制台管理工作站上的 Sophos Anti-Virus，那么，在此所作的更改不会被理会。要避免这种情况，请参见控制台的帮助文件。


1. 要更改 **读写扫描** 的设置，请在 **配置** 菜单中，单击 **读写扫描**。

要更改 **即时扫描** 和 **单击右键扫描**，在 **配置** 菜单中，单击 **即时扫描文件扩展名和排除文件**。

2. 单击 **扩展名** 标签。请按以下说明设置选项。


扫描所有文件

单击该选择，以启用扫描所有文件，该扫描忽略文件的扩展名。

 Sophos 不推荐使用这一选项，除非 Sophos 技术支持建议这样做。选择 **扫描所有文件** 选项会使扫描进程变慢，通常并不需要使用。

允许精确控制扫描的项目

单击该选择，以限制扫描仅针对那些在文件扩展名列表中所指定的，带有特定扩展名的文件。

 扩展名列表中包括了 Sophos 建议扫描的所有文件类型。如果您要更改该列表，请按照以下的说明仔细地做。

要添加文件扩展名到该列表中，请单击 **添加**。您可以使用通配符 **?** 替代任何单一的字符。


要从列表中删除文件扩展名，请选择该扩展名，然后，单击 **删除**。


要从列表中更改文件扩展名，请选择该扩展名，然后，单击 **编辑**。

当您选择 **允许精确控制扫描的项目** 选项时，**扫描没有扩展名的文件** 选项会成为默认选项。要禁用扫描不带文件扩展

名的文件，请取消勾选 扫描不带文件扩展名的文件。

排除扫描的项目

 如果使用了管理控制台管理工作站上的 Sophos Anti-Virus，那么，在此所作的更改不会被理会。要避免这种情况，请参见控制台的帮助文件。

 以下所描述的过程，可以应用于 所有的 即时扫描。要从某一个 特定的 即时扫描中排除项目，请参见 [编辑扫描](#)。

1. 要更改 *读写扫描* 的设置，请在 *配置* 菜单中，单击 *读写扫描*。

要更改 *即时扫描* 和 *单击右键扫描*，在 *配置* 菜单中，单击 *即时扫描文件扩展名和排除文件*。

2. 单击 *排除文件* 标签。请按以下说明设置选项。

排除项目


要指定从扫描中排除的项目，单击 *添加*。在 *排除项目* 对话框中，指定要排除的项目的类型和名称。请参见 *指定排除项目*。

要从该列表中删除排除项目，单击 *删除*。

要从该列表中更改排除项目，单击 *编辑*。

指定排除项目

在 *排除项目* 对话框中，选择 *项目类型*。*所有远程文件* 是指所有不在此计算机上的文件。除非您选择了 *所有远程文件*，否则，请使用 *浏览* 按钮，或在文本框中输入文字，以指定项目名称。

 如果您使用的是 64 位的操作系统，*浏览* 按钮在 *排除项目* 对话框中将不可见。

以下进一步说明如何指定项目。

- 文件名

您可以只指定文件名，而 Sophos Anti-Virus 会排除具有该文件名的所有文件，无论这些文件在哪个路径中。比如

fred.bmp

会使 Sophos Anti-Virus 排除所有文件名为 fred.bmp 的文件，无论这些文件在哪个路径中。

- **完整路径**

您可以指定完整的路径和文件名，这样 Sophos Anti-Virus 会只排除该文件。路径中可包含驱动器名和共享名。比如

C:\Miscellaneous\fred.bmp

会使 Sophos Anti-Virus 排除驱动器 C: 中 Miscellaneous 文件夹里的 fred.bmp 文件。

\\Server1\Users\Fred\Letter.rtf

会使 Sophos Anti-Virus 排除在 Server1 中的 Users 共享里的 Fred 文件夹里的 Letter.rtf 文件。

如果您不指定驱动器名或共享名，Sophos Anti-Virus 会从每个驱动器的根目录中，或每个共享中比对给出的路径。

- **局部路径**

您可以指定驱动器或者共享，Sophos Anti-Virus 可以排除所指定的驱动器或共享中的一切内容。比如

A:

会使 Sophos Anti-Virus 排除驱动器 A: 中的一切内容。

您可以指定文件夹，Sophos Anti-Virus 可以排除所指定的文件夹中的一切内容。比如

D:\Tools\

会使 Sophos Anti-Virus 排除驱动器 D: 及其所有子文件夹中的 Tools 文件夹里的一切内容。

您可以指定文件夹和文件名，Sophos Anti-Virus 可以排除所匹配的一切文件夹中和文件。比如

logs\log.txt

会使 Sophos Anti-Virus 排除在任何驱动器 , 或共享中的 , 任何名为 logs 的文件夹中的 log.txt 文件。

通配符

通配符 ? 只能用于文件名或文件扩展名中。一般地 , 它可以匹配任何单一的字符。然而 , 在文件名或扩展名的最后使用通配符时 , 它匹配单个字符 , 或者 , 不匹配字符。例如 :file???.txt 可以匹配 file.txt , file1.txt 和 file12.txt , 但是不匹配 file123.txt。

通配符 * 只能用于文件名或扩展名中 , 形式为 [文件名].* 或者 *.*[扩展名]。比如 , file*.txt , file.txt* 及 file.*txt 是无效的。

多扩展名的文件名


在带有多个扩展名的文件名中 , 最后一个扩展名被视为扩展名 , 其余部分被视为文件名。比如

[文件名].[扩展名 1].[扩展名 2] 中的文件名是 [文件名].[扩展名 1] , 而扩展名是 [扩展名 2]。

标准命名协定

文件名或路径都会依据标准命名协定被校验 (如 : 一个文件夹的名称可以包含空格 , 但不能全部为空格)。

更改实行读写扫描的时间

 如果使用了管理控制台管理工作站上的 Sophos Anti-Virus , 那么 , 在此所作的更改不会被理会。要避免这种情况 , 请参见控制台的帮助文件。

您可以指定当文件被打开 , 保存 , 或者重命名时 , Sophos Anti-Virus 是否对其进行扫描。

1. 在 配置 菜单中 , 单击 读写扫描。
2. 在 本计算机的读写扫描设置 对话框 , 单击 扫描 标签。请


按以下说明设置选项。


要指定在打开时必须对其进行扫描的文件，请选择 **读文件时**。这是推荐使用的选项。

要指定在保存时必须对其进行扫描的文件，请选择 **写文件时**。

要指定在重命名时必须对其进行扫描的文件，请选择 **重命名文件时**。


扫描可疑文件

 如果使用了管理控制台管理工作站上的 Sophos Anti-Virus，那么，在此所作的更改不会被理会。要避免这种情况，请参见控制台的帮助文件。


 **可疑文件** 是可能感染了尚无法具体识别的病毒的文件。

1. 打开您想要配置的扫描类型的扫描设置对话框。（请参见 [打开扫描设置对话框。](#)）
2. 在扫描设置对话框中，单击 **选项** 标签。
3. 选择 **扫描可疑文件 (HIPS)**。


扫描广告软件 / 可能不想安装的应用程序


 如果使用了管理控制台管理工作站上的 Sophos Anti-Virus，那么，在此所作的更改不会被理会。要避免这种情况，请参见控制台的帮助文件。

1. 打开您想要配置的扫描类型的扫描设置对话框。（请参见 [打开扫描设置对话框。](#)）
2. 在扫描设置对话框中，单击 **选项** 标签。
3. 扫描 **扫描广告软件 / 可能不想安装的应用程序**。


 高级设置都非常地专业，您应该只在得到 Sophos 技术支持的建议时，才使用高级设置。

扫描受控程序

 如果使用了管理控制台管理工作站上的 Sophos Anti-Virus，那么，在此所作的更改不会被理会。要避免这种情况，请参见控制台的帮助文件。


 受控程序 是正当的客户应用程序，但它会影响工作效率，以及网络运行效率。

如果读写扫描受控程序，已在您的计算机上启用，它可能会阻止您卸载某些应用程序。如果是这样，您可以按照以下说明，禁用读写扫描受控程序。

 您需要成为 SophosAdministrator 组的成员，才能更改此设置。

1. 在 配置 菜单中，单击 应用程序控制。
2. 在 应用程序控制 对话框中，取消勾选 读写扫描未批准的受控程序。
3. 在您卸载完毕应用程序之后，重新勾选 读写扫描未批准的受控程序。

扫描打包文件内部


 扫描打包文件内部会显著减慢扫描进程，通常并不需要使用。即使您没有选择该选项，当您试图访问从打包文件中解包的文件时，该解包文件也会被扫描。Sophos 因此不推荐使用这一选项。

无论您是否选择了该选项，使用动态压缩工具 (PKLite, LZEXE 和 Diet) 压缩的文件，也会被扫描。


1. 打开您想要配置的扫描类型的扫描设置对话框。(请参见 [打开扫描设置对话框](#)。)
2. 在扫描设置对话框中，单击 选项 标签。
3. 选择 扫描打包文件内部。

要启用只扫描特定的打包文件类型的内部，单击 高级。在

高级扫描设置 对话框,选择您想要 Sophos Anti-Virus 扫描其内部的打包文件类型。

 高级设置都非常地专业,您应该只在得到 Sophos 技术支持的建议时,才使用高级设置。


扫描 Macintosh 文件

 如果使用了管理控制台管理工作站上的 Sophos Anti-Virus,那么,在此所作的更改不会被理会。要避免这种情况,请参见控制台的帮助文件。


您可以启用 Sophos Anti-Virus 扫描存储在 Windows 计算机上的 Macintosh 文件。

1. 打开您想要配置的扫描类型的扫描设置对话框。(请参见 [打开扫描设置对话框。](#))
2. 在扫描设置对话框中,单击 **选项** 标签。
3. 选择 **扫描 Macintosh 病毒**。这会启用 Sophos Anti-Virus 扫描可执行的 Macintosh 文件。

扫描文件的全部内容

 如果使用了管理控制台管理工作站上的 Sophos Anti-Virus,那么,在此所作的更改不会被理会。要避免这种情况,请参见控制台的帮助文件。


要检测某些病毒,您必须对启用扫描每个文件的全部内容。


 Sophos 不推荐使用这一选项,除非 Sophos 技术支持建议这样做。

1. 打开您想要配置的扫描类型的扫描设置对话框。(请参见 [打开扫描设置对话框。](#))
2. 在扫描设置对话框中,单击 **选项** 标签。
3. 在 **扫描级别** 窗格板中,单击 **扩展**。
4. 当您已经清除了病毒之后,请单击 **普通**。


8 配置运行时行为分析

检测可疑行为和缓冲区溢出

 如果使用了管理控制台管理工作站上的 Sophos Anti-Virus，那么，在此所作的更改不会被理会。要避免这种情况，请参见控制台的帮助文件。


 可疑行为 是看起来带有恶意的程序活动。

如果您想更改检测可疑行为和缓冲区溢出的设置，请按照以下说明做。


 您需要成为 SophosAdministrator 组的成员，才能更改这些设置。

1. 在 **配置** 菜单中，单击 **HIPS 运行时行为分析**，显示 **HIPS 运行时行为分析** 对话框。
2. 要启用或禁用可疑行为检测，请分别勾选或取消勾选 **检测可疑行为**。

要启用或禁用缓冲区溢出检测，请分别勾选或取消勾选 **检测缓冲区溢出**。

 缓冲区溢出检测功能，不能用于 Windows Vista 和 64 位版本的 Windows 操作系统。这些操作系统使用 Microsoft 的数据执行保护 (DEP) 功能防范缓冲区溢出。


3. 如果在此计算机上是新安装的 Sophos Anti-Virus，依照默认值，可疑行为和缓冲区溢出会被 **检测到**，但是，不会被 **阻断**。如果是升级安装，依照默认值，可疑行为和缓冲区溢出不会被检测到。

 Sophos 建议您在“仅限检测”的模式下，运行一次 Sophos Anti-Virus，在启用自动阻断可疑行为和缓冲区溢出之前，批准您想要的程序。此方法可以避免阻断您的用户可能需要的程序。

要在 **检测** 的同时，启用 **阻断** 可疑行为和缓冲区溢出，请取消勾选 **仅限警报**。

9 配置警报

桌面消息发送

 如果使用了管理控制台管理工作站上的 Sophos Anti-Virus，那么，在此所作的更改不会被理会。要避免这种情况，请参见控制台的帮助文件。

要使 Sophos Anti-Virus 在发现安全隐患时，显示桌面消息，请按照以下说明做。这仅仅应用于读写扫描。

1. 在 配置 菜单中，单击 消息发送。
2. 在 消息发送 对话框中，单击 桌面消息发送 标签。请按以下说明设置选项。

启用桌面消息发送

选择该项，启用 Sophos Anti-Virus 在发现安全隐患时，显示桌面消息。


要发送的消息

选择您想要 Sophos Anti-Virus 发送桌面消息的事件。

用户定义消息

在此文本框中，您可以输入一段消息文字，它会被添加到标准的消息文字之后。

电子邮件警报发送

 如果使用了管理控制台管理工作站上的 Sophos Anti-Virus，那么，在此所作的更改不会被理会。要避免这种情况，请参见控制台的帮助文件。

要启用 Sophos Anti-Virus 在发现安全隐患，或出现错误时，发送电子邮件警报，请按以下说明做。这应用于读写扫描，即时扫描和单击右键扫描。

1. 在 **配置** 菜单中 ,单击 **消息发送**。
2. 在 **消息发送** 对话框中 ,单击 **电子邮件警报** 标签。请按以下说明设置选项。

启用电子邮件警报

选择该项 ,以启用 Sophos Anti-Virus 发送电子邮件警报。

要发送的消息

选择您想要 Sophos Anti-Virus 发送电子邮件警报的事件。
扫描错误 中包括 Sophos Anti-Virus 被拒绝访问试图扫描的项目的情况。

收件人

单击 **添加** 或 **删除** 分别添加或删除电子邮件警报的寄往地址。单击 **编辑** 更改您所添加的电子邮件地址。

配置 SMTP

单击该项 ,更改 SMTP 服务器和电子邮件警报语言的设置。
(请参见 **配置 SMTP 设置**。)

配置 SMTP 设置

SMTP 服务器

在文本框中 ,输入主机名或 SMTP 服务器的 IP 地址。单击 **测试** 以测试到 SMTP 服务器的连接。(这不会发送测试的电子邮件。)

SMTP “发送人 ” 地址

在文本框中 ,输入退回邮件和未送达报告将要寄往的地址。


SMTP “回复 ” 地址

由于电子邮件警报是从无人照管的邮箱发出的 ,您可以在文本框中 ,输入电子邮件警报的回复地址。

语言

单击下拉箭头，然后选择寄送电子邮件警报所使用的语言。

SNMP 消息发送

 如果使用了管理控制台管理工作站上的 Sophos Anti-Virus，那么，在此所作的更改不会被理会。要避免这种情况，请参见控制台的帮助文件。

要启用 Sophos Anti-Virus 在发现安全隐患，或出现错误时，发送 SNMP 消息，请按以下说明做。这应用于读写扫描，即时扫描和单击右键扫描。

1. 在 **配置** 菜单中，单击 **消息发送**。
2. 在 **消息发送** 对话框中，单击 **SNMP 消息发送** 标签。请按以下说明设置选项。

启用 **SNMP** 消息发送

选择该项，以启用 Sophos Anti-Virus 发送 SNMP 消息。

要发送的消息

选择您想要 Sophos Anti-Virus 发送 SNMP 消息的事件。扫描错误 中包括 Sophos Anti-Virus 被拒绝访问试图扫描的项目的情况。

SNMP 陷阱目标

在文本框中，输入寄送警报的计算机的 IP 地址或名称。

SNMP 团体名

在文本框中，输入 SNMP 团体名。

测试

单击该按钮，发送 SNMP 测试消息到您所指定的 SNMP 陷阱

目标。

事件日志记录

要使 Sophos Anti-Virus 在发现安全隐患,或出现错误时,能够将警报添加到 Windows 2000 或以后的事件日志中,请按照以下说明做。这应用于读写扫描,即时扫描和单击右键扫描。

1. 在 **配置** 菜单中,单击 **消息发送**。
2. 在 **消息发送** 对话框中,单击 **事件日志** 标签。请按以下说明设置选项。

启用事件日志记录


选择该项,启用 Sophos Anti-Virus 向 Windows 事件日志寄送消息。

要发送的消息

选择您想要 Sophos Anti-Virus 发送消息的事件。扫描错误中包括 Sophos Anti-Virus 被拒绝访问试图扫描的项目的情况。

10 日志记录

查看本计算机的日志记录


 本计算机的日志记录是在本计算机上所进行的一切扫描活动的日志记录。

1. 在 **Sophos Anti-Virus** 窗口中的 主页里,单击 **配置 Sophos Anti-Virus**。
2. 在 **配置** 页中,单击 **查看和配置日志记录**,显示本计算机的日志记录。
3. 您可以从日志记录页中,复制日志记录到剪贴板,也可以用

电子邮件发送日志记录,或者,直接打印日志记录。

要在日志记录中查找特定的文本,单击 **查找** 并输入您想查找的文本内容。

配置本计算机的日志记录

 本计算机的日志记录是在本计算机上所进行的一切扫描活动的日志记录。

它存储在以下路径中：

C:\Documents and Settings\All Users\Application Data\Sophos\Sophos Anti-Virus\logs\SAV.txt

1. 在 **配置** 菜单中,单击 **日志记录**。
2. 在 **配置本计算机的日志记录** 对话框中,按照以下说明设置选项。


日志记录级别

要停止所有日志记录,单击 **无记录**。要记录摘要信息,出错消息等,单击 **普通记录**。要记录详细信息,包括被扫描的文件,扫描的主要阶段的情况等,单击 **详尽记录**。

日志记录归档

要启用每月归档日志文件,选择 **启用归档**。归档文件与日志文件存储在同一个文件夹中。选择 **归档文件数** 设定最旧的文件被删除前,所能存储的归档文件数。选择 **压缩日志记录** 以减少日志文件的大小。

查看即时扫描的日志记录

 即时扫描的日志记录是对最近一次运行即时扫描时所作的日志记录。


1. 在 **Sophos Anti-Virus** 窗口的 主页 中,在 可用的扫描 列

表中,选择您想要启用查看和配置日志记录的扫描。单击摘要。

2. 在摘要对话框中,单击底部的链接文字。
3. 您可以从日志记录窗口中,复制日志记录到剪贴板,也可以用电子邮件发送日志记录,或者,直接打印日志记录。

11 更新

即时更新


 如果您已经按照 Sophos 技术文档中所推荐的方式安装了 Sophos Anti-Virus,更新将会自动进行。

如果您想要即时更新 Sophos Anti-Virus,您可以这样做:

1. 找到系统托盘中的 Sophos Anti-Virus 图标(如下所示)。



2. 右击图标,弹出菜单,然后,选择 现在更新。

 或者,双击 Sophos Anti-Virus 系统托盘图标。


如果 Sophos Anti-Virus 已经正确地配置,它就会检查常规更新源中是否有新的软件,如有必要,就进行更新。

有关配置更新的信息,请见本部分的其它页面。

设置自动更新

如果您的计算机是在网络中,或者,您的网络管理员已经为您安装了 Sophos Anti-Virus,那么 Sophos Anti-Virus 应该已经配置了进行自动更新。

如果自动更新尚未设置,请进行以下步骤。有关每一步骤的选项的完整信息,请参见对该配置页作具体说明的部分。

 您需要成为 SophosAdministrator 组的成员，才能设置自动更新。

1. 找到系统托盘中的 Sophos Anti-Virus 图标 (如下所示)。



2. 右击图标，弹出菜单，然后，选择 **配置更新**。
3. 在 **Sophos AutoUpdate** 属性对话框中，单击 **主服务器** 标签和 设置更新源。您的网络管理员会提供给您所需要输入的详情。
4. 单击 **计划** 标签和 计划更新。

设置更新源

如果您想要 Sophos Anti-Virus 能够自动进行更新，您就必须为 Sophos Anti-Virus 指定获取更新文件的地方。


1. 找到系统托盘中的 Sophos Anti-Virus 图标 (如下所示)。



2. 右击图标，弹出菜单，然后，选择 **配置更新**。
3. 在 **Sophos AutoUpdate** 属性对话框中，单击 **主服务器** 标签并按照以下说明输入所需的详情。


地址

输入 Sophos Anti-Virus 通常可以获取更新文件的地址 (UNC (网络) 路径或网站地址)。如果您选择 **Sophos**，Sophos Anti-Virus 将通过因特网直接从 Sophos 下载更新文件。

 您的网络管理员可以提供您所需的地址和帐户的详情。

用户名

如有必要，在 **用户名** 中输入将用来接入服务器的帐户名，然后，输入并确认 **密码**。

 如果用户名需要指明域，才算合格有效，请使用“域\用户名”的形式。

如果您想限制所使用的带宽，单击 高级。

如果您是通过代理服务器接入因特网的，单击 应用，然后单击 代理详情。请注意，有的因特网服务提供商 (ISP)，要求将网页请求送到代理服务器上。

设置备用更新源

您可以设置一个备用更新源。如果 Sophos Anti-Virus 无法连接到常规的更新源，它会尝试从备用更新源进行更新。


1. 找到系统托盘中的 Sophos Anti-Virus 图标 (如下所示)。



2. 右击图标，弹出菜单，然后选择 **配置更新**。
3. 在 **Sophos AutoUpdate** 属性对话框，单击 **副服务器** 标签。然后，按照以下说明输入所需的详情。


地址

输入如果 Sophos Anti-Virus 无法连接到常规的更新源时，可以另外用来获取更新文件的地址 (UNC (网络) 路径或网站地址)。如果您选择 **Sophos**，Sophos Anti-Virus 将通过因特网直接从 Sophos 下载更新文件。

 您的网络管理员可以提供您所需的地址和帐户的详情。

用户名

如有必要，在用户名中输入将用来接入服务器的帐户名，然后，输入并确认密码。


 如果用户名需要指明域，才算合格有效，请使用“域\用户名”的形式。

如果您想限制所使用的带宽，单击 高级。

如果您是通过代理服务器接入该地址的，单击 **应用**，然后单击 **代理详情**。请注意，有的因特网服务提供商 (ISP)，要求将网页请求送到代理服务器上。

计划更新

您可以指定 Sophos Anti-Virus 进行的更新时间或频率。


 如果使用了管理控制台管理工作站上的 Sophos Anti-Virus，那么，在此所作的更改不会被理会。要避免这种情况，请参见控制台的帮助文件。

1. 找到系统托盘中的 Sophos Anti-Virus 图标 (如下所示)。



2. 右击图标，弹出菜单，然后选择 **配置更新**。
3. 在 **Sophos AutoUpdate** 属性对话框中，单击 **计划** 标签。然后，按照以下说明输入所需的详情。

如果您想要 Sophos Anti-Virus 以规律的间隔进行更新，请选择 **启用自动更新**。然后，输入更新频率 (以分钟为单位)，Sophos Anti-Virus 将按照此频率检查更新文件。默认值是 60 分钟。

 如果更新文件是直接 from Sophos 下载的，您的更新频率的设定值不能少于 60 分钟。

如果您是通过拨号连接因特网进行更新的，请选择 **在拨号连接时进行更新检查**。每当您连接到因特网时，Sophos Anti-Virus 就会尝试进行更新。

通过代理服务器更新

如果 Sophos Anti-Virus 是通过因特网来获取更新文件的，您就必须输入任何您用以连接到因特网的代理服务器的详情。

1. 找到系统托盘中的 Sophos Anti-Virus 图标 (如下所示)。



2. 右击图标,弹出菜单,然后选择 **配置更新**。
3. 在 **Sophos AutoUpdate** 属性对话框中,根据要求,单击 **主服务器** 标签或 **副服务器** 标签。确保准确无误地输入了所有的详情。然后,单击 **应用**,然后,单击 **代理明细**。
4. 在 **代理明细** 对话框中,选择 **通过代理接入服务器**。然后,输入代理服务器的 **地址** 和 **端口号**。输入用来接入代理服务器的 **用户名** 和 **密码**。如果用户名需要指明域,才算合格有效,请使用“域\用户名”的形式。

限制带宽使用量

您可以限制更新所使用的带宽量。这将避免在您需要一些带宽以作它用时(如:下载电子邮件),Sophos Anti-Virus 占用了所有的带宽。

1. 找到系统托盘中的 Sophos Anti-Virus 图标(如下所示)。



2. 右击图标,弹出菜单,然后选择 **配置更新**。
3. 在 **Sophos AutoUpdate** 属性对话框中,根据要求,单击 **主服务器** 标签或 **副服务器** 标签。然后,单击 **高级**。
4. 在 **高级设置** 对话框中,选择 **限制带宽使用量**,并使用滑动控制条指定以“千字节/每秒”为单位的带宽量。如果您指定的带宽量超过了计算机所能提供的量,Sophos Anti-Virus 将使用计算机能提供的所有带宽。

记录更新日志

您可以配置 Sophos Anti-Virus 以便在日志文件中记录更新活动。

1. 找到系统托盘中的 Sophos Anti-Virus 图标(如下所示)。



2. 右击图标，弹出菜单，然后选择 **配置更新**。
3. 在 **Sophos AutoUpdate** 属性对话框中，单击 **日志记录** 标签。确保选择 **记录 Sophos AutoUpdate** 活动。然后，按照以下说明设置其它选项。如果想打开日志文件，单击 **查看日志文件**。

日志文件最大尺寸


以兆字节 (MB) 为单位，设定日志文件的最大尺寸。

日志级别

您可以选择 **普通记录** 或 **详尽记录** 进行日志记录。详尽的日志记录提供比通常的活动多得多的活动的信息，因而，日志文件的尺寸也会快速增大。请只有在需要用它来处理出现的问题时，才使用这一设置。

12 进行清除

什么是清除？

 清除是把安全隐患从您的计算机中消除。具体地说，清除就是将病毒从文件或引导区中消除，移动或删除可疑文件，或者，删除广告软件 / 可能不想安装的应用程序。不过，清除并不能够将安全隐患已经实施的操作更改回去。

获取清除信息

当您的计算机中发现了安全隐患时，查看 Sophos 网站中的安全隐患分析，获取该安全隐患的相关信息，及其清除建议，是非常重要的。要做到这一点，您可以通过

- 桌面消息警报 (读写扫描)

- 扫描进程对话框 (即时扫描和单击右键扫描)
- 隔离区管理器 (所有扫描类型)

通过桌面消息警报获取信息

如果您的计算机中启用了读写扫描，Sophos Anti-Virus 会在发现安全隐患时，出现桌面消息警报。在消息框中，单击您想要获取相关信息的安全隐患的名称。

Sophos Anti-Virus 会将您连接到 Sophos 网站的安全隐患分析部分。

通过扫描进程对话框获取信息

在即时扫描，或从单击右键菜单中运行的扫描中，在扫描进程对话框 (或者，在扫描结束后，出现的扫描摘要对话框) 中的日志记录里，单击您想要了解的安全隐患的名称。

Sophos Anti-Virus 会将您连接到 Sophos 网站的安全隐患分析部分。

通过隔离区管理器获取信息

打开隔离区管理器。要打开隔离管理器，在 **Sophos Anti-Virus** 窗口中的 主页里，单击 管理隔离 项目。

在 名称 栏中，单击您想要了解的安全隐患的名称。

Sophos Anti-Virus 会将您连接到 Sophos 网站的安全隐患分析部分。

设置自动清除病毒 / 间谍软件




如果使用了管理控制台管理工作站上的 Sophos Anti-Virus，那么，在此所作的更改不会被理会。要避免这种情况，请参见控制台的帮助文件。

当读写扫描开启时，或者，当您运行即时扫描或单击右键扫描时，Sophos Anti-Virus 可以自动：

- 清除许多感染项目中的病毒。

- 以安全的方式处理没有进行清除的感染项目。

 在读写扫描中,无法自动清除多组件感染。要从计算机中清除多组件感染,请使用 隔离区管理器。


Sophos Anti-Virus 针对被感染项目所采取的任何措施,都会被记录在本计算机的日志记录或即时扫描的日志记录中。

要从您的计算机中彻底清除某些多组件感染,您需要重新启动计算机。如果出现这种情况,会有选项出现,您可以选择立即重新启动计算机,或者稍后重新启动计算机。在计算机重新启动之后,会进行清除的最终步骤。

1. 打开您想要配置的扫描类型的扫描设置对话框。(请参见 打开扫描设置对话框。)
2. 在扫描设置对话框中,单击 **清除** 标签。请按以下说明设置选项。


选择 **自动清除包含病毒 / 间谍软件** 的项目,使 Sophos Anti-Virus 能够清除软盘引导区,文档,程序,以及其它任何被选择的扫描项目中所感染的病毒 / 间谍软件。清除文档,并不会修复病毒已对文档造成的损害。(请参见 获取清除信息以了解,怎样从 Sophos 网站中查看有关病毒的破坏作用的详情。)

Sophos Anti-Virus 可以不进行清除,而用其它方式安全地处理被感染的文件。如果您没有使用自动清除功能,或者清除失败,您可以选择 Sophos Anti-Virus 采取您想要的其它措施来处理被感染的文件。不过,


 您应该只在 Sophos 技术支持的建议下才使用这些选项。否则,请使用 隔离区管理器 来清除 Sophos Anti-Virus 在您的计算机中发现的病毒 / 间谍软件。

单击 **删除** 可以丢弃文件。单击 **移至** 可以将感染病毒的移到,您通过使用 **浏览** 而选择的文件夹中。移走可执行文件,可以减少它们被运行的机会。


您无法自动移动多组件感染中的组件。

 要了解怎样通过隔离区管理器，清除您的计算机中的病毒 / 间谍软件，请参见 [处置隔离区中的病毒 / 间谍软件](#)。

设置自动清除可疑文件


 如果使用了管理控制台管理工作站上的 Sophos Anti-Virus，那么，在此所作的更改不会被理会。要避免这种情况，请参见控制台的帮助文件。

当读写扫描开启时，或者，当您运行即时扫描或单击右键扫描时，Sophos Anti-Virus 可以自动删除或移动可疑文件。


 可疑文件 是可能感染了尚无法具体识别的病毒的文件。

Sophos Anti-Virus 针对可疑文件所采取的任何措施，都会被记录在本计算机的日志记录_或_即时扫描的日志记录_中。

1. 打开您想要配置的扫描类型的扫描设置对话框。（请参见 [打开扫描设置对话框](#)。）
2. 在扫描设置对话框中，单击 **清除** 标签。在 **可疑文件** 窗格板中，按照以下说明设置选项。


 您应该只在 Sophos 技术支持的建议下才使用这些选项。否则，请使用 [隔离区管理器来清除 Sophos Anti-Virus 在您的计算机中发现的可疑文件](#)。

单击 **删除** 可以丢弃文件。单击 **移至** 可以将感染病毒的移到，您通过使用 **浏览** 而选择的文件夹中。移走可执行文件，可以减少它们被运行的机会。

 要了解怎样通过隔离区管理器，清除您的计算机中的可疑文件，请参见 [处置隔离区中的可疑文件](#)。

设置自动清除广告软件 / 可能不想安装的应用程序


当您运行即时扫描，或单击右键扫描时，Sophos Anti-Virus 能够自动清除您的计算机中的广告软件 / 可能不想安装的应用程序。

 在读写扫描中，不能对广告软件 / 可能不想安装的应用程序进行自动清除。要从您的计算机中清除广告软件 / 可能不想安装的应用程序，请使用 隔离区管理器。

Sophos Anti-Virus 针对广告软件 / 可能不想安装的应用程序所采取的任何措施，都会被记录在 本计算机的日志记录_或_即时扫描的日志记录_中。

要从您的计算机中彻底清除某些涉及数个组件的广告软件 / 可能不想安装的应用程序，您需要重新启动计算机。如果出现这种情况，会有选项出现，您可以选择立即重新启动计算机，或者稍后重新启动计算机。在计算机重新启动之后，会进行清除的最终步骤。

1. 打开您想要配置的扫描类型的扫描设置对话框。（请参见 打开扫描设置对话框。）
2. 在扫描设置对话框中，单击 清除 标签。
3. 选择 自动清除广告软件 / 可能不想安装的应用程序 可以使 Sophos Anti-Virus 为所有用户删除在计算机上发现的，广告软件 / 可能不想安装的应用程序的所有组件。对此所作的清除，并不会修复广告软件 / 可能不想安装的应用程序，已经对计算机所做的任何改变。（请参见 获取清除信息以了解怎样从 Sophos 网站中查看有关广告软件 / 可能不想安装的应用程序的破坏作用的详情。）

 要了解怎样通过隔离区管理器，清除您的计算机中的广告软件 / 可能不想安装的应用程序，请参见 处置隔离区中的广告软件 / 可能不想安装的应用程序。

运行完全的计算机扫描

在 Sophos Anti-Virus 能够将安全隐患从您的计算机中清除之前，您可能需要对计算机进行完全扫描，检测多组件安全隐患或广告软件 / 可能不想安装的应用程序所涉及的所有组件。

1. 要扫描计算机上的所有硬盘，包括其引导扇区，请运行 扫描我的电脑。要了解具体怎样做，请参见 扫描我的电脑。

2. 如果安全隐患或广告软件 / 可能不想安装的应用程序还是没有被彻底检测到, 这可能是因为您的读写权限不足, 或者, 因为计算机中有些含有广告软件 / 可能不想安装的应用程序的组件的驱动器, 或文件夹, 被排除在了扫描之外。请检查排除扫描项目的列表。要了解具体怎样做, 请参见 从扫描中排除项目。如果有些项目在列表中, 请将这些项目从列表中删除, 然后再次扫描您的计算机。

如果您没有足够的权限扫描您的整个计算机, 请与您的系统管理员。

Sophos Anti-Virus 可能不能够彻底检测到或者删除, 有组件安装在网络驱动器上的广告软件 / 可能不想安装的应用程序。


欲寻求建议, 请联系 Sophos 技术支持。

13 管理隔离项目

什么是隔离区管理器？


隔离区管理器使您能够处置, 在运行扫描时发现的, 并且没有自动清除的项目。隔离区中的每个项目, 都是由于以下之一的某个原因, 而被隔离的。

- 在发现该项目的那个扫描类型的设置中, 没有选择清除选项 (清除, 删除, 移动)。
- 在发现该项目的那个扫描类型的设置中, 已经选择了清除选项, 但是该选项不起作用。
- 该项目受到多重感染, 并且仍然含有其它的安全隐患。
- 该安全隐患只是部分地被检测到, 需要进行完整的计算机扫描, 才能彻底检测该安全隐患。要了解具体怎样做, 请参见 运行完整的计算机扫描。
- 具有可疑行为的项目。
- 受控程序项目。

 在读写扫描中检测到的，广告软件 / 可能不想安装的应用程序和组件感染，会在隔离区管理器中列表显示。在读写扫描中，不能对广告软件 / 可能不想安装的应用程序和组件感染进行自动清除。

清除选项不起作用，因为没有足够的访问权限。如果您拥有更大的权限，您可以使用隔离区管理器处置项目。

处置隔离区中的病毒 / 间谍软件

 这里所称的 **病毒** 是指任何病毒，蠕虫，特洛伊木马，或者其他恶意软件。

1. 打开隔离区管理器。要打开隔离管理器，在 **Sophos Anti-Virus** 窗口的 主页 中，单击 管理隔离项目。
2. 在 **隔离区管理器** 页面中，单击 **显示** 框中的下拉箭头，然后，选择 **病毒 / 间谍软件**。

被感染项目的详情

有关每个项目的信息都显示在此栏中。

名称 显示 Sophos Anti-Virus 检测到的项目名称。要了解更多关于该病毒 / 间谍软件的信息，单击该名称，然后 Sophos Anti-Virus 会将您连接到 Sophos 网站的病毒 / 间谍软件分析部分。

详情 显示项目的名称和路径。如果有 **更多信息** 链接出现在文件名旁，这说明该项目是多组件感染。单击该链接，可以查看其它的感染组件的列表。

可用措施 显示您可以针对该项目所采取的措施。有三种措施可以采用：清除，删除，移动，说明如下。如果您单击其中一个措施，该措施会在该项目上执行，并会给与确认信息。

处置感染项目

要处置病毒 / 间谍软件，请使用以下说明的按钮。

全选 / 取消全选

单击这两个按钮可以全选，或者取消全选所有的项目。这使您能够针对一组项目，同时施行相同的措施。要勾选或者取消勾选特定的项目，请勾选项目类型左边的勾选框。

从列表中清除

单击它，可以将所选的项目从列表中清除，如果您确信这些项目中不含有病毒 / 间谍软件。不过，这并不会从磁盘中删除该项目。

执行操作

单击它，可以显示您可以针对所选项目而执行的操作的列表。

单击 **清除** 可以删除所选项目中的病毒 / 间谍软件。清除文档，并不会修复病毒已对文档造成的损害。



要从您的计算机中彻底清除某些涉及数个组件的病毒 / 间谍软件，您需要重新启动计算机。如果出现这种情况，会有选项出现，您可以选择立即重新启动计算机，或者稍后重新启动计算机。在计算机重新启动之后，会进行清除的最终步骤。

单击 **删除** 可以从您的计算机中删除所选项目。请谨慎使用此功能。

单击 **移至** 可以将所选的项目移至其它文件夹。这些项目所移至的文件夹，是在设置清除时，所指定的那个文件夹。移走可执行文件，可以减少它们被运行的机会。请谨慎使用此功能。




有些时候，如果您删除或者移除了某个被感染的文件，您的计算机系统可能会工作不正常，因为无法找到该文件。还有，某个被感染的文件可能仅仅只是多重感染的一部分。在这种情况下，删除或移除某个特定的文件，并不能彻底清除计算机中的感染。出现这种情况时，请联系 [Sophos 技术支持](#) 寻求处置该项目的帮助。

要配置您可以执行何种措施，请参见 [配置用户使用隔离区管](#)

理器的权限。

处置隔离区中的可疑行为

 可疑行为 是看起来带有恶意的程序活动。

1. 打开隔离区管理器。要打开隔离管理器，在 **Sophos Anti-Virus** 窗口的 主页中，单击 管理隔离项目。
2. 在 **隔离区管理器** 页面中，单击 **显示** 框中的下拉箭头，然后，选择 **可疑行为**。

可疑行为详情

有关每个项目的信息都显示在此栏中。

名称 显示 Sophos Anti-Virus 检测到的项目名称。要了解更多关于该可疑行为的信息，单击该名称，然后 Sophos Anti-Virus 会将您连接到 Sophos 网站的可疑行为分析部分。

详情 显示项目的名称和路径。

可用措施 显示您可以针对该项目所采取的措施。如果您已启用了阻断可疑行为，可采用的措施为：**批准**，说明如下。如果您单击该措施，该措施会在该项目上执行，并会给与确认信息。

处置可疑行为

要处置可疑行为，请使用以下说明的按钮。

全选 / 取消全选

单击这两个按钮可以全选，或者取消全选所有的项目。这使您能够针对一组项目，同时施行相同的措施。要勾选或者取消勾选特定的项目，请勾选项目类型左边的勾选框。

从列表中清除

如果您信任该项目，单击该按钮，可以将所选择的项目从列表中清除。不过，这并不会从磁盘中删除该项目。

执行操作


单击它，可以显示您可以针对所选项目而执行的操作的列表。

单击 **批准** 以批准所选项目在计算机上运行，如果您信任这些项目。这会将项目添加到已批准的可疑项目的列表中，这样 Sophos Anti-Virus 将不会阻止该行为。

要配置您可以执行何种措施，请参见 [配置用户使用隔离区管理器的权限](#)。

要查看已批准的可疑行为，请单击 **配置批准**。

处置隔离区中的可疑文件

 **可疑文件** 是可能感染了尚无法具体识别的病毒的文件。

1. 打开隔离区管理器。要打开隔离管理器，在 **Sophos Anti-Virus** 窗口的 [主页](#) 中，单击 **管理隔离项目**。
2. 在 **隔离区管理器** 页面中，单击 **显示** 框中的下拉箭头，然后，选择 **可疑文件**。

可疑文件详情

有关每个项目的信息都显示在此栏中。

名称 显示 Sophos Anti-Virus 检测到的项目名称。要了解更多关于该可疑文件的信息，单击该名称，然后 Sophos Anti-Virus 会将您连接到 Sophos 网站的可疑文件分析部分。

详情 显示项目的名称和路径。

可用措施 显示您可以针对该项目所采取的措施。有三种措施可以采用：**批准**，**删除**，**移动**，说明如下。如果您单击其中一个措施，该措施会在该项目上执行，并会给与确认信息。

处置可疑文件

要处置可疑文件，请使用以下说明的按钮。

全选 / 取消全选

单击这两个按钮可以全选，或者取消全选所有的项目。这使您能够针对一组项目，同时施行相同的措施。要勾选或者取消勾选特定的项目，请勾选项目类型左边的勾选框。

从列表中清除

如果您信任该项目，单击该按钮，可以将所选择的项目从列表中清除。不过，这并不会从磁盘中删除该项目。


执行操作

单击它，可以显示您可以针对所选项目而执行的操作的列表。

单击 **批准** 以批准所选项目在计算机上运行，如果您信任这些项目。这会将项目添加到已批准的可疑项目的列表中，这样 Sophos Anti-Virus 将不会阻止对这些文件的访问。

单击 **删除** 可以从您的计算机中删除所选项目。请谨慎使用此功能。

单击 **移至** 可以将所选的项目移至其它文件夹。这些项目所移至的文件夹，是在设置清除时，所指定的那个文件夹。移走可执行文件，可以减少它们被运行的机会。请谨慎使用此功能。

 有些时候，如果您删除或者移除了某个可疑文件，您的计算机系统可能会工作不正常，因为无法找到该文件。

要配置您可以执行何种措施，请参见 [配置用户使用隔离区管理器的权限](#)。

要查看已批准的可疑文件，请单击 **配置批准**。

处置隔离区中的广告软件 / 可能不想安装的应用程序

1. 打开隔离区管理器。要打开隔离管理器，在 **Sophos Anti-**

Virus 窗口的主页中,单击 管理隔离项目。

2. 在 **隔离区管理器** 页面中,单击 **显示** 框中的下拉箭头,然后,选择 **广告软件 / 可能不想安装的应用程序**。

广告软件 / 可能不想安装的应用程序详情

有关每个项目的信息都显示在此栏中。

名称 显示 Sophos Anti-Virus 检测到的项目名称。要了解更多关于该广告软件 / 可能不想安装的应用程序的信息,单击该名称,然后 Sophos Anti-Virus 会将您连接到 Sophos 网站的广告软件 / 可能不想安装的应用程序分析部分。

详情 显示广告软件 / 可能不想安装的应用程序的子类型。如果有 **更多信息** 链接出现在子类型旁,这说明该项目是多组件的广告软件 / 可能不想安装的应用程序。单击该链接,可以查看其它的广告软件 / 可能不想安装的应用程序组件的列表。

可用措施 显示您可以针对该项目所采取的措施。有两种措施可以采用:批准和清除,说明如下。如果您单击其中一个措施,该措施会在该项目上执行,并会给与确认信息。

处置广告软件 / 可能不想安装的应用程序

要处置广告软件 / 可能不想安装的应用程序,请使用以下说明的按钮。

全选 / 取消全选

单击这两个按钮可以全选,或者取消全选所有的项目。这使您能够针对一组项目,同时施行相同的措施。要勾选或者取消勾选特定的项目,请勾选项目类型左边的勾选框。

从列表中清除

如果您信任该项目,单击该按钮,可以将所选择的项目从列表中清除。不过,这并不会从磁盘中删除该项目。

执行操作

单击它，可以显示您可以针对所选项目而执行的操作的列表。

单击 **批准** 以批准所选项目在计算机上运行，如果您信任这些项目。这会将项目添加到已批准的广告软件 / 可能不想安装的应用程序的列表中，这样 Sophos Anti-Virus 将不会阻止该项目在您的计算机上运行。

单击 **清除** 以从所有用户的计算机上删除所选项目的所有已知组件。要从计算机中清除广告软件 / 可能不想安装的应用程序，用户必须同时是 Windows Administrators 和 SophosAdministrator 组的成员。




要从您的计算机中彻底清除某些涉及数个组件的广告软件 / 可能不想安装的应用程序，您需要重新启动计算机。如果出现这种情况，会有选项出现，您可以选择立即重新启动计算机，或者稍后重新启动计算机。在计算机重新启动之后，会进行清除的最终步骤。

要配置您可以执行何种措施，请参见 [配置用户使用隔离区管理器的权限](#)。

要查看已知的和已批准的广告软件 / 可能不想安装的应用程序，请单击 **配置批准**。

处置隔离区中的受控程序

 **受控程序** 是正当的客户应用程序，但它会影响工作效率，以及网络运行效率。

1. 打开隔离区管理器。要打开隔离管理器，在 **Sophos Anti-Virus** 窗口的 主页中，单击 管理隔离项目。
2. 在 **隔离区管理器** 页面中，单击 **显示** 框中的下拉箭头，然后，选择 **受控程序**。

受控程序详情

有关每个项目的信息都显示在此栏中。

名称 显示 Sophos Anti-Virus 检测到的项目名称。要了解更多关于该受控程序的信息，单击该名称，然后 Sophos Anti-Virus 会将您连接到 Sophos 网站的受控程序分析部分。

详情 显示受控程序的子类型。如果 **更多信息** 的链接出现在子类型旁，单击它可以查看受控程序的其它组件的列表。

可用措施 显示您可以针对该项目所采取的措施。不过，除了以下说明的，从列表中清空该项目之外，没有措施可以用于受控程序。

处置受控程序

要处置受控程序，请使用以下说明的按钮。


全选 / 取消全选

单击这两个按钮可以全选，或者取消全选所有的项目。这使您能够针对一组项目，同时施行相同的措施。要勾选或者取消勾选特定的项目，请勾选项目类型左边的勾选框。

从列表中清除

单击该按钮，可以从列表中删除所选择的项目。不过，这并不会从磁盘中删除该项目。受控程序必须通过中央控制台批准之后，才能使用。

配置用户使用隔离区管理器的权限

 您需要成为 SophosAdministrator 组的成员，才能更改这些设置。

1. 在 **配置** 菜单中，单击 **用户使用隔离区管理器的权限**。
2. 在 **配置用户使用隔离区管理器的权限** 对话框中，选择可以执行每种类型的措施的不同级别的用户。有关用户类型的更多信息，请参见 用户类型。请记住您在此所设定的用户权限，仅适用于隔离区管理器。每种类型的措施解释如下。

清除扇区

这是指清除软盘的启动区。

清除文件

这是指清除文档和程序。对文档所作的清除，并不会修复病毒已对文档所作的任何改变。对程序所作的清除，应该只是作为一种临时的措施。您应该接着就用原盘或者无病毒的备份，重新替换被清除过的程序。

删除文件


这是指丢弃被感染的文件。

移动文件

这是指将被感染的文件移至其它文件夹。移走可执行文件，可以减少它们被运行的机会。


批准

这是指批准可疑项目和广告软件 / 可能不想安装的应用程序，以便它们能够在计算机上运行。它应用于“批准管理器”和“隔离区管理器”。

 要清除广告软件 / 可能不想安装的应用程序，用户必须同时是 Windows Administrators 和 SophosAdministrator 组的成员。

14 批准使用项目


批准使用广告软件 / 可能不想安装的应用程序

 如果使用了管理控制台管理工作站上的 Sophos Anti-Virus，那么，在此所作的更改不会被理会。要避免这种情况，请参见控制台的帮助文件。


如果您想运行被 Sophos Anti-Virus 归类为可能不想安装的应用程序的某个广告软件或应用程序，您可以按照以下说明批准它。

1. 在 **配置** 菜单中,单击 **批准**。
2. 在 **批准管理器** 对话框中,单击 **广告软件 / 可能不想安装** 的应用程序 标签。
3. 在 **已知的广告软件 / 可能不想安装的应用程序** 列表框中,选择您想批准的广告软件 / 可能不想安装的应用程序,然后单击 **添加**。该广告软件 / 可能不想安装的应用程序将会出现在 **已批准的广告软件 / 可能不想安装的应用程序** 列表框中。

如果您不想要当前已批准的广告软件 / 可能不想安装的应用程序运行,请在 **已批准的广告软件 / 可能不想安装的应用程序** 列表中选择它们,然后单击 **删除**。


 您也可以在隔离区管理器中批准广告软件 / 可能不想安装的应用程序。有关怎样在隔离区管理器中批准广告软件 / 可能不想安装的应用程序的信息,请参见 [处置隔离区中的广告软件 / 可能不想安装的应用程序](#)。

批准使用可疑项目

 如果使用了管理控制台管理工作站上的 Sophos Anti-Virus,那么,在此所作的更改不会被理会。要避免这种情况,请参见控制台的帮助文件。

如果您想运行被 Sophos Anti-Virus 归类为可疑项目的项目,您可以按照以下说明预批准它。

1. 在 **配置** 菜单中,单击 **批准**。
2. 在 **批准管理器** 对话框中,单击被检测到的项目的类型的标签页 (如 **:缓冲区溢出**)。
3. 要批准该项目,请在 **已知项目** 列表中选择它,然后将它移动到 **已批准项目** 列表。

 您还可以在隔离管理器中批准可疑项目。欲了解怎样在隔离管理器中批准可疑项目的有关信息,请参见 [处置隔离区中的可疑文件](#) 以及 [处置隔离区中的可疑行为](#)。

如果您想运行尚未被 Sophos Anti-Virus 归类为可疑项目的项

目，您可以按照以下说明预批准它。

1. 单击 新项目。
2. 浏览找到该项目，并选择和添加它到 已批准项目 列表中。

15 排疑解难

系统托盘图标上出现白色的叉

如果在 Sophos Anti-Virus 系统托盘图标上出现红色的圈和在其中有个白色的叉，这说明更新失败了。



要了解更多的更新失败的信息，可查看更新日志。右击 Sophos Anti-Virus 系统托盘图标，弹出菜单。选择 配置更新。然后，单击 日志记录 标签，并单击 查看日志文件。

以下各节将解释，为什么更新可能会失败，以及您可以怎样更改设置，以解决这个问题。



您需要成为 SophosAdministrator 组的成员，才能更改更新设置。

Sophos Anti-Virus 联系的是错误的更新源

1. 右击 Sophos Anti-Virus 系统托盘图标，弹出菜单。选择 配置更新。
2. 单击 主服务器 标签。请核查由您的网络管理员所提供的地址和帐户的细节。

Sophos Anti-Virus 无法使用您的代理服务器

如果您的 Sophos Anti-Virus 是经由因特网进行更新的，您必须确保您设定代理服务器 (如果有) 是可以使用的。

1. 右击 Sophos Anti-Virus 系统托盘图标，弹出菜单。选择 配置更新。

2. 单击 **主服务器** 标签。然后,单击 **代理明细**。
3. 在 **代理明细** 对话框中,输入代理服务器的地址和端口号,以及帐户详情。

没有正确地计划安排自动更新

1. 右击 Sophos Anti-Virus 系统托盘图标,弹出菜单。选择 **配置更新**。
2. 单击 **计划** 标签。如果您的计算机是在网络中的,或者您的计算机是通过宽带连接因特网进行更新的,请选择 **启用自动更新**,并输入更新频率。如果您是通过拨号连接因特网进行更新的,请选择 **在拨号连接时进行更新检查**。

没有保留更新源

您的公司可能已经移走了,您通过其进行更新(在网络中,或者在网页服务器中)的目录。另一种情况是,他们可能没有保留该目录。如果您认为可能是这种情况,请联系您的网络管理员。

系统托盘图标呈灰白显示

如果 Sophos Anti-Virus 系统托盘图标呈灰白显示,说明该计算机没有受到读写扫描的保护。



要为该计算机上的所有用户启用读写扫描,请参见 [为计算机开启或关闭扫描保护](#)。

没有清除安全隐患

如果 Sophos Anti-Virus 没有从您的计算机上清除安全隐患,这可能是由于以下的原因。

自动清除被禁用

如果 Sophos Anti-Virus 没有试图进行清除,请检查是否已启用

了自动清除。要启用自动清除功能,请参见 [清除](#)。在读写扫描中,不能对广告软件 / 可能不想安装的应用程序进行自动清除。

清除失败

如果 Sophos Anti-Virus 无法清除安全隐患 ("清除失败"),这可能是因为它无法清除该类型的安全隐患,或者,您没有足够的读写权限。

要求完全的计算机扫描

在 Sophos Anti-Virus 能够将安全隐患从您的计算机中清除之前,您可能需要对计算机进行完全扫描,检测多组件安全隐患所涉及的所有组件。

1. 要扫描计算机上的所有硬盘,包括其引导扇区,请运行 [扫描我的电脑](#)。
2. 如果安全隐患还是没有被彻底检测到,这可能是因为您的读写权限不足,或者,因为计算机中有些含有安全隐患的组件的驱动器,或文件夹,被排除在扫描外。[请检查排除扫描项目的列表](#)。如果有些项目在列表中,请将这些项目从列表中删除,然后,再次扫描您的计算机。

可移动介质被写保护

如果处理的是可移动介质 (如 :软盘 ,CD),请确保它没有被写保护。

NTFS 卷被写保护

如果处理的是 NTFS 卷 (Windows 2000 或以后),请确保它没有被写保护。

报告发现病毒 / 间谍软件碎片

Sophos Anti-Virus 不会对病毒 / 间谍软件碎片进行清除,因为它并没有发现与之确切对应的病毒 / 间谍软件。请参见 [报告发现病毒 / 间谍软件碎片](#)。

报告发现病毒 / 间谍软件碎片

如果报告发现了病毒 / 间谍软件碎片，请更新受到影响的计算机上的 Sophos Anti-Virus，以便得到最新的病毒识别文件。然后，运行扫描该计算机。如果仍然报告发现病毒 / 间谍软件碎片，请联系 [Sophos 技术支持寻求建议](#)。

报告病毒 / 间谍软件碎片，表明文件的某一部分与病毒 / 间谍软件的某一部分一致。出现这种情况，可能有三种原因：

已知病毒 / 间谍软件的变种

许多新病毒 / 间谍软件都是建立在已知病毒 / 间谍软件的基础之上的，所以某些已知病毒 / 间谍软件的典型的病毒 / 间谍软件代码的碎片，就可能会出现在新的病毒 / 间谍软件中。如果报告发现了病毒 / 间谍软件碎片，这就有可能是 Sophos Anti-Virus 发现了有可能会活动起来的新的病毒 / 间谍软件。

已损坏的病毒

许多病毒在复制自身的过程中出现缺陷，这使得它们在感染目标文件时出错。病毒中不能起作用的部分 (可能是实质部分) 就可能出现在宿主文件中，而 Sophos Anti-Virus 检测到的就是这一部分。已损坏的病毒是不会传播的。

含有病毒 / 间谍软件的数据库

在运行完全的扫描时，Sophos Anti-Virus 可能会报告在数据库文件中有病毒 / 间谍软件碎片。如果出现这种情况，不要删除该数据库。请联系 [Sophos 技术支持寻求建议](#)。

部分检测到的安全隐患

如果 Sophos Anti-Virus 部分检测到了安全隐患 (特洛伊木马或广告软件 / 可能不想安装的应用程序)，那么，就需要对计算机的进行完全扫描，以检测该安全隐患的所有组件。

1. 要扫描计算机上的所有硬盘，包括其引导扇区，请运行 [扫描我的电脑](#)。

2. 如果安全隐患还是没有被彻底检测到，这可能是因为您的读写权限不足，或者因为计算机中有些含有安全隐患的组件的驱动器，或文件夹，被排除在扫描外。请检查排除扫描项目的列表。如果有些项目在列表中，请将这些项目从列表中删除，然后，再次扫描您的计算机。

Sophos Anti-Virus 可能不能够彻底检测到或者删除，有组件安装在网络驱动器上的安全隐患。

欲寻求建议，请联系 [Sophos 技术支持](#)。

从隔离区中消失的广告软件 / 可能不想安装的应用程序

如果被 Sophos Anti-Virus 检测到的广告软件 / 可能不想安装的应用程序，未经您采取任何措施，就从隔离区管理器中消失，那么，该广告软件 / 可能不想安装的应用程序可能已被其它用户通过 Sophos Enterprise Console 批准可以使用，或者清除。请检查已批准的广告软件 / 可能不想安装的应用程序列表，查看该项目是否已被批准。要了解具体怎样做，请参见 [批准使用广告软件 / 可能不想安装的应用程序](#)。

计算机的运行变慢

如果您的计算机的运行变慢，这有可能是有可能不想安装的应用程序，正在您的计算机上运行和监控。如果您启用了读写扫描，您也许可能会看到许多桌面消息警报，提醒您发现了可能不想安装的应用程序。要解决这一问题，请按照以下说明做。


1. 运行 [扫描我的电脑](#)，以检测该可能不想安装的应用程序的所有组件。



如果在扫描之后，该可能不想安装的应用程序只是部分被检测到，则请参见 [部分检测到的安全隐患中的步骤 2](#)。


2. 清除您的计算机上的广告软件 / 可能不想安装的应用程序。要了解具体怎样做，请参见 [处置隔离区中的广告软件 / 可能不想安装的应用程序](#)。

无法访问引导区感染了病毒的磁盘

 如果使用了管理控制台管理工作站上的 Sophos Anti-Virus，那么，在此所作的更改不会被理会。要避免这种情况，请参见控制台的帮助文件。

依照默认值，Sophos Anti-Virus 会阻止访问引导区感染了病毒的可移动介质。要访问它们（如：从感染了引导区病毒的软盘上复制文件），请按以下说明做：

1. 在 **配置** 菜单中，单击 **读写扫描**。
2. 在本计算机的读写扫描设置对话框，单击 **扫描** 标签。
3. 选择 **允许访问引导区感染病毒的驱动器**。

 在您访问完毕该磁盘后，请取消勾选该选项。请将磁盘从计算机中移走，这样它就不可能在计算机重新启动时，再次感染计算机。

无法访问 Sophos Anti-Virus 的某些部分

如果您无法使用或者配置 Sophos Anti-Virus 的某些特定部分，这可能是由于，特定类型的用户访问这些部分受到限制。请参见 *限制访问权限*。

弥补安全隐患造成的破坏

本部分包括以下内容。

- 弥补病毒造成的破坏
- 弥补广告软件 / 可能不想安装的应用程序造成的破坏

弥补广告软件 / 可能不想安装的应用程序造成的破坏

在清除广告软件 / 可能不想安装的应用程序的过程中，并不一定能完全弥补已造成的破坏。

操作系统已被修改

某些广告软件 / 可能不想安装的应用程序会修改 Windows 操作系统, 比如, 更改您的因特网连接设置。Sophos Anti-Virus 无法总能够将系统中的设置, 恢复到被安装了广告软件 / 可能不想安装的应用程序之前的值。比如, 如果某个广告软件 / 可能不想安装的应用程序, 更改了浏览器的默认主页, 但 Sophos Anti-Virus 是无法知道先前的那个默认主页是什么的。

没有清除的实用小程序

某些广告软件 / 可能不想安装的应用程序会安装一些实用小程序到您的计算机上, 如扩展名为 .dll 或 .ocx 等的文件。如果这些实用小程序是无害的 (也就是说, 它们并不具有广告软件 / 可能不想安装的应用程序的那些特性), 比如, 某个语言库, 而且也没有被整合到广告软件 / 可能不想安装的应用程序中, 那么, Sophos Anti-Virus 并不会将其检测为广告软件 / 可能不想安装的应用程序的一部分。在这种情况下, 这样的文件不会在广告软件 / 可能不想安装的应用程序被清除后, 也被从计算机中清除。

广告软件 / 可能不想安装的应用程序是您所需要的软件程序的一部分

有时候某些广告软件 / 可能不想安装的应用程序, 是您想要安装的软件程序的一部分, 并且是运行该软件程序所必需的。如果您删除这样的广告软件 / 可能不想安装的应用程序, 则整个软件程序可能会停止在您的计算机上运行。

做些什么?

阅读 Sophos 网站中的安全隐患分析部分是很重要的。请参见 [获取清除信息](#) 以了解怎样从 [Sophos 网站](#) 中查看有关广告软件 / 可能不想安装的应用程序的破坏作用的详情。

为了能够将您的系统及其设置恢复到先前的状态, 您应该定时备份您的系统。您还应该备份, 您想要使用的软件的原始的可执行程序文件。欲知更多有关弥补广告软件 / 可能不想安装的应用程序造成的破坏的信息和建议, 请联系 [Sophos 技术支持](#)。

报告密码错误

如果您在计划一次扫描时，出现有关密码的出错信息，那么，请确认：

- 帐户的密码是否正确
- 密码不能为空

请使用‘控制面板’查看帐户的属性，来检查密码是否正确。(必要时请参考您的 Windows 技术文档)。

技术支持

欲获取技术支持，请访问 www.sophos.com/support。

如果您要与技术支持联系，请提供尽量多的信息，包括：

- Sophos 软件版本号
- 操作系统和补丁包级别
- 出错信息的原文

索引

M

Macintosh 文件 , 扫描 24

S

SNMP 消息发送 28

Sophos Anti-Virus

窗口 , 用户界面 , GUI , 工具栏 , 状态 , 帮助和信息 , 活动摘要 , 可用的扫描 , 主页 5

Z

本计算机的日志记录 30

编辑扫描 , 即时扫描 13

病毒 , 间谍软件 , 清除 , 清除感染 42

部分检测到的安全隐患 , 部分检测 55

打包文件 , 扫描 23

代理服务器 34

带宽 35

单击右键扫描 8

单击右键扫描 , 扫描 , 单个项目扫描 14

电子邮件警报发送 26

读写扫描 8

访问磁盘 57

访问权限 49

访问权限 , 用户权限 , 用户组 57

副服务器 33

感染了病毒的引导区 57

更新 , 即时更新 31

更新 , 系统托盘图标 , Sophos Anti-Virus 系统托盘图标 , 盾牌图标 52

广告软件 , 可能不想安装的应用程序 56

广告软件 , 弥补造成的破坏 , 可能不想安装的应用程序 , 造成的破坏 57

广告软件 , 清除 , 可能不想安装的应用程序 , 批准 46

即时扫描 8

计划更新 , 更新 34

计划扫描 , 即时扫描 12

记录更新日志 , 更新 35

技术支持 , 支持 59

检查扫描保护是否开启 , 监控读写扫描 , 保护 , 读写扫描 , 系统托盘图标 , Sophos Anti-Virus 系统托盘图标 , 盾牌图标 9

开启或关闭扫描保护 , 启动读写扫描 , 停止读写扫描 , 读写扫描 , 保护 9

可能不想安装的应用程序 , 广告软件 , 扫描 22

可疑文件 , 清除 , 批准 45

可疑文件 , 扫描 22

- 可疑行为,批准,缓冲区溢出 44
- 可用扫描,即时扫描 12
- 排除扫描的项目 19

- 批准,广告软件,可能不想安装的应用程序 50

- 批准,可疑行为,可疑文件,缓冲区溢出 51
- 清除,清除感染 36

- 清除,清除感染,安全隐患分析,安全信息,清除信息 36
- 清除,清除感染,碎片 53
- 扫描,即时扫描 10
- 扫描的日志记录 30

- 扫描的文件类型,扫描的文件扩展名,扫描,全部文件:扫描 18
- 扫描级别,扫描,扩展的扫描 24
- 设置扫描,创建扫描,即时扫描 11
- 事件日志记录 29
- 碎片 55
- 图标:要扫描的项目 14
- 完全的计算机扫描 40
- 为计算机上的所有用户更改设置 17
- 为所有计算机更改设置,中央配置 16
- 系统托盘图标,Sophos Anti-Virus 系统托盘图标,盾牌图标 53
- 用户权限 49
- 用户组 49
- 用户组,访问权限,用户权限 15
- 用户组,用户权限,访问权限 16

- 运行慢的计算机 56
- 运行时行为分析 8

- 运行时行为分析,可疑行为,缓冲区溢出,检测 25
- 主服务器 32
- 桌面消息发送 26
- 自动更新,更新 31
- 自动清除,清除,病毒,间谍软件 37

- 自动清除,清除,广告软件,可能不想安装的应用程序 39
- 自动清除,清除,可疑文件 39