

# SOPHOS

## CONTROL CENTER 2.0

### 用戶手冊

文档日期：2006 年 9 月





# 目录

<b>1 关于 Sophos 小企业解决方案(SBS)</b>	<b>4</b>
1.1 Sophos 小企业解决方案(SBS)概览	4
<b>2 关于 Sophos Control Center</b>	<b>4</b>
2.1 什么是 Sophos Control Center ?	5
2.2 关于 Sophos Control Center 用户界面	5
2.3 图标的含义	7
<b>3 怎样学会使用 ?</b>	<b>8</b>
3.1 学会使用 Sophos Control Center	8
3.2 保护网络中的计算机	8
3.3 手动保护计算机	9
<b>4 怎样清除安全隐患 ?</b>	<b>9</b>
4.1 发现了安全隐患时会怎样 ?	10
4.2 清除病毒	10
4.3 清除可能不想安装的应用程序	11
4.4 清除防火墙检测到的安全隐患	12
4.5 查找有关安全隐患的信息	12
4.6 设置自动清除	12
4.7 处理出错警报	13
<b>5 怎样升级计算机 ?</b>	<b>13</b>
5.1 最近一次升级发生在何时 ?	14
5.2 下一次升级发生在何时 ?	14
5.3 升级成功吗 ?	14
5.4 怎样获得有关升级问题的警报 ?	14
5.5 关闭自动升级	15
5.6 手动升级	15
5.7 升级个别的计算机	15
<b>6 怎样配置升级 ?</b>	<b>15</b>
6.1 更改升级内容	16
6.2 通过代理服务器升级	16
6.3 更改用于升级的用户ID	16
6.4 关闭自动升级	16

6.5 更改计算机在服务器上检查升级文件的频率	16
6.6 升级并不总是在网络中计算机	17
6.7 指定升级警告出现的时间	17
<b>7 怎样保护新计算机？</b>	<b>17</b>
7.1 保护新计算机	17
7.2 保护新操作系统	18
<b>8 怎样重新保护计算机？</b>	<b>18</b>
8.1 重新保护计算机	18
<b>9 怎样监控已被保护的计算机？</b>	<b>19</b>
9.1 哪些计算机已受到保护？	19
9.2 哪些计算机未受到保护？	19
9.3 哪些计算机已被管理？	20
9.4 哪些计算机已连接？	20
9.5 哪些计算机的软件未及时升级？	20
9.6 哪些计算机带有未处理的警报？	20
9.7 哪些计算机未连接？	21
9.8 哪些计算机未被管理？	21
9.9 哪些是本地配置的计算机？	21
9.10 哪些计算机遵照统一配置？	21
9.11 哪些计算机被隐藏了？	22
9.12 打印安全隐患摘要和计算机列表	22
<b>10 怎样配置扫描？</b>	<b>22</b>
10.1 扫描病毒，特洛伊木马，间谍软件和蠕虫	22
10.2 扫描可能不想安装的应用程序	22
10.3 设置读写扫描选项	23
10.4 更改扫描的文件类型	24
10.5 从读写扫描中排除项目	24
10.6 设置自动清除	24
10.7 批准可以使用的应用程序	25
10.8 在设定的时间扫描计算机	25
10.9 设置计划扫描选项	26
10.10 从计划扫描中排除项目	26
10.11 单独配置计算机的扫描	26
<b>11 怎样配置通告？</b>	<b>27</b>
11.1 设置扫描警报	27
11.2 设置升级警报	27

11.3 设置定期发送报告	28
11.4 删除旧警报	28
11.5 指定允许针对警报采取措施的时间	29
<b>12 怎样配置防火墙？</b>	<b>29</b>
12.1 使用防火墙保护计算机	29
12.2 开启或关闭防火墙	30
12.3 防火墙厂商设置	30
12.4 自定义防火墙配置	30
12.5 单独配置计算机上的防火墙	31
<b>13 怎样生成报告？</b>	<b>31</b>
13.1 生成报告	31
13.2 以表的形式显示报告	32
13.3 以图的形式显示报告	32
13.4 显示每个安全隐患的警报数	32
13.5 显示每台计算机的警报数	32
13.6 显示警报率	33
13.7 显示警报历史记录	33
13.8 打印报告	34
13.9 导出报告到文件	34
13.10 更改报告页面布局	34
<b>14 排疑解难</b>	<b>35</b>
14.1 清除失败	35
14.2 有关可能不想安装的应用程序的频繁警报	35

# 1 关于 Sophos 小企业解决方案 (SBS)

## 关于 Sophos 小企业解决方案 (SBS)

Sophos 小企业解决方案 (SBS) 是专门为 IT 资源有限的各种企业精心打造的，为它们提供简便易用，稳定可靠的保护方案，防止病毒，特洛伊木马，蠕虫，间谍软件，垃圾邮件，以及其它安全隐患，侵袭网络中的 Windows 和 Mac 计算机。

要了解 Sophos 小企业解决方案 (SBS) 中包括哪些产品，请参见 [Sophos 小企业解决方案 \(SBS\) 概览](#)。

## 1.1 Sophos 小企业解决方案 (SBS) 概览

### Sophos 小企业解决方案 (SBS) 概览

Sophos 小企业解决方案 (SBS) 由三个产品组成：Sophos Security Suite，Sophos Computer Security，以及 Sophos Anti-Virus。下面的表格显示各产品中所包含的软件。

	Sophos Security Suite	Sophos Computer Security	Sophos Anti-Virus
Sophos Control Center	✓	✓	✓
Sophos Anti-Virus	✓	✓	✓
Sophos Client Firewall	✓	✓	
Sophos PureMessage	✓		

**Sophos Control Center** 使您能够统一在计算机上部署，升级，监控防病毒和防火墙软件，从而保护计算机不受病毒，蠕虫，特洛伊木马，间谍软件，黑客，以及可能不想安装的应用程序 (PUA) 等的侵袭。

**Sophos Anti-Virus** (供 Windows 98/Me/2000 及以后，以及 MacOS X 计算机使用) 可以检测和清除您的计算机或网络中的病毒，蠕虫，特洛伊木马，以及间谍软件。Sophos Anti-Virus for Windows 2000 及以后，还可以检测和删除可能不想安装的应用程序，诸如广告软件，拨号程序，远程管理工具，以及黑客工具等。

特别地，Sophos Anti-Virus 可以：

- 扫描计算机或网络中的安全隐患和可能不想安装的应用程序。
- 在读写文件时检查安全隐患。
- 在发现安全隐患时，发出警报。
- 从文件或引导区中删除病毒，清除被感染项目中的病毒。
- 阻止可能不想安装的应用程序在计算机上运行。
- 删除计算机中的可能不想安装的应用程序。
- 保存活动日志记录。
- 不断升级以检测最新的安全隐患。

**Sophos Client Firewall** (供 Windows 2000 及以后的计算机使用) 可以限制对公司网络或因特网的访问，以及允许特定的经批准的应用程序进入网络。它积极主动地锁定计算机，保护网络，防范因特网蠕虫，黑客和来自未被保护的，尤其是直接与因特网连接的，计算机传播病毒的风险。

**Sophos PureMessage** (供 Windows/Exchange 使用) 提供综合的电子邮件网关和消息发送保护，防范病毒，间谍软件，以及垃圾邮件。它扫描所有往来因特网和公司内部网络的电子邮件，以及扫描 Exchange Message Store，并使用安全隐患消除技术，针对新出现的，或未知由电子邮件引发的安全隐患，提供保护。

要了解更多关于 Sophos 安全软件的信息，请参见相应的帮助文件或用户手册。

要了解更多关于安全隐患的信息，请访问 [Sophos 安全信息网页](#)。

# 2 关于 Sophos Control Center

## 关于 Sophos Control Center

本节包括以下内容：

- [什么是 Sophos Control Center?](#)
- [关于用户界面](#)

- [图标的含义](#)

## 2.1 什么是 Sophos Control Center ?

### 什么是 Sophos Control Center ?

Sophos Control Center 使您能够保护计算机，免遭病毒，蠕虫，特洛伊木马，间谍软件，黑客，和可能不想安装的应用程序(PUA)的侵袭。

通过使用 Sophos Control Center，您可以

- 在您的网络中安装防病毒和(如果您的使用许可证协议包括)防火墙软件。



Sophos Security Suite 和 Sophos Computer Security 的使用许可证协议包括使用防火墙软件的许可；Sophos Anti-Virus 的使用许可证协议则不包括该许可。要大概了解 Sophos 小企业解决方案 (SBS) 的产品范围，请参见 [Sophos 小企业解决方案\(SBS\)概览](#)。

- 通过因特网保持自动升级软件。
- 统一配置检测和清除病毒，蠕虫，特洛伊木马，间谍软件，以及可能不想安装的应用程序，如：广告软件，拨号程序，远程管理工具，以及黑客工具等。
- 统一配置防火墙
- 监控网络并检查计算机是否被保护。
- 提供安全隐患摘要。
- 生成安全隐患趋势报告。

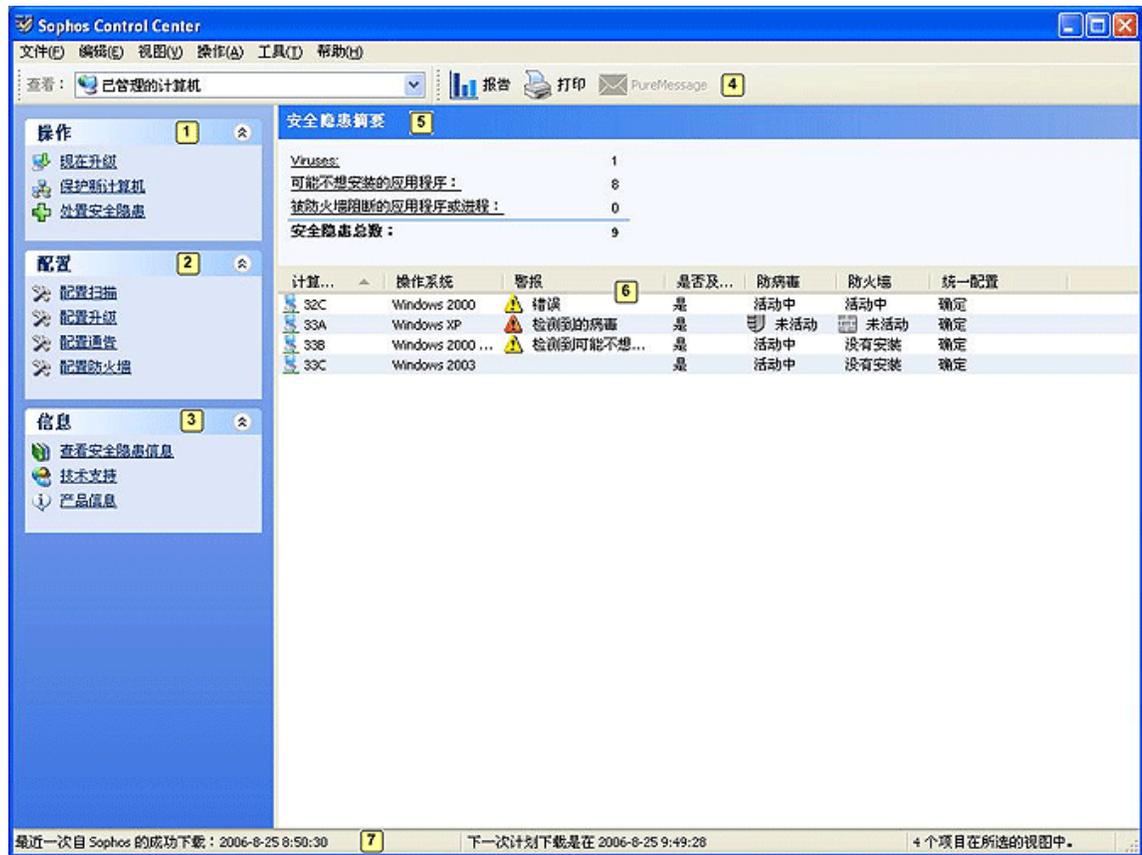
您可以使用 Sophos Control Center 保护：

- Windows 2000 及以后计算机
- Windows 98/Me 计算机
- Mac OS X 计算机

## 2.2 关于 Sophos Control Center 用户界面

### 关于用户界面

您现在所看到的窗口是 Sophos Control Center 用户界面，您通过它，使用和配置 Sophos 的防病毒和防火墙软件。它的主要功能描述如下。



 如果您使用 Sophos Security Suite 或 Sophos Computer Security, 与防火墙有关的信息, 如被阻断的应用程序的数量, 和防火墙的状态等, 才会出现在 Sophos Control Center 中。

## 1 操作菜单

该菜单使您能够升级防病毒软件和(如果您的许可证协议包括)防火墙软件, 保护新的计算机, 以及处置安全隐患。

## 2 配置菜单

该菜单使您能够配置防病毒和防火墙软件, 以及设置安全隐患警报。

## 3 信息菜单

该菜单使您能够访问 Sophos 网站中有关安全隐患的信息, 获得技术支持, 以及产品信息。

## 4 工具栏

### 报告

单击该按钮可以打开 发送报告 对话框。有关怎样生成报告的指导, 请参见 [怎样生成报告?](#)

### 打印

单击该按钮可以打印计算机列表。

### PureMessage

如果您是 PureMessage 用户, 单击该按钮可以启动 PureMessage 控制台。只有 PureMessage 控制台与 Sophos Control Center 是安装在同一台计算机上时, 该按钮才会被启用。

## 5 安全隐患摘要

该窗格中包含在您的计算机中所发现的安全隐患的信息, 以及到 处置警报和错误 对话框的链接。

## 6 计算机列表

这使您能够查看:

- 计算机是否在运行及时更新的防病毒软件。
- 防病毒和防火墙保护是否在活动中，或者是否已安装。
- 计算机是否遵照通过 Sophos Control Center 统一完成的配置设定。
- 哪里出现了警报。

要了解计算机列表中的图标的含义，请参见 [图标含义](#)



要依照某个栏目将计算机列表排序，请单击该栏目的标题。

要查看某计算机的详情，如：防病毒和防火墙软件的版本和状态，未处理的警报，以及安全隐患检测历史记录等，请单击列表中的计算机名，以显示 **计算机详情** 窗口。或者，请高亮显示计算机名，单击右键，并选择 **查看计算机详情**。

## 7 状态栏

窗口底部的状态栏，向您显示 Sophos Control Center 最近一次自 Sophos 下载升级文件的时间，以及计划中的下一次下载升级文件的时间。

## 2.3 图标的含义

### 图标的含义

在计算机列表中，图标用来表示：

- 警报
- 保护被禁用或未及时升级
- 各台计算机的状态，如：是否已安装了软件等。

### 警报

标识	释意
	警报栏中的红色警告标识，表示检测到了病毒。
	黄色的警告标识表示出现以下一个或数个情况： <ul style="list-style-type: none"> <li>• 检测到了可能不想安装的应用程序。</li> <li>• 防火墙已阻断了某个应用程序。</li> <li>• 该计算机没有遵照统一设置。</li> <li>• 出现了错误。</li> </ul>

同时请参看 [哪些计算机带有未处理的警报？](#)

### 保护被禁用或未及时升级

标识	释意
	在计算机列表中的 <b>防病毒</b> 栏中，出现灰白的盾牌和“未活动”字样，表示读写扫描未在活动中。
	在 <b>防火墙</b> 栏中，灰白的防火墙标识和“未活动”字样，表示防火墙未启用。
	在 <b>是否及时升级</b> 栏中，时钟图标和“否”字样，表示软件未及时升级。

同时请参看 [哪些计算机未受到保护？](#)

### 计算机状态

标识	释意
	蓝色计算机标识，表示该计算机已被 Sophos Control Center 管理。
	带有沙漏的计算机标识，表示 Sophos Anti-Virus 的自动升级组件已安装，并且正在下载该产品的最新版本。
	灰色计算机标识，表示该计算机未被 Sophos Control Center 管理。



计算机旁带有红叉的标识，表示该计算机已断开连接。

## 3 怎样学会使用？

### 怎样学会使用？

本节包括以下内容：

- [学会使用 Sophos Control Center](#)
- [保护网络中的计算机](#)
- [手动保护计算机](#)

## 3.1 学会使用 Sophos Control Center

### 学会使用 Sophos Control Center

本节就使用 Sophos Control Center 保护您的网络，为您提供快速的指南。这仅仅是一个概览，因此，您可能还会参看所提到的其它各节。



要大概了解 Sophos 小企业解决方案(SBS)的产品范围，请参见 [Sophos 小企业解决方案\(SBS\)概览](#)。

1. 在您首次启动 Sophos Control Center 时，会有一个向导启动。它会在保护网络中的计算机的过程中，为您提供指南。

如果您在首次启动 Sophos Control Center 时，没有完成该向导，并且需要了解更多怎样完成该向导的信息，请参见 [保护网络中的计算机](#)。

2. 如果 Sophos Control Center 无法在某些计算机上自动安装软件，请转到这些计算机上，并按照 [手动保护计算机](#) 中的说明做。
3. 如果您想要更改扫描，请在 **配置** 菜单中，单击 **配置扫描**。相关的分步指导，请参见 [怎样配置扫描？](#)
4. 依照默认值，Sophos Anti-Virus 可以检测病毒，特洛伊木马，间谍软件，以及蠕虫等。您还可以配置它检测可能不想安装的应用程序(PUA)。要了解怎样管理可能不想安装的应用程序，请参见
  - \$ [扫描可能不想安装的应用程序](#)
  - \$ [批准可以使用的应用程序](#)
  - \$ [清除可能不想安装的应用程序](#)
5. 如果您想要设置警报，请在 **配置** 菜单中，单击 **配置通告**。请参见 [怎样配置通告？](#)
6. 如果您想要更改进行升级的方式，请在 **配置** 菜单中，单击 **配置升级**。请参见 [怎样配置升级？](#)
7. 在安装结束时，查看计算机列表。在 **防病毒** 和 (如果您使用 Sophos Client Firewall) **防火墙** 栏中，您应该看到“活动中”字样：这表明该计算机处于读写扫描和防火墙的保护中，并且现在由 Sophos Control Center 管理。



如果您随后添加了新的计算机到网络中，请按照以下说明保护它们。

在 **操作** 菜单中，单击 **保护新计算机**。Sophos 网络保护向导会启动。有关怎样完成该向导的指导，请参见 [怎样保护新计算机？](#)

## 3.2 保护网络中的计算机

### 保护网络中的计算机

在您首次启动 Sophos Control Center 时，Sophos 网络保护向导启动。它会在保护网络中的计算机的过程中，为您提供指南。按照以下说明完成该向导：

1. 在向导的 **欢迎** 页面中，单击 **下一步**。
2. 在 **初始化安装** 页面中，等候 Sophos Control Center 执行初始设置任务。在初始设置完成后，**下一步** 按钮会变为可用状态。单击 **下一步**。
3. 在 **选择软件** 页面中，根据您的计算机上所运行的操作系统，选择相应的软件。

选项 **Windows 2000** 及以后 和 **Windows 98/Me** 是被默认勾选。Sophos Control Center 总是会为 Windows 2000 及以后的计算机提供保护。您不能够更改这一设置。如果您没有 Windows 98/Me 计算机，请取消勾选 **Windows 98/Me** 勾选框。

如果您具有 MacOS X 计算机，请勾选 **Mac OS X** 勾选框。这将使您稍后能够在这些计算机上安装防病毒软件。

4. 在 **Sophos 下载帐户详情** 页面中，输入 Sophos 提供的用户名和密码。单击 **下一步**。

如果您通过代理服务器访问因特网，请参见 [代理服务器详情](#)。

如果在安装之前，您想要更改放置所下载的软件和升级文件的路径，请参见 [更改下载文件夹](#)。

5. 在 **Windows 用户帐户详情** 页面中，输入对于网络中的所有计算机都有效的系统管理员帐户的详情，以使 Sophos Control Center 能够在这些计算机上安装软件。

6. 在 **保护计算机** 页中，等待计算机被找到。



只有 Windows 2000 及以后的计算机将被列示在此页中，因为在 Windows 98/Me 或 Mac OS X 计算机上不可能进行自动安装或升级。

选择您想要在计算机上安装的保护类型。防病毒软件已被默认选择为安装在所有计算机上。如果您不想在某个计算机上安装防病毒软件，请取消勾选该计算机旁的 **防病毒** 勾选框。要勾选或取消勾选列表中所有 **防病毒** 勾选框，请勾选或取消勾选 **防病毒** 栏标题的勾选框。



**Sophos Client Firewall** 只能安装在运行 Windows 2000 或以后的工作站上，它无法被安装在运行服务器操作系统的计算机上。安装防火墙之前要求先安装 **Sophos Anti-Virus**。



您必须重新启动每一台已经安装了 **Sophos Client Firewall** 的计算机，以便激活该防火墙。

如果您想要安装防火墙，请勾选相应的计算机旁的 **防火墙** 勾选框。

单击 **下一步**。

7. 在 **下载进程** 页面中，会出现进度条。在向导完成软件下载，并做好安装准备后，**下一步** 按钮会变为可用状态。

单击 **下一步**。

8. 如果有计算机列示在 **必须手动保护的计算机** 页面中，请单击 **打印** 将这些未受到保护的计算机列表打印出来。或者，单击 **另存为** 保存该列表，或者，将这些计算机记下来。单击 **下一步**。
9. 在向导的最后页面中，单击 **完成**。

在您关闭向导之后，**Sophos Control Center** 将在尽可能多的，所选择的计算机上自动安装软件。您会看到这些计算机，及其状态信息，列示在 **Sophos Control Center** 中。

10. 按照 **手动保护计算机** 中的说明，到未受到保护的计算机列表中的各台计算机上，手动安装 **Sophos Anti-Virus** 和（如果您的用户使用许可证协议包括）**Sophos Client Firewall**。

### 3.3 手动保护计算机

#### 手动保护计算机

要在这些计算机上手动安装 **Sophos Anti-Virus** 和（如果您的用户使用许可证协议包括）**Sophos Client Firewall**，请分别到各台计算机上，登录为系统管理员，按照以下说明做。



**Sophos Anti-Virus 6** 支持 Windows 2000 及以后，**Sophos Anti-Virus 4.6** 支持 Windows 98/Me；**Sophos Anti-Virus 4.8** 支持 Mac OS X。

#### Windows 2000 及以后计算机

如果您的用户使用许可证协议包括 **Sophos Client Firewall**，浏览找到升级文件夹（默认为 \\<服务器名>\Sophos\SAVSCFXP，这里的 **服务器名** 是运行 **Sophos Control Center** 的那台计算机的名称），然后运行 **setup.exe**。要在安装 **Sophos Anti-Virus** 时，同样安装 **Sophos Client Firewall**，请在 **安装** 对话框中，勾选 **安装 Sophos Client Firewall** 勾选框，并单击 **确定**。



**Sophos Client Firewall** 只能安装在运行 Windows 2000 或以后的工作站上，它无法被安装在运行服务器操作系统的计算机上。您不应该将防火墙安装到已经安装了 **Sophos Control Center** 的那台计算机上。安装防火墙之前要求先安装 **Sophos Anti-Virus**。



您必须重新启动每一台已经安装了 **Sophos Client Firewall** 的计算机，以便激活该防火墙。

如果您的用户使用许可证协议没有包括 **Sophos Client Firewall**，浏览找到升级文件夹（默认为 \\<服务器名>\Sophos\SAVSCFXP，这里的 **服务器名** 是运行 **Sophos Control Center** 的那台计算机的名称），然后运行 **setup.exe**。

#### Windows 98/Me 计算机

浏览找到升级文件夹（默认为 \\<服务器名>\Sophos\ES9x，这里的 **服务器名** 是运行 **Sophos Control Center** 的那台计算机的名称），然后运行 **setup.exe**。

#### Mac OS X 计算机

从 \\<服务器名>\Sophos\ESOSX 中复制安装软件包 **Sophos Anti-Virus.mkpg** 到您想要安装 **Sophos Anti-Virus** 的那台计算机上。然后，双击 **Sophos Anti-Virus.mkpg**。

## 4 怎样清除安全隐患？

#### 怎样清除安全隐患？

本节将告诉您 **发现了安全隐患时会怎样**，以及怎样使用 **Sophos Control Center**：

- [查找有关安全隐患的信息](#)
- [清除病毒](#)
- [清除可能不想安装的应用程序](#)
- [清除防火墙检测到的安全隐患](#)（如果您的许可证协议包括 **Sophos Client Firewall**）

- [设置自动清除](#)
- [处理出错警报](#)

## 4.1 发现了安全隐患时会怎样？

### 发现了安全隐患时会怎样？

如果在您的网络中发现了安全隐患，并且它还没有被[自动清除](#)：

- Sophos Control Center 将向您发送警报(如果[扫描警报已启用](#))。
- 在 Sophos Control Center 的计算机列表中，与此相关的计算机都会出现警报图标。



要了解出现警报的原因，请高亮显示计算机列表中的计算机名，单击右键，然后选择 [查看计算机详情](#)。

- 了解更多有关警报图标的信息，请参见[图标含义](#)。
- 在 Sophos Control Center 的 [安全隐患摘要](#) 窗格中，会显示在网络中发现的病毒和间谍软件的总数。

## 4.2 清除病毒

### 清除病毒

要处理在计算机中发现的病毒和间谍软件，请按照以下说明做：

在 [安全隐患摘要](#) 窗格中，单击 [病毒/间谍软件](#) 链接。会出现 [处置警报和错误](#) 对话框，显示 [病毒警报](#) 标签页。或者，在 [操作](#) 菜单中，单击 [处置安全隐患](#)。

#### 被感染计算机的详情

有关每个被感染计算机的信息都显示在此栏中。特别地，您可以查看被感染的计算机的名称，安全隐患首次在计算机中被发现的日期和时间，病毒名称，感染项目的数量，以及警报的状态等。

状态 显示以下内容之一：

- 可清除

在这种情况下，如稍后将说明的那样，可以通过 [清除](#) 按钮，清除被感染的项目。

- 不可清除

要清除在 Sophos Control Center 中显示为“不可清除”的项目，请到被感染的计算机上，进行手动清除。如果安全隐患没有被清除，请参见[清除失败](#)。

- 部分可清除(当计算机上有多个项目感染了病毒，而其中的一部分项目中的病毒可以被清除时，会出现此状态提示)

在这种情况下，如稍后将说明的那样，可以通过 [清除](#) 按钮，清除“可清除”的项目中的病毒。要清除剩下的项目中的病毒，请按照针对“不可清除”的项目所采取的措施做。

- 清除正在进行中(开始于[清除启动时刻](#))
- 清除超时(开始于[清除启动时刻](#))

出现这种情况，计算机可能没有连接到网络中。请确保该计算机连接到了网络中，然后再次清除该计算机。

如果您想要查看计算机上单个的安全隐患的更多信息，请双击该安全隐患条目，或者，按照稍后的说明，使用 [详情](#) 按钮。

#### 针对被感染项目采取措施

要处理病毒，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条目。这使您能够针对一组条目，同时执行相同的操作。

要勾选或者取消勾选特定的条目，请单击它的左边的勾选框。

##### 详情

单击该按钮可以显示 [计算机病毒警报详情](#) 窗口，出现计算机中该安全隐患感染的所有项目，各次感染发生的日期和时间，清除状态，等等信息的列表。要了解更多关于该安全隐患的详情，请单击它的名称，Sophos Control Center 会将您连接到 Sophos 网站的病毒分析部分。

##### 清除

单击该按钮，可以清除所选择的计算机。这将清除文件或引导区中的病毒，也就是，将病毒从文件或引导区中移除。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。

 Sophos 建议您试图将多组件的安全隐患从计算机清除之前，对计算机进行一次完全的[计划扫描](#)，以检测到多组件安全隐患的所有组件。

 要从计算机中彻底清除一些涉及数个组件的安全隐患，您可能需要重新启动计算机。如果是这种情况，相关的计算机中会出现消息框，给出立即重新启动计算机，或稍后重新启动计算机的选项。在计算机重新启动之后，会进行清除的最终步骤。

确认已知

如果确定某项目没有感染病毒，单击该按钮，可以将所选的条目从列表中删除。不过，这并不会从磁盘中删除该项目。

如果病毒没有被清除，请参见[清除失败](#)。

## 4.3 清除可能不想安装的应用程序

### 清除可能不想安装的应用程序

要处理在计算机中发现的[可能不想安装的应用程序](#)，请按照以下说明做：

在 **安全隐患摘要** 窗格中，单击 **可能不想安装的应用程序** 链接。会出现 **处置警报和错误** 对话框，显示 **可能不想安装的应用程序警报** 标签页。

或者，在 **操作** 菜单中，单击 **处置安全隐患**，然后，单击 **可能不想安装的应用程序警报** 标签页。

#### 可能不想安装的应用程序详情

有关每个发现了可能不想安装的应用程序的计算机的信息都显示在此栏中。特别地，您可以查看发现应用程序的计算机的名称，应用程序在计算机中被发现的日期和时间，应用程序名称，以及警报的状态等。

状态 显示以下内容之一：

- **可清除**  
在这种情况下，请按照稍后说明的那样，清除或批准该应用程序。
- **不可清除**  
如果您想使用某个“不可清除”的应用程序，您可以批准它。要从计算机中清除该应用程序，请到被感染的计算机上，进行手动清除。如果该应用程序没有被清除，请参见[清除失败](#)。
- **批准正在进行中**
- **清除正在进行中(启动清除启动时间)**
- **清除超时(开始于清除启动时刻)**

出现这种情况，计算机可能没有连接到网络中。请确保该计算机连接到了网络中，然后再次清除该计算机。

 要了解更多关于该应用程序的信息，请在 Sophos Control Center 的计算机列表中，高亮显示发现该应用程序的计算机，单击右键，然后选择 **查看计算机详情**。在 **计算机详情** 窗口中，下拉滚动条到 **未处理的警报**，然后，单击该应用程序的名称。Sophos Control Center 会将您连接到 Sophos 网站的应用程序分析部分。

#### 针对可能不想安装的应用程序采取措施

要处理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条目。这使您能够针对一组条目，同时执行相同的操作。

要勾选或者取消勾选特定的条目，请单击它的左边的勾选框。

##### 清除

单击该按钮，可以从所选计算机中删除该应用程序已知的所有组件。

 Sophos 建议您试图将多组件的可能不想安装的应用程序从计算机清除之前，对计算机进行一次完全的[计划扫描](#)，以检测到多组件可能不想安装的应用程序的所有组件。

 要从计算机中彻底清除一些涉及数个组件的应用程序，您可能需要重新启动计算机。如果是这种情况，相关的计算机中会出现消息框，给出立即重新启动计算机，或稍后重新启动计算机的选项。在计算机重新启动之后，会进行清除的最终步骤。

确认已知

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

批准

如果您信任该应用程序，单击该按钮，可以批准所选择的应用程序。这会将应用程序添加到已批准的应用程序的列表中，这样 Sophos Control Center 将不会阻止该应用程序在您的网络中运行。

## 4.4 清除防火墙检测到的安全隐患

### 清除防火墙检测到的安全隐患

要批准防火墙阻断的应用程序或清除防火墙警报：

1. 在 **操作** 菜单中，单击 **处置安全隐患**。
2. 在 **处置警报和错误** 对话框中，单击 **防火墙警报** 标签页。

#### 防火墙警报的详情

在该栏目中，您可以看到被防火墙阻断应用程序和发出警报的各台计算机的信息。特别地，您可以查看发出警报的计算机的名称，警报的日期和时间，被防火墙阻断的应用程序的文件，版本，名称和类型等。



要了解更多关于被防火墙阻断的应用程序的信息，请在 Sophos Control Center 的计算机列表中，高亮显示应用程序被阻断的计算机，单击右键，然后选择 **查看计算机详情**。在计算机详情窗口中，下拉滚动条到 **未处理的警报**，然后，单击该应用程序的名称。Sophos Control Center 会将您连接到 Sophos 网站的应用程序分析部分。

#### 针对防火墙警报采取措施

要处理防火墙警报，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条目。这使您能够针对一组条目，同时执行相同的操作。

要勾选或者取消勾选特定的条目，请单击它的左边的勾选框。

##### 允许

选择一个或多个警报，然后单击该按钮，允许所选择的应用程序—如果您认为它们是安全的。这会为该应用程序创建新的规则，并在防火墙配置中配置它为“信任的”。

##### 确认已知

单击该按钮，以将警报标识为已处理。被清空的警报不会再显示。

## 4.5 查找有关安全隐患的信息

### 查找有关安全隐患的信息

如果报告发现了安全隐患，您可以查找有关该安全隐患的影响，以及清除该安全隐患的建议的信息。

1. 在 Sophos Control Center 的计算机列表中，高亮显示发现安全隐患的计算机，单击右键，然后选择 **查看计算机详情**。
2. 在计算机详情窗口中，下拉滚动条到 **未处理的警报**，然后，单击安全隐患的名称。

Sophos Control Center 会将您连接到 Sophos 网站的安全隐患分析部分。



您还可以到 Sophos 网站中，浏览您对想要了解的安全隐患的分析内容。要这样做，请：

1. 记下安全隐患的名称。
2. 在 **信息** 菜单中，单击 **查看安全隐患信息**。  
或者，在 **帮助** 菜单中，单击 **查看安全隐患信息**。
3. Sophos Control Center 会打开 Sophos 网站中的安全隐患信息部分。点击链接查看您要了解的安全隐患的详情。

## 4.6 设置自动清除

### 设置自动清除

您可以在一旦发现病毒时，就立即在计算机中自动清除它们。要做到这一点，请按照以下说明，更改读写扫描设置。



读写扫描不能够清除可能不想安装的应用程序。您应该按照 [清除可能不想安装的应用程序](#) 中的说明处理它们。按照稍后的说明，您还可以启用在计划扫描中自动清除未批准的应用程序。

### 要自动清除病毒(读写扫描和计划扫描)

1. 在 **配置** 菜单中，单击 **配置扫描**。
2. 要更改读写扫描的设置，在 **配置扫描设置** 对话框中，单击 **读写扫描** 按钮。在 **读写扫描设置** 对话框中，单击 **清除** 标签页。

要更改计划扫描的设置，在 **配置扫描设置** 对话框中，选择 **计划扫描**，并单击 **编辑**。在 **计划扫描设置** 对话框中，单击 **配置**。在 **扫描和清除设置** 对话框中，单击 **清除** 标签。

3. 勾选 **自动清除感染项目中的病毒**。
4. 您还可以指定如果清除失败，应该采取什么措施。选项为：

- S 不采取措施
- S 删除
- S 移至默认的路径
- S 移至 **UNC** 路径(这里的 **UNC** 路径是您指定的完整的 **UNC** 路径)。



Mac 计算机无法读取 **UNC** 路径。如果您选择 **移至**，并指定了路径，MacOSX 计算机仍会将感染项目移至默认的路径。

### 要自动清除可能不想安装的应用程序(仅限计划扫描)

1. 在 **配置** 菜单中，单击 **配置扫描**。
2. 在 **配置扫描设置** 对话框，选择该计划扫描，然后，单击 **编辑**。
3. 在 **计划扫描设置** 对话框中，单击 **配置**。
4. 在 **扫描和清除设置** 对话框中，单击 **清除** 标签。
5. 选择 **自动清除可能不想安装的应用程序**。这将使 Sophos Anti-Virus 能够删除您的计算机上，没有事先 **批准** 的可能不想安装的应用程序。



该选项只能应用于运行在 Windows2000 或以后的计算机上的 Sophos Anti-Virus 中。



要了解怎样通过 **处置警报和错误** 对话框，清除您的计算机中的病毒或可能不想安装的应用程序，请参见 [清除病毒](#) 或 [清除可能不想安装的应用程序](#)。

## 4.7 处理出错警报

### 处理出错警报

要处置防病毒和防火墙错误：

1. 在 **操作** 菜单中，单击 **处置安全隐患**。
2. 在 **处置警报和错误** 对话框中，单击 **错误** 标签页。

#### 未处理的错误的详情

有关未处理的在最近 30 天发生的扫描和防火墙错误的信息，会显示在该栏中。特别地，您可以查看出现错误的计算机的名称，出现错误的日期和时间，以及错误类型，代码和描述等。

#### 针对错误采取措施

要处理错误，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条目。这使您能够针对一组条目，同时执行相同的操作。

要勾选或者取消勾选特定的条目，请单击它的左边的勾选框。

##### 确认已知

单击该按钮，以将错误标识为已处理。被清空的警报不会再显示。

## 5 怎样升级计算机？

### 怎样升级计算机？

Sophos Control Center 每隔 60 分钟就会从 Sophos 检查是否有升级文件，如果有新的升级文件，就会下载它。

这样，软件会被下载到您运行 Sophos Control Center 的那台计算机上。被 Sophos Control Center 管理的计算机从这个统一的拷贝上自动升级它们(依照默认值，它们会每隔 5 分钟就检查是否有升级文件)。

本节将告诉您怎样：

- [检查最近一次升级发生的时间](#)

- [检查下一次升级发生的时间](#)
- [检查升级是否成功](#)
- [设置关于升级问题的警报](#)
- [关闭自动升级](#)
- [手动升级](#)
- [升级单独的计算机](#)

## 5.1 最近一次升级发生在何时？

### 最近一次升级发生在何时？

最近一次从 Sophos 升级的时间会出现在 Sophos Control Center 底部的状态栏中。

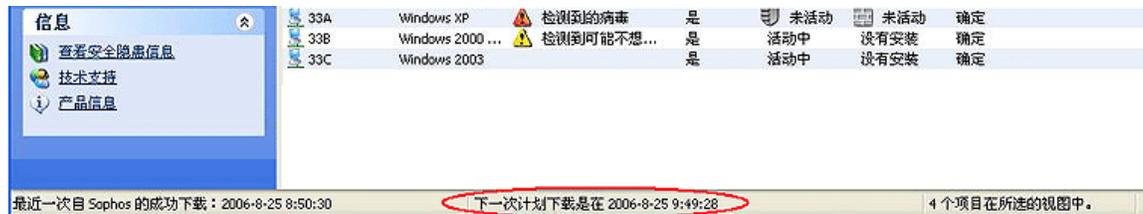


## 5.2 下一次升级发生在何时？

### 下一次升级发生在何时？

计划中的下一次从 Sophos 升级的时间会出现在 Sophos Control Center 底部的状态栏中。

这是下一次 Sophos Control Center 将任何升级软件下载到您的计算机上的时间。网络中的计算机会在下一次检查升级文件时，升级它们自身(依照默认值，它们会每隔10分钟就检查是否有升级文件)。



## 5.3 升级成功吗？

### 升级成功吗？

升级活动分为两步：

1. Sophos Control Center 从 Sophos 下载升级文件。
2. 网络中的计算机从您的服务器上升级。

如果任何一个步骤失败，您将收到如下警报。

#### Sophos Control Center 下载升级文件失败

如果下载失败，Sophos Control Center 的状态栏中会出现消息。如果您[设置了升级警报](#)，您还将收到发出的警报。

#### 计算机自身升级失败

在计算机列表中，“否”字样会出现在没有及时升级的计算机旁的 **是否及时升级** 栏中。要强制计算机进行升级，请在该计算机名上单击右键，然后选择 **升级**。

## 5.4 怎样获得有关升级问题的警报？

### 怎样获得有关升级问题的警报？

您可以配置 Sophos Control Center 在从 Sophos 下载升级出现问题时，发出警报。

1. 在 **配置** 菜单，单击 **配置通告**。
2. 在 **配置通告** 对话框中，单击 **升级警报** 标签页。然后，按照以下说明，选择您想要的警报类型。

#### 电子邮件警报

选择 **电子邮件**。单击 **配置**，然后输入您的 SMTP 服务器的详情。然后，单击 **添加**，输入警报将要寄至的电子邮件地址。

#### 网络消息发送

选择 **网络消息发送** 使 Sophos Control Center 能够向指定的计算机发送网络消息。单击 **添加**，并输入网络消息将要寄至的计算机的名称。当计算机收到网络消息时，会弹出显示消息文字的消息框。

Windows 98/Me 计算机必须运行 WinPopup 应用程序，才能收到消息。

#### 事件日志记录

如果您想要 Sophos Control Center 在计算机的事件日志记录中记录详尽的下载信息，请选择 **使用详尽模式的事件日志记录**。

## 5.5 关闭自动升级

### 关闭自动升级

如果您需要关闭自动升级(例如：如果您使用拨号连结)，请按照以下说明做：



如果您要这样做，您必须定期[手动升级](#)。

1. 在 **配置** 菜单，单击 **升级**。
2. 在 **配置升级** 对话框中，单击 **计划** 标签页。不要勾选 **从 Sophos 自动下载升级文件** 勾选框。

## 5.6 手动升级

### 手动升级

要手动升级您的防病毒软件：

1. 在 **操作** 菜单中，单击 **现在升级**。
2. 在出现询问您是否要执行升级操作的消息框时。单击 **确定**。

Sophos Control Center 会联系 Sophos 并下载最新版的防病毒和(如果您选择了该选项)防火墙软件。您网络中所有计算机都会在下一次检查您的服务器上的升级文件时，升级它们自身。

## 5.7 升级个别的计算机

### 升级个别的计算机

如果某个别的计算机显示为未及时升级(“否”字样出现在 **是否及时升级** 栏中)，您现在可以使它升级自身。

在计算机列表中，高亮选择您想要升级的计算机。单击右键并选择 **升级**。

## 6 怎样配置升级？

### 怎样配置升级？

您可以更改进行升级的方式。

本节将告诉您怎样：

- [更改升级内容\(软件标签页\)](#)
- [启用通过代理服务器进行升级\(代理服务器标签页\)](#)
- [更改用于升级的用户ID\(用户ID标签页\)](#)
- [关闭自动升级\(计划标签页\)](#)
- [更改计算机在服务器上检查升级文件的频率\(计划标签页\)](#)

- [升级并不总是在网络中计算机\(备用升级源\)](#)
- [指定升级警告出现的时间\(警告标签页\)](#)

## 6.1 更改升级内容

### 更改升级内容

您可以更改所要升级的软件。

您需要这样做，如果：

- 您添加的计算机使用了与您的网络中的其它计算机不同的操作系统，例如：MacOSX，您需要下载相应的 Sophos Anti-Virus。
- 您将所有某种操作系统的计算机从网络中移除。

要更改下载的软件，请按照以下说明做：

1. 在 **配置** 菜单，单击 **升级**。
2. 在 **配置升级** 对话框中，单击 **软件** 标签页。然后选择一个或多个操作系统的 Sophos Anti-Virus，并单击 **确定**。



Sophos Control Center 总是为 Windows2000 及以后的计算机提供保护。您不能够更改这一设置。

3. 如果您选择的是以前没有保护过的操作系统(Windows98/Me 或 Mac OS X)，请继续步骤3和步骤4。
3. 回到 **Sophos Control Center** 主窗口。在 **操作** 菜单中，单击 **现在升级** 以下载新软件。
4. 按照 [手动保护计算机](#) 中的说明，到各台新类型的计算机上安装 Sophos Anti-Virus。

## 6.2 通过代理服务器升级

### 通过代理服务器升级

如果您使用代理服务器访问因特网，您必须使 Sophos Control Center 能够通过该代理服务器下载升级文件。

1. 在 **配置** 菜单，单击 **升级**。
2. 在 **配置升级** 对话框中，单击 **代理服务器** 标签页。输入代理服务器地址和端口号。请输入用来访问该服务器的帐户的用户名和密码(您的网络管理员可以为您提供这些详情)。

## 6.3 更改用于升级的用户 ID

### 更改用于升级的用户 ID

您可以更改用于下载升级的用户 ID。

1. 在 **配置** 菜单，单击 **升级**。
2. 在 **配置升级** 对话框中，单击 **用户 ID** 标签页。请输入由 Sophos 提供的用户名和密码。

## 6.4 关闭自动升级

### 关闭自动升级

如果您需要关闭自动升级(例如：如果您使用拨号连结)，请按照以下说明做：



如果您要这样做，您必须定期 [手动升级](#)。

1. 在 **配置** 菜单，单击 **升级**。
2. 在 **配置升级** 对话框中，单击 **计划** 标签页。不要勾选 **从 Sophos 自动下载升级文件** 勾选框。

## 6.5 更改计算机在服务器上检查升级文件的频率

### 更改计算机在服务器上检查升级文件的频率

依照默认值，您的网络中计算机，每隔10分钟检查一次，查看是否有提供了升级的防病毒软件。

要更改这一频率：

1. 在 **配置** 菜单，单击 **升级**。
2. 在 **配置升级** 对话框中，单击 **计划** 标签页。请确保勾选了 **启用网络中的计算机自动使用 Sophos 升级文件** 勾选框。在该选项之下文本框中输入以分钟为单位的时间。

## 6.6 升级并不总是在网络中计算机

### 升级并不总是在网络中计算机

依照默认值，您的网络中的计算机从您运行 Sophos Control Center 中的那台计算机上的升级文件夹中升级它们自身。如果对某计算机该升级文件夹不可用，如：该计算机连接到了因特网中，但并没有连接到公司网络中，那么，该计算机将直接从 Sophos 升级。

1. 在 **配置** 菜单，单击 **升级**。
2. 在 **配置升级** 对话框中，单击 **备用升级源** 标签页中，确保勾选了 **自 Sophos**。

#### 自 Sophos

这是默认的选项。Sophos 建议您保留该选项，如果您有并不总是连接到公司网络中的计算机，如：笔记型电脑。这些计算机将使用与 Sophos Control Center 所使用的认证资料相同。

#### 自您的公司



如果您指定的是公司网络或网站中的文件夹，您必须确保定时升级该文件夹中的安全软件。要做到这一点，您可以那里安装 Sophos Control Center。您还可以安排发布升级文件中的拷贝。

如果在主升级源不可用时，您想要网络中的计算机从公司网站或目录中升级，请选择该选项。请输入网络文件夹的地址(UNC 路径)或网站(HTTP地址)。

如果需要，请输入您的计算机可以用来访问该文件夹或网站的帐户的用户名和密码。该帐户应该具备访问您在上面的地址文本框中输入的那个目录的读权限。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。

## 6.7 指定升级警告出现的时间

### 指定升级警告出现的时间

Sophos Control Center 会在您的软件未及升级时向您给出警告(这会在您的服务器从 Sophos 下载升级文件失败时出现)。您可以指定在未及升级的多少天之后给出警告。警告将在您启动 Sophos Control Center 时显示。

要指定该天数：

1. 在 **配置** 菜单，单击 **升级**。
2. 在 **配置升级** 对话框中，单击 **警告** 标签页，然后输入天数。默认的天数为7天。

## 7 怎样保护新计算机？

### 怎样保护新计算机？

如果您在网络中添加了新计算机，您必须使 Sophos Control Center 能够保护它们免遭病毒，蠕虫，黑客，以及其它安全隐患的侵袭。

本节将告诉您怎样：

- [保护新计算机](#)
- [保护新操作系统](#)

## 7.1 保护新计算机

### 保护新计算机

如果有新的计算机添加到您的网络中，您必须保护使用防病毒和(如果您的许可证协议包括)防火墙软件。



如果您的新计算机运行的是与您之前所使用的操作系统不同的操作系统(如：MacOSX)，请参见[保护新操作系统](#)。

1. 在 **操作** 菜单中，单击 **保护新计算机**。Sophos 网络保护向导 会启动。
2. 在向导的 **欢迎** 页面中，单击 **下一步**。
3. 在 **Windows** 用户帐户详情 页面中，输入可以用来在您的网络中的计算机上，安装软件的系统管理员帐户详情。
4. 在 **保护计算机** 页中，等待计算机被找到。



只有 Windows2000 及以后的计算机将被列示在此页中，因为在 Windows98/Me 或 MacOSX 计算机上不可能进行自动安装或升级。

选择您想要在计算机上安装的保护类型。防病毒软件已被默认选择为安装在所有计算机上。如果您不想在某个计

计算机上安装防病毒软件，请取消勾选该计算机旁的 **防病毒** 勾选框。要勾选或取消勾选列表中所有 **防病毒** 勾选框，请勾选或取消勾选 **防病毒** 栏目标题的勾选框。



**Sophos Client Firewall** 只能安装在运行 Windows 2000 或以后的工作站上，它无法被安装在运行服务器操作系统的计算机上。安装防火墙之前要求先安装 **Sophos Anti-Virus**。



您必须重新启动每一台已经安装了 **Sophos Client Firewall** 的计算机，以便激活该防火墙。

如果您想要安装防火墙，请勾选相应的计算机旁的 **防火墙** 勾选框。

单击 **下一步**。

- 如果有计算机列示在 **必须手动保护的计算机** 页面中，请单击 **打印** 将这些未受到保护的计算机列表打印出来。或者，单击 **另存为** 保存该列表，或者，将这些计算机记下来。
- 在向导的最后页面中，单击 **完成**。

在您关闭向导之后，**Sophos Control Center** 将在尽可能多的，所选择的计算机上自动安装软件。您会看到这些计算机，及其状态信息，列示在 **Sophos Control Center** 中。

- 按照 [手动保护计算机](#) 中的说明，到未受保护的计算机列表上的各台计算机中安装软件。

## 7.2 保护新操作系统

### 保护新操作系统

如果您添加了新的类型的计算机到网络中，例如，您第一次添加 Windows 98 或 MacOS X 计算机，您必须使 **Sophos Control Center** 能够下载针对该类型的计算机的防病毒软件。



**Sophos Control Center** 总是会为 Windows 2000 及以后的计算机提供保护。您不能够更改这一设置。



**Sophos Client Firewall** 只能安装在运行 Windows 2000 或以后的工作站上。

- 在 **配置** 菜单，单击 **升级**。
- 在 **配置升级** 对话框中的 **软件** 标签页中，选择您想要保护的一种或多种操作系统。除了总是被选择的 **Windows 2000** 及以后 之外，还有两种选项：

§ Windows 98/Me  
§ Mac OS X

**Windows 98/Me** 是默认的选择。如果您没有 Windows 98/Me 计算机，请取消勾选 **Windows 98/Me** 勾选框。

如果您具有 MacOS X 计算机，请勾选 **Mac OS X** 勾选框。这将使您稍后能够在这些计算机上安装防病毒软件。

- 回到 **Sophos Control Center** 主窗口。在 **操作** 菜单中，单击 **现在升级**。
- 按照 [手动保护计算机](#) 中的说明，到各台新类型的计算机上安装软件。

## 8 怎样重新保护计算机？

### 怎样重新保护计算机？

如果您需要重新安装原先安装在网络中的计算机上的防病毒和(如果您的许可证协议包括)防火墙软件，请按照以下说明做。

在计算机列表中，高亮选择您想要重新安装防火墙的计算机。打开 **工具** 菜单，并选择 **重新保护计算机**。**重新保护计算机** 向导 会启动。它会在重新安装软件的过程中，为您提供指南。

如果您需要帮助以完成向导，请参见 [重新保护计算机](#)。

### 8.1 重新保护计算机

#### 重新保护计算机

如果您需要重新安装软件到网络中的任何计算机上，请按照以下说明做。

- 在计算机列表中，高亮选择您想要重新安装防火墙的计算机。在菜单栏中，打开 **工具** 菜单，选择 **重新保护计算机**。**重新保护计算机** 向导 会启动。
- 在向导的 **欢迎** 页面中，单击 **下一步**。
- 在 **Windows** 用户帐户详情 页面中，输入可以用来在您的网络中的计算机上，重新安装软件的系统管理员帐户详情。
- 在 **在工作站上重新安装** 页面中，选择在计算机上重新安装软件。

要在所有的计算机上重新安装软件，请勾选 **重新安装软件** 栏目标题的勾选框。然后，单击 **下一步**。

5. 在 [必须手动保护的计算机](#) 页面中，单击 [打印](#)，以打印需要手动安装的计算机列表。或者，单击 [另存为](#) 保存该列表，或者，将这些计算机记录下来。单击 [下一步](#)。
6. 在向导的最后页面中，单击 [完成](#)。  
在您关闭向导之后，Sophos Control Center 将在尽可能多的，所选择的计算机上自动重新安装软件。您会看到这些计算机，及其状态信息，列示在 [Sophos Control Center](#) 中。
7. 按照 [手动保护计算机](#) 中的说明，到要求手动安装的计算机列表上的各台计算机中安装软件。

## 9 怎样监控已被保护的计算机？

### 怎样监控已被保护的计算机？

在 Sophos Control Center 中，您可以监控网络中的计算机，确保它们防范各种安全隐患。

本节将怎样检查计算机是否

- [受到防范各种安全隐患的保护](#)
- [未受到防范各种安全隐患的保护](#)
- [已被 \[Sophos Control Center\]\(#\) 管理](#)
- [已连接到网络中](#)
- [使用的是未及时升级的保护](#)
- [显示需要注意的警报](#)
- [未连接到网络中](#)
- [未被 \[Sophos Control Center\]\(#\) 管理](#)
- [本地配置](#)
- [遵照统一配置](#)
- [隐藏](#)

本节还将告诉您怎样 [打印安全隐患摘要和计算机列表](#)。

### 9.1 哪些计算机已受到保护？

#### 哪些计算机已受到保护？

在 Sophos Control Center 中，查看计算机列表。

计算...	操作系统	警报	是否及...	防病毒	防火墙	统一配置
32C	Windows 2000	错误	是	活动中	活动中	确定
33A	Windows XP	检测到的病毒	是	未活动	未活动	确定
33B	Windows 2000 ...	检测到可能不想...	是	活动中	没有安装	确定
33C	Windows 2003		是	活动中	没有安装	确定

在 [是否及时升级](#) 栏中，“是”字样表示 Sophos 保护在相应的计算机上已及时升级。时钟图标和“否”字样表示 Sophos 保护没有及时升级。

在 [防病毒](#) 栏中，“活动中”字样表示读写扫描正在保护相应的计算机。灰白的盾牌和“未活动”字样则表示没有读写扫描保护。



只要用户的工作站受到读写扫描的保护，通常不需要在 Windows 2000 或 Windows 2003 的文件服务器上运行读写扫描。

如果软件没有安装在相应的计算机上，您会看到“没有安装”字样出现在此栏中。

在 [防火墙](#) 栏中，“活动中”字样表示防火墙正在保护相应的计算机。灰白的防火墙图标和“未活动”字样则表示没有防火墙保护。如果软件没有安装在相应的计算机上，您会看到“没有安装”字样出现在此栏中。

### 9.2 哪些计算机未受到保护？

#### 哪些计算机未受到保护？

在 Sophos Control Center 中，查看计算机列表。

计算...	操作系统	警报	是否及...	防病毒	防火墙	统一配置
32C	Windows 2000	错误	是	活动中	活动中	确定
33A	Windows XP	检测到的病毒	是	未活动	未活动	确定
33B	Windows 2000 ...	检测到可能不想...	否	活动中	没有安装	确定
33C	Windows 2003		是	活动中	没有安装	确定

在 是否及时升级 栏中，时钟图标和“否”字样，表示 Sophos 保护未及时升级。

要根据计算机是否及时升级来排序计算机列表，请单击 是否及时升级 栏的标题。

在 防病毒 栏中，灰白的盾牌和“未活动”字样，表示读写扫描没有保护相应的计算机。

在 防火墙 栏中，灰白的防火墙图标和“未活动”字样，表示防火墙没有保护相应的计算机。



只要用户的工作站受到读写扫描的保护，通常不需要在 Windows 2000 或 Windows 2003 的文件服务器上运行读写扫描。

## 9.3 哪些计算机已被管理？

### 哪些计算机已被管理？

您可以显示已被 Sophos Control Center 管理的计算机的列表。

在 视图 下拉菜单中，单击 已管理的计算机。



在所有计算机的列表中，没有被管理的计算机的详情是灰白显示的。

## 9.4 哪些计算机已连接？

### 哪些计算机已连接？

您可以显示目前已连接到网络中，并受到 Sophos Control Center 管理的计算机列表。

在 视图 下拉菜单中，单击 已连接的计算机。

## 9.5 哪些计算机的软件未及时升级？

### 哪些计算机的软件未及时升级？

您可以用两种方式识别仍使用未及时升级的防病毒软件的计算机。

#### 检查计算机列表中的图标

查看计算机列表。如果某计算机在 是否及时升级 栏中，出现时钟图标和“否”字样，则该计算机需要升级。

#### 只显示未及时升级的计算机

您可以显示未及时升级的计算机的列表。在 视图 下拉菜单中，选择 未及时升级的计算机。



要单独升级计算机，请在列表的计算机名上，单击右键并选择 升级。

## 9.6 哪些计算机带有未处理的警报？

### 哪些计算机带有未处理的警报？

您可以用两种方式识别仍带有未处理的警报(如：病毒警报)的计算机。

#### 检查计算机列表中的图标

查看计算机列表。如果某计算机在 警报 栏中出现警报图标，则表示该计算机上出现警报。

如果某计算机上有多个警报，则显示优先级最高的警报的图标。

要了解更多有关警报图标的信息，请参见 [图标含义](#)。

### 只显示发出警报的计算机

您可以显示发出警报的计算机的列表。在 **视图** 下拉菜单中，选择 **发出警报的计算机**。



要了解出现警报的原因，请高亮显示计算机列表中的计算机名，单击右键，然后选择 **查看计算机详情**。

## 9.7 哪些计算机未连接？

### 哪些计算机未连接？

您可以显示目前未连接到网络中的计算机的列表。

在 **视图** 下拉菜单中，单击 **未连接的计算机**。

如果某计算机未连接到网络中，在计算机列表中的该计算机名旁边会出现一个红色的叉。



## 9.8 哪些计算机未被管理？

### 哪些计算机未被管理？

您可以显示未被 Sophos Control Center 管理的计算机的列表。

在 **视图** 下拉菜单中，单击 **未管理的计算机**。



在所有计算机的列表中，您可以确定没有被 Sophos Control Center 管理的计算机，因为所有这样的计算机的详情都是灰白显示的。

## 9.9 哪些是本地配置的计算机？

### 哪些是本地配置的计算机？

您可以用两种方式识别防病毒或防火墙软件是本地配置的计算机。

#### 只显示本地配置的计算机

您可以只显示本地配置的计算机。

在 **视图** 下拉菜单中，选择 **防病毒本地配置的计算机** 或 **防火墙本地配置的计算机**。

#### 检查单个的计算机

要查看单个的计算机是否是本地配置，请在该计算机名上单击右键。

如果 **使用统一防病毒配置** 没有打勾，那么该计算机上的防病毒软件是本地配置的。

如果 **使用统一防火墙配置** 没有打勾，那么该计算机上的防火墙软件是本地配置的。

## 9.10 哪些计算机遵照统一配置？

### 哪些计算机遵照统一配置？

您可以查看是否所有的计算机都遵照了，通过 Sophos Control Center 统一完成的防病毒，升级，和防火墙配置。

查看计算机列表。在 **统一配置** 栏中，“是”字样表示该计算机遵照了统一配置。

如果某计算机没有遵照统一配置(例如：如果已从该计算机上更改了该计算机的配置，并且该计算机没有在 Sophos Control Center 中标记为本地配置)，您会在 **统一配置** 栏中看到黄色的警报标识和“已更改”字样。

如果某计算机上没有安装任何安全软件，您会在该计算机旁的 **统一配置** 栏中看到“没有安装”字样。如果软件是 **本地配置** 的，您将会看到“本地配置”。如果某计算机正在等待来自 Sophos Control Center 的统一配置，您会在 **统一配置** 栏中看到“等待”字样。

要重新将统一配置应用到某计算机，请高亮显示该计算机，右击，然后选择 **重新应用统一配置**。

## 9.11 哪些计算机被隐藏了？

### 哪些计算机被隐藏了？

您可以显示被隐藏的计算机的列表，这些计算机在所有其它的计算机列表中都是被隐藏的。

在 视图 下拉菜单中，单击 隐藏的计算机。

要再次显示某个被隐藏的计算机，右击该计算机名称，然后选择 显示。

## 9.12 打印安全隐患摘要和计算机列表

### 打印安全隐患摘要和计算机列表

您可以打印出计算机上的安全隐患摘要，以及所选视图的计算机列表。

1. 在 Sophos Control Center 窗口中，在工具栏中单击 打印。会出现 打印 对话框。
2. 设置打印选项，并单击 确定。所打印的文档中将包括以下信息：

- \$ 公司名
- \$ 打印时间
- \$ 显示在摘要窗格中的信息
- \$ 所选视图的计算机列表中所显示的数据

## 10 怎样配置扫描？

### 怎样配置扫描？

您可以使用 Sophos Control Center 更改 Sophos Anti-Virus 保护网络中的计算机的方式。

要查看针对不同操作系统的扫描选项的列表，请参见 [针对不同操作系统的扫描选项](#)。

本节将告诉您怎样：

- [确保启用了读写扫描保护](#)
- [启用扫描可能不想安装的应用程序](#)
- [启用扫描打包文件内部](#)
- [设置读写扫描选项](#)
- [更改扫描的文件类型](#)
- [从读写扫描中排除项目](#)
- [设置自动清除选项](#)
- [批准可以使用的应用程序](#)
- [计划扫描网络中的计算机](#)
- [设置计划扫描选项](#)
- [从计划扫描中排除项目](#)

如果您愿意，您还可以 [单独配置计算机](#)。

## 10.1 扫描病毒，特洛伊木马，间谍软件和蠕虫

### 扫描病毒，特洛伊木马，间谍软件和蠕虫

依照默认值，只要用户试图读写文件时，Sophos Anti-Virus 就会自动扫描其中是否包含病毒，特洛伊木马，间谍软件，以及蠕虫等。

1. 在 配置 菜单中，单击 配置扫描。
2. 在 配置扫描设置 对话框中，在 配置 Sophos Anti-Virus 面板中，确保勾选了 启用读写扫描 勾选框。

您可以配置 Sophos Anti-Virus：

- [扫描可能不想安装的应用程序](#)
- [在设定的时间扫描计算机](#)

## 10.2 扫描可能不想安装的应用程序

### 扫描可能不想安装的应用程序

依照默认值，Sophos Anti-Virus 可以检测病毒，特洛伊木马，间谍软件，以及蠕虫等。您还可以配置它检测可能不想安装的应用程序。



该选项只能应用于运行在 Windows2000 或以后的计算机上的 Sophos Anti-Virus 中。

Sophos 建议您使用计划扫描来检测可能不想安装的应用程序作为开始。这使您能够安全地处理那些已经在网络中运行的应用程序。然后，您从那以后可以启用读写扫描来保护计算机。

1. 在 **配置** 菜单中，单击 **配置扫描**。
2. 在 **配置扫描设置** 对话框中，在 **计划扫描** 面板中，单击 **添加** 创建新扫描，或在列表中选择某个扫描，并单击 **编辑** 以编辑它。
3. 在 **计划扫描设置** 对话框中，单击 **配置**（在页面底部）。
4. 在 **扫描和清除设置** 对话框中，单击 **扫描** 标签页。在 **其它扫描选项** 面板中，确保 **扫描可能不想安装的应用程序** 已被选择。单击 **确定**。
5. 当扫描完成时，Sophos Anti-Virus 可能会报告发现某些“可能不想安装的应用程序”。

如果您想要在计算机上运行这些应用程序，您必须 [批准它们](#)。否则，[删除它们](#)。

6. 如果您想要启用读写扫描，请在 **配置扫描设置** 对话框中，单击 **读写扫描**。在出现的 **读写扫描设置** 对话框中，在 **扫描选项** 中，选择 **扫描可能不想安装的应用程序**。



有些应用程序会“监控”文件，并试图频繁地访问文件。如果您启用了读写扫描，它会检测到每一次这样的访问，并发出多个警报。请参见 [有关可能不想安装的应用程序的频繁警报](#)。

## 10.3 设置读写扫描选项

### 设置读写扫描选项

要设置读写扫描选项：

1. 在 **配置** 菜单中，单击 **配置扫描**。
2. 在 **配置扫描设置** 对话框中，单击 **读写扫描** 按钮。
3. 在 **读写扫描设置** 对话框中，按照以下说明选择选项。

#### 扫描级别

Sophos 建议您不要改变 **普通** 扫描级别的选择。

#### 扫描选项

##### 扫描打包文件内部

您可以选择扫描打包文件内部。不过，在启用该选项之前，请了解以下信息。



当您访问打包文件时，读写扫描会自动检测打包文件内部。因此，扫描打包文件内部是可选的。



扫描打包文件内部会对计算机的运行产生影响，并不建议在读写扫描中使用。

##### 扫描可能不想安装的应用程序

依照默认值，Sophos Anti-Virus 可以检测病毒，特洛伊木马，间谍软件，以及蠕虫等。您还可以配置它检测可能不想安装的应用程序。



该选项只能应用于运行在 Windows2000 或以后的计算机上的 Sophos Anti-Virus 6 中。

Sophos 建议您使用计划扫描来检测可能不想安装的应用程序作为开始。这使您能够安全地处理那些已经在网络中运行的应用程序。然后，您从那以后可以启用读写扫描来保护计算机。要了解详情，请参见 [扫描可能不想安装的应用程序](#)。

#### 读写扫描特性

您的防病毒软件自动在“读写”文件时进行扫描。依照默认值，当用户打开文件时（“读文件时”）进行扫描。

您还可以选择在用户进行其它操作时，扫描文件。如果您想要在关闭文件时，扫描文件，请选择 **写文件时**；或者，如果您想要在重新命名文件时，扫描文件，请选择 **重命名时**。



这些选项针对向计算机中写入内容和/或重新命名文件，提供更有力的防病毒保护。不过，这些增加的运行活动，或许会影响到计算机的运行效率。

### 可移动介质

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)，请选择 允许访问引导区感染病毒的驱动器。

## 10.4 更改扫描的文件类型

### 更改扫描的文件类型

依照默认值，Sophos Anti-Virus 将扫描所有容易受到病毒感染的文件类型。您可以在扫描中添加文件类型，或者，选择从扫描中排除某些文件类型。

默认扫描的文件类型，会因操作系统不同而不同，当产品升级时也会有变化。要查看文件类型列表，请到相应的操作系统的计算机上，打开 Sophos Anti-Virus 窗口，找到“扩展名”配置页面。



这些选项只应用于 Windows 计算机。



您可以使用 Sophos Update Manager 在 MacOS X 计算机上进行更改，Sophos Update Manager 是随 Sophos Anti-Virus for Mac OS X 一道提供的实用工具程序。要开启 Sophos Update Manager，在 MacOS X 计算机上，在 **Finder** 窗口中，浏览找到 Sophos Anti-Virus:ESOSX 文件夹。双击 **Sophos Update Manager**。欲知更多详情，请参见 Sophos Update Manager 帮助文件。



在 Windows 2000 或以后的计算机上，您可以分别更改读写扫描和计划扫描的设置。在 Windows 98/Me 的计算机上，在计划扫描的设置中所做的更改，同样适用于读写扫描的设置。

要更改扫描的文件类型

1. 在 **配置** 菜单中，单击 **配置扫描**。会出现 **配置扫描设置** 对话框。  
要配置读写扫描，请在 **配置 Sophos Anti-Virus** 面板中，单击 **读写扫描**。  
要配置计划扫描，请在 **计划扫描** 面板中，单击 **扩展名和排除文件**。
2. 在出现的对话框中，单击 **扩展名** 标签页。选择 **允许精确控制扫描** 的项目。  
要扫描添加的文件类型，单击 **添加**，然后在“扩展名”文本框中，输入文件扩展名，如：**PDF**。  
要排除某些通常默认扫描的文件类型，请单击 **排除**。这会打开 **排除文件类型** 对话框。请输入文件扩展名。

### 扫描不带扩展名的文件

依照默认值，不带扩展名的文件会被扫描。

## 10.5 从读写扫描中排除项目

### 从读写扫描中排除项目

本节将告诉您怎样从读写扫描中排除项目(如：驱动器，文件夹，或文件)。

您还可以通过在 **排除文件扩展名列表** 中添加文件扩展名，来将某些类型的文件从扫描中排除。有关怎样将某些类型的文件从扫描中排除的指导，请参见 [更改扫描的文件类型](#)。



这些“排除项目”选项仅应用于 Windows 2000 或以后和 MacOS X 计算机中。



要在 Windows 98/Me 计算机上排除项目，请使用 [计划扫描配置页](#)，在此所做的配置同样应用于读写扫描。

1. 在 **配置** 菜单中，单击 **配置扫描**。
2. 在 **配置扫描设置** 对话框中，单击 **读写扫描** 按钮。
3. 在 **读写扫描设置** 对话框中，单击 **Windows 排除项目** 或 **MAC 排除项目** 标签页。要将项目添加到列表中，单击 **添加**，并在 **排除项目** 文本框中，输入完整路径。

您能够排除的项目，根据计算机的操作系统的不同会有所不同。欲了解详情，请参见 [不能从扫描中排除的项目](#)。

### 排除远程文件

该选项可以避免 Sophos Anti-Virus 扫描网络驱动器上的文件。

## 10.6 设置自动清除

### 设置自动清除

您可以在一旦发现病毒时，就立即在计算机中自动清除它们。要做到这一点，请按照以下说明，更改读写扫描设置。



读写扫描不能清除可能不想安装的应用程序。您应该按照[清除可能不想安装的应用程序](#)中的说明处理它们。按照稍后的说明，您还可以启用在计划扫描中自动清除未批准的应用程序。

### 要自动清除病毒(读写扫描和计划扫描)

1. 在 **配置** 菜单中，单击 **配置扫描**。
2. 要更改读写扫描的设置，在 **配置扫描设置** 对话框中，单击 **读写扫描** 按钮。在 **读写扫描设置** 对话框中，单击 **清除** 标签页。  
要更改计划扫描的设置，在 **配置扫描设置** 对话框中，选择计划扫描，并单击 **编辑**。在 **计划扫描设置** 对话框中，单击 **配置**。在 **扫描和清除设置** 对话框中，单击 **清除** 标签。
3. 勾选 **自动清除感染项目中的病毒**。
4. 您还可以指定如果清除失败，应该采取什么措施。选项为：

- \$ 不采取措施
- \$ 删除
- \$ 移至默认的路径
- \$ 移至 **UNC** 路径(这里的 **UNC** 路径是您指定的完整的 **UNC** 路径)。



Mac 计算机无法读取 **UNC** 路径。如果您选择移至，并指定了路径，MacOSX 计算机仍会将感染项目移至默认的路径。

### 要自动清除可能不想安装的应用程序(仅限计划扫描)

1. 在 **配置** 菜单中，单击 **配置扫描**。
2. 在 **配置扫描设置** 对话框中，选择该计划扫描，然后，单击 **编辑**。
3. 在 **计划扫描设置** 对话框中，单击 **配置**。
4. 在 **扫描和清除设置** 对话框中，单击 **清除** 标签。
5. 选择 **自动清除可能不想安装的应用程序**。这将使 Sophos Anti-Virus 能够删除您的计算机上，没有事先[批准](#)的可能不想安装的应用程序。



该选项只能应用于运行在 Windows 2000 或以后的计算机上的 Sophos Anti-Virus 中。



要了解怎样通过 **处置警报和错误** 对话框，清除您的计算机中的病毒或可能不想安装的应用程序，请参见[清除病毒](#)或[清除可能不想安装的应用程序](#)。

## 10.7 批准可以使用的应用程序

### 批准可以使用的应用程序

如果您已经启用了 Sophos Anti-Virus 检测可能不想安装的应用程序，则有可能造成不能使用您想要使用的应用程序。

您可以按照以下说明，批准想要使用的应用程序。

1. 在 **配置** 菜单中，单击 **配置扫描**。
2. 在 **配置扫描设置** 对话框中，单击 **批准应用程序** 按钮。
3. 在 **批准应用程序** 对话框中，在 **已知的应用程序** 列表中，选择您想要批准的应用程序。单击 **添加** 将其添加到 **已批准的应用程序** 列表中。对每个您想要批准的应用程序，重复以上步骤。单击 **确定**。
4. 如果您不能在列表中看到想要批准的应用程序，请单击 **新项目**。在 **添加新的应用程序** 对话框中，单击 **Sophos 可能不想安装的应用程序链接**。找到您想要批准的应用程序，并将它的名称输入 **名称** 文本框中。单击 **确定**。

## 10.8 在设定的时间扫描计算机

### 在设定的时间扫描计算机

您可以在设定的时间扫描计算机。

1. 在 **配置** 菜单中，单击 **配置扫描**。
2. 在 **配置扫描设置** 对话框中，在 **计划扫描** 面板中，单击 **添加**。
3. 在 **计划扫描设置** 对话框中，请输入扫描任务的名称。
4. 选择扫描项目：
  - \$ 扫描本地硬盘
  - \$ 软盘和可移动驱动器
  - \$ 光盘驱动器
5. 依照默认值，所有的本地硬盘都会被扫描。
5. 选择您想要运行扫描的日期和时间。

要查看计划扫描的默认设置的列表，请参看[计划扫描的默认设置](#)。

如果您想要更改默认的扫描，或更改扫描的清除选项，请单击 **计划扫描设置** 对话框底部的 **配置** 按钮。要了解更多的信息，请参见[设置计划扫描选项](#)或[设置自动清除选项](#)。

要了解怎样在计划扫描中更改所扫描的文件类型，或者排除特定的文件，请参见[更改扫描的文件类型](#)或[从计划扫描中排除项目](#)。

## 10.9 设置计划扫描选项

### 设置计划扫描选项

要设置计划扫描选项：

1. 在 **配置** 菜单中，单击 **配置扫描**。
2. 在 **配置扫描设置** 对话框中，选择某个计划扫描，然后，单击 **编辑**。
3. 在 **计划扫描设置** 对话框中，单击 **配置**。
4. 在 **扫描和清除设置** 对话框中，单击 **扫描** 标签页。

#### 扫描级别

Sophos 建议您不要改变 **普通** 扫描级别的选择。

#### 扫描选项

##### 扫描打包文件内部

您可以选择扫描打包文件内部。不过，在启用该选项之前，请了解以下信息。



当您访问打包文件时，读写扫描会自动检测打包文件内部。因此，扫描打包文件内部是可选的。

##### 扫描可能不想安装的应用程序



该选项只能应用于运行在 Windows 2000 或以后的计算机上的 Sophos Anti-Virus 6 中。

该选项是默认选项。如果您不想在扫描运行时，扫描可能不想安装的应用程序，请取消勾选该勾选框。

## 10.10 从计划扫描中排除项目

### 从计划扫描中排除项目

本节将告诉您怎样从计划扫描中排除项目(如：驱动器，文件夹，或文件)。

您还可以通过在 **排除文件扩展名列表** 中添加文件扩展名，来将某些类型的文件从扫描中排除。有关怎样将某些类型的文件从扫描中排除的指导，请参见[更改扫描的文件类型](#)。



在 Windows 98/Me 的计算机上，在计划扫描的设置中所做的更改，同样适用于读写扫描的设置。

1. 在 **配置** 菜单中，单击 **配置扫描**。会出现 **配置扫描设置** 对话框。
2. 在 **计划扫描** 面板中，单击 **扩展名和排除文件**。
3. 在 **计划扫描扩展名和排除文件名** 对话框，单击 **排除文件** 标签页。要将项目添加到列表中，单击 **添加**，并在 **排除项目** 文本框中，输入完整路径。

您能够排除的项目，根据计算机的操作系统的不同会有所不同。欲了解详情，请参见[不能从扫描中排除的项目](#)。

## 10.11 单独配置计算机的扫描

### 单独配置计算机的扫描

如果您想要某些计算机使用的配置选项，与在 Sophos Control Center 中统一设置的不同，请按照以下说明做：

1. 在计算机列表中，高亮选择相关的一个或多个计算机。单击右键，取消选择 **使用统一防病毒配置**。
2. 现在，请到计算机上单独配置防病毒选项。

要到计算机上单独配置防病毒选项，右键单击 Sophos Anti-Virus 任务栏图标(如下所示)。



单击打开 **Sophos Anti-Virus**。在 **Sophos Anti-Virus** 窗口中，单击 **配置 Sophos Anti-Virus**。然后，在 **配置** 中单击 **读写扫描** 并编辑设置。



欲知怎样单独配置计算机的更多信息，请参见 **Sophos Anti-Virus** 帮助文件。或者，请参见 *Sophos Anti-Virus Small Business Edition for Windows 用户手册* 或 *Sophos Anti-Virus Small Business Edition for Mac OS X 用户手册*。您可以在 **Sophos** 安装 CD 中找到这些用户手册。

## 11 怎样配置通告？

### 怎样配置通告？

您可以配置 **Sophos Control Center** 在检测到安全隐患，以及从 **Sophos** 下载升级出现问题时，发出警报。您还可以配置 **Sophos Control Center** 发送报告，提供在您所设定的期间内，所检测到的安全隐患的数量，及其详情。除此之外，您可以选择 **Sophos Control Center** 处理旧警报的方式，以及指定针对警报采取措施时，所允许的时间。

本节将告诉您怎样：

- [设置安全隐患和出错警报](#)
- [设置升级警报](#)
- [设置定期发送报告](#)
- [删除旧警报](#)
- [指定允许针对警报采取措施的时间](#)

### 11.1 设置扫描警报

#### 设置扫描警报

如果在网络中检测到了病毒或可能不想安装的应用程序，**Sophos Control Center** 可以向您发送警报。它还可以就扫描错误向您发出警报。

1. 在 **配置** 菜单，单击 **配置通告**。
2. 在 **配置通告** 对话框中，单击 **扫描警报** 标签页。然后，按照以下说明，选择您想要的警报类型，以及发送方式。

#### 事件

选择您想要为此发出警报的事件。您可以选择收到在网络中检测到病毒的警报，收到在网络中检测到可能不想安装的应用程序的警报，以及收到扫描出错的警报。

#### 警报发送方式

要通过电子邮件寄送警报，请选择 **电子邮件**。单击 **配置**，然后输入您的 **SMTP** 服务器地址，以及回复地址。然后，单击 **添加**，输入警报将要寄至的电子邮件地址。

要通过桌面消息发送警报，请选择 **桌面消息发送**。该选项是默认选项，并且只在被感染的计算机上显示警报。请输入您想要 **Sophos Control Center** 在桌面消息中显示的文字。

### 11.2 设置升级警报

#### 设置升级警报

**Sophos Control Center** 可以就升级过程或问题向您发出警报。

1. 在 **配置** 菜单，单击 **配置通告**。
2. 在 **配置通告** 对话框中，单击 **升级警报** 标签页。然后，按照以下说明，选择您想要的警报类型。

#### 警报发送方式

##### 电子邮件

选择 **电子邮件**。单击 **配置**，然后输入您的 **SMTP** 服务器地址，以及回复地址。然后，单击 **添加**，输入警报将要寄至的电子邮件地址。

##### 网络消息发送

选择 **网络消息发送** 使 Sophos Control Center 能够向指定的计算机发送网络消息。单击 **添加**，并输入网络消息将要寄至的计算机的名称。当计算机收到网络消息时，会弹出显示消息文字的消息框。

Windows 98/Me 计算机必须运行 WinPopup 应用程序，才能收到消息。

### 事件日志记录

如果您想要 Sophos Control Center 将下载的全部详情记录到计算机的事件日志中，请选择 **使用详尽模式的事件日志记录**。

## 11.3 设置定期发送报告

### 设置定期发送报告

Sophos Control Center 可以发送报告，提供在您所设定的期间内，所检测到的安全隐患的数量，及其详情。

收件人将收到包含以下信息的电子邮件报告：

- 报告日期
- 公司名
- 检测到的病毒，特洛伊木马，以及蠕虫的数量
- 检测到的可能不想安装的应用程序的数量
- 防火墙警报的数量
- 按照发生的时间顺序，列示安全隐患的名称和感染的数量
- 按照发生的时间顺序，列示应用程序的名称和相关计算机的数量

1. 在 **配置** 菜单，单击 **配置通告**。
2. 在 **配置通告** 对话框中，单击 **报告发送** 标签页。然后，按照以下说明，启用和设置报告发送通告。

#### 启用报告发送

勾选 **启用报告发送** 勾选框。

#### 报告发送设置

##### 公司名

输入将出现在报告中的您的公司名称。公司名称会出现在所有报告中，无论是由电子邮件寄发的自动生成的报告，还是在 [通过报告发送对话框创建的报告](#)。

##### 选择日期

选择在一星期中的哪一天，通过电子邮件将报告寄送给您选择的收件人。报告会每星期寄送一次，寄发时间是您所选择的寄送日期的凌晨 00:01。

##### 报告格式

请选择将寄送给您的收件人的报告的文本格式。报告可以用 HTML，CSV，或纯文本格式发送。

##### 保存报告

您还可以将报告保存到磁盘上。单击 **报告** 将保存在以下路径中：**栏**旁边的 **浏览** 按钮，选择保存报告的路径。

##### 电子邮件收件人

在 **电子邮件收件人** 面板中，单击 **配置**，然后输入您的 SMTP 服务器地址，以及回复地址。然后，单击 **添加**，输入警报将要寄至的电子邮件地址。

## 11.4 删除旧警报

### 删除旧警报

您可以设置 Sophos Control Center 自动删除旧警报。

1. 在菜单栏中，打开 **工具** 菜单，选择 **选项**。会出现 **选项** 对话框。
2. 单击 **警报** 标签页。在 **清空** 面板中，根据您发送报告的要求，选择您想怎样处理旧警报。有三种选项：

- § 不要清空旧警报。
- § 清空早于  $n$  个月的警报(这里的  $n$  是您指定的数字)。
- § 限制警报的数量为  $m$ (这里的  $n$  是您指定的数字)。

依照默认值，警报将在数据中保存 12 个月之后被删除。

## 11.5 指定允许针对警报采取措施的时间

### 指定允许针对警报采取措施的时间

在清除计算机上的安全隐患时，如果在清除超时期间内，没有收到计算机的响应，清除操作将被视为失败。

 清除超时期间 是允许从计算机收到响应的时间长度(时间长度的计算为自从 Sophos Control Center 向计算机发出操作指令起)。

要指定清除超时期间：

1. 在菜单栏中，打开 **工具** 菜单，选择 **选项**。会出现 **选项** 对话框。
2. 单击 **警报** 标签页。在 **清除失败警报** 面板中，输入以小时计的清除超时期间。默认的期间为 1 小时。

## 12 怎样配置防火墙？

### 怎样配置防火墙？

 防火墙只作为 Sophos Computer Security 和 Sophos Security Suite 产品的一部分提供。

本节将说明怎样设置防火墙并更改关键设置。特别地，本节将告诉您怎样：

- [安装防火墙](#)
- [开启和关闭防火墙](#)
- 设置防火墙

设置防火墙时，您可以选择下列选项之一：

- [厂商设置](#)
- [自定义设置](#)

“自定义设置”选项，使您能够更多地控制对防火墙的配置。

如果您愿意，您还可以[单独配置计算机](#)。

### 12.1 使用防火墙保护计算机

#### 使用防火墙保护计算机

 Sophos Client Firewall 只能安装在运行 Windows 2000 或以后的工作站上，它无法被安装在运行服务器操作系统的计算机上。您不应该将 Sophos Client Firewall 安装到已经安装了 Sophos Control Center 的那台计算机上。

 安装 Sophos Client Firewall 要求先安装 Sophos Anti-Virus。

 您必须重新启动每一台已经安装了 Sophos Client Firewall 的计算机，以便激活该防火墙。

如果您在运行 **Sophos** 网络保护向导 时没有安装防火墙，您可以按照以下说明，将防火墙安装到计算机上：

1. 在计算机列表中，高亮选择您想要安装防火墙的计算机。在菜单栏中，打开 **工具** 菜单，选择 **添加防火墙到已有防病毒保护的计算机**。防火墙安装向导会启动。
  2. 在向导中的 **Windows 用户帐户详情** 页面中，输入您将用来在网络中的计算机上，安装软件的系统管理员帐户详情。单击 **下一步**。
  3. 在 **在工作站上安装 Sophos Client Firewall** 页中，选择您想要安装防火墙的计算机。单击 **下一步**。
- 您将看到防火墙正在被安装到计算机上。
4. 在 **必须手动保护的计算机** 页中，如果有必须手动保护的计算机，您会看到一个计算机列表，列表中的计算机需要手动安装防火墙。单击 **打印**，打印该列表。完成该向导。
  5. 到打印出的列表中的各台计算机上，以系统管理员身份登录，按照以下说明安装 Sophos Client Firewall。

浏览找到您从中安装 Sophos Control Center 的那台计算机上的升级文件夹(默认为 \\<您的服务器名称>\Sophos\SAV\SCFXP)，然后运行 setup.exe 文件。在 **设置** 对话框中，勾选 **安装 Sophos Client Firewall** 勾选框，并单击 **确定**。

## 12.2 开启或关闭防火墙

### 开启或关闭防火墙

依照默认值，防火墙是启用的，不过，您也可以禁用防火墙，这样会允许网络中所有的通讯流。



对于日常使用，Sophos 建议您保持防火墙为 已启用 状态。

您可以在 Sophos Control Center 中统一地开启或关闭防火墙，也可以在计算机上单独地开启或关闭防火墙。

#### 要在 Sophos Control Center 中关闭防火墙：

1. 在 配置 菜单，单击 配置防火墙。 防火墙配置向导 会启动。
2. 在向导中的 启用防火墙 页面中，不要勾选 开启防火墙 勾选框。 向导完成。

#### 要在计算机上单独关闭防火墙：

1. 在计算机列表中，高亮选择相关的计算机。单击右键，取消选择 使用统一防火墙配置。
2. 现在，按照以下的说明，在计算机上单独关闭防火墙。

找到 Sophos 防火墙任务栏图标(如下所示)。



在图标上单击右键，在显示的菜单中，选择 配置。

在 **Sophos Client Firewall** 配置编辑器 对话框中，单击 常规 标签页，并选择 允许所有通讯流。单击 确定

## 12.3 防火墙厂商设置

### 防火墙厂商设置

当您首次安装防火墙时，它会被启用，并使用一组默认(暨厂商)设置。如果您想要更多地控制对防火墙的配置，请参见 [自定义防火墙配置](#)。

#### 什么是厂商设置？

依照默认值，防火墙将：

- 在并不询问各台计算机用户，要求进行确认的情况下，应用各种规则，这也就是，工作在“非交互”模式中(从而使您的计算机用户的工作不受打扰)。
- 允许所有流出的通讯流(不计算应用程序的检查和)。
- 阻断所有未批准的流入的通讯流。
- 允许文件和打印共享。
- 允许基本的网络功能。



要了解防火墙厂商设置的完整列表，请查看此链接：<http://www.sophos.com/support/knowledgebase/article/6608.html>。

#### 还原厂商设置

如果您在更改了防火墙的设置后，想要还原防火墙的厂商设置，请按照以下说明做：

1. 在 配置 菜单，单击 配置防火墙。 防火墙配置向导 会启动。
2. 在向导中的 启用防火墙 页面中，确保勾选了 开启防火墙 勾选框。单击 下一步。
3. 在 保护类型 页面中，选择 厂商设置。
4. 在最后的页面中，单击 完成，结束向导。

## 12.4 自定义防火墙配置

### 自定义防火墙配置

要通过创建自定义规则来配置防火墙：

1. 在 配置 菜单，单击 配置防火墙。 防火墙配置向导 会启动。
2. 在向导中的 启用防火墙 页面中，确保勾选了 开启防火墙 勾选框。单击 下一步。
3. 在 保护类型 页面中，选择 自定义设置。
4. 在 文件和打印共享 页中，如果您想要允许局域网中的其它计算机访问打印机，以及您计算机上的共享文件夹，请选择 允许文件和打印共享。

5. 在 **网络通讯流规则** 页中，请选择下列选项之一。

- § 阻断流入的通讯流，并允许流出的通讯流。
- § 阻断流入和流出的通讯流。

如果您选择该选项，除了您通过单击选项右边的 **信任** 按钮来指定的应用程序以外，防火墙将阻断所有流出的通讯流。对于“信任的”应用程序，会被允许进行所有的网络活动。

- § 创建自定义规则

该选项使您能够完全控制防火墙设置。您可以使用高级防火墙配置编辑器，为所有通讯流创建自定义规则。



这是高级选项，您应该只有在能够明白，您所做的更改将产生的后果的情况下，才使用这一选项。

要打开 **高级防火墙配置** 对话框，请单击 **创建自定义规则** 选项右边的 **自定义** 按钮。

要了解所有防火墙选项的详情，请参见 **Sophos Client Firewall 帮助文件**。

## 12.5 单独配置计算机上的防火墙

### 单独配置计算机上的防火墙

如果您想要某些计算机使用的配置选项，与在 **Sophos Control Center** 中统一设置的不同，请按照以下说明做：

1. 在计算机列表中，高亮选择相关的计算机。单击右键，取消选择 **使用统一防火墙配置**。
2. 现在，按照以下的说明，在计算机上单独配置防火墙选项：

找到 **Sophos 防火墙** 任务栏图标(如下所示)。



在图标上单击右键，在显示的菜单中，选择 **配置**。

在 **Sophos Client Firewall 配置编辑器** 对话框中，编辑防火墙设置。



这是高级选项，您应该只有在能够明白，您所做的更改将产生的后果的情况下，才使用这一选项。

要了解所有防火墙选项的详情，请参见 **Sophos Client Firewall 帮助文件**。

## 13 怎样生成报告？

### 怎样生成报告？

您可以生成有关网络中的警报的报告。

本节将告诉您怎样：

- [生成报告](#)
- [以表的形式显示报告](#)
- [以图的形式显示报告](#)
- [显示每个安全隐患的警报数](#)
- [显示每台计算机的警报数](#)
- [显示警报率](#)
- [显示警报历史记录](#)
- [打印报告](#)
- [导出报告到文件](#)
- [更改报告页面布局](#)

您还可以配置 **Sophos Control Center** 发送报告，提供在您所设定的期间内，所检测到的安全隐患的数量，及其详情。要了解怎样设置这一报告功能，请参见 [设置定期设置报告](#)。

### 13.1 生成报告

#### 生成报告

要创建报告，请按照以下说明做。

1. 在 **Sophos Control Center** 窗口中，在工具栏中单击 **报告**。会出现 **报告发送** 对话框。

- 在下拉菜单中，单击您想要发送的报告类型。

§ 按照安全隐患给出警报 将显示在网络中检测到的每个安全隐患的警报数。  
 § 按照计算机给出警报 将显示每台计算机或每组计算机中的警报数。  
 § 按照时间给出警报 将显示在设定的时间内发生警报的次数。  
 § 警报历史记录 将显示每个警报的完整详情。

在 配置 标签页，您可以自定义报告发送。

然后，单击 表 或 图 标签页查看报告。

## 13.2 以表的形式显示报告

### 以表的形式显示报告

- 在 Sophos Control Center 窗口中，在工具栏中单击 报告。
- 在 报告发送 对话框下拉菜单中，选择您想要创建的报告类型。在 配置 标签页中，配置报告。然后，单击 表 标签页。
- 会出现表。 报告描述 会出现在各页的上方，摘要显示创建该报告的标准(如：涉及的时间长度)。

## 13.3 以图的形式显示报告

### 以图的形式显示报告



不能以图的形式显示“警报历史记录”的报告。

- 在 Sophos Control Center 窗口中，在工具栏中单击 报告。
- 在 报告发送 对话框的下拉菜单中，选择您想要创建的报告类型。在 配置 标签页中，配置报告。然后，单击 图 标签页。
- 会出现图。 报告描述 会出现在各页的上方，摘要显示创建该报告的标准(如：涉及的时间长度)。

## 13.4 显示每个安全隐患的警报数

### 显示每个安全隐患的警报数

- 在 Sophos Control Center 窗口中，在工具栏中单击 报告。
- 在 报告发送 对话框的下拉菜单中，选择 按照安全隐患给出警报。
- 在 配置 标签页中，您可以选择以下说明的选项。在完成之后，单击其中之一的标签页，以显示图或表形式的报告。

#### 报告的时间跨度

在 时间跨度 文本框中，单击下拉箭头，并选择时间跨度。您既可以选择固定的时间跨度，如：上月，也可以选择 自定义，并在 始于 和 止于 文本框中指定您自己的时间。

#### 路径

单击 组计算机 或 单个计算机。然后，单击下拉箭头指定组或计算机的名称。

#### 过滤

依照默认值，报告列示的 只限于病毒，以及每个病毒的警报数。

不过，您可以更改安全隐患的列示 只限于可能不想安装的应用程序 或 所有安全隐患（即：病毒和可能不想安装的应用程序）。

您还可以配置报告显示：

- § 引发最多的警报的  $n$  个安全隐患(这里的  $n$  为您指定的数字)，或者
- § 引发超过某个指定数量的警报的安全隐患。

#### 排序

依照默认值，报告列示的安全隐患是按照每个安全隐患的警报数降序排列的。如果您想以字母为序按照安全隐患名称列示，请勾选 安全隐患名。

## 13.5 显示每台计算机的警报数

### 显示每台计算机的警报数

1. 在 Sophos Control Center 窗口中，在工具栏中单击 **报告**。
2. 在 **报告发送** 对话框的下拉菜单中，选择 **按照计算机给出警报**。
3. 在 **配置** 标签页中，您可以选择以下说明的选项。在完成之后，单击其中之一的标签页，以显示图或表形式的报告。

### 报告的时间跨度

在 **时间跨度** 文本框中，单击下拉箭头，并选择时间跨度。您既可以选择固定的时间跨度，如：上月，也可以选择 **自定义**，并在 **始于** 和 **止于** 文本框中指定您自己的时间。

### 过滤

依照默认值，报告列示的只限于病毒，以及每个计算机的警报数。不过，您可以更改安全隐患的列示只限于可能不想安装的应用程序或所有安全隐患（即：病毒和可能不想安装的应用程序）。

或者，您可以配置报告只显示带有某种特定的安全隐患的计算机。要指定单个的安全隐患，单击 **显示具有这类安全隐患的计算机** 文本框的下拉箭头，然后，单击列表中的安全隐患名称。要指定多于一个的安全隐患，请在文本框中输入名称，使用通配符。使用 **?** 替代名称中的单个字符，使用 **\*** 替代名称中的任意字符串。例如：W32/\* 将指定所有的名称以 W32/开头的病毒。

依照默认值，报告将显示所有计算机。不过，您可以配置它仅显示 **S** 带有最多的警报的 **n** 个计算机（这里的 **n** 为您指定的数字），或者，**S** 带有超过某个指定数量的警报的计算机。

### 排序

依照默认值，报告列示的计算机是按照每个计算机的警报数降序排列的。如果您想以字母为序按照计算机名称列示，请勾选 **计算机**。

## 13.6 显示警报率

### 显示警报率

1. 在 Sophos Control Center 窗口中，在工具栏中单击 **报告**。
2. 在 **报告发送** 对话框的下拉菜单中，选择 **按照时间给出警报**。
3. 在 **配置** 标签页中，您可以选择以下说明的选项。在完成之后，单击其中之一的标签页，以显示图或表形式的报告。

### 报告的时间跨度

在 **时间跨度** 文本框中，单击下拉箭头，并选择时间跨度。您既可以选择固定的时间跨度，如：上月，也可以选择 **自定义**，并在 **始于** 和 **止于** 文本框中指定您自己的时间。

### 路径

单击 **组计算机** 或 **单个计算机**。然后，单击下拉箭头指定组或计算机的名称。

### 过滤

依照默认值，报告列示的只限于病毒，以及每个病毒的统计数字。

如果您想要有关可能不想安装的应用程序的统计数字，或者所有安全隐患的统计数字，请使用 **仅显示这些安全隐患类型** 下拉菜单。

如果您想要报告仅显示特定的某个或某组安全隐患的统计数字，请使用 **仅显示这些安全隐患** 文本框。要指定单个的安全隐患，请单击下拉箭头，并单击列表中的安全隐患名。要指定多于一个的安全隐患，请在文本框中输入名称，使用通配符。使用 **?** 替代名称中的单个字符，使用 **\*** 替代名称中的任意字符串。例如：W32/\* 将指定所有的名称以 W32/开头的病毒。

### 测算警报率的时间间隔

要指定测算警报率的时间间隔，如：每小时或每天，请单击下拉箭头，并选择时间间隔。

## 13.7 显示警报历史记录

### 显示警报历史记录

1. 在 Sophos Control Center 窗口中，在工具栏中单击 **报告**。
2. 在 **报告发送** 对话框的下拉菜单中，选择 **警报历史记录**。
3. 在 **配置** 标签页中，您可以选择以下说明的选项。在完成之后，单击 **表** 标签页，以显示报告。

### 报告的时间跨度

在 **时间跨度** 文本框中，单击下拉箭头，并选择时间跨度。您既可以选择固定的时间跨度，如：上月，也可以选择自定义，并在 **始于** 和 **止于** 文本框中指定您自己的时间。

### 路径

选择 **组计算机** 或 **单个计算机**。然后，单击下拉箭头指定组或计算机的名称。

### 过滤

依照默认值，报告所列表的内容只限于病毒。不过，您可以更改安全隐患的列示只限于可能不想安装的应用程序或所有安全隐患（即：病毒和可能不想安装的应用程序）。

如果您想要有关可能不想安装的应用程序的统计数字，或者所有安全隐患的统计数字，请使用 **仅显示这些安全隐患类型** 下拉菜单。要指定单个的安全隐患，请单击下拉箭头，并单击列表中的安全隐患名。要指定多于一个的安全隐患，请在文本框中输入名称，使用通配符。使用 **?** 替代名称中的单个字符，使用 **\*** 替代名称中的任意字符串。例如：W32/\* 将指定所有的名称以 W32 开头的病毒。

### 排序

依照默认值，警报详情根据 **安全隐患名** 排序。不过，警报也可以根据 **计算机名称** 或 **日期和时间**。

## 13.8 打印报告

### 打印报告

要打印报告，单击报告上方工具栏中的 **打印** 图标。



## 13.9 导出报告到文件

### 导出报告到文件

要导出报告到文件

1. 单击报告上方工具栏中的 **导出** 图标。



2. 在 **导出报告** 对话框中，选择您想要导出的文件格式。选项为：

- § PDF (Acrobat)
- § HTML
- § Microsoft Excel
- § Microsoft Word
- § 多文本格式 (RTF)
- § CSV
- § XML

3. 单击 **文件名** 文本框的 **浏览** 按钮，选择路径。
4. 在 **另存为** 对话框中，浏览找到您想要保存报告的路径，输入保存报告的文件名，然后单击 **保存**。
5. 在 **导出报告** 对话框中，单击 **确定**。

## 13.10 更改报告页面布局

### 更改报告页面布局

您可以报告的页面布局。例如，您可以使用横向(宽页)页面布局格式显示报告。

1. 单击报告上方工具栏中的 **页面布局** 图标。



2. 在 **页面设置** 对话框中，请指定页面大小，方向和页边距。单击 **确定**。这样报告会根据页面设置来呈现。

当您打印或导出报告时，同样会使用这些页面设置。

## 14 排疑解难

### 排疑解难

本节将说明怎样处理在使用 Sophos Control Center 的过程中可能会出现的问题。

- [清除失败](#)
- [有关可能不想安装的应用程序的频繁警报](#)

### 14.1 清除失败

#### 清除失败

如果无法统一清除某个安全隐患，请到被感染的计算机上，进行手动清除。

如果安全隐患还是没有被清除，要寻求帮助处理它，您应该：

1. 记下安全隐患的名称。
2. 在 **信息** 菜单中，单击 **查看安全隐患信息**，以链接到 Sophos 网站中的安全隐患分析页面中。
3. 在安全隐患分析页面中，搜索该安全隐患。跟随链接查看清除建议。

如果您自己无法清除该安全隐患，您应该：

1. 在 **信息** 菜单中，单击 **技术支持**。
2. 请输入安全隐患名称，以及受影响的计算机的详情。然后，寄发电子邮件。

### 14.2 有关可能不想安装的应用程序的频繁警报

#### 有关可能不想安装的应用程序的频繁警报

您可能会收到大量的有关可能不想安装的应用程序的警报，包括多次报告同一个应用程序。

发生这种情况，是因为有一些类型的可能不想安装的应用程序会“监控”文件，试图频繁访问这些文件。如果您启用了读写扫描，Sophos Anti-Virus 会检测到每一次这样的文件访问，并发出警报。

您应该做下列之一：

- 禁用读写扫描可能不想安装的应用程序。您可以使用计划扫描作为替代。
- [批准应用程序](#)（如果您想要在计算机上运行该应用程序）。
- [清除应用程序](#)—您没有批准的应用程序。