SOPHOS

Sophos Enterprise Console 版本 3.1
用户手册

文档日期：2008 年 4 月

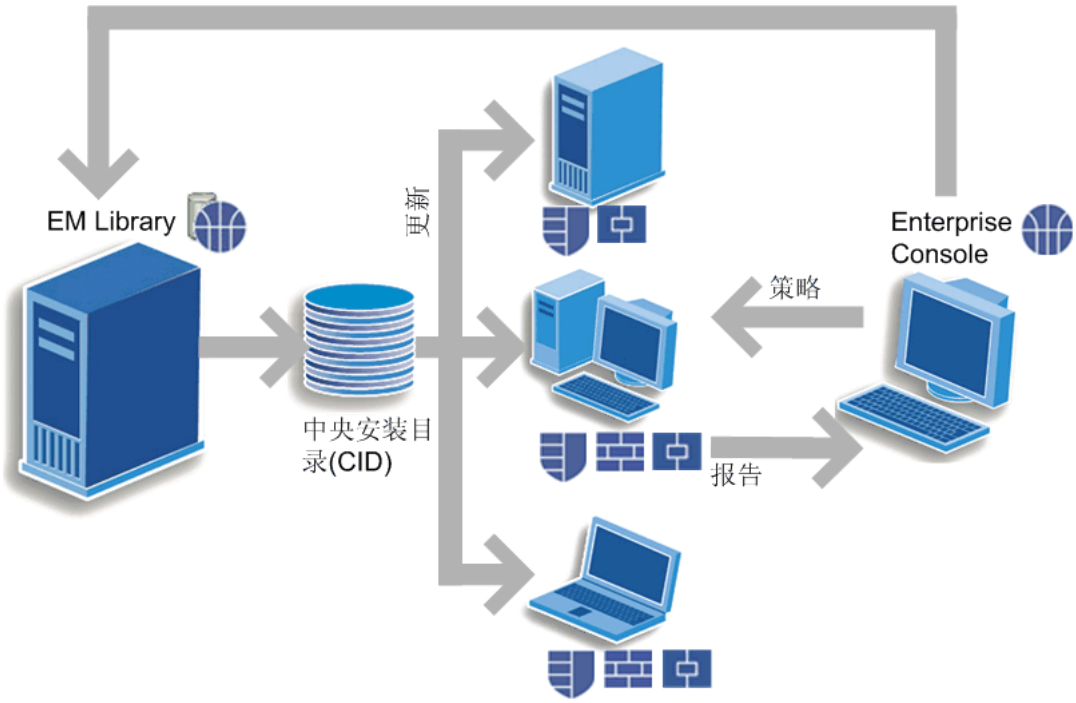
目录

1 关于 Sophos Endpoint Security and Control

关于 Sophos Endpoint Security and Control

Sophos Endpoint Security and Control 可以为文件服务器，台式机和笔记型电脑，防范已知的，和未知的计算机安全隐患，广告软件，以及其它的可能不想安装的应用程序，和不想要的程序行为；并提供简明，统一的网络管理。它由 Sophos Anti-Virus，Sophos Client Firewall，Sophos Network Access Control，以及 Sophos Enterprise Console （包括用于从 Sophos 自动下载软件和更新文件的 EM Library）组成。

以下示意图，说明 Sophos Endpoint Security and Control 组件是怎样共同工作的。



Sophos Enterprise Console 使您能够在计算机上统一部署，更新，以及监控防病毒和防火墙软件，由此防范病毒，蠕虫，特洛伊木马，间谍软件，黑客，未知的计算机安全隐患，以及不想要的程序行为。Enterprise Console 中包括用于从 Sophos

自动下载软件和更新文件的 EM Library。

Sophos Anti-Virus（用于 Windows 98/Me/2000 及以后，Mac OS X，Linux，以及 UNIX）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，还可以检测和阻断未知的计算机安全隐患，广告软件，以及其它可能不想安装的应用程序，不想要的程序行为。

特别地，Sophos Anti-Virus 能够：

- 针对安全隐患，可疑文件，广告软件，以及其它可能不想安装的应用程序，对计算机或网络进行扫描。
- 针对安全隐患和可疑行为，对所访问的每一个文件进行检查。
- 在发现安全隐患，可疑文件，或不想要的应用程序时，发出警报。
- 从文件或磁盘引导区中删除病毒，从而清除项目的感染。
- 阻止可能不想安装的应用程序在计算机上运行。
- 删除计算机上的可能不想安装的应用程序。
- 阻断“受控程序”— 正当合法的用户应用程序，但是，可能影响工作效率，以及网络运行表现。
- 记录活动日志。
- 保持更新，以检测最新的安全隐患和可能不想安装的应用程序。

Sophos Client Firewall（用于 Windows 2000 及以后）可以只允许特许的某应用程序，或某类应用程序进入公司网络或因特网。它可以事先锁定计算机，保护网络免遭来自未受保护的计算机，特别是直接与因特网连接的计算机的，因特网蠕虫，黑客，和病毒的侵袭。

Sophos Network Access Control (NAC)（供 Windows 2000 及以后的计算机使用）可以防范未遵照策略或者未得到信任的计算机连接到公司的网络中。它可以控制基于安全策略集并受到系统管理员管理的网络访问，并且能够强制实施策略遵

照。

要了解更多有关 Sophos EM Library，Sophos Anti-Virus，Sophos Client Firewall，或者 Sophos Network Access Control 的信息，请分别参见相应的帮助文件或用户手册。

要了解更多有关计算机安全隐患的信息，请访问：Sophos 安全信息网页。

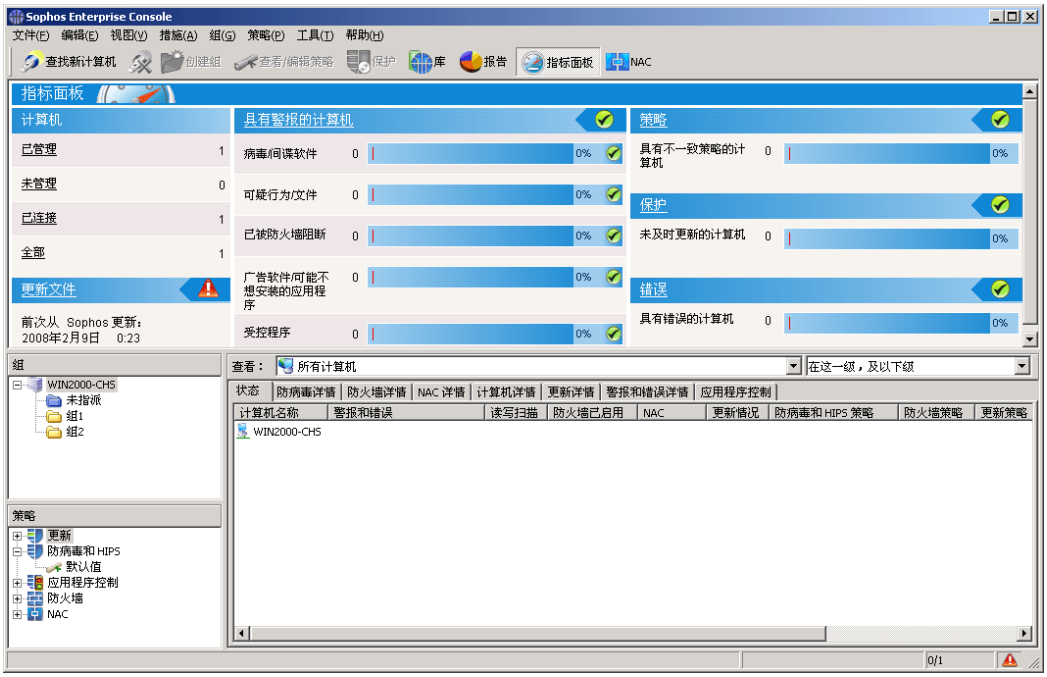
2 介绍 Enterprise Console

本节向您概述 Sophos Enterprise Console 的界面和主要功能

- 关于界面
- 什么是组？
- 什么是策略？
- 什么是未指派文件夹？
- 什么是库？
- 图标的含义

关于界面

Enterprise Console 的界面帮助您保护网络中的计算机，确保能够计算机及时更新，以及查看任何检测到的安全隐患，潜在的安全隐患，或不安装的应用程序，并将它们清除。请参见以下对各功能的说明。



指标面板

指标面板 可以提供对网络安全状态的“一览图”。要显示或隐藏指标面板，单击工具栏中的 **指标面板** 按钮。

组窗格板

在 **组** 窗格板中，您可以创建组，并将联网计算机放置到组中。您可以自己创建组，或者从 Active Directory 导入组，导入的组中可以带有计算机，也可不带有计算机。您还可以设置与 Active Directory 同步化，这样 Active Directory 中的新计算机和组，以及其它更改，都会自动复制到 Enterprise Console 中。

未指派 文件夹用于尚未放置到组中的计算机。要管理某个组，请选择并右击它。

策略窗格板

在 **策略** 窗格板中，您创建，或者，更改应用到计算机组中的那些策略。要管理某个策略，请选择并右击它。

计算机列表

计算机列表（右手边的窗格板）显示被选中的组中的计算机。

如果您有从控制台管理的 Linux 或 UNIX 计算机，请确保为每台计算机配置了唯一的主机名。否则，每台计算机都将以默认的名称 “localhost ”出现在控制台中。

状态 标签页，显示计算机是否受到读写扫描的保护，是否启用了防火墙，是否启用了 NAC（网络访问控制），以及是否及时更新了软件。该页还显示是否出现了任何警报。其它的标签页会就上述的每个方面，给出更多的详细信息。

要了解出现在计算机列表中的图标的含义，请参见图标的含义

任务栏

查找新计算机 是搜索网络中的计算机，并将其添加到控制台中。

创建组 是为计算机创建新的组。

查看/编辑策略 使您能够打开和更改在 **策略** 窗格板中选择的策略。

保护 使您能够将防病毒软件和防火墙软件，安装到在计算机列表中选择的计算机上。

库 可以开启 Sophos EM Library，您可以使用它下载最新的软件包，并将其提供到网络中。

报告 使您能够生成有关网络中的各种警报的报告。

指标面板 可以打开用于概览网络安全状态的指标面板。

NAC 可以打开 Sophos NAC Manager，您可以用它来编辑 NAC（网络访问控制）策略。

什么是组？

组是用来放置数个计算机的文件夹。

您可以自己创建组，或者从 Active Directory 导入组，导入的组中可以带有计算机，也可不带有计算机。您还可以设置与 Active Directory 同步化，这样 Active Directory 中的新计算机和组，以及其它更改，都会自动复制到 Enterprise Console 中。

每个组都有针对更新，防病毒和 HIPS 保护，防火墙保护，应用程序控制，以及 NAC（网络访问控制）的设置。属于组的所有计算机通常应该使用这些设置，它被称为“策略”。

组可以包含子组。

什么是策略？

策略是可以应用于一个组中的所有计算机上的所有设置的集合。

- **更新** 策略 指定计算机更新新安全软件的方式。
- **防病毒和 HIPS** 策略 指定安全软件扫描和清除计算机中的病毒，特洛伊木马，蠕虫，间谍软件，广告软件，可能不想安装的应用程序，可疑行为，以及可疑文件的方式。
- **应用程序控制** 策略 指定要在您的计算机上阻断哪些应用程序，允许哪些应用程序。
- **防火墙** 策略 指定防火墙软件保护计算机的方式。
- **NAC** 策略 指定在访问网络之前，必须遵照的条件。

什么是未指派文件夹？

未指派文件夹是，Enterprise Console 在您将计算机放入组中之前，放置计算机的文件夹。

您不能够：

- 将策略应用到 未指派 文件夹。
- 在 未指派 文件夹中创建子文件夹。
- 移动或删除未指派文件夹。

什么是库？

库从 Sophos 下载最新的软件，并将其放到您的服务器上，供网络中的计算机安装。

一个称为 EM Library 的组件，用来保持库处于及时更新的状态。要使用 EM Library，请单击工具栏中的 **库** 图标。

图标的含义

在计算机的列表中，图标会用来表明：

- 警报
- 保护被禁用，或者未及时更新。
- 每台计算机的状态，如：软件是否正在被安装。

警报

标志	释意
	出现在 **警报和错误** 栏中的红色警报标志表明，检测到了病毒，蠕虫，特洛伊，间谍软件，或可疑行为。
	出现在 **警报和错误** 栏中的黄色警告标志表明，以下情况之一： • 检测到了可疑文件。 • 检测到了广告软件或其它可能不想安装的应用程序。 • 检测到了受控程序。 • 防火墙已阻断了某个应用程序。 • 出现错误。 出现在 **防病毒和 HIPS 策略防火墙策略更新策略**，或 **应用程序控制策略** 栏中的黄色警告标志表明，计算机使用的相应的策略与同组的其它计算机的不一致。

如果计算机中出现了多个警报和错误，具有最高的优先级的警报的图标，会出现 **警报和错误** 栏中。以下列示的警报类型，以降序排列优先级。

警报优先级

1. 病毒／间谍软件警报
2. 可疑行为警报
3. 可疑文件警报
4. 防火墙警报
5. 广告软件／可能不想安装的应用程序警报
6. 受控程序警报
7. Sophos Anti-Virus，更新，以及 Sophos Client Firewall 错误。

保护被禁用，或者没有及时更新。

标志	释意
	灰色的盾牌说明读写扫描处于没有激活状态。
	灰色防火墙标志说明防火墙处于禁用的状态。
	时钟图标说明所使用的软件没有及时更新。

计算机状态

标志	释意
	蓝色的计算机标识说明，该计算机已被 Enterprise Console 管理。
	带有黄色箭头的计算机标识说明，防病毒软件和防火墙软件的安装处于等待状态。
	带有绿色箭头的计算机标识说明，软件的安装正在进行中。
	带有沙漏的计算机标识说明，Sophos Anti-Virus 的自动更新组件已安装，并且正在下载软件的最新版本。
	灰色的计算机标志说明，该计算机未被 Enterprise Console 管理。
	旁边带有红色叉的计算机标识说明，该计算机已断开了连接。

3 怎样开始使用？

您可以按照以下说明，使用 Enterprise Console 保护网络中的计算机：

这只是一个概要，您也许还要参考涉及的其它内容和章节。

- 步骤 1：为软件和更新文件建立库
- 步骤 2：创建组
- 步骤 3：设置策略
- 步骤 4：添加计算机到控制台
- 步骤 5：保护计算机
- 步骤 6：检查计算机是否已被保护
- 步骤 7：防范广告软件，其它可能不想安装的应用程序 (PUA)，以及可疑或不想要的程序行为。
- 步骤 8：清除计算机

步骤 1：为软件和更新文件建立库

在安装了 Enterprise Console 之后，您需要设置“库”，库将用于从 Sophos 下载和更新计算机安全软件和数据，并使您的联网计算机可以使用它们。

在您首次启动 Enterprise Console 时，会出现 **欢迎使用 Sophos Endpoint Security** 对话框。在对话框中，选择您想要设置类型。有两个选项：

- **快速设置** – 如果您想要使用默认设置，快速预订 Sophos 更新文件，请选择此选项。这会启动 **预订 Sophos 更新文件向导**。您所选择的软件会被放置到默认路径，并每小时更新一次。如果您使用 Active Directory，组和计算机将从 Active Directory 中导入 Enterprise Console。

- **高级设置** – 如果您想要更多地控制库的设置，请选择此选项。这将打开 EM Library 控制台。要了解怎样用它设置库，请参见 EM Library 帮助文件中的 "How do I get started?" 部分。

在您首次启动 Enterprise Console 时，会出现 **欢迎使用 Sophos Endpoint Security** 对话框，该对话框只会出现一次。在您关闭了此对话框之后，它将不再出现，您从此将不能使用 **快速设置** 选项。

步

骤 2：创建组

根据最适合您的情况，您可以在以下三种方法中选择创建组的方式。

- **使用快速设置选项**

  如果您使用 Active Directory，并且按照步骤 1中的说明，选择了 **快速设置** 选项，那么，**预订 Sophos 更新文件向导** 就已经将组和计算机从 Active Directory 中导入到 Enterprise Console 中了。在这种情况下，您不必进行任何操作。

- **依次创建组**

  您可以使用 **创建组** 选项，依次地创建组。要依次创建组，请单击工具栏上的 **创建组** 图标。会有一个新组出现在 **组** 窗格板中。请重命名它。要了解更多的信息，请参见 怎样创建和使用组？

- **从 Active Directory 中导入组**

  您可以从 Active Directory 导入组结构，带有或不带有计算机。要从 Active Directory 导入组结构，请按照从 Active Directory 中导入组中的指导说明做。

步

骤 3：设置策略

更新策略

如果您在安装了 Enterprise Console 之后，选择了 **快速安装** 选项，并完成了 **预订 Sophos 更新文件向导**，默认的更新策略就已经设置了。

⚠ 如果您没有完成 **预订 Sophos 更新文件向导**，请输入获取更新文件的路径的详情（请参见 设置自动更新）。直到更新策略中包含更新路径之前，计算机不会被保护和更新。

要了解更多的配置更新的信息，请参见怎样更新计算机？

防病毒和 HIPS 策略

如果您想要更改扫描和设置警报，双击 **防病毒和 HIPS**。然后，单击 **默认值**。请参见怎样更改防病毒和 HIPS 设置？以及怎样设置警报？

应用程序控制策略

要了解设置应用程序控制策略的指导说明，请参见怎样更改应用程序控制设置？

防火墙策略

要了解配置防火墙策略的指导说明，请参见怎样更改防火墙设置？

NAC 策略

要了解配置 NAC 策略的指导说明，请参见怎样更改 NAC 设置？

步

骤 4：添加计算机到控制台

根据最适合您的情况，您可以在以下四种方法中选择添加组到

控制台的方式。

- **使用快速设置选项**

  如果您使用 Active Directory，并且按照步骤1中的说明，选择了 **快速设置** 选项，那么，**预订 Sophos 更新文件向导** 就已经将组和计算机从 Active Directory 中导入到 Enterprise Console 中了。在这种情况下，您不必进行任何操作。

- **使用查找新计算机选项**

  在工具栏中，单击 **查找新计算机** 图标。选择您想要使用的搜索方式，单击 **确定**，然后，按照出现的向导或对话框中的指导说明做。要了解更多详情，请参见 怎样将计算机添加到控制台中？

  如果您使用 **从 Active Directory 导入** 之外的选项，请单击 **未指派** 文件夹，查看所找到的计算机。选择您要将其放入新组中的计算机。将所选的计算机拖放到新建的组中。

- **从 Active Directory 中导入组和计算机**

  或者，选择一个您想将 Active Directory 容器和计算机导入的组，右击并选择 **从 Active Directory 导入**。您还可以在 **组** 菜单中选择 **导入 Active Directory**。该选项在上面说明的 **查找新计算机** 对话框中可以找到。

  按照 **从 Active Directory 导入向导** 中的指导说明做。要在导入组时，也导入计算机，请在 **从 Active Directory 导入向导** 里的 **请选择导入什么** 页面中，选择 **计算机和组**。要了解更多信息，请参见 从 Active Directory 导入组。

- **与 Active Directory 同步化**

  选择您想要与 Active Directory 同步化的组，右击并选择 **与 Active Directory 同步化**。或者，在 **组** 菜单中，选择 **与 Active Directory 同步化**。按照 **与 Active Directory 同步化向导** 中的指导说明做。要了解更多的信息，请参见怎样与 Active Directory 同步化？

步

骤 5：保护计算机

根据最适合您的情况，您可以在以下二种方法中选择保护联网计算机的方式。

- **使用保护计算机向导**

  当您从 **未指派** 文件夹中将计算机拖放到组中时，会有一个向导启动，帮助您保护计算机。请参见怎样保护新加入网络中的计算机？

  如果您想要使用 Sophos Client Firewall，请先只将它安装到几台有代表性的计算机上。防火墙必须先配置好之后，再安装到所有的计算机上，因为防火墙是用来防止未经授权的应用程序访问网络的。请参见设置防火墙。

  按照保护要求手动安装的计算机中的说明，保护要求手动安装的计算机。

- **在与 Active Directory 同步化时自动保护计算机**

  如果您选择了与 Active Directory 同步化，您还可以选择自动保护 Windows 2000 或以后的计算机。您可以在 **与 Active Directory 同步化向导**中，或者在 **同步化属性** 对话框中，这样做。要了解操作指导，请参见 自动保护计算机。

  运行 Windows 95/98/Me，Windows Server，Mac，Linux，或 UNIX 等操作系统的计算机，不会自动被保护。您必须，按照保护要求手动安装的计算机中的说明，手动保护这样的计算机。

步

骤 6：检查计算机是否已被保护

当安装完成时，再次查看在新组中的计算机列表。在 **读写扫描** 栏中，您应该看到 '活动中 '的字样。这表明该计算机已受到读写

扫描的保护，并且受到 Enterprise Console 的管理。要了解更多的有关信息，请参见 怎样检查网络是否受保护？

步

骤 7：防范广告软件，其它可能不想安装的应用程序 (PUA)，以及可疑或不想要的程序行为。

依照默认值，Sophos Anti-Virus 会检测病毒，特洛伊木马，蠕虫，以及间谍软件。Windows 2000 及以后的计算机上的 Sophos Anti-Virus 7 及以后，还可以分析在系统中运行的程序的行为。要添加进一步的保护，您可以：

- 扫描可疑文件
- 扫描广告软件／可能不想安装的应用程序
- 控制您的网络的应用程序

步

骤 8：清除计算机

如果在您的网络中检测到了病毒，或其他项目，或可能不想安装的应用程序，请按照 怎样清除计算机？ 中的说明，清除受影响的计算机。

4 怎样创建和使用组？

本节将说明怎样创建和管理计算机组。

在规划和创建组结构时，请记住良好的组结构应该是：

- 可以管理的

  您必须决定您将要创建的组，可以管理的规模是多大。您应该能够方便地部署软件，扫描和清除计算机。这对初始的部署尤其重要。

- 体现公司中不同用户的需要

  在创建组时考虑用户的个别需要。例如，如果您想要在某些计算机上阻断某个应用程序，但是在另一些计算机上允许该应用程序运行，那么，您应该为此创建两个不同的组。

您可以自己手动创建组，并设置组结构，也可以从 Active Directory 导入组结构。

如果您想要创建与您的 Active Directory 容器中的组相对应的组结构，请参见 从 Active Directory 导入组。

- 组是干什么的？
- 创建组
- 添加计算机到组
- 从组中删除计算机
- 剪切和粘贴组
- 删除组
- 重命名组
- 将策略应用到组
- 查看组采用的策略

组是干什么的？

在保护和管理计算机之前，您必须创建组，并将计算机放到组中。

组是很有用的，因为您可以：

- 从不同的更新源，或者，按照不同的时间计划，更新不同组中的计算机。
- 对不同的组使用不同的防病毒和 HIPS，应用程序控制，防火墙，或 NAC（网络访问控制）策略。
- 更轻松地管理计算机。

您可以在组中创建组，并应用特定的策略集到每个组和子组。

创建组

要为计算机创建新组，请按以下说明做：

1. 在 **组** 窗格板（控制台左手边）中，选择您要创建新组的位置。如果您要创建一个新的最高一级的组，请单击最高一级的那台计算机的名称。如果您要创建一个子组，请单击某个现存的组。
2. 在工具栏，单击 **创建组** 图标。
3. 一个 '新组 '已被添加到列表中，该组的名称会高亮显示。为该组输入新的名称。

更新，防病毒和 HIPS，应用程序控制，防火墙，以及 NAC（网络访问控制）将会自动应用到新组中。您可以编辑这些策略，或者，应用不同的策略。

如果新建的组是一个子组，它在创建时会使用它所在的组的设置。

添加计算机到组

要添加计算机到组，请按以下说明做：

1. 选择您要添加到组中的计算机。比如，单击 **未指派** 文件夹，并从中选择计算机。
2. 将所选的计算机拖放到新建的组中。

如果您从 **未指派** 文件夹中将未受到保护的计算机，移至某一设置了自动更新的组中时，向导程序会启动，指导您为其设置保护。

如果您将计算机从一个组移到另一个组，它们将采用与所移入的组中的其它计算机相同的策略。

从组中删除计算机

您可以从组中删除计算机，比如，您想删除已不在网络中的计算机。

如果您所删除的是仍然在网络中的计算机，控制台将不会再列示和管理它们。

要删除计算机：

1. 选择您要删除的计算机。
2. 右击并选择 **删除**。

如果您想再次查看该计算机，请单击工具栏中的 **查找新计算机** 图标。这些计算机只有在重新启动后，才会被显示为是已管理的计算机。

剪切和粘贴组

要剪切和粘贴组，请按以下说明做：

1. 选择您要剪切和粘贴的组。在 **编辑** 菜单中，单击 **剪切**。
2. 选择您要将剪切下来的组，粘贴到其中的组。在 **编辑** 菜单中，单击 **粘贴**。

删除组

要删除组，请按以下说明做：

任何在被删除的组中的计算机，都将被置入 **未指派** 文件夹。

1. 选择您要删除的组。
2. 右击并选择 **删除**。在得到提示时，确认您想要删除的组，以及它的子组，如果该组带有任何子组。

重命名组

要重命名组，请按以下说明做：

1. 选择您要重新命名的组。
2. 右击并选择 **重新命名**。

将策略应用到组

您可以按照以下说明，将策略应用到组：

1. 在 **策略** 窗格板中，高亮选择将要应用的策略。
2. 单击该策略，并将其拖放到您想要应用该策略的组中。在出现提示时，确认您想要继续。


或者，您可以右击组，然后，选择 **查看组策略详情**。接着，您就可以从下拉菜单中为组选择所要应用的策略。

查看组采用的策略

要查看组采用了哪些策略，请按照以下说明做：

1. 在 **组** 窗格板中，右击该组。选择 **查看组策略详情**。
2. 在组详情对话框中，您可以查看当前所应用的策略。

5 怎样创建和使用策略？

本节将说明怎样创建策略，以及将它们应用到计算机组中。本节还将告诉您怎样确保，组中的所有计算机使用相同的更新，防病毒和 HIPS，应用程序控制，防火墙，以及 NAC（网络访问控制）策略设置。

- 策略是干什么的？
- 什么是默认的策略？
- 需要创建自己的策略吗？

- 创建策略
- 应用策略
- 编辑策略
- 重命名策略
- 删除策略
- 查看采用策略的组
- 检查计算机是否使用组策略
- 使计算机采用组策略

策略是干什么的？

策略是可以应用于一个组中的所有计算机上的所有设置的集合。

- **更新** 策略 指定计算机更新新安全软件的方式。
- **防病毒和 HIPS** 策略 指定安全软件扫描和清除计算机中的病毒，特洛伊木马，蠕虫，间谍软件，广告软件，可能不想安装的应用程序，可疑行为，以及可疑文件的方式。
- **应用程序控制** 策略 指定要在您的计算机上阻断哪些应用程序，允许哪些应用程序。
- **防火墙** 策略 指定防火墙软件保护计算机的方式。
- **NAC** 策略 指定在访问网络之前，必须遵照的条件。

每一种类型的策略，您都可以创建多个策略。

您可以将同一个策略应用到多个组中。

什么是默认的策略？

安装 Enterprise Console 时，会为您创建 '默认的 ' 策略。

更新策略

默认的更新策略提供：

- 只要策略中包括获取更新文件的路径的详情，就会每隔五分钟进行一次自动更新。

如果您在安装了 Enterprise Console 之后，选择了 **快速安装** 选项，并完成了 **预订 Sophos 更新文件向导**，默认的更新策略中已经包括了更新路径。

如果您没有完成 **预订 Sophos 更新文件向导**，请输入获取更新文件的路径的详情（请参见 设置自动更新）。直到更新策略中包含更新路径之前，计算机不会被保护和更新。

防病毒和 HIPS 策略

默认的防病毒和 HIPS 策略提供：

- 读写扫描病毒／间谍软件（但不包括可疑文件，广告软件和其它可能不想安装的应用程序）。
- 分析运行在系统（Windows 2000 及以后中的 Sophos Anti-Virus 7）中的程序的代码执行情况。
- 在所涉及的计算机桌面上，显示安全警报，并添加安全警报到事件日志中。

应用程序控制策略

依照默认值，所有程序和程序类型都将被允许。读写扫描受控程序是禁用的。

防火墙策略

依照默认值，Sophos Client Firewall 会被启用，并会阻断所有可有可无的网络通讯流。在您启用它之前，您在整个网络中使用它之前，您应该按照设置防火墙中的说明，配置防火墙，以便允许使用您想要使用的应用程序。

该防火墙的其它默认设置如下：

- 不要求用户的确认信息，就应用各种规则（'非交互'模式）。
- 如果在已管理的计算机上，规则被个别地更改了，就会在

Enterprise Console 中显示警报。

- 如果其它应用程序更改了内存，就会阻断线程。
- 扣下发送到被封闭了的端口的通讯包（“隐形”）操作。
- 使用总和检查识别新的和被更改过的应用程序。
- 向 Enterprise Console 报告新的和被更改过的应用程序。
- 针对可能会启动隐藏线程的应用程序发出警报。

NAC 策略

依照默认值，计算机会被允许进入网络（除非您已经修改了默认策略，或者，更改了 NAC 服务器上的“策略模式”）。

需要创建自己的策略吗？

安装 Enterprise Console 时，会为您创建“默认的”策略。这些策略将应用到您创建的任何组中。

默认策略提供了基本的安全防范，但是，如果您想要使用诸如“网络访问控制”或“应用程序控制”等功能，那么，需要创建新的策略，或者更改默认策略。

更新策略

如果，您在安装了 Enterprise Console 之后，选择了 **快速安装** 选项，并完成了 **预订 Sophos 更新文件向导**，那么，默认的更新策略就已经设置了。

如果您没有完成 **预订 Sophos 更新文件向导**，请输入获取更新文件的路径的详情（请参见 设置自动更新）。直到更新策略中包含更新路径之前，计算机不会被保护和更新。

防病毒和 HIPS

默认的防病毒和 HIPS 策略将保护计算机防范病毒和其它恶意软件。不过，您可能还想创建新的策略，或者，更改默认策略，以便能够检测其它的不想要的应用程序或行为。请参见怎样更改防病毒和 HIPS 设置？

应用程序控制

您需要配置应用程序控制策略，以便指定可以使用哪些应用程序。请参见怎样更改应用程序控制的设置？

防火墙

您需要配置防火墙，以便允许应用程序可以在您的计算机上使用。请参见设置防火墙。

NAC

依照默认值，Sophos NAC 允许所有的计算机访问网络。您需要配置 NAC 策略，以便控制网络访问。请参见编辑 NAC 策略。

创建策略

要创建策略，请按以下说明做：

您无法创建 NAC 策略。您只能编辑它们。请参见编辑 NAC 策略。

1. 在 **策略** 窗格板中，右击您想要创建的策略的类型，如：“更新策略”，然后，选择 **创建策略**。
2. “新策略”将被添加到列表中，该组的名称会高亮显示。为该策略输入新的名称。
3. 双击该新策略。输入您想要的设置。

   要了解怎样设置不同的策略，请参见：

   怎样更改防病毒和 HIPS 设置？

   怎样更改应用程序控制的设置？

   怎样更改防火墙设置？

   怎样更新计算机？

至此，您已经创建了可以应用到组的策略。

应用策略

您可以按照以下说明，将策略应用到组：

1. 在 **策略** 窗格板中，高亮选择将要应用的策略。
2. 单击该策略，并将其拖放到您想要应用该策略的组中。在出现提示时，确认您想要继续。

或者，您可以右击组，然后，选择 **查看组策略详情**。接着，您就可以从下拉菜单中为组选择所要应用的策略。

编辑策略

要编辑一个或多个计算机组的策略，请按照以下说明做：

1. 在 **策略** 窗格板中，双击您想要编辑的策略。
2. 编辑设置。

   要了解怎样设置不同的策略，请参见：

   怎样更改防病毒和 HIPS 设置？

   怎样更改应用程序控制的设置？

   怎样更改防火墙设置？

   怎样更改 NAC 设置？

   怎样更新计算机？

重命名策略

要重命名策略，请按以下说明做：

您不能够重新命名 '默认的 ' 策略。

1. 在 **策略** 窗格板中，选择您想要重新命名的策略。
2. 右击并选择 **重命名策略**。

删除策略

要删除策略，请按以下说明做：

⚠ 您不能够删除 '默认的 '策略。

1. 在 **策略** 窗格板中，右击您想要删除的策略，然后选择 **删除策略**。
2. 任何被删除策略的组，都会恢复使用默认策略。

查看采用策略的组

要查看某个特定的策略被哪些组采用了，请按照以下说明做：

1. 在 **策略** 窗格板中，右击您想要查看的策略，然后选择 **查看使用策略的组**。
2. 会出现采用了该策略的组的列表。

检查计算机是否使用组策略

您可以检查组中的所有计算机是否遵照了该组的更新，防病毒和 HIPS，应用程序控制，防火墙，以及 NAC 策略。

1. 选择您要检查的组。
2. 在 **状态** 页中，查看各个策略栏目，例如：**防病毒和 HIPS 策略**。如果某计算机使用的策略与组中的其它计算机不同，您会看到警告符号和 "与组不一致 "的字样。

如果您想要计算机遵照它们的组策略，请参见使计算机采用组策略。

使计算机采用组策略

如果您发现计算机没有遵照它所在的组的更新，防病毒和 HIPS，应用程序控制，防火墙，或 NAC 策略，那么，您可以将组策略应用到该计算机上。

1. 选择没有遵照组策略的一个或数个计算机。
2. 右击并选择 **遵照**。然后选择相应的策略类型，例如：**组防病毒和 HIPS 策略**。

6 怎样将计算机添加到控制台中？

您可以使用“查找新计算机”功能，选择相应的选项，这些选项使您能够查找联网计算机，并将它添加到 Enterprise Console 中。

如果您使用 Active Directory，您可以导入 Active Directory 组结构，以及计算机。

如果您只选择添加计算机，这些计算机将被放置到 **组** 窗格板中的 **未指派** 文件夹中。在您能够保护和管理计算机之前，您必须创建组设置组策略，以及将计算机放置到组中。

使用下列选项之一，可以查找联网计算机，并将它们列示在 Enterprise Console 中：

- 从 Active Directory 导入
- 通过 Active Directory 查找
- 在网络中查找
- 通过 IP 地址范围查找
- 从文件导入

从 Active Directory 导入组

从 Active Directory 导入组，是从 Active Directory 中获取组结构，并将其复制到 Enterprise Console 中。您可以只导入组结构，或同时导入组和计算机。如果您选择后者，在 Active Directory 中找到的计算机会被放置到他们各自的组中，而不是放置到 **未指派** 文件夹。

您可以同时拥有自己创建和管理的“普通”的组，以及从 Active Directory 导入的组。您还可以将导入的组与 Active Directory 同步化。

要从 Active Directory 中导入组：

1. 在工具栏中，单击 **查找新计算机** 图标。
2. 在 **查找新计算机** 对话框中，选择 **从 Active Directory 导入**，并单击 **确定**。**从 Active Directory 导入向导** 会启动。

   或者，选择一个您想将 Active Directory 容器导入的组，右击并选择 **从 Active Directory 导入**。您还可以在 **组** 菜单中选择 **导入 Active Directory**。
3. 在向导的 **概览** 页中，单击 **下一步**。
4. 在 **选择一个 Enterprise Console 组** 页面中，请选择或创建一个您要将计算机和子组导入的 Enterprise Console 组。单击 **下一步**。
5. 在 **选择一个 Active Directory 容器** 页面中，请选择一个从中要将计算机和子组导出的 Active Directory 容器。输入容器名称（如：LDAP://CN=Computers，DC=domain_name，DC=local）或单击 **浏览** 浏览找到 Active Directory 中的容器。单击 **下一步**。
6. 在 **请选择导入什么** 页面中，根据您想要导入什么，选择 **计算机和组** 或 **仅限于组**。
7. 在 **确认您的选择** 页面中，检查详情，然后单击 **下一步** 继续。
8. 在向导的最后一页中，您可以查看已导入的组，计算机的详情。要关闭向导，请单击 **完成**。
9. 在您从 Active Directory 中导入组之后，请应用策略到组中。请参见怎样创建和使用策略？

在您从 Active Directory 中导入了组，并将组策略应用到组之后，如果您愿意，您可以将这些组与 Active Directory 同步化。要了解怎样做，请参见 与 Active Directory 同步化。

使用 Active Directory 查找计算机

您可以使用 Active Directory 查找网络中的计算机，并将它们放入 **未指派** 文件夹中。

1. 在工具栏中，单击 **查找新计算机** 图标。
2. 在 **查找新计算机** 对话框中，选择 **通过 Active Directory 查找** 并单击 **确定**。
3. 您会被提示输入用户名和密码。如果您需要提供帐户详情，才能访问的计算机（如：Windows XP SP 2），您就需要输入用户名和密码。该帐户必须是域管理员帐户，或者，对所要操作的 Windows XP 计算机有完全的管理权限。

   
   如果您使用域帐户名，您**必须**以“域名\用户”的形式输入用户名。
4. 在 **查找计算机** 对话框中，选择您想搜索的域。单击 **确定**。
5. 单击 **未指派** 文件夹，可以查看已经找到的计算机。

开始管理这些计算机之前，请选择它们，并将它们拖放到组中。

使用网络浏览查找计算机

要将在 Windows 域和工作组中找到的计算机的列表添加到 **未指派** 文件夹中。

1. 在工具栏中，单击 **查找新计算机** 图标。
2. 在 **查找新计算机** 对话框中，选择 **在网络中查找** 并单击 **确定**。
3. 您会被提示输入用户名和密码。如果您需要提供帐户详情，才能访问的计算机（如：Windows XP SP 2），您就需要输入用户名和密码。该帐户必须是域管理员帐户，或者，对所要操作的 Windows XP 计算机有完全的管理权

限。

如果您使用域帐户名，您**必须**以“域名\用户”的形式输入用户名。

4. 在 **查找计算机** 对话框中，选择您想搜索的域或工作组。单击 **确定**。
5. 单击 **未指派** 文件夹，可以查看已经找到的计算机。

开始管理这些计算机之前，请选择它们，并将它们拖放到组中。

使用 IP 地址范围查找计算机

您可以使用 IP 地址范围查找网络中的计算机，并将它们放入 **未指派** 文件夹中。

您无法使用 IPV6 地址。

1. 在工具栏中，单击 **查找新计算机** 图标。
2. 在 **查找新计算机** 对话框中，选择 **通过 IP 地址范围查找** 并单击 **确定**。
3. 在 **查找计算机** 对话框中，输入 **IP 地址范围起点** 和 **IP 地址范围终点**。单击 **确定**。
4. 单击 **未指派** 文件夹，可以查看已经找到的计算机。

开始管理这些计算机之前，请选择它们，并将它们拖放到组中。

从文件中导入计算机

要使 Enterprise Console 列示您的计算机，您可以从文件中导入计算机名称。

包含计算机名称的文件，必须是下列之一：

- 符合下列要求的文件

- 从 Sophos SAVAdmin 中导出的 SGR 文件

您可以按以下形式创建文件：

[组名1]
域名1| Windows2000| 计算机名1
域名1| Windows2000Server| 计算机名2


您不一定非要指定放入计算机的组。如果您输入 **[]** 作为组名，计算机会被放到“未指派”文件夹中。


有效的操作系统名称如下：Windows95，Windows98，Windows9x，WindowsMe，WindowsNT，WindowsNTServer，Windows2000，Windows2000Server，WindowsXP，Windows2003，WindowsVista，Windows Server 2008，MACOS9，MACOSX，Linux，以及 Unix。

域名和操作系统都是可选项。所以，也可能有以下形式：

[组名1]
| | 计算机名1

您可以按以下说明，导入计算机名：

1. 在 **文件** 菜单中，单击 **从文件中导入计算机**。
2. 在打开的窗口中，选择导入计算机名称的文件。
3. 单击 **未指派** 文件夹，可以查看已经找到的计算机。
4. 开始管理这些计算机之前，请选择它们，并将它们拖放到组中。

7 怎样与 Active Directory 同步化？

本节描述怎样将 Enterprise Console 组与 Active Directory 容器同步化。

- 关于 Active Directory 同步化
- 什么是同步化点？
- 什么是已同步化的组？

关于 Active Directory 同步化

Active Directory 同步化能做些什么？

通过 Active Directory 同步化，您可以将 Enterprise Console 组与 Active Directory 容器同步化。在 Active Directory 中找到的新的计算机和组，会被自动复制到 Enterprise Console 组中。您还可以选择自动保护找到的 Windows 2000 或以后的工作站。这将最大限度地缩短计算机可能感染到病毒的时间，同时减少您安排保护计算机所需要做的大量工作。

运行 Windows 95/98/Me，Windows Server，Mac，Linux，或 UNIX 等操作系统的计算机，不会自动被保护。您必须手动保护这样的计算机。

在您设置了同步化之后，您可以设置电子邮件警报，以便在今后的同步化过程中，找到新的计算机和组时，可以向您所选择的收件人寄送警报。如果您选择了自动保护已同步化的组中的计算机，那么，您还可以设置在自动保护失败时，发出警报。

Active Directory 同步化是怎样工作的？

在 Enterprise Console 中，您可以同时拥有自己管理的“普通”的，未经同步化的组，以及已经与 Active Directory 同步化了的组。

在设置同步化时，您选择或创建一个同步化点，一个将要与某个 Active Directory 容器同步化的 Enterprise Console 组。Active Directory 容器中所有子组和计算机都将被复制到 Enterprise Console 中，并被保持与 Active Directory 同步化。

要了解更多有关同步化点的信息，请参见什么是同步化点？要了解更多有关同步化的组的信息，请参见什么是已同步化的组？

在您设置了与 Active Directory 同步化之后，Enterprise Console 中的已同步化的组的结构，与其在 Active Directory 容器中与之同步化的组的结构是完全一致的。这意味着：

- 如果有新的计算机添加到 Active Directory 容器中，那么，它也出现在 Enterprise Console 中。
- 如果某计算机从 Active Directory 中删除，或者被移动到尚未同步化的组，那么，该计算机在 Enterprise Console 中会被移动到 **未指派** 文件夹中。

  当某计算机被移动到 **未指派** 文件夹之后，它将停止接收新的策略。
- 如果某计算机从一个同步化的容器中移到另一个同步化的容器中，那么，该计算机从一个 Enterprise Console 组中移到另一个 Enterprise Console 组。
- 如果某计算机在首次同步化时，已经在某个 Enterprise Console 组中，那么，它会被从该组中移动到与 Active Directory 相对应的那个 Enterprise Console 同步化的组中。
- 当计算机被移动到具有不同的策略的新组中时，新的策略将被应用到该计算机中。

依照默认值，同步化每60分钟进行一次。如果您想要，您可以更改同步化频率。

怎样运用同步化？

将哪些组与 Active Directory 同步化，以及设置多少个同步化点，是完全由您来决定的。您必须考虑，将要创建的组在同步化之后的大小，是能够易于管理的。您应该能够方便地部署软件，扫描和清除计算机。这对初始的部署尤其重要。

推荐的运用方式如下：

1. 使用 **从 Active Directory 导入**，导入组结构（没有计算

机）。要了解怎样做，请参见从 Active Directory 导入组。

2. 检查导入的组结构，并选择您的同步化点。
3. 设置组策略，并将其应用到组和子组。要了解怎样做，请参见怎样创建和使用策略？
4. 将您所选择的同步化点与 Active Directory 进行同步化，一次进行一个。要了解怎样做，请参见 与 Active Directory 同步化。

什么是同步化点？

同步化点 是某个 Enterprise Console 组，它指向 Active Directory 中的某个容器（或子树）。同步化点用于容纳从 Active Directory 中导入的同步化的组。

在 **组** 窗格板中，会出现如下的一个同步化点：

您***可以***移动，重命名，或删除同步化点。您还可以更改同步化点的策略和同步化设置，包括更改自动保护设置。

您***无法***在同步化点中创建或删除子组，或将其它的组移动到同步化点中。您无法将计算机移入或移出同步化点中。

什么是已同步化的组？

已同步化的组 是从 Active Directory 中导入的同步化点的子组。

在 **组** 窗格板中，会出现如下的一个已同步化的组：

您***可以***更改指派给已同步化的组的策略。

您***无法***更改除了组策略以外的，任何其它的已同步化的组的设置。您无法重命名，移动，或删除已同步化的组。您无法将计

算机或组移入或移出已同步化的组。您无法在已同步化的组中创建或删除子组。您无法更改已同步化的组的同步化设置。

与 Active Directory 同步化

要与 Active Directory 同步化：

1. 请选择某个组作为您将来的同步化点，右击鼠标并选择 **与 Active Directory 同步化**。**与 Active Directory 同步化向导** 会启动。
2. 在向导的 **概览** 页中，单击 **下一步**。
3. 在 **选择一个 Enterprise Console 组** 页面中，请选择或创建一个您想要用来保持与 Active Directory 进行同步化的 Enterprise Console 组（同步化点）。单击 **下一步**。
4. 在 **选择一个 Active Directory 容器** 页面中，请选择一个想要将组与之进行同步化的 Active Directory 容器。输入容器名称（如：LDAP://CN=Computers，DC=domain_name，DC=local）或单击 **浏览** 浏览找到 Active Directory 中的容器。单击 **下一步**。
5. 如果您想要自动保护 Windows 2000 或以后的工作站，请在 **自动保护计算机** 页面中，选择您想要安装的软件。如果您想自动删除其它软件商的类似软件，请保留选择 **删除第三方安全软件**。

   如果您需要删除其它软件商的更新工具，请参见删除第三方安全软件。

   
   您不能在运行服务器版的操作系统的计算机上，安装防火墙。

   
   您必须单击链接，指定 NAC 服务器的 URL 之后，才能将 Sophos NAC 安装到计算机上。

   从现在起，所有在同步化过程中找到的 Windows 2000 或以后的工作站，都将自动被保护，并遵照它们各自的组策略。

运行 Windows 95/98/Me，Windows Server，Mac OS，Linux，或 UNIX 等操作系统的计算机，不会自动被保护。您必须，按照保护要求手动安装的计算机中的说明，手动保护这样的计算机。

您可以按照查看和编辑同步化属性中的说明，在以后启用或禁用自动保护。

单击 **下一步**。

6. 如果您选择自动保护计算机，请在 **请输入 Active Directory 认证资料** 页面中，输入将要用来在计算机上安装软件的系统管理员帐户的详情。单击 **下一步**。
7. 在 **请选择同步化频率** 页面中，选择您想要 Enterprise Console 组与 Active Directory 容器同步化的频率。默认值是 60 分钟。

   您可以按照查看和编辑同步化属性中的说明，在以后更改同步化的频率。
8. 在 **确认您的选择** 页面中，检查详情，然后单击 **下一步** 继续。
9. 在向导的最后一页中，您可以查看已同步化的组，计算机的详情。

   您还可以设置电子邮件警报，以便在今后的同步化过程中，找到新的计算机和组时，可以向您所选择的收件人寄送警报。如果您选择了自动保护已同步化的组中的计算机，那么，您还可以设置在自动保护失败时，发出警报。要在您单击 **完成** 之后，打开 **配置电子邮件警报** 对话框，请勾选向导最后一页中的勾选框。要了解怎样做，请参见 设置 Active Directory 电子邮件警报。

   要关闭向导，请单击 **完成**。

自动保护计算机

在与 Active Directory 同步化的过程中找到的计算机中，只有运行 Windows 2000 或以后的计算机会获得自动保护。

运行 Windows 95/98/Me，Windows Server，Mac OS，Linux，或 UNIX 等操作系统的计算机，不会自动被保护。您必须，按照保护要求手动安装的计算机中的说明，手动保护这样的计算机。

在运行 **与 Active Directory 同步化** 向导时，或者，在 **同步化属性** 对话框中编辑同步化属性时，您可以设置自动保护已同步化的组中的计算机。

您不能在运行服务器版的操作系统的计算机上，安装防火墙。

您必须单击链接，指定 NAC 服务器的 URL 之后，才能将 Sophos NAC 安装到计算机上。

在 与 Active Directory 同步化 向导中，启用自动保护。

1. 在 **自动保护计算机** 页面中，选择您想安装的软件。如果您想自动删除其它软件商的类似软件，请保留选择 **删除第三方安全软件**。

   如果您需要删除其它软件商的更新工具，请参见删除第三方安全软件。

2. 在本向导的 **请输入 Active Directory 认证资料** 页面中，输入将要用来在计算机上安装软件的系统管理员帐户的详情。单击 **下一步** 并完成向导。

在 同步化属性 对话框中启用自动保护。

1. 在 **组** 窗格板中，选择您想要为之启用自动保护的组（同步化点）。右击该组，然后选择 **同步化属性**。
2. 在 **同步化属性** 对话框中，选择您想安装的软件。如果您想自动删除其它软件商的类似软件，请保留选择 **删除第三方安全软件**。
3. 输入将要用来在计算机上安装软件的系统管理员帐户的详情。单击 **确定**。

禁用自动保护

如果您将来想要禁用自动保护，请在 **同步化属性** 对话框中，取消勾选 **自动安装 Sophos Anti-Virus** 勾选框。

查看和编辑同步化属性

1. 在 **组** 窗格板中，选择您想要为之编辑同步化属性的组（同步化点）。右击该组，然后选择 **同步化属性**。
2. 在 **同步化属性** 对话框中，按照以下说明设置选项。

Active Directory 容器

此区域显示组与之同步的 Active Directory 容器。

此区域是无法编辑的。您无法从 **同步化属性** 对话框中，更改容器。如果想要将组与不同的 Active Directory 容器同步化，请删除同步化，然后，再次运行 **与 Active Directory 同步化 向导。**

同步化频率

依照默认值，同步化每60分钟进行一次。您可以更改同步化频率。最高的同步化频率是每5分钟一次。

自动保护

如果您想要自动保护所有找到的新的 Windows 2000 或以后的工作站，并遵照它们各自的组策略，请选择 **自动安装 Sophos Anti-Virus**。

如果您在安装防病毒软件的同时，还想安装防火墙或网络访问控制，请选择 **自动安装 Sophos Client Firewall**，或者 **自动安装 Sophos Network Access Control**。

您必须单击链接，指定 NAC 服务器的 URL 之后，才能将 Sophos NAC 安装到计算机上。

只有 Windows 2000 或以后的工作站才会获得自动保护。运行 Windows 95/98/Me，Windows Server，Mac OS，Linux，或 UNIX 等操作系统的计算机，不会自动被保护。您必须，按照保护要求手动安装的计算机中的说明，手动保护这样的计算机。

在 **用户名** 文本框中，输入将要用来在计算机上安装软件的系统管理员帐户的用户名。

在 **密码** 文本框中，输入将要用来在计算机上安装软件的系统管理员帐户的密码。

开启或关闭同步化

要开启同步化，请按照 与 Active Directory 同步化 中的说明，运行 **与 Active Directory 同步化** 向导。

要关闭同步化，请选择您不再想要其与 Active Directory 同步化的组（同步化点），右击该组，并选择 **删除同步化**。单击 **是** 确认。

8 怎样保护新加入网络中的计算机？

本节说明怎样在联网的计算机上，安装 Sophos Anti-Virus，Sophos Client Firewall，以及 Sophos Network Access Control。

- 保护新计算机
- 保护新类型的计算机
- 保护已在某个组中的计算机
- 保护需要手动安装的计算机
- 使用登录脚本保护计算机
- 使用登录脚本保护 Windows 95/98/Me 操作系统的计算机
- 在已受保护的计算机上添加防火墙

- 选择软件下载包
- 默认的更新目录
- 删除第三方安全软件

保护新计算机

新 **Windows** 计算机可以自动从控制台获得保护。

这些指导说明，假设您已经创建了组，并针对它们应用了更新策略。

自动安装不能在 Windows 95/98/Me，Mac，Linux，和 UNIX 计算机上进行。请用手动安装代替。

如果您从控制台自动保护 Windows XP 计算机，请确保 "简单文件共享 "已关闭。要了解防病毒软件和防火墙软件的安装要求的完整列表，请参见 *Sophos Endpoint Security and Control 网络安装指南*。要了解 Sophos NAC 系统要求列表，请参见 *Sophos NAC 安装指南*。

如果您选择了与 Active Directory 同步化，并自动保护计算机，那么，您**不**需要执行以下步骤。要了解详情，请参见 怎样与 Active Directory 同步化？

1. 在工具栏中，单击 **查找新计算机** 图标。在 **查找新计算机** 对话框中，选择您想怎样查找计算机。

   根据您的选择，Enterprise Console 要么会创建一个镜像 Active Directory 容器的组结构，要么会将新计算机放置到 **未指派** 文件夹中。（请参见 怎样将计算机添加到控制台中？） for details.

2. ***如果您有计算机在 未指派 文件夹中***，将计算机拖放到组上。

   如果您已从 Active Directory 导入组和计算机，请选择您想要保护的计算机，右击并选择 **保护计算机**。

   会启动 **保护计算机向导**。

3. 在向导的 **欢迎** 页面中，单击 **下一步**。

4. 在 **选择计算机安全软件** 页中，选择您想要的软件。如果您想自动删除其它软件商的类似软件，请保留选择 **删除第三方安全软件**。

   如果您需要删除其它软件商的更新工具，请参见删除第三方安全软件。

   第三方软件删除，仅卸载与您所要安装的产品的功能相同的那些产品。

   Sophos Client Firewall 和 Sophos NAC 只能用于 Windows 2000 或以后，并且需要在您的用户授权使用许可协议得到授权。

   您不能在运行服务器版的操作系统的计算机上，安装防火墙。

   您必须单击链接，指定 NAC 服务器的 URL 之后，才能将 Sophos NAC 安装到计算机上。如果安装 Sophos NAC 的是多台服务器，那么，请使用运行了应用程序本身的那台服务器的 URL，而不要使用安装了数据库的那台服务器的 URL。

   单击 **下一步**。

5. 在 **保护摘要** 页中，安装中的任何问题都会显示在 **保护问题** 栏中。请参见排疑解难部分，或者，在这些计算机上进行手动安装。单击 **下一步**。

6. 在 **认证资料** 页中，输入可以用来安装软件的帐户的详情。该帐户通常都是域系统管理员帐户。它必须：

   拥有您要保护的计算机的管理员权限

   可以登录您安装了 Management Server 的那台计算机。

   可以读取您在 **更新** 策略中，所指定的 主服务器 的路径。

   如果您使用域帐户名，您必须以 "域名\用户 "的形式输入用户名。

保护新类型的计算机

如果您添加到网络中的计算机所使用的操作系统，是以前没有保护过的，请按照以下步骤做。

Sophos 将 Windows 2000 及以后计算机视为同一类型的计算机，而将 Windows 95/98//Me 视为另一类型的计算机。如果在您的网络中已经有受到保护的 Windows 2000 计算机，然后，添加 Windows 2003 计算机，您可以使用通常的步骤保护新计算机。

1. 如果您尚未使用 EM Library 选择并下载针对新的操作系统的软件下载包。要了解怎样做，请参见 选择软件包。
2. 在 Enterprise Console 中查找网络中的新计算机，并将它们放置到 **未指派** 文件夹。
3. 右击您将要放置新的计算机的组，并选择 **查看组策略详情**。记下该组所使用的更新策略。
4. 在 **策略** 窗格板中，双击更新策略。
5. 选择新的操作系统。单击 **配置**。
6. 在 **设置更新策略** 对话框中的 **主服务器** 标签页中，输入计算机将要从中进行更新的文件夹的详情。输入用户名和密码。单击 **确定**。再次单击 **确定**。
7. 将新计算机拖放到该组中。会有向导启动，帮助您保护这些计算机。
8. 在向导的 **欢迎** 页面中，单击 **下一步**。
9. 在 **选择计算机安全软件** 页中，选择您想要的软件。如果您想自动删除其它软件商的类似软件，请保留选择 **删除第三方安全软件**。

   如果您需要删除其它软件商的更新工具，请参见删除第三方安全软件。

   Sophos Client Firewall 和 Sophos NAC 只能用于 Windows 2000 或以后，并且需要在您的用户授权使用许可协议得到授权。

您不能在运行服务器版的操作系统的计算机上，安装防火墙。

您必须单击链接，指定 NAC 服务器的 URL 之后，才能将 Sophos NAC 安装到计算机上。

单击 **下一步**。

10. 在 **保护摘要** 页中，安装中的任何问题都会显示在 **保护问题** 栏中。请参见排疑解难部分，或者在这些计算机上进行手动安装。单击 **下一步**。

11. 在 **认证资料** 页中，输入可以用来安装软件的帐户的详情。该帐户通常都是域系统管理员帐户。它必须：

    拥有您要保护的计算机的管理员权限

    可以登录您安装了 Management Server 的那台计算机。

    可以读取您在 **更新** 策略中，所指定的主服务器的路径。

    如果您使用域帐户名，您**必须**以“域名\用户”的形式输入用户名。

12. 针对您想放入新计算机的任何其它组，重复步骤 3 到步骤 11。

保护已在某个组中的计算机

如果您已经将计算机放入了一个用户定义了的组中，但尚未为它们提供保护，您可以按照以下步骤自动保护它们：

这些指导说明，假设您已经为组应用了更新策略。

自动安装不能在 Windows 95/98/Me 计算机上进行。请用手动安装代替。

1. 选择计算机。右击并选择 **保护计算机**。会启动 **保护计算机向导**。
2. 在向导的 **欢迎** 页面中，单击 **下一步**。
3. 在 **选择计算机安全软件** 页中，选择您想要的软件。如果

您想自动删除其它软件商的类似软件，请保留选择 **删除第三方安全软件**。

如果您需要删除其它软件商的更新工具，请参见删除第三方安全软件。

Sophos Client Firewall 和 Sophos NAC 只能用于 Windows 2000 或以后，并且需要在您的用户授权使用许可协议得到授权。

您不能在运行服务器版的操作系统的计算机上，安装防火墙。

您必须单击链接，指定 NAC 服务器的 URL 之后，才能将 Sophos NAC 安装到计算机上。

单击 **下一步**。

4. 在 **保护摘要** 页中，安装中的任何问题都会显示在 **保护问题** 栏中。请参见排疑解难部分，或者，在这些计算机上进行手动安装。单击 **下一步**。
5. 在 **认证资料** 页中，输入可以用来安装软件的帐户的详情。该帐户通常都是域系统管理员帐户。它必须：

   拥有您要保护的计算机的管理员权限

   可以登录您安装了 Management Server 的那台计算机。

   可以读取您在 **更新** 策略中，所指定的 主服务器 的路径。

   如果您使用域帐户名，您**必须**以 "域名\用户 "的形式输入用户名。

保护需要手动安装的计算机

如果 Enterprise Console 不能在某些计算机上自动安装防病毒，防火墙，或 NAC 软件，您可以实行手动安装。

Enterprise Console 随后会管理和更新这些手动进行的安装，只要您将这些计算机放入了组中。

另外，您也可以使用脚本，实施自动安装.请参见使用登录脚本保护计算机。

如果您在 Windows 95/98/Me 操作系统的计算机上安装了先前版本的 Sophos Anti-Virus，那么，您必须先卸载它，才能安装最新版本的 Sophos Anti-Virus .

您可以按照以下说明，进行手动安装：

1. 在 Enterprise Console 中，选择您想要手动安装的计算机。单击 **更新详情** 标签，并查看**主服务器** 栏。在该栏中会向您显示各计算机从中更新的目录。

   或者，如果您使用默认目录，请参见默认的更新目录，查看默认目录列表。

   如果您的用户授权使用许可协议中包括防火墙，您就可以将其与 NAC 和防病毒软件一道，安装到 Windows 2000 或以后的计算机上。找到针对 Sophos Endpoint Security and Control 软件包的目录。该目录名是 SAVSCFXP。

2. 在相应的计算机上，浏览找到它将从中更新的目录。

   在 **Windows** 计算机中，双击 setup.exe.

   要在 Windows 2000 或以后的计算机上，安装防火墙和防病毒软件，请打开命令行窗口，并运行带有 相应限定符的 setup.exe：
   要仅安装防病毒软件，请键入： setup.exe -sav
   要安装防病毒和防火墙软件，请键入： setup.exe -scf
   要安装防病毒，防火墙，以及 NAC（并指定 NAC 服务器的路径），请键入： setup.exe -scf -nac http://<nacserver>

   在 **Mac OS X** 计算机中，双击 Sophos Anti-Virus.mpkg。

   在 **Linux** 或 **UNIX** 计算机上，按照 *Sophos Endpoint Security and Control 网络安装指南* 中的说明，使用分发包安装 Sophos Anti-Virus。

   如果您有从控制台管理的 Linux 或 UNIX 计算机，请确保为每台计算机配置了唯一的主机名。否则，每台计算机都将以默认的名称 “localhost ”出现在控制台中。

使用登录脚本保护计算机

您可以通过运行带有脚本的安装程序，或者类似 Microsoft SMS 的程序，来提供防病毒软件（以及防火墙软件，如果您的用户授权使用许可协议中包括），保护您的计算机。

Enterprise Console 随后会管理和更新这些手动进行的安装，只要您将这些计算机放入了组中。

查找您需要的安装程序

安装程序在 EM Library 放置 Sophos 更新文件的目录中。要检查是哪一个目录，请查看计算机列表，找到您想要提供保护的计算机。单击 **更新详情** 标签，并查看**主服务器** 栏。

或者，如果您使用默认目录，请参见默认的更新目录，查看默认目录列表。

保护 Windows 95/ 98/ Me 计算机

对于 Windows 95/98/Me 计算机，使用登录脚本运行 setup.exe。要了解怎样做，请参见 使用登录脚本保护 Windows 95/98/Me 计算机。

保护 Mac OS X 计算机

对于 Mac OS X 操作系统计算机，请使用 Apple Remote Desktop。在使用 Apple Remote Desktop 之前，请从中央安装目录中将 Installer 复制到要运行 Apple Remote Desktop 的计算机上。

保护 Windows 2000 或以后的计算机

如果您要使用防火墙和/或网络访问控制，以及防病毒软件为 Windows 2000 或以后的计算机提供保护，您必须：

- 确保使用了正确的安装程序。该安装程序是 Sophos Endpoint Security 包的安装程序，它所在的目录是 SAVSCFXP。
- 请运行带有 -scf 限定符的安装程序（安装防火墙），运行

带有 -nac 限定符的安装程序（安装网络访问控制）。

使用登录脚本保护 Windows 95/ 98/ Me 操作系统的计算机

要使用登录脚本保护 Windows 95/98/Me 操作系统的计算机，请按照以下说明做：

1. 如果您还不知道安装程序所在的目录的路径，请查找它。

   要查找它，请查看计算机使用的是哪个更新策略。在 **策略** 窗格板中，双击该策略。选择 **Windows 95/ 98/ Me**，然后，单击 **配置**。然后，记录下所显示的 **地址** 路径。

2. 将以下指令行添加到登录脚本中

   [路径]\setup.exe -user [域名] -pwd [密码] -login -s

   这里的[路径]是包含安装程序的目录路径（如：\\服务器名\InterChk\ES9x），可以登录您的 Windows 95/98/Me 计算机的帐户的用户名和密码，具有读取 CID 共享文件的权限（在此例中是：\\服务器名\InterChk）。

   如果您使用任何 Windows 95 操作系统的计算机，那么，您必须在安装之前，在该计算机上运行一个小实用程序。从 Sophos Endpoint Security and Control Network Install CD 中，复制 Tools/Utils/w95ws2setup.exe 文件到您的服务器上。然后，请在登录脚本中的上述指令行之前，在添加一行运行该实用程序的指令。

   您指定的用户帐户必须

   能够登录您想要保护的计算机。

   拥有您要保护的计算机的管理员权限。

   可以读取您在 **更新** 策略中，所指定的 主服务器 的路径。

   如果您不想使用 Enterprise Console 管理计算机，您应该将添加参数 -mng no。

在下一次用户登录时，他们的计算机就会安装防病毒软件。

在已受保护的计算机上添加防火墙

如果您已经安装了 Sophos Anti-Virus 来保护您的计算机，您还可以为其安装 Sophos Client Firewall，只要您的用户授权使用许可协议中包括了防火墙软件。

防火墙只能安装在运行 Windows 2000 或以后的计算机上。

您不能在运行服务器版的操作系统的计算机上，安装防火墙。

1. 如果您尚未使用 EM Library 选择并下载，包括了防火墙软件的 Sophos Endpoint Security 下载包。要了解怎样做，请参见 选择软件包。
2. 选择您想要安装防火墙的计算机。右击并选择 **保护计算机**。会有一个向导启动。
3. 在向导的 **欢迎** 页面中，单击 **下一步**。
4. 在 **选择计算机安全软件** 页中，选择 **安装 Sophos Client Firewall**。
5. 在 **保护摘要** 页中，安装中的任何问题都会显示在 **保护问题** 栏中。请参见排疑解难部分，或者，在这些计算机上进行手动安装。单击 **下一步**。
6. 在 **认证资料** 页中，输入可以用来安装软件的帐户的详情。该帐户通常都是域系统管理员帐户。

选择软件下载包

在您将新的防病毒，防火墙，或网络访问控制软件安装到联网的计算机上之前，您必须确保选择了正确的，从 Sophos 下载的软件包。

您可以按照以下的说明做：

1. 单击工具栏中的 **Libraries** 图标。会出现 Sophos EM

Library 窗口。

2. 依照默认值，**配置** 视图会开启。单击 **Select Packages**。右击您想要的下载包。选择 **Subscribe**，然后，按照提示做。

"Sophos Endpoint Security and Control" 下载包中包含 Sophos Anti-Virus for Windows 2000/XP/2003/Vista，Sophos Client Firewall，和 Sophos NAC。

更快地获取新软件包的方法是到 **Library** 菜单中，并选择其中的 **Select Packages**。这样可以将软件包放到默认的路径中。

3. 单击 **Download Packages**。
4. 在 **EM Library** 消息框中，单击 **是**。
5. 关闭 **EM Library** 窗口，返回到 Enterprise Console。

默认的更新目录

如果您在安装 Sophos EM Library 时接受了默认设置，那么，各产品的安装和更新所使用的文件夹，应该如下：

在“Sophos Endpoint Security and Control”下载包的目录中包含着针对 Sophos Anti-Virus，Sophos Client Firewall，和 Sophos NAC 等程序的安装程序。

Sophos Endpoint Security and Control for Windows 2000/XP/2003/Vista	\\服务器名称\InterChk\SAVSCFXP
Sophos Anti-Virus for Windows 2000/XP/2003/Vista	\\服务器名称\InterChk\ESXP
Sophos Anti-Virus for Windows NT	\\服务器名称\InterChk\ESNT
Sophos Anti-Virus for Windows 95/98/Me	\\服务器名称\InterChk\ES9X
Sophos Anti-Virus for Mac OS X	\\服务器名称\InterChk\ESOSX
Sophos Anti-Virus for Linux	\\Servername\InterChk\savlinux
Sophos Anti-Virus for UNIX	\\Servername\InterChk\EESAVUNIX

删除第三方安全软件

如果您想要删除任何先前安装的安全软件，您应该在运行 **保护计算机向导** 的中的 **删除第三方安全软件** 选项**之前**，按照以下说明做：

- 如果计算机上运行的是其它软件商的防病毒软件，请确保该软件的用户界面已关闭。
- 如果计算机上运行的是其它软件商的防火墙软件或 HIPS 软件，请确保该软件已关闭，或已配置为允许运行 Sophos 安装程序。
- 如果您想删除的不仅是其它软件商的软件，而且还包括它的更新工具（以避免它重新自动安装该软件），请按照以下步骤做：如果计算机没有安装更新工具，您可以忽略以下步骤。


您必须重新启动您从中删除了第三方防病毒软件的所有计算机。

如果计算机上安装了其它软件商的更新工具，并且您希望删除该更新工具，那么，在运行 **保护计算机** 向导中的 **删除第三方安全软件** 选项之前，您需要修改配置文件：

1. 在中央安装目录中，找到 data.zip 文件。
2. 从 data.zip 文件中提取 crt.cfg 配置文件。
3. 编辑该 crt.cfg 文件，更改行 "RemoveUpdateTools=0" 为 "RemoveUpdateTools=1"。
4. 保存您的更改，并保存 crt.cfg 到 data.zip 文件所在的同一个目录中。不要将 crt.cfg 文件放回 data.zip 中，否则，在下一次更新 data.zip 文件时，它会被覆盖。

当您运行 **保护计算机** 向导，并选择 **删除第三方安全软件**，修改了的配置文件会删除任何第三方安全软件的更新工具，以及第三方安全软件。

如果计算机运行了其它软件商的防火墙或 HIPS 产品，那么，您可能需要保留该软件商的更新工具。请参见该软件商的技术文档，了解详情。

9 怎样检查网络是否受保护？

本节将说明怎样使用和配置指标面板，以及怎样确保计算机已被妥善保护。本节还将告诉您怎样使用计算机列表过滤，确定有问题的计算机，以及采取措施解决问题。

- 指标面板概述
- 配置指标面板
- 哪些计算机受到了保护？
- 哪些计算机已及时更新？
- 查找未受保护的计算机
- 查找没有安装防火墙的计算机
- 查找出现病毒警报需要关注的计算机
- 查找未及时更新的计算机
- 查找未受控制台管理的计算机
- 查找与网络断开了连接的计算机

您还可以按照检查计算机是否使用了组策略中的说明，检查组中的所有计算机是否遵照了该组的策略。

指标面板概述

使用指标面板检查您的网络安全状况。要显示或隐藏指标面板，单击工具栏中的 **指标面板** 按钮。

指标面板界面

指标面板由以下六个部分组成：

计算机

此部分显示网络中的计算机的总数，以及联网的，已管理的，未管理的计算机的数量。

要查看已管理的，未管理的，联网的，或所有计算机的列表，请单击 **计算机** 栏中的链接之一。

更新文件

本节显示上次从 Sophos 更新的日期和时间。

要打开 EM Library 控制台，单击栏目标题：**更新**。

发出警报的计算机

此部分显示具有下列类型的警报的，已管理的计算机的数量和百分比：

- 已知的和未知的病毒和间谍软件
- 可疑行为和文件
- 被防火墙阻断的应用程序
- 广告软件和其它可能不想安装的应用程序
- 受控程序

要查看具有未处理的警报的已管理的计算机的列表，请单击栏

目标题：**具有警报的计算机**。

策略

此部分显示具有组策略不一致，或者策略比较出错的，已管理的计算机的数量和百分比。它还包括控制台已向其发出已更改的策略，但尚未回应的计算机。

要查看具有不一致策略的已管理的计算机的列表，请单击栏目标题：**策略**。

保护

此部分显示 Sophos Anti-Virus 未及时更新，或者使用未知的检测数据的，已管理的联网计算机的数量和百分比。

要查看未及时更新的已管理的联网计算机的列表，请单击栏目标题：**保护**。

错误

此部分显示具有未处置的 Sophos Anti-Virus 错误，更新错误，或 Sophos Client Firewall 错误的，已管理的计算机的数量和百分比。

要查看具有未处理的 Sophos 产品错误的已管理的计算机的列表，请单击栏目标题：**错误**。

指标面板安全状态指示器

指标面板可以显示三种安全状态指示器。

标志	释意
	绿色的指示器，表示“普通”状态。受影响的计算机的数量低于警告级指标。
	黄色的指示器，表示“警告”状态。已达到警告级指标。
	红色的指示器，表示“紧要”状态。已达到紧要级指标。

指示器出现在各个部分，以及出现在整个指标面板中。

指标面板部分的健康指示器 是出现在指标面板部分右上角的栏目标题旁的图标，它显示所在的部分所表示的特定领域的安全状态。

指标面板部分的健康指示器，显示某个部分的最高程度的安全状态，它们是：

- 只要有一个指示器的指标达到了警告级，指标面板部分的健康指示器就会从“普通”变为“警告”。
- 只要有一个指示器的指标达到了紧要级，指标面板部分的健康指示器就会从“警告”变为“紧要”。

网络综合健康指标 是出现在 Enterprise Console 窗口的右下角状态栏中的一个图标，它显示整个网络的综合安全状态。

网络综合健康指示器，显示指标面板部分的最高程度的安全状态，它们是：

- 只要有一个指标面板指示器的指标达到了警告级，网络综合健康指示器就会从“普通”变为“警告”。
- 只要有一个指标面板指示器的指标达到了紧要级，网络综合健康指示器就会从“警告”变为“紧要”。

当您首次安装或更新 Enterprise Console 时，指标面板会使用默认中警告和紧要级设置。您可以在 **配置指标面板** 对话框中，配置自己的警告和紧要级设置。要了解怎样做，请参见 配置指标面板。

您还可以设置电子邮件警报，当指标面板中的某部分达到了“警告级”或“紧要级”时，可以向您所选择的收件人寄送警报。要了解怎样做，请参见 设置网络状态电子邮件警报。

配置指标面板

指标面板显示警告，或者，紧要状态指标。这些指标基于具有未处理的警报或错误的已管理的计算机的百分比；或者，基于最近一次从 Sophos 更新的时间。

您可以设置您想要使用的“警告级”和“紧要级”设置。

1. 在 **工具** 菜单中，选择 **配置**，然后单击 **指标面板**。会出现 **配置指标面板** 对话框。

   要了解有关默认的指标面板配置设置的信息，请参见 什么是默认的指标面板配置设置？

2. 更改 **警告级** 和 **紧要级** 文本框中的值为适当的值。

   如果您设置级别的值为零，那么，只要出现第一个警报，警告就会被触发。

   在 **具有未处理的警报的计算机具有 Sophos 产品错误的计算机**，以及 **策略和保护** 下，输入受到特定的问题影响的已管理的计算机的百分比，该值会触发相应的指示器从“警告”转为“紧要”。

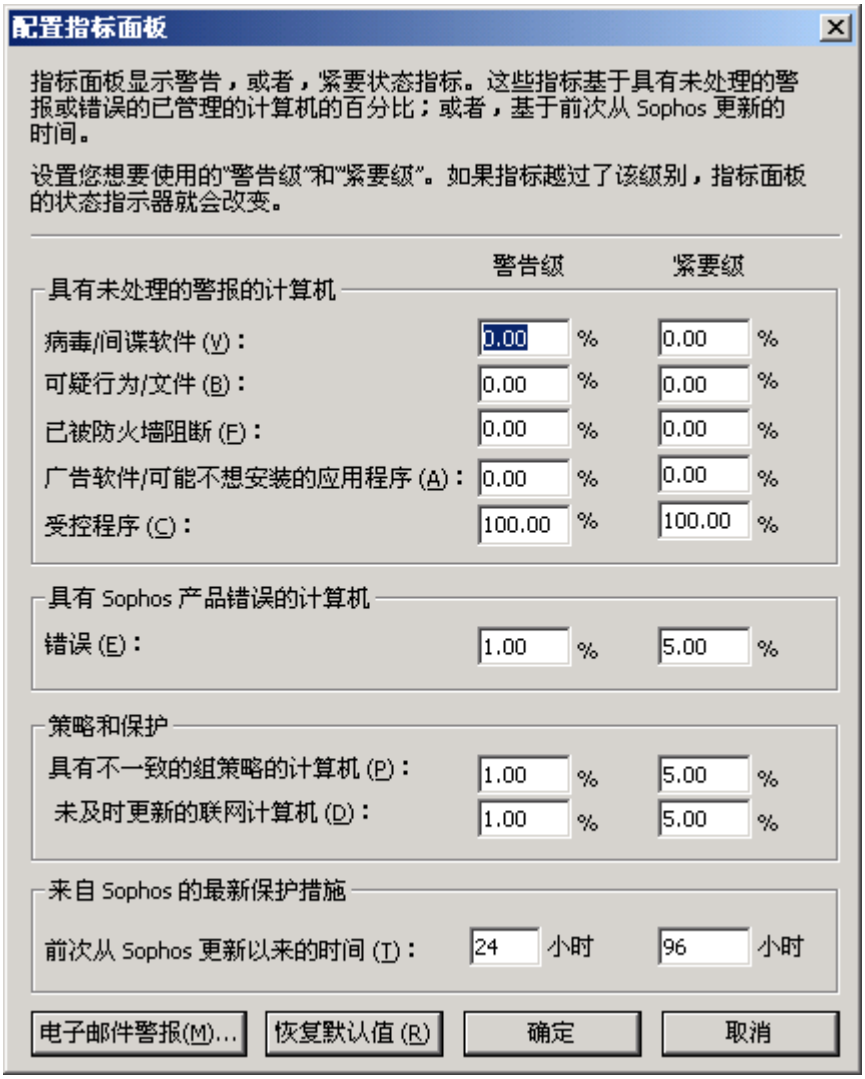
   在 **来自 Sophos 的最新保护措施** 下，输入以小时计的，从上一次自 Sophos 成功完成更新的时间间隔，该值会触发“更新”指示器从“警告”转为“紧要”。

   单击 **确定**。

您还可以设置电子邮件警报，当达到了“警告级”或“紧要级”时，可以向您所选择的收件人寄送警报。要了解怎样做，请参见 设置网络状态电子邮件警报。

什么是默认的指标面板配置设置？

默认的指标面板配置设置显示在如下的图示中。



哪些计算机受到了保护？

如果计算机中运行了读写扫描和开启了防火墙（如果安装了），计算机就受到了保护。要获得完全的保护，软件还必须及时更新。

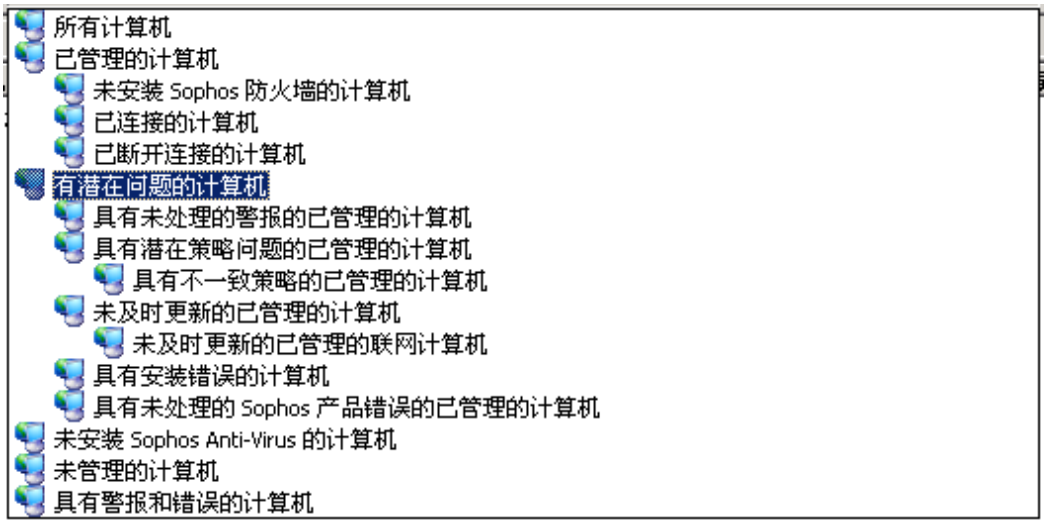
您也许选择了，在某种特定的计算机上，比如：文件服务器，不使用读写扫描。在这种情况下，请确保这些计算机使用了计划扫描，并且使用的是最新的防病毒软件版本。

要检查计算机是否受到保护：

1. 选择您要检查的计算机所在的组。

2. 如果您要检查在该组中的子组里的计算机，请在顶部的下拉列表中选择 **在这一级，及以下级**。
3. 在计算机的列表中，查看 **读写扫描** 栏。如果看到“活动”字样，则该计算机上正在运行读写扫描。如果看到的是灰色的盾牌，则该计算机上没有运行读写扫描。
4. 如果您安装了防火墙，请查看 **防火墙已启用** 栏。如果您看到“是”字样，说明计算机已经受到保护。
5. 接下来，查看 **更新情况** 栏。如果看到“是”字样，则该计算机使用的是最新的防病毒软件版本。如果看到一个钟的图标及日期，则该计算机使用的不是最新的防病毒软件版本。

您可以显示没有妥善保护的，或者，存在其它保护方面的问题的计算机的列表。转到 **视图** 的下拉列表中，选择 **有潜在问题的计算机**。您还可以选择此项下的子项，以显示被特定的问题影响的计算机（如：与组策略不一致的计算机，或出现 Sophos 产品错误的计算机）。



哪些计算机已及时更新？

如果您是依照建议设置的 Enterprise Console，计算机应该自动收到更新文件。

1. 选择您要检查的计算机所在的组。

2. 如果您要检查在任何子组里的计算机，请在顶部的下拉列表中选择 **在这一级，及以下级**。
3. 查看 **更新情况** 栏。

   如果看到“是”字样，则该计算机使用的是最新的防病毒软件版本。

   如果看到一个钟的图标，则该计算机使用的是未及时更新的防病毒软件版本。旁边的文字，说明是该计算机已有多长时间没有及时更新了。


要立即更新该计算机，请选择该计算机。右击并选择 **现在更新计算机**。

查找未受保护的计算机

如果某台计算机上没有运行读写扫描，或者，禁用了防火墙（安装了的话），那么，该计算机就没有被妥善保护。


您也许选择了，在某种特定的计算机上，比如：文件服务器，不使用读写扫描。在这种情况下，请确保这些计算机使用了计划扫描，并且使用的是最新的防病毒软件版本。

如果某计算机上没有运行读写扫描，一个灰色的盾牌和“未活动”字样会显示在 **状态页** 中的 **读写扫描** 栏中。

如果防火墙是禁用的，一个灰色的防火墙图标（一堵砖墙）会出现在 **防火墙已启用** 栏中。

要显示所有没有被妥善保护的计算机，以及处理该问题，请按照以下说明做：

1. 选择您要在其中查找这类计算机的组。
2. 在工具栏的 **视图** 下拉列表中，选择 **有潜在问题的计算机**。您还可以选择此项下的子项，以显示被特定的问题影响的计算机（如：与组策略不一致的计算机，或出现 Sophos 产品错误的计算机）。
3. 如果该组含有子组，请选择您是**仅在这一级** 或在 **在这一级，及以下级**。

4. 任何保护有问题的计算机，都将被列示出来。

   如果存在没有运行读写扫描的计算机，请检查哪个防病毒策略被这些计算机采用了。确保在那个策略中启用读写扫描。

   如果存在禁用了防火墙的计算机，请检查哪个防火墙策略被这些计算机采用了。确保在那个策略中启用防火墙。

5. 确保这些计算机遵照组策略。

查找没有安装防火墙的计算机

如果某计算机没有安装防火墙，一个灰色的防火墙图标（一堵砖墙）会显示在 **状态页** 中的 **防火墙已启用** 栏中。

要显示所有这样的计算机，并解决问题，请按照以下说明做：

1. 选择您要在其中查找出现警报计算机的组。
2. 在工具栏的 **视图** 下拉列表中，选择 **没有安装 Sophos 防火墙的计算机**。
3. 如果该组含有子组，请选择您是**仅在这一级** 或在 **在这一级，及以下级**。
4. 如果有您想在其中安装防火墙的计算机，选择这些计算机，右击并选择 **保护计算机**。当提示选择软件时，选择 **安装 Sophos Client Firewall**。

查找出现病毒警报需要关注的计算机

如果某计算机出现需要关注的安全隐患警报，在 **状态** 页中的 **警报和错误** 栏中会出现一个警报图标。

红色警告标志表明发现了病毒或间谍软件。黄色标志表明发现了可疑行为或文件，广告软件或其它可能不想安装的应用程序，被防火墙阻断的应用程序，受控程序，或错误等。

要显示仍然需要关注的带有警报的计算机，请按以下说明做：

1. 选择您要在其中查找出现警报计算机的组。
2. 在工具栏的 **视图** 下拉列表中，选择 **具有未处理的警报的**

已管理的计算机。

3. 如果该组含有子组，请选择您是**仅在这一级** 或在 **在这一级，及以下级**。
4. 如果有计算机感染了安全隐患，或者安装了您不想安装的应用程序，请参见立即清除计算机。

   如果在计算机上检测到了您**想要**的广告软件或其它可能不想安装的应用程序，请参见批准广告软件／可能不想安装的应用程序。

   如果计算机上的防火墙阻断了您**想要**运行的应用程序，请参见允许使用被阻断的应用程序。

   如果有未及时更新的计算机，请参见查找未及时更新的计算机以帮助诊断和解决问题。

如果您不在需要显示警报，您可以清除它。选择出现警报的计算机，右击并选择 **确认已知警报和错误**。

查找未及时更新的计算机

如果计算机中有未及时更新的防病毒软件，会有一个时钟图标出现在**状态**页中的 **更新情况** 栏中。旁边的文字，说明是该计算机已有多长时间没有及时更新了。

计算机可能由于以下两个原因之一，而未及时更新：

- 该计算机从服务器获取更新文件失败。
- 供更新所用的服务器中不是最新的 Sophos 软件。

本节将告诉您诊断问题和及时更新计算机。

1. 选择您要在其中查找未及时更新的计算机的组。
2. 在 **状态** 页中，单击 **更新情况** 栏将计算机按照更新情况排序。
3. 单击 **更新详情** 标签，并查看**主服务器** 栏。在该栏中会向您显示各计算机从中更新的目录。

4. 现在，查看从某一特定目录中更新的所有计算机。

   如果其中有一些计算机已及时更新，而另外一些却没有，那么，是个别的计算机有问题。选择它们，右击并选择 **现在更新计算机**。

   如果所有的计算机都未及时更新，那么，可能是供更新的目录有问题。单击工具栏中的 **Libraries** 图标。在 EM Library 控制台中，单击库的名称（在左手边的窗格板中），然后，单击 **Central Installations**。选择您认为可能未及时更新的目录，右击并选择 **Update CID**。然后，回到 Enterprise Console 中，选择未及时更新的计算机，右击并选择 **现在更新计算机**。

查找未受控制台管理的计算机

Windows，Mac，Linux，和 UNIX 计算机都应该被 Enterprise Console 管理，这样它们都可以被及时更新和监控。

如果某计算机没有被管理，有关它的详情，在 **状态** 页中会被灰白显示。

您可以按照以下说明查找和修复未被管理的计算机：

1. 在工具栏的 **视图** 下拉列表中，选择 **未被管理的计算机**。
2. 选择列示出的任何计算机。右击并选择 **保护计算机**，安装被管理的 Sophos Anti-Virus 版本。
3. 如果有任何计算机，Enterprise Console 无法为其自动安装 Sophos Anti-Virus，请进行 手动安装。

Enterprise Console 不会自动显示和管理新加入到网络中的计算机，除非您使用了 Active Directory 同步化。单击工具栏中的 **查找新计算机** 图标，可以搜索新加入到网络中的计算机，并可以将它们放置到 **未指派** 文件夹。

查找与网络断开了连接的计算机

如果某计算机与网络断开了连接，在 **状态** 页中，它的名称旁的

图标的一侧，会出现一个红色的叉。

要显示与网络断开连接的计算机列表，请按以下说明做：

1. 选择您要在其中查找与网络断开连接的计算机的组。
2. 在工具栏的 **视图** 下拉列表中，选择 **断开连接的计算机**。
3. 如果该组含有子组，请选择您是**仅在这一级** 或在 **在这一级，及以下级**。

这里“与网络断开了连接的计算机”是指那些通常由 Enterprise Console 管理的计算机，但是目前与网络断开了连接。没有被管理的与网络断开了连接的计算机，不会被显示。

10 怎样更新计算机？

本节将说明怎样设置和配置自动更新各个组中的计算机，以及怎样随时更新计算机。

- 设置自动更新
- 选择更新源
- 选择备用更新源
- 计划更新
- 现在更新计算机
- 使计算机在拨号连接时更新
- 指定用于更新的代理服务器
- 限制带宽使用量
- 选择不同的初始安装源
- 日志记录更新活动

设置自动更新

您可以按照以下说明，设置自动更新：

您必须针对将要应用该更新策略的组中的各个类型的计算机（如：Windows 2000 及以后），按照以下步骤做。

1. *要创建新的更新策略*，在 **策略** 窗格板中，右击 **更新**，然后选择 **创建策略**。输入策略名称，然后按 **输入** 按钮保存该名称。双击新策略，可以编辑它。

   要编辑默认策略，双击 **更新**，然后，双击 **默认值**。

   *要编辑早先创建的策略*检查哪个更新策略被您想要配置的计算机组所使用。在 **策略** 窗格板中，双击 **更新**。然后，双击您想要更改的那个策略。

2. 在 **更新策略** 对话框中，选择一个操作系统。单击 **配置**。
3. 在 **设置更新策略** 对话框，单击 **主服务器** 标签，并设置以下说明的选项。

   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）。

   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**。该帐户应该拥有读取您在上面的地址栏中输入的路径的权限。

   
   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。

   高级和代理详情

   如果您想限制带宽使用量，或者设置计算机在需要更新时，自动进行拨号连接，请单击 **高级。**

   如果您是通过代理服务器接入因特网的，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。**

4. 单击 **计划** 标签，然后按照以下说明输入详情。

启用网络中的计算机自动使用 Sophos 更新文件

如果您想要计算机定期更新，请选择此项。然后，输入更新频率（以分钟为单位），计算机将按照此频率检查更新文件。默认值是5分钟。

如果计算机是直接从 Sophos 下载更新文件，则该频率设置不会被应用。运行 Sophos PureMessage 的计算机会每隔15分钟检查一次更新文件。没有运行 Sophos PureMessage 的计算机将每隔60分钟更新一次。

在拨号连接时作更新检查

如果计算机是通过拨号连接到因特网进行更新工作的，请选择该项。每当您连接到因特网时，计算机就会尝试进行更新。

5. 在 **策略** 窗格板中，单击新的策略，并将其拖放到您想要配置的计算机组中。

如果您只不过是编辑某个已经应用到组中的策略，如：默认的策略，那么，您不必进行步骤5。

选择更新源

如果您想要计算机能够自动更新，您必须为它们指定取得更新文件的地方。

您必须指定，各个类型的计算机（如：Windows 2000 及以后）取得更新文件的地方。

1. 检查哪个更新策略被您想要配置的计算机组所采用了。
2. 在 **策略** 窗格板中，双击 **更新**。然后，双击您想要更改的那个策略。
3. 在 **更新策略** 对话框中，选择一个操作系统。单击 **配置**。
4. 在 **设置更新策略** 对话框，单击 **主服务器** 标签。请按以下说明设置选项。

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）。

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**。该帐户应该拥有读取您在上面的地址栏中输入的路径的权限。


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。

高级和代理详情

如果您想限制带宽使用量，或者设置计算机在需要更新时，自动进行拨号连接，请单击 **高级。**

如果您是通过代理服务器接入因特网的，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。**

选择备用更新源

您可以设置一个备用更新源。如果计算机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。

如果您使用并不总是连接到网络中的计算机，例如：笔记型电脑，Sophos 建议您为更新文件设置备用更新源。


您必须指定，各个类型的计算机（如：Windows 2000 及以后）取得更新文件的地方。

1. 检查哪个更新策略被您想要配置的计算机组所采用了。
2. 在 **策略** 窗格板中，双击 **更新**。然后，双击您想要更改的那个策略。
3. 在 **更新策略** 对话框中，选择一个操作系统。单击 **配置**。
4. 在 **设置更新策略** 对话框，单击 **副服务器** 标签。选择 **指定副服务器详情**。然后，按照以下说明输入所需的详情。

地址

输入如果计算机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。

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**。该帐户应该拥有读取您在上面的地址栏中输入的路径的权限。

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。

高级和代理详情

如果您想限制带宽使用量，或者设置计算机在需要更新时，自动进行拨号连接，请单击 **高级。**

如果您是通过代理服务器接入该地址的，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

您可以指定计算机的更新时机和频率。

您要针对各个类型的计算机（如：Windows 2000 及以后），分别输入这些设置。

1. 检查哪个更新策略被您想要配置的计算机组所采用了。
2. 在 **策略** 窗格板中，双击 **更新**。然后，双击您想要更改的那个策略。
3. 在 **更新策略** 对话框中，选择一个操作系统。单击 **配置**。
4. 在 **设置更新策略** 对话框，单击 **计划** 标签。按照以下说明输入所需的详情。

启用网络中的计算机自动使用 Sophos 更新文件

如果您想要计算机定期更新，请选择此项。然后，输入更新频率（以分钟为单位），计算机将按照此频率检查更新文件。默认值是5分钟。

如果计算机是直接从 Sophos 下载更新文件，则该频率设置不会被应用。运行 Sophos PureMessage 的计算机会每隔15分钟检查一次更新文件。没有运行 Sophos PureMessage 的计算机将每隔60分钟更新一次。

在拨号连接时作更新检查

如果计算机是通过拨号连接到因特网进行更新工作的，请选择该项。每当您连接到因特网时，计算机就会尝试进行更新。

现在更新计算机

您可以立即更新一个或数个计算机，无需等到下一次自动更新。

选择您要更新的计算机。右击并选择 **现在更新计算机**。

使计算机在拨号连接时更新

如果您想要计算机，只要一拨号连接，就进行更新，请按以下说明做：

您要针对各个类型的计算机（如：Windows 2000 及以后），分别输入这些设置。

1. 检查哪个更新策略被您想要配置的计算机组所采用了。
2. 在 **策略** 窗格板中，双击 **更新**。然后，双击您想要更改的那个策略。
3. 在 **更新策略** 对话框中，选择一个操作系统。单击 **配置**。

4. 在 **设置更新策略** 对话框，单击 **计划** 标签。选择 **在拨号连接时作更新检查**。

指定用于更新的代理服务器

如果计算机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。


您要针对各个类型的计算机（如：Windows 2000 及以后），分别输入这些设置。

1. 如果您尚未这样做，请检查哪个更新策略被您想要配置的计算机组所使用。在 **策略** 窗格板中，双击 **更新**。然后，双击您想要更改的那个策略。在 **更新策略** 对话框中，选择一个操作系统。单击 **配置**。
2. 在 **设置更新策略** 对话框，单击 **主服务器** 标签或者，如果需要，单击 **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 **代理详情**。
3. 在 **代理详情** 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。这将避免在计算机需要一些带宽以作它用时（如：下载电子邮件），更新工作占用了所有的带宽。


您要针对各个类型的计算机（如：Windows 2000 及以后），分别输入这一设置。

1. 如果您尚未怎样做，请 检查哪个更新策略 被您想要配置的计算机组所使用。在 **策略** 窗格板中，双击 **更新**。然后，双击您想要更改的那个策略。在 **更新策略** 对话框中，选择一个操作系统。单击 **配置**。
2. 在 **设置更新策略** 对话框，单击 **主服务器** 标签或者，如果

需要，单击 **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 **高级**。

3. 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，更新工作将使用计算机能提供的所有带宽。

选择不同的初始安装源

依照默认值，防病毒软件安装和不断更新的来源（“主服务器”），是您第一次设置计算机组时所指定的。如果您想从不同的来源进行初始安装，您可以按照以下说明做：

这一设置仅仅应用于 Windows 2000 及以后的计算机上。

如果您的主服务器使用的是 HTTP 地址，而您想从控制台实施安装程序，那么，您必须在此指定初始安装源。

1. 检查哪个更新策略被您想要配置的计算机组所采用了。
2. 在 **策略** 窗格板中，双击 **更新**。然后，双击您想要更改的那个策略。
3. 在 **设置更新策略** 对话框中，选择一个操作系统，如：Windows 2000 及以后。单击 **配置**。
4. 在 **设置更新策略** 对话框中，单击 **初始安装源** 标签。不勾选 **使用主服务器地址**。然后，输入您想使用的安装源的地址。

日志记录更新活动

您可以配置计算机，对其更新活动进行日志记录。

您要针对各个类型的计算机（如：Windows 2000 及以后），分别输入这些设置。

1. 检查哪个更新策略被您想要配置的计算机组所采用了。
2. 在 **策略** 窗格板中，双击 **更新**。然后，双击您想要更改的

那个策略。

3. 在 **更新策略** 对话框中，选择一个操作系统。单击 **配置**。
4. 在 **设置更新策略** 对话框，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。

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。

11 怎样更改防病毒和 HIPS 设置？

本节说明怎样更改用于检测和清除病毒，特洛伊木马，蠕虫，间谍软件，以及广告软件和其它可能不想安装的应用程序的各种设置。本节还说明怎样扫描您的计算机。您可以对每一组计算机，使用不同的设置。

- 什么是 HIPS?
- 扫描病毒、特洛伊木马、蠕虫、和间谍软件
- 检测可疑行为
- 扫描可疑文件
- 批准可疑项目
- 扫描广告软件／可能不想安装的应用程序
- 批准广告软件／可能不想安装的应用程序
- 更改要扫描的文件类型
- 从读写扫描中排除项目

- 扫描打包文件内部
- 扫描 Macintosh 文件
- 开启或关闭读写扫描
- 更改实行读写扫描的时机
- 在设定的时间扫描计算机
- 更改计划扫描设置
- 从计划扫描中排除项目
- 可以从扫描中排除的项目

您还可以在一旦发现病毒或其它安全隐患时，就立即自动清除计算机中。要这样做，您可以按照自动清除计算机中的说明更改读写扫描的设置。

什么是 HIPS?

主机入侵防范系统(HIPS) 是保护计算机免遭可疑文件，未知病毒，以及可疑行为侵害的一种安全技术。

HIPS 选项只应用于 Windows 2000 及以后的计算机上的 Sophos Anti-Virus 7 及以后。

有以下几种 HIPS 方法：

- **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。

  要了解更多信息，请参见 分析运行时行为。

- **可疑文件检测**

  Sophos Anti-Virus 7 或以后，能够扫描可疑文件。它们具有某些恶意软件共有的特征，但是又不足以确定为新出现的恶意软件。

要了解更多信息，请参见扫描可疑文件。

扫描病毒、特洛伊木马、蠕虫、和间谍软件

依照默认值，Sophos Anti-Virus 会在用户读写文件时，自动对文件中的已知和未知的病毒，特洛伊木马，蠕虫，以及间谍软件进行检测。Windows 2000 及以后的计算机上的 Sophos Anti-Virus 7 及以后，还可以分析在系统中运行的程序的行为。

您还可以配置 Sophos Anti-Virus：

- 扫描可疑文件
- 扫描广告软件／可能不想安装的应用程序
- 在设定的时间扫描计算机

检测可疑行为

依照默认值，Sophos Anti-Virus 会检测病毒，特洛伊木马，蠕虫，以及间谍软件。Windows 2000 及以后的计算机上的 Sophos Anti-Virus 7 及以后，还可以分析在系统中运行的程序的行为。

运行时行为分析包括：

- **可疑行为检测**

  “可疑行为检测”可以动态地分析运行在系统中的所有程序的行为，以便检测和阻断看似恶意的活动。可疑行为，包括更改注册表，使得在计算机启动时，病毒会自动运行。

- **缓冲区溢出检测**

  “缓冲区溢出检测”可以动态地分析运行在系统中的所有程序的行为，以便检测缓冲区溢出攻击。

“缓冲区溢出检测”功能，不能用于 Windows Vista，以及64位版的 Windows 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。

要查看或更改运行时行为分析的设置：

1. 检查哪个防病毒和 HIPS 策略被您想要配置的计算机组所采用了。
2. 在 **策略** 窗格板中，双击 **防病毒和 HIPS**。然后，双击您想要更改的那个策略。
3. 在 **防病毒和 HIPS 策略** 对话框中，单击 **HIPS 运行时行为** 按钮。
4. 会出现 **HIPS 运行时行为分析设置** 对话框。有两个选项：

   检测可疑行为

   检测缓冲区溢出

   依照默认值，这些选项都是启用的。Sophos Anti-Virus 会检测到这样的行为，并向 Enterprise Console 发送警报。但是，它不阻断任何检测到程序。

   Sophos 建议您在“仅限警报”模式下，运行一次 Sophos Anti-Virus，并批准您需要的程序之后，再启用自动阻断可疑行为。

5. 保留这些选项的启用状态，或者，如果您想要，更改这些设置，然后单击 **确定**。

   当检测到可疑行为或缓冲区溢出时，您可以删除或批准可疑项目。

6. 当您已准备好启用阻断可疑行为时，请取消勾选 **仅限警报** 勾选框。

扫描可疑文件

依照默认值，Sophos Anti-Virus 会检测已知和未知的病毒，特洛伊木马，蠕虫，以及间谍软件。您还可以配置它检测可疑文

件。

可疑文件 是指具有某些恶意软件共有的特征，但是又不足以确定为新出现恶意软件的文件（例如：含有恶意软件通常会使用的动态解压缩代码的文件）。

这些设置只应用于 Windows 2000 及以后的计算机上的 Sophos Anti-Virus 7 及以后。

1. 检查哪个防病毒和 HIPS 策略被您想要配置的计算机组所采用了。
2. 在 **策略** 窗格板中，双击 **防病毒和 HIPS**。然后，双击您想要更改的那个策略。
3. 在 **防病毒和 HIPS 策略** 对话框中，按照以下说明设置选项：

   读写扫描

   要配置读写扫描，在 **配置 Sophos Anti-Virus 和 HIPS** 面板中，确保勾选了 **启用读写扫描** 勾选框。单击 **读写扫描** 按钮。

   在 **扫描** 标签页的 **扫描选项** 面板中，勾选 **扫描可疑文件 (HIPS)** 勾选框。单击 **确定**。

   计划扫描

   要配置计划扫描，在 **计划扫描** 面板中，单击 **添加** （或者，选择某个现有的扫描，单击 **编辑**）。

   在 **计划扫描设置** 对话框中，输入您的设置，然后，单击 **配置**。

   在 **扫描和清除设置** 对话框中的 **扫描** 标签页中，在 **扫描选项** 面板中，勾选 **扫描可疑文件 (HIPS)** 勾选框。单击 **确定**。

当检测到可疑文件时，您可以删除 或 批准 该文件。

批准可疑项目

如果您启用了一个或多个 HIPS 选项（如：可疑行为检测，缓冲区溢出检测，或可疑文件检测），但是，您想使用某些检测到的项目，您可以按照以下说明批准它们：

1. 检查哪个防病毒和 HIPS 策略被您想要配置的计算机组所采用了。
2. 在 **策略** 窗格板中，双击 **防病毒和 HIPS**。然后，双击您想要更改的那个策略。
3. 在 **防病毒和 HIPS 策略** 对话框中，单击 **批准** 按钮。
4. 在 **批准管理器** 对话框中，单击已检测到的行为的类型的标签页，如：缓冲区溢出。找到已检测到的程序，将它从 **已知的** 列表移到 **已批准** 列表中。

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. 浏览到该项目，选择并将它添加到 **已批准** 列表中。

如果您想从该列表中删除某个项目，请选择该项目，并单击 **删除项目**。如果您已经批准了该项目，从该列表中删除该项目，将再次阻断该项目；所以，请只有在确信不再需要批准该项目的情况下，才使用这一选项。选择此选项不会从磁盘中删除项目。

扫描广告软件／可能不想安装的应用程序

依照默认值，Sophos Anti-Virus 会检测病毒，特洛伊木马，蠕虫，以及间谍软件。您还可以配置 Sophos Anti-Virus 检测广告软件和其它的可能不想安装的应用程序 (PUA)。

⚠ 这些设置只应用于 Windows 2000 及以后的计算机上的 Sophos Anti-Virus 6 及以后。

Sophos 建议您在开始时，使用计划扫描检测可能不想安装的应

用程序。这使您可以安全地处理**已经**运行在您的网络中的可能不想安装的应用程序。此后，您可以再启用读写扫描来检测和保护您的计算机。

1. 检查哪个防病毒和 HIPS 策略被您想要配置的计算机组所采用了。
2. 在 **策略** 窗格板中，双击 **防病毒和 HIPS**。然后，双击您想要更改的那个策略。会出现 **防病毒和 HIPS 策略** 对话框。
3. 在 **计划扫描** 面板中，单击 **添加** 以创建一个新扫描，或者，双击列表中的某个扫描以编辑它。
4. 在 **计划扫描设置** 对话框中，单击 **配置** （在页面的底部）。
5. 在 **扫描和清除设置** 对话框中的 **扫描** 标签里，在 **扫描选项** 选项下，选择 **扫描广告软件／可能不想安装的应用程序**。单击 **确定**。
6. 在执行该扫描时，Sophos Anti-Virus 可能会报告发现一些“广告软件和其它可能不想安装的应用程序”。

   如果您想允许在您的计算机上运行这些应用程序，您必须批准安装使用它们。否则，请删除它们。
7. 如果您想要启用读写扫描，请再次打开 **防病毒和 HIPS 策略** 对话框。在 **配置 Sophos Anti-Virus 和 HIPS** 面板中，确保勾选了 **启用读写扫描** 勾选框。单击 **读写扫描** 按钮。在 **读写扫描设置** 对话框中，选择 **扫描广告软件/可能不想安装的应用程序**。

有一些“监控”文件的应用程序，会试图频繁地访问文件。如果您启用了读写扫描，则读写扫描会检测到每一次读写，并发出多重警报。请参见 频繁发出有关可能不想安装的应用程序的警报。

批准广告软件／可能不想安装的应用程序

如果您已启用了 Sophos Anti-Virus 检测广告软件／可能不想安

装的应用程序(PUA)，它可能阻止您使用您想要使用的应用程序。

您可以按照如下说明批准这样的应用程序。

1. 检查哪个防病毒和 HIPS 策略被您想要配置的计算机组所采用了。
2. 在 **策略** 窗格板中，双击 **防病毒和 HIPS**。然后，双击您想要更改的那个策略。
3. 在 **防病毒和 HIPS 策略** 对话框中，单击 **批准** 按钮。
4. 在 **批准管理器** 对话框中的 **广告软件／可能不想安装的应用程序** 标签里，在 **已知的广告软件／可能不想安装的应用程序** 列表，选择您想要的应用程序。单击 **添加** 将其添加到 **已批准的广告软件/可能不想安装的应用程序** 列表中。

如果您无法看见您想要批准的应用程序，请按照以下说明做：

1. 单击 **新项目**。会出现 **添加新的广告软件／可能不想安装的应用程序** 对话框。
2. 转到 Sophos 安全隐患分析网页 http://www.sophos.com/security/analyses 中。
3. 在 **View by type（按类型查看）** 栏中，根据您想要批准的应用程序的类型，选择 **Adware（广告软件）** 或 **PUA（可能不想安装的应用程序）**。单击 **Go**。
4. 找到您想要批准的应用程序，将应用程序的名称输入到 **添加新的广告软件／可能不想安装的应用程序** 对话框中。单击 **确定**。该程序将被添加到 **已知的广告软件／可能不想安装的应用程序** 列表中。
5. 选择该应用程序，并单击 **添加** 将其添加到 **已批准的广告软件／可能不想安装的应用程序** 列表中。

如果您想从该列表中删除某个应用程序，请选择该应用程序，并单击 **删除项目**。

更改要扫描的文件类型

依照默认值，Sophos Anti-Virus 会对各种容易被病毒感染的文件类型进行扫描。您可以扫描附加的文件类型，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，在不同的操作系统上会有所不同，并且在软件更新后，可能发生改变。要查看文件类型，请在相应的操作系统的计算机上，打开 Sophos Anti-Virus 窗口，找到 '排除 '配置页面。


这些选项仅仅应用于 Windows 计算机。


在 Windows 2000 或以后的操作系统中，您可以分别为读写扫描和计划扫描更改设置。在 Windows NT/95/98/Me 操作系统中，在计划扫描中所作的更改，会同时被应用于读写扫描。


您可以使用 Sophos Update Manager 在 Mac OS X 计算机上更改防病毒设置，Sophos Update Manager 是随 Sophos Anti-Virus for Mac OS X 提供的一个工具软件。要打开 Sophos Update Manager，请在 Mac OS X 计算机的 **Finder** 窗口中，浏览找到 Sophos Anti-Virus:ESOSX 文件夹。双击 **Sophos Update Manager**。要了解更多详情，请参见 Sophos Update Manager 帮助文件。

您可以按照 Sophos Anti-Virus for Linux 用户手册中的说明，使用 savconfig 和 savscan 命令，在 Linux 计算机上进行更改。

您可以按照 Sophos Anti-Virus for UNIX 用户手册中的说明，使用 savscan 命令，在 UNIX 计算机上进行更改。

要更改要扫描的文件类型：

1. 检查哪个防病毒和 HIPS 策略被您想要配置的计算机组所采用了。
2. 在 **策略** 窗格板中，双击 **防病毒和 HIPS**。然后，双击您想要更改的那个策略。
3. 在 **防病毒和 HIPS 策略** 对话框中，按照以下说明设置选

项：

要配置读写扫描，在 **配置 Sophos Anti-Virus 和 HIPS** 面板中，确保勾选了 **启用读写扫描** 勾选框。单击 **读写扫描** 按钮。

要配置计划扫描，请在 **计划扫描** 栏中，单击 **扩展名和排除文件**。

4. 在 **扩展名** 标签页中，选择 **扫描可执行和可感染文件**。

   要扫描附加的文件类型，请单击 **添加**，然后，在 **扩展名** 栏中，键入文件类型的扩展名，如：PDF。

   要免去扫描某些，通常默认扫描的文件类型，请单击 **排除文件**。这会打开 **排除文件扩展名** 对话框。输入文件扩展名。

   依照默认值，会扫描没有扩展名的文件。


您还可以选择扫描所有文件，尽管这会影响计算机的运行效率。

从读写扫描中排除项目

您可以排除要进行读写扫描的项目。


这些选项只应用于 Windows 2000 或以后，Mac OS X，Linux，以及 UNIX。


要在 Windows NT/95/98/Me 计算机上排除项目，请使用计划扫描配置页，在该页面中的配置同样可以应用于读写扫描。

1. 检查哪个防病毒和 HIPS 策略被您想要配置的计算机组所采用了。
2. 在 **策略** 窗格板中，双击 **防病毒和 HIPS**。然后，双击您想要更改的那个策略。
3. 会出现 **防病毒和 HIPS 策略** 对话框。在 **配置 Sophos Anti-Virus 和 HIPS** 面板中，单击 **读写扫描** 按钮。

4. 单击 **Windows 排除项目**，**Mac 排除项目**，或 **Linux/Unix 排除项目** 标签页。要添加项目到列表中，请单击 **添加**，然后，在 **排除项目** 对话框中输入完整的路径。您可以从扫描中排除的项目，因计算机的类型会有所不同。请参见可以从扫描中排除的项目。

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。

1. 检查哪个防病毒和 HIPS 策略被您想要配置的计算机组所采用了。
2. 在 **策略** 窗格板中，双击 **防病毒和 HIPS**。然后，双击您想要更改的那个策略。
3. 在 **防病毒和 HIPS 策略** 对话框的 **计划扫描** 面板中，单击 **添加**（或者选择现有的扫描，并单击 **编辑**）。
4. 在 **计划扫描设置** 对话框中，输入您的设置，然后，单击 **配置**（在该页的底部）。
5. 在 **扫描和清除设置** 对话框中的 **扫描** 标签页里，选择 **扫描打包文件内部**。单击 **确定**。

扫描 Macintosh 文件

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

这些设置只应用于 Windows 2000 及以后的计算机上的 Sophos Anti-Virus 7 及以后。

1. 检查哪个防病毒和 HIPS 策略被您想要配置的计算机组所采用了。
2. 在 **策略** 窗格板中，双击 **防病毒和 HIPS**。然后，双击您

想要更改的那个策略。

3. 在 **防病毒和 HIPS 策略** 对话框中，按照以下说明设置选项：

读写扫描

要配置读写扫描，在 **配置 Sophos Anti-Virus 和 HIPS** 面板中，确保勾选了 **启用读写扫描** 勾选框。单击 **读写扫描** 按钮。

在 **扫描** 标签页的 **扫描选项** 面板中，勾选 **扫描 Macintosh 病毒** 勾选框。

计划扫描

要配置计划扫描，在 **计划扫描** 面板中，单击 **添加**（或者，选择某个现有的扫描，单击 **编辑**）。

在 **计划扫描设置** 对话框中，输入您的设置，然后，单击 **配置**。

在 **扫描和清除设置** 对话框中的 **扫描** 标签页中，勾选 **扫描 Macintosh 病毒** 勾选框。

开启或关闭读写扫描

依照默认值，Sophos Anti-Virus 会在用户读写文件时扫描该文件，如果发现该文件感染了病毒，则会拒绝用户访问该文件。

您出于提高运行效率的考虑，可能会决定在 Exchange 服务器或其它服务器上，关闭读写扫描。在这种情况下，请将这些服务器放到一个专门的组中，并按照下面的说明更改组的防病毒和 HIPS 策略。


如果您关闭了服务器上的读写扫描，建议您在与该服务器相关的工作站上设置计划扫描。

1. 检查哪个防病毒和 HIPS 策略被您想要配置的计算机组所采用了。

2. 在 **策略** 窗格板中，双击 **防病毒和 HIPS**。然后，双击您想要更改的那个策略。
3. 会出现 **防病毒和 HIPS 策略** 对话框。要关闭读写扫描，请取消勾选 **启用读写扫描** 勾选框。然后，在 **计划扫描** 面板中，单击 **添加** 并设置计划扫描。

如果您以后想重新启用读写扫描，请勾选该勾选框。

更改实行读写扫描的时机

您可以指定，当您打开文件（"读文件时"），保存文件（"写文件时"），或者，文件重命名时，是否扫描文件。

⚠ 在"写文件时"或"重命名文件时"进行扫描，会对计算机的运行效率产生影响。这些选项一般不建议使用。

⚠ 这些选项仅仅应用于 Windows 计算机。

1. 检查哪个防病毒和 HIPS 策略被您想要配置的计算机组所采用了。
2. 在 **策略** 窗格板中，双击 **防病毒和 HIPS**。然后，双击您想要更改的那个策略。
3. 在 **防病毒和 HIPS 策略** 对话框的 **配置 Sophos Anti-Virus 和 HIPS** 栏中，单击 **读写扫描** 按钮。
4. 在 **读写扫描设置** 对话框中的 **扫描** 标签页中，在 **读写扫描行为** 面板中，选择您想要的选项。

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。

⚠ 计划扫描只在 Windows 和 UNIX 操作系统计算机上运行。在 Windows 95/98/Me 计算机中，计划扫描只在 Sophos Anti-Virus 窗口打开时，才会运行。

1. 检查哪个防病毒和 HIPS 策略被您想要配置的计算机组所采用了。

2. 在 **策略** 窗格板中，双击 **防病毒和 HIPS**。然后，双击您想要更改的那个策略。
3. 在 **防病毒和 HIPS 策略** 对话框的 **计划扫描** 面板中，单击 **添加**。
4. 在 **计划扫描设置** 对话框中，为扫描任务输入名称。选择要扫描的项目（依照默认值，会扫描所有的本地硬盘或挂上(mounted)的文件系统）。选择您想运行该扫描的日期和时间。

   如果您更改其它扫描选项，或配置该扫描清除计算机，请单击在该对话框底部的 **配置**。

   要了解关于怎样更改计划扫描的选项的信息，请参见 更改计划扫描设置。

更改计划扫描设置

您可以更改计划扫描的设置。

1. 检查哪个防病毒和 HIPS 策略被您想要配置的计算机组所采用了。
2. 在 **策略** 窗格板中，双击 **防病毒和 HIPS**。然后，双击您想要更改的那个策略。
3. 在 **防病毒策略和 HIPS** 对话框中，在 **计划扫描** 面板中，您可以更改两种不同的设置：

   要更改**所有**的计划扫描都扫描的文件类型，单击 **扩展名和排除文件名**。

   要更改针对每一个扫描的具体设置（扫描项目，时间，扫描选项，清除），高亮选择该扫描，并单击 **编辑**。然后，在 **计划扫描设置** 对话框中，单击 **配置**。

   要了解怎样使用扫描选项的详情，请参见 扫描可疑文件，扫描广告软件／可能不想安装的应用程序，以及扫描打包文件内部。要了解怎样使用清除选项，请参见 自动清除计算机。

从计划扫描中排除项目

您可以排除要进行计划扫描的项目。

⚠ 在 Windows NT/95/98/Me 操作系统中，在计划扫描中所作的更改，会同时被应用于读写扫描。

⚠ 计划扫描中的“排除项目”设置，同样应用于从控制台运行的完整系统扫描，以及应用于在联网计算机上运行的“扫描我的电脑”。

1. 检查哪个防病毒和 HIPS 策略被您想要配置的计算机组所采用了。
2. 在 **策略** 窗格板中，双击 **防病毒和 HIPS**。然后，双击您想要更改的那个策略。
3. 会出现 **防病毒和 HIPS 策略** 对话框。在 **计划扫描** 面板中，单击 **扩展名和排除文件**。
4. 单击 **排除文件** 标签。要添加项目到列表中，请单击 **添加**，然后，在 **排除项目** 对话框中输入完整的路径。您可以从扫描中排除的项目，因计算机的类型会有所不同。请参见可以从扫描中排除的项目。

可以从扫描中排除的项目

在每种不同的操作系统的计算机上，对所能够从扫描中排除的项目，会有不同的限制。

Windows 2000 和以后

在 Windows 2000 或以上的计算机中，您可以排除驱动器，文件夹和文件。

您可以使用通配符 * 和 ?

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 * 仅能以 [filename].* 或 *.[extension] 的形式用于文件名或扩展名中。比如，file*.txt，file.txt* 及 file.*txt 是无效的。

要了解更多的详情，请参见 Sophos Anti-Virus for Windows 2000 和以后的有关帮助文件或用户手册。

Windows NT

在 Windows NT 计算机中，您可以排除文件和目录。

Windows 95/ 98/ Me

在 Windows 95/98/Me 计算机中，您可以排除文件，目录（针对计划扫描），以及驱动器。

Mac OS X

在 Mac OS X 中，您可以排除卷，文件夹，以及文件。

尽管不支持使用通配符，您还是可以通过在欲排除的项目的前面或后面添加斜线或双斜线，来将其排除。

要了解更多的详情，请参见 Mac OS X 的有关帮助文件或用户手册。

Linux 和 UNIX

在 Linux 和 UNIX 中，您可以通过指定路径（带有或不带有通配符）来排除目录和文件。

Enterprise Console 只支持基于路径的 Linux 和 UNIX 排除项目。您还可以在已管理的计算机上，直接设置其它类型的排除项目。然后，您可以使用通常表示方式，排除文件类型和文件系统。要了解操作指导，请参见 Sophos Anti-Virus for Linux 用户手册，或 Sophos Anti-Virus for UNIX 用户手册。

如果您在已管理的 Linux 或 UNIX 计算机上，设置另一个基于路径的排除项目，该计算机将被作为具有不一致的组策略的计算机，报告给控制台。

12 怎样更改应用程序控制的设置？

Enterprise Console 使您能够检测和阻断“受控程序”，即：是正当的，并非安全隐患的应用程序，但是您认为它不适合在办公环境使用。类似的应用程序包括：即时消息(IM)客户端，语音IP电话(VoIP)客户端，游戏，数字影像软件，媒体播放器，浏览器插件，等等。


这些设置只应用于 Windows 2000 及以后的计算机上的 Sophos Anti-Virus 7 及以后。

应用程序可以被阻断或被批准给不同的计算机组，具有很大的灵活性。例如：可以在办公室的台式机上关闭，但在远程计算机上批准 VoIP。


此受控程序列表由 Sophos 提供，并定期更新。您不能添加新的应用程序到此列表中。

本节将说明怎样选择您想在网络中控制的应用程序，以及怎样设置扫描受控程序。

- 选择想要控制的应用程序
- 扫描想要控制的应用程序
- 卸载不想要的受控程序

选择想要控制的应用程序

依照默认值，会允许所有的应用程序。按照以下说明，您可以选择想要控制的应用程序：

1. 检查哪个应用程序控制策略被您想要配置的计算机组所采用了。
2. 在 **策略** 窗格板中，双击 **应用程序控制**。然后，双击您想要更改的那个策略。
3. 在 **应用程序控制策略** 对话框中，单击 **批准** 标签。
4. 选择某个 **应用程序类型**，如：**文件共享**。包含在该组中的应用程序的完整列表会出现在下面的 **已批准** 列表。

要阻断某个应用程序，请选择该应用程序，并单击“添加”按钮，将它移到 **已阻断** 列表中。

要阻断将来会由 Sophos 添加到此类型中的任何新的应用程序，请移动 **将来全部由 Sophos 添加** 到 **已阻断** 列表中。

要阻断该类型的所有应用程序，请单击“全部添加”按钮，将所有的应用程序从 **已批准** 列表中移到 **已阻断** 列表中。

5. 在 **应用程序控制策略** 对话框的 **扫描** 标签中，确保启用了扫描受控程序。（请参见 扫描您想要控制的应用程序，了解更多详情。）单击 **确定**。

扫描想要控制的应用程序

您可以配置 Sophos Anti-Virus 读写扫描您想在网络中控制的应用程序。

1. 检查哪个应用程序控制策略被您想要配置的计算机组所采用了。
2. 在 **策略** 窗格板中，双击 **应用程序控制**。然后，双击您想要更改的那个策略。会出现 **应用程序控制策略** 对话框。
3. 在 **扫描** 标签中，按照以下说明设置选项：

   要启用读写扫描，请勾选 **启用读写扫描** 勾选框。如果您想要在读写时检测应用程序，但是不想阻断它们，请选择 **检测但允许运行** 勾选框。

   要启用即时和计划扫描，请勾选 **启用即时和计划扫描** 勾选框。

   您的防病毒和 HIPS 策略设置，将决定哪些文件会被扫描（即：扩展名和排除项目）。

如果您想要删除在联网计算机上发现的受控程序，请按照 卸载不想要的受控程序 中的指导说明做。

如果组中的任何一台计算机中出现受控程序，您还可以向特定的用户寄送警报。要了解怎样做，请参见设置应用程序控制警报。

卸载不想要的受控程序

在您卸载受控程序之前，请确保读写扫描受控程序已被禁用。这种类型的扫描会阻断用于安装和卸载应用程序的程序，所以它会干扰卸载过程。

您可以使用以下两种方法之一删除应用程序：

- 转到每一台计算机，运行该应用程序的卸载程序。您通常可以使用 Windows 控制面板中的“添加/删除程序”来实现这一点。
- 在服务器上，使用您的脚本程序或管理工具，运行卸载程序，卸载联网计算机中的应用程序。

现在，您可以重新启用读写扫描受控程序了。

13 怎样更改防火墙设置？

本节将说明怎样设置防火墙，以及怎样更改防火墙设置。

- 设置防火墙
- 什么是默认的设置？
- 允许使用文件和打印共享
- 允许使用被阻断的应用程序
- 选择交互式或非交互式工作模式
- 开启或关闭防火墙
- 获取有关高级选项的帮助

设置防火墙

当您安装防火墙时，依照默认值，它会被设为启用，并会阻断所有可有可无的网络通讯流。要了解更多详情，请单击默认设置。

您在网络中的计算机上开始使用防火墙之前，您必须配置它，以便允许正常的应用程序可以运行。您难以容易地通过 Enterprise Console 做到这一点，因为各台计算机可能使用的是同一个应用程序的不同版本。变通的办法是，采用样本计算机进行配置，然后将这些配置应用为策略。

1. 在您的网络中具有代表性的计算机上安装防火墙。
2. 到该计算机上，右击任务栏上的防火墙图标（如下所示）。

   单击 **配置**。
3. 在 **Sophos Client Firewall 配置编辑器** 对话框中，单击 **应用程序** 标签。单击 **添加** 然后浏览找到您想要添加的每一个应用程序。于是，该应用程序会被“信任”。如要更高的安全性，可以高亮选择该程序，然后，单击 **自定义** （对话框的右下方）然后创建规则。

   或者，在 **常规** 标签页中，选择 **交互**。当每一个应用程序被使用时，防火墙会提示您决定允许使用，还是阻断它。
4. 对防火墙的配置完成后，在 **常规** 标签页中，单击 **导出** 以将配置导出到您选择的路径中。
5. 在您的每一台样本计算机上，重复上述步骤。
6. 现在请转到 Enterprise Console。在 **策略** 窗格板中，双击 **防火墙** 然后双击您想要编辑的策略。
7. 在 **防火墙策略** 对话框中，在 **常规** 标签页中，单击 **导入**，然后，导入您稍早前完成的配置。

当您导入每一个配置时，会出现选项，让您将导入的配置与已经导入的其它配置合并。

8. 至此，您已经完成了对防火墙的配置，允许使用通常使用的应用程序。您还可以更改其它的设置（比如，允许使用文件和打印共享）。有关全部选项的详情，请参见 Sophos Client Firewall 帮助文件。

什么是默认的设置？

依照默认值，Sophos Client Firewall 会被启用，并会阻断所有可有可无的网络通讯流。在您启用它之前，您在整个网络中使用它之前，您应该按照设置防火墙中的说明，配置防火墙，以便允许使用您想要使用的应用程序。

该防火墙的其它默认设置如下：

- 不要求用户的确认信息，就应用各种规则（"非交互"模式）。
- 如果在被管理的计算机上，规则被个别地更改了，就会在 Enterprise Console 中显示警报。
- 如果其它应用程序更改了内存，就会阻断线程。
- 扣下发送到被封闭了的端口的通讯包（"隐形"操作）
- 使用总和检查识别新的和被更改过的应用程序。
- 阻断 IPv6 包（只应用于 Sophos Client Firewall 1.5）。
- 向 Enterprise Console 报告新的和被更改过的应用程序。
- 针对可能会启动隐藏线程的应用程序发出警报.

允许使用文件和打印共享

您可以按照以下说明，允许计算机使用文件和打印共享：

1. 检查哪个防火墙策略被您想要配置的计算机组所采用了。
2. 在 **策略** 窗格板中，双击 **防火墙**。然后，双击您想要更改

的那个策略。

3. 在 **防火墙策略** 对话框中，单击 **LAN** 标签，然后，单击 **检测** 以检测局域网中的地址。
4. 勾选列表中地址旁的 **NetBIOS** 勾选框。

允许使用被阻断的应用程序

如果在您的网络中的计算机上，防火墙阻断了某个应用程序，会在 **状态** 页中计算机名称旁出现警报。

按照以下说明，您可以查看被阻断的应用程序的详情，并允许使用它们，或者为其创建新的规则：

1. 检查哪个防火墙策略被计算机采用了。
2. 在 **策略** 窗格板中，双击 **防火墙**。然后，双击您想要更改的那个策略。
3. 在 **防火墙策略** 对话框中，单击 **应用程序** 标签。
4. 在 **应用程序** 标签中，单击 **添加**。会出现 **应用程序管理器**。从列表中选择一个应用程序，并单击 **确定**。
5. 在 **应用程序规则** 对话框中，单击 **信任** 以允许使用该应用程序，或者，单击 **自定义** 为其运行创建特定的自定义规则。

选择交互式或非交互式工作模式

Sophos Client Firewall 可以有两种不同的工作模式：

- **交互式** 防火墙会询问用户怎样处置通讯流中的种种情形。
- **非交互式** 防火墙将应用您制定的规则，自动处置通讯流中的种种情形。

要改变针对某个计算机组的工作模式，请按以下说明做：

1. 检查哪个防火墙策略被您想要配置的计算机组所采用了。
2. 在 **策略** 窗格板中，双击 **防火墙**。然后，双击您想要更改

的那个策略。

3. 在 **防火墙策略** 对话框中的 **常规** 标签中，选择 **非交互** 或 **交互**。单击 **确定**。

开启或关闭防火墙

在首次安装后，依照默认值，Sophos Client Firewall 会被启用。

要开启／关闭针对某个计算机组的防火墙，请按以下说明做：

1. 检查哪个防火墙策略被您想要配置的计算机组所采用了。
2. 在 **策略** 窗格板中，双击 **防火墙**。然后，双击您想要更改的那个策略。
3. 在 **防火墙策略** 对话框中的 **常规** 标签里，勾选或取消勾选 **允许所有通讯流** 勾选框。单击 **确定**。

获取有关高级选项的帮助

有关全部防火墙选项的完整详情，请参见 Sophos Client Firewall 帮助文件。

14 怎样更改 NAC 设置？

本节将说明怎样设置 NAC（网络访问控制），以及编辑 NAC 策略。

- 设置 NAC
- 设置 NAC 服务器的 URL
- 启动 NAC Manager
- 什么是默认的 NAC 设置？
- 什么是预设的 NAC 策略？
- 编辑 NAC 策略

设置 NAC

您可以设置网络访问控制(NAC)，这样只有遵照您所设置的条件的计算机，才能登录到网络中。

Enterprise Console 与 Sophos NAC 一起工作，为网络提供保护。您需要已经安装了：

- Sophos NAC Server 与 Enterprise Console 分开安装
- Sophos NAC 代理 安装它到联网计算机上，这样，联网计算机就能够与 NAC 服务器通讯。您可以使用保护计算机功能安装它。

本节假定您已经安装了两者。

依照默认值，计算机会被允许访问网络。

设置 NAC 服务器的 URL

如果要使用 Sophos NAC，您必须在 Enterprise Console 中指定安装了 Sophos NAC 的那台服务器的 URL。只有这样：

- 您的计算机才能够与该 NAC 服务器通讯，并接收它们的 NAC 策略。
- 您才能够可以配置 NAC 策略，这些策略由 NAC 服务器保存。

当您首次安装 Enterprise Console 时，它会试图寻找并连接该 NAC 服务器。总之，如果连接不成功，或者，如果您更改了该 NAC 服务器的路径，那么，您需要指定该 URL。

要输入或更改该 URL：

1. 在 **工具** 菜单中，选择 **配置 NAC URL**。
2. 在 **Sophos NAC URL** 对话框中，输入 NAC 服务器的 URL（如：http://server

如果安装 Sophos NAC 的是多台服务器，那么，请使用运行了应用程序本身的那台服务器的地址，而不要使用安装了数据库的那台服务器的地址。

3. 要核实 Enterprise Console 是否能通过所提供的 URL 连接到 NAC 服务器，请单击 **测试连接**。

启动 NAC Manager

Sophos NAC Manager 是用来编辑 NAC 策略的界面。

要启动 NAC Manager：

1. 单击工具栏上的 **NAC** 按钮。或者，在 **工具** 菜单中，选择 **管理 NAC**。

如果事先没有指定，或者，没有检测到 NAC 服务器 URL，您会被提示指定它。

2. 使用您的 Sophos NAC 用户认证资料（它由 Sophos NAC 系统管理员提供）登录。

要了解该界面的完整详情，请参见 Sophos NAC Manager 帮助文件，或 *Sophos NAC Manager Guide*（英文）。

什么是默认的 NAC 设置？

依照默认值，**默认的** NAC 策略将应用到安装了 Sophos NAC 的计算机上。除非您已经更改了“策略模式”，这意味着：

- 计算机将被允许访问网络
- Sophos NAC 以仅限报告模式运行

要了解预设的 **已管理** 和 **未管理** 策略，请参见什么是预设的 NAC 策略？

什么是预设的 NAC 策略？

有三种预设的策略。您可以按照编辑 NAC 策略中的说明，编辑每个策略中的设置。

默认

该策略将以默认方式应用到安装了 Sophos NAC 的计算机上。计算机会被允许访问网络，除非您已经更改了该策略的设置。Sophos NAC 以仅限报告模式运行

已管理

该策略可以用于已被 Enterprise Console 管理的，安装了 Sophos NAC 的计算机上。它的初始设置与默认策略相同。

未管理

该策略可以用于来自公司之外的计算机，这些计算机没有被 Enterprise Console 管理，也没有安装 Sophos NAC。您的公司可以要求这样的来宾用户，连接到某个网站上，那里会有一个网页代理，在允许来宾用户的计算机访问网络之前，对照策略对它们进行评估。

要了解更多信息，请参见 *Sophos NAC Manager Guide*（英文）中的"Using pre-defined policies"。

编辑 NAC 策略

您可以更改任何预设的 NAC 策略中的设置。

1. 在 **策略** 窗格板中，双击 **NAC**。双击您想要更改的策略。
2. Sophos NAC Manager 会启动。使用您的认证资料登录。
3. 在该策略的页面中，编辑选项。

要了解有关选项的信息，请参见 *Sophos NAC Manager Guide*（英文）中的 "Updating policies"。

15 怎样扫描计算机？

依照默认值，Sophos Anti-Virus 会在用户读写文件时，自动对文件中的已知和未知的病毒，特洛伊木马，蠕虫，以及间谍软件进行检测。Windows 2000 及以后的计算机上的 Sophos Anti-Virus 7 及以后，还可以分析在系统中运行的程序的行为。

您还可以配置 Sophos Anti-Virus：

- 扫描可疑文件
- 扫描广告软件／可能不想安装的应用程序
- 在设定的时间扫描计算机

要了解更多有关配置扫描的信息，请参见 怎样更改防病毒和 HIPS 设置？

本节将说明怎样立即在所选择的计算机上执行完整系统扫描。

现在扫描计算机

您可以立即扫描一个或数个计算机，无需等到下一次的计划扫描。


只有运行在 Windows 计算机上的 Sophos Anti-Virus 7 或以后，或 UNIX 计算机，可以执行从控制台启动的即时完整系统扫描。

1. 请选择计算机列表中的计算机，或窗格板中的 **组**。右击并选择 **完整系统扫描**。

   或者，在 **措施** 菜单中，选择 **完整系统扫描**。

2. 在 **完整系统扫描** 对话框中，查看将要被扫描的计算机的详情，然后，单击 **确定** 以启动扫描。

16 怎样设置警报？

在 Enterprise Console 中可以使用数种警报方法。

- **控制台中显示的警报**

  如果在计算机上发现了需要关注的项目，或出现了错误，Sophos Anti-Virus 会向 Enterprise Console 发送警报。警报会出现在计算机列表中。要了解更多有关警报的信息，请参见 怎样处置警报？

  这些警报总是会显示在控制台。您不必专门设置。

- **控制台向您选择的收件人发送警报**

  依照默认值，当计算机中检测到某个项目时，会出现桌面警报，以及记录会添加到 Windows 事件日志中。

  您也可以为网络管理员设置电子邮件警报，或 SNMP 警报。

本节说明怎样设置发送给您所选择的收件人的警报。

- 设置防病毒和 HIPS 电子邮件警报
- 设置防病毒和 HIPS SNMP 警报
- 配置防病毒和 HIPS 桌面警报
- 设置应用程序控制警报
- 设置网络状态电子邮件警报
- 设置 Active Directory 同步化电子邮件警报
- 配置事件日志记录

设置防病毒和 HIPS 电子邮件警报

如果组中的任何一台计算机中出现病毒，可疑行为，可能不想安装的应用程序，或错误，您可以向特定的用户寄送电子邮件警报。

Mac OS X 计算机只能向一个地址寄送电子邮件警报。

1. 在 **策略** 窗格板中，双击您想要更改的防病毒和 HIPS 策略。
2. 在 **防病毒和 HIPS 策略** 对话框的 **配置 Sophos Anti-Virus 和 HIPS** 面板中，单击 **消息发送**。
3. 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。

启用电子邮件警报发送

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 发送电子邮件的事件：

病毒／间谍软件检测和清除

可疑行为检测

可疑文件检测

病毒／间谍软件检测和清除

扫描出错（如：拒绝访问）

其它错误

可疑行为检测 和 **可疑文件检测** 的设置只应用于 Windows 2000 及以后的计算机上的 Sophos Anti-Virus 7 及以后。

广告软件／可能不想安装的应用程序检测和清除 的设置只应用于 Windows 2000 及以后的计算机上的 Sophos Anti-Virus 6 及以后。

其它错误 的设置只应用于 Windows 计算机。

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 **重命名** 更改您所添加的电子邮件地址。

Mac OS X 计算机将只向列表中的第一个收件人发送邮件。

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。在 **配置 SMTP 设置** 对话框中，按照以下说明输入详情。

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** 发送测试的电子邮件警报。

SMTP '寄件人' 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。

Linux 和 UNIX 计算机将忽略 SMTP 寄件人和回复地址，并使用地址 “root@<hostname>”。

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。

设置防病毒和 HIPS SNMP 警报

如果组中的任何一台计算机中出现病毒或错误，您可以向特定的用户寄送 SNMP 警报。

这些设置只应用于 Windows 2000 及以后的计算机上的 Sophos Anti-Virus 6 及以后。

1. 在 **策略** 窗格板中，双击您想要更改的防病毒和 HIPS 策

略。

2. 在 **防病毒和 HIPS 策略** 对话框的 **配置 Sophos Anti-Virus 和 HIPS** 面板中，单击 **消息发送**。
3. 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 消息的事件类型：

病毒／间谍软件检测和清除

可疑行为检测

可疑文件检测

病毒／间谍软件检测和清除

扫描出错（如：拒绝访问）

其它错误

可疑行为检测 和 **可疑文件检测** 的设置只应用于 Windows 2000 及以后的计算机上的 Sophos Anti-Virus 7 及以后。

SNMP 陷阱目标

在该文本框中，输入收件人的 IP 地址。

SNMP 团体名

在该文本框中，输入 SNMP 团体名。

配置防病毒和 HIPS 桌面警报

依照默认值，桌面警报会显示在发现病毒，可疑项目，或可能不想安装的应用程序的计算机上。您可以配置这些警报。

1. 在 **策略** 窗格板中，双击您想要更改的防病毒和 HIPS 策略。
2. 在 **防病毒和 HIPS 策略** 对话框的 **配置 Sophos Anti-Virus 和 HIPS** 面板中，单击 **消息发送**。
3. 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，以启用 Sophos Anti-Virus 显示桌面消息。

要发送的消息

选择您想要 Sophos Anti-Virus 显示桌面消息的事件类型：

病毒／间谍软件检测和清除

可疑行为检测

可疑文件检测

病毒／间谍软件检测和清除

可疑行为检测 和 **可疑文件检测** 的设置只应用于 Windows 2000 及以后的计算机上的 Sophos Anti-Virus 7 及以后。

广告软件／可能不想安装的应用程序检测和清除 的设置只应用于 Windows 2000 及以后的计算机上的 Sophos Anti-Virus 6 及以后。

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。

设置应用程序控制警报

当发现受控程序时，您可以向特定的用户发送警报。

1. 在 **策略** 窗格板中，双击您想要更改的应用程序控制策略。
2. 在 **应用程序控制策略** 对话框中，在 **消息发送** 标签页中，按照以下说明设置选项。

消息发送

依照默认值，已勾选 **启用桌面消息发送** 勾选框。当读写扫描检测到，并阻断了未经批准的受控程序时，会有桌面消息显示给用户，告知他们该应用程序已被阻断。

在 **消息** 文本框中，您可以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。

勾选 **启用电子邮件警报发送** 勾选框，以启用 Sophos Anti-Virus 寄送电子邮件警报。

勾选 **启用 SNMP 消息发送** 勾选框，以启用 Sophos Anti-Virus 寄送 SNMP 消息。

您的防病毒和 HIPS 策略设置，将决定电子邮件和 SNMP 消息发送的配置和收件人。

控制台警报发送

依照默认值，在首次检测到某个应用程序，会有警报出现在控制台中。

如果您想要在每次检测到该应用程序时，都看到警报，请取消勾选 **只在首次检测到时出现警报** 勾选框。

设置网络状态电子邮件警报

您可以设置电子邮件警报，当指标面板中出现 '警告 '或 '越过了紧要级 '时，可以向您所选择的收件人寄送警报。

1. 在 **工具** 菜单中，选择 **配置电子邮件警报**。会出现 **配置电**

子邮件警报 对话框。

2. 如果尚未配置 SMTP 设置，或者，如果您想要查看或更改设置，请单击 **配置**。在 **配置 SMTP 设置** 对话框中，按照以下说明输入详情。

   在 **服务器地址** 文本框中，输入主机名或 SMTP 服务器的 IP 地址。

   在 **寄件人** 文本框中，输入退回邮件和未送达报告将要寄往的地址。

   单击 **测试** 测试连接情况。

3. 在 **收件人** 面板中，单击 **添加**。会出现 **添加新的电子邮件警报收件人** 对话框。
4. 在 **电子邮件地址** 文本框中，输入您的收件人的地址。
5. 在 **语言** 文本框中，选择寄送电子邮件警报所使用的语言。
6. 在 **预订** 窗格板中，选择您想要寄给该收件人的 "越过了警告级 "和 "越过了紧要级 "电子邮件警报。

   "越过了警告级 "电子邮件警报：

   警报

   错误

   未及时更新的计算机

   具有不一致策略的计算机

   "越过了紧要级 "电子邮件警报：

   警报

   错误

   未及时更新的计算机

   具有不一致策略的计算机

   最近一次从 Sophos 更新以来的时间

设置 Active Directory 同步化电子邮件警报

您还可以设置电子邮件警报，以便在与 Active Directory 同步化过程中，找到新的计算机和组时，可以向您所选择的收件人寄送警报。如果您选择了自动保护已同步化的组中的计算机，那么，您还可以设置在自动保护失败时，发出警报。

1. 在 **工具** 菜单中，选择 **配置电子邮件警报**。会出现 **配置电子邮件警报** 对话框。
2. 如果尚未配置 SMTP 设置，或者，如果您想要查看或更改设置，请单击 **配置**。在 **配置 SMTP 设置** 对话框中，按照以下说明输入详情。

   在 **服务器地址** 文本框中，输入主机名或 SMTP 服务器的 IP 地址。

   在 **寄件人** 文本框中，输入退回邮件和未送达报告将要寄往的地址。

   单击 **测试** 测试连接情况。
3. 在 **收件人** 面板中，单击 **添加**。会出现 **添加新的电子邮件警报收件人** 对话框。
4. 在 **电子邮件地址** 文本框中，输入您的收件人的地址。
5. 在 **语言** 文本框中，选择寄送电子邮件警报所使用的语言。
6. 在 **预订** 窗格板中，选择您想要寄给该收件人的 “Active Directory 同步化 ”电子邮件警报。

   “Active Directory 同步化 ”电子邮件警报：

   找到的新组

   找到的新计算机

   自动保护计算机失败

配置事件日志记录

要使 Sophos Anti-Virus 能够在检测到某个项目，或在发生错误时，添加警报到 Windows 2000 或以后的事件日志中，请按照

以下说明做：

1. 在 **策略** 窗格板中，双击您想要更改的防病毒和 HIPS 策略。
2. 在 **防病毒和 HIPS 策略** 对话框的 **配置 Sophos Anti-Virus 和 HIPS** 面板中，单击 **消息发送**。
3. 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。

17 怎样处置警报？

本节将说明怎样处置警报。

它包括：

- 警报图标的含义
- 处置病毒和间谍软件警报
- 处置可疑行为警报
- 处置可疑文件警报
- 处置防火墙警报
- 处置广告软件／可能不想安装的应用程序警报
- 处置受控程序警报
- 从控制台中清空警报

警报图标的含义

如果有病毒，间谍软件，可疑项目，广告软件，或其它可能不想安装的应用程序，警告图标会出现在 Enterprise Console **状态**页中。

以下是警报图标的示例。在本节的其它页中，您可以找到针对这些警报的相关建议。

如果软件已禁用，或者未及时更新，在控制台中也会出现警告信息。要了解更多的有关信息，请参见 怎样检查网络是否受保护？

警报图标

标志	释意
	出现在 **警报和错误** 栏中的红色警报标志表明，检测到了病毒，蠕虫，特洛伊，间谍软件，或可疑行为。
	出现在 **警报和错误** 栏中的黄色警告标志表明，以下情况之一： • 检测到了可疑文件。 • 检测到了广告软件或其它可能不想安装的应用程序。 • 检测到了受控程序。 • 防火墙已阻断了某个应用程序。 • 出现错误。 出现在 **防病毒和 HIPS 策略**，**防火墙策略**，**更新策略**，或 **应用程序控制策略** 栏中的黄色警告标志表明，计算机使用的相应的策略与同组的其它计算机的不一致。

如果计算机中出现了多个警报和错误，具有最高的优先级的警报的图标，会出现 **警报和错误** 栏中。以下列示的警报类型，以降序排列优先级。

警报优先级

1. 病毒／间谍软件警报
2. 可疑行为警报
3. 可疑文件警报
4. 防火墙警报
5. 广告软件／可能不想安装的应用程序警报
6. 受控程序警报
7. Sophos Anti-Virus，更新，以及 Sophos Client Firewall 错误。

处置病毒和间谍软件警报

如果检测到了病毒／间谍软件，您会在 **状态** 页中，看到一个红色三角警告标志⚠，以及 '检测到病毒／间谍软件 '的字样。

要了解更多详情，请单击 **警报和错误详情** 标签页。要处置发现的病毒或间谍软件，请按照立即清除计算机中的说明做。

处置可疑行为警报

如果在运行时行为分析中，检测到了可疑行为或缓冲区溢出，您会在 **状态** 页中，看到一个红色三角警告标志⚠，以及 '检测到可疑行为 '的字样。

要了解更多详情，请单击 **警报和错误详情** 标签页。要删除可疑项目，请按照现在清除计算机中的指导说明做。如果您想要批准它，请参见批准可疑项目。

处置可疑文件警报

如果检测到了可疑文件，您会在 **状态** 页中，看到一个黄色三角警告标志⚠，以及 '检测到可疑文件 '的字样。

要了解更多详情，请单击 **警报和错误详情** 标签页。在 **检测到的项目** 栏中，会出现该文件的名称。

要删除该文件，请参见立即清除计算机。

要批准该文件，请按照批准可疑项目中的指导说明做。

处置防火墙警报

如果防火墙阻断了某个应用程序，您会在 **状态** 页中，看到一个黄色三角警告标志⚠，以及 '防火墙警报 '字样。

该图标也同样用于表示来自 Sophos Anti-Virus 的广告软件／可能不想安装的应用程序警报。在该图标旁会出现 '检测到广告软件／可能不想安装的应用程序 '的字样。

要了解更多详情，请单击 **警报和错误详情** 标签页。在 **检测到的项目** 栏中，会出现被防火墙阻断的应用程序的名称。

如果您想要允许使用被阻断的应用程序，或者，想为其制定新的策略，请按照允许使用被阻断的应用程序中的说明做。

处置广告软件／可能不想安装的应用程序警报

如果检测到了广告软件／可能不想安装的应用程序(PUA)，您会在 **状态** 页中，看到一个黄色三角警告标志⚠，以及 '检测到广告软件／可能不想安装的应用程序 '的字样。

该图标同样用于防火墙警报。在图标旁会出现 '防火墙警报 '的字样。

要了解更多详情，请单击 **警报和错误详情** 标签页。在 **检测到的项目** 栏中，会出现该应用程序的名称。

要删除该应用程序，请参见立即清除计算机。

要批准该应用程序，请按照批准广告软件／可能不想安装的应用程序中的说明做。

处置受控程序警报

如果检测到了受控程序，您会在 **状态** 页中，看到一个黄色三角警告标志⚠，以及 "检测到受控程序 "的字样。

要了解更多详情，请单击 **警报和错误详情** 标签页。在 **检测到的项目** 栏中，会出现该应用程序的名称。

要删除该应用程序，请参见 卸载不想要的受控程序。

从控制台中清空警报

如果您正在处置警报，或者，您确信发出警报的计算机是安全的，您可以清除显示在控制台中的警报标志。

您无法清除有关安装错误的警报。直到 Sophos Anti-Virus 成功地安装到了计算机上，这些警报才会被清除。

1. 选择您要清除警报的一台或数台计算机。右击并选择 **确认已知警报和错误**。
2. 会出现 **确认已知警报和错误** 对话框。

   要从控制台中清空警报，请在 **确认已知警报和错误** 对话框中的 **警报** 标签页，选择您想要清空的警报，然后单击 **确认**。确认已知的（清空的）警报不再出现在控制台中。

   要从控制台中清空 Sophos 产品错误，在 **确认已知警报和错误** 对话框的 **Sophos Anti-Virus 错误** 或 **Firewall 错误** 标签中，从控制台中选择您想要清空的错误，单击 **确定**。

18 怎样清除计算机？

本节将说明怎样清除感染了病毒，或者，带有不想安装的程序的计算机。

您可以：

- 立即清除计算机

- 处置清除失败的已检测到的项目
- 设置自动清除

立即清除计算机

您可以从 Enterprise Console 立即清除计算机中的病毒，或者，不想安装的程序。

此选项只能应用于运行在 Windows 2000 或以上的 Sophos Anti-Virus 6 或以上。

要清除 Windows 95/98/Me/NT4，Mac，Linux 或 UNIX 计算机，您既可以从控制台设置自动清除，也可以按照处置清除失败的已检测到的项目中的说明，个别地清除计算机。

Sophos Anti-Virus 可能会报告某个项目（如：特洛伊木马，或者，可能不想安装的应用程序）被“部分地检测到”。这说明 Sophos Anti-Virus 没有找到该应用程序的所有组件。在您能够清除该项目之前，您需要在受到影响的计算机上，进行完整系统扫描，以便找到其它的组件。要了解更多的信息，请参见部分地检测到的项目。

1. 在计算机列表中，右击您想要清除的计算机。选择 **清除已检测到的项目**。
2. 在 **清除检测到的项目** 对话框中，勾选您想要清除的每个项目旁的勾选框，或者，单击 **全选**。
3. 单击 **确定** 以清除计算机。
4. 如果清除成功，在计算机列表中出现的警报会消失。

如果还有警报剩下，您应该进行手动清除计算机。请参见 处置清除失败的感染项目。

处置清除失败的已检测到的项目

如果您无法从控制台中清除计算机中的安全隐患，您可以按照以下说明进行手动清除：

1. 在计算机列表中，单击 **警报和错误详情** 标签。在 **检测到的项目** 栏中，查找该项目的名称。
2. 在 **帮助** 菜单中，单击 **查看项目信息**。这会为您连接到 Sophos 网站，您可以从中搜索该项目的名称，找到如何清除该项目的建议。
3. 转到每一台计算机上，进行手动清除的工作。


Sophos 的网站可提供一些特别针对某些病毒和蠕虫的可下载的清除病毒小程序。

设置自动清除

您可以在一旦发现病毒或其它项目时，就立即自动清除计算机。要这样做，您可以按照以下说明更改读写扫描和计划扫描。


读写扫描不能够清除的广告软件／可能不想安装的应用程序 (PUA)。您应该按照 立即清除计算机 中的说明，处置它们。或者，在计划扫描中启用自动清除广告软件/可能不想安装的应用程序。

1. 检查哪个防病毒和 HIPS 策略被您想要配置的计算机组所采用了。
2. 在 **策略** 窗格板中，双击 **防病毒和 HIPS**。然后，双击您想要更改的那个策略。会出现 **防病毒和 HIPS 策略** 对话框。

读写扫描

在 **配置 Sophos Anti-Virus 和 HIPS** 面板中，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。请按以下说明设置选项。

病毒／间谍软件

选择 **自动清除项目中的病毒／间谍软件**。您还可以指定如果清除失败，应该处置这些项目。

不采取措施（默认值）

删除

移至默认路径

移至<指定的UNC路径>

有关“如果清除失败，应该处置这些项目？”的任何设置都不应用于 Windows 95/98/Me 计算机。

即使您选择了 **移至** 并指定了路径，Mac OS X 计算机仍然会将文件移至默认的路径。

移至默认路径 和 **移至** 的设置不应用于 Linux 和 UNIX 计算机，这些计算机将忽略这两种设置。

可疑文件

“可疑文件”的设置只应用于 Windows 2000 及以后的计算机上的 Sophos Anti-Virus 7 及以后。

您可以指定如果检测到了可疑文件，应该处置它们。

不采取措施（默认值）

删除

移至默认路径

移至<指定的UNC路径>

计划扫描

在 **防病毒和 HIPS 策略** 对话框的 **计划扫描** 面板中，选中该扫描，然后单击 **编辑**。然后，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。请按以下说明设置选项。

病毒／间谍软件

选择 **自动清除项目中的病毒／间谍软件**。您还可以指定如果清除失败，应该处置这些项目。

不采取措施（默认值）

删除

移至默认路径

移至<指定的UNC路径>

即使您选择了 **移至** 并指定了路径，Windows 95/98/Me 计算机将仍然会将文件移至默认的路径。

广告软件／可能不想安装的应用程序

如果您想要，请选择 **自动清除广告软件／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"的设置只应用于 Windows 2000 及以后的计算机上的 Sophos Anti-Virus 6 及以后。

可疑文件

"可疑文件"的设置只应用于 Windows 2000 及以后的计算机上的 Sophos Anti-Virus 7 及以后。

您可以指定如果检测到了可疑文件，应该处置它们。

不采取措施（默认值）

删除

移至默认路径

移至<指定的UNC路径>

19 怎样生成报告？

您可以生成有关网络中的警报的报告。

要生成有关网络中的病毒警报的报告，请单击工具栏中的 **报告** 图标，然后，按照本节中的说明使用 **报告** 选项。

您可以：

生成报告

要创建一份报告，请按以下说明做：

1. 在 Enterprise Console 中，打开 **工具** 菜单，并选择 **查看报告**。会出现 **报告** 对话框。
2. 在下拉菜单中，单击想要的报告类型。

   按照项目名称给出警报 显示在您的网络中检测到的，每个项目（比如某病毒或不想安装的应用程序）的警报数。

   每一路径的警报数 报告每台计算机或每组计算机中出现的警报数。

   每段时间的警报数 报告在设定的时间中警报的发生率。

   警报历史 报告每种警报的完整细节。

   在 **配置** 标签页中，您可以自定义报告。

   然后，单击 **表** 或 **图** 标签查看报告。

将报告显示为表

1. 在 Sophos Enterprise Console 中，打开 **工具** 菜单，并选择 **查看报告**。
2. 在 **报告** 对话框中的下拉菜单里，选择您想创建的报告类型。在 **配置** 标签页中，配置自定义报告。然后，单击 **表** 标签。
3. 会显示表。**报告描述** 将简要说明创建报告的各项指标（如：报告的时间跨度）。

将报告显示为图

“警报历史”的报告不能提供图。

1. 在 Sophos Enterprise Console 中，打开 **工具** 菜单，并选择 **查看报告**。
2. 在 **报告** 对话框中的下拉菜单里，选择您想创建的报告类型。在 **配置** 标签页中，配置自定义报告。然后，单击 **图** 标签。
3. 会显示图。**报告描述** 将简要说明创建报告的各项指标（如：报告的时间跨度）。

显示每个项目名称的警报数

1. 在 Sophos Enterprise Console 中，单击工具栏中的 **报告** 图标。
2. 在 **报告** 对话框中的下拉菜单里，选择 **按照项目名称给出警报**。
3. 在 **配置** 标签页中，您可以选择以下说明的选项。选择完毕后，单击其中的一个标签页，以图或表的形式显示报告。

报告的时间跨度

在 **时间跨度** 文本框中，单击下拉箭头，并选择一个时间跨

度。您既可以选择一个固定的时间，如：**上个月**，也可以选择 **自定义** 并在 **始于** 和 **止于** 框中指定您自己的时间跨度。

路径

单击 **计算机组** 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，报告会显示所有警报，以及每个警报出现的次数。您可以更改所显示的警报为下列类型之一：

全部（除受控程序之外）

仅限病毒／间谍软件

仅限可疑行为

仅限可疑文件

仅限防火墙

仅限广告软件／可能不想安装的应用程序

仅限受控程序

您还可以配置报告仅显示：

前 *n* 个警报（这里的 *n* 是您指定的数值），或者

发生率不低于 *m* 的警报（这里的 *m* 是您指定的数值）。

排序

依照默认值，报告列示的警报，是按照警报数发生数，降序排列的。如果您想要它们以字母为序，按安全隐患名称排列，请选择 **警报名称**。

显示每一路径的警报数

1. 在 Sophos Enterprise Console 中，单击工具栏中的 **报告** 图标。

2. 在 **报告** 对话框中的下拉菜单里，选择 **按照路径给出警报**。
3. 在 **配置** 标签页中，您可以选择以下说明的选项。选择完毕后，单击其中的一个标签页，以图或表的形式显示报告。

报告的时间跨度

在 **时间跨度** 文本框中，单击下拉箭头，并选择一个时间跨度。您既可以选择一个固定的时间，如：**上个月**，也可以选择 **自定义** 并在 **始于** 和 **止于** 框中指定您自己的时间跨度。

路径

单击 **计算机** 可显示每一计算机的警报，或单击 **组** 可显示每一计算机组的警报。

过滤

依照默认值，报告会显示所有警报，以及每个警报出现的次数。您可以更改所显示的警报为下列类型之一：

全部（除受控程序之外）

仅限病毒／间谍软件

仅限可疑行为

仅限可疑文件

仅限防火墙

仅限广告软件／可能不想安装的应用程序

仅限受控程序

另外，您可以配置报告，仅显示报告了特定的警报的路径。要指定单一的警报，单击下拉箭头，并单击列表中的警报名称。要指定多个警报，使用通配符，在文本框中输入安全隐患名称。使用 ?替代名称中的单个字符，以及使用 * 替代名称中的字符串。例如：使用 W32/* 将指定名称以 W32/ 开头的所有病毒。

依照默认值，报告显示所有计算机或组（取决于对 **路径** 所

作的选择）。不过，您可以配置报告，仅显示

前 *n* 个记录了最多次警报的路径（这里的 *n* 是您指定的数值），或者

不少于 *m* 个警报以上的路径（这里的 *m* 是您指定的数值）。

排序

依照默认值，报告列示的路径，是按照每一路径记录的警报数，从高到低排列的。如果您想要它们以字母为序，按路径名称排列，请选择 **路径**。

显示警报率

1. 在 Sophos Enterprise Console 中，单击工具栏中的 **报告** 图标。
2. 在 **报告** 对话框中的下拉菜单里，选择 **每段时间的警报数**。
3. 在 **配置** 标签页中，您可以选择以下说明的选项。选择完毕后，单击其中的一个标签页，以图或表的形式显示报告。

报告的时间跨度

在 **时间跨度** 文本框中，单击下拉箭头，并选择一个时间跨度。您既可以选择一个固定的时间，如：**上个月**，也可以选择 **自定义** 并在 **始于** 和 **止于** 框中指定您自己的时间跨度。

路径

单击 **计算机组** 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，报告会显示所有警报，以及每个警报出现的次数。您可以更改所显示的警报为下列类型之一：

全部（除受控程序之外）

仅限病毒／间谍软件

仅限可疑行为

仅限可疑文件

仅限防火墙

仅限广告软件／可能不想安装的应用程序

仅限受控程序

如果您想要报告，仅显示特定的警报或警报组的统计数据，请使用 **只显示类似的警报** 文本框。要指定单一的警报，单击下拉箭头，并单击列表中的警报名称。要指定多个警报，使用通配符，在文本框中输入安全隐患名称。使用 ?替代名称中的单个字符，以及使用 * 替代名称中的字符串。例如：使用 W32/* 将指定名称以 W32/ 开头的所有病毒。

测算病毒警报率的时间跨度

要指定测算安全隐患警报率的时间跨度，如：每小时或每天，单击下拉箭头并选择时间跨度。

显示警报历史

1. 在 Sophos Enterprise Console 中，打开 **工具** 菜单，并选择 **查看报告**。
2. 在 **报告** 对话框中的下拉菜单里，选择 **病毒历史**。
3. 在 **配置** 标签页中，您可以选择以下说明的选项。当您完成后，单击 **表** 标签页可以显示报告。

报告的时间跨度

在 **时间跨度** 文本框中，单击下拉箭头，并选择一个时间跨度。您既可以选择一个固定的时间，如：**上个月**，也可以选择 **自定义** 并在 **始于** 和 **止于** 框中指定您自己的时间跨度。

路径

选择 **计算机组** 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，报告会显示所有警报，以及每个警报出现的次数。您可以更改所显示的警报为下列类型之一：

全部（除受控程序之外）

仅限病毒／间谍软件

仅限可疑行为

仅限可疑文件

仅限防火墙

仅限广告软件／可能不想安装的应用程序

仅限受控程序

如果您想要报告，仅显示特定的警报或警报组的统计数据，请使用 **只显示类似的警报** 文本框。要指定单一的警报，单击下拉箭头，并单击列表中的警报名称。要指定多个警报，使用通配符，在文本框中输入安全隐患名称。使用 ?替代名称中的单个字符，以及使用 * 替代名称中的字符串。例如：使用 W32/* 将指定名称以 W32/ 开头的所有病毒。

排序

依照默认值，警报详情是按照 **警报名称** 排序的。不过，报告也可以按照 **计算机名称**，计算机的 **组名**，或者 **日期和时间**。

打印报告

要打印报告，单击报告顶端，工具栏中的 **打印** 图标。

将报告导出到文件

要将报告导出到文件

1. 单击单击报告顶端，工具栏中的 **导出** 图标。

2. 在 **导出报告** 对话框中，选择您想要将报告导出的文档或电子报表类型。有选项为：

   PDF (Acrobat)

   HTML

   Microsoft Excel

   Microsoft Word

   Rich Text Format (RTF)

   逗号分隔值格式(CSV)

   XML

3. 单击 **文件名** 浏览按钮选择路径。然后，输入文件名。单击 **确定**。

更改报告的页面格式

您可以更改报告的页面格式。比如，您可以横向（宽页）的格式呈现报告。

1. 单击单击报告顶端，工具栏中的页面格式图标。

2. 在 **页面设置** 对话框中，指定页面大小，打印方向和页边距等。单击 **确定**。报告将会按照页面设置的格式呈现。

当您打印或导出报告时，也会使用该页面设置。

20 别的用户怎样使用 Enterprise Console？

只有 **Sophos Console Administrators** 组的成员才能使用 Enterprise Console。

如果您想要让别的用户使用 Enterprise Console，请使用 Windows 工具将该用户添加到 Sophos Console Administrators 组中。

21 怎样开启或关闭发送报告至 Sophos？

您可以选择允许 Sophos Enterprise Console 每周向 Sophos 报告已管理的计算机的数量，以及有关操作系统类型和版本，所使用的 Sophos 产品的信息。Sophos 将利用这些信息来提供更好的技术支持服务，以及进一步了解客户使用 Sophos 产品的情况。任何向 Sophos 报告的有关您的计算机的信息，都不会确定个人身份，以及确定具体的计算机。Sophos 不会利用向 Sophos 报告的信息来确定您的公司，除非您向我们提供了您的 EM 下载用户名和／或电子邮件地址。

在安装或更新控制台时，您有机会在 Sophos Enterprise Console 安装向导中，选择启用发送报告至 Sophos 选项。

在安装之后，如果您想要开启或关闭向 Sophos 发送报告，请按照以下说明做：

1. 在 **工具** 菜单中，选择 **配置**，然后单击 发送报告至 Sophos。
2. 会出现 **发送报告至 Sophos** 对话框。

   如果您想要发送报告至 Sophos，请阅读协议，并选择 **我同意** 勾选框，如果您同意协议中的条款。

如果您想要启用 Sophos 客户支持可以直接与您联系，如：出现操作系统或版本问题时，请输入您的 EM 下载用户名和／或电子邮件地址。

如果您愿意报告这些信息，但是又想匿名，那么，您可以不必提供用户名或电子邮件地址。

如果您想禁用发送报告至 Sophos， 请取消勾选 **我同意** 勾选框。

3. 单击 **确定**。

22 排疑解难

本节将说明怎样处理在使用 Enterprise Console 时可能出现的问题。

- 无法保护在未指派文件夹中的计算机
- Sophos Anti-Virus 安装失败
- 计算机未被更新
- 防病毒设置在 Mac 计算机上不起作用
- 防病毒设置在 Linux 计算机上不起作用
- 未遵照策略的 Linux 计算机
- 读写扫描设置不起作用
- 在 Windows 2000 或以后的计算机中出现未预期的新扫描
- 连接和超时问题
- 不能检测广告软件／可能不想安装的应用程序
- 部分检测到项目
- 频繁发出有关可能不想安装的应用程序的警报
- 清除失败
- 弥补病毒造成的破坏
- 弥补可能不想安装的应用程序造成的破坏

- 技术支持

无法保护在未指派文件夹中的计算机

未指派文件夹只是用来放置尚未归入组中的计算机。将计算机放置到某个组中之前，您是无法为它们提供保护的。

Sophos Anti-Virus 安装失败

如果保护计算机向导在计算机中安装 Sophos Anti-Virus 失败，原因可能如下：

- Enterprise Console 不知道计算机运行的是哪种操作系统。这可能是因为在查找计算机时，您没有以“域名\用户”的格式输入用户名。
- 该计算机上运行了防火墙（这种情况通常出现在 Windows XP SP2 和 Windows Vista 计算机上）。
- 计算机上的“简单文件共享”没有关闭。

要了解防病毒软件和防火墙软件的安装要求的完整列表，请参见 *Sophos Endpoint Security and Control 网络安装指南*。

计算机未被更新

如果计算机中有未及时更新的防病毒软件，会有一个时钟图标出现在**状态**页中的 **更新情况** 栏中。旁边的文字，说明是该计算机已有多长时间没有及时更新了。

计算机可能由于以下两个原因之一，而未及时更新：

- 该计算机从服务器获取更新文件失败。
- 供更新所用的服务器中不是最新的 Sophos 软件。

本节将告诉您诊断问题和及时更新计算机。

1. 选择您要在其中查找未及时更新的计算机的组。

2. 在 **状态** 页中，单击 **更新情况** 栏将计算机按照更新情况排序。
3. 单击 **更新详情** 标签，并查看**主服务器** 栏。在该栏中会向您显示各计算机从中更新的目录。
4. 现在，查看从某一特定目录中更新的所有计算机。

   如果其中有一些计算机已及时更新，而另外一些却没有，那么，是个别的计算机有问题。选择它们，右击并选择 **现在更新计算机**。

   如果所有的计算机都未及时更新，那么，可能是供更新的目录有问题。单击工具栏中的 **Libraries** 图标。在 EM Library 控制台中，单击库的名称（在左手边的窗格板中），然后，单击 **Central Installations**。请选择您怀疑未及时更新的目录。单击右键，然后选择 **Update CID**。然后，回到 Enterprise Console 中，选择未及时更新的计算机，右击并选择 **现在更新计算机**。

防病毒设置在 Mac 计算机上不起作用

某些防病毒设置无法被应用到 Mac 计算机上。在这种情况下，在设置页面中会出现警告标志。

您可以使用 Sophos Update Manager 在 Mac 计算机上更改防病毒设置，Sophos Update Manager 是随 Sophos Anti-Virus for Mac 提供的一个工具软件。要打开 Sophos Update Manager，请在 Mac OS X 计算机的 **Finder** 窗口中，浏览找到 Sophos Anti-Virus:ESOSX 文件夹。双击 **Sophos Update Manager**。要了解更多详情，请参见 Sophos Update Manager Help 文件。

防病毒设置在 Linux 或 UNIX 计算机上不起作用

某些防病毒设置无法被应用到 Linux 或 UNIX 计算机上。在这种情况下，在设置页面中会出现警告标志。

您可以按照 Sophos Anti-Virus for Linux 用户手册中的说明，使

用 savconfig 和 savscan 命令，更改 Linux 计算机上的防病毒设置。您可以按照 Sophos Anti-Virus for UNIX 用户手册中的说明，使用 savscan 命令，更改 UNIX 计算机上的防病毒设置。

未遵照策略的 Linux 或 UNIX 计算机

如果您在CID中使用的是联合配置文件，并且该文件中的配置值与策略冲突，那么，计算机会显示为“未遵照策略”。

选择 **遵照策略** 选项只会使计算机暂时与策略一致，直到重新应用基于CID的配置为止。

要解决这个问题，请查看联合配置文件，并且在可能的情况下，用基于控制台的配置替换它。

读写扫描设置不起作用

在 Windows NT/95/98/Me 计算机中，更改读写扫描设置页面中的某些设置后，不起作用。在相应的页面中会出现警告标志。

在这些情况下，您在计划扫描设置页面中，所作的设置会同时应用于计划扫描和读写扫描中。这是因为早期的 Windows 版本的 Sophos Anti-Virus 的设计。

在 Windows 2000 或以后的计算机中出现未预期的新扫描

如果您查看在 Windows 2000 或以后的计算机中的本地 Sophos Anti-Virus，您也许会看到有一个新的“可用扫描”列示出来，即使用户还没有创建新扫描。

这个新扫描实际上是您已经从控制台上，设置了的计划扫描。您不应该删除它。

连接和超时问题

如果 Enterprise Console 和联网计算机之间的通讯变慢，或者计算机不响应，则可能有连接问题。

请查看 Sophos 网络通讯报告，该报告提供计算机和 Enterprise Console 之间的通讯现状的概览。要查看该报告，请到出现问题的计算机中。在任务栏中，单击 **开始** 按钮，选择 **所有程序|Sophos|Sophos Anti-Virus**，然后，单击 **查看 Sophos 网络通讯报告**。

报告会显示可能出现问题的地方，如果已经检测到了问题，则会提供解决措施。

不能检测广告软件／可能不想安装的应用程序

如果不能检测广告软件／其它可能不想安装的应用程序(PUA)，您应该检查：

- 是否启用了检测可能不想安装的应用程序的功能。请参见扫描广告软件／可能不想安装的应用程序。
- 要检测可能不想安装的应用程序的计算机，是否为 Windows 2000 或以后，并且运行了 Sophos Anti-Virus 6 或以后的计算机。

部分检测到项目

Sophos Anti-Virus 可能会报告某个项目（如：特洛伊木马，或者，可能不想安装的应用程序）被 "部分地检测到"。这说明 Sophos Anti-Virus 没有找到该应用程序的所有组件。

要找到其它组件，您需要对被涉及的计算机做完整系统扫描。在运行 Sophos Anti-Virus 7 for Windows 2000/XP/2003/Vista 的计算机上，您可以通过选择计算机，右击并选择 **完整系统扫描**。您也可以通过设置针对广告软件，和其它可能不想安装的应用程序的计划扫描，来实现。

如果该应用程序还是不能够被完全检测到，则可能是因为：

- 您的访问权限不足。
- 计算机中的某些包含着该应用程序组件的驱动器，或文件夹，被排除在了扫描之外。

如果是后一种情况，请检查从扫描中排除的项目的列表。如果有项目出现在列表中，请从列表中删除这些项目，然后，再次扫描您的计算机。

Sophos Anti-Virus 可能无法完全检测或删除，将组件安装到网络驱动器中的广告软件，和其它可能不想安装的应用程序。

要寻求建议，请联系 Sophos 技术支持。

频繁发出有关可能不想安装的应用程序的警报

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，包括对同一个应用程序发出多重报告。

出现这种情况的原因是，某些类型的可能不想安装的应用程序会“监控”文件，试图频繁地访问各种文件。如果您启用了读写扫描，Sophos Anti-Virus 则会检测每一个文件的访问，并因此发出警报。

您应该按照以下说明做：

- 禁用针对广告软件／可能不想安装的应用程序的读写扫描。您可以使用计划扫描来替代。
- 批准使用应用程序（假如您想要在计算机上运行该应用程序）。
- 清除计算机，删除您没有批准的应用程序。

清除失败

如果 Sophos Anti-Virus 清除项目失败（“清除失败”），原因可能如下：

- 它没有找到多组件项目中的所有组件。请对计算机运行一次完整系统扫描，以找到其它组件。

- 某些包含着项目组件的驱动器，或文件夹，被排除在了扫描之外。请检查从扫描中排除的项目。如果有项目出现在列表中，请从列表中删除这些项目。
- 您的访问权限不足。
- 它无法清除该类型的项目。
- 它发现的是病毒碎片，而非确切的病毒。
- 该项目在写保护的软盘上，或者在光盘上。
- 该项目在写保护的 NTFS 卷上（Windows 2000 或以后）。

弥补病毒造成的破坏

清除可以将病毒从计算机中删除，但并不总是能够弥补病毒所造成的破坏。

有些病毒并不会造成破坏。另一些病毒则可能以各种方式更改或损毁数据，并且令人难以觉察。要处理这种情况，您应该：

- 在 **帮助** 菜单中，单击 **查看项目信息**。您将会被连接到 Sophos 网站中，您可以在那里阅读病毒分析。
- 使用备份的，或者原始的程序拷贝，替换被感染过的程序。如果您之前没有做这样的备份，请立即制作或获取一份，以备将来遭到病毒感染时之需。

有时，您可以从被病毒损坏的磁盘上恢复数据。Sophos 可以提供一些工具软件，修复某些病毒造成的损害。请联系 Sophos 技术支持寻求建议。

弥补可能不想安装的应用程序造成的破坏

清除可以将不想安装的应用程序删除，但并不总是能够弥补应用程序所造成的破坏。

有些应用程序会更改操作系统的设置，如：更改您的因特网的连接设置。Sophos Anti-Virus 不能够总是恢复所有的设置。例如，某应用程序更改了浏览器的主页，而 Sophos Anti-Virus 不

可能知道之前所设置的浏览器主页是什么。

有些应用程序会安装一些实用程序，如：.dll 或.ocx 文件等，到您的计算机上。如果某个实用程序是无害的（也就是说，它不具有可能不想安装的应用程序的那些特点），如：某个语言库，并且不是不想安装的应用程序中不可缺少的部分，那么，Sophos Anti-Virus 可能不会将其检测为不想安装的应用程序的一部分。在这种情况下，清除将不会从您的计算机中将文件删除。

有时某个应用程序，如：广告软件，是您打算安装的软件中的一部分，并且是运行该程序所要求的。如果您删除了该应用程序，则该软件会停止在您的计算机上运行。

您应该：

- 在 **帮助** 菜单中，单击 **查看项目信息**。您将会被连接到 Sophos 网站中，您可以在那里阅读应用程序分析。
- 使用备份恢复您的系统设置，或者您所安装的软件。如果您之前没有做这样的备份，请立即制作一份，以备将来之需。

要了解更多的有关弥补广告软件／可能不想安装的应用程序造成的破坏的信息或建议，请联系 Sophos 技术支持。

技术支持

欲获技术支持，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

23 用语表

A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z

-A-

Active Directory 同步化

Sophos Enterprise Console 组与 Active Directory 容器的单向同步化。

回页首

-B-

病毒

通过将自身附着在其它程序上，并复制自身，在计算机之间和网络中传播的程序。

回页首

-D-

逗号分隔值格式(CSV)

是逗号分界格式(comma-delimited format)的另一个名称，它是每一个数据都用逗号分隔开的一种数据文件格式。这是一种将数据从一个应用程序转移到另一个应用程序时，普遍使用的文件格式，因为大多数的数据库系统，都可以导入和导出逗号分隔值格式的数据。例如，.csv 文件可以被导入

Microsoft Excel 作进一步的分析。

回页首

-E-

恶意软件

是故意编写出来破坏和干扰计算机系统的软件，如：病毒，蠕虫，特洛伊木马，或间谍软件。

回页首

-G-

广告软件

是显示广告的软件 — 诸如弹出消息等，它会影响用户的工作效率和计算机系统的运行效率。

回页首

-J-

间谍软件

通过隐蔽，欺骗，或劝诱等方式，将自身安装到用户的计算机上，并且未经用户的许可或知晓，将计算机上的信息发送给第三方的程序。间谍软件包括击键记录程序，后门特洛伊木马，密码窃取程序，以及 Botnet 蠕虫，这些软件会造成公司数据失窃，财务损失，以及网络破坏等。

回页首

-K-

可能不想安装的应用程序(PUA)

一种并非恶意软件，但是普遍认为，不适合用于绝大多数公司网络的软件。可能不想安装的应用程序执行显示广告，追踪网页访问情况，或更改计算机的配置等，诸如此类的操作。它们包括诸如广告软件，拨号软件，远程控制工具，以及黑客软件等，范围广泛的软件程序。

可疑行为

通常是来自恶意软件的行为，应用程序所展示的这些行为，在其出现是，尚未被确认是恶意的。

可疑文件

是指具有某些恶意软件共有的特征，但是又不足以确定为新出现恶意软件的文件（例如：含有恶意软件通常会使用的动态解压缩代码的文件）。

回页首

-S-

受控程序

是指并非安全隐患的，正当合法的应用程序，但是您认为该应用程序不适合在办公环境中使用。受控应用程序包括：游戏，即时消息(IM)客户端，语音IP电话(VoIP)客户端，数字影像软件，媒体播放器，浏览器插件，等等。

回页首

-T-

同步化点

是某个 Enterprise Console 组，它指向 Active Directory 中的某个容器（或子树）。

回页首

-W-

网络访问控制(NAC)

能够限制未经批准的，未遵照策略的，或者感染了病毒的计算机访问网络资源，从而降低安全隐患的一种系统。

未确定的病毒

识别特征尚未确定的未知的病毒。

回页首

-Y-

已同步化的组

是从 Active Directory 中导入的，同步化点的子组。

应用程序控制

Sophos Anti-Virus 的一项功能，它使您能够根据公司的政策，阻断或批准执行正当合法的应用程序。

运行时行为分析

通过执行“可疑行为检测”和“缓冲区溢出检测”等功能，动态地分析运行在计算机系统中的程序的行为。

回页首

-Z-

指标面板

是提供网络安全状态“一览图”的用户界面。

主机入侵防范系统 (HIPS)

是用于防范可疑文件，未被确定的病毒，以及可疑行为入侵计算机的一种安全技术。

回页首

索引

A

E

H

M

N

P

S