SOPHOS

Cybersecurity made simple.

Sophos Enterprise Console 帮助

产品版本号： 5.5

内容

1 关于 Sophos Enterprise Console

Sophos Enterprise Console 是独立的、自动化控制台，它管理和更新运行 Windows、Mac OS X、Linux 和 UNIX 操作系统的计算机上，以及 VMware vShield 虚拟环境中的 Sophos 安全软件。

Enterprise Console 使您能够：

- 保护您的网络免受恶意软件、风险的文件类型和网站、恶意网络数据流，以及广告软件和其他可能不需要的应用程序的攻击。
- 控制用户可以浏览的网站，进一步保护网络免遭恶意软件的侵害，以及防止用户浏览不合适的网站。
- 控制哪些应用程序可以在网络中运行。
- 管理端点计算机上的客户端防火墙保护。
- 评估计算机遗漏的补丁。
- 减少从端点计算机意外丢失数据，例如：无意中传输的敏感数据。
- 防止用户在端点计算机上使用未经批准的外部存储设备和无线网络连接技术。
- 防止用户重新配置，禁用，或者，卸载 Sophos 安全软件。

注释
上述的有些功能没有包含在全部的用户授权使用许可协议中。如果您想要使用它们，您可能需要更改您的用户授权使用许可协议。有关可用的许可证的详细信息，请参阅 www.sophos.com/zh-cn/products/enduser-protection-suites/how-to-buy.aspx 和 www.sophos.com/zh-cn/products/server-security/how-to-buy.aspx。

2 Sophos Enterprise Console 界面指南

2.1 用户界面布局

Enterprise Console 用户界面由以下区域组成：

工具栏

工具栏中包含使用和配置您的 Sophos 安全软件时，所需要的最常用命令的快捷按钮。

要了解更多信息，请参见工具栏按钮 （第 2 页）。

Dashboard

指标面板 为您提供网络安全状态的“一览图”。

要了解更多信息，请参见指标面板 （第 3 页）。

计算机列表

计算机列表显示在右下方。它包括两个视图：

- 终结点 视图，会显示在左下方的 组 窗格板中所选择的组中的计算机。要了解更多信息，请参见浏览端点视图 （第 5 页）。
- 更新管理器 视图，会显示安装了 Sophos Update Manager 的计算机。要了解更多信息，请参见浏览更新管理器视图 （第 8 页）。

2.2 工具栏按钮

以下表格将说明工具栏按钮。有些工具栏按钮只在特定的情况下可以使用。例如，用于安装防病毒和防火墙软件的 保护 按钮，只有在 端点 视图的 组 窗格板中选择了一组计算机时，才可以使用。

工具栏按钮	描述	说明
	发现计算机	搜索联网计算机，并将它们添加到控制台。 要了解更多信息，请参见发现网络中的计算机 （第 29 页）。
	创建组	创建新的计算机组： 要了解更多信息，请参见创建组 （第 21 页）。
	查看/编辑 NAC 策略	打开在 策略 窗格板中选择的策略，以便进行编辑。 要了解更多信息，请参见编辑策略 （第 27 页）。

工具栏按钮	描述	说明
	保护	安装防病毒和防火墙软件到在计算机列表中所选择的计算机上。 要了解更多信息，请参见自动保护计算机 （第 39 页）。
	端点计算机	在计算机列表中转换到 端点 视图。 端点 视图中会显示在 Groups 窗格板中所选择的组中的计算机。 要了解更多信息，请参见浏览端点视图 （第 5 页）。
	更新管理器	在计算机列表中转换到 更新管理器 视图。 更新管理器 视图中会显示安装了 Sophos Update Manager 的计算机。 要了解更多信息，请参见浏览更新管理器视图 （第 8 页）。
	指标面板	显示或隐藏 指标面板。 指标面板 为您提供网络安全状态的“一览图”。 要了解更多信息，请参见指标面板 （第 3 页）。
	报告	启动 报告管理器，使您能够生成有关您的网络中的警报和事件的报告。 要了解更多信息，请参见生成报告 （第 171 页）。
	Sophos Central	将转到 Sophos Central。 有关 Sophos Central 的信息，请参阅知识库文章 119598。有关迁移到 Sophos Central 的信息，请参阅知识库文章 122264。
	Sophos Mobile	Sophos Mobile URL 完成配置后，会打开 Sophos Mobile 的 Web 控制台。这是针对移动设备（如智能手机和平板电脑）的设备管理解决方案，可以帮助您管理应用和安全设置。 要了解更多信息，请参见配置 Sophos Mobile URL （第 37 页）。

2.3 指标面板

指标面板 包含以下部分：

指标面板	描述
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 部分中的链接。
更新文件	此部分显示更新管理器的状态。

指标面板	描述
具有警报的计算机	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 • 广告软件和其它可能不想安装的应用程序 要查看具有未处理的警报的已管理的计算机的列表，请单击标题：具有警报的计算机。
超过事件限制级别的计算机	此部分显示在最近 7 天中，超过事件限制级别的计算机的数量。 要查看具有设备控制事件，数据控制事件，受控程序事件，或防火墙事件的计算机列表，请单击 超过事件限制级别的计算机 部分中的链接。 注释 根据您的用户授权使用许可协议，一些事件类型可能不会显示。
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，请单击标题：策略。
保护	此部分显示 Sophos Endpoint Security and Control 或 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，请单击标题：保护。
错误	此部分显示具有未处理的扫描，更新，或防火墙错误的受管理的计算机的数量或百分比。 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，请单击标题：错误。

2.4 安全状态图标

以下表格说明在指标面板和 Enterprise Console 状态栏中出现的安全状态图标的含义。

安全状态图标	描述
	正常 受影响的计算机的数量低于警告级指标。
	警告 已超过警告级指标。
	紧要 已超过紧要级指标。

指标面板健康图标

指标面板 健康图标会出现在指标面板的右上角。它指标面板中特定安全领域的状态。

指标面板 健康图标，显示某个面板图标的最高程度的安全状态，它们是：

- 只要有一个图标的指标超过警告级，指标面板健康图标就会从 正常 变为 警告。
- 只要有一个图标的指标超过了紧要级，指标面板健康图标就会从 警告 变为 紧要。

网络健康图标

网络健康图标出现在 Enterprise Console 状态栏的右边。它显示您的网络的总体安全状态。

网络健康图标，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的图标的指标超过了警告级，网络综合健康图标就会从 正常 变为 警告。
- 只要有一个 指标面板 的图标超过了紧要级，网络综合健康图标就会从 警告 变为 紧要。

当您首次安装或更新 Enterprise Console 时，指标面板 会使用默认的警告和紧要级设置。要配置您自己的警告和紧要级，请参见指标面板 （第 3 页）。

您还可以设置电子邮件警报，当 指标面板 中的图标超过了“警告级”或“紧要级”时，可以向您所选择的收件人寄送警报。要了解操作指导，请参见设置网络状态电子邮件警报 （第 159 页）。

2.5 浏览端点视图

计算机列表

在 端点 视图中，计算机列表会显示在 组 窗格板中所选择的组中的计算机。

此视图包含数个标签页。状态 标签页，显示计算机是否受到读写扫描的保护，它们是否遵照各自的组策略，那些功能处于启用状态，以及软件是否已及时更新。此标签页还显示是否有任何警报发出。其它的标签页会就不同的主题给出更详细的信息。

您可以使用 查看 过滤器筛选计算机列表。在 查看 下拉列表中，选择您想要查看的哪些计算机。例如，选择 具有潜在问题的计算机，以显示有问题的计算机。

您也可以通过使用检测到的项目名称，如恶意软件、可能不想安装的应用程序或可疑文件来筛选计算机列表。要了解更多信息，请参见通过检测到的项目名称筛选计算机 （第 7 页）。

您可以按照“计算机名”，“计算机描述”，或者， IP 地址来搜索计算机。要了解更多信息，请参见在 Enterprise Console 中查找计算机 （第 8 页）。

要了解显示在计算机列表中的图标的含义，请参见计算机列表图标 （第 6 页）。

您可以复制或打印显示在计算机列表中的信息。有关详细信息，请参阅从计算机列表复制数据 （第 181 页）和从计算机列表打印数据 （第 181 页）。

组窗格板

在 组 窗格中，您可以创建组

并将联网计算机放置其中。您可以自己创建组，也可以从 Active Directory 容器中导入组（所导入

的组可以包含计算机，也可以不包含计算机。），并将这些组用作为 Enterprise Console 计算机组。

要了解更多信息，请参见创建和使用组 （第 20 页）。

未指派 组

用于尚未指派给您创建的组的计算机。

策略窗格板

在 策略 窗格中，您可以创建和配置应用到计算机组中的策略。要了解更多信息，请参见创建和使用策略 （第 23 页）。

2.6 计算机列表图标

警报

图标	释意
	出现在 状态 标签页里的 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 状态 标签页里的 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。 • 出现错误。 出现在 策略遵照 栏中的黄色警告标志表明，该计算机没有使用与它所在的组中的其它计算机使用的策略相同的策略。

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。

1. 病毒和间谍软件警报
2. 可疑行为警报
3. 可疑文件警报
4. 广告软件和可能不想安装的应用程序 (PUA) 警报
5. 软件应用程序错误（例如，安装错误）

如果同一个计算机收到数个带有相同优先级的警报，那么最近收到的警报将显示在计算机列表上。

保护被禁用，或者没有及时更新

在 状态 标签页的功能状态栏中出现的灰色的功能图标，表明该功能是禁用的。例如，读写扫描 栏中出现灰色的盾牌


，表明读写扫描没有激活。

在 更新情况 栏中出现时钟图标


，表明软件未及时更新。

计算机状态

图标	释意
	带有绿色连接器图案的计算机标识说明，计算机已受到 Enterprise Console 的管理。
	带有黄色沙漏的计算机标识说明，安全软件的安装处于挂起状态。
	带有黄色下拉箭头的计算机标识说明，安全软件的安装正在进行中。
	灰色的计算机标识说明，该计算机尚未受 Enterprise Console 管理。
	带有红色十字叉图案的计算机标识表明，该通常受 Enterprise Console 管理的该计算机已经断开了与网络的连接。（没有被管理的与网络断开了连接的计算机，不会被显示。）

2.7 通过检测到的项目名称筛选计算机

您可以通过检测到的项目名称，如恶意软件、可能不想安装的应用程序或可疑软件，筛选计算机列表。您可以通过配置筛选器为“受...影响的托管计算机”进行筛选。筛选器和其他计算机列表筛选器一起显示在视图下拉菜单列表中。

若要配置筛选器，请执行以下操作：

1. 在工具菜单中，单击配置筛选器。
2. 在配置计算机筛选器对话框中，输入您想筛选的已j检测项目的名称。您可以在网络的以下位置查找检测到的项目名称：
   - 计算机列表视图，警报和错误详情选项卡，检测到的项目栏。

     请注意如果计算机有多个检测到的项目，那么已检测的项目栏会仅显示最新最优先的项目，且该项目可能不是您筛选的项目。
   - 处置警报和错误对话框。若要打开对话框，在群组窗格中的计算机列表或一组计算机中选择一个计算机或多个计算机，右击并单击处置警报和错误。
   - 计算机详细信息对话框。若要打开该对话框，双击受影响的计算机。然后拖动滚动条找到未处置的警报和错误部分。
   - 报告（例如，警报摘要或按照项目名称给出警报和事件）。若要打开报告管理器，在工具菜单中，单击管理报告。

   您可以使用通配符。使用 ？ 替代单个字符，以及使用 * 替代字符串。例如，如果您输入 "Mal*"，然后应用筛选，计算机列表视图将会显示受到名字以 "Mal" 开头的恶意软件感染的计算机，例如 "Mal/Conficker-A" 和 "Mal/Packer"。

2.8 在 Enterprise Console 中查找计算机

您可以按照以下标准，在 Enterprise Console 中搜索计算机：

- 计算机名称
- 计算机描述
- IP 地址

1. 要查找计算机，请按照以下步骤之一做：
   - 同时按 CTRL 和 F 键。
   - 在 编辑 菜单中，单击 查找计算机。
   - 在计算机列表上单击，右击，然后，单击 查找计算机。
2. 在 查找 对话框中，输入搜索标准。
   查找内容 栏中的内容是不区分大小写的。已假定在结尾处使用了通配符。
   您可以使用通配符 * 和 ？
   例如：

搜索标准	搜索结果
UKlapt	将查找所有以 “uklapt” 开始的字串，如： UKlaptop-011，UKlaptop-155，uklaptop132。
Ukla*	将查找所有以 “ukla” 开始的字串。此处的通配符，并无必要， 因为它已假定为存在；搜索结果将会与前一个示例的结果相同，即： UKlaptop-011，UKlaptop-155，uklaptop132。
*ukla	将查找所有包含 “ukla” 的字串，如： UKlaptop-011，055uklax，056-Dukla-sales。
Ukl*t	将查找所有以 “ukl” 开始，包含一个 “t”，以任何字符结尾的字串，如：UKlaptop-011，ukLite55。
?klap	将查找所有以任何单个字符开始，紧接着是 “klap”，并且以任何字符结尾的字串，如：UKlaptop-011，uklapland33。
UKl??t	将查找所有以 “ukl” 开始，紧接着两个字符，接着是一个 “t”，以任何字符结尾的字串，如：UKlaptop-011，uklist101。

2.9 浏览更新管理器视图

计算机列表

在 更新管理器 视图中，您可以设置自动从 Sophos 网站更新 Sophos 安全软件，并查看各更新管理器的状态和详情。

计算机列表会显示安装了 Sophos Update Manager 的计算机。

软件预订

在 软件预订 窗格中，您可以创建或编辑软件预订，指定为在何种操作系统上使用的 Sophos 下载哪个版本的端点计算机软件。

3 开始使用 Sophos Enterprise Console

这是在您安装了 Enterprise Console 和完成了下载安全软件向导之后，需要执行的，保护网络的任务的概览。要了解更多有关使用 Enterprise Console 的信息，请参见提及的其它材料和章节。

我们建议您参见 Sophos Enterprise ConsoleSophos Enterprise Console 策略设置指南，寻求有关使用和管理 Sophos 安全软件的最佳使用方式的建议。Sophos 技术文档发布在 http://www.sophos.com/zh-cn/support/documentation 中。

如果您尚未完成下载安全软件向导，请参见运行下载安全软件向导 （第 57 页）。

要保护您的网络，请按照以下步骤做：

1. 创建组。

   您可以自己一个一个地创建组，也可以从 Active Directory 容器中导入组（所导入的组可以包含计算机，也可以不包含计算机。），并将这些组用作为 Enterprise Console 计算机组。

   如果您想要导入 Active Directory 容器，请参见从 Active Directory 中导入容器和计算机（第 29 页）。我们建议首先导入没有计算机的 Active Directory 容器，然后，指定组策略到组中，然后添加计算机到组中，例如，通过同步化 Active Directory 计算机的方式。

   有关手动创建组的信息，请参见创建和使用组 （第 20 页）。
2. 设置策略。

   Enterprise Console 具有一组默认的策略，它们对保护您的网络非常重要。您可以立即就使用默认的 更新 和 防病毒和 HIPS 策略。要配置防火墙策略，请运行 防火墙策略 向导。请参阅设置基本的防火墙策略 （第 95 页）。
3. 发现网络中的计算机，并将它们添加到控制台。

   如果您已经在步骤1中导入了 Active Directory 容器和计算机，那么，您需要进行任何操作。否则，请参见发现网络中的计算机 （第 29 页）。
4. 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 组中将计算机拖放到其它组中时，会有一个向导启动，帮助您保护计算机。请参阅自动保护计算机 （第 39 页）。

   - 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 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，请参见使用同步化自动保护计算机 （第 35 页）。
5. 检查计算机是否受到保护

   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。要了解更多信息，请参见检查网络是否受到保护 （第 40 页）。
6. 清除计算机。

   如果在您的网络中检测到了病毒，不想安装的应用程序，或其他项目，或可能不想安装的应用程序，请按照立即清除计算机 （第 46 页）中的说明，清除受影响的计算机。

附加的保护选项

默认情况下，Sophos Endpoint Security and Control 会检测恶意软件（病毒、木马、蠕虫、间谍软件）、广告软件和其他可能不想安装的应用程序、可疑行为和恶意网络数据流。它也会阻断已知含有

恶意软件的网站，并且会扫描从该网站下载的内容。可以按创建和使用组 （第 20 页）中的说明，启用更多安全和产品功能。

管理权限选项

您可以在 Enterprise Console 中设置不同的角色，添加权限到角色中，然后指派 Windows 用户和组到角色中。包括了 Sophos Full Administrators Windows 组的 System Administrator 角色具有完全的权限，不需要设置。要了解更多信息，请参见管理角色和子领域 （第 12 页）。

您可以将 IT 领域分成多个子领域，并将Enterprise Console的计算机组指派给这些子领域。这样您可以通过指派 Windows 用户和组给子领域，从而控制对子领域的访问。默认子领域包含包括未指派组在内的所有 Enterprise Console 组。要了解更多有关子领域的信息，请参见管理角色和子领域 （第 12 页）。

提示
查看如何设置和使用 Enterprise Console 的视频（SophosGlobalSupport YouTube 频道，Sophos Enduser Protection 部分）。

4 设置 Sophos Enterprise Console

4.1 管理角色和子领域

重要提示
如果您已使用基于角色的管理，您必须具有 基于角色的管理 权限，才能设置角色和子领域。包括了 Sophos Full Administrators Windows 组的 System Administrator 角色具有完全的权限，不需要设置。有关详细信息，请参阅什么是预置角色？ （第 13 页）和各种权限有权处理什么任务？ （第 16 页）。

通过设置角色，添加权限到该角色，然后，指派 Windows 用户和组到角色中，您可以设置基于角色的控制台访问。例如，提供桌面支持的工程师可以更新或清除计算机，但是，不能配置策略 — 这是系统管理员所负责的工作。

要开启 Enterprise Console，用户必须是 Sophos Console Administrators 组的成员，并且至少被指派给一个 Enterprise Console 角色和一个子领域。Sophos Full Administrators 组的成员具备完全访问 Enterprise Console 的权限。

注释
如果您想允许用户使用远程的或附加的 Enterprise Console，请参见其它用户怎样使用 Sophos Enterprise Console？ （第 20 页）。

您可以创建自己的角色，也可以使用预设的角色。

您可以指派某用户为各种角色，方法是添加该单个的用户或添加该用户所属的 Windows 组到各种角色中。

如果某用户没有在控制台中执行某特定任务的权限，他们仍然可以查看相关任务的配置设置。您指派给任何角色的用户，将无法打开 Enterprise Console。

您还可以限制用户在某些计算机和计算机组中执行操作。您可以将 IT 领域分成多个子领域，并将 Enterprise Console 的计算机组指派给这些子领域。这样您可以通过指派 Windows 用户和组给子领域，从而控制对子领域的访问。默认 子领域包含包括 未指派 组在内的所有 Enterprise Console 组。

用户只能查看它们被指派的子领域。如果用户被指派到多个子领域，他们可以选择查看哪个子领域，一次只能查看一个子领域。在 Enterprise Console 中开启的子领域是 活动子领域。用户不能编辑应用于他们的活动子领域之外的策略。

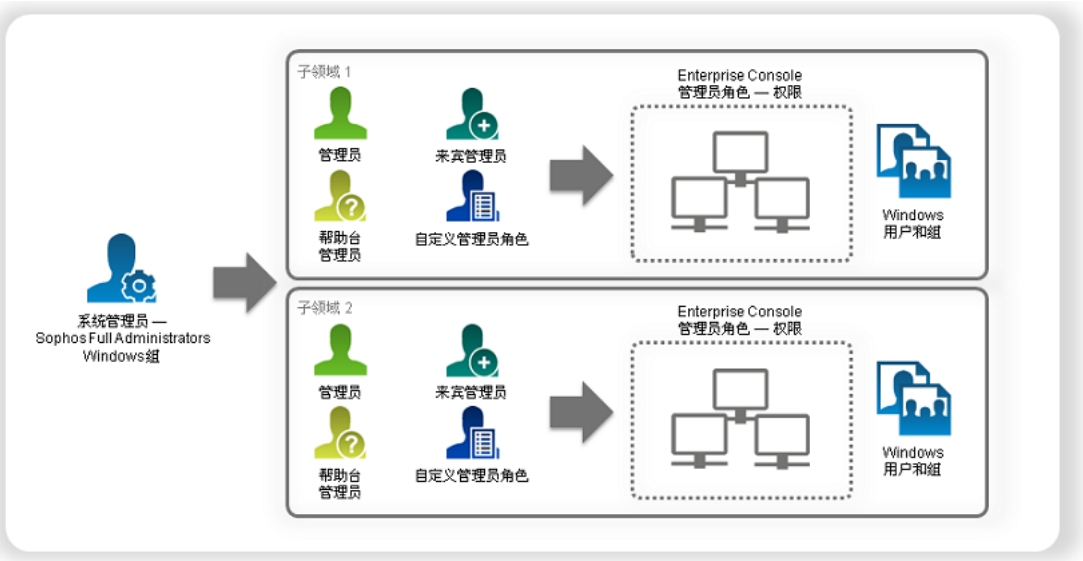


图 1: 关于角色和子领域

4.1.1 什么是预置角色?

在 Enterprise Console 中有四个预设的角色:

角色	描述
系统管理员	预置角色，具有管理网络中的 Sophos 安全软件，以及管理 Enterprise Console 中的角色的所有权限。系统管理员角色不能被编辑或删除。
管理员	具有权限管理网络中的 Sophos 安全软件，但是不能管理 Enterprise Console 中的角色的预设的角色。管理员角色可以被重新命名，编辑，或删除。
帮助台	只具有调整权限，例如，清除或更新计算机，的预设的角色。桌面帮助角色可以被重新命名，编辑，或删除。
来宾	只具有读访问 Enterprise Console 权限的预设的角色。来宾角色可以被重新命名，编辑，或删除。

您可以编辑管理员，桌面帮助，以及来宾角色，或按照 创建角色 （第 13 页） 中的说明创建您自己的角色。

4.1.2 创建角色

如果您已经使用基于角色的管理，您必须具备 基于角色的管理 权限，才能执行此任务。要了解更多信息，请参见管理角色和子领域 （第 12 页）。

1. 在 工具 菜单中，单击 管理角色和子领域。
2. 在 管理角色和子领域 对话框的 管理角色 标签页中，单击 创建。
   会出现 创建角色 对话框。
3. 在 名称 栏中，输入角色名称。
4. 在 权限 窗格板中，选择您想指派给角色的一个或多个角色的权限，并单击 添加。

5. 在 用户和组 窗格板中，单击 添加。
6. 在 选择用户或组 对话框，输入想要指派给角色的 Windows 用户或组的名称。单击 确定。

如果需要，按照步骤 5 和 6 中的说明，指定更多的用户或组给角色。

4.1.3 删除角色

如果您已经使用基于角色的管理，您必须具备 基于角色的管理 权限，才能执行此任务。要了解更多信息，请参见管理角色和子领域 （第 12 页）。

1. 在 工具 菜单中，单击 管理角色和子领域。
2. 在 管理角色和子领域 对话框的 管理角色 标签页中，选择您想要删除的角色，并单击 删除。

注释
预设的 System Administrator 角色不能被删除。

4.1.4 编辑角色

如果您已经使用基于角色的管理，您必须具备 基于角色的管理 权限，才能执行此任务。要了解更多信息，请参见管理角色和子领域 （第 12 页）。

1. 在 工具 菜单中，单击 管理角色和子领域。
2. 在 管理角色和子领域 对话框的 管理角色 标签页中，选择您想要编辑的角色，并单击 编辑。
   会出现 编辑角色 对话框。
3. 在 权限 窗格板中，将权限指派给角色，或者，如需要，删除现有的权限。
4. 在 用户和组 窗格板中，添加 Windows 用户或组到角色，或者，如需要，删除现有的用户或组。

4.1.5 赋予权限给角色

如果您已经使用基于角色的管理，您必须具备 基于角色的管理 权限，才能执行此任务。要了解更多信息，请参见管理角色和子领域 （第 12 页）。

1. 在 工具 菜单中，单击 管理角色和子领域。
2. 在 管理角色和子领域 对话框的 管理角色 标签页中，选择您想要添加权限的角色，并单击 编辑。
   会出现 编辑角色 对话框。
3. 在 权限 窗格板的 可用权限 列表中，选择权限，并单击 添加。

4.1.6 创建子领域

如果您已经使用基于角色的管理，您必须具备 基于角色的管理 权限，才能执行此任务。要了解更多信息，请参见管理角色和子领域 （第 12 页）。

1. 在 工具 菜单中，单击 管理角色和子领域。
2. 在 管理角色和子领域 对话框的 管理子领域 标签页中，单击 创建。
   会出现 创建子领域 对话框。
3. 在 子领域名称 栏中，输入子领域名称。
4. 在 Enterprise Console 组 窗格中，选择您想要添加子领域的组。
5. 在 用户和组 窗格中，单击 添加，以添加 Windows 用户或组到子领域中。

4.1.7 更改活动子领域

如果您指派了多个子领域，您可以选择当开启 Enterprise Console 时，您想要查看哪个子领域，或者，在 Enterprise Console 中您可以在子领域之间转换。

您一次只能查看一个子领域。在您更改了活动子领域后，带有新的子领域的 Enterprise Console 会被重载。

要更改活动子领域：

1. 在 工具 菜单，单击 选择活动子领域。
2. 在 选择活动子领域 对话框中，选择您想要打开的子领域，并单击 确定。

4.1.8 编辑子领域

如果您已经使用基于角色的管理，您必须具备 基于角色的管理 权限，才能执行此任务。要了解更多信息，请参见管理角色和子领域 （第 12 页）。

1. 在 工具 菜单中，单击 管理角色和子领域。
2. 在 管理角色和子领域 对话框的 管理子领域 标签页中，选择您想要编辑的子领域，并单击 编辑。
3. 在 编辑子领域 对话框中，更改子领域的名称，更改哪些 Enterprise Console 组包括在子领域中，或者，如需要，更改哪些 Windows 用户和组具有访问子领域的权限。单击 确定。

4.1.9 复制子领域

如果您已经使用基于角色的管理，您必须具备 基于角色的管理 权限，才能执行此任务。要了解更多信息，请参见管理角色和子领域 （第 12 页）。

1. 在 工具 菜单中，单击 管理角色和子领域。
2. 在 管理角色和子领域 对话框的 管理子领域 标签页中，选择您想要复制的子领域，并单击 复制。子领域的拷贝会出现在子领域列表中。
3. 选择刚创建的子领域，并单击 编辑。重新命名子领域。如果您想要，可以更改包括在子领域和/或具有访问该子领域的权限的 Windows 用户和组中的组。

4.1.10 删除子领域

如果您已经使用基于角色的管理，您必须具备 基于角色的管理 权限，才能执行此任务。要了解更多信息，请参见管理角色和子领域 （第 12 页）。

1. 在 工具 菜单中，单击 管理角色和子领域。
2. 在 管理角色和子领域 对话框的 管理子领域 标签页中，选择您想要删除的子领域，并单击 删除。

   您不能删除默认的子领域。

4.1.11 查看用户或组的角色和子领域

要查看已指派给 Windows 用户或组的角色和子领域：

1. 在 工具 菜单中，单击 管理角色和子领域。
2. 在 管理角色和子领域 对话框的 用户和组查看 标签页中，单击 选择用户或组 按钮。

3. 在 选择用户或组 对话框中，选择您想要查看角色和子领域的用户或组，并单击 确定。

4.1.12 各种权限有权处理什么任务？

注释
根据您的用户授权使用许可协议，一些权限可能不可用。

权限	任务
Auditing	启用审核，禁用审核
计算机搜索，保护和组	开始搜索，停止搜索，为 Network 搜索，IP 范围搜索，以及 Active Directory 搜索查找各个域 从 Active Directory 导入计算机和组；从 Active Directory 导入组 从文件中导入计算机 删除计算机 保护计算机 与 Active Directory 同步化组 更改组的同步化属性 删除组同步化 移动计算机 创建组 重命名组 移动组 删除组 指派策略到组
自定义数据控制	创建数据控制规则 编辑数据控制规则 复制数据控制规则 删除数据控制规则 从数据控制扫描中排除文件 创建内容控制列表 编辑内容控制列表 复制内容控制列表 删除内容控制列表
数据控制事件	显示数据控制事件查看器 在计算机详情中显示数据控制事件

权限	任务
策略设置 — 防病毒和 HIPS	创建防病毒和 HIPS 策略 复制防病毒和 HIPS 策略 重新命名防病毒和 HIPS 策略 编辑防病毒和 HIPS 策略 恢复默认的防病毒和 HIPS 设置 删除防病毒和 HIPS 策略 从安全隐患控制列表中添加或删除条目
策略设置 — 应用程序控制	创建应用程序控制策略 复制应用程序控制策略 重新命名应用程序控制策略 编辑应用程序控制策略 恢复默认的应用程序控制设置 删除应用程序控制策略
策略设置 — 数据控制	创建数据控制策略 复制数据控制策略 重新命名数据控制策略 编辑数据控制策略 恢复默认的数据控制设置 删除数据控制策略
策略设置 — 设备控制	创建设备控制策略 复制设备控制策略 重新命名设备控制策略 编辑设备控制策略 恢复默认的设备控制设置 删除设备控制策略
策略设置 — 防火墙	创建防火墙策略 复制防火墙策略 重新命名防火墙策略 编辑防火墙策略 恢复默认的防火墙设置 删除防火墙策略

权限	任务
策略设置 — 补丁	创建补丁策略 复制补丁策略 重新命名补丁策略 编辑补丁策略 恢复默认的补丁设置 删除补丁策略
策略设置 - 介入防范	创建介入防范策略 复制介入防范策略 重命名介入防范策略 编辑介入防范策略 恢复默认的介入防范设置 删除介入防范策略
策略设置 — 更新	创建更新策略 复制更新策略 重新命名更新策略 编辑更新策略 恢复默认的更新设置 删除更新策略 创建软件预订 编辑软件预订 重新命名软件预订 复制软件预订 删除软件预订 配置更新管理器
策略设置 — 网页控制	创建网页控制策略 复制网页控制策略 重新命名网页控制策略 编辑网页控制策略 重置默认的网页控制策略 删除网页控制策略

权限	任务
策略设置 - 漏洞防御	创建漏洞防御策略 复制漏洞防御策略 重新命名漏洞防御策略 编辑漏洞防御策略 添加攻击缓解排除项目 删除攻击缓解排除项目 重置漏洞防御策略 删除漏洞防御策略
调整 — 清除	清除已检测到的项目 确认已知警报 确认已知错误
调整 — 更新和扫描	立即更新计算机 运行完整扫描计算机 使计算机遵照组策略 使更新管理器遵照配置 指示更新管理器立即更新
报告配置	创建，编辑，或删除报告
基于角色的管理	创建角色 重新命名角色 删除角色 修改角色的权限 添加用户或组到角色 从角色中删除用户或组 子领域管理：创建子领域；重新命名子领域；删除子领域；添加子领域根组；删除子领域根组；添加用户或组到子领域；从子领域中删除用户或组
系统配置	修改 SMTP 服务器设置；测试 SMTP 服务器设置；修改电子邮件警报收件人 配置指标面板的警告和紧要级别 配置报告：配置数据库警报清空；设置在报告中出现的公司名称 配置发送报告至 Sophos：启用或禁用发送报告至 Sophos；修改用户名；修改电子邮件联系地址 配置固定版本软件包的使用

权限	任务
网页事件	显示网页事件查看器 在计算机详情对话框中显示网页事件

4.1.13 其它用户怎样使用 Sophos Enterprise Console?

Sophos Full Administrators 组的成员具备完全访问 Enterprise Console 的权限。

您可以允许别的用户使用 Enterprise Console。要打开 Enterprise Console，用户必须：

- 是 Sophos Console Administrators 组中的成员。
- 被指派给至少一个 Enterprise Console 角色。
- 被指派给至少一个 Enterprise Console 子领域。

如果您想要指派某个用户给 Sophos Console Administrators 组，请使用 Windows 工具将该用户添加到组中。

要指派某个用户给某个 Enterprise Console 角色或子领域，请在 工具 菜单中，单击 管理角色和子领域。要了解更多有关角色和子领域的信息，请参见管理角色和子领域 （第 12 页）。

要使用远程或附加的 Enterprise Console，用户必须：

- 是 Enterprise Console Management Server 所安装的那台服务器上的 Sophos Console Administrators 组中的成员。
- 是 Enterprise Console Management Server 所安装的那台服务器上的 Distributed COM Users 组中的成员。（Distributed COM Users 组位于Active Directory Users and Computers 工具的 Builtin 容器中）。
- 被指派给至少一个 Enterprise Console 角色。
- 被指派给至少一个 Enterprise Console 子领域。

4.2 创建和使用组

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。

4.2.1 组是干什么的?

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。
- 针对不同的组，使用不同的防病毒和 HIPS 策略，应用程序控制策略，防火墙策略，以及其它策略。
- 更轻松地管理计算机。

提示
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。

4.2.2 什么是组？

组

是包括多个计算机的文件夹。

您可以自己创建组，也可以从 Active Directory 容器中导入组（所导入的组可以包含计算机，也可以不包含计算机。），并将这些组用作为 Enterprise Console 计算机组。您还可以设置与 Active Directory 同步化，这样在 Active Directory 中新添的计算机和容器，以及其它更改都会被自动复制到 Enterprise Console 中。

各个组都有针对更新，防病毒和 HIPS 保护，防火墙保护，等等的设置。在组中的所有计算机应该通常使用这些设置，它们被称为“策略”。

组可以包含子组。

4.2.3 什么是未指派组？

未指派 组是 Enterprise Console 放置尚未放置到组中的计算机的文件夹。

您不能：

- 应用策略到 未指派 组。
- 在 未指派 组中创建子组。
- 移动或删除 未指派 组。

4.2.4 创建组

如果您使用基于角色的管理，您必须具备 计算机搜索，保护和组 权限，才能执行此任务。要了解更多信息，请参见管理角色和子领域 （第 12 页）。

要创建新的计算机组：

1. 在 端点 视图的 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. 在工具栏上，单击 创建组 图标。
   一个“新组”即被添加到列表中，该组的名称会高亮显示。
3. 为该组输入名称。

更新、防病毒和 HIPS、应用程序控制、防火墙、补丁、数据控制、设备控制、介入防范以及网页控制策略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。请参阅 编辑策略 （第 27 页） 或者 指派策略到组 （第 27 页）。

注释
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。

4.2.5 添加计算机到组

如果您使用基于角色的管理，您必须具备 计算机搜索，保护和组 权限，才能执行此任务。要了解更多信息，请参见管理角色和子领域 （第 12 页）。

1. 选择您要添加到组中的计算机。比如，单击 未指派 组，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 组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。

4.2.6 从组中删除计算机

如果您使用基于角色的管理，您必须具备 计算机搜索，保护和组 权限，才能执行此任务。要了解更多信息，请参见管理角色和子领域 （第 12 页）。

您可以从组中删除计算机，例如，您可以删除已不再在网络中的计算机的条目。

重要提示

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。

如果已从之前版本的 Enterprise Console 升级，并且有计算机使用以前的 Enterprise Console 管理的全盘加密功能加密，请勿从控制台中删除这些计算机。加密恢复在此情况中可能不适用。

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 发现计算机 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。

4.2.7 剪切和粘贴组

如果您使用基于角色的管理，您必须具备 计算机搜索，保护和组 权限，才能执行此任务。要了解更多信息，请参见管理角色和子领域 （第 12 页）。

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。

4.2.8 删除组

如果您使用基于角色的管理，您必须具备 计算机搜索，保护和组 权限，才能执行此任务。要了解更多信息，请参见管理角色和子领域 （第 12 页）。

任何在被删除的组中的计算机，都将被置入 未指派 组。

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。

4.2.9 重命名组

如果您使用基于角色的管理，您必须具备 计算机搜索，保护和组 权限，才能执行此任务。要了解更多信息，请参见管理角色和子领域 （第 12 页）。

1. 选择您要重新命名的组。
2. 右击并选择 重新命名。

4.2.10 查看组采用的策略

要查看哪些策略已被指派到了组中：

- 在组窗格中，右键单击该组。选择查看/编辑组策略详细信息。

  在组详细信息对话框中，您可以查看当前使用的策略。

4.3 创建和使用策略

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。

当您安装 Enterprise Console 时，安装过程会为您创建默认的策略，提供基本的安全保护。这些策略会应用到您创建的任何组中。您可以编辑默认策略，或者，创建新的策略。

注释
您的用户授权使用许可协议中没有包括的功能，将不可用。

您可以为各种类型创建多个策略。

您可以应用同一策略到多个组。

4.3.1 有哪些策略可用？

注释
您的用户授权使用许可协议中没有包括的功能，将不可用。

- 更新 策略指定计算机怎样更新安全软件。
- 防病毒和 HIPS 策略指定安全软件怎样扫描计算机中的病毒，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，可疑行为和可疑文件；以及怎样清除它们。
- 应用程序控制 策略指定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 策略指定防火墙怎样保护计算机。
- 数据控制 策略指定根据文件内容，文件名，或文件类型来监控或限制文件传输的规则。
- 设备控制 策略指定哪些存储和网络设备不能允许用于工作站计算机上。
- 补丁 策略指定是否启用补丁评估，以及对计算机进行补丁评估的频率。
- 介入防范 策略会指定密码，允许经过授权的端点计算机用户重新配置，禁用，或者，卸载 Sophos 安全软件。

- 网页控制 策略会指定用户可以浏览的网站。对于被配置为“阻断”或“警告”的网站，会向用户发送通告。
- 漏洞防御策略指定哪些应用程序、功能和进程将受到保护，例如保护文档文件免受勒索软件（CryptoGuard）侵害或保护Web浏览器的重要功能（安全浏览）。

4.3.2 什么是默认策略？

当您安装 Enterprise Console 时，会为您创建默认的策略。

注释
您的用户授权使用许可协议中没有包括的功能，将不可用。

更新策略

Enterprise Console 全新安装中的默认策略提供：

- 每隔 10 分钟自动从默认的路径更新计算机。默认的路径是一个 UNC 共享路径：\\<计算机名>\SophosUpdate，这里的“计算机名”是更新管理器安装所在的计算机。

防病毒和 HIPS 策略

Enterprise Console 全新安装中的默认防病毒和 HIPS 策略提供：

- 读写扫描病毒、特洛伊木马、蠕虫、间谍软件、广告软件和其它可能不想安装的应用程序（但是不包括可疑文件）。
- 检测到缓冲区溢出、在系统中运行的程序的恶意和可疑行为，以及恶意网络数据流。
- 阻断访问已知的带有恶意软件的网站。
- 扫描从互联网中下载的内容。
- 安全警报会出现在受影响的计算机的桌面上，并添加到事件日志中。

更多有关在 Enterprise Console 全新安装中的防病毒和 HIPS 策略的默认设置的完整列表的信息，请转到 知识库文章 27267。

应用程序控制策略

依照默认值，所有的应用程序和应用程序类型都会被允许。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。在网络中使用防火墙策略之前，您应该配置它允许您想要使用的应用程序。请参阅设置基本的防火墙策略 （第 95 页）。

要了解默认的防火墙设置的完整列表，请参见 知识库文章 57757。

数据控制策略

依照默认值，数据控制是关闭的，并且没有指定任何规则监控或限制因特网中的，或向存储设备进行的文件传输。

设备控制策略

依照默认值，设备控制是关闭的，所有的设备都会被允许。

补丁策略

依照默认值，补丁评估是关闭的。对于新建的补丁策略，补丁评估是开启。一旦开启了补丁评估，计算机会每天被评估一次（除非您更改了补丁评估的频率），查看是否有遗漏的补丁。

介入防范策略

依照默认值，介入防范是关闭的，并且没有指定密码，该密码是允许经过授权的端点用户重新配置，禁用或卸载 Sophos 安全软件时所需要的。

网页控制策略

依照默认值，网页控制是关闭的，用户可以访问任何网站，只要它们没有被 Enterprise Console 的 Web 保护限制。请参阅Web 保护 （第 85 页）。

漏洞防御策略

默认情况下，漏洞防御已开启。请参阅漏洞防御策略 （第 151 页）。

4.3.3 需要创建自己的策略吗？

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

默认的策略提供的是基本的安全保护，但是，如果要使用诸如“网络访问控制”或“应用程序控制”等功能，您需要创建新的策略或更改默认策略。

注释
当您更改默认策略时，更改将应用到您创建的所有策略中。

注释
如果您使用基于角色的管理，那么，您必须具有相应的 策略设置 权限，才能创建或编辑策略。例如，您必须具备 策略设置 - 防病毒和 HIPS 的权限，才能创建或编辑防病毒和 HIPS 策略。要了解更多信息，请参见管理角色和子领域 （第 12 页）。

更新策略

默认的更新策略会终结点计算机每隔 10 分钟从默认的软件分发 UNC 共享中，检查建议的预订是否有更新文件。要更改预订、更新路径和其它设置，请按照 配置更新策略 （第 58 页） 中的说明配置更新策略。

Anti-virus and 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，要启用检测其它不想要/可疑的应用程序或行为，您可能需要创建新的策略，或者，更改默认策略。请参阅防病毒和 HIPS 策略 （第 67 页）。

Application control

要定义和阻断未经批准的应用程序，请按照 应用程序控制策略 （第 120 页） 中的说明配置应用程序控制策略。

防火墙策略

要允许真实可信的应用程序访问网络，请按照 防火墙策略 （第 94 页） 中的说明配置防火墙策略。

Data control

依照默认值，数据控制是关闭的。要防止数据泄露，请按照 数据控制策略 （第 123 页） 中的说明配置数据控制策略。

Device control

依照默认值，设备控制是关闭的。要限制所允许的硬件设备，请按照 设备控制策略 （第 135 页） 中的说明配置设备控制策略。

补丁

依照默认值，补丁评估是关闭的。对于新建的补丁策略，补丁评估是开启。一旦开启了补丁评估，计算机会每天被评估一次（除非您更改了补丁评估的频率），查看是否有遗漏的补丁。要开启或关闭补丁评估，或者要更改补丁评估的频率，请按照 补丁策略 （第 143 页） 中的说明配置补丁策略。

Tamper protection

依照默认值，介入防范是关闭的。要启用介入防范，请按照 介入防范策略 （第 140 页） 中的说明配置介入防范。

Web control

依照默认值，网页控制是关闭的。要开启网页控制，以及配置网页控制策略，请参见网页控制策略（第 145 页）。

漏洞防御

默认情况下，漏洞防御已开启。要配置漏洞防御，请参见漏洞防御策略 （第 151 页）。

4.3.4 创建策略

如果您使用基于角色的管理，您必须具有相应的 策略设置 权限，才能执行此任务。要了解更多信息，请参见管理角色和子领域 （第 12 页）。

要创建策略：

1. 在 终结点 视图的 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。
   “新策略”将被添加到列表中，该组的名称会高亮显示。
2. 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。

   要了解怎样选择设置的有关操作指导，请参见配置相关策略的部分。

至此，您已经创建了可以应用到组的策略。

4.3.5 指派策略到组

如果您使用基于角色的管理，您必须具备 计算机搜索，保护和组 权限，才能执行此任务。要了解更多信息，请参见管理角色和子领域 （第 12 页）。

1. 在 策略 窗格板中，高亮选择将要指派的策略。
2. 单击该策略，将其拖曳到您想应用该策略的计算机组中。在出现提示时，确认您想要继续。

注释
或者，您可以右击某个组，然后，选择 查看/编辑组策略详情。接着，您就可以从下拉菜单中为组选择所要应用的策略。

4.3.6 编辑策略

如果您使用基于角色的管理，那么：

- 您必须具备相应的 策略设置 权限，才能执行此任务。
- 您不能编辑应用于您的活动子领域之外的策略。

要了解更多信息，请参阅 管理角色和子领域 （第 12 页）。

要编辑一个或多个计算机组的策略：

1. 在 策略 窗格板中，双击您想要编辑的策略。

2. 编辑设置。

要了解怎样配置不同策略的操作指导，请参见相关的部分。

4.3.7 重命名策略

如果您使用基于角色的管理，那么：

- 您必须具备相应的 策略设置 权限，才能执行此任务。
- 您不能重命名应用于您的活动子领域之外的策略。

要了解更多信息，请参见管理角色和子领域 （第 12 页）。

注释
您不能够重新命名“默认的”策略。

要重命名策略：

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。

4.3.8 删除策略

如果您使用基于角色的管理，那么：

- 您必须具备相应的 策略设置 权限，才能执行此任务。
- 您不能删除应用于您的活动子领域之外的策略。

要了解更多信息，请参见管理角色和子领域 （第 12 页）。

注释
您不能够删除“默认的”策略。

要删除策略：

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。

4.3.9 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：

- 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。
  会出现采用了该策略的组的列表。

4.3.10 检查计算机是否使用组策略

您可以检查是否某个组中的所有计算机都遵照该组的策略。

1. 选择您要检查的组。
2. 在计算机列表的 终结点 视图中的 状态 标签页中，查看 策略遵照 栏。

- 如果您看到“策略相同”的字样，说明该计算机遵照它所在的组的策略。
- 如果您看到黄色的警告标志和“策略不同”的字样，说明该计算机使用的策略与它所在的组中的其它计算机使用的策略不同。

要了解更多有关计算机的安全功能的状态，以及应用到计算机上的策略的详细信息，请参见 终结点视图中相应的标签页，例如，防病毒详情 标签页。

如果您想要计算机遵照它们所在的组的策略，请参见使计算机采用组策略 （第 29 页）。

4.3.11 使计算机采用组策略

如果您使用基于角色的管理，您必须具备 调整 - 更新和扫描 权限，才能执行此任务。要了解更多信息，请参见管理角色和子领域 （第 12 页）。

如果您发现计算机没有遵照它所在的组的策略，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。

4.4 发现网络中的计算机

要管理 Enterprise Console 中的计算机，您首先必须将它们添加到 Enterprise Console 中。您可以使用“发现计算机”功能，通过选择不同的选项，能够搜索联网的计算机，并将它们添加到 Enterprise Console 中。有以下几个选项：

- 从 Active Directory 中导入容器和计算机 （第 29 页）
- 通过 Active Directory 发现计算机 （第 30 页）
- 通过浏览网络发现计算机 （第 30 页）
- 通过 IP 范围发现计算机 （第 30 页）
- 从文件中导入计算机 （第 31 页）

如果您使用基于角色的管理，您必须具备 计算机搜索，保护和组 权限，才能添加计算机到控制台中。要了解更多信息，请参见管理角色和子领域 （第 12 页）。

4.4.1 从 Active Directory 中导入容器和计算机

如果您使用基于角色的管理，您必须具备 计算机搜索，保护和组 权限，才能执行此任务。要了解更多信息，请参见管理角色和子领域 （第 12 页）。

从 Active Directory 中导入组可以获取 Active Directory 容器结构，将该它复制到 Enterprise Console 中作为计算机组的结构。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 组中。

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 发现计算机 图标。
2. 在 发现新计算机 对话框的 从 Active Directory 导入 窗格中，选择 导入 并单击 确定。

   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。

从 Active Directory 导入向导 会启动。

3. 请按照向导中的操作指导做。在被询问选择导入什么时，根据您想要导入什么，选择 计算机和容器 或 仅限容器。

在您从 Active Directory 中导入容器之后，请应用策略到组中。请参阅有哪些策略可用？ （第 23 页）。

在您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。要了解操作指导，请参见与 Active Directory 同步化 （第 32 页）。

4.4.2 通过 Active Directory 发现计算机

如果您使用基于角色的管理，您必须具备 计算机搜索，保护和组 权限，才能执行此任务。要了解更多信息，请参见管理角色和子领域 （第 12 页）。

您可以使用 Active Directory 发现查找网络中的计算机，并将它们添加到 未指派 组中。

1. 在工具栏中，单击 发现计算机 图标。
2. 在 发现新计算机 对话框中，选择 通过 Active Directory 发现 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 发现计算机 对话框中，选择您想搜索的域。单击 确定。
5. 单击 未指派 组，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。

4.4.3 通过浏览网络发现计算机

如果您使用基于角色的管理，您必须具备 计算机搜索，保护和组 权限，才能执行此任务。要了解更多信息，请参见管理角色和子领域 （第 12 页）。

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 组中。

1. 在工具栏中，单击 发现计算机 图标。
2. 在 发现计算机 对话框中，选择 在网络中发现 并单击 确定。
3. 在 认证资料 对话框中，输入具备足够权限获得计算机信息的帐户的用户名和密码。

   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。

   如果您所要操作的计算机无需帐户详情即可访问，那么，您可以跳过此步骤。
4. 在 发现计算机 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 组，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。

4.4.4 通过 IP 范围发现计算机

如果您使用基于角色的管理，您必须具备 计算机搜索，保护和组 权限，才能执行此任务。要了解更多信息，请参见管理角色和子领域 （第 12 页）。

您可以使用 IP 范围发现网络中的计算机，并将它们添加到 未指派 组中。

注释
您无法使用 IPV6 地址。

1. 在工具栏中，单击 发现计算机 图标。
2. 在 发现计算机 对话框中，选择 通过 IP 范围发现 并单击 确定。
3. 在 认证资料 对话框中，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。
   在 SNMP 窗格板中，您可以输入 SNMP 团体名。
4. 在 发现计算机 对话框中，输入 IP 范围起点 和 IP 范围终点。单击 确定。
5. 单击 未指派 组，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。

4.4.5 从文件中导入计算机

如果您使用基于角色的管理，您必须具备 计算机搜索，保护和组 权限，才能执行此任务。要了解更多信息，请参见管理角色和子领域 （第 12 页）。

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。您可以按以下形式创建文件 ：

```
[GroupName1]
 Domain1|Windows7|ComputerName1
 Domain1|Windows2008ServerR2|ComputerName2
```

注释
您不一定非要指定计算机防置在哪个组中，如果您输入 [] （括号之间没有空格）作为组名，计算机将被放置在 未指派 组中。

有效的操作系统名称如下：
WindowsXP，Windows2003，WindowsVista，Windows7，WindowsServer2008，Windows2008ServerR2，Windows8，Windo
和 Unix。

域名和操作系统都是可选项。所以，也可能有以下形式：

```
[GroupName1]
 ComputerName1
```

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 组，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。

4.5 与 Active Directory 同步化

本节概述 Active Directory 同步化。

Active Directory 同步化能做什么？

与 Active Directory 同步化，您可以将 Enterprise Console 组与 Active Directory 容器同步化。在 Active Directory 中找到的新计算机和容器会被自动复制到 Enterprise Console 中。您还可以选择自动保护找到的 Windows 的工作站计算机。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。

注释
运行 Windows Server，Mac OS，Linux，或 UNIX 等操作系统的计算机不会自动受到保护。您必须手动保护这样的计算机。

在设置了同步化之后，您可以设置在今后的同步化中，向指定的收件人发送有关找到新的计算机和容器的电子邮件警报。如果您选择了自动保护已同步化的 Enterprise Console 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 同步化怎样工作？

在 Enterprise Console 中，您可以同时具有您自己管理的“普通的”，未同步化的组，以及与 Active Directory 同步化的组。

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 容器中所有计算机和子组都将被复制到 Enterprise Console 中，并被保持与 Active Directory 同步化。

注释
要了解更多有关同步化点的信息，请参见什么是同步化点？ （第 33 页）。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？ （第 33 页）。

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：

- 如果新的计算机添加到 Active Directory 容器中，那么，它同样会出现在 Enterprise Console 中。
- 如果某计算机从 Active Directory 中删除，或者被已移动到未同步化的容器中，那么，在 Enterprise Console 中该计算机会被移动到未指派组中。

  注释
  当某个计算机被移至未指派组中后，它将停止接收新的策略。

- 如果某个计算机从一个已同步化的容器中移至另一个已同步化的容器中，那么，在 Enterprise Console 中该计算机会从一个组中移至另一个组中。
- 如果某个计算机首次被同步化时，已经在 Enterprise Console 组中存在，那么，它会被从该组中移至与在 Active Directory 中的路径一致的已同步化的那个组中。

- 当某个计算机被移至策略不同的新组中时，新的策略会被发送给该计算机。

依照默认值，同步化每60分钟进行一次。如果需要，您可以更改该同步化进行的频率。

怎样运用同步化？

使哪些组与 Active Directory 同步化，以及设置多少同步化点，将由您来决定。请考虑，将要创建的组在同步化之后的大小，以便易于管理。您应该考虑到能够从容地部署软件，扫描和清除计算机。这对初始的部署尤其重要。

注释
如果有复杂的 Active Directory 结构，并想同步域本地组或嵌套的 Active Directory 组，请参阅知识库文章 122529 了解有关启用此功能的信息。

推荐的运用方式如下：

1. 使用 从 Active Directory 导入 功能，导入组结构（没有计算机）。要了解操作指导，请参见从 Active Directory 中导入容器和计算机 （第 29 页）。
2. 查看导入的组结构，并选择同步化点。
3. 设置组策略，并应用它们到组和子组。要了解操作指导，请参见创建策略 （第 27 页）和指派策略到组 （第 27 页）。
4. 与 Active Directory 同步化您选择的同步化点，一次进行一个同步化点。要了解操作指导，请参见与 Active Directory 同步化 （第 34 页）。

4.5.1 什么是同步化点？

同步化点 是一个指向 Active Directory 中的某个容器（或子树）的一个 Enterprise Console 组。同步化点可以容纳从 Active Directory 中导入的已同步化的组。

在 组 窗格板中，同步化点会显示如下：

您可以移动，重命名，或删除同步化点。您还可以更改策略和同步化策略，包括对同步化点的自动保护设置。

您不能在同步化点中创建或删除子组，或将其它组移动到同步化点中。您不能将计算机移至或移出同步化点。

4.5.2 什么是已同步化的组？

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

在 组 窗格板中，已同步化的组会显示如下：

您可以更改指派到已同步化的组中的策略。

您不能更改除了组策略以外的任何已同步化的组的设置。您不能重命名，移动，或删除已同步化的组。您不能将计算机或组移至或移出已同步化的组中。您不能在已同步化的组中创建或删除子组。您不能更改已同步化的组的同步化设置。

4.5.3 与 Active Directory 同步化

在执行此任务之前：

- 如果您使用基于角色的管理，那么，您必须具备 计算机搜索，保护和组 权限。要了解更多信息，请参见管理角色和子领域 （第 12 页）。
- 如果您想要自动保护同步化的组中的计算机，请确保您已经按照准备安装安全软件 （第 38 页）中的说明准备好了计算机。
- 如果有复杂的 Active Directory 结构，并想同步域本地组或嵌套的 Active Directory 组，请按知识库文章 122529.中所述启用此功能。

要与 Active Directory 同步化：

1. 选择将要作为同步化点的计算机组，单击鼠标右键，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，选择或创建一个，您想保持与 Active Directory 同步化（同步化点）的 Enterprise Console 组。单击 下一步。
4. 在 请选择一个 Active Directory 容器 对话框中，选择一个组将用来与之同步化的 Active Directory 容器。请输入容器的名称，（例如，LDAP://CN=Computers,DC=domain_name,DC=local），或者，单击 浏览 找到 Active Directory 中的该容器。单击 下一步。

   重要提示
   如果某个计算机存在于多个已同步化的 Active Directory 容器中，那么，它会出问题，会不断地在计算机和 Enterprise Console 之间交换消息。各个计算机应该只在 Enterprise Console 中列示一次。

5. 如果您想要自动保护 Windows 工作站计算机，请在 自动保护计算机 页面，勾选 自动安装 Sophos 安全软件 复选框，然后，选择您想要安装的软件。

   注释
   有关针对这些软件的系统要求的列表，请参见 Sophos 网站（http://www.sophos.com/en-us/products/all-system-requirements.aspx）中的系统要求页面。

   - 在计算机上安装 Firewall 之前，请确保您已配置了防火墙允许您想要使用的通讯流，应用程序，以及进程。依照默认值，防火墙会被启用，并会阻断所有可有可无的通讯流。请参阅防火墙策略 （第 94 页）。
   - 如果您想自动删除其它软件商的类似软件，请保留选择 第三方安全软件检测。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 38 页）。

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

   重要提示
   运行 Windows Server，Mac OS，Linux，或 UNIX 等操作系统的计算机不能被自动保护。您必须按照 Sophos Enterprise Console 高级安装指南中的说明，手动保护此类计算机。

注释
您稍后可以在 同步化属性 对话框中，启用或禁用自动保护。要了解操作指导，请参见查看和编辑同步化属性 （第 36 页）。

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。

注释
您稍后可以在 同步化属性 对话框中，更改同步化频率。要了解操作指导，请参见查看和编辑同步化属性 （第 36 页）。

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，请选中向导最后一页中的复选框。要了解操作指导，请参见设置 Active Directory 同步化电子邮件警报 （第 160 页）。

   要关闭向导，请单击 完成。

4.5.4 使用同步化自动保护计算机

在执行此任务之前：

- 如果您使用基于角色的管理，那么，您必须具备 计算机搜索，保护和组 权限。要了解更多信息，请参见管理角色和子领域 （第 12 页）。
- 请确保您已按照准备安装安全软件 （第 38 页）中的说明，准备好了计算机，能够自动安装安全软件。

在与 Active Directory 同步化的过程中发现的计算机中，运行 Windows 的计算机会获得自动保护。

重要提示
运行 Windows Server，Mac OS，Linux，或 UNIX 等操作系统的计算机不能被自动保护。您必须按照 Sophos Enterprise Console 高级安装指南中的说明，手动保护此类计算机。

您可以在设置同步化时（请参见与 Active Directory 同步化 （第 34 页）），或在稍后编辑同步化属性时，自动保护已同步化的组中的计算机。

以下的操作指导，说明怎样通过编辑同步化属性，来保护计算机。

1. 在 组 窗格中，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，勾选 自动安装 Sophos 安全软件 复选框，然后，选择您想要安装的软件。
   - 在计算机上安装 Firewall 之前，请确保您已配置了防火墙允许您想要使用的通讯流，应用程序，以及进程。依照默认值，防火墙会被启用，并会阻断所有可有可无的通讯流。请参阅防火墙策略 （第 94 页）。

- 如果您想自动删除其它软件商的类似软件，请保留选择 第三方安全软件检测。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 38 页）。

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。

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 安全软件复选框。

4.5.5 查看和编辑同步化属性

在执行此任务之前：

- 如果您使用基于角色的管理，那么，您必须具备 计算机搜索，保护和组 权限。要了解更多信息，请参见管理角色和子领域 （第 12 页）。
- 如果您想要自动保护同步化的组中的计算机，请确保您已经按照准备安装安全软件 （第 38 页）中的说明准备好了计算机。
- 如果有复杂的 Active Directory 结构，并想同步域本地组或嵌套的 Active Directory 组，请按知识库文章 122529.中所述启用此功能。

要查看和编辑同步化属性：

1. 在 组 窗格中，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。
   会出现 同步化属性 对话框。
2. 在 Active Directory 容器 栏，您可以看到组与之同步化的容器。如果您想要将组与不同的容器同步化，请删除同步化，然后，再次运行 与 Active Directory 同步化 向导。请参阅 开启或关闭同步化 （第 37 页） 和 与 Active Directory 同步化 （第 34 页）。
3. 在 同步化频率 栏中，设定同步化频率。默认值是60分钟。最小值是5分钟。
4. 如果您想要自动保护所有找到的新的 Windows 工作站，并遵照它们各自的组策略，请选择 自动安装 Sophos 安全软件。在 功能 下，已默认选择防病毒保护。如果想安装其它的 Sophos 安全软件，请选中相应的复选框。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。

注释
只有 Windows 工作站才能获得自动保护。运行 Windows Server，Mac OS，Linux，或 UNIX 等操作系统的计算机不能被自动保护。您必须按照 Sophos Enterprise Console 高级安装指南中的说明，手动保护此类计算机。

4.5.6 立即与 Active Directory 同步

在执行此任务之前：

- 如果您使用基于角色的管理，那么，您必须具备 计算机搜索，保护和组 权限。要了解更多信息，请参见管理角色和子领域 （第 12 页）。
- 如果您想要自动保护同步化的组中的计算机，请确保您已经按照准备安装安全软件 （第 38 页）中的说明准备好了计算机。
- 如果有复杂的 Active Directory 结构，并想同步域本地组或嵌套的 Active Directory 组，请按知识库文章 122529.中所述启用此功能。

您可以立即与 Active Directory 容器同步化 Enterprise Console 组（同步化点），不用等到计划中的下一次同步化。

要立即与 Active Directory 同步：

1. 在 组 窗格中，选择您想要与 Active Directory 同步化的组（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，进行相应的更改，然后，单击 确定。

4.5.7 开启或关闭同步化

在执行此任务之前：

- 如果您使用基于角色的管理，那么，您必须具备 计算机搜索，保护和组 权限。要了解更多信息，请参见管理角色和子领域 （第 12 页）。
- 如果您想要自动保护同步化的组中的计算机，请确保您已经按照准备安装安全软件 （第 38 页）中的说明准备好了计算机。
- 如果有复杂的 Active Directory 结构，并想同步域本地组或嵌套的 Active Directory 组，请按知识库文章 122529.中所述启用此功能。

要开启或关闭阻断“与 Active Directory 同步化”：

- 要开启同步化，请按照与 Active Directory 同步化 （第 34 页）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。

4.6 配置 Sophos Mobile URL

Sophos Mobile 是适用于诸如智能手机和平板电脑的移动设备管理解决方案。Sophos Mobile 通过管理应用程序和安全设置有助于保护企业数据的安全。

您可以通过单击 Sophos Mobile 工具栏按钮从 Enterprise Console 打开 Sophos Mobile Web 控制台。若要这样做，您首先需要配置 Sophos Mobile URL。

1. 在工具按钮中，单击配置 Sophos Mobile URL。
2. 在Sophos Mobile URL对话框中，输入 Sophos Mobile Web 控制台的 URL，并单击确定。

5 保护计算机

您可以按照以下方式安装 Sophos 安全保护软件：

- 要自动保护计算机，请使用 Enterprise Console（请参见自动保护计算机 （第 39 页））中提供的保护计算机向导。
- 或者，您可以通过与 Active Directory 同步化来自动保护计算机，请参见与 Active Directory 同步化 （第 32 页）。
- 要手动保护计算机，Enterprise Console 可以帮助找到所要求的软件，请参见手动查找保护计算机的安装程序 （第 40 页）。然后转到相应的计算机上，手动安装安全软件。

5.1 准备安装安全软件

在确保计算机满足总的系统要求的同时，在能够自动安装软件之前，您必须完成几个步骤。

注释
自动安装不能在 Mac，Linux，和 UNIX 计算机上进行。

如果您使用 Active Directory，那么，您可以通过“组策略对象” (GPO) 来准备计算机。如果您使用工作组，那么，您必须在本地配置计算机。

要了解操作指导，请参阅 Sophos 端点部署指南。要观看部署视频，请转到知识库文章 111180。

5.2 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，那么，在 保护计算机向导 中勾选 Third-Party Security Software Detection 选项之前，请按照以下说明做：

- 如果计算机使用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。
- 如果计算机正在运行其它软件商的防火墙或 HIPS 产品，请确保它已被关闭，或者已配置为允许运行 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。

注释
您必须从本地重新启动您从中删除了第三方防病毒软件的所有计算机。

注释
HitmanPro.Alert可能已作为独立产品或从Sophos Central中安装。在Sophos Enterprise Console应用本地管理之前，需要先删除HitmanPro.Alert。

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，在勾选 保护计算机向导中的 Third-Party Security Software Detection 之前，您需要修改配置文件：

注释
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。

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. 保存更改，并将 crt.cfg 保存在 data.zip 所在的同一个目录中。不要将 crt.cfg 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 Third-Party Security Software Detection，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。

5.3 自动保护计算机

在您从控制台中保护计算机之前：

- 在保护组中的计算机之前，您必须应用某个更新策略到该组。
- 请确保您已按照准备安装安全软件 （第 38 页）中的说明，准备好了计算机，能够自动安装安全软件。
- 如果您使用基于角色的管理，那么，您必须具备 计算机搜索，保护和组 权限，才能保护计算机。要了解更多信息，请参见管理角色和子领域 （第 12 页）。

自动安装不能在 Mac，Linux，和 UNIX 计算机上进行。请用手动安装代替。要了解具体的操作指导，请参见 Sophos Enterprise Console 高级安装指南。

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，请参阅 与 Active Directory 同步化 （第 32 页） 以及其它相关的主题。

要自动保护计算机：

1. 根据您想要保护的计算机是否已在计算机组中，按照以下说明之一做：
   - 如果您想要保护的计算机在 未指派 组中，请将该计算机拖放到其它某个组中。
   - 如果您想要保护的计算机已在某个计算机组中，请选择该计算机，单击鼠标右键，然后，单击保护计算机。

   保护计算机向导 会启动。请按照向导中的操作指导做。
2. 在 选择功能 页中，选择您想要的功能。

   注释
   有关针对这些功能的系统要求的列表，请参阅 Sophos 网站 (http://www.sophos.com/zh-cn/products/all-system-requirements) 中的系统要求页面。

   某些功能，包括防病毒保护总是会被选择，必须被安装。您还可以选择安装以下列示的功能：有些功能只有在您的用户授权使用许可协议中包含它们时，才会提供使用。

   - Firewall

     在计算机上安装防火墙之前，请确保您已配置了防火墙允许您想要使用的通讯流，应用程序，以及进程。依照默认值，防火墙会被启用，并会阻断所有可有可无的通讯流。请参阅防火墙策略 （第 94 页）。

- Patch
- Exploit Prevention, Sophos Clean

  这将防御勒索软件和漏洞攻击。如果您的许可证包括此功能，默认情况下它是选中的。

  注释
  如果您升级许可证并将 Exploit Prevention（和 Sophos Clean）包括在内，它不会在您已经在管理的计算机上自动安装。您需要重新保护计算机以安装该组件。

- Third-Party Security Software Detection

  如果您想自动删除其它软件商的类似软件，请保留选择 Third-Party Security Software Detection。第三方软件检测，仅卸载与您所要安装的产品的功能相同的那些产品。如果您需要删除其它软件商的更新工具，请参阅 删除第三方安全软件 （第 38 页）。

3. 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。安装过程的排疑解难（请参见 Sophos Endpoint Security and Control 安装失败 （第 184 页）），或者，在这些计算机上进行手动安装（请参见 Sophos Enterprise Console 高级安装指南）。单击 下一步。
4. 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。
   - 可以读取在 更新 策略中，所指定的主服务器的路径。请参阅配置更新服务器 （第 59 页）。

   注释
   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。

   如果计算机在同一 Active Directory 架构覆盖的不同的域中，那么，请在 Active Directory 中使用 Enterprise Administrator 帐户。

5.4 手动查找保护计算机的安装程序

如果 Enterprise Console 不能在某些计算机上自动安装防病毒、防火墙或补丁等功能，您可以实行手动安装。

要找到安装程序：

1. 在 查看 菜单中，单击 引导路径。
2. 在 引导路径 对话框中，对于每个软件预订，您将看到包含软件的安装程序的路径，以及支持该软件的操作平台和软件的版本。记录下您所需要的安装程序的路径。

要了解怎样在不同的操作系统上手动安装安全软件的信息，请参见 Sophos Enterprise Console 高级安装指南。

5.5 检查网络是否受到保护

要了解网络安全状态的“一览图”，请使用指标面板。有关详细信息，请参阅指标面板 （第 3 页）和配置指标面板 （第 41 页）。

您可以通过使用计算机列表和计算机列表过滤器，识别有问题的计算机。例如，您可以查看哪些计算机没有安装防火墙或补丁功能，或者，出现了需要注意的警报。有关详细信息，请参见检查计算机是否受到保护 （第 41 页）、检查计算机是否及时更新 （第 42 页）和查找有问题的计算机 （第 42 页）。

您还可以检查是否组中所有的计算机都遵照该组的策略，具体说明请见检查计算机是否使用组策略（第 28 页）。

5.5.1 配置指标面板

如果您使用基于角色的管理，那么，您必须具有 系统配置 权限，才能配置指标面板。要了解更多信息，请参见管理角色和子领域 （第 12 页）。

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，单击 配置指标面板。
2. 在 配置指标面板 对话框的 警告级 和 紧要级 文本框中，按照以下说明更改指标级别值。
   a) 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”。
   b) 在 发生事件的计算机 窗格板中，输入事件数，如果该数量的事件在7日之内发生，就会触发显示在指标面板中的警报。
   c) 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。

   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。

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。要了解操作指导，请参见设置警报和消息 （第 154 页）。

5.5.2 检查计算机是否受到保护

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。

注释
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. 在计算机列表中的 状态 标签页中，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，则防火墙是启用的。如果您看到灰色的防火墙图标和“否”字样，则防火墙是禁用的。
5. 如果您使用其它功能，如：应用程序控制，数据控制，或补丁，请检查相应的栏中的状态。

要了解有关怎样检查计算机是否及时更新的信息，请参见检查计算机是否及时更新 （第 42 页）。

要了解通过计算机列表筛选查找有问题的计算机的信息，请参见查找有问题的计算机 （第 42 页）。

5.5.3 检查计算机是否及时更新

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。

要检查计算机是否及时更新：

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. 在 状态 标签页中，查看 及时更新 栏，或者，转到 更新详情 标签页。
   - 如果您在 及时更新 栏中看到“是”字样，那么，该计算机已及时更新。
   - 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。

要了解更多有关更新诸如未及时更新的计算机的信息，请参见更新未及时更新的计算机 （第 65 页）。

5.5.4 查找有问题的计算机

要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：

1. 选择您要检查的计算机所在的组。
2. 在 查看 下拉列表中，选择您想要显示的计算机，例如，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，具有未处置的警报的计算机，或者，出现安装错误的计算机）。
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。
   任何保护有问题的计算机，都将被列示出来。

您也可以通过检测到的项目名称，如恶意软件、可能不想安装的应用程序或可疑软件，筛选计算机列表。要了解更多信息，请参见通过检测到的项目名称筛选计算机 （第 7 页）。

要了解处置保护问题的信息，请参见排疑解难 （第 182 页）部分的计算机没有运行读写扫描 （第 182 页）和其它主题。

5.6 处置警报和错误

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，警告图标会出现在端点 视图的 状态 标签页中。

有关警报图标的重要信息，请参见警报图标的含义 （第 43 页）。在本节的其他主题中，您可以找到针对这些警报的相关建议。

注释
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。要了解有关的信息，请参见检查网络是否受到保护 （第 40 页）。

要了解更多有关某个警报的详情，例如，检测到的项目的名称，请单击 警报和错误详情 标签页。

要了解有关更新管理器警报的信息，请参见监控更新管理器 （第 64 页）。

5.6.1 警报图标的含义

图标	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。 • 出现错误。 出现在 策略遵照 栏中的黄色警告标志表明，该计算机没有使用与它所在的组中的其它计算机使用的策略相同的策略。

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。

1. 病毒和间谍软件警报
2. 可疑行为警报
3. 可疑文件警报
4. 广告软件和可能不想安装的应用程序 (PUA) 警报
5. 软件应用程序错误（例如，安装错误）

5.6.2 处置检测到项目的警报

如果您使用基于角色的管理，您必须具备 调整 - 清除 权限，才能从控制台清除检测到的项目，或者清除警报。要了解更多信息，请参见管理角色和子领域 （第 12 页）。

要针对在控制台中显示的警报采取措施：

1. 在 端点 视图中，选择您想要查看警报的计算机。右击并选择 处置警报和错误。会出现 处置警报和错误 对话框。
2. 针对警报您可以采取的措施，取决于警报的清除状态。查看 清除状态 栏目，并决定您要采取什么措施。

提示
您可以单击栏标排序警报。例如，要按照清除状态排序警报，请单击 清除状态 栏标。

清除状态	描述和采取的措施
可清除	您可以删除该项目。要这样做，请勾选一个或多个警报，并单击 清除。
不能清除的安全隐患类型	检测到的这种类型的项目，如可疑文件、可疑行为或恶意网络数据流，无法在控制台中进行清理。您只能决定允许或阻断该项目。如果您不信任该项目，您可以将它发送给 Sophos 进行分析。要了解更多信息，请参见查找检测到的项目的信息 （第 44 页）。

清除状态	描述和采取的措施
不可清除	此项目无法通过控制台清除。要了解更多有关此项目的信息，以及您可以采取的措施，请参见查找检测到的项目的信息 （第 44 页）。
要求完整扫描	此项目可能可以清除，但是需要对端点计算机进行完整扫描，才能进行清除工作。要了解操作指导，请参见立即扫描计算机 （第 45 页）。
要求重新启动	该项目已部分地被删除，但是端点计算机需要重新启动，以完成清除工作。 注释 必须从本地，而不是从 Enterprise Console 中，重新启动端点计算机。
清除失败	该项目不能被删除。要求手动清除。要了解更多信息，请参见立即清除计算机（第 46 页）。
清除正在进行中（启动 <时间>）	清除正在进行。
清除超时（启动 <时间>）	清除已超时。该项目可能没有被清除。这可能发生在，例如，端点计算机与网络的连接断开，或网络繁忙时。您可以稍后在尝试清除项目。

如果您想要允许某个项目，请参见批准广告软件和可能不想安装的应用程序 （第 91 页）或批准可疑项目 （第 92 页）。

5.6.3 查找检测到的项目的信息

如果您想要了解更多有关安全隐患或终结点计算机上检测到，并在控制台中报告的项目的信息，或者，需要有关针对该项目应该采取何种措施的建议，请按照以下步骤做：

1. 在 终结点 视图的计算机列表中，双击有关的计算机。
2. 在 计算机详情 对话框中，拖动滚动条找到 未处置的警报和错误 部分。在已检测到的项目列表中，单击您想要相关的项目名称。
   这会将链接到 Sophos 网站，您可以在那里阅读项目的描述，有关针对该项目应该采取何种措施的建议

注释
或者，您可以访问 Sophos 网站上的安全分析页面 (http://www.sophos.com/zh-cn/threat-center/threat-analyses/viruses-and-spyware.aspx)，选择您想要查找的项目类型，然后在搜索栏中输入项目的名称。

5.6.4 处置勒索软件相关警报

如果您使用基于角色的管理，您必须具备 调整 - 清除 权限，才能从控制台清除检测到的项目，或者清除警报。要了解更多信息，请参见管理角色和子领域 （第 12 页）。

CryptoGuard将在终结点阻止触发勒索软件警报的进程。仅当您确认警报后才可解除该阻止操作。

注释
如果重新启动终结点，阻止操作将被解除。如果受感染的进程重新启动，则会触发新的勒索软件警报。

记住
您必须在触发检测的计算机上手动运行 Sophos Clean。否则，计算机将触发警报，并且该进程会在每次运行时再次被阻止。

要针对在控制台中显示的勒索软件警报采取措施：

1. 在 端点 视图中，选择您想要查看警报的计算机。右击并选择 处置警报和错误。
   会出现 处置警报和错误 对话框。
2. 选择要清除的勒索软件警报，并单击确认。
   确认已知的（清空的）警报不再出现在控制台中。这将解除对进程的阻止。

5.6.5 从控制台清除终结点计算机的警报或错误

如果您使用基于角色的管理，您必须具备 调整 - 清除 权限，才能从控制台清除警报或错误。要了解更多信息，请参见管理角色和子领域 （第 12 页）。

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。

注释
您无法清除有关安装错误的警报。只有在计算机上顺利安装了 Sophos Endpoint Security and Control，您才能清除它们。

1. 在 终结点 视图中，选择您想要清除警报的计算机。右击并选择 处置警报和错误。
   会出现 处置警报和错误 对话框。
2. 要从控制台中清除警报或 Sophos 产品的错误，请相应地转到“警报”或“错误”标签页中，选择您想要清除的警报或错误，然后，单击 确认已知。
   确认已知的（清空的）警报不再出现在控制台中。

要了解更多有关从控制台清除更新管理器警报的信息，请参见从控制台中清空更新管理器警报 （第 65 页）。

5.7 立即扫描和清除计算机

5.7.1 立即扫描计算机

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。

如果您使用基于角色的管理，您必须具备 调整 - 更新和扫描 权限，才能扫描计算机。要了解更多信息，请参见管理角色和子领域 （第 12 页）。

注释
只有 Windows，Linux 和 UNIX 计算机，可以执行从控制台启动的即时完整系统扫描。

要即时扫描计算机：

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。

注释
如果扫描检测到内存中有安全隐患的组件，那么，扫描会中止，并有警报发送到 Enterprise Console。这是因为继续扫描，有可能会扩散安全隐患。您必须在清除该安全隐患之后，再运行扫描。

5.7.2 立即清除计算机

您可以立即清除 Windows 或 Mac 计算机中的病毒，或者，不想安装的程序。

如果您使用基于角色的管理，您必须具备 调整 - 清除 权限，才能清除计算机。要了解更多信息，请参见管理角色和子领域 （第 12 页）。

注释
要清除 Linux 或 UNIX 计算机，您既可以从控制台（参见为读写扫描设置自动清除 （第 71 页）），也可以按照处置清除失败的已检测到的项目 （第 46 页）中的说明，个别地清除计算机。

如果某个项目（例如，特洛伊木马或可能不想安装的应用程序）被“部分地检测到”，那么，在清除受到影响的计算机之前，您需要对该计算机进行完整系统扫描，找到该“部分地检测到”的项目的所有组件。在计算机列表的 终结点 视图中，右击受到影响的计算机，并单击 完整系统扫描。要了解更多信息，请参见部分检测到项目 （第 185 页）。

要立即清除计算机：

1. 在计算机列表的 终结点 视图中，右击您想要清除的计算机，并单击 处置警报和错误。
2. 在 处置警报和错误 对话框的 警报 标签页中，选择您想要清除的各个项目，或者，单击 全选。单击 清除。

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。请参阅处置清除失败的已检测到的项目 （第 46 页）。

注释
清除某些病毒时，会导致在相关的计算机上进行完整系统扫描，以清除所有病毒。这可能会耗费较长时间。在扫描结束时，警报会被更新。

5.7.3 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，您可以进行手动清除。

1. 在计算机列表中，双击被感染的计算机。
2. 在 计算机详情 对话框中，拖动滚动条找到 未处置的警报和错误 部分。在已检测到的项目列表中，单击您想要从计算机中删除的项目名称。
   这将连接到 Sophos 网站，您可以在那里阅读这样清除计算机的建议。
3. 转到该计算机上，进行手动清除的工作。

注释
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。

6 更新计算机

6.1 配置更新管理器

更新管理器使您能够设置从 Sophos 网站自动更新 Sophos 安全软件。更新管理器与 Enterprise Console 安装在一起，并由 Enterprise Console 管理。

您可以安装多个更新管理器。例如，如果您具有带有数个路径的复杂网络，您可能想在远程路径中安装附加的更新管理器。要了解信息，请参见添加附加的更新管理器 （第 52 页）。

6.1.1 更新管理器怎样工作？

一旦您配置了更新管理器，它会：

- 定时连接 Sophos 或您的网络中的数据分发仓库。
- 下载更新文件到安全隐患检测数据，以及下载系统管理员预订的安全软件的更新文件。
- 以适合在终结点计算机进行安装的形式，将更新后的软件放置到一个或多个网络共享中。

计算机会自动从共享文件夹中进行更新，只要安装在这些计算机上 Sophos 软件已经 — 例如，通过应用更新策略，— 进行了这样的配置。

6.1.2 查看或编辑更新管理器配置

如果您使用基于角色的管理，您必须具有 策略设置 - 更新 权限，才能配置更新管理器。要了解更多信息，请参见管理角色和子领域 （第 12 页）。

1. 如果您在 终结点 视图中，单击工具栏上的 更新管理器 按钮，以显示 更新管理器 视图。
2. 在更新管理器列表中，选择您想要查看或编辑其配置的更新管理器。单击鼠标右键，并单击 查看/编辑配置。

   注释
   或者，选择更新管理器，转到 措施 菜单，指向 更新管理器，然后，单击 查看/编辑配置。

   会出现 配置更新管理器 对话框。
3. 按照以下主题中的说明，编辑配置：
   - 为更新管理器选择更新源 （第 49 页）。
   - 选择要下载的软件 （第 49 页）。
   - 指定在何处放置软件 （第 50 页）。
   - 创建或编辑更新计划 （第 51 页）。
   - 配置更新管理器日志记录 （第 51 页）。
   - 配置更新管理器更新自身 （第 52 页）。

要了解更多有关从控制台清除更新管理器警报的信息，请参见从控制台中清空更新管理器警报 （第 65 页）。

在您配置了更新管理器之后，您可以配置更新策略，并将它们应用到终结点计算机上。

6.1.3 为更新管理器选择更新源

如果您使用基于角色的管理，您必须具有 策略设置 - 更新 权限，才能配置更新管理器。要了解更多信息，请参见管理角色和子领域 （第 12 页）。

您需要选择一个更新源，更新管理器将从那里下载安全软件和更新文件，以将它们分发到网络中。

您可以选择数个更新源。列表中的第一个更新源是主更新源。列表中附加的更新源，是可选的备用路径，以备更新管理器无法从主更新源获取更新文件时使用。

1. 如果您在 终结点 视图中，单击工具栏上的 更新管理器 按钮，以显示 更新管理器 视图。
2. 在更新管理器列表中，选择您想要为其选择更新源的更新管理器。单击鼠标右键，并单击 查看/编辑配置。
3. 在 配置更新管理器 对话框的 更新源 标签页中，单击 添加。
4. 在 更新源详情 对话框中的 地址 栏中，输入更新源地址。该地址可以是 UNC 或 HTTP 路径。

   如果您想要直接从 Sophos 下载软件和更新文件，请选择 Sophos。
5. 如果需要，可在 用户名 和 密码 栏中，输入将要用来访问更新源的帐户的用户名和密码。
   - 如果更新源是 Sophos，请输入由 Sophos 提供的下载认证资料。
   - 如果更新源是由位于较高的更新层级中的更新管理器创建默认更新共享，那么，用户名 和 密码 栏会被事先输入。

     默认的更新共享，是一个 UNC 共享：\\<计算机名>\SophosUpdate， 这里的“计算机名”是更新管理器安装所在的计算机的名称。
   - 如果更新共享不是您的网络中默认的更新共享，请输入对网络共享具备读权限的认证资料。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. 如果您通过代理服务器访问更新源，那么，请选择 使用代理服务器连接。然后，输入代理服务器的地址和端口号。输入用于访问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。单击 “确定”。
   新的更新源会出现在 配置更新管理器 对话框中的列表里。

如果您已在不同的计算机上安装了更新管理器，那么，该更新管理器从中下载软件和更新文件的共享文件夹将出现在地址列表中。您可以选择该共享文件夹作为您正在配置的更新管理器的更新源。然后，使用列表右侧的 上移 或 下移 按钮，您可以将想要作为主更新源的地址移动到列表的最上方。

6.1.4 选择要下载的软件

如果您使用基于角色的管理，您必须具有 策略设置 - 更新 权限，才能配置更新管理器。要了解更多信息，请参见管理角色和子领域 （第 12 页）。

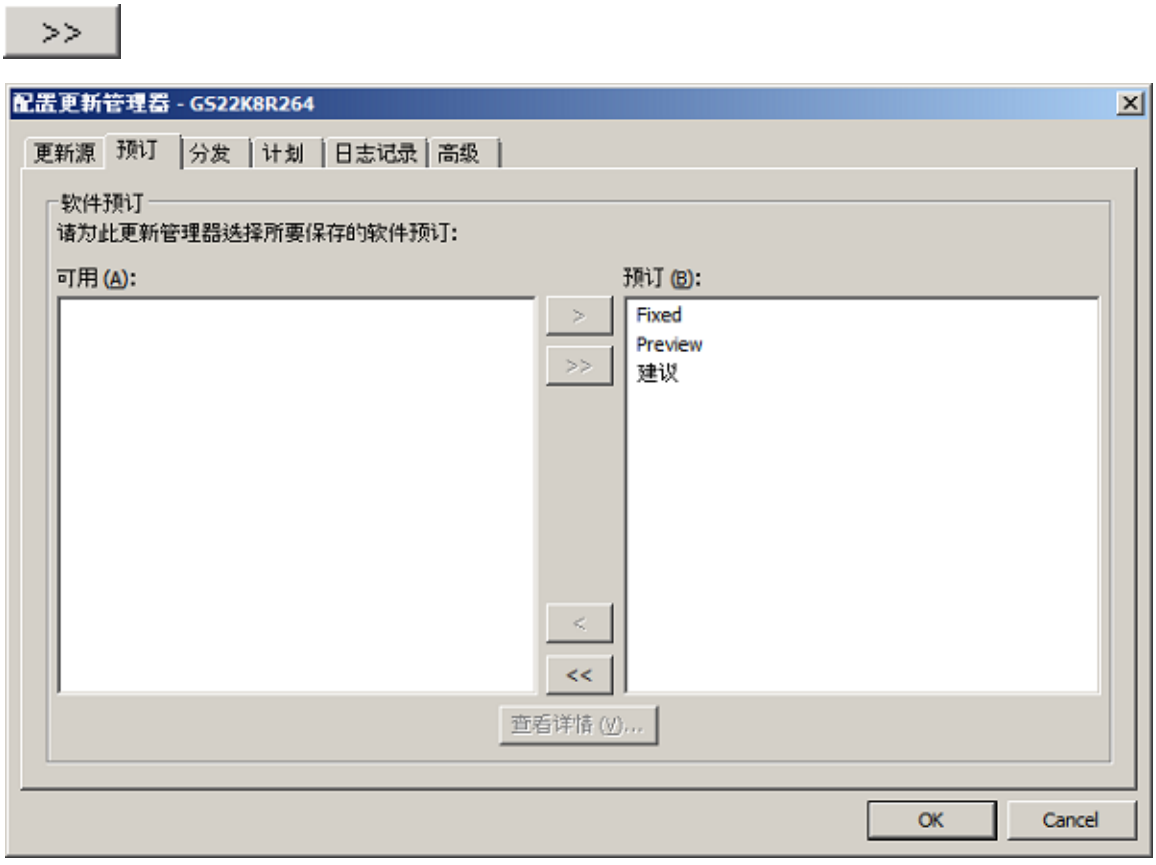
您需要为更新管理器选择将保持及时更新的软件预订。

1. 如果您在 终结点 视图中，单击工具栏上的 更新管理器 按钮，以显示 更新管理器 视图。
2. 在更新管理器列表中，选择您想要为其选择下载的软件的更新管理器。单击鼠标右键，并单击 查看/编辑配置。
3. 在 配置更新管理器 对话框的 预订 标签页中，从可用的软件预订列表中选择软件预订。

   要查看软件预订详情，如：软件预订中包括什么软件，请单击 查看详情。
4. 要将所选的软件预订移动到“已预订”列表中，请单击“添加”按钮。

   要将所有的软件预订移动到“已预订”列表中，请单击“全部添加”按钮。



6.1.5 指定在何处放置软件

如果您使用基于角色的管理，您必须具有 策略设置 - 更新 权限，才能配置更新管理器。要了解更多信息，请参见管理角色和子领域 （第 12 页）。

在您选择要下载的软件后，您可以指定在网络中的何处放置它。依照默认值，软件将放置在 UNC 共享文件夹 \\<计算机名>\SophosUpdate 中，这里的“计算机名”是更新管理器安装所在的计算机。

您可以将已下载的软件分发到网络中的附加的共享中。要这样做，请将现有的网络共享添加到可用共享列表中，然后，按照以下说明，将它移动到更新共享列表中。确保更新管理器用户帐户 (SophosUpdateMgr) 对共享具有读取权限。

注释
安装 Enterprise Console 前，需创建更新管理器用户帐户。要了解更多帐户信息，请参见 Enterprise Console 启动文档。

要指定在何处放置软件：

1. 如果您在 终结点 视图中，单击工具栏上的 更新管理器 按钮，以显示 更新管理器 视图。
2. 在更新管理器列表中，选择您想要为其选择用来分发软件的网络共享的更新管理器。单击鼠标右键，并单击 查看/编辑配置。
3. 在 配置更新管理器 对话框的 分发 标签页中，从列表中选择软件预订。
4. 从“可用”共享列表中选择一个共享文件夹，并单击“添加”按钮(>)，将它移到“更新至”列表中。

默认的共享 \\<计算机名>\SophosUpdate 总是会出现在“更新至”列表中。您无法从列表中删除此共享。

“可用的”共享列表包括 Enterprise Console 已知的，没有被其它的更新管理器使用的所有共享。

您可以使用“添加”(>)或“删除”(<) 按钮，添加现有的共享到“可用”共享列表，或者，从“可用”共享列表中删除共享。

5. 如果您想要输入共享描述，或者，输入写访问共享所需的认证资料，请选择该共享，并单击 配置。在 共享管理器 对话框中，输入描述和认证资料。

   如果您想为多个共享输入同样的认证资料，请在“更新到”列表中选择这些共享，并单击 配置。在 配置多个共享 对话框中，输入写访问所需要的认证资料。

6.1.6 创建或编辑更新计划

如果您使用基于角色的管理，您必须具有 策略设置 - 更新 权限，才能配置更新管理器。要了解更多信息，请参见管理角色和子领域 （第 12 页）。

依照默认值，更新管理器会每隔 10 分钟检查一次 Sophos Databank 中是否有更新的安全隐患检测数据。

您可以更改此更新频率。最小值为 5 分钟，最大值为 1440 分钟（24 小时）。我们建议每隔 10 分钟做一次安全隐患检测数据更新检查，这样，您可以在 Sophos 发布检测数据后，立即就接收到最新的安全隐患保护。

依照默认值，更新管理器会每隔 60 分钟检查一次 Sophos Databank 中是否有更新的软件。

您可以更改此更新频率。最小值为 10 分钟，最大值为 1440 分钟（24 小时）。

对于软件更新文件，您既可以指定某个频率，在每天的每个小时中使用，也可以创建一个更周密的计划，具体指定每周各天中的更新频率，以及在各天中的不同时段，使用不同的更新频率。

注释
您可以为每周中的各天创建不同的计划每周中的各天只能于一个计划关联。

1. 如果您在 终结点 视图中，单击工具栏上的 更新管理器 按钮，以显示 更新管理器 视图。
2. 在更新管理器列表中，选择您想要为其创建更新计划的更新管理器。单击鼠标右键，并单击 查看/编辑配置。
3. 在 配置更新管理器 对话框中的 计划 标签页中，输入检查安全隐患检测数据更新文件的频率。
4. 输入检查软件更新文件的频率。
   - 如果您想指定在每天的每个小时中使用的更新频率，请选择 每 n 分钟检查一次更新文件 选项，并输入以分钟计的时间间隔。
   - 如果您想要创建更周密的计划，或者，创建针对每周中的各天的不同的计划，请选择 设置和管理计划的更新 选项，并单击 添加。

     在 更新计划 对话框中，输入计划名称，选择一周中的某一天，并输入更新频率。

6.1.7 配置更新管理器日志记录

如果您使用基于角色的管理，您必须具有 策略设置 - 更新 权限，才能配置更新管理器。要了解更多信息，请参见管理角色和子领域 （第 12 页）。

1. 如果您在 终结点 视图中，单击工具栏上的 更新管理器 按钮，以显示 更新管理器 视图。

2. 在更新管理器列表中，选择您想要为其配置日志文件的更新管理器。单击鼠标右键，并单击 查看/编辑配置。
3. 在 配置更新管理器 对话框的 日志记录 标签页中，选择您想要保持日志记录的天数，以及日志文件的最大容量。

6.1.8 配置更新管理器更新自身

如果您使用基于角色的管理，您必须具有 策略设置 - 更新 权限，才能配置更新管理器。要了解更多信息，请参见管理角色和子领域 （第 12 页）。

1. 如果您在 终结点 视图中，单击工具栏上的 更新管理器 按钮，以显示 更新管理器 视图。
2. 在更新管理器列表中，选择您想要配置更新自身的更新管理器。单击鼠标右键，并单击 查看/编辑配置。
3. 在 配置更新管理器 对话框的 高级 标签页中，选择您想要保持及时更新的更新管理器的版本。例如，如果您选择“建议”，那么，更新管理器将总是升级到 Sophos 提供的具有此标签的版本。实际的更新管理器版本将改变。

6.1.9 使更新管理器立即检查更新文件

如果您使用基于角色的管理，您必须具备 调整 - 更新和扫描 权限，才能执行此任务。要了解更多信息，请参见管理角色和子领域 （第 12 页）。

在您配置了更新管理器之后，它会按照设定的计划，检查更新文件，并自动将它们从更新源下载到它所维护的更新共享文件夹中。如果您想要某个更新管理器，立即检查并下载安全隐患检测数据更新文件，终结点计算机的软件更新文件，以及更新管理器自身的软件更新文件，请按照以下步骤做：

1. 如果您在 终结点 视图中，单击工具栏上的 更新管理器 按钮，以显示 更新管理器 视图。
2. 在更新管理器列表中，选择您想要更新的更新管理器。单击鼠标右键，并单击 立即更新。

6.1.10 使更新管理器遵照配置设置

如果您使用基于角色的管理，您必须具有 策略设置 - 更新 权限，才能配置更新管理器。要了解更多信息，请参见管理角色和子领域 （第 12 页）。

1. 如果您在 终结点 视图中，单击工具栏上的 更新管理器 按钮，以显示 更新管理器 视图。
2. 在更新管理器列表中，选择您想要遵照配置设置的更新管理器。单击鼠标右键，并单击 遵照配置。

6.1.11 添加附加的更新管理器

Sophos Update Manager (SUM) 总是安装在您安装 Enterprise Console 的计算机上。如果您在安装期间，选择了 自定义安装，那么，SUM 所安装的计算机，是安装了 Management Server 的计算机。

您添加一个或多个附加的更新管理器到网络中。这样做您可以减轻已安装的更新管理器的负荷，并且可以更有效地分发更新文件。您安装附加的更新管理器的计算机，不一定非要已经安装了其它的更新管理器。

重要提示
不要删除安装在 Enterprise Console 所在的管理服务器上的更新管理器。在此更新管理器被配置更新源之前，Enterprise Console 无法彻底保护网络。此操作会使 Enterprise Console 能够收到必要的更新文件（例如，终结点计算机应该运行的安全软件的版本的信息，新的和更新的数据控制所使用的“内容控制列表”，或者新的受控设备和受控程序的列表）。

要启用其他更新管理器以通过 HTTP 从 Sophos 或其他更新管理器下载安全软件，请打开要安装其他更新管理器的计算机上的 TCP 端口 80（出站）。要启用更新管理器以通过 UNC 路径从其他更新管理器下载安全软件，请在计算机上打开以下出站端口：UDP 端口 137、UDP 端口 138、TCP 端口 139 和 TCP 端口 445。

如果计算机运行的 Windows 操作系统版本中包括 Network Discovery 功能，而该功能是关闭的，那么，请开启该功能并重新启动计算机。

如果计算机上启用了用户帐户控制 (UAC)，则关闭 UAC，然后重新启动计算机。在安装完毕更新管理器，并预订 Sophos 更新文件之后，您可以重新开启 UAC。

如果计算机在域中，请以域管理员的身份登录。

如果计算机在工作组中，请以本地管理员的身份登录。

更新管理器安装程序在安装了 Enterprise Console 的管理服务器上的共享文件夹 \\Servername \SUMInstallSet 中。要查看更新管理器安装程序的路径，转到 视图 菜单，并单击 Sophos Update Manager 安装程序路径。

您可以使用 Windows Remote Desktop 安装 Sophos Update Manager。

要安装附加的更新管理器：

1. 运行 Sophos Update Manager 安装程序文件 Setup.exe。
   会出现一个安装向导。
2. 在向导的 欢迎 页面中，单击 下一步。
3. 在 用户使用许可协议 页面中，仔细阅读许可证协议，如果您同意所有的条款，请单击 我接受许可证协议中的条款。单击 下一步。
4. 在 目标文件夹 页面中，接受默认设置，或者，单击 更改 并输入新的目标文件夹。单击 下一步。
5. 在 Sophos Update Manager 帐户 页中，选择终结点计算机将要用来访问由更新管理器创建的默认的更新共享的帐户。（默认的更新路径是：\\<计算机名>\SophosUpdate，这里的“计算机名”是更新管理器安装所在的计算机。）此帐户必须具备对共享的读权限，但不必具有管理员权限。
   您可以选择默认用户 ，选择现有的用户，或创建新的用户。
   依照默认值，安装程序会创建对默认的更新共享具有读权限的 SophosUpdateMgr 帐户，该帐户没有交互登录权限。
   如果您稍后想要添加更多的更新共享，请选择一个现有帐户，或创建对这些共享具备读权限的新帐户。否则，请确保 SophosUpdateMgr 帐户对这些共享具有对权限。
6. 在 Sophos Update Manager 帐户详情 页中，根据您在先前的页面中选择的选项，输入默认用户的密码，或新用户的详情，或选择现有的帐户。
   帐户的密码必须遵照您的密码策略。
7. 在 准备安装程序 页中，单击 安装。
8. 当安装完成时，单击 完成。

您安装 Sophos Update Manager 的那台计算机，应该出现在 Enterprise Console 的 更新管理器 视图中。在 查看 菜单中，单击 更新管理器。

要配置更新管理器，请选择它，单击鼠标右键，然后，单击 查看/编辑配置。

6.1.12 在网页服务器上发布安全软件

您可能想在网页服务器上发布 Sophos 安全软件，使计算机可以通过 HTTP 进行访问。

要在网页服务器上发布安全软件：

1. 要查找放置已下载的安全软件的共享文件夹的路径（也称为“引导路径”）：
   a) 在 Enterprise Console 的查看菜单中，单击引导路径。
   在 引导路径 对话框中，路径 栏中会显示每个操作平台的引导路径。
   b) 记录下该路径，但是不要包括最后的 中央安装目录 (CID) 文件夹。例如：
   \\服务器名称\SophosUpdate
2. 使引导路径（包括子文件夹）能够在网页服务器上可用。要了解操作指导，请参阅 Sophos 技术支持知识库文章 38238。

6.2 配置软件预订

软件预订指定从 Sophos 为各操作平台的计算机下载哪个版本的终结点软件。

下载安全软件向导 可以设置一个名为“建议”的软件预订。该软件预订包括任何所选的软件的建议版本。

如果您想要将软件添加到您的预订中或者预订不是建议版的版本，请按照预订安全软件 （第 56 页）中的说明配置预订。

如果您在安装 Enterprise Console 了之后，没有结束此向导，请参见运行下载安全软件向导 （第 57 页）。

6.2.1 可以使用什么类型的更新？

对于每个平台（例如，Windows），不同的软件包代表不同类型的更新，并且包含不同版本的端点软件。通过在软件预订中选择以下更新类型，您可以选择从 Sophos 下载的，将要部署到端点计算机中的软件包。

更新类型	描述
建议	这是默认的软件包。如果您使用此软件包，Sophos 将会定期更新您的软件（通常每月更新一次），包括： • 修复客户发现的问题。 • 提供准备全面发行的新功能。 如果您是首次安装 Enterprise Console 并接受默认设置，您将会安装此版本。
预览版本	此软件包针对于 IT 和安全管理员。 如果您使用此版本，您可以在它们发布为推荐版本之前收到新的功能。这就意味着您可以在软件正式发布之前在测试网络中对它们进行测试和评估。 注释 有时，预览软件包可以给您和推荐软件相同的软件。只有在没有新功能需要在用户环境中测试时，才会发生这种情况。

更新类型	描述
扩展版本	扩展版本适用于对在其网络上安装更新的软件有严格或稳定流程要求的客户。 如果您使用此版本，您会在延迟几个月后收到和推荐渠道相同的更新。这意味着产品中的任何问题都会在安装于您的网络之前予以确定和修复。
先前的推荐	当前推荐的软件包的先前版本。 如果您希望在推广到网络之前需要更长时间测试新软件，此版本会对您很有帮助。
先前的扩展版本	当前扩展软件包的先前版本。 如果您希望在推广到网络之前需要更长时间测试新软件，此版本会对您很有帮助。
固定版本	请参阅固定版本软件包 （第 55 页）。

注释
我们也许会在将来更改软件包。更多有关当前可用软件包的信息，请访问 Sophos 知识库文章 19216。

下载安全软件向导 可以设置软件预订，指定任何所选的软件的建议版本。

实际所下载的版本通常每个月会有所不同。若要检查实际下载了哪一种软件版本，在软件包订阅对话框中，选择您要检查的软件包并单击详细信息。

6.2.2 固定版本软件包

固定版本是指随新的安全隐患数据而更新，而不是随每个月的最新软件版本而更新的版本。例如，Windows 版 Sophos Endpoint Security and Control 的固定版本为 "10.3.15 VE3.60.0"。它包括三部分的版本标识符（主要版本标识符 (10)、次要版本标识符 (3) 和维护版本标识符 (15)）以及威胁检测引擎版本 (VE3.60.0)。

使用固定包

默认情况下，禁用了固定版本软件包的使用（在工具 > 配置固定包的使用下）。它们不会显示在软件预订对话框中，且不可预订。

提示
如果您预订了一个固定软件版本，为确保获得最好的保护，建议您将您的预订更改为“推荐”软件包。更多有关软件包的信息，请参见可以使用什么类型的更新？ （第 54 页）

如果之前未使用过固定版本软件包，但想要使用，可以在工具 > 配置固定包的使用下启用固定包的使用。启用固定包的使用后，它们将显示在软件预订对话框中，并且可以预订。

注释
如果您使用基于角色的管理，则必须有系统配置权限才能配置固定包的使用。

如果您在仍然预订某个固定包的情况下禁用固定包的使用，您将预订该包并且它会继续下载，直至您取消预订。但是，您将不能查看或重新预订其他固定包。

如果您有远程控制台，在其中一个控制台中更改此配置选项将影响所有控制台。如果您已按 Sophos 知识库文章 117348 中所述在注册表中启用了固定包的使用，注册表设置将只影响对它进行了配置的计算机，并且它将优先于控制台中的配置选项。

固定包的生命周期

只要 Sophos 提供了固定版本，就可以随时下载它。如果某个固定版本将停止服务，您将在任何预订该版本的更新管理器旁的更新管理器视图中看到相关的警报。如果启用了电子邮件警报发送，管理员还会收到相关的电子邮件警报。

预订的固定版本停止服务后，如果您没有在支持结束前修改您的预订，您将会自动预订新的固定扩展包。要了解更多信息，请参阅Sophos 知识库文章 121139。

有关 Sophos Endpoint 生命周期策略的详细信息，请参阅 Sophos 知识库文章 112580。

6.2.3 预订安全软件

若要使用基于角色的管理：

- 您必须具有 策略设置 - 更新 权限，才能编辑软件预订。
- 如果某个软件预订所应用的更新策略是被应用到您的活动子领域之外的，那么，您不能编辑该软件预订。

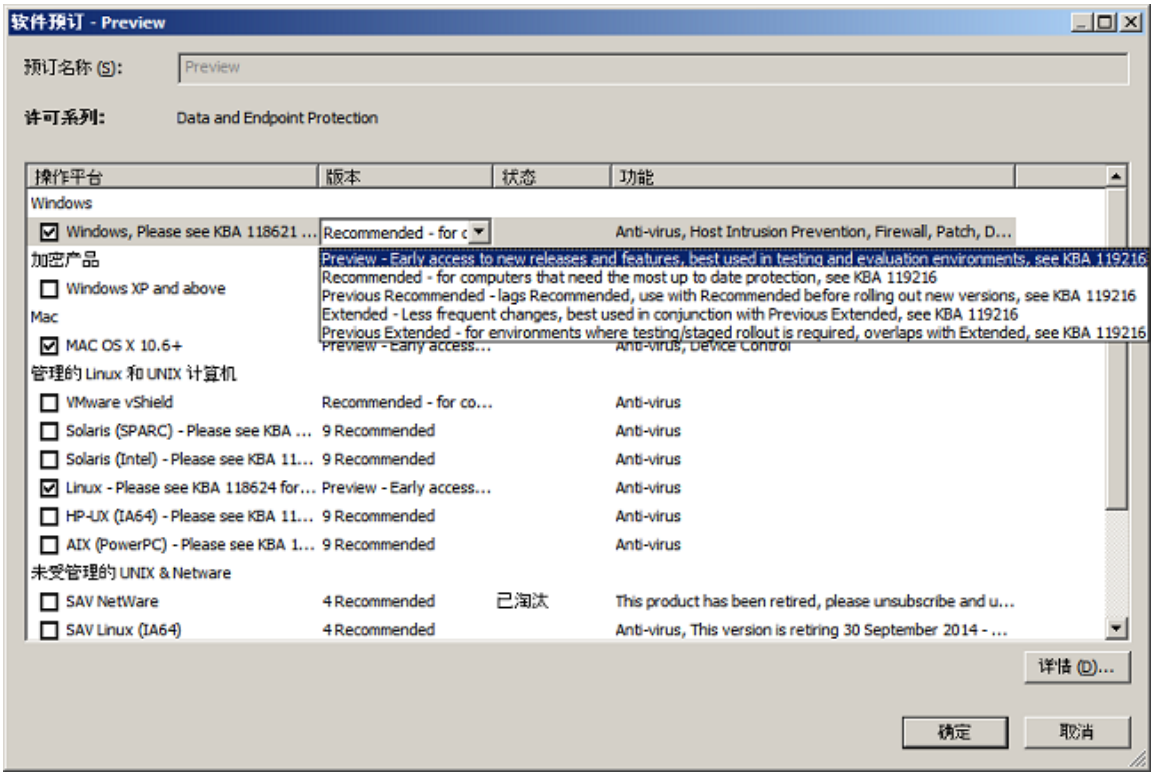
要了解更多有关基于角色的管理的信息，请参见管理角色和子领域 （第 12 页）。

要预订安全软件：

1. 在 查看 菜单中，单击 更新管理器。
2. 在 软件预订 窗格板中，双击您想要更改的预订，或单击窗格板顶部的 添加 按钮，以创建新的预订。

   会出现 软件预订 对话框。

   或者，如果您想要复制一份现有的预订，请选择该预订，单击鼠标右键，然后单击 复制预订。为预订输入新的名称，然后，双击它，打开 软件预订 对话框。
3. 在 软件预订 对话框中，如果您想要，可以编辑软件预订的名称。
4. 选择您想要下载软件的操作平台。
5. 依据默认值，您预订了“推荐”版本的软件包。您也可以选择非默认的软件包（例如，您想要预览新功能）。若要这样做，单击您想要更改软件包的平台旁边的版本字段，然后再次单击。在可用版本的下拉菜单中，选择您想要下载的版本（例如“预览”）。



要了解其他可用的软件包，请参见可以使用什么类型的更新？ （第 54 页）

在预定了安全软件之后，您可以设置软件预订的电子邮件警报。要了解更多有关软件预订电子邮件警报的信息，请参见设置软件预订警报 （第 154 页）。

如果您创建了新的软件预订，请按照查看或编辑更新管理器配置 （第 48 页）中的说明配置更新管理器以维护它。

6.2.4 运行下载安全软件向导

如果您使用基于角色的管理，您必须具备 策略设置 - 更新 权限，才能运行 下载安全软件向导。要了解更多信息，请参见管理角色和子领域 （第 12 页）。

如果您在安装了 Enterprise Console 了之后，尚未完成 下载安全软件向导，请按照以下说明做：

- 在 措施 菜单中，单击 运行下载计算机软件向导。

  下载安全软件向导 会指导您完成选择和下载软件。

注释
成功完成向导后，运行下载安全软件向导选项会从措施菜单中消失。

6.2.5 查看哪个更新策略使用软件预订

要查看哪个更新策略使用了特定的软件预订：

- 选择预订，单击鼠标右键，然后，单击 查看预订用法。

在 软件预订用法 对话框中，您可以看到使用软件预订的更新策略的列表。

6.3 配置更新策略

更新策略使您能够保持您的计算机及时更新您所选择的安全软件。Enterprise Console 将按照设定的频率检查更新文件，并更新计算机。

默认的更新策略使您能够安装和更新在“建议”软件预订中指定的软件。

如果您想要更改默认的更新策略，或者，想要创建新的更新策略，请按照以下主题中的操作指导做：

- 选择预订 （第 58 页）
- 配置更新服务器 （第 59 页）
- 计划更新 （第 63 页）
- 选择不同的初始安装源 （第 63 页）
- 日志记录更新活动 （第 64 页）

注释
如果您使用基于角色的管理，那么：

- 您必须具备 策略设置 - 更新 权限，才能配置更新策略。
- 您不能编辑应用于您的活动子领域之外的策略。

要了解更多有关基于角色的管理的信息，请参见管理角色和子领域 （第 12 页）。

6.3.1 选择预订

如果您使用基于角色的管理，那么：

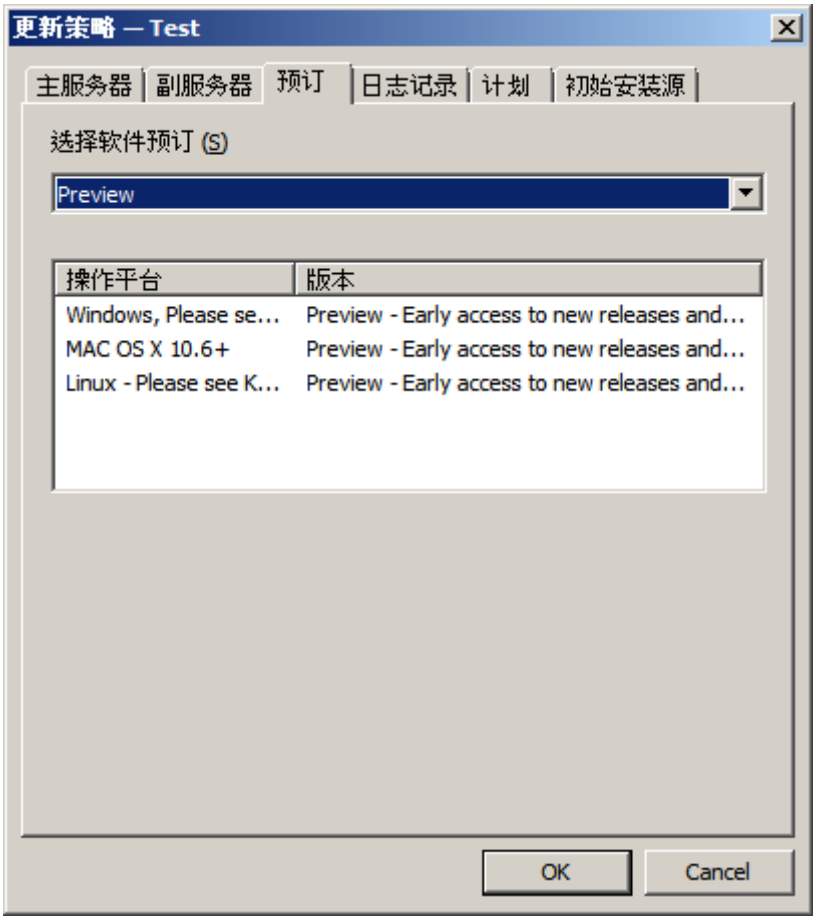
- 您必须具备 策略设置 - 更新 权限，才能配置更新策略。
- 您不能编辑应用于您的活动子领域之外的策略。

要了解更多信息，请参阅 管理角色和子领域 （第 12 页）。

预订指定从 Sophos 为各操作平台的计算机下载哪个版本的端点软件。默认的预订包括针对 Windows 的最新软件。

要选择预订：

1. 请检查您想要配置的计算机组采用了哪个更新策略。
   请参阅查看组采用的策略 （第 23 页）。
2. 在 策略 窗格板中，双击 更新。然后，双击您想要更改的策略。
3. 在 更新策略 对话框中，单击 预订 标签，并为您想要保持及时更新的软件选择预订。



6.3.2 配置更新服务器

依照默认值，计算机会从单个的主更新源 UNC 共享 \\<计算机名>\SophosUpdate 中进行更新，这里的 <计算机名> 是升级管理器所在的计算机的名称。还可以为更新文件指定备用的副更新源、启用路径漫游和启用带宽限制。

如果端点计算机无法连接它们的主更新源，它们则将尝试从副更新源（如果已指定）进行更新。我们建议您总是指定副更新源。

主更新源和副更新服务器路径，可以是您的网络中任何可以访问的更新管理器上的 UNC 共享或 HTTP URL。副更新服务器路径也可以设定为通过 HTTP 在因特网上直接从 Sophos 获得更新文件

注释
取决于您的设置，更新管理器可以有多个分发共享。

主服务器

主服务器自动设置在默认的主服务器位置。默认情况下，计算机会从单个主源 UNC 共享文件夹 \\<计算机名>\SophosUpdate 进行更新，其中 <计算机名> 是安装 Sophos Update Manager 的计算机的名称。

要访问该共享文件夹，计算机将使用您在安装 Enterprise Console 时输入的 Sophos Update Manager 凭据。如果您遵循了 Enterprise Console 启动指南的建议，该帐户将命名为“SophosUpdateMgr”。

如果需要更改凭据，请参见更改主服务器的认证资料 （第 61 页）。

如果通过代理服务器访问更新源，请单击代理详细信息，并输入代理详细信息。

如果要启用位置漫游，请参见笔记本电脑的路径漫游 （第 60 页）。

还可以启用带宽限制，以限制更新时计算机可以使用的带宽量。在更新策略的主服务器选项卡上，单击高级按钮。在高级设置对话框中，选中限制带宽使用量复选框，然后使用滑块控件指定最大的带宽，单位是 Kb/秒。

笔记本电脑的路径漫游

某些笔记型电脑用户可能会在公司内部外部以漫游方式使用计算机。当（在针对漫游的笔记型电脑的更新策略中）启用路径漫游时，漫游的笔记型电脑会通过问询所连接到的本地网络中的其它（固定的）端点计算机，尝试找到最近的更新服务器路径，并进行更新，从而节省带宽，避免耽误更新。

漫游的笔记型电脑通过问询问询所连接到的本地网络中的固定计算机，可以获得更新服务器地址和认证资料。如果返回多个路径，那么，笔记型电脑会确定并使用最近的路径。如果不成功，那么，笔记型电脑会使用在更新策略中定义的主（然后副）路径。

注释
当固定的计算机向笔记型电脑发送更新路径和认证资料时，密码在传输和存储中都会被加密。不过，为端点计算机设置的，可以读取更新服务器路径的帐户，应该尽量严格，只运行读访问。请参阅指定在何处放置软件 （第 50 页）。

如果您想要了解更多有关路径漫游怎样工作的详情，请参见路径漫游怎样工作？ （第 60 页）。

可以使用路径漫游的条件：

- 漫游的和固定的端点计算机，共同使用单一的 Enterprise Console。
- 固定的端点计算机与漫游的计算机使用同样的软件预订。
- 在更新策略中指定了一个供漫游的笔记型电脑使用的主更新路径。
- 任何第三方的防火墙，都配置为允许更新路径问询和响应。所用端口通常为 UDP 端口 51235，但是可对所用端口进行配置；详细信息请参见 Sophos 知识库文章 110371。

启用路径漫游作为指定更新源的一部分。路径漫游只应该在经常在办公室之间漫游的计算机上启用。要了解有关怎样启用路径漫游的信息，请参见更改主服务器的认证资料 （第 61 页）。

有关路径漫游的常见问题，请参见 Sophos 知识库文章 112830。

路径漫游怎样工作？

路径漫游是一种供漫游的笔记型电脑使用的智能更新方法，它能使更新活动从“最佳”的更新路径进行，并且更新活动并不仅仅依赖于在笔记型电脑的更新策略中指定的那个主/副更新路径。

在路径漫游启用后，会发生以下情形：

1. 当某台笔记型电脑改变它的所在的位置时，安装在该笔记型电脑上 Endpoint Security and Control 的 Sophos AutoUpdate 组件会确定出自从最近一次更新之后，在所连接的网络中的那个默认的网关的 MAC 地址已经发生了改变。然后，路径漫游会默认使用 UDP 端口 51235 将本地子网上的 ICMP 广播发送到邻近安装的 AutoUpdate。
2. 邻近安装的 AutoUpdate 会通过相同的端口回复它们的更新策略。在回答中只会发送主更新路径。

   所有安装的 Endpoint Security and Control 都会听到广播，无论它们是否启用了路径漫游功能。

   回复中的敏感信息会被加密，敏感部分会经过哈希加密处理，以保证真实性。

   回复的时间是随机安排的，以避免回复消息蜂拥而至。回复同样也是 ICMP 广播，这样其它任何将要回复相同内容的计算机，将收到广播，从而知道不必回答。

3. AutoUpdate 会从收到的路径中选择“最佳”路径，并检查寄件人是否也是被相同的 Enterprise Console 管理，以及预订 ID 是否与笔记型电脑上的 AutoUpdate 所使用的那个预订 ID 匹配。

   “最佳”路径取决于访问该更新路径所需要的网络跃点 (hop) 的数量。

4. 接着会尝试进行更新，如果顺利，该路径会被存储在高速缓存中。

   最多有4个带有相同的预订 ID 和最少的网络跃点(hop)的可访问的更新路径，会被存储在笔记型电脑中（在以下路径中的 iustatus.xml 文件中：C:\Program Files\Sophos\AutoUpdate\data\status\iustatus.xml）。

   每次 AutoUpdate 进行更新工作时，这些更新路径都会被检查。

   注释
   如果您想要恢复使用在更新策略中指定的那个主/副更新路径（比如，您希望从在策略中指定那个路径中展开部署自定义内容），那么，您需要禁用路径漫游。

启用路径漫游

如果您使用基于角色的管理，那么：

- 您必须具备 策略设置 - 更新 权限，才能配置更新策略。
- 您不能编辑应用于您的活动子领域之外的策略。

要了解更多信息，请参阅 管理角色和子领域 （第 12 页）。

您只应该在经常在办公室之间漫游的计算机上启用路径漫游。

要启用路径漫游：

1. 在 策略 窗格板中，双击 更新。然后，双击您想要更改的那个更新策略。
2. 在 更新策略 对话框中的 主服务器 标签页，勾选 允许路径漫游 勾选框。
3. 在 组 窗格板中，选择使用您刚更改的更新策略的某个组。右击鼠标，并选择 遵照，组更新策略。为使用此更新策略的各个组重复此步骤。

注释
如果以后您需要转换回来使用在更新策略中指定的主/副更新路径，请禁用路径漫游。

更改主服务器的认证资料

如果您使用基于角色的管理，那么：

- 您必须具备 策略设置 - 更新 权限，才能配置更新策略。
- 您不能编辑应用于您的活动子领域之外的策略。

要了解更多信息，请参阅 管理角色和子领域 （第 12 页）。

要更改主服务器的认证资料：

1. 在 策略 窗格板中，双击 更新。然后，双击您想要更改的那个更新策略。
2. 在 更新策略 对话框的 主服务器 标签页中，输入访问该服务器时所使用的新的认证资料。如果需要，更改其它的详情。

注释
如果您的主更新源是您的网站中的某个文件夹，并且您使用匿名身份验证的 Internet 信息服务 (IIS)，那么，您仍然需要在 主服务器 标签页中输入身份验证资料。请使用用于 UNC 共享中的“初始安装源”的身份认证资料，即使您并不需要用它来访问网站服务器。如果您保留 主服务器 标签页中的 用户名 和 密码 栏为空白，那么，您将无法从控制台保护终结点计算机。

3. 在 组 窗格板中，选择使用您刚更改的更新策略的某个组。右击鼠标，并选择 遵照，组更新策略。
为使用此更新策略的各个组重复此步骤。

设置副更新服务器

如果您使用基于角色的管理，那么：

- 您必须具备 策略设置 - 更新 权限，才能配置更新策略。
- 您不能编辑应用于您的活动子领域之外的策略。

要了解更多信息，请参阅 管理角色和子领域 （第 12 页）。

要设置副更新服务器路径

1. 请检查您想要配置的计算机组采用了哪个更新策略。
请参阅查看组采用的策略 （第 23 页）。
2. 在策略窗格中，双击更新，然后，双击您想要更改的策略。
3. 在 更新策略 对话框中，单击 副服务器 标签页，然后，勾选 指定副服务器详情 复选框。
4. 在 地址 （HTTP 或 UNC） 文本框中，按照以下说明之一做：
   - 输入更新服务器共享的 HTTP URL 或 UNC 网络路径。
   - 选择 Sophos。

重要提示
如果您选择的 HTTP URL 或共享，不是由受管理的更新管理器维护的，那么，Enterprise Console 将无法检查指定的软件预订是否可用。您必须通过手动方式确保共享中包含了指定的软件预订，否则，计算机将无法被更新。

5. 如果策略中包含 Mac 端点计算机，并且您在 地址 文本栏中指定了 UNC 路径，那么，请在 为 Mac OS X 选择文件共享协议 下，选择针对 Mac 计算机的协议，以便能够访问更新共享。
6. 如果必要，请在 用户名 栏中，输入将要用来访问服务器的帐户的用户名，然后，输入并确认密码。对于 Sophos HTTP 而言，这是您的预订认证资料。
对于您在上述的地址栏中输入的共享，此帐户应该只具有“只读（浏览）”的权限。

注释
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。要了解更多有关怎样检查 Windows 用户帐户的信息，请参见Sophos 知识库文章 11637。

7. 要节制带宽，请单击高级。在高级设置对话框中，选中限制带宽使用量复选框，然后使用滑块控件指定最大的带宽，单位是 Kb/秒。
8. 如果您是通过代理服务器接入更新源的，请单击 代理详情。在代理详情对话框中，选中通过代理访问服务器复选框，然后，输入代理服务器 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。

注释
有的因特网服务提供商（ISP），要求将 HTTP 请求送到代理服务器上。

9. 单击 确定，以关闭 更新策略 对话框。
10. 在 组 窗格中，右击使用您刚才更改的更新策略的组，然后，单击 遵照 > 组更新策略。
为使用此更新策略的各个组重复此步骤。

6.3.3 计划更新

如果您使用基于角色的管理，那么：

- 您必须具备 策略设置 - 更新 权限，才能配置更新策略。
- 您不能编辑应用于您的活动子领域之外的策略。

要了解更多信息，请参阅 管理角色和子领域 （第 12 页）。

依照默认值，计算机会每隔 5 分钟检查一次网络共享中是否有更新文件。

注释
如果计算机是直接从 Sophos 下载更新文件，则该更新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。

要指定更新频率：

1. 请检查您想要配置的计算机组采用了哪个更新策略。
请参阅查看组采用的策略 （第 23 页）。
2. 在 策略 窗格板中，双击 更新。然后，双击您想要更改的策略。
3. 在 更新策略 对话框的 计划 标签页中，保留勾选 启用联网计算机自动使用 Sophos 更新文件 勾选框。请输入软件更新的频率（以分钟计）。
4. 如果计算机是通过拨号连接因特网进行更新的，请选择 在拨号连接时进行更新检查。
每当您连接到因特网时，计算机就会尝试进行更新。

6.3.4 选择不同的初始安装源

如果您使用基于角色的管理，那么：

- 您必须具备 策略设置 - 更新 权限，才能配置更新策略。
- 您不能编辑应用于您的活动子领域之外的策略。

要了解更多信息，请参阅 管理角色和子领域 （第 12 页）。

依照默认值，计算机软件安装在计算机上之后，就从在 主服务器 标签页中指定的更新源保持更新。您可以指定不同的初始安装源

注释
此设置仅应用于 Windows。

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。

要从不同的安装源进行安装：

1. 请检查您想要配置的计算机组采用了哪个更新策略。
   请参阅查看组采用的策略 （第 23 页）。
2. 在 策略 窗格板中，双击 更新。然后，双击您想要更改的策略。
3. 在 更新策略 对话框的 初始安装源 标签种，取消勾选 使用主服务器地址 勾选框。然后，输入您想使用的安装源的地址。

6.3.5 日志记录更新活动

如果您使用基于角色的管理，那么：

- 您必须具备 策略设置 - 更新 权限，才能配置更新策略。
- 您不能编辑应用于您的活动子领域之外的策略。

要了解更多信息，请参阅 管理角色和子领域 （第 12 页）。

依照默认值，计算机会日志记录它们的更新活动。默认的日志记录的最大容量为 1 MB。默认的日志级别为“普通”。

要更改日志记录设置：

1. 请检查您想要配置的计算机组采用了哪个更新策略。
   请参阅查看组采用的策略 （第 23 页）。
2. 在 策略 窗格板中，双击 更新。然后，双击您想要更改的策略。
3. 在 更新策略 对话框的 日志记录 标签页中，保留勾选 记录 Sophos AutoUpdate 活动日志 勾选框。在 日志文件大小上限 栏中，指定日志文件的最大值。
4. 在 日志记录级别 栏中，选择 普通 或 详尽 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。

6.4 监控更新管理器

在指标面板上查看更新管理器的状态

更新管理器的状态显示在 指标面板 的 更新文件 面板中它将告诉您前次从 Sophos 下载更新文件的时间，并且，在如果前次下载以来的时间间隔超过了“警告”级或“紧要”级时，显示警报消息。

注释
如果更新管理器只是暂时无法进行更新，指标面板中的 更新 部分不会发出警报或出错消息。只有在自前次进行更新以来的时间已超过了在 配置指标面板 （第 41 页） 中设定的提醒级别或紧要级别，才会发出警报和出错消息。

检查更新管理器警报和错误

更新管理器警报和错误会分别显示在 更新管理器 视图的 警报 和 错误 栏中。

如果您预订了固定版本的软件，当该版本即将淘汰或已淘汰时，会出现警报。如果您的产品的用户授权使用许可协议已更改，那么，会出现提示。

要检查更新管理器警报和错误：

1. 如果您在 终结点 视图中，单击工具栏上的 更新管理器 按钮，以显示 更新管理器 视图。
2. 在更新管理器列表中，查看 警报 和 错误 栏发现任何可能存在的问题。
3. 如果在某个更新管理器旁出现警报或错误图标，请单击该更新管理器，并单击 查看更新管理器详情。

   在 更新管理器详情 对话框中，您可以看到前次安全隐患检测数据和软件更新的时间，软件预订或更新管理器保持及时更新的软件预订的状态，以及更新管理器的状态。
4. 要了解更多有关某个特定的更新管理器的状态，以及有关怎样处置它的信息，请参见 描述 栏中的链接。

如果您需要查看或更改您的预订，例如，如果您过去预订的产品即将被淘汰，或者，您的产品的用户授权使用许可协议已更改，并且新的协议中不包含此产品，请参见预订安全软件 （第 56 页）。

如果由于用户授权许可协议的更改，可以使用新的功能，那么，您可能需要先配置新的策略，然后才能使用这些功能。

预订电子邮件警报

您可以设置，当您过去预订的产品版本即将淘汰，或者已经淘汰时，或者，当您的 Sophos 产品的功能由于用户授权使用许可协议的更改，而产生变更时，向您选择的收件人发送电子邮件警报。要了解更多信息，请参见设置软件预订警报 （第 154 页）。

6.4.1 从控制台中清空更新管理器警报

如果您使用基于角色的管理，您必须具备 调整 - 清除 权限，才能从控制台清除警报。要了解更多信息，请参见管理角色和子领域 （第 12 页）。

要从控制台中清除更新管理器警报：

1. 在 更新管理器 视图中，选择您想要清除警报的更新管理器。单击鼠标右键，并选择 确认已知警报。
   会出现 更新管理器警报 对话框。
2. 要从控制台清除警报，请选择您想要清除的警报，然后，单击 确认已知。
   确认已知的（清空的）警报不再出现在控制台中。

6.5 更新未及时更新的计算机

如果您使用基于角色的管理，您必须具备 调整 - 更新和扫描 权限，才能更新计算机。要了解更多信息，请参阅 管理角色和子领域 （第 12 页）。

在您设置了更新策略，并将它们应用到联网计算机之后，计算机会自动保持更新。除非更新出现问题，您不必手动更新计算机。

如果在 端点 视图的计算机列表中，您看到 状态 标签页的 更新情况 栏中的计算机旁出现一个时钟图标，则表明该计算机未及时更新计算机软件。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。

要诊断问题并更新计算机。

1. 在 端点 视图中，选择含有未及时更新的计算机的组。

2. 在状态选项卡上，单击更新情况列标题，将计算机按更新情况排序。
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，单击鼠标右键，并单击 立即更新计算机。
   - 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。在 查看 菜单中，单击 更新管理器。选择维护您认为未及时更新的那个路径的更新管理器，单击鼠标右键，并单击 立即更新。然后在 视图 菜单中，单击 端点。选择未及时更新的计算机，单击鼠标右键，并单击 立即更新计算机。

   如果您具有多个更新管理器，而不清楚哪个更新管理器维护未及时更新的路径，请使用“更新层级”报告，查看各个更新管理器维护的是哪些共享文件夹。要查看“更新层级”报告，请在 工具 菜单中，单击 管理报告。在 报告管理器 对话框中，选择 更新层级 并单击 运行。查看报告中的“由更新管理器管理的共享”部分。

7 配置策略

7.1 防病毒和 HIPS 策略

防病毒和 HIPS 策略使您能够：

- 在用户试图复制，移动，或者打开文件时，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。
- 扫描广告软件和其他可能不想安装的应用程序。
- 扫描计算机中的可疑文件和 Rootkit。
- 检测恶意网络数据流，即僵尸网络或其他恶意软件攻击中涉及的端点计算机和命令与控制服务器之间的通信。
- 一旦发现病毒或其他安全隐患，就自动清除计算机。

  要了解有关更改自动清除设置的信息，请参见为读写扫描设置自动清除 （第 71 页）。
- 分析正在系统中运行的程序的行为。

  要了解更多信息，请参见行为监控 （第 80 页）。
- 在设定的时间扫描计算机。

  要了解更多信息，请参见创建计划扫描 （第 74 页）。

您可以对各组计算机进行不同的设置。要了解有关配置扫描设置的详细信息，请参阅以下主题：

- 配置读写扫描 （第 69 页）
- 为计划扫描配置扫描设置 （第 75 页）

注释
SophosLabs 可独立控制扫描哪些文件。为提供最佳的保护，它们可以添加或删除特定文件类型的扫描。

要了解不适用于 Mac，Linux 或 UNIX 计算机的扫描和清除选项的有关信息，请参见设置不适用于 Mac，Linux 或 UNIX （第 67 页）。

有关不适用于 Sophos Anti-Virus for VMware vShield 的扫描和清除选项的信息，请参见 Sophos 知识库文章 121745。对于 Sophos Anti-Virus for VMware vShield 版本 2.x，另请参见 Sophos Anti-Virus for VMware vShield 配置指南（可在 www.sophos.com/en-us/support/documentation/sophos-anti-virus-for-vmware-vshield 找到）。

7.1.1 设置不适用于 Mac，Linux 或 UNIX

在 Windows 计算机上，各种类型的扫描和清除，都可以从 Enterprise Console 全面管理，但是有一些设置不适用于 Mac，Linux 或 UNIX。

Mac OS X

更多有关适用于 Mac 的防病毒和 HIPS 策略设置的信息，请访问 Sophos 技术支持知识库文章 118859。

Linux

以下的自动清除选项不应用于 Linux 计算机，这些计算机将忽略它们。

读写扫描的自动清除设置：

- 拒绝访问并移至默认的路径
- 拒绝访问并移至

计划扫描的自动清除设置：

- 移至默认路径
- 移至

要了解更多有关自动清除设置的信息，请参见为计划扫描设置自动清除 （第 76 页）和计划扫描的自动清除设置 （第 77 页）。

更多有关适用于 Linux 计算机的防病毒和 HIPS 策略设置的信息，请访问 Sophos 技术支持知识库文章 117344。

UNIX

- Enterprise Console 无法在 UNIX 计算机上执行读写扫描。

  您可以从 Enterprise Console 统一配置计划扫描，警报发送，日志记录，以及更新。

  注释
  这些功能中包括一些不能通过 Enterprise Console 来设置的参数。您可以在各台 UNIX 计算机上，通过 Sophos Anti-Virus 命令行界面本地设置这些参数。Enterprise Console 会忽略它们。

  您也可以在各台 UNIX 计算机上，通过 Sophos Anti-Virus 命令行界面本地配置即时扫描。

  要了解更多有关本地设置附加的参数或配置 Sophos Anti-Virus for UNIX 的信息，请参见 Sophos Anti-Virus for UNIX 配置指南（英文）。

- 以下供计划扫描使用的自动清除选项不适用于 UNIX 计算机，这些计算机将忽略它们。

  — 移至默认路径

  — 移至

  要了解更多有关计划扫描的自动清除设置的信息，请参见计划扫描的自动清除设置 （第 77 页）。

更多有关应用于 UNIX 计算机的防病毒和 HIPS 策略设置的信息，请访问 Sophos 技术支持知识库文章 117344。

7.1.2 读写扫描

关于读写扫描的最佳保护

本节中提供的建议将帮助您获得读写扫描的最佳效果。

我们建议您使用默认的读写扫描设置，因为它在保护您的计算机免遭安全隐患的威胁与不影响整个计算机系统之间取得了最佳的平衡。要了解有关调整默认的读写扫描设置的详细建议，请参见 Sophos 技术支持知识库文章 114345 (http://www.sophos.com/zh-cn/support/knowledgebase/114345.aspx)（英文）。

我们建议您参见 Sophos Enterprise ConsoleSophos Enterprise Console 策略设置指南，寻求有关使用和管理 Sophos 安全软件的最佳使用方式的建议。Sophos 技术文档发布在 http://www.sophos.com/zh-cn/support/documentation 中。

配置读写扫描

如果您使用基于角色的管理，那么：

- 您必须具备 策略设置 - 防病毒和 HIPS 权限，才能执行此任务。
- 您不能编辑应用于您的活动子领域之外的策略。

要了解更多信息，请参阅 管理角色和子领域 （第 12 页）。

警告
如果安装了某些加密软件，那么，读写扫描可能会检测不到病毒。更改启动进程，确保在读写扫描开始时，加密的文件已被解密。要了解更多有关怎样针对加密软件使用防病毒和 HIPS 策略的信息，请参见 Sophos 技术支持知识库文章 （英文）。

要配置读写扫描：

1. 请检查您想要配置的计算机组采用了哪个防病毒和 HIPS 策略。
   请参阅查看组采用的策略 （第 23 页）。
2. 在 策略 窗格板中，双击 防病毒和 HIPS。
3. 双击您想要更改的策略。
   会出现 防病毒和 HIPS 策略 对话框。
4. 在 读写扫描 面板中的 启用读写扫描 旁，单击 配置。
5. 要更改进行读写扫描的时机，请在 检查文件的时机 中，按照以下说明设置选项。

选项	描述
读取	• 当文件被复制，移动，或打开时， 扫描文件。 • 当程序被启动时，扫描程序。
重命名	当文件被重新命名时，扫描文件。
写入	当保存，或创建文件时，扫描文件。

6. 在 扫描 下，按照以下说明设置选项。

选项	描述
广告软件和可能不想安装的应用程序	• 广告软件显示广告活动（例如：弹出消息），它会影响用户的工作效率和系统的运行效率。 • 可能不想安装的应用程序 (PUA) 不是恶意软件，但是通常被认为不适合在公司网络中使用。
可疑文件	可疑文件中会显示出恶意软件中通常共有的，但又不是独有的某些特征（例如：动态解压代码）。不过，凭这些特征而将某个文件识别为新的恶意软件，则还不够充分。 注释 此选项只应用于 Sophos Endpoint Security and Control for Windows。

7. 在 其它扫描选项 下，按照以下说明设置选项。

选项	描述
允许访问引导区受到感染的驱动器	允许访问被感染的，可以用于启动的移动介质，如：CD 启动盘，软盘，或者，USB 闪存。 只在 Sophos 技术支持的建议下才使用此选项。
扫描打包文件内部	在打包文件或压缩文件被下载到您的计算机之前，或者，从受管理的计算机中通过电子邮件发送出去之前，扫描它们的内容。 我们建议您关闭此选项，因为，它会显著增加扫描的时间。 用户将仍然受到保护，免遭打包文件或压缩文件中的任何安全隐患的威胁，因为，打包文件或压缩文件中的任何可能是恶意软件的组件，都会被读写扫描阻断： • 当用户打开解压缩自打包文件的文件时，该解压缩的文件会被扫描。 • 使用动态压缩工具，如：PKLite，LZEXE，以及 Diet 压缩的文件都会被扫描。
扫描系统内存	每小时运行一次的后台扫描，它可以检测隐藏在计算机系统内存（操作系统所使用的内存）中的恶意软件。

开启或关闭读写扫描

如果您使用基于角色的管理，那么：

- 您必须具备 策略设置 - 防病毒和 HIPS 权限，才能执行此任务。

- 您不能编辑应用于您的活动子领域之外的策略。

要了解更多信息，请参阅 管理角色和子领域 （第 12 页）。

依照默认值，Sophos Endpoint Security and Control 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。

要开启或关闭读写扫描：

1. 检查哪个防病毒和 HIPS 策略被您想要配置的一个或多个计算机组所采用了。
   请参阅查看组采用的策略 （第 23 页）。
2. 在 策略 窗格板中，双击 防病毒和 HIPS。然后，双击您想要更改的策略。
   会出现 防病毒和 HIPS 策略 对话框。
3. 在 读写扫描 面板中，勾选或取消勾选 启用读写扫描 勾选框。

重要提示
如果您关闭了服务器上的读写扫描，我们建议您在与该服务器相关的工作站上设置计划扫描。要了解怎样设置不同的策略，请参见创建计划扫描 （第 74 页）。

为读写扫描设置自动清除

如果您使用基于角色的管理，那么：

- 您必须具备 策略设置 - 防病毒和 HIPS 权限，才能执行此任务。
- 您不能编辑应用于您的活动子领域之外的策略。

要了解更多信息，请参阅 管理角色和子领域 （第 12 页）。

依照默认值，Sophos Endpoint Security and Control 在一旦发现病毒或其它安全隐患时，会自动清除计算机。您可以按照以下说明，更改自动清除的设置。

1. 请检查您想要配置的计算机组采用了哪个防病毒和 HIPS 策略。
   请参阅查看组采用的策略 （第 23 页）。
2. 在 策略 窗格板中，双击 防病毒和 HIPS。
3. 双击您想要更改的策略。
   会出现 防病毒和 HIPS 策略 对话框。
4. 在 读写扫描 面板中的 启用读写扫描 旁，单击 配置。
5. 在 读写扫描设置 对话框中，单击 清除 标签。
6. 请按照读写扫描的自动清除设置 （第 71 页）中的说明设置选项。

读写扫描的自动清除设置

病毒 / 间谍软件

勾选或取消勾选 自动清除项目中包含的病毒 / 间谍软件 勾选框。

您还可以指定如果清除失败，应该处置这些项目。

- 仅拒绝访问
- 删除
- 拒绝访问并移至默认的路径

- 拒绝访问并移至（输入完整的 UNC 路径）

注释
拒绝访问并移至默认的路径 和 拒绝访问并移至 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

注释
这些设置仅应用于 Windows 计算机。

您可以指定如果检测到了可疑文件，应该处置它们。

- 仅拒绝访问
- 删除
- 拒绝访问并移至默认的路径
- 拒绝访问并移至（输入完整的 UNC 路径）

指定读写扫描文件扩展名

如果您使用基于角色的管理，那么：

- 您必须具备 策略设置 - 防病毒和 HIPS 权限，才能执行此任务。
- 您不能编辑应用于您的活动子领域之外的策略。

要了解更多信息，请参阅 管理角色和子领域 （第 12 页）。

您可以指定进行读写扫描时，扫描的文件扩展名。

1. 请检查您想要配置的计算机组采用了哪个防病毒和 HIPS 策略。
   请参阅查看组采用的策略 （第 23 页）。
2. 在策略窗格中，双击防病毒和 HIPS。
3. 双击您想要更改的策略。
   会出现 防病毒和 HIPS 策略 对话框。
4. 在 读写扫描 面板中的 启用读写扫描 旁，单击 配置。
5. 单击 扩展名 标签页，然后，按照以下说明配置选项。

选项	描述
扫描所有文件	扫描所有的文件，无论文件扩展名是什么。如果您开启此选项，那么，扩展名 标签页中的其它选项会被关闭。 扫描所有文件将会影响计算机的运行效率，所以，我们建议您仅仅在每周一次的计划扫描中开启此选项。
只扫描可执行文件和其它薄弱文件	• 检查所有带有可执行文件的扩展名（例如：.exe, .bat, .pif）的文件，或者，有可能被感染的文件（例如：.doc, .chm, .pdf）。

选项	描述
	• 快速检查所有文件的结构，如果它们的格式是某种可执行文件，则扫描它们。
扫描附加的文件类型扩展名	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。您可以使用通配符 ？ 替代任何单一的字符。 要停止扫描某种文件类型，请在列表中选择它的扩展名，然后，单击 删除。 要更改某种文件类型，请在列表中选择它的扩展名，然后，单击 编辑。
扫描不带扩展名的文件	不带扩展名的文件可能是恶意软件，所以，我们建议您保留开启此选项。
排除	要从读写扫描中排除指定的文件类型，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。 要开始扫描某种文件类型，请在列表中选择它的扩展名，然后，单击 删除。 要更改某种文件类型，请在列表中选择它的扩展名，然后，单击 重命名。

从读写扫描中排除项目

如果您使用基于角色的管理，那么：

- 您必须具备 策略设置 - 防病毒和 HIPS 权限，才能执行此任务。
- 您不能编辑应用于您的活动子领域之外的策略。

要了解更多信息，请参阅 管理角色和子领域 （第 12 页）。

您可以排除要进行读写扫描的项目。

注释
这些选项只应用于 Windows，Mac OS X，以及 Linux。

Enterprise Console 无法在 UNIX 计算机上执行读写扫描。

1. 请检查您想要配置的计算机组采用了哪个防病毒和 HIPS 策略。
   请参阅查看组采用的策略 （第 23 页）。
2. 在 策略 窗格板中，双击 防病毒和 HIPS。然后，双击您想要更改的策略。
   会出现 防病毒和 HIPS 策略 对话框。
3. 在 读写扫描 面板中，单击 配置 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。请参阅可以从扫描中排除的项目 （第 88 页）。

要排除扫描没有存储在本地驱动器上的文件，请勾选 排除远程文件 勾选框。如果您想要加快访问此类文件的速度，并且您信任所提供的远程文件的来源，您可以勾选此选项。

重要提示
如果您选择 Windows 排除项目 标签页中的 排除远程文件，那么，数据控制将不会扫描使用受监控的应用程序（例如：电子邮件客户端，网页浏览器，或者，即时消息 (IM) 客户端）从网络路径中上传或附带的文件。这是因为数据控制使用 Sophos Anti-Virus 读写扫描器 (InterCheck ™) 所使用的同一组排除文件。如果禁用了远程文件扫描，那么，不会有任何远程文件发送给数据控制进行检查。此限制不应用于存储设备监控。

您可以将 Windows 排除项目列表导出到某个文件中，然后，将它导入到另外的策略中。要了解更多信息，请参见导入或导出读写扫描排除项目 （第 74 页）。

导入或导出读写扫描排除项目

如果您使用基于角色的管理，那么：

- 您必须具备 策略设置 - 防病毒和 HIPS 权限，才能执行此任务。
- 您不能编辑应用于您的活动子领域之外的策略。

要了解更多信息，请参阅 管理角色和子领域 （第 12 页）。

您可以将供读写扫描使用的 Windows 排除项目导出到某个文件中，然后，将它导入到另一个策略中。

1. 请检查您想要配置的计算机组采用了哪个防病毒和 HIPS 策略。
   请参阅查看组采用的策略 （第 23 页）。
2. 在 策略 窗格板中，双击 防病毒和 HIPS。
3. 双击您想要更改的策略。
   会出现 防病毒和 HIPS 策略 对话框。
4. 在 读写扫描 面板中的 启用读写扫描 旁，单击 配置。
5. 在 Windows 排除项目 标签页中，单击 导出 或 导入。

7.1.3 即时扫描和计划扫描

在防病毒和 HIPS 策略的即时扫描面板中，可以：

- 设置计划扫描。
- 配置扫描选项，如单个计算机上所有即时扫描类型（计划扫描、整个系统扫描和默认的即时扫描）的扩展项和排除项。

创建计划扫描

如果您使用基于角色的管理，那么：

- 您必须具备 策略设置 - 防病毒和 HIPS 权限，才能执行此任务。
- 您不能编辑应用于您的活动子领域之外的策略。

要了解更多信息，请参阅 管理角色和子领域 （第 12 页）。

为了使 Sophos Endpoint Security and Control 能够按照设定的时间扫描计算机，您可以创建计划扫描。

1. 请检查您想要配置的计算机组采用了哪个防病毒和 HIPS 策略。
   请参阅查看组采用的策略 （第 23 页）。

2. 在策略窗格中，双击防病毒和 HIPS。
3. 双击您想要更改的策略。
   会出现 防病毒和 HIPS 策略 对话框。
4. 在即时扫描面板中的设置和管理计划扫描下，单击添加。
   会出现 计划扫描设置 对话框。
5. 在 扫描名称 文本框中，输入扫描的名称。
6. 在 需要扫描 下， 勾选要扫描的项目。依照默认值，会扫描所有的本地硬盘，以及 UNIX 挂载的文件系统。
7. 在 扫描时机 下，勾选运行扫描的时间。
8. 要指定运行扫描的时间，单击 添加。
   - 要更改时间，请在 运行扫描的时间 列表中选择要更改的时间，然后，单击 编辑。
   - 要删除时间，请在 运行扫描的时间 列表中选择要删除的时间，然后，单击 删除。

注释
如果扫描检测到内存中有安全隐患的组件，并且您尚未设置为扫描进行自动清除，那么，扫描会中止，并有警报发送到 Enterprise Console。这是因为继续扫描，有可能会扩散安全隐患。您必须在清除该安全隐患之后，再运行扫描。

要更改扫描和清除设置，请参阅以下主题：

- 为计划扫描配置扫描设置 （第 75 页）
- 为读写扫描设置自动清除 （第 71 页）

为计划扫描配置扫描设置

如果您使用基于角色的管理，那么：

- 您必须具备 策略设置 - 防病毒和 HIPS 权限，才能执行此任务。
- 您不能编辑应用于您的活动子领域之外的策略。

要了解更多信息，请参阅 管理角色和子领域 （第 12 页）。

要为计划扫描配置扫描设置：

1. 请检查您想要配置的计算机组采用了哪个防病毒和 HIPS 策略。
   请参阅查看组采用的策略 （第 23 页）。
2. 在策略窗格中，双击防病毒和 HIPS。
3. 双击您想要更改的策略。
   会出现 防病毒和 HIPS 策略 对话框。
4. 在 设置和管理计划扫描 列表中，选择扫描，然后，单击 编辑。
5. 在 计划扫描设置 对话框，单击 配置。
6. 在 扫描 下，按照以下说明配置设置。

选项	描述
广告软件和可能不想安装的应用程序	• 广告软件显示广告活动（例如：弹出消息），它会影响用户的工作效率和系统的运行效率。 • 可能不想安装的应用程序 (PUA) 不是恶意软件，但是通常被认为不适合在公司网络中使用。

选项	描述
可疑文件	可疑文件中会显示出恶意软件中通常共有的，但又不是独有的某些特征（例如：动态解压代码）。不过，凭这些特征而将某个文件识别为新的恶意软件，则还不够充分。 注释 此选项只应用于 Sophos Endpoint Security and Control for Windows。
Rootkit	Rootkit 是一种特洛伊木马或类似的技术，它用来隐藏恶意的对象（进程，文件，注册键，或网络端口），避免计算机用户或系统管理员发现它们。

7. 在 其它扫描选项 下，按照以下说明设置选项。

选项	描述
扫描打包文件内部	扫描打包文件和其它压缩文件的内容。 我们不建议您在计划扫描中扫描打包文件内部，因为它会显著增加扫描所需的时间。在这种情况下，我们建议使用读写扫描（在读和写文件时）来保护您的网络。未解压的打包文件中的任何恶意软件组件，都会在被访问时，被读写扫描程序阻断。 如果您想要使用计划扫描，在少许的计算机上扫描所有的打包文件，我们建议您按照以下说明做： • 创建一个额外的计划扫描。 • 在配置 > 即时扫描设置对话框的扩展名选项卡上，只将存档文件扩展名添加到要扫描的扩展名列表中。 • 请确保 扫描所有文件 是禁用的。 这将使您在扫描打包文件时，扫描所花费的时间尽量地短。
扫描系统内存	检测隐藏在计算机系统内存（操作系统所使用的内存）中的恶意软件。
以较低的优先级运行扫描	在 Windows Vista 及以上的操作系统中，以较低的优先级运行计划扫描，以便最大限度地降低对用户应用程序运行效率的影响。

要了解有关为计划扫描更改默认扫描设置的详细建议，请参见Sophos 知识库文章 63985。

为计划扫描设置自动清除

如果您使用基于角色的管理，那么：

- 您必须具备 策略设置 - 防病毒和 HIPS 权限，才能执行此任务。
- 您不能编辑应用于您的活动子领域之外的策略。

要了解更多信息，请参阅 管理角色和子领域 （第 12 页）。

依照默认值，Sophos Endpoint Security and Control 在一旦发现病毒或其它安全隐患时，会自动清除计算机。您可以按照以下说明，更改自动清除的设置。

1. 请检查您想要配置的计算机组采用了哪个防病毒和 HIPS 策略。
   请参阅查看组采用的策略 （第 23 页）。
2. 在 策略 窗格板中，双击 防病毒和 HIPS。
3. 双击您想要更改的策略。
   会出现 防病毒和 HIPS 策略 对话框。
4. 在 设置和管理计划扫描 列表中，选择扫描，然后，单击 编辑。
5. 在 更改扫描和清除设置 旁，单击 配置。
   会出现 扫描和清除设置 对话框。
6. 单击 清除 标签。
7. 请按照读写扫描的自动清除设置 （第 71 页）中的说明设置选项。

计划扫描的自动清除设置

病毒 / 间谍软件

勾选或取消勾选 自动清除项目中包含的病毒 / 间谍软件 勾选框。

您还可以指定如果清除失败，应该处置这些项目。

- 仅记录
- 删除
- 移至默认路径
- 移至（输入完整的 UNC 路径）

注意

- 移走可执行文件，可以减少它们被运行的机会。
- 您无法自动移动多组件感染中的组件。

广告软件和可能不想安装的应用程序 (PUA)

选择 自动清除广告软件和可能不想安装的应用程序。

注意

- 此设置仅应用于 Windows 计算机。

可疑文件

您可以指定如果检测到了可疑文件，应该处置它们。

- 仅记录
- 删除

- 移至默认路径
- 移至（输入完整的 UNC 路径）

注意

- 这些设置仅应用于 Windows 计算机。
- 移走可执行文件，可以减少它们被运行的机会。
- 您无法自动移动多组件感染中的组件。

指定即时扫描和计划扫描的文件扩展名

如果您使用基于角色的管理，那么：

- 您必须具备 策略设置 - 防病毒和 HIPS 权限，才能执行此任务。
- 您不能编辑应用于您的活动子领域之外的策略。

要了解更多信息，请参阅 管理角色和子领域 （第 12 页）。

可以指定进行即时扫描和计划扫描时扫描的文件扩展名。

1. 请检查您想要配置的计算机组采用了哪个防病毒和 HIPS 策略。
   请参阅查看组采用的策略 （第 23 页）。
2. 在策略窗格中，双击防病毒和 HIPS。
3. 双击您想要更改的策略。
   会出现 防病毒和 HIPS 策略 对话框。
4. 在即时扫描面板中，单击配置。
   会出现 按需扫描设置 对话框。
5. 在 扩展名 标签页中，按照以下说明配置选项。

选项	描述
扫描所有文件	扫描所有的文件，无论文件扩展名是什么。如果您开启此选项，那么，扩展名 标签页中的其它选项会被关闭。 扫描所有文件将会影响计算机的运行效率，所以，我们建议您仅仅在每周一次的计划扫描中开启此选项。
只扫描可执行文件和其它薄弱文件	• 检查所有带有可执行文件的扩展名（例如：.exe，.bat，.pif）的文件，或者，有可能被感染的文件（例如：.doc，.chm，.pdf）。 • 快速检查所有文件的结构，如果它们的格式是某种可执行文件，则扫描它们。
扫描附加的文件类型扩展名	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。您可以使用通配符 ？ 替代任何单一的字符。 要停止扫描某种文件类型，请在列表中选择它的扩展名，然后，单击 删除。 要更改某种文件类型，请在列表中选择它的扩展名，然后，单击 编辑。

选项	描述
扫描不带扩展名的文件	不带扩展名的文件可能是恶意软件，所以，我们建议您保留开启此选项。
排除	要从计划扫描中排除指定的文件类型，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。 要开始扫描某种文件类型，请在列表中选择它的扩展名，然后，单击 删除。 要更改某种文件类型，请在列表中选择它的扩展名，然后，单击 重命名。

要了解有关为计划扫描配置扩展名设置的详细建议，请参阅 Sophos 技术支持知识库文章 63985 （英文）。

从即时扫描和计划扫描中排除项目

如果您使用基于角色的管理，那么：

- 您必须具备 策略设置 - 防病毒和 HIPS 权限，才能执行此任务。
- 您不能编辑应用于您的活动子领域之外的策略。

要了解更多信息，请参阅 管理角色和子领域 （第 12 页）。

可以从即时扫描和计划扫描中排除项目。

注释
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”。请参阅立即扫描计算机 （第 45 页）。

1. 请检查您想要配置的计算机组采用了哪个防病毒和 HIPS 策略。
   请参阅查看组采用的策略 （第 23 页）。
2. 在策略窗格中，双击防病毒和 HIPS。然后，双击您想要更改的策略。
3. 会出现 防病毒和 HIPS 策略 对话框。在即时扫描面板中，单击配置。
4. 单击 Windows 排除项目，Linux/UNIX 排除项目，或 Mac 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。请参阅可以从扫描中排除的项目 （第 88 页）。

您可以将 Windows 排除项目列表导出到某个文件中，然后，将它导入到另外的策略中。要了解更多信息，请参见导入或导出读写扫描排除项目 （第 74 页）。

导入或导出即时扫描和计划扫描的 Windows 排除项目

如果您使用基于角色的管理，那么：

- 您必须具备 策略设置 - 防病毒和 HIPS 权限，才能执行此任务。
- 您不能编辑应用于您的活动子领域之外的策略。

要了解更多信息，请参阅 管理角色和子领域 （第 12 页）。

可以将即时扫描和计划扫描的 Windows 排除项目导出到文件，然后导入到其他策略中。

1. 请检查您想要配置的计算机组采用了哪个防病毒和 HIPS 策略。
   请参阅查看组采用的策略 （第 23 页）。
2. 在策略窗格中，双击防病毒和 HIPS。
3. 双击您想要更改的策略。
   会出现 防病毒和 HIPS 策略 对话框。
4. 在即时扫描面板中，单击配置。
5. 在 Windows 排除项目 标签页中，单击 导出 或 导入。

7.1.4 行为监控

作为读写扫描的一部分，Sophos Behavior Monitoring 保护 Windows 计算机免遭未被识别的或“零天”安全隐患，以及可疑行为的威胁。

运行时检测可以中止那些在执行前无法检测到的安全隐患。行为监控使用以下的运行时检测的方法中止安全隐患：

- 恶意和可疑行为检测
- 恶意数据流检测
- 缓冲区溢出检测

恶意和可疑行为检测

可疑行为检测，通过 Sophos 的主机入侵防范系统 (HIPS)，动态地分析所有在计算机上运行的程序，以检测并阻断可能带有恶意的程序活动。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。

可疑行为检测会监测所有系统进程中恶意软件的活动迹象，如：可疑的注册表写入操作，或文件复制操作等。可以设置提醒管理员和/或阻断进程。

恶意行为检测，可以对所有运行在计算机上的程序进行动态分析，以检测并阻断已知的恶意行为。

恶意数据流检测

恶意数据流检测可以检测僵尸网络或其他恶意软件攻击中涉及的端点计算机和命令与控制服务器之间的通信。

注释
恶意数据流检测需要启用 Sophos Live Protection，以便执行查找和获取数据。（默认情况下，Sophos Live Protection 处于启用状态。）

缓冲区溢出检测

缓冲区溢出检测对于处理当天最新出现的安全隐患很重要。

它可以动态地分析正在系统中运行的程序的行为，以便及时检测到使用缓冲区溢出手段利用正在运行的进程的企图。它可以捕捉针对操作系统软件和应用程序软件中的安全漏洞发起的攻击。

开启或关闭行为监控

如果您使用基于角色的管理，那么：

- 您必须具备 策略设置 - 防病毒和 HIPS 权限，才能执行此任务。
- 您不能编辑应用于您的活动子领域之外的策略。

要了解更多信息，请参阅 管理角色和子领域 （第 12 页）。

默认情况下，行为监控是启用的。

要开启或关闭行为监控：

1. 检查哪个防病毒和 HIPS 策略被您想要配置的一个或多个计算机组所采用了。
   请参阅查看组采用的策略 （第 23 页）。
2. 在 策略 窗格板中，双击 防病毒和 HIPS。
3. 双击您想要更改的策略。
   会出现 防病毒和 HIPS 策略 对话框。
4. 在读写扫描面板中，勾选或取消勾选启用行为监控复选框。

检测恶意行为

如果您使用基于角色的管理，那么：

- 您必须具备 策略设置 - 防病毒和 HIPS 权限，才能执行此任务。
- 您不能编辑应用于您的活动子领域之外的策略。

要了解更多信息，请参阅 管理角色和子领域 （第 12 页）。

恶意行为检测，是对所有运行在计算机上的程序进行动态分析，以检测并阻断已知的恶意行为。

默认情况下，恶意行为检测是启用的。

要更改检测和报告恶意行为的设置：

1. 检查哪个防病毒和 HIPS 策略被您想要配置的一个或多个计算机组所采用了。
   请参阅查看组采用的策略 （第 23 页）。
2. 在 策略 窗格板中，双击 防病毒和 HIPS。
3. 双击您想要更改的策略。
   会出现 防病毒和 HIPS 策略 对话框。
4. 在读写扫描面板中，确保勾选启用行为监控复选框。
5. 在 启用行为监控 旁，单击 配置。
6. 在 配置行为监控 对话框中：
   - 要提醒管理员，并阻断恶意行为，请勾选 检测恶意行为 勾选框。
   - 要禁用恶意行为检测，请取消勾选检测恶意行为复选项。

   注释
   如果禁用恶意行为检测，可疑行为检测也将禁用。请注意，恶意数据流检测将不会禁用。

检测恶意数据流

如果您使用基于角色的管理，那么：

- 您必须具备 策略设置 - 防病毒和 HIPS 权限，才能执行此任务。
- 您不能编辑应用于您的活动子领域之外的策略。

  要了解更多信息，请参阅 管理角色和子领域 （第 12 页）。

- 恶意数据流检测需要启用 Sophos Live Protection。（默认情况下，Sophos Live Protection 处于启用状态。）

恶意数据流检测可以检测僵尸网络或其他恶意软件攻击中涉及的端点计算机和命令与控制服务器之间的通信。

注释
恶意数据流检测使用相同的排除设置作为 Sophos Anti-Virus 读写扫描器 (InterCheck ™)。要了解更多有关配置读写扫描排除文件的信息，请参见从读写扫描中排除项目 （第 73 页）。

默认情况下，新安装的 Enterprise Console 5.3 或之后版本会启用恶意数据流检测。如果从之前版本的 Enterprise Console 升级，则需要启用恶意数据流检测以使用该功能。

要更改用于检测恶意数据流的设置：

1. 检查哪个防病毒和 HIPS 策略被您想要配置的一个或多个计算机组所采用了。
   请参阅查看组采用的策略 （第 23 页）。
2. 在策略窗格中，双击防病毒和 HIPS。
3. 双击您想要更改的策略。
   会出现 防病毒和 HIPS 策略 对话框。
4. 在读写扫描面板中，确保勾选启用行为监控复选框。
5. 在 启用行为监控 旁，单击 配置。
6. 在配置行为监控对话框中，确保勾选检测恶意行为复选框。
7. 要开启或关闭恶意行为检测，请选中或取消勾选检测可疑数据流复选框。

检测可疑行为

如果您使用基于角色的管理，那么：

- 您必须具备 策略设置 - 防病毒和 HIPS 权限，才能执行此任务。
- 您不能编辑应用于您的活动子领域之外的策略。

要了解更多信息，请参阅 管理角色和子领域 （第 12 页）。

可疑行为检测会监测所有系统进程中恶意软件的活动迹象，如：可疑的注册表写入操作，或文件复制操作等。可以设置提醒管理员和/或阻断进程。

默认情况下，会检测并报告可疑行为，但不阻止。

要更改检测和报告可疑行为的设置：

1. 检查哪个防病毒和 HIPS 策略被您想要配置的一个或多个计算机组所采用了。
   请参阅查看组采用的策略 （第 23 页）。
2. 在 策略 窗格板中，双击 防病毒和 HIPS。
3. 双击您想要更改的策略。
   会出现 防病毒和 HIPS 策略 对话框。
4. 在读写扫描面板中，确保勾选启用行为监控复选框。
5. 在 启用行为监控 旁，单击 配置。
6. 在配置行为监控对话框中，确保勾选检测恶意行为复选框。
   - 要提醒管理员，并阻止可疑进程，请勾选检测可疑行为复选框，并取消勾选仅限警报，但不阻止可疑行为复选框。
   - 要提醒管理员，但不阻止可疑进程，请勾选检测可疑行为复选框和仅限警报，但不阻止可疑行为复选框。

为了获得最可靠的保护，我们建议您启用可疑文件检测。请参阅配置读写扫描 （第 69 页）。

检测缓冲区溢出

如果您使用基于角色的管理，那么：

- 您必须具备 策略设置 - 防病毒和 HIPS 权限，才能执行此任务。
- 您不能编辑应用于您的活动子领域之外的策略。

要了解更多信息，请参阅 管理角色和子领域 （第 12 页）。

缓冲区溢出检测可以动态地分析正在系统中运行的程序的行为，以便及时检测到使用缓冲区溢出手段利用正在运行的进程的企图。

默认情况下，会检测和阻止缓冲区溢出。

要更改检测和报告缓冲区溢出攻击的设置：

1. 检查哪个防病毒和 HIPS 策略被您想要配置的一个或多个计算机组所采用了。
   请参阅查看组采用的策略 （第 23 页）。
2. 在 策略 窗格板中，双击 防病毒和 HIPS。
3. 双击您想要更改的策略。
   会出现 防病毒和 HIPS 策略 对话框。
4. 在读写扫描面板中，确保勾选启用行为监控复选框。
5. 在 启用行为监控 旁，单击 配置。在 配置行为监控 对话框中：
   - 要提醒管理员，并阻断缓冲区溢出，请勾选 检测缓冲区溢出 勾选框，并取消勾选 仅限警报，但不阻断 勾选框。
   - 要提醒管理员，但并不阻断缓冲区溢出，请同时勾选 检测缓冲区溢出 勾选框，和 仅限警报，但不阻断 勾选框。

7.1.5 Sophos Live Protection

Sophos Live Protection 使用云计算技术，不断地判断可疑文件是否成为安全隐患，并随时采取在“防病毒和 HIPS”策略中所指定的措施。

Sophos Live Protection 可以显著提高对新出现的恶意软件的检出率，同时也不会做无谓的检测活动。能够做到这一点，是因为能够随时比对最新的已知的恶意软件。一旦确认了新的恶意软件，Sophos 即可立即发出更新文件。

要充分利用 Sophos Live Protection 的优势，您必须确保启用了以下选项。

- 启用 Live Protection

  如果端点计算机上的即时扫描发现某个文件可疑，但无法根据存储在计算机上的威胁识别文件 (IDE) 进一步确定该文件中是否有恶意代码，将把某些文件特征（如校验和）发送给 Sophos 进行进一步分析。云计算检查会在 SophosLabs 数据库中迅速查看可疑文件。如果该文件被确定为有害的，或无害的，此信息会被发送回计算机，并且此文件的状态会被自动更新。

  重要提示
  恶意数据流检测和下载信誉功能需要启用 Live Protection，以便在 SophosLabs 在线数据库中执行即时查找，并获取最新的威胁或信誉数据。

- 针对即时扫描的 Live Protection

  如果要让即时扫描使用与读写扫描相同的云计算检查，请选中此选项。

- 自动发送文件样本给 Sophos

如果某个文件肯定会有恶意行为，但是却又不能仅仅根据其特征就肯定地确认它具有恶意代码，那么，Sophos Live Protection 会响应 Sophos 对此文件的样本的请求。启用 Live Protection 后，如果启用此选项，并且 Sophos 尚未具有该文件的样本，将自动提交该文件。

提交类似的样本文件，有助于 Sophos 不断增强检测恶意软件的能力，并且降低误报的几率。

注释
样本的最大容量为 10 MB。样本上传的超时时限为 30 秒。不建议通过低速连接（低于 56 Kbps）自动发送样本。

重要提示
您必须确保在网页过滤方案中将 Sophos 的域名设置为“信任的”，文件数据将会被寄往该域名。要了解详情，请参见技术支持知识库文章 62637 (http://www.sophos.com/zh-cn/support/knowledgebase/62637.aspx)。

如果您使用的是 Sophos 的网页过滤方案，例如，WS1000 Web Appliance，那么，您不必进行任何操作 — Sophos 的域名已经是受信任的域名。

开启或关闭 Sophos Live Protection

如果您使用基于角色的管理，那么：

- 您必须具备 策略设置 - 防病毒和 HIPS 权限，才能执行此任务。
- 您不能编辑应用于您的活动子领域之外的策略。

要了解更多信息，请参阅 管理角色和子领域 （第 12 页）。

Sophos Live Protection 根据 SophosLabs 数据库中的最新信息检查可疑文件。

默认情况下，Live Protection 会向 Sophos 发送用于检查的文件数据（如校验和），但不会发送用于分析的样本文件。为充分利用 Live Protection，应选中发送样本文件的选项。

要开启或关闭 Live Protection 选项：

1. 检查哪个防病毒和 HIPS 策略被您想要配置的一个或多个计算机组所采用了。
   请参阅查看组采用的策略 （第 23 页）。
2. 在策略窗格中，双击防病毒和 HIPS。然后，双击您想要更改的策略。
3. 在防病毒和 HIPS 策略对话框中，单击 Sophos Live Protection 按钮。
4. 在 Sophos Live Protection 对话框中：
   - 选中或清除启用 Live Protection 复选框。将开启或关闭 Live Protection 的即时扫描功能。

     重要提示
     恶意数据流检测和下载信誉功能需要启用 Live Protection，以便在 SophosLabs 在线数据库中执行即时查找，并获取最新的威胁或信誉数据。

   - 选中或清除启用 Live Protection 的即时扫描功能复选框。将开启或关闭 Live Protection 的即时扫描功能。
   - 选中或清除自动发送文件样本给 Sophos 复选框。
     样本仅在启用 Live Protection 时才会发送。

注释
向 Sophos 发送文件样本进行在线扫描时，总是将文件数据（校验和等）同样本一起发送。

7.1.6 Web 保护

网页防范能加强对网页中的安全隐患的防范。它有以下功能：

- 实时 URL 筛选
- 扫描下载的内容
- 检查下载文件的信誉

实时 URL 筛选

实时 URL 筛选可以阻断对已知的带有恶意软件的网站的访问。此功能通过实时比对 Sophos 的感染网站在线数据库来实现。

注释
如果您想要进一步控制用户能够访问的网站，比如，您想要杜绝用户访问某些网站，以便避免公司为此担负法律责任，请使用“网页控制”功能。要了解更多信息，请参见网页控制策略 （第 145 页）。

内容扫描

内容扫描可以扫描从因特网（或内部网）下载的数据和文件，并预先检测恶意内容。此功能可以扫描来自所有网站的内容，包括那些并没有在感染网站在线数据库的列表中的网站的内容。

下载信誉

下载信誉按文件的时间、来源、普遍性、深度内容分析和其他特征进行计算。

注释
下载信誉仅在 Windows 7 及更高版本上得到支持。

默认情况下，当您尝试下载低信誉或未知信誉的文件时，将显示警报。我们建议您不要下载此类文件。如果您信任文件的来源和发布者，您可以选择下载该文件。您的操作和文件的 URL 将记录在扫描日志中。

注释
下载信誉是根据 SophosLabs 的云端数据库中的数据进行计算的，需要启用 Sophos Live Protection 才能执行查找和获得该数据。（默认情况下，Sophos Live Protection 处于启用状态。）

有关下载信誉的详细信息，请参阅知识库文章 121319。

Web 保护配置设置

默认情况下，Web 保护处于启用状态：会阻止对恶意网站的访问、扫描下载内容并检查下载文件的信誉。

有关 Web 保护设置及其更改方法的详细信息，请参见配置 Web 保护选项 （第 86 页）。

支持的 Web 浏览器

网页防范功能支持以下的网页浏览器：

- IE
- Edge
- Google Chrome
- Firefox（除下载信誉外）
- Safari（除下载信誉外）
- Opera

通过不受支持的网页浏览器访问的网页内容不会被过滤，也不会被阻断。

Web 保护事件

当阻断了对某恶意网站的访问时，会在日志记录中记录该事件，并且可以通过“网页事件查看器”查看，也可以在发生事件的那台端点计算机上的 计算机详情 中查看。如果您使用“网页控制”功能，那么，网页防范事件和网页控制事件都会出现在“网页事件查看器”和 计算机详情 中。请参阅查看网页事件 （第 167 页） 和 查看计算机上最新的网页事件 （第 168 页）。

配置 Web 保护选项

如果您使用基于角色的管理，那么：

- 您必须具备 策略设置 - 防病毒和 HIPS 权限，才能执行此任务。
- 您不能编辑应用于您的活动子领域之外的策略。

要了解更多信息，请参阅 管理角色和子领域 （第 12 页）。

要开启或关闭网页防范：

1. 检查哪个防病毒和 HIPS 策略被您想要配置的一个或多个计算机组所采用了。
   请参阅查看组采用的策略 （第 23 页）。
2. 在策略窗格中，双击防病毒和 HIPS。
3. 双击您想要更改的策略。
4. 在 防病毒和 HIPS 策略 对话框中，单击 网页保护 按钮。
5. 在 Web 保护对话框的恶意软件防护下，选中阻止访问恶意网站旁边的开启或关闭，以阻止或不阻止访问恶意网站。此选项默认为启用。
   要了解有关怎样批准特定的网站的信息，请参见批准网站 （第 93 页）。
6. 要启用或禁用对下载数据和文件的扫描，请在内容扫描旁边，选择在读写扫描时、开或关。
   默认情况下，在读写文件时是选中的，下载扫描的禁用或启用是与读写扫描同步改变的。

7. 要更改用户尝试下载低信誉或未知信誉的文件时的操作，请在下载信誉下的操作旁边，选择提示用户（默认）或仅记录。

   注释
   下载信誉需要启用 Sophos Live Protection。（默认情况下，Sophos Live Protection 处于启用状态。）

   - 如果选择提示用户，每次用户尝试下载低信誉文件时，将会显示警报告知您这种情况，并让您确定是阻止还是允许下载。我们建议用户不要下载此类文件。如果他们信任文件的来源和发布者，可以选择下载该文件。阻止或允许该下载的选择，以及文件的 URL 都将记录在扫描日志中，并在 Enterprise Console 中记录为 Web 事件。
   - 如果选择只记录，将不会显示任何警报，下载将被允许并记录在扫描日志中，并在 Enterprise Console 中记录为 Web 事件。

8. 要选择信誉扫描的严格程度，请在阈值旁边，选择推荐（默认）或严格。
   - 如果选择推荐，每次用户尝试下载低信誉或未知信誉的文件时，将显示警报并/或创建日志记录，并创建事件。
   - 如果选择严格，每次用户尝试下载低信誉、未知信誉或中等信誉的文件时，将显示警报并/或创建日志记录，并创建事件。

7.1.7 扫描的文件类型和排除项目

依照默认值，Sophos Endpoint Security and Control 会对各种容易被病毒感染的文件类型进行扫描。默认扫描的文件类型，不仅在不同的操作系统上会有所不同，并且在软件产品更新后，也会发生改变。

要查看默认扫描的文件类型列表，请在相应的操作系统的计算机上，打开 Sophos Endpoint Security and Control 或 Sophos Anti-Virus，然后，找到“扩展名”配置页面。

您可以选择扫描附加的文件类型或排除扫描某些文件。

Windows

要查看 Windows 计算机上的默认扫描的文件类型的列表：

1. 打开 Sophos Endpoint Security and Control。
2. 在 防病毒和 HIPS 下，单击 配置防病毒和 HIPS，然后，单击 即时扫描文件扩展名和排除文件。

要了解有关在 Windows 计算机上扫描附加的文件类型，或者，排除扫描某些文件的信息，请参阅以下主题：

- 指定读写扫描文件扩展名 （第 72 页）
- 指定即时扫描和计划扫描的文件扩展名 （第 78 页）

Mac OS X

Sophos Anti-Virus for Mac OS X 在进行读写扫描时会扫描所有文件的扩展名。要更改计划扫描的设置，请参见指定即时扫描和计划扫描的文件扩展名 （第 78 页）。

Linux 或 UNIX

要在 Linux 计算机上进行更改，请使用 savconfig 和 savscan 命令，说明请参见 Sophos Anti-Virus for Linux configuration guide （英文）。

要在 UNIX 计算机上进行更改，请使用 savscan 命令，说明请参阅 Sophos Anti-Virus for UNIX configuration guide （英文）。

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

在 Windows 计算机中，您可以排除驱动器，文件夹，文件和进程。

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。

Mac OS X

在 Mac OS X 计算机中，您可以排除文件，文件夹，以及卷。

您可以在要排除的项目加上“/”作为前缀，或者加上“/”作为后缀来排除该项目，或者，您可以加上“//”作为后缀来排除该项目。

要了解更多信息，请参阅 Sophos Anti-Virus for Mac OS X Help （英文）。

Linux 或 UNIX

在 Linux 和 UNIX 计算机上，您可以排除目录和文件。

您指定任何 POSIX 路径，无论它是文件，还是目录，例如：/folder/file.您可以使用通配符 ? 和 *。

注释

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。要了解有关怎样操作的信息，请参见 Sophos Anti-Virus for Linux 配置指南或 Sophos Anti-Virus for UNIX 配置指南。

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。

要了解有关从扫描中排出项目的信息，请参阅以下主题：

- 从读写扫描中排除项目 （第 73 页）

- 从即时扫描和计划扫描中排除项目 （第 79 页）

为 Windows 计算机指定扫描排除项目

标准命名协定

Sophos Anti-Virus 会根据标准的 Windows 命名协定，校验扫描排除项目的文件名和路径。例如，某个文件夹名可以使用空格，但是不能仅仅是空格。

多重文件扩展名

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

MySample.txt.doc = 文件名 MySample.txt + 扩展名 .doc。

排除特定的文件、文件夹或驱动器

排除类型	描述	示例	注释
特定的文件	同时指定文件名和路径，才能排除特定的文件。路径中可以包含驱动器盘符或网络共享名。	C:\Documents\CV.doc \\Server\Users\Documents\CV.doc	要确保排除项目能够正确地找到，请添加长文件名或文件夹名，以及 8.3 文件名和文件夹名(8.3-compliant file and folder names)： C:\Program Files\Sophos\Sophos Anti-Virus C:\Progra~1\Sophos\Sophos~1 有关详细信息，请参阅知识库文章 13045。
名称相同的所有文件	指定不带路径的文件名，可以排除文件系统中所有路径中以该名字命名的所有文件。	spacer.gif	

排除类型	描述	示例	注释
驱动器或网络共享中的所有文件	指定驱动器盘符，或网络共享，可以排除驱动器或网络共享上的所有文件。	D: \\Server \<sharename>\	指定网络共享时，请在共享名后包括末尾的斜杠。
特定的文件夹	指定的文件夹的路径中包含驱动器盘符，或网络共享名，可以排除该文件夹，及其所有子文件夹中的所有文件。	D:\Tools\logs\	在文件夹名称后包括末尾的斜杠。
名称相同的所有文件夹	指定的文件夹的路径中不包含驱动器盘符，或网络共享名，可以排除任何驱动器或网络共享中的该文件夹，及其所有子文件夹中的所有文件。	\Tools\logs\ (排除以下文件夹：C:\Tools\logs\，\\Server\Tools\logs\)	您必须指定包括驱动器盘符或网络共享名的完整路径。在此示例中，指定 \logs\ 将不会排除任何文件。

通配符

可以使用通配符 ？ 和 *。

在文件名或文件扩展名中使用通配符 ？ 可以匹配任何单个字符。

在文件名或文件扩展名的结尾，使用通配符 ？ 可以匹配任何单个字符，或无字符。例如，file??.txt 可以匹配 file.txt，file1.txt，和 file12.txt，但是不匹配 file123.txt。

在文件名或文件扩展名中还可以使用通配符 * ，格式为 [文件名].* 或 *.[扩展名]：

正确

file.*

*.txt

不正确

file.txt*

file.*txt

还可以排除带有特定开始字符和扩展名的文件：

file*.txt

以上示例可以在扫描中排除以下文件：

file.txt

file1.txt

file12.txt

file.1.txt

file.12.txt

file12.12.txt

使用上面定义的排除规则，不会排除以下文件：

file.1txt

file.12txt

file.txt1

file.txt12

1file.txt

1file.txt1

7.1.8 批准使用项目

批准广告软件和可能不想安装的应用程序

如果您使用基于角色的管理，那么：

- 您必须具备 策略设置 - 防病毒和 HIPS 权限，才能执行此任务。
- 您不能编辑应用于您的活动子领域之外的策略。

要了解更多信息，请参阅 管理角色和子领域 （第 12 页）。

如果您已启用了 Sophos Endpoint Security and Control 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。

要批准广告软件或可能不想安装的应用程序：

1. 请检查您想要配置的计算机组采用了哪个防病毒和 HIPS 策略。
   请参阅查看组采用的策略 （第 23 页）。
2. 在 策略 窗格板中，双击 防病毒和 HIPS。
3. 双击您想要更改的策略。
   会出现 防病毒和 HIPS 策略 对话框。
4. 单击 批准。
   会出现 批准管理器 对话框。
5. 在 广告软件和可能不想安装的应用程序 标签页中的 已知的广告软件和可能不想安装的应用程序 列表中，选择您想要批准的应用程序。
   如果找不到想要批准的应用程序，您可以自行将它添加到“已知的广告软件和可能不想安装的应用程序”列表中。要了解有关怎样做的信息，请参见预批准广告软件和可能不想安装的应用程序 （第 91 页）。
6. 单击 添加。

广告软件或可能不想安装的应用程序会出现在 已批准的广告软件和可能不想安装的应用程序 列表中。

预批准广告软件和可能不想安装的应用程序

如果您使用基于角色的管理，那么：

- 您必须具备 策略设置 - 防病毒和 HIPS 权限，才能执行此任务。
- 您不能编辑应用于您的活动子领域之外的策略。

要了解更多信息，请参阅 管理角色和子领域 （第 12 页）。

如果您想允许使用某个尚未被 Sophos Endpoint Security and Control 归类为“广告软件和可能不想安装的应用程序”的应用程序，您可以预批准它，方法是将该应用程序添加到“已批准的广告软件和可能不想安装的应用程序”列表中。

1. 请到 Sophos Adware and PUAs 网页 (http://www.sophos.com/zh-cn/threat-center/threat-analyses/adware-and-puas.aspx)。
2. 找到并复制您想要预批准的那个应用程序的名称。
3. 请检查您想要配置的计算机组采用了哪个防病毒和 HIPS 策略。
   请参阅查看组采用的策略 （第 23 页）。
4. 在 策略 窗格板中，双击 防病毒和 HIPS。
5. 双击您想要更改的策略。
   会出现 防病毒和 HIPS 策略 对话框。
6. 单击 批准。
   会出现 批准管理器 对话框。
7. 在 广告软件和可能不想安装的程序 标签页中，单击 新项目。
8. 在 添加新的广告软件或可能不想安装的应用程序 对话框中，将您在步骤 2 中复制的应用程序的名称粘贴到对话框中。

广告软件或可能不想安装的应用程序会出现在 已批准的广告软件和可能不想安装的应用程序 列表中。

如果您添加的应用程序的名称不正确，或者，就是想从 批准管理器 中删除某个应用程序，您可以将它从“已知的广告软件和可能不想安装的应用程序”列表中删除：

1. 在 已批准的广告软件和可能不想安装的应用程序 列表中，选择该应用程序。
2. 单击 删除。
3. 在 已知的广告软件或可能不想安装的应用程序 列表中，选择该应用程序。
4. 单击 删除项目。

阻断已批准的广告软件和可能不想安装的应用程序

如果您使用基于角色的管理，那么：

- 您必须具备 策略设置 - 防病毒和 HIPS 权限，才能执行此任务。
- 您不能编辑应用于您的活动子领域之外的策略。

要了解更多信息，请参阅 管理角色和子领域 （第 12 页）。

要避免当前批准的广告软件和可能不想安装的应用程序在计算机上运行：

1. 请检查您想要配置的计算机组采用了哪个防病毒和 HIPS 策略。
   请参阅查看组采用的策略 （第 23 页）。
2. 在 策略 窗格板中，双击 防病毒和 HIPS。然后，双击您想要更改的策略。
3. 在 防病毒和 HIPS 策略 对话框中，单击 批准 按钮。
4. 在 广告软件或可能不想安装的应用程序 标签页中的 已批准的广告软件和可能不想安装的应用程序 列表中，选择您想要批准的应用程序。
5. 单击 删除。

批准可疑项目

如果您使用基于角色的管理，那么：

- 您必须具备 策略设置 - 防病毒和 HIPS 权限，才能执行此任务。
- 您不能编辑应用于您的活动子领域之外的策略。

要了解更多信息，请参阅 管理角色和子领域 （第 12 页）。

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一个或多个计算机组所采用了。
   请参阅查看组采用的策略 （第 23 页）。
2. 在 策略 窗格板中，双击 防病毒和 HIPS。
3. 双击您想要更改的策略。
   会出现 防病毒和 HIPS 策略 对话框。
4. 单击 批准。
   会出现 批准管理器 对话框。
5. 单击已检测到的行为类型的标签页。
   在以下的例子中，我们使用 缓冲区溢出 标签页。
6. 在 已知的应用程序 列表中，选择您想要批准的应用程序。
   如果找不到想要批准的应用程序，您可以自行将它添加到“已批准的应用程序”列表中。要了解有关怎样做的信息，请参见预批准广告软件和可能不想安装的应用程序 （第 91 页）。
7. 单击 添加。

可疑的应用程序会出现在 批准的应用程序 列表中。

预批准可能的可疑项目

如果您想允许使用某个尚未被 Sophos Endpoint Security and Control 归类为“可疑项目”的应用程序，您可以预批准它，方法是将该应用程序添加到“已批准项目”列表中。

1. 检查哪个防病毒和 HIPS 策略被您想要配置的一个或多个计算机组所采用了。
   请参阅查看组采用的策略 （第 23 页）。
2. 在策略窗格中，双击防病毒和 HIPS。
3. 双击要更改的策略。
   会出现 防病毒和 HIPS 策略 对话框。
4. 单击 批准。
   会出现 批准管理器 对话框。
5. 单击已检测到的行为类型的标签页。
   在以下的例子中，我们使用 缓冲区溢出 标签页。
6. 单击 新项目。
   会出现 打开 对话框。
7. 浏览找到该应用程序，然后，双击它。

可疑的应用程序会出现在 批准的应用程序 列表中。

如果您添加的应用程序的名称不正确，或者，就是想从 批准管理器 中删除某个应用程序，您可以将它从“已知的文件”列表中删除：

1. 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。
   在以下的例子中，我们使用 可疑文件 标签页。
2. 在 已批准的文件 列表中，选择该文件。
3. 单击 删除。
4. 在 已知的文件 列表中，选择该文件。
5. 单击 删除项目。

批准网站

如果您使用基于角色的管理，那么：

- 您必须具备 策略设置 - 防病毒和 HIPS 权限，才能执行此任务。

- 您不能编辑应用于您的活动子领域之外的策略。

要了解更多信息，请参阅 管理角色和子领域 （第 12 页）。

如果您想批准已被 Sophos 归类为恶意网站的某个网站，那么，您可以将它添加到已批准的网站的列表中。批准某个网站，将会使该网站的 URL 避免 Sophos 的扫描网站过滤服务的验证。

警告
批准已被 Sophos 归类为恶意网站的网站，会使您的用户受到安全隐患的威胁。在批准网站之前，请确保访问它是完全的。

要批准网站：

1. 请检查您想要配置的计算机组采用了哪个防病毒和 HIPS 策略。
   请参阅查看组采用的策略 （第 23 页）。
2. 在 策略 窗格板中，双击 防病毒和 HIPS。
3. 双击您想要更改的策略。
   会出现 防病毒和 HIPS 策略 对话框。
4. 单击 批准。
   会出现 批准管理器 对话框。
5. 在 网站 标签中，单击 添加。
   - 要编辑网站项目，请在 批准的网站 列表中勾选它，然后，单击 编辑。
   - 要删除网站项目，请在 批准的网站 列表中勾选它，然后，单击 删除。

网站会出现在 批准的网站 列表中。

注意

- 如果您启用了扫描下载内容，并且您的用户访问某个含有安全隐患的网站，那么，即使该网站已列示在已批准的网站列表中，对它的访问仍然会被阻断。
- 如果您使用“网页控制”功能，当您批准某个已被您的 网页控制 策略阻断的网站时，该网站仍然会被阻断。要允许访问该网站，您需要将该网站从网页控制过滤机制中免除，并且在“防病毒和 HIPS”策略中批准它。要了解更多有关网页控制的信息，请参见网页控制策略 （第 145 页）。

7.2 防火墙策略

防火墙 策略指定防火墙怎样保护计算机。

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。在网络中使用防火墙策略之前，您应该配置它允许您想要使用的应用程序。请参阅设置基本的防火墙策略 （第 95 页）。

要了解默认的防火墙设置的完整列表，请参见 知识库文章 57757。

注释
针对 Windows 8 和更高版本的很多 Sophos Client Firewall 3.0 功能已经删除，并且只适用于运行 Windows 7 或更高版本的计算机。这些功能包括：

- 交互模式
- 隐藏线程检测
- 修改内存检测
- 原始套接字应用程序（原始套接字的处理方式与其他连接相同）
- 非状态规则
- 用于 TCP 规则的并发连接选项
- 本地端口等同于远程端口的地方选项

7.2.1 基本防火墙配置

设置基本的防火墙策略

依照默认值，防火墙会被启用，并会阻断所有可有可无的通讯流。因此，您应该配置防火墙允许您想要使用的应用程序，并在将它安装到所有的计算机上之前，测试它。要了解详细的建议，请参见 Sophos Enterprise Console 策略设置指南。

要了解有关默认的防火墙设置的信息，请参见 Sophos 技术支持知识库文章 57757 （英文）。

要了解更多有关避免网络桥接的信息，请参见设备控制策略 （第 135 页）。

重要提示
当您应用新的或更新的策略到计算机中时，在新的策略被完全应用之前，先前被允许的应用程序可能会被短暂阻断。您应该在应用新的策略之前，告知您的用户此信息。

注释
如果您使用基于角色的管理，那么：

- 您必须具备 策略设置 - 防火墙 权限，才能配置防火墙策略。
- 您不能编辑应用于您的活动子领域之外的策略。

要了解更多有关基于角色的管理的信息，请参见管理角色和子领域 （第 12 页）。

要设置基本的防火墙策略

1. 在 策略 窗格板中，双击 防火墙。
2. 双击 默认 策略，以编辑它。
   会出现 防火墙策略 向导。按照屏幕上的说明做。以下是有关某些选项的附加信息。
3. 在 配置防火墙 页中，选择路径类型：
   - 为总是在网络中的计算机，如：台式机，请选择 单一路径。
   - 如果您想要防火墙，根据计算机使用时的路径，如：在办公室（网络中）和不在办公室（网络外），使用不同的设置，请选择 双重路径。您可能会为笔记型电脑设置双重路径。
4. 在 操作模式 页面中，选择防火墙将怎样处理流入和流出的通讯流：

模式	描述
阻断入站和出站的通讯流。	• 默认级别。提供最高级别的安全性。 • 只允许必要的通讯流通过防火墙，并且使用检查和认证应用程序。 • 要允许在您的公司中常用的应用程序能够通过防火墙进行通讯，请单击 信任。要了解更多信息，请参见关于信任应用程序 （第 102 页）。
阻断入站的通讯流，并允许出站的通讯流。	• 提供的安全性级别低于 阻断流入和流出通讯流。 • 允许您的计算机无需您创建特别的规则，就能访问网络和因特网。 • 允许所有的应用程序通过防火墙进行通讯。
监控	• 应用您设置的规则到网络通讯流中。如果通讯流没有匹配规则，它会向控制台报告，并且只允许流出通讯流。 • 使您能够收集有关网络的信息，并因此能够在部署防火墙到计算机之前，创建适合的规则。要了解更多信息，请参见关于使用监控模式 （第 96 页）。

5. 在 文件和打印机共享 页中，如果您想要允许计算机共享网络中的本地打印机和文件夹，请选择 允许文件和打印机共享。

在您设置了防火墙之后，您可以在 防火墙 - 事件查看器 中查看防火墙事件（如：被防火墙阻断的应用程序）。有关详细信息，请参见查看防火墙事件 （第 163 页）。

在最近七日之内，发生事件的数量超过了指定的级别的计算机，同样会显示在指标面板中。

关于使用监控模式

您可以在供测试的计算机上启用监控模式，并使用“防火墙事件查看器”查看正在使用的是哪些通讯流，应用程序，或线程。

然后，您可以按照创建防火墙事件规则 （第 99 页）中的说明，使用“事件查看器”创建规则，允许或阻断报告的通讯流、应用程序和线程。

注释
当您使用“防火墙事件查看器”创建某个规则，并将它添加到防火墙策略中时，防火墙模式会从 监控 变为 自定义。

如果您不想默认允许未知的通讯流，您可以使用 交互模式。

在交互模式中，防火墙会询问用户允许或阻断任何没有应用规则的应用程序和通讯流。有关详细信息，请参见交互模式 （第 101 页）。

添加和信任应用程序

受信任的应用程序会被允许完全的，无条件的网络访问，包括访问因特网。

要添加某应用程序到防火墙策略中，并信任它：

1. 在 防火墙策略 向导的 操作模式 页中，单击 信任。
   会出现 防火墙策略 对话框。
2. 单击 添加。
   会出现 防火墙策略 - 添加信任的应用程序 对话框。
3. 在 搜索时间跨度 栏中，单击下拉箭头，并选择您想要显示的应用程序事件所在的时间跨度。
   您可以选择固定的时间跨度，如：24 小时内，或者，选择 自定义，通过选择开始日期和时间，以及结束日期和时间，来指定您自定义的时间跨度。
4. 如果您想查看某个类型的应用程序事件，请在 事件类型 栏中，单击下拉箭头，并选择事件类型。
5. 如果您想查看某个文件的应用程序事件，请在 文件名 栏中，输入文件名称。
   如果您保留此栏为空，所有文件的应用程序事件都会显示。
   您可以在此栏中使用通配符。使用 ？ 替代单个字符，以及使用 * 替代字符串。
6. 单击 搜索 可显示应用程序事件列表。
7. 选择某个应用程序事件，然后，单击 确定。

该应用程序会被添加到防火墙策略中，并被标记为 信任的。

基于角色的管理

注释
如果您使用基于角色的管理，那么：

- 您必须具备 策略设置 - 防火墙 权限，才能配置防火墙策略。
- 您不能编辑应用于您的活动子领域之外的策略。

要了解更多信息，请参阅 管理角色和子领域 （第 12 页）。

允许 LAN 上所有的通讯流

要允许 LAN（局域网）上的计算机之间的所有通讯流：

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。
   请参阅查看组采用的策略 （第 23 页）。
2. 在 策略 窗格板中，双击 防火墙 然后双击您想要更改的策略。
3. 在 防火墙策略 向导的 文件和打印机共享 页面中，选择 使用自定义设置，然后，单击 自定义。
4. 在 LAN 设置 列表中，为网络勾选 信任的 勾选框。

注释
如果您允许 LAN（局域网）上的计算机之间的所有通讯流，您同时也就允许 LAN 上的文件和打印机共享。

基于角色的管理

注释
如果您使用基于角色的管理，那么：

- 您必须具备 策略设置 - 防火墙 权限，才能配置防火墙策略。
- 您不能编辑应用于您的活动子领域之外的策略。

要了解更多信息，请参阅 管理角色和子领域 （第 12 页）。

允许文件和打印机共享

要允许计算机共享网络中的本地打印机和文件夹：

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。
   请参阅查看组采用的策略 （第 23 页）。
2. 在 策略 窗格板中，双击 防火墙 然后双击您想要更改的策略。
3. 在 防火墙策略 向导的 文件和打印机共享 页面中，选择 允许文件和打印机共享。

基于角色的管理

注释
如果您使用基于角色的管理，那么：

- 您必须具备 策略设置 - 防火墙 权限，才能配置防火墙策略。
- 您不能编辑应用于您的活动子领域之外的策略。

要了解更多信息，请参阅 管理角色和子领域 （第 12 页）。

允许灵活控制文件和打印机共享

如果您想要更灵活地控制网络中的文件和打印机共享（例如：单项 NetBIOS 通讯流），您可以这样做：

- 允许文件和打印机在 LAN 设置 列表中没有列示的其它的局域网 (LAN) 中共享。这将允许按照防火墙的规则来处理这些局域网中的 NetBIOS 通讯流。
- 创建“高优先级通用规则”，允许与具有适当的 NetBIOS 端口和协议的主机往来通讯。建议您不是通过使用默认规则，而是通过创建通用规则，明确地阻断所有不想要的文件和打印机共享通讯流。

要允许文件和打印机在 LAN 设置 列表中没有列示的其它的局域网 (LAN) 中共享：

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。
   请参阅查看组采用的策略 （第 23 页）。
2. 在 策略 窗格板中，双击 防火墙 然后双击您想要更改的策略。
3. 在 防火墙策略 向导的 文件和打印机共享 页面中，选择 使用自定义设置，然后，单击 自定义。
4. 取消勾选 阻断其它网络的文件和打印机共享 勾选框。

基于角色的管理

注释
如果您使用基于角色的管理，那么：

- 您必须具备 策略设置 - 防火墙 权限，才能配置防火墙策略。
- 您不能编辑应用于您的活动子领域之外的策略。

要了解更多信息，请参阅 管理角色和子领域 （第 12 页）。

阻断不想要的文件和打印机共享

注释
如果您使用基于角色的管理，那么：

- 您必须具备 策略设置 - 防火墙 权限，才能配置防火墙策略。
- 您不能编辑应用于您的活动子领域之外的策略。

要了解更多信息，请参阅 管理角色和子领域 （第 12 页）。

要阻断没有在 LAN 标签页中的 LAN 设置 列表中指定的局域网上的文件和打印机共享：

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。
   请参阅查看组采用的策略 （第 23 页）。
2. 在 策略 窗格板中，双击 防火墙 然后双击您想要更改的策略。
3. 在 防火墙策略 向导的 文件和打印机共享 页面中，选择 使用自定义设置，然后，单击 自定义。
4. 勾选 阻断其它网络的文件和打印机共享 勾选框。

创建防火墙事件规则

注释
如果您使用基于角色的管理，那么：

- 您必须具备 策略设置 - 防火墙 权限，才能配置防火墙策略。
- 您不能编辑应用于您的活动子领域之外的策略。

要了解更多信息，请参阅 管理角色和子领域 （第 12 页）。

您可以为除了“修改了内存”事件之外的所有防火墙事件创建规则。

要创建防火墙事件规则：

1. 在 事件 菜单中，单击 防火墙事件。
2. 在 防火墙 - 事件查看器 对话框，为您想要为它创建规则的应用程序选择事件，并单击 创建规则。
3. 在出现的对话框中，选择您想要应用到应用程序的选项。
4. 选择您想要将该规则应用到哪个路径（主路径，副路径，或两者）。如果您选择应用规则到副路径，或两者，那么，规则只会被添加到配置了副路径的策略中。单击 确定。

   注释
   “新的应用程序”和“修改的应用程序”事件不依赖于路径（它们添加由两个路径共享的检查和）。您不能为这些事件选择路径。

5. 从防火墙策略的列表中，选择您想要应用规则的一个或多个策略。单击 确定。

   注释
   您不能添加规则到应用于您的活动子领域的之外的策略中。

注释
如果您想要使用高级防火墙策略配置页，直接从防火墙策略创建某个应用程序规则，请参见从防火墙策略中创建应用程序规则 （第 113 页）。

临时禁用防火墙

注释
如果您使用基于角色的管理，那么：

- 您必须具备 策略设置 - 防火墙 权限，才能配置防火墙策略。
- 您不能编辑应用于您的活动子领域之外的策略。

要了解更多信息，请参阅 管理角色和子领域 （第 12 页）。

依照默认值，防火墙是启用的。有时，为了维护或排疑解难，您可能需要暂时禁用防火墙，然后，在重新启用它。

要针对某个计算机组的防火墙：

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。
   请参阅查看组采用的策略 （第 23 页）。
2. 在 策略 窗格板中，双击 防火墙。然后，双击您想要更改的策略。
   会出现 防火墙策略 向导。
3. 在向导的欢迎页面，按照以下说明做：
   - 如果您想要关闭所设置的所有路径（主路径和副路径，如果您配置了某一个）中的防火墙，请单击 下一步。在 配置防火墙 页中，选择 允许所有通讯流（关闭防火墙）。结束向导。
   - 如果您想要关闭某一个路径（主路径或副路径）中的防火墙，请单击 高级防火墙策略 按钮。在出现的 防火墙策略 对话框，选择 主路径 或 副路径 旁的 允许所有通讯流。单击 确定。结束防火墙策略 向导。

如果您禁用防火墙，您的计算机将处于非保护状态，直到您重新启用防火墙。要启用防火墙，请取消勾选 允许所有通讯流 勾选框。

7.2.2 高级防火墙配置

打开高级配置页

注释
如果您使用基于角色的管理，那么：

- 您必须具备 策略设置 - 防火墙 权限，才能配置防火墙策略。
- 您不能编辑应用于您的活动子领域之外的策略。

要了解更多信息，请参阅 管理角色和子领域 （第 12 页）。

如果您想要更多地控制防火墙设置，并且能够微调它们，您可以使用高级防火墙策略配置页配置防火墙。

要打开高级防火墙配置页：

1. 双击您想要更改的防火墙策略。

2. 在 防火墙策略 向导的欢迎 页面中，单击 高级防火墙策略。
3. 在 配置 下，单击您想要配置防火墙的路径旁的 配置。

交互模式

在运行 Windows 7 或更早版本的计算机上，可以启用交互模式。然后，每次未知应用程序或服务请求网络访问时，防火墙将在端点计算机上显示学习对话框。学习对话框会询问用户是允许还是阻断通讯流，或者，是否为该类型的通讯流创建规则。

注释
在 Windows 8 和之后版本的计算机上，交互式模式不可用。必须添加特定的策略规则以允许或阻止应用程序。可以使用防火墙-事件查看器以交互方式管理应用程序规则，如创建防火墙事件规则（第 99 页）中所述。

启用交互模式

注释
如果您使用基于角色的管理，那么：

- 您必须具备 策略设置 - 防火墙 权限，才能配置防火墙策略。
- 您不能编辑应用于您的活动子领域之外的策略。

要了解更多信息，请参阅 管理角色和子领域 （第 12 页）。

防火墙可以在交互模式中工作，询问用户如何处理检测到的通讯流。要了解更多信息，请参见交互模式 （第 101 页）。

要使计算机组中的防火墙在交互模式中工作：

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。
   请参阅查看组采用的策略 （第 23 页）。
2. 在 防火墙策略 向导的欢迎 页面中，单击 高级防火墙策略。
3. 在 配置 下，单击您想要配置的路径旁的 配置。
4. 在 常规 标签页的 工作模式 下，单击 交互式。

更改到非交互模式

注释
如果您使用基于角色的管理，那么：

- 您必须具备 策略设置 - 防火墙 权限，才能配置防火墙策略。
- 您不能编辑应用于您的活动子领域之外的策略。

要了解更多信息，请参阅 管理角色和子领域 （第 12 页）。

有两种非交互模式：

- 默认允许
- 默认阻断

在非交互模式中，防火墙使用您的规则自动处理网络通讯流。没有匹配任何规则的网络通讯流，要么全部被允许（如果它是流出通讯流），要么全部被阻断。

要更改计算机组到非交互模式中：

1. 在 策略 窗格板中，双击 防火墙 然后双击您想要更改的策略。

2. 在 防火墙策略 向导的欢迎 页面中，单击 高级防火墙策略。
3. 在 配置 下，单击您想要配置的路径旁的 配置。
4. 单击 常规 标签。
5. 在 工作模式 下，单击 默认允许 或 默认阻断。

配置防火墙

关于信任应用程序

为了提高您的计算机的安全性，防火墙会阻断计算机中未能识别的应用程序的通讯流。不过，在您的公司中通常使用的应用程序可能会被阻断，使用户不能进行日常工作。

您可以信任这些应用程序，这样它们就可以通过防火墙进行通讯。受信任的应用程序会被允许进行完全的和无条件的访问网络和因特网。

注释
为了更安全，您可以应用一个或多个应用程序规则到特定的条件中，应用程序须满足该条件才能运行。要了解有关怎样做的信息，请参见从防火墙策略中创建应用程序规则 （第 113 页）。

添加应用程序到防火墙策略

注释
如果您使用基于角色的管理，那么：

- 您必须具备 策略设置 - 防火墙 权限，才能配置防火墙策略。
- 您不能编辑应用于您的活动子领域之外的策略。

要了解更多信息，请参阅 管理角色和子领域 （第 12 页）。

要添加应用程序到防火墙策略

1. 在 配置 下，单击您想要配置的路径旁的 配置。
2. 单击 应用程序 标签。
3. 单击 添加。
   会出现 防火墙策略 - 添加应用程序 对话框。
4. 在 搜索时间跨度 栏中，单击下拉箭头，并选择您想要显示的应用程序事件所在的时间跨度。
   您可以选择固定的时间跨度，如：24 小时内，或者，选择 自定义，通过选择开始日期和时间，以及结束日期和时间，来指定您自定义的时间跨度。
5. 如果您想查看某个类型的应用程序事件，请在 事件类型 栏中，单击下拉箭头，并选择事件类型。
6. 如果您想查看某个文件的应用程序事件，请在 文件名 栏中，输入文件名称。
   如果您保留此栏为空，所有文件的应用程序事件都会显示。
   您可以在此栏中使用通配符。使用 ？ 替代单个字符，以及使用 * 替代字符串。
7. 单击 搜索 可显示应用程序事件列表。
8. 选择某个应用程序事件，然后，单击 确定。

- 该应用程序会被添加到防火墙策略中，并被标记为 信任的。
- 该应用程序的检查和会被添加到允许的检查和的列表中。

从防火墙策略中删除应用程序

注释
如果您使用基于角色的管理，那么：

- 您必须具备 策略设置 - 防火墙 权限，才能配置防火墙策略。
- 您不能编辑应用于您的活动子领域之外的策略。

要了解更多信息，请参阅 管理角色和子领域 （第 12 页）。

要从防火墙策略中删除应用程序：

1. 在 配置 下，单击您想要配置的路径旁的 配置。
2. 单击 应用程序 标签。
3. 在列表中选择应用程序，然后，单击 删除。

信任某个应用程序

注释
如果您使用基于角色的管理，那么：

- 您必须具备 策略设置 - 防火墙 权限，才能配置防火墙策略。
- 您不能编辑应用于您的活动子领域之外的策略。

要了解更多信息，请参阅 管理角色和子领域 （第 12 页）。

要信任计算机组中的某应用程序：

1. 在 配置 下，单击您想要配置的路径旁的 配置。
2. 单击 应用程序 标签。
   如果该应用程序没有在列表中，请按照 添加应用程序到防火墙策略 （第 102 页） 中的操作指导将它添加到列表中。
3. 在列表中选择应用程序，然后，单击 信任。

- 该应用程序会被添加到防火墙策略中，并被标记为 信任的。
- 该应用程序的检查和会被添加到允许的检查和的列表中。

受信任的应用程序会被允许完全的，无条件的网络访问，包括访问因特网。为了更安全，您可以应用一个或多个应用程序规则到特定的条件中，应用程序须满足该条件才能运行。

- 要创建应用程序规则 （第 112 页）
- 应用预置的应用程序规则 （第 115 页）

通过防火墙事件查看器信任应用程序

注释
如果您使用基于角色的管理，那么：

- 您必须具备 策略设置 - 防火墙 权限，才能配置防火墙策略。
- 您不能编辑应用于您的活动子领域之外的策略。

要了解更多信息，请参阅 管理角色和子领域 （第 12 页）。

如果防火墙报告您的联网计算机上发现某个未知的应用程序或阻断某个应用程序，那么，在“防火墙事件查看器”中会显示该事件。此主题说明怎样从“防火墙事件查看器”中信任某应用程序，以及怎样应用新的规则到您选择的防火墙策略中。

要了解在“防火墙事件查看器”中报告或阻断的应用程序的详情，以及信任它们或为它们创建新的规则：

1. 在 事件 菜单中，单击 防火墙事件。
2. 在 防火墙 - 事件查看器 对话框中，选择想要信任它，或者为它创建规则的应用程序条目，然后，单击 创建规则。
3. 在出现的对话框中，选择是否信任该应用程序，或者，使用现有的预设为它创建规则。
4. 从防火墙策略列表中，选择您想要应用该规则的防火墙策略。要应用规则到所有策略，选择 全选，然后，单击 确定。

- 如果您使用检查和，那么，您必须将应用程序的检查和添加到“允许的检查和”列表中。请参阅添加应用程序检查和 （第 106 页）。
- 您还可以使用高级防火墙配置页面，将某应用程序作为可信任的应用程序直接添加防火墙策略中。请参阅从防火墙策略中创建应用程序规则 （第 113 页）。

阻断应用程序

注释

如果您使用基于角色的管理，那么：

- 您必须具备 策略设置 - 防火墙 权限，才能配置防火墙策略。
- 您不能编辑应用于您的活动子领域之外的策略。

要了解更多信息，请参阅 管理角色和子领域 （第 12 页）。

要阻断计算机组中的某应用程序：

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。
   请参阅查看组采用的策略 （第 23 页）。
2. 在 策略 窗格板中，双击 防火墙 然后双击您想要更改的策略。
3. 在 防火墙策略 向导的欢迎 页面中，单击 高级防火墙策略。
4. 在 配置 下，单击您想要配置的路径旁的 配置。
5. 单击 应用程序 标签。
   如果该应用程序没有在列表中，请按照 添加应用程序到防火墙策略 （第 102 页） 中的操作指导将它添加到列表中。
6. 在列表中选择应用程序，然后，单击 阻断。

允许应用程序启动隐藏进程

注释

如果您使用基于角色的管理，那么：

- 您必须具备 策略设置 - 防火墙 权限，才能配置防火墙策略。
- 您不能编辑应用于您的活动子领域之外的策略。

要了解更多信息，请参阅 管理角色和子领域 （第 12 页）。

应用程序有时会启动另外的隐藏进程，为它执行某些网络访问。

恶意的应用程序可以通过以下技巧避开防火墙：它启动某个受信任的应用程序去访问网络，而不是自己去访问。

要允许应用程序启动隐藏进程，请按以下步骤操作。

注释
该选项在 Windows 8 及以后版本中不可用，因为它通过 Sophos Anti-Virus HIPS 技术自动进行处理。

1. 在 防火墙策略 向导的欢迎 页面中，单击 高级防火墙策略。
2. 在 配置 下，单击您想要配置防火墙的路径旁的 配置。
3. 单击 进程 标签。
4. 在上方区域，单击 添加。
   会出现 防火墙策略 - 添加应用程序 对话框。
5. 在 搜索时间跨度 栏中，单击下拉箭头，并选择您想要显示的应用程序事件所在的时间跨度。
   您可以选择固定的时间跨度，如：24 小时内，或者，选择 自定义，通过选择开始日期和时间，以及结束日期和时间，来指定您自定义的时间跨度。
6. 如果您想查看某个文件的应用程序事件，请在 文件名 栏中，输入文件名称。
   如果您保留此栏为空，所有文件的应用程序事件都会显示。
   您可以在此栏中使用通配符。使用 ? 替代单个字符，以及使用 * 替代字符串。
7. 单击 搜索 可显示应用程序事件列表。
8. 选择某个应用程序事件，然后，单击 确定。

如果启用了交互模式，当检测到新的启动程序时，防火墙会在端点计算机上显示学习对话框。有关详细信息，请参见启用交互模式 （第 101 页）。交互模式在 Windows 8 及以后版本中不可用。

允许应用程序使用原始套接字

注释
如果您使用基于角色的管理，那么：

- 您必须具备 策略设置 - 防火墙 权限，才能配置防火墙策略。
- 您不能编辑应用于您的活动子领域之外的策略。

要了解更多信息，请参阅 管理角色和子领域 （第 12 页）。

某些应用程序可以通过原始套接字访问网络，这允许它们控制数据在网络中传输的各个环节。

恶意的应用程序可以通过虚假的 IP 地址利用原始套接字，或发送蓄意损坏的消息。

要允许应用程序通过原始套接字访问网络，请按以下步骤操作。

注释
此选项在 Windows 8 及以后版本中不可用。防火墙以与普通套接字相同的方式对待原始套接字。

1. 双击您想要更改的防火墙策略。
2. 在 防火墙策略 向导的欢迎 页面中，单击 高级防火墙策略。
3. 在 配置 下，单击您想要配置防火墙的路径旁的 配置。
4. 单击 进程 标签。
5. 在下方区域，单击 添加。
   会出现 防火墙策略 - 添加应用程序 对话框。
6. 在 搜索时间跨度 栏中，单击下拉箭头，并选择您想要显示的应用程序事件所在的时间跨度。
   您可以选择固定的时间跨度，如：24 小时内，或者，选择 自定义，通过选择开始日期和时间，以及结束日期和时间，来指定您自定义的时间跨度。
7. 如果您想查看某个文件的应用程序事件，请在 文件名 栏中，输入文件名称。
   如果您保留此栏为空，所有文件的应用程序事件都会显示。

您可以在此栏中使用通配符。使用 ？ 替代单个字符，以及使用 * 替代字符串。

8. 单击 搜索 可显示应用程序事件列表。
9. 选择某个应用程序事件，然后，单击 确定。

如果启用了交互模式，当检测到原始套接字时，防火墙会在端点计算机上显示学习对话框。有关详细信息，请参见启用交互模式 （第 101 页）。

添加应用程序检查和

注释

如果您使用基于角色的管理，那么：

- 您必须具备 策略设置 - 防火墙 权限，才能配置防火墙策略。
- 您不能编辑应用于您的活动子领域之外的策略。

要了解更多信息，请参阅 管理角色和子领域 （第 12 页）。

每个版本的应用程序都具有独一无二的检查和。防火墙可以使用此检查和决定是否允许某个应用程序。

依照默认值，防火墙会检查每个运行的应用程序的检查和。如果检查和是未知的，或是已被更改，那么，防火墙会阻断它。

要添加检查和到允许的检查和列表中：

1. 双击您想要更改的防火墙策略。
2. 在 防火墙策略 向导的欢迎 页面中，单击 高级防火墙策略。
3. 单击 检查和 标签。
4. 单击 添加。
   会出现 防火墙策略 - 添加应用程序检查和 对话框。
5. 在 搜索时间跨度 栏中，单击下拉箭头，并选择您想要显示的应用程序事件所在的时间跨度。
   您可以选择固定的时间跨度，如：24 小时内，或者，选择 自定义，通过选择开始日期和时间，以及结束日期和时间，来指定您自定义的时间跨度。
6. 在事件类型栏中，单击下拉箭头，并选择您是否想为已更改的应用程序，或者为新的应用程序添加检查和。
7. 如果您想查看某个文件的应用程序事件，请在 文件名 栏中，输入文件名称。
   如果您保留此栏为空，所有文件的应用程序事件都会显示。
   您可以在此栏中使用通配符。使用 ？ 替代单个字符，以及使用 * 替代字符串。
8. 单击 搜索 可显示应用程序事件列表。
9. 选择您想要添加检查和的应用程序事件，然后，单击 确定。

应用程序检查和已被添加到 防火墙策略 对话框中的允许的检查和列表中。

如果启用了交互模式，当检测到新的或修改过的应用程序时，防火墙会在终结点计算机上显示学习对话框。有关详细信息，请参见启用交互模式 （第 101 页）。

开启或关闭阻断已修改的进程

注释

如果您使用基于角色的管理，那么：

- 您必须具备 策略设置 - 防火墙 权限，才能配置防火墙策略。
- 您不能编辑应用于您的活动子领域之外的策略。

要了解更多信息，请参阅 管理角色和子领域 （第 12 页）。

恶意软件可能会通过修改所运行的受信任的程序在内存中的进程，而越过防火墙，然后，通过已修改的进程代表恶意软件自身访问网络。

您可以配置防火墙检测并阻断在内存中已修改的进程。

要开启或关闭阻断已修改的进程：

1. 双击您想要更改的防火墙策略。
2. 在 防火墙策略 向导的欢迎 页面中，单击 高级防火墙策略。
3. 在 配置 下，单击您想要配置防火墙的路径旁的 配置。
4. 在 常规 标签页的 阻断 部分中，取消勾选 如果内存被其它应用程序修改，则阻断进程。 复选框，关闭阻断已修改的进程。

   要开启阻断已修改的进程，请选中该复选框。

如果防火墙检测到内存中的某个进程已被修改，它会添加规则，以防止已修改的进程访问网络。

注意

- 我们不建议您永久地关闭阻断已修改的进程。您应该只在需要时，才关闭它。
- 在 64 位版的 Windows 和 Windows 8 及以后版本上不支持阻止已修改的进程。在 Windows 8 及以后版本中，它通过 Sophos Anti-Virus HIPS 技术自动进行处理。
- 只会阻断已修改的进程。不会阻断修改的程序访问网络。

开启或关闭使用校验和

默认情况下，防火墙使用校验和对应用程序进行验证。信任或阻止应用程序时，将通过其校验和自动识别应用程序（也可以手动添加校验和）。如果应用程序不匹配校验和，它将被阻止。

如果禁用此选项，应用程序通过它们的文件名来被识别。

要开启或关闭使用校验和验证应用程序：

1. 双击您想要更改的防火墙策略。
2. 在 防火墙策略 向导的欢迎 页面中，单击 高级防火墙策略。
3. 在 配置 下，单击您想要配置防火墙的路径旁的 配置。
4. 在常规选项卡中的阻止下，选中或清除使用校验和验证应用程序复选框。

允许或阻止 IPv6 数据包

要允许或阻止 IPv6 数据包：

1. 双击您想要更改的防火墙策略。
2. 在 防火墙策略 向导的欢迎 页面中，单击 高级防火墙策略。
3. 在 配置 下，单击您想要配置防火墙的路径旁的 配置。
4. 在常规选项卡中的阻止下，清除或选中阻止 IPv6 数据包筛选框。

筛选 ICMP 消息

注释
如果您使用基于角色的管理，那么：

- 您必须具备 策略设置 - 防火墙 权限，才能配置防火墙策略。
- 您不能编辑应用于您的活动子领域之外的策略。

要了解更多信息，请参阅 管理角色和子领域 （第 12 页）。

Internet 控制消息协议 (ICMP) 消息允许联网计算机共享出错和状态信息。您可以允许或阻断特定类型的流入或流出的 ICMP 消息。

您应该只在熟悉网络协议的情况下，才筛选 ICMP 消息。要了解有关 ICMP 消息类型的说明，请参见ICMP 消息类型说明 （第 108 页）。

要筛选 ICMP 消息：

1. 双击您想要更改的防火墙策略。
2. 在 防火墙策略 向导的欢迎 页面中，单击 高级防火墙策略。
3. 在 配置 下，单击您想要配置防火墙的路径旁的 配置。
4. 在 ICMP 标签中，勾选 流入 或 流出 勾选框，以允许流入或流出特定类型的消息。

ICMP 消息类型说明

回显请求，回显回复	用于测试目标是否能够访问，及其状态。主机会发送一个回显请求，并监听回应的回显回复。最常见的做法是使用 ping 命令。
目标不可访问，回显回复	当路由器不能送达某 IP 数据报时，会发出此消息。数据报是在 TCP/IP 网络中传输的数据单元，或数据包。
源抑制	如果主机或路由器接收到数据的速度太快，而无法应付时，会发出此消息。此消息是请求源降低数据报的传输率。
重定向消息	如果某路由器收到本应该发送给别的路由器的数据报，会发出此消息。此消息包含源在今后应该定向发送数据报的地址。它被用来优化网络通讯流的路由。
路由器公告，路由器请求	允许主机知晓路由器的存在状况。路由器通过 路由器公告 消息，定期播报它们的 IP 地址。主机也会通过播报 路由器请求 消息来请求某个路由器的地址，对此，路由器会使用 路由器公告 来回复
超时	如果数据报在路由器中传输时，达到了路由器的最大限制，路由器会发出此消息。
参数问题	如果在传输数据报的过程中，出现问题而无法继续时，路由器会发出此消息。此问题的一个潜在根源是无效的数据报报头。
时间戳请求，时间戳回复	用于同步化主机之间的时钟，以及估计传输时间。
信息请求，信息回复	已过时这些消息早先被主机用来决定它们的内部网络地址，但现在被认为已过时，不应该再使用。
地址掩码请求，地址掩码回复	用于查找子网掩码（即：定义网络的地址位）。主机向路由器发送 地址掩码请求，并为此接收 地址掩码回复。

防火墙规则

全局规则

全局规则应用于所有的网络通讯和应用程序，即使这些应用程序具有应用程序规则。

应用程序规则

针对一个应用程序您可以具有一个或多个规则。您可以既可以使用 Sophos 创建的预设的规则，也可以创建子定义的规则，更好地控制应用程序的访问。

要了解默认全局和应用程序规则的相关信息，请参见 Sophos 技术支持知识库文章 57757。

规则应用次序

对于要使用低级插口的连接，只会检查全局规则。

对于不使用低级插口的连接，根据连接的网络地址是否在 LAN 标签页里的列表中，会检查不同的规则。

如果是在 LAN 标签页中列示的网络地址，那么，会检查以下规则：

- 如果该地址已标记为 信任的，那么，该连接中的所有通讯流都会被允许，不会做进一步的检查。
- 如果该地址已标记为 NetBIOS，那么，会允许在连接中满足以下标准的任何文件和打印机共享：

连接	端口	范围
TCP	远程	137-139 或 445
TCP	本地	137-139 或 445
UDP	远程	137 或 138
UDP	本地	137 或 138

如果网络地址没有列示在 LAN 标签页中，那么，会按照以下次序检查其它的防火墙规则：

1. 任何在 LAN 标签页中不被允许的 NetBIOS 通讯流，会按照 阻断其它网络的文件和打印机共享 复选框的设置情况来处理。
   - 如果该复选框是勾选的，那么，该通讯流会被阻断。
   - 如果该复选框是取消勾选的，那么，该通讯流会按照现存的规则处理。
2. 最优先的通用规则，会按照列示它们的次序，依次检查。
3. 如果尚未有任何规则应用到连接中，那么，会检查应用程序规则。
4. 如果连接仍然未被处理，那么，会按照列示它们的次序，应用通常优先的全局规则。
5. 如果没有找到用于处理连接的规则，那么：
   - 在 默认允许 模式中，通讯流会被允许（如果它是流出通讯流）。
   - 在 默认阻断 模式中，通讯流会被阻断。
   - 在 交互 模式中，用户会被要求决定如何处理。此模式在 Windows 8 及以后版本中不可用。

   注释
   如果您尚未更改工作模式，那么，防火墙将会处于 默认阻断 模式。

本地网络检测

注释
此功能在 Windows 8 及以后版本中不可用。

您可以为计算机的本地网络指派防火墙规则。

当防火墙启动时，它将确定计算机的本地网络，然后，监控本地网络在运行过程发生的一切更改。如果检测到任何更改，防火墙会为新的本地网络地址更新本地网络规则。

警告
我们强烈建议在将本地网络作为副路径的一部分时，谨慎从事。如果计算机是笔记型电脑，并且用于办公场所之外，那么，它可能会连接未知的本地网络。如果发生这种情况，那么，将本地网络作为地址的副路径配置中的防火墙规则，可能会意想不到地允许未知的通讯流。

全局规则

创建全局规则

注释
如果您使用基于角色的管理，那么：

- 您必须具备 策略设置 - 防火墙 权限，才能配置防火墙策略。
- 您不能编辑应用于您的活动子领域之外的策略。

要了解更多信息，请参阅 管理角色和子领域 （第 12 页）。

重要提示
我们建议您只有在熟悉网络协议的情况下，才创建全局规则。

全局规则应用于所有的网络通讯，以及尚未有任何规则的应用程序。

要创建全局规则：

1. 双击您想要更改的防火墙策略。
2. 在 防火墙策略 向导的欢迎 页面中，单击 高级防火墙策略。
3. 在 配置 下，单击您想要配置防火墙的路径旁的 配置。
4. 单击 全局规则 标签。
5. 单击 添加。
6. 在 规则名称 下，输入规则的名称。
   该规则名称必须不同于列表中的任何规则的名称。两个全局规则不能具有相同的名称。
7. 要在任何应用程序规则或普通优先的通用规则之前应用规则，请选中 最优先规则 复选框。
   要了解有关规则应用的次序的信息，请参见规则应用次序 （第 109 页）。
8. 在 请选择规则将要处理的事件 下，选择为了应用规则，连接必须满足的条件。
9. 在 请选择规则的响应措施，选择 允许它 或 阻断它。
10. 按照以下的说明之一做：
    - 要在初始连接存在的同时，允许其它连接从同一个远程地址进行流入和流出，那么，请选中 并发连接。

      注释
      此选项仅供 TCP 规则使用，TCP 规则为默认的状态。

    - 要灵活地允许来自基于初始连接的远程计算机的回答，请选择 状态检查。

      注释
      此选项仅适用于 UDP 和 IP 规则。

注释
在 Windows 8 及以后版本中，这些选项不适用，因为始终会使用状态检测，且不支持并行连接。

11. 在 规则描述 下，单击一个下划线值。例如，如果您单击 状态 TCP 链接， 选择协议 对话框会开启。

编辑全局规则

注释
如果您使用基于角色的管理，那么：

- 您必须具备 策略设置 - 防火墙 权限，才能配置防火墙策略。
- 您不能编辑应用于您的活动子领域之外的策略。

要了解更多信息，请参阅 管理角色和子领域 （第 12 页）。

重要提示
我们建议您只有在熟悉网络协议的情况下，才更改全局规则。

要编辑全局规则：

1. 双击您想要更改的防火墙策略。
2. 在 防火墙策略 向导的欢迎 页面中，单击 高级防火墙策略。
3. 在 配置 下，单击您想要配置防火墙的路径旁的 配置。
4. 单击 全局规则 标签。
5. 在 规则 列表中，选择您想要编辑的规则。
6. 单击 编辑。

   要了解更多有关全局规则设置的信息，请参见 Sophos 技术支持知识库文章 57757 。

复制全局规则

注释
如果您使用基于角色的管理，那么：

- 您必须具备 策略设置 - 防火墙 权限，才能配置防火墙策略。
- 您不能编辑应用于您的活动子领域之外的策略。

要了解更多信息，请参阅 管理角色和子领域 （第 12 页）。

要复制全局规则，并将它添加到规则列表中：

1. 双击您想要更改的防火墙策略。
2. 在 防火墙策略 向导的欢迎 页面中，单击 高级防火墙策略。
3. 在 配置 下，单击您想要配置防火墙的路径旁的 配置。
4. 单击 全局规则 标签。
5. 在 规则 列表中，选择您想要复制的规则。
6. 单击 复制。

删除全局规则

注释
如果您使用基于角色的管理，那么：

- 您必须具备 策略设置 - 防火墙 权限，才能配置防火墙策略。
- 您不能编辑应用于您的活动子领域之外的策略。

要了解更多信息，请参阅 管理角色和子领域 （第 12 页）。

1. 双击您想要更改的防火墙策略。
2. 在 防火墙策略 向导的欢迎 页面中，单击 高级防火墙策略。
3. 在 配置 下，单击您想要配置防火墙的路径旁的 配置。
4. 单击 全局规则 标签。
5. 在 规则 列表中，选择您想要删除的规则。
6. 单击 删除。

更改全局规则应用的次序

注释
如果您使用基于角色的管理，那么：

- 您必须具备 策略设置 - 防火墙 权限，才能配置防火墙策略。
- 您不能编辑应用于您的活动子领域之外的策略。

要了解更多信息，请参阅 管理角色和子领域 （第 12 页）。

全局规则是按照它们在规则列表中从上自下出现的次序来应用的。

要更改全局规则应用的次序

1. 双击您想要更改的防火墙策略。
2. 在 防火墙策略 向导的欢迎 页面中，单击 高级防火墙策略。
3. 在 配置 下，单击您想要配置防火墙的路径旁的 配置。
4. 单击 全局规则 标签。
5. 在 规则 列表中，单击您想要在列表中移动的规则。
6. 单击 上移 或 下移。

应用程序规则

要创建应用程序规则

注释
如果您使用基于角色的管理，那么：

- 您必须具备 策略设置 - 防火墙 权限，才能配置防火墙策略。
- 您不能编辑应用于您的活动子领域之外的策略。

要了解更多信息，请参阅 管理角色和子领域 （第 12 页）。

要创建允许精确地控制应用程序访问的自定义的规则：

1. 双击您想要更改的防火墙策略。
2. 在 防火墙策略 向导的欢迎 页面中，单击 高级防火墙策略。
3. 在 配置 下，单击您想要配置防火墙的路径旁的 配置。

4. 单击 应用程序 标签。
5. 在列表中选择应用程序，然后，单击 自定义。
6. 在 应用程序规则 对话框中，单击 添加。
7. 在 规则名称 下，输入规则的名称。
   该规则名称必须不同于列表中的任何规则的名称。两个应用程序规则，并能具有同样的名称，但是两个应用程序可以各有一个具有同样名称的规则。
8. 在 请选择规则将要处理的事件 下，选择为了应用规则，连接必须满足的条件。
9. 在 请选择规则的响应措施，选择 允许它 或 阻断它。
10. 按照以下的说明之一做：
    - 要在初始连接存在的同时，允许其它连接从同一个远程地址进行流入和流出，那么，请选中 并发连接。

      注释
      此选项仅供 TCP 规则使用，TCP 规则为默认的状态。

    - 要灵活地允许来自基于初始连接的远程计算机的回答，请选择 状态检查。

      注释
      此选项仅适用于 UDP 和 IP 规则。

    注释
    在 Windows 8 及以后版本中，这些选项不适用，因为始终会使用状态检测，且不支持并行连接。

11. 在 规则描述 下，单击一个下划线值。例如，如果您单击 状态 TCP 链接， 选择协议 对话框会开启。

从防火墙策略中创建应用程序规则

注释
如果您使用基于角色的管理，那么：

- 您必须具备 策略设置 - 防火墙 权限，才能配置防火墙策略。
- 您不能编辑应用于您的活动子领域之外的策略。

要了解更多信息，请参阅 管理角色和子领域 （第 12 页）。

您可以使用高级防火墙策略配置页，直接从防火墙策略中创建应用程序规则。

要从防火墙策略中创建应用程序规则：

1. 双击您想要更改的策略。
2. 在 防火墙策略 向导的欢迎页面中，单击 高级防火墙策略 按钮。
3. 在出现的 防火墙策略 对话框中，单击您想要配置防火墙的路径旁的 配置。
4. 按照以下的说明之一做：
   - 如果您想要添加应用程序到防火墙策略，请在出现的对话框中，转到 应用程序 标签中，并单击 添加。
   - 如果您想要允许应用程序启动隐藏的线程，请转到 线程 标签页中，单击位于上方的 添加。

- 如果您想要允许应用程序通过低级插口访问网络，请转到 线程 标签页中，单击位于下方的 添加。

会出现 防火墙策略 - 添加应用程序 对话框。

5. 如果您是添加应用程序，请在 事件类型 文本框中，选择您是添加已修改的应用程序，新的应用程序，还是添加在防火墙策略没有为其设置应用程序规则的应用程序。
6. 选择您想要添加，或想要允许启动隐藏线程，或允许使用低级插口的应用程序的条目，并单击 确定。
   该应用程序已被添加到防火墙策略。

如果您在 应用程序 标签页中添加应用程序，那么，该应用程序会作为“受信任的”应用程序添加。如果您想要，您可以阻断它，或为它创建自定义规则。

编辑应用程序规则

注释
如果您使用基于角色的管理，那么：

- 您必须具备 策略设置 - 防火墙 权限，才能配置防火墙策略。
- 您不能编辑应用于您的活动子领域之外的策略。

要了解更多信息，请参阅 管理角色和子领域 （第 12 页）。

1. 双击您想要更改的防火墙策略。
2. 在 防火墙策略 向导的欢迎 页面中，单击 高级防火墙策略。
3. 在 配置 下，单击您想要配置防火墙的路径旁的 配置。
4. 单击 应用程序 标签。
5. 在列表中选择应用程序，然后，单击 自定义。
6. 在 应用程序规则 对话框，单击 编辑。
7. 在 规则名称 下，输入规则的名称。
   该规则名称必须不同于列表中的任何规则的名称。两个应用程序规则，并能具有同样的名称，但是两个应用程序可以各有一个具有同样名称的规则。
8. 在 请选择规则将要处理的事件 下，选择为了应用规则，连接必须满足的条件。
9. 在 请选择规则的响应措施，选择 允许它 或 阻断它。
10. 按照以下的说明之一做：

- 要在初始连接存在的同时，允许其它连接从同一个远程地址进行流入和流出，那么，请选中 并发连接。

  注释
  此选项仅供 TCP 规则使用，TCP 规则为默认的状态。

- 要灵活地允许来自基于初始连接的远程计算机的回答，请选择 状态检查。

  注释
  此选项仅适用于 UDP 和 IP 规则。

注释
在 Windows 8 及以后版本中，这些选项不适用，因为始终会使用状态检测，且不支持并行连接。

11. 在 规则描述 下，单击一个下划线值。例如，如果您单击 状态 TCP 链接， 选择协议 对话框会开启。

应用预置的应用程序规则

注释
如果您使用基于角色的管理，那么：

- 您必须具备 策略设置 - 防火墙 权限，才能配置防火墙策略。
- 您不能编辑应用于您的活动子领域之外的策略。

要了解更多信息，请参阅 管理角色和子领域 （第 12 页）。

Sophos 创建了一组预置的应用程序规则。要添加预置的规则到某应用程序的规则列表中：

1. 双击您想要更改的防火墙策略。
2. 在 防火墙策略 向导的欢迎 页面中，单击 高级防火墙策略。
3. 在 配置 下，单击您想要配置防火墙的路径旁的 配置。
4. 单击 应用程序 标签。
5. 在列表中选择应用程序，然后，单击 自定义。
6. 指向 从预置中添加规则，然后，单击预置。

复制应用程序规则

注释
如果您使用基于角色的管理，那么：

- 您必须具备 策略设置 - 防火墙 权限，才能配置防火墙策略。
- 您不能编辑应用于您的活动子领域之外的策略。

要了解更多信息，请参阅 管理角色和子领域 （第 12 页）。

要复制应用程序规则，并将它添加到规则列表中：

1. 双击您想要更改的防火墙策略。
2. 在 防火墙策略 向导的欢迎 页面中，单击 高级防火墙策略。
3. 在 配置 下，单击您想要配置防火墙的路径旁的 配置。
4. 单击 应用程序 标签。
5. 在列表中选择应用程序，然后，单击 自定义。
6. 在 应用程序规则 对话中，选择您想要计划的报告，并单击 计划。

删除应用程序规则

注释
如果您使用基于角色的管理，那么：

- 您必须具备 策略设置 - 防火墙 权限，才能配置防火墙策略。
- 您不能编辑应用于您的活动子领域之外的策略。

要了解更多信息，请参阅 管理角色和子领域 （第 12 页）。

1. 双击您想要更改的防火墙策略。
2. 在 防火墙策略 向导的欢迎 页面中，单击 高级防火墙策略。
3. 在 配置 下，单击您想要配置防火墙的路径旁的 配置。
4. 单击 应用程序 标签。
5. 在列表中选择应用程序，然后，单击 自定义。
6. 在 应用程序规则 对话中，选择您想要计划的报告，并单击 计划。

更改应用程序规则应用的次序

注释
如果您使用基于角色的管理，那么：

- 您必须具备 策略设置 - 防火墙 权限，才能配置防火墙策略。
- 您不能编辑应用于您的活动子领域之外的策略。

要了解更多信息，请参阅 管理角色和子领域 （第 12 页）。

应用程序规则是按照它们在规则列表中从上自下出现的次序来应用的。

要更改应用程序规则应用的次序：

1. 双击您想要更改的防火墙策略。
2. 在 防火墙策略 向导的欢迎 页面中，单击 高级防火墙策略。
3. 在 配置 下，单击您想要配置防火墙的路径旁的 配置。
4. 单击 应用程序 标签。
5. 在列表中选择应用程序，然后，单击 自定义。
6. 在 应用程序规则 列表中，在规则列表中，单击您想要在列表中移动的规则。
7. 单击 上移 或 下移。

位置感知

位置感知是 Sophos Client Firewall 中的功能，它可以根据当前计算机的网络适配器的路径，将防火墙配置指派给计算机上的各个网络适配器。

最常使用此功能的情形是，公司职员使用公司的笔记型电脑在家中工作。他们同时使用两个网络连接：

- 他们通过 VPN 客户端和 虚拟网络适配器，连接到办公网络，以便工作。
- 他们通过网线和 物理网络适配器，连接他们的 ISP，以便个人使用。

在这种情形下，您需要将办公配置应用到虚拟的办公连接中，以及（通常限制更严格的）非办公配置应用到非办公的 ISP 连接中。

注释
非办公配置要求足够的规则，以允许建立“虚拟的”办公连接。

关于设置位置感知

1. 定义您的主路径的网关 MAC 地址或域名的列表。一般地，它们是您的办公网络。
2. 创建将用于您的主路径的防火墙配置。一般地，这些配置的限制相对较少。
3. 创建副路径的防火墙配置。一般地，这些配置的限制相对较多。
4. 选择要应用的配置。

根据您使用的检测方法，防火墙会获得各个计算机网络适配器的 DNS 或网关地址，然后，将这些地址与您的地址列表进行匹配。

- 如果您的列表中的任何地址与任何网络适配器的地址匹配，那么，该适配器会被指派针对 主路径 的配置。
- 如果您的列表没有任何地址与任何网络适配器的地址匹配，那么，该适配器会被指派针对 副路径 的策略。

重要提示
当以下两个条件同时满足时，计算机上的副路径的配置将从 交互 模式转到 默认阻断 模式。

- 主路径和副路径都处于活动状态。
- 主路径配置不是交互模式。

定义主路径

1. 双击您想要更改的防火墙策略。
2. 在 防火墙策略 向导的欢迎 页面中，单击 高级防火墙策略。
3. 在 配置 下，单击您想要配置防火墙的路径旁的 配置。
4. 单击 路径检测 标签页。
5. 在 检测方法 下，单击您想要用来定义主路径的方法旁的 配置：

选项	描述
通过 DNS 识别路径	您创建对应主路径的域名和预期 IP 地址的列表。
通过 网关 MAC 地址识别路径	您创建对应主路径的网关 MAC 地址的列表。

6. 按照屏幕上的说明做。

创建副路径配置

1. 双击您想要更改的防火墙策略。
2. 在 防火墙策略 向导的欢迎 页面中，单击 高级防火墙策略。
3. 在 配置 下，单击您想要配置防火墙的路径旁的 配置。
4. 勾选 为副路径添加配置 勾选框。

现在设置您的副路径配置。要了解有关怎样做的信息，请参见打开高级配置页 （第 100 页）。

警告
我们强烈建议在将本地网络作为副路径的一部分时，谨慎从事。如果计算机是笔记型电脑，并且用于办公场所之外，那么，它可能会连接未知的本地网络。如果发生这种情况，那么，将本地网络作为地址的副路径配置中的防火墙规则，可能会意想不到地允许未知的通讯流。

选择要应用的配置

1. 双击您想要更改的防火墙策略。
2. 在 防火墙策略 向导的欢迎 页面中，单击 高级防火墙策略。
3. 在 配置 下，单击您想要配置防火墙的路径旁的 配置。
4. 在 常规 标签页的 应用的路径 下，单击以下选项之一：

选项	描述
为检测到的路径应用配置	防火墙会根据位置感知的检测设置（按照关于设置位置感知 （第 117 页）中的说明）将主路径或副路径的配置应用到各个网络连接中。
应用主路径配置	防火墙会将主路径配置应用到所有的网络连接中。
应用副路径配置	防火墙会将副路径配置应用到所有的网络连接中。

防火墙报告发送

默认情况下，终结点计算机上的防火墙会向 Enterprise Console 报告状态的更改、事件和错误。

防火墙状态更改

防火墙将以下更改视为状态更改：

- 更改工作模式
- 更改软件版本
- 更改防火墙是否允许所有通讯流的配置
- 更改防火墙是否遵照策略

如果您工作在交互式模式中，您的防火墙配置可能会有意地与通过 Enterprise Console 应用的策略不同。在这种情况下，当您更改某些防火墙配置时，您可以选择不向 Enterprise Console 发送“策略不一致”的警报。

要了解更多信息，请参见关闭或打开报告本地更改 （第 119 页）。

防火墙事件

事件 是指终结点计算机的操作系统，或终结点计算机上的未知的应用程序，试图通过网络连接与其它的计算机进行通讯。

您可以避免防火墙向 Enterprise Console 报告事件。

要了解更多信息，请参见关闭报告未知的网络通讯流 （第 119 页）。

关闭或打开报告本地更改

注释
如果您使用基于角色的管理，那么：

- 您必须具备 策略设置 - 防火墙 权限，才能配置防火墙策略。
- 您不能编辑应用于您的活动子领域之外的策略。

要了解更多信息，请参阅 管理角色和子领域 （第 12 页）。

如果终结点计算机上的防火墙配置与策略不一致，您可以关闭报告本地更改。

注释
此选项在 Windows 8 及以后版本中不支持。

关闭报告本地更改，可以使防火墙停止向 Enterprise Console 发送，有关更改了全局策略，应用程序，进程，或检查和的“与策略不一致”的警报。您想要这样做的原因可能是，例如，当端点计算机在交互模式中时，有些设置可能会被使用学习对话框而更改。

如果终结点计算机上的防火墙配置，应该与策略一致，那么，您应该打开报告本地更改。

要关闭报告本地更改：

1. 双击您想要更改的防火墙策略。
2. 在 防火墙策略 向导的欢迎 页面中，单击 高级防火墙策略。
3. 在 配置 下，单击您想要配置防火墙的路径旁的 配置。
4. 单击 常规 标签。
5. 在 报告发送 下，按照以下说明之一做：
   - 要打开报告本地更改，请选中 如果对全局规则，应用程序，进程，或检查和进行了本地更改，那么，在管理控制台显示相关的警报。 复选框。
   - 要关闭报告本地更改，请取消勾选 如果对全局规则，应用程序，进程，或检查和进行了本地更改，那么，在管理控制台显示相关的警报。 复选框。

关闭报告未知的网络通讯流

注释
如果您使用基于角色的管理，那么：

- 您必须具备 策略设置 - 防火墙 权限，才能配置防火墙策略。
- 您不能编辑应用于您的活动子领域之外的策略。

要了解更多信息，请参阅 管理角色和子领域 （第 12 页）。

您可以避免终结点计算机上的防火墙向 Enterprise Console 报告未知的网络通讯流。防火墙将没有规则可依照的通讯流，视为未知的通讯流。

要避免终结点计算机上的防火墙向 Enterprise Console 报告未知的网络通讯流：

1. 双击您想要更改的防火墙策略。
2. 在 防火墙策略 向导的欢迎 页面中，单击 高级防火墙策略。
3. 在 配置 下，单击您想要配置防火墙的路径旁的 配置。
4. 单击 常规 标签。
5. 在 阻断 下，勾选 使用检查和鉴定应用程序 勾选框。
6. 在 报告发送 下，取消勾选 向管理控制台报告未知的应用程序和通讯流 勾选框。

关闭报告防火墙错误

重要提示
我们不建议您永久性地关闭报告防火墙错误。您应该只在需要时，才关闭报告。

要避免终结点计算机上的防火墙向 Enterprise Console 报告错误：

1. 双击您想要更改的防火墙策略。
2. 在 防火墙策略 向导的欢迎 页面中，单击 高级防火墙策略。
3. 在 配置 下，单击您想要配置防火墙的路径旁的 配置。
4. 单击 常规 标签。
5. 在 报告发送 下，取消勾选 向管理控制台报告出错 勾选框。

导入或导出防火墙配置

注释
如果您使用基于角色的管理，那么：

- 您必须具备 策略设置 - 防火墙 权限，才能配置防火墙策略。
- 您不能编辑应用于您的活动子领域之外的策略。

要了解更多信息，请参阅 管理角色和子领域 （第 12 页）。

您可以将防火墙的常规设置和规则，以配置文件 (*.conf) 的形式导入或导出。您可以使用此功能，完成以下任务：

- 备份和恢复您的防火墙配置。
- 导入在某个计算机上创建的应用程序规则，并使用这些规则为运行了相同的应用程序的其它计算机创建策略。
- 将在不同的计算机上创建的配置合并，以创建能在网络中一个或多个计算机组上有效使用的策略。

要导入或导出防火墙配置：

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。
   请参阅查看组采用的策略 （第 23 页）。
2. 在 策略 窗格板中，双击 防火墙，然后双击您想要导出或导入的策略。
3. 在 防火墙策略 向导的欢迎 页面中，单击 高级防火墙策略。
4. 在 防火墙策略 对话框的 常规 标签页下的 管理配置 中，单击 导入 或 导出。

7.3 应用程序控制策略

Enterprise Console 使您能够检测和阻断“受控程序”，即：不对计算机安全构成威胁的，正当合法的程序，但是，您认为这些程序不适合在办公环境中使用。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，数字影像软件，媒体播放器，浏览器插件，等等。

注释
此选项只应用于 Sophos Endpoint Security and Control for Windows。

凭借充分的灵活性，可以根据不同的计算机组，阻断或批准同样的应用程序。例如，可以阻断办公室计算机上的语音IP电话(VoIP)的应用程序，但是在远程计算机上允许该应用程序。

受控程序列表由 Sophos 提供，并且定期更新。您不能添加新的应用程序到此列表中，但是，您可以向 Sophos 提交请求，添加您想要在您的网络中控制的非恶意的应用程序。

要了解详情，请参见 Sophos 知识库文章 63656（英文）。

本节说明怎样选择您想在您的网络中控制的应用程序，以及设置扫描受控程序。

注释
如果您使用基于角色的管理，那么：

- 您必须具备 策略设置 - 应用程序控制 权限，才能配置应用程序控制策略。
- 您不能编辑应用于您的活动子领域之外的策略。

要了解更多有关基于角色的管理的信息，请参见管理角色和子领域 （第 12 页）。

应用程序控制事件

当某个应用程序控制事件发生时，例如，在网络中检测到某个受控程序，该事件会被记录到应用程序控制事件日志中，并且能够从 Enterprise Console 中查看它。有关详细信息，请参见查看应用程序控制事件 （第 162 页）。

在最近七日之内，发生事件的数量超过了指定的级别的计算机，会显示在指标面板中。

您还可以设置当发生应用程序控制事件时，向您选择的收件人发送警报。有关详细信息，请参见设置应用程序控制警报和消息 （第 157 页）。

7.3.1 选择想要控制的应用程序

如果您使用基于角色的管理，那么：

- 您必须具备 策略设置 - 应用程序控制 权限，才能配置应用程序控制策略。
- 您不能编辑应用于您的活动子领域之外的策略。

要了解更多信息，请参阅 管理角色和子领域 （第 12 页）。

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。
   请参阅查看组采用的策略 （第 23 页）。
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，例如，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。（参见 扫描想要控制的应用程序 （第 122 页） 了解详细信息。）单击 确定。

7.3.2 扫描想要控制的应用程序

如果您使用基于角色的管理，那么：

- 您必须具备 策略设置 - 应用程序控制 权限，才能配置应用程序控制策略。
- 您不能编辑应用于您的活动子领域之外的策略。

要了解更多信息，请参阅 管理角色和子领域 （第 12 页）。

您可以配置 Sophos Endpoint Security and Control 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。
   请参阅查看组采用的策略 （第 23 页）。
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。
   - 要启用即时扫描，请勾选 启用即时和计划扫描 勾选框。

   注释
   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 （第 122 页）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。要了解操作指导，请参见设置应用程序控制警报和消息 （第 157 页）。

7.3.3 卸载不想要的受控程序

在您卸载受控程序之前，请确保已禁用读写扫描受控程序功能。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。

您可以使用两种方法删除某个应用程序：

- 到各台计算机上，运行卸载程序，卸载该软件产品。您通常可以打开 Windows 控制面板，然后使用“添加 / 删除程序”来实现。
- 在服务器上，使用脚本程序或管理工具，运行卸载程序，卸载联网计算机上的该软件产品。

现在您可以启用读写扫描受控程序了。

7.4 数据控制策略

注释
此功能没有包括在所有的用户授权使用许可协议中。如果您想要使用它，您可能需要更改您的用户授权使用许可协议。要了解更多信息，请参见http://www.sophos.com/zh-cn/products/complete/comparison.aspx。

数据控制，通过监控和限制传输包含敏感数据的文件，使您能够减少从工作站计算机意外丢失数据的机会。您通过创建各种数据控制规则，并将这些规则添加到数据控制策略中，来进行数据控制。

您可以监控传输到特定的存储设备（如：移动存储设备或光驱）的文件，或监控通过特定的应用程序（如：电子邮件客户端或网页浏览器）传输的文件。

为了使您能够迅速定义和部署数据控制策略，SophosLabs 提供了一个敏感数据定义库（内容控制列表(Content Control List)）。这个库主要集中于个人身份识别信息，不过，它也保护其它常用的数据结构。您可以按照本节中的进一步的说明，在 Enterprise Console 中使用内容控制列表 (Content Control List)。

7.4.1 数据控制怎样工作？

数据控制，可以识别意外的数据丢失，这通常是由职员不当处理敏感数据造成。例如，用户通过基于网页的电子邮件将包含敏感数据的文件寄回家。

数据控制使您能够监控从计算机到存储设备和连接到因特网的应用程序的文件传输。

- 存储设备：数据控制会介入分析通过“资源管理器”（包括 Windows 桌面）复制到受控的存储设备的所有文件。不过，直接在应用程序（如：Microsoft Word）内部进行的复制，或者，使用命令行提示窗进行的传输，不会被介入分析。

  通过 允许用户接受的传输和日志事件 措施选项，或 阻断传输和日志事件 措施选项，可以强制所有向受控的存储设备进行的传输，都要使用“资源管理器”进行。在这两种情况中，任何试图直接从应用程序中保存文件，或者，从命令行提示窗中传输文件的操作，都会被数据控制阻断，并且会显示桌面警报，要求用户使用“资源管理器”进行文件传输。

  当数据控制策略只包含具有 允许文件传输和日志事件 措施选项时，任何直接在应用程序内部进行的保存，或者，使用命令行提示窗进行的文件传输，不会被介入分析。这样将使用户能够不受限制地使用存储设备。不过，使用“资源管理器”进行的传输，仍然会作为数据控制事件被日志记录。

  注释
  此限制不应用于应用程序监控。

- 应用程序：为了确保只监控用户上传的文件，某些系统文件所在的路径会从数据控制监控中排除。这将显著地减少由应用程序开启配置文件生成数据控制事件，而不用户上传文件生成数据控制事件的情况。

  重要提示
  如果您遇到错误地由某应用程序开启配置文件而生成事件的情况，解决此问题的通常是添加自定义的排除路径，或配置数据控制规则减低敏感度。有关详细信息，请参阅 Sophos 知识库文章 113024。

注释
读写扫描排除项目并非始终应用于数据控制。

数据控制什么时间使用读写扫描排除项目呢？

根据复制或移动文件的方式和位置，数据控制可能会或不会考虑在防病毒和 HIPS 策略中设置的读写扫描排除项目。

使用监控应用程序（如电子邮件客户端、Web 浏览器或即时消息 (IM) 客户端）上传或附加文件时，数据控制将使用读写扫描排除项目。要了解更多有关配置读写扫描排除文件的信息，请参见从读写扫描中排除项目 （第 73 页）。

重要提示
如果已经在读写扫描中排除远程文件，数据控制将不会扫描从网络位置上传或附加到监控应用程序（如电子邮件或 Web 浏览器）的文件。另请参阅数据控制不扫描上传或附带的文件 （第 187 页）。

使用 Windows 资源管理器复制或移动文件时，数据控制将不使用读写扫描排除项目。因此，排除将不起作用。例如，将文件复制到存储设备（如 USB）或将文件复制或移动到某个网络位置时。即便在读写扫描中排除了远程文件，仍将扫描所有文件。

注释
如果将存档文件复制或移动到一个网络位置，整个过程可能需要一些时间，如每 100MB 的数据超过 1 分钟，具体取决于您的网络连接。这是因为扫描存档文件的时间比扫描非存档文件的时间长。

数据控制策略

数据控制使您能够通过定义数据控制策略和应用这些策略到您的网络中的计算机组中，来监控文件的传输活动。

重要提示
数据控制不支持 Windows 2008 Server Core，并且必须在运行此操作系统的计算机上被禁用。要从数据控制扫描中排除 Windows 2008 Server Core 计算机，请将这些计算机放置到具有禁用数据控制扫描的数据控制策略的计算机组中。有关详细信息，请参见开启或关闭数据控制 （第 127 页）。

数据控制策略包括一个或多个数据控制规则，这些规则指定检测条件，以及当规则被匹配使将要采取的措施。一个数据控制规则可以被包括在多个策略中。

在某个数据控制策略中包含多个规则时，某文件只要匹配该数据控制策略中的任一规则，就会被视为违反了该策略。

数据控制规则条件

数据控制规则条件包括目标路径，文件名及其扩展名，或文件内容。

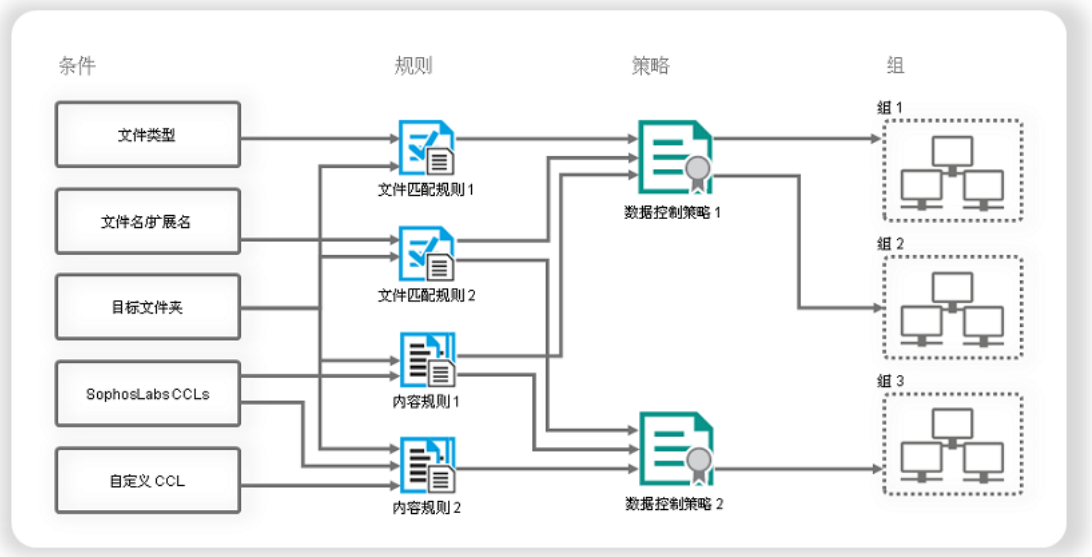
目标路径包括设备（例如，类似 USB 闪存的移动存储设备）和应用程序（例如，因特网浏览器和电子邮件客户端程序）。

文件内容的匹配是通过内容控制列表（CCL）来定义的。内容控制列表（CCL）是基于 XML 的结构化数据描述。SophosLabs 提供了一个内容控制列表（CCL）的扩展集，它可以用于您的数据控制规则中。

要了解更多有关应用数据控制规则和条件到文件中的信息，请参见关于数据控制规则 （第 125 页）。

要了解更多有关定义文件内容的内容控制列表（CCL）的信息，请参见关于内容控制列表 （第 126 页）。

数据控制



数据控制规则措施

当数据控制检测到在规则中指定的所有条件时，即为规则被匹配，则数据控制将采取在规则中指定的措施，并将此事件记录到日志中。您可以指定以下措施之一：

- 允许文件传输和日志事件
- 允许用户接受的传输和日志事件
- 阻断传输和日志事件

如果某文件匹配指定了不同措施的两条数据控制规则，那么，指定的措施最严格的规则将被应用。阻断文件传输的数据控制规则的优先性，高于允许用户接受的文件传输的数据控制规则。允许用户接受的文件传输的数据控制规则的优先性，高于允许文件传输的数据控制规则。

依照默认值，当规则被匹配后文件的传输被阻断时，或者，当要求用户确认文件的传输时，会有消息出现在端点计算机的桌面上。被匹配的规则，会在消息中指出。您可以添加您自定义的消息到，供用户确认文件传输和阻断文件传输所使用的标准消息中。要了解更多信息，请参见设置数据控制警报和消息 （第 157 页）。

7.4.2 关于数据控制规则

数据控制规则指定数据控制扫描的检测条件，指定当规则被匹配时，采取的措施，以及指定要从扫描中排除的文件。

您可以创建自己的规则或使用提供的样本规则。我们提供了一些预先配置的数据控制规则，您可以现成地使用它们，也可以修改它们满足您的需要。这些规则只作为范例提供，并不进行更新。

有两种类型的数据控制规则：文件匹配规则 和 内容规则。

文件匹配规则

文件匹配规则，是如果当用户试图传输具有某些特定的文件名或特定的文件类型（真实的文件类型类别，如：电子表格文件）的文件到特定的路径时，指定所要采取的措施的规则。例如，阻断传输数据库文件到移动存储设备。

数据控制包括针对 150 多个文件格式的真实文件类型的定义。我们会不时添加更多的真实的文件类型。新添加的文件类型，将被自动添加到所有使用该相关的真实文件类型类别的数据控制规则中。

没有包括在真实文件类型定义中的文件类型，可以通过它们的文件扩展名来识别。

内容规则

内容规则，是包括一个或多个内容控制列表，并指定，如果用户试图传输匹配了规则中的全部内容控制列表的数据到指定目标路径 (destination) 时，指定所要采取的措施的规则。

7.4.3 关于内容控制列表

内容控制列表 (CCL)，是描述结构化的文件内容的条件集合。内容控制列表 (Content Control List) 可能描述单一的数据类型（例如，家庭住址或社会保险号），或者，描述各种数据类型组合（例如，几乎等同于“机密”二字的某个项目名称）。

您可以使用 Sophos 提供的 SophosLabs Content Control Lists，或创建您自己的内容控制列表。

SophosLabs Content Control Lists 提供针对常用的财务和个人身份识别数据类型（例如，信用卡好，社会保险号，家庭住址，或电子邮件地址等）的专业定义。诸如总和检查等，高级技巧被用于 SophosLabs Content Control Lists 之中，增加了检测敏感数据的精确性。

您不能够编辑 SophosLabs Content Control Lists，但是您可以提交请求给 Sophos，要求创建新的 SophosLabs Content Control List。有关详细信息，请参阅 Sophos 知识库文章 51976。

注释
当前版本的内容控制列表(CCL)不保证支持双字节字符（例如，日语或中文字符）。不过，您可以在内容控制列表(CCL)编辑器中输入双字节字符。

为 SophosLabs Content Control Lists 设置数量

大多数的 SophosLabs Content Control Lists 都被指派了数量。

数量，是在内容控制列表被匹配之前，必须在文件中找到的内容控制列表 (CCL) 的键数据类型 (key data type) 的数量。您可以在包含内容控制列表 (CCL) 的内容规则中编辑 SophosLabs Content Control List 的数量值。

使用数量，可以微调数据控制规则，并避免阻止不包含敏感信息的文件（例如，在信头、页脚或签名中，可能包含邮寄地址或一个或两个电话号码的文件）。如果您只是单一地查找邮寄地址，那么，会有成千个文件匹配规则，并触发数据控制事件。但是，如果您想要避免流失客户名单，您可能会检测所传输的文件中包含，比如，50 个以上的邮寄地址的文件。不过，在其它情况下，建议您单一地查找内容实体，比如，信用卡号。

7.4.4 关于数据控制事件

当发生数据控制事件时，例如，复制包含敏感数据的文件到 USB 闪存中，该事件会被发送到 Enterprise Console 中，并且可以在 数据控制 - 事件查看器 中查看它。该事件还会被日志记录到本地的终结点计算机上，并且在具有相应的权限的情况下，可以在 Sophos Endpoint Security and Control 中查看它。

注释
一个终结点计算机每小时最多可以向 Enterprise Console 发送 50 个数据控制事件。所有的事件都会日志记录到本地的终结点计算机上。

在 数据控制 - 事件查看器 对话框中，您可以使用筛选挑选仅仅显示您感兴趣的事件。您还可以将数据控制事件列表导出到文件中。有关详细信息，请参见关于数据控制事件 （第 127 页）和导出事件列表到文件中 （第 169 页）。

在最近七日之内，发生数据控制事件的数量超过了指定的级别的计算机，会显示在指标面板中。要了解怎样设置级别的信息，请参见指标面板 （第 3 页）。

您还可以设置当发生数据控制事件时，向您选择的收件人发送警报。有关详细信息，请参见设置数据控制警报和消息 （第 157 页）。

7.4.5 开启或关闭数据控制

如果您使用基于角色的管理，那么：

- 您必须具备 策略设置 - 数据控制 权限，才能配置数据控制策略。
- 您不能编辑应用于您的活动子领域之外的策略。

要了解更多信息，请参阅 管理角色和子领域 （第 12 页）。

依照默认值，数据控制是关闭的，并且没有指定任何规则监控或限制网络中的文件传输。

要开启数据控制：

1. 请检查您想要配置的计算机组使用的是哪个数据控制策略。
   请参阅查看组采用的策略 （第 23 页）。
2. 在 策略 窗格板中，双击 数据控制。然后，双击您想要更改的策略。
   会出现 数据控制策略 对话框。
3. 在 策略规则 标签页中，勾选 启用数据控制扫描 勾选框。
4. 单击 添加规则 按钮。在 数据控制规则管理 对话框中，选择您想要添加到策略中的规则，并单击确定。

重要提示
在您添加任何数据控制规则之前，数据控制将不会监控或限制任何文件传输。

如果您稍后想要禁用数据控制扫描，请取消勾选 启用数据控制扫描 勾选框。

7.4.6 创建文件匹配规则

如果您使用基于角色的管理，那么：

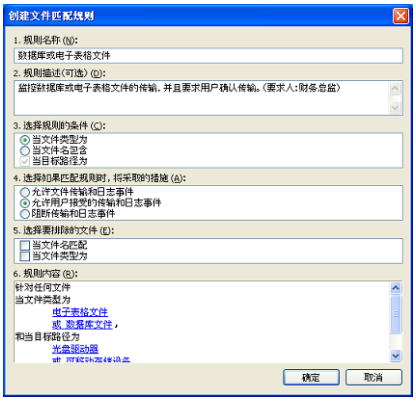
- 您必须具备 数据控制 - 自定义 权限，才能创建或编辑数据控制规则。
- 您必须具备 策略设置 - 数据控制 权限，才能设置数据控制策略。
- 您不能编辑应用于您的活动子领域之外的策略。

要了解更多信息，请参阅 管理角色和子领域 （第 12 页）。

要了解文件匹配规则概述，请参见关于数据控制规则 （第 125 页）。

要创建文件匹配规则，并将它添加到数据控制策略中：

1. 请检查您想要配置的计算机组使用的是哪个数据控制策略。
   请参阅查看组采用的策略 （第 23 页）。
   或者，您可以从 工具 菜单创建规则，并稍后将它添加到一个或多个策略中。在 工具 菜单中，指向 管理数据控制，然后，单击 数据控制规则，然后，执行步骤 4 到步骤 10。
2. 在 策略 窗格板中，双击 数据控制。然后，双击您想要更改的策略。
3. 在 数据控制策略 对话框的 策略规则 标签页中，确保已勾选 启用数据控制扫描 勾选框，然后，单击 管理规则。
4. 在 数据控制规则管理 对话框中，单击 添加文件匹配规则 按钮。
5. 在 创建文件匹配规则 对话框中的 规则名称 下，输入规则的名称。
6. 在 规则描述（可选） 中，如果您需要，输入对规则的描述。
7. 在 选择规则规则的条件 中，为规则选择条件。
   目标路径条件是预先选择的，并且必须包括在规则中。
   依照默认值，所有的文件类型都会被扫描。如果您只想扫描某些特定的文件类型，请选择 当文件类型为。然后，您可以按照步骤 10 中的说明，设置此条件。
8. 在 选择如果匹配规则时，将采取的措施。，选择措施。
9. 如果您想要从数据控制扫描中排除某些文件，请在 选择要排除的文件 下，勾选 当文件名匹配 或 当文件类型为 勾选框。
10. 在 规则内容 下，单击各个下划线的值，并设置规则的条件。
    例如，如果您单击 选择目标路径，匹配目标类型条件 对话框会开启，您可以在对话框中选择想要限制数据传输的设备和/或应用程序。
    为各个下划线的值选择或输入条件。



    单击 确定。
    新的规则会出现在 数据控制规则管理 对话框中。
11. 要添加规则到策略中，请勾选规则名称旁的勾选框，并单击 确定。
    该规则会被添加到数据控制策略。

您可以设置当数据控制策略中的规则被匹配时，发送给用户的警报和消息。请参阅设置数据控制警报和消息 （第 157 页）。

7.4.7 创建内容规则

如果您使用基于角色的管理，那么：

- 您必须具备 数据控制 - 自定义 权限，才能创建或编辑数据控制规则和内容控制列表 (CCL)。
- 您必须具备 策略设置 - 数据控制 权限，才能设置数据控制策略。
- 您不能编辑应用于您的活动子领域之外的策略。

要了解更多信息，请参阅 管理角色和子领域 （第 12 页）。

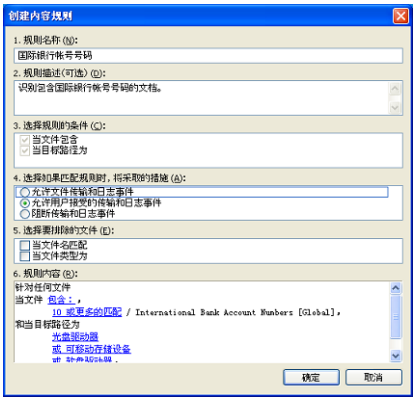
要了解内容规则和内容控制列表概述，请参见关于数据控制规则 （第 125 页）。

要创建内容规则，并将它添加到数据控制策略中：

1. 请检查您想要配置的计算机组使用的是哪个数据控制策略。
   请参阅查看组采用的策略 （第 23 页）。
   或者，您可以从 工具 菜单创建规则，并稍后将它添加到一个或多个策略中。在 工具 菜单中，指向 管理数据控制，然后，单击 数据控制规则，然后，执行步骤 4 到步骤 13。
2. 在 策略 窗格板中，双击 数据控制。然后，双击您想要更改的策略。
3. 在 数据控制策略 对话框的 策略规则 标签页中，确保已勾选 启用数据控制扫描 勾选框，然后，单击 管理规则。
4. 在 数据控制规则管理 对话框中，单击 添加内容规则 按钮。
5. 在 创建内容规则 对话框的 规则名称 下，输入规则的名称。
6. 在 规则描述（可选） 中，如果您需要，输入对规则的描述。
7. 在 选择规则的条件 ，文件内容和目标路径条件已被选择。您必须为内容规则设置这两种条件。
8. 在 选择如果匹配规则时，将采取的措施。，选择措施。
9. 如果您想要从数据控制扫描中排除某些文件，请在 选择要排除的文件 下，勾选 当文件名匹配 或 当文件类型为 复选框。
10. 在 规则内容 下，单击“选择文件内容”下划线值。
11. 在 内容控制列表管理 对话框中，选择您想要包括在规则中的内容控制列表。
    如果要添加 SophosLabs 内容控制列表，请为每个需要的国家选择一个。

    提示
    如果不需要支持所有国家，请勿选择全局内容控制列表。而是只为所需的国家选择内容控制列表。这可以大大缩短扫描时间，并降低不需要的、巧合匹配的风险。

    如果您想要创建新的内容控制列表，请参见创建或编辑简单内容控制列表 (CCL) （第 132 页）或创建或编辑高级内容控制列表 （第 133 页）。
    单击确定。
12. 如果您想要更改指派给 SophosLabs Content Control List 的数量，请在 规则内容 下，单击您想要更改的“数量”下划线值（“n 或更多的匹配”）。在 数量编辑器 对话框中，输入新的数量值。要了解更多信息，请参见关于内容控制列表 （第 126 页）。
13. 在 规则内容 下，选择或输入剩下的下划线值的条件。



单击 确定。

新的规则会出现在 数据控制规则管理 对话框中。

14. 要添加规则到策略中，请选中规则名称旁的复选框，并单击 确定。
    该规则会被添加到数据控制策略。

您可以设置当数据控制策略中的规则被匹配时，发送给用户的警报和消息。请参阅设置数据控制警报和消息 （第 157 页）。

7.4.8 添加数据控制规则到策略中

如果您使用基于角色的管理，那么：

- 您必须具备 策略设置 - 数据控制 权限，才能执行此任务。
- 您不能编辑应用于您的活动子领域之外的策略。

要了解更多信息，请参阅 管理角色和子领域 （第 12 页）。

要添加数据控制到策略中：

1. 请检查您想要配置的计算机组使用的是哪个数据控制策略。
   请参阅查看组采用的策略 （第 23 页）。
2. 在 策略 窗格板中，双击 数据控制。然后，双击您想要更改的策略。
   会出现 数据控制策略 对话框。
3. 在 策略规则 标签页中，单击 添加规则。
   会出现 数据控制规则管理器 对话框。
4. 请选择您想要添加到策略中的规则，并单击 确定。

7.4.9 从策略中删除数据控制规则

如果您使用基于角色的管理，那么：

- 您必须具备 策略设置 - 数据控制 权限，才能执行此任务。
- 您不能编辑应用于您的活动子领域之外的策略。

要了解更多信息，请参阅 管理角色和子领域 （第 12 页）。

要从策略中删除数据控制规则：

1. 请检查您想要配置的计算机组使用的是哪个数据控制策略。
   请参阅查看组采用的策略 （第 23 页）。
2. 在 策略 窗格板中，双击 数据控制。然后，双击您想要更改的策略。

会出现 数据控制策略 对话框。

3. 在 策略规则 标签页中，选择您想要删除的规则，然后，单击 删除规则。

7.4.10 从数据控制中排除文件或文件类型

如果您使用基于角色的管理，那么，您必须具备 数据控制 - 自定义 权限，才能从数据控制中排除文件。要了解更多信息，请参见管理角色和子领域 （第 12 页）。

您可以通过在数据控制规则中，设置排除项目来从数据控制中排除文件和文件类型。

要从数据控制中排除文件或文件类型，请在规则中排除它，并赋予最高的优先级（即：指定最严格的限制措施）。

要从数据控制中排除文件或文件类型：

1. 在 工具 菜单中，指向 管理数据控制，然后，单击 数据控制规则。
2. 在 数据控制规则管理 对话框中，选择您想要编辑的规则，并单击 编辑，或者，通过单击 添加文件匹配规则 或 添加内容规则 按钮，创建新的规则。
3. 要从数据控制中排除文件，请在 规则编辑器 对话框的 选择要排除的文件 下，勾选 当文件名匹配 勾选框。
4. 在 规则内容 下，单击下划线值以指定被排除的文件的名称。
5. 在 排除文件名条件 对话框中，单击 添加 并指定您想要排除的文件的名称。

   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。
6. 要从数据控制中排除文件类型，请在 规则编辑器 对话框的 选择要排除的文件 下，勾选 当文件类型为 勾选框。
7. 在 规则内容 下，单击下划线值以指定被排除的文件类型。
8. 在 排除文件类型条件 对话框中，选择您想要排除的文件类型，并单击 确定。

7.4.11 导入或导出数据控制规则

如果您使用基于角色的管理，您必须具备 数据控制 - 自定义 权限，才能导入或导出数据控制规则。要了解更多信息，请参见管理角色和子领域 （第 12 页）。

数据控制规则可以作为 XML 文件导入或导出 Enterprise Console。

要导入或导出数据控制规则：

1. 在 工具 菜单中，指向 管理数据控制，然后，单击 数据控制规则。
2. 在 数据控制规则管理 对话框中，单击 导入 或 导出。
   - 如果您想导入规则，请在 导入 对话框中，浏览找到您想要导入的规则，选择它并单击 打开。
   - 如果您想导出规则，请在 导出 对话框中，浏览找到将要保存导出文件的目标路径，输入文件的名称，并单击 保存。

7.4.12 创建或编辑简单内容控制列表（CCL）

如果您使用基于角色的管理，那么，您必须具备 数据控制自定义 权限，才能创建内容控制列表（CCL）。要了解更多信息，请参见管理角色和子领域 （第 12 页）。

要了解内容控制列表（CCL）概述，请参见关于内容控制列表 （第 126 页）。

要创建或编辑内容控制列表（CCL）

1. 在 工具 菜单中，指向 管理数据控制，然后，单击 数据内容控制列表（CCL）。
2. 在 内容控制列表管理 对话框中，单击 添加 以创建新的内容控制列表（CCL），或者，选择某个现有的内容控制列表（CCL），并单击 编辑。
3. 在 添加内容控制列表 对话框的 名称 栏中，输入内容控制列表（CCL）的名称。
4. 在 描述 栏中，如果您需要，输入对内容控制列表（CCL）的描述。
5. 如果您想要添加标识或编辑指定给内容控制列表（CCL）的标识，请单击 标识 栏旁的 更改 按钮。您可以指派标识，以识别内容控制列表（CCL）的类型和它所应用的地区。
6. 在 编辑内容控制列表标识 对话框的 可用标识 列表中，选择您想要指派的标识，并将它们移动到已选择的标识 列表中。单击 确定。
7. 在 扫描内容匹配 部分，选择某个搜索条件（“任何这些条件”，“所有这些条件”，或“完全匹配此表达”），并输入您想在文档中找到的搜索词，使用空格分隔。单击 确定。

   注释
   搜索词是区分大小写的。

   简单内容控制列表（CCL）不支持使用引号。请使用“完全匹配此表达”条件，扫描完全一致的表达。

   要创建更复杂的表达式，请按照 创建或编辑高级内容控制列表 （第 133 页） 中的说明，使用高级内容控制列表（CCL）编辑器。

新的内容控制列表会出现在 内容控制列表管理 对话框中。

示例

搜索条件	示例	描述
匹配任何条件	机密	匹配包含“机密”或“秘密”字样的文档。
匹配所有条件	项目机密	匹配包含“项目”和“机密”字样的文档。
完全匹配	仅供内部使用	匹配包含“仅供内部使用”字样的文档。

现在，您可以将此新建的内容控制列表（CCL）添加到内容规则中。

7.4.13 创建或编辑高级内容控制列表

如果您使用基于角色的管理，那么，您必须具备 数据控制自定义 权限，才能创建内容控制列表 (CCL)。要了解更多信息，请参见管理角色和子领域 （第 12 页）。

要了解内容控制列表 (CCL) 概述，请参见关于内容控制列表 （第 126 页）。

您可以创建包含一个或多个正则表达式和触发积分的内容控制列表 (CCL)。要这样做，请使用高级编辑器。

要使用高级编辑器创建或编辑内容控制列表 (CCL)：

1. 在 工具 菜单中，指向 管理数据控制，然后，单击 数据内容控制列表 (CCL)。
2. 在 内容控制列表管理 对话框中，单击 添加 以创建新的内容控制列表 (CCL)，或者，选择某个现有的内容控制列表 (CCL)，并单击 编辑。
3. 在 添加内容控制列表 对话框的 名称 栏中，输入内容控制列表 (CCL) 的名称。
4. 在 描述 栏中，如果您需要，输入对内容控制列表 (CCL) 的描述。
5. 如果您想要添加标识或编辑指定给内容控制列表 (CCL) 的标识，请单击 标识 栏旁的 更改 按钮。
   您可以指派标识，以识别内容控制列表 (CCL) 的类型和它所应用的地区。
6. 在 编辑内容控制列表标识 对话框的 可用标识 列表中，选择您想要指派的标识，并将它们移动到已选择的标识 列表中。单击 确定。
7. 单击 高级 按钮。
8. 在 高级 窗格板，单击 创建 以创建新的表达式，或者，选择某个现有的表达式，然后，单击 编辑。
9. 在 内容控制列表 - 高级 对话框中，输入 Perl 5 正则表达式。
   要了解 Perl 5 正则表达式的说明，请参见 Perl 技术文档或访问 http://www.boost.org/doc/libs/1_34_1/libs/regex/doc/syntax_perl.html。
10. 在 表达式积分 栏中，输入当满足正则表达式时，需要添加到内容控制列表 (CCL) 中的总积分的积分数。
11. 在 最大计数 栏中，输入可以添加到总计中的最多的匹配正则表达数。
    例如，某个具有 5 分以及最大计数为 2 的表达式，将添加最多10分到内容控制列表 (CCL) 的总计积分中。如果该表达式被发现 3 次，它仍然是添加 10 分到总计积分中。
    单击 确定。
12. 如果您想添加更多的正则表达式到内容控制列表 (CCL) 中，请重复步骤 5 到步骤 11。
13. 在 触发积分 栏中，输入在匹配内容控制列表之前，正则表达式必须被匹配的次数。
    例如，设想某个内容控制列表的触发积分为 8，并且由 3 个表达式（A，B，和 C）组成，它们具有以下的积分和最大计数：

表达式	积分	最大计数
表达式 A	5	2
表达式 B	3	1
表达式 C	1	5

    如果数据控制发现 2 个表达式 A 的匹配，或者，发现 1 个表达式 A 的匹配，和 1 个表达式 B 的匹配，或者，1 个表达式 B 的匹配，和 5 个表达式 C 的匹配，那么，此内容控制列表 (CCL) 则被匹配。
    单击 确定。

新的内容控制列表（CCL）会出现在 内容控制列表管理 对话框中。

正则表达式示例

(?i)\b[a-ceghj-npr-tw-z][a-ceghj-npr-tw-z]\s?\d{2}\s?\d{2}\s?\d{2}\s?[abcd]?\b

此正则表达式匹配社会保险号号，例如，AA 11 11 11 A.

(?i)	使匹配区分大小写。
\b	匹配某个字符符号和非字符符号之间的边界值。
[a-ceghj-npr-tw-z]	匹配字符范围（A 到 C E G H J 到 N P R 到 T W 到 Z）中的任一单一字符。
?	匹配前置元素（preceding element）零次或一次。
\s?	匹配零或一个空白(whitespace)。
\d{2}	匹配两个数位。
[abcd]	匹配列表（A，B，C，或 D）中的任何单个字符。

现在，您可以将此新建的内容控制列表（CCL）添加到内容规则中。

7.4.14 导入或导出内容控制列表（CCL）

如果您使用基于角色的管理，您必须具备 数据控制 - 自定义 权限，才能导入或导出内容控制列表(CCL)。要了解更多信息，请参见管理角色和子领域 （第 12 页）。

内容控制列表（CCL）可以作为 XML 文件导入或导出 Enterprise Console。您可以在支持内容控制列表（CCL）的 Sophos 产品之间共享内容控制列表（CCL）。

注释
SophosLabs Content Control List 无法被导出。

要导入或导出内容控制列表（CCL）：

1. 在 工具 菜单中，指向 管理数据控制，然后，单击 数据控制内容控制列表。
2. 在 内容控制列表管理 对话框中，单击 导入 或 导出。
   - 如果您想导入内容控制列表（CCL），请在 导入 对话框中，浏览找到您想要导入的内容控制列表(CCL)，选择它并单击 打开。
   - 如果您想导出内容控制列表（CCL），请在 导出 对话框中，浏览找到将要保存导出文件的目标路径，输入文件的名称，并单击 保存。

7.5 设备控制策略

注释
此功能没有包括在所有的用户授权使用许可协议中。如果您想要使用它，您可能需要更改您的用户授权使用许可协议。要了解更多信息，请参见http://www.sophos.com/zh-cn/products/complete/comparison.aspx。

重要提示
Sophos 设备控制不应该与其它软件供应商的设备控制软件共同部署。

设备控制可以使您防止用户在他们的计算机上，使用未经批准的外部硬件设备，移动存储介质，以及无线连接技术。这能够极大地降低您意外流失数据的风险，限制用户将外来软件安装到网络中的能力。

移动存储设备，光盘启动器，以及软盘驱动器还可以被设置为仅提供只读访问。

使用设备控制，您还可以显著降低公司网络和非公司网络之间的网络桥接风险。阻断桥接模式可用于无线和调制解调类型的设备。此模式的工作方式为，当某终结点计算机（通常是通过以太网连接的方式）连接到物理网络时，则禁用无线或调制解调网络适配器。一旦终结点计算机与物理网络断开了连接，无线或调制解调网络适配器会顺畅地重新启用。

依照默认值，设备控制是关闭的，所有的设备都会被允许。

如果您想首次启用设备控制，我们建议您：

- 选择要控制的设备类型。
- 检测但不阻断它们。
- 通过设备控制事件来决定阻断哪些设备类型，以及或许要免除的设备。
- 检测并阻断设备，或者，允许只读访问存储设备。

要了解更多有关针对设备控制的建议设置，请参见 Sophos Enterprise Console 策略设置指南。

注释
如果您使用基于角色的管理，那么：

- 您必须具备 策略设置 - 设备控制 权限，才能配置应用程序控制策略。
- 您不能编辑应用于您的活动子领域之外的策略。

要了解更多信息，请参阅 管理角色和子领域 （第 12 页）。

7.5.1 关于设备控制事件

当发生设备控制事件时，例如，某移动存储设备被阻断，该事件会被发送到 Enterprise Console 中，并且可以在 设备控制 - 事件查看器 对话框中查看它。

注释
如果您将可选的磁盘驱动器设置为“只读”，这些磁盘驱动器的事件将不会发送给 Enterprise Console 或记录到本地日志。这样就可以阻止不需要的事件报告。

在 设备控制 - 事件查看器 对话框中，您可以使用筛选挑选仅仅显示您感兴趣的事件。您还可以将设备控制事件列表导出到文件中。有关详细信息，请参见关于设备控制事件 （第 135 页）和导出事件列表到文件中 （第 169 页）。

您可以通过设备控制事件，将特定的设备或设备型号作为免除项目添加到设备控制策略中。要了解更多有关免除设备的信息，请参见从单个策略中免除设备 （第 139 页）或从所有策略中免除设备 （第 138 页）。

在最近七日之内，发生设备控制事件的数量超过了指定的级别的计算机，会显示在指标面板中。要了解怎样设置级别的信息，请参见配置指标面板 （第 41 页）。

您还可以设置当发生设备控制事件时，向您选择的收件人发送警报。有关详细信息，请参见设置设备控制警报和消息 （第 158 页）。

7.5.2 可以控制什么类型的设备？

设备控制可以使您阻断以下类型的设备：存储设备、网络设备、短距设备以及媒体设备。

存储

- 可移动存储设备（如：USB 闪存，PC 读卡器，以及外置硬盘）
- 光学介质驱动器（CD-ROM/DVD/Blu-ray 驱动器）
- 软盘驱动器
- 安全的移动存储设备（例如，硬件加密的 USB 闪存）

要了解所支持的安全移动存储设备的列表，请参阅 Sophos 知识库文章 63102。

提示
通过使用安全的可移动存储分类，您可以在阻断其它可移动存储设备的同时，方便地允许使用受到支持的安全的可移动存储设备。

网络

- 调制解调器
- 无线连接（Wi-Fi 接口，802.11 标准）

对于网络接口，您还可以选择 阻断桥接 模式，以帮助您显著降低公司网络和非公司网络之间的网络桥接风险。此模式的工作方式为，当某端点计算机（通常是通过以太网连接的方式）连接到物理网络时，则禁用无线或调制解调网络适配器。一旦端点计算机与物理网络断开了连接，无线或调制解调网络适配器会顺畅地重新启用。

短距 (short range)

- 蓝牙接口
- 红外接口（(IrDA 红外接口）

设备控制会同时阻断内置和外置的设备和接口。例如，某个阻断蓝牙接口的策略，将会阻断以下两者：

- 计算机中内建的蓝牙接口

- 任何通过 USB 接入计算机的蓝牙适配器

媒体

- MTP/PTP

  这包括手机、平板电脑、数码相机、媒体播放器和其他使用媒体传输协议 (MTP) 或图片传输协议 (PTP) 连接到电脑的设备。

7.5.3 选择要控制的设备类型

如果您使用基于角色的管理，那么：

- 您必须具备 策略设置 - 设备控制 权限，才能编辑应用程序控制策略。
- 您不能编辑应用于您的活动子领域之外的策略。

要了解更多信息，请参阅 管理角色和子领域 （第 12 页）。

重要提示
您不应该阻断 Enterprise Console 通过 Wi-Fi 来进行管理的计算机上的 Wi-Fi 连接。

1. 检查哪个设备控制策略被您想要配置的计算机组所采用了。
   请参阅查看组采用的策略 （第 23 页）。
2. 在 策略 窗格板中，双击 设备控制。然后，双击您想要更改的策略。
3. 在 设备控制策略 对话框中 配置 标签页的 存储 下，选择您想要控制的存储设备的类型。
4. 单击设备类型旁的 状态 栏，然后，单击出现的下拉箭头。选择您想要允许的访问权限类型。
   依照默认值，设备具有完全访问权限。对可移动的存储设备，光盘驱动器，和软盘驱动器，您可以更改它们为“已阻断”或“只读”。对安全的可移动的存储设备，您可以更改它为“已阻断”。
5. 在 网络 下，选择您想要阻断的网络设备的类型。
6. 单击网络设备类型旁的 状态 栏，然后，单击出现的下拉箭头。
   - 勾选“阻断”，如果您想要阻断该设备类型。
   - 勾选“阻断桥接”，如果您想要避免公司网络和非公司网络之间的网络桥接。当某端点计算机（通常是通过以太网连接的方式）连接到物理网络时，该设备类型会被阻断。一旦端点计算机与物理网络断开了连接，该设备类型会重新启用。
7. 在 短距 下，勾选您想要阻断的短距设备的类型。在设备类型旁的 状态 栏中，选择“已阻断”。
   单击 确定。
8. 要阻止使用媒体传输协议 (MTP) 或图像传输协议 (PTP) 连接到计算机的媒体设备，如手机、平板电脑、数码相机或媒体播放器，请在媒体下选择MTP/PTP。在状态列中，选择“阻止”。

7.5.4 检测但不阻断它们

如果您使用基于角色的管理，那么：

- 您必须具备 策略设置 - 设备控制 权限，才能编辑应用程序控制策略。
- 您不能编辑应用于您的活动子领域之外的策略。

要了解更多信息，请参阅 管理角色和子领域 （第 12 页）。

您可以检测设备，但不阻断它们。如果您想今后阻断设备，但需要首先检测和免除您需要的设备，那么，这一功能将很有用。

检测设备但不阻断它们，请在设备控制策略中，启用设备控制扫描，并开启 仅限检测 模式。更改您想要检测设备的状态“已阻断”。当策略被违反时，这将在终结点计算机上生成设备事件，但是设备将不会被阻断。

要了解有关查看设备控制事件的信息，请参见关于设备控制事件 （第 135 页）。

要检测设备但不阻断它们：

1. 检查哪个设备控制策略被您想要配置的计算机组所采用了。
   请参阅查看组采用的策略 （第 23 页）。
2. 在 策略 窗格板中，双击 设备控制。然后，双击您想要更改的策略。
3. 在 设备控制策略 对话框的 配置 标签页中，选择 启用设备控制扫描。
4. 选择 检测但不阻断设备。
5. 如果您尚未这样做，那么，更改您想要检测的设备的状态为“已阻断”。（有关详细信息，请参见选择要控制的设备类型 （第 137 页）。）
   单击 确定。

7.5.5 检测和阻断设备

如果您使用基于角色的管理，那么：

- 您必须具备 策略设置 - 设备控制 权限，才能编辑应用程序控制策略。
- 您不能编辑应用于您的活动子领域之外的策略。

要了解更多信息，请参阅 管理角色和子领域 （第 12 页）。

1. 检查哪个设备控制策略被您想要配置的计算机组所采用了。
   请参阅查看组采用的策略 （第 23 页）。
2. 在 策略 窗格板中，双击 设备控制。然后，双击您想要更改的策略。
3. 在 设备控制策略 对话框的 配置 标签页中，勾选 启用设备控制扫描 勾选框。
4. 取消勾选 检测但不阻断设备 勾选框。
5. 如果您尚未这样做，那么，更改您想要阻断的设备的状态为“已阻断”。（有关详细信息，请参见选择想要控制的应用程序 （第 121 页）。）
   单击 确定。

7.5.6 从所有策略中免除设备

如果您使用基于角色的管理，那么：

- 您必须具备 策略设置 - 设备控制 权限，才能编辑应用程序控制策略。
- 您不能编辑应用于您的活动子领域之外的策略。

要了解更多信息，请参阅 管理角色和子领域 （第 12 页）。

您可以从所有的策略中免除设备，包括默认的策略。该免除随后将会被添加到您创建的所有新策略中。

您可以免除设备实例（“仅限此设备”）或者，免除特定设备型号（“此型号 ID 的所有设备”）。请勿对同一设备在型号 ID 和设备实例级别上设置多种免除。如果同时定义了两者，那么，设备实体的设置将优先。

要从所有设备控制策略中免除设备：

1. 在 事件 菜单中，单击 设备控制事件。
   会出现 设备控制 - 事件查看器 对话框。

2. 如果您只想查看特定的事件，请在 搜索标准 窗格板中，设置合适的筛选项，然后，单击 搜索 按钮，以显示事件。

   要了解更多信息，请参见关于设备控制事件 （第 135 页）。

3. 选择您想从策略中免除的设备项目，然后，单击 免除设备。

   会出现 免除设备 对话框。在设备详情中，您可以看到设备的类型、型号、型号 ID 和设备 ID。在免除详情 的 范围 中，您可以看到“所有策略” 字样。

   注释
   如果没有您想要免除的设备的事件，例如，某端点计算机上内建的 CD 或 DVD 驱动器，那么，请到带有此设备的计算机上，在 “设备管理器” 中启用此设备。（要访问“设备管理器”，请右击 我的电脑，单击 管理，然后，单击 设备管理器。）这将生成新的“阻断”事件，它将出现在 设备控制 - 事件查看器 对话框中。您然后可以按照此步骤中先前的说明来免除该设备。

4. 选择您想免除“仅限此设备”或“此型号 ID 的所有设备”。
5. 选择您想允许“完全访问”或“只读访问”该设备。
6. 在 说明 栏中，如果愿意，输入您的说明文字。例如，您可以说明是谁要求免除该设备的。
7. 单击 确定。

7.5.7 从单个策略中免除设备

如果您使用基于角色的管理，那么：

- 您必须具备 策略设置 - 设备控制 权限，才能编辑应用程序控制策略。
- 您不能编辑应用于您的活动子领域之外的策略。

要了解更多信息，请参阅 管理角色和子领域 （第 12 页）。

您可以从设备控制策略中免除特定的设备。

您可以免除设备实例（“仅限此设备”）或者，免除特定设备型号（“此型号 ID 的所有设备”）。请勿对同一设备在型号 ID 和设备实例级别上设置多种免除。如果同时定义了两者，那么，设备实体的设置将优先。

要从单个策略中免除设备：

1. 检查哪个设备控制策略被您想要配置的计算机组所采用了。

   请参阅查看组采用的策略 （第 23 页）。

2. 在 策略 窗格板中，双击 设备控制。然后，双击您想要更改的策略。
3. 在 设备控制策略 对话框的 配置 标签页中，单击 添加免除项目。
   会出现 设备控制 - 事件查看器 对话框。
4. 如果您只想查看特定的事件，请在 搜索标准 窗格板中，设置合适的筛选项，然后，单击 搜索 按钮，以显示事件。

   要了解更多信息，请参见关于设备控制事件 （第 135 页）。

5. 选择您想从策略中免除的设备项目，然后，单击 免除设备。

   会出现 免除设备 对话框。在设备详情中，您可以看到设备的类型、型号、型号 ID 和设备 ID。在免除详情 的 范围 中，您可以看到“仅限此策略”字样。

注释
如果没有您想要免除的设备的事件，例如，某端点计算机上内建的 CD 或 DVD 驱动器，那么，请到带有此设备的计算机上，在 “设备管理器” 中启用此设备。（要访问“设备管理器”，请右击 我的电脑，单击 管理，然后，单击 设备管理器。）这将生成新的“阻断”事件，它将出现在 设备控制 - 事件查看器 对话框中。您然后可以按照此步骤中先前的说明来免除该设备。

6. 选择您想免除“仅限此设备”或“此型号 ID 的所有设备”。
7. 选择您想允许“完全访问”或“只读访问”该设备。
8. 在 说明 栏中，如果愿意，输入您的说明文字。例如，您可以说明是谁要求免除该设备的。
9. 单击 确定。

7.5.8 查看或编辑免除设备列表

如果您使用基于角色的管理，那么：

- 您必须具备 策略设置 - 设备控制 权限，才能编辑应用程序控制策略。
- 您不能编辑应用于您的活动子领域之外的策略。

要了解更多信息，请参阅 管理角色和子领域 （第 12 页）。

要查看或编辑免除设备列表：

1. 检查哪个设备控制策略被您想要配置的计算机组所采用了。
   请参阅查看组采用的策略 （第 23 页）。
2. 在 策略 窗格板中，双击 设备控制。然后，双击您想要更改的策略。
3. 在 设备控制策略 对话框的 配置 标签页中，选择您想要查看的免除设备类型，例如：光盘驱动器。单击 查看免除项目。
   会出现 <设备类型> 免除项目 对话框。如果是免除某型号 ID 的所有设备，那么，设备 ID 栏将是空白。
4. 如果您想要编辑免除设备列表，请按照以下说明之一做：
   - 如果您想要添加免除项目，请单击 添加。要了解更多信息，请参见从单个策略中免除设备 （第 139 页）。
   - 如果您想要编辑免除项目，请选择该免除项目，并单击 编辑。编辑 免除设备 对话框中相应的设置。
   - 如果您想要删除免除项目，请选择该免除项目，并单击 删除。

     这将从您正在编辑的策略中删除免除项目。如果您想从其他策略中删除该设备，请在各个策略中重复此任务中的这些步骤。

7.6 介入防范策略

介入防范使您能够防范已知的恶意软件，以及防止未经授权的用户（对计算机安全了解不多的本地管理员和用户）通过 Sophos Endpoint Security and Control 用户界面，卸载或禁用 Sophos 安全软件。

注释
介入防范不针对具备丰富的计算机技术知识的用户。它也无法防范专门瓦解操作系统的检测功能的恶意软件。此类的软件只能通过对安全隐患和可疑行为的扫描，才能被发现。（要了解更多信息，请参见防病毒和 HIPS 策略 （第 67 页）。）

在您启用了介入防范，并创建了介入密码之后，终结点计算机上的 SophosAdministrator 组中不知道密码的成员，将不能够：

- 在 Sophos Endpoint Security and Control 中重新配置读写扫描或可疑行为检测设置。
- 禁用介入防范。
- 卸载 Sophos Endpoint Security and Control（Sophos Anti-Virus，Sophos Client Firewall，Sophos AutoUpdate，或 Sophos Remote Management System）。

如果您想要启用 SophosAdministrators 执行这些任务，您必须向他们提供介入防范密码，这样他们才能够在介入防范中进行身份验证。

介入防范不会影响 SophosUser 和 SophosPowerUser 组中的成员。当介入防范启用时，他们将能够执行所有通常已经授权执行的任务，并不需要输入介入防范密码。

注释
如果您使用基于角色的管理，那么：

- 您必须具备 策略设置 - 介入防范 权限，才能配置介入防范策略。
- 您不能编辑应用于您的活动子领域之外的策略。

要了解更多信息，请参阅 管理角色和子领域 （第 12 页）。

介入防范事件

当出现介入防范事件时，例如，阻止了某个未经授权的用户试图卸载某个终结点计算机上的 Sophos Anti-Virus 时，该事件会被记录到日志中，并可以从 Enterprise Console 中查看该日志记录。有关详细信息，请参见查看介入防范事件 （第 164 页）。

介入防范事件有两种类型：

- 顺利的介入防范验证事件，显示已验证的用户的名称，以及验证的时间。
- 不成功的介入尝试事件，显示涉及的 Sophos 软件产品或组件的名称，介入尝试的时间，以及进行介入尝试的用户的详情。

7.6.1 开启或关闭介入防范

如果您使用基于角色的管理，那么：

- 您必须具备 策略设置 - 介入防范 权限，才能配置介入防范策略。
- 您不能编辑应用于您的活动子领域之外的策略。

要了解更多信息，请参阅 管理角色和子领域 （第 12 页）。

要开启或关闭介入防范：

1. 检查您想要配置的计算机组所采用了哪个介入防范策略。
   请参阅查看组采用的策略 （第 23 页）。
2. 在 策略 窗格板中，双击 介入防范。然后，双击您想要更改的策略。

3. 在 介入防范策略 对话框中，勾选或取消勾选 启用介入防范 勾选框。
   如果您是首次启用介入防范，请单击 密码 框下的 设置。在 介入防范密码 对话框中，输入并确认密码。

   提示
   我们建议密码长度应该至少有 8 个字符，并且包含大小写字母和数字。

7.6.2 更改介入防范密码

要更改介入防范密码

1. 检查您想要配置的计算机组所采用了哪个介入防范策略。
   请参阅查看组采用的策略 （第 23 页）。
2. 在 策略 窗格板中，双击 介入防范。然后，双击您想要更改的策略。
3. 在 介入防范策略 对话框中，单击 密码 文本框下的 更改。在 介入防范密码 对话框中，输入并确认新的密码。

   提示
   密码长度应该至少有 8 个字符，并且包含大小写字母和数字。

7.6.3 关于增强的防篡改保护

增强的防篡改保护以防篡改保护功能为基础。如果启用增强的防篡改保护，将阻止 Sophos Anti-Virus、Sophos AutoUpdate、Sophos Management Communication System、Sophos Remote Management System 和 Sophos Endpoint Defense 的以下操作：

- 从服务用户界面停止服务
- 从任务管理器用户界面停止服务
- 从服务用户界面修改服务配置
- 从命令行停止服务/编辑服务配置
- 卸载
- 重新安装
- 从任务管理器用户界面停止进程
- 删除或修改受保护的文件或文件夹
- 删除或修改受保护的注册表项

重要提示
要启用增强的防篡改保护，必须启用防篡改保护。如果禁用防篡改保护，将自动禁用增强的防篡改保护。

7.6.4 增强的防篡改保护设置

1. 在 策略 窗格板中，双击 介入防范。然后，双击您想要更改的策略。

2. 在防篡改保护策略对话框中，确保选中启用防篡改保护复选框，然后选中启用增强的防篡改保护复选框。
3. 如果这是新安装或更新，请在防篡改保护策略对话框中，单击密码框下的设置。

   如果防篡改保护已启用，请单击密码框下的更改。在 介入防范密码 对话框中，输入并确认密码。

   注释
   防篡改保护和增强的防篡改保护使用相同的密码。启用增强的防篡改保护后，它将取代防篡改保护。这是设置防篡改保护密码后必须修改密码的原因。

   我们建议您对每个策略使用不同的密码。

7.7 补丁策略

注释
此功能没有包括在所有的用户授权使用许可协议中。如果您想要使用它，您可能需要更改您的用户授权使用许可协议。要了解更多信息，请参见http://www.sophos.com/zh-cn/products/complete/comparison.aspx。

Enterprise Console 使您能够检查计算机是否安装了及时更新的补丁。

SophosLabs 提供的评级可以帮助您了解最重要的安全补丁问题，以便您能够迅速解决它们。SophosLabs 的评级将考虑最新的安全实例，因此该评级可能与软件商提供的严重性级别不同。

在使用补丁之前，您必须在联网的计算机上安装补丁代理，这样它们才能够执行补丁评估，并将评估情况发送给 Enterprise Console。您可以通过 保护计算机向导 安装 NAC 代理。请参阅自动保护计算机 （第 39 页）。

本节假定您已安装了补丁代理。

注释
如果您使用基于角色的管理，那么：

- 您必须具备 策略设置 - 补丁 权限，才能配置补丁策略。
- 您不能编辑应用于您的活动子领域之外的策略。

要了解更多有关基于角色的管理的信息，请参见管理角色和子领域 （第 12 页）。

7.7.1 补丁评估怎样工作？

“补丁评估”在默认策略中是禁用的。一旦启用了补丁评估，计算机立即就会进行一次评估。这会花费几分钟的时间。以后的评估则按照在策略中设定的频率进行，它的默认值为每天一次。

注释
如果计算机在 Enterprise Console 首次从 Sophos 下载补丁数据之前，就进行评估，那么，“补丁事件”查看器中不会显示任何结果。下载可能会花费数小时。要检查这是否已完成，请在 事件 > 补丁评估事件 中查看 补丁更新文件 栏。

如果补丁代理（无论由于何种原因）无法从 Enterprise Console 进行更新，那么，它会继续使用先前下载的补丁检测文件对计算机进行评估。

评估只针对安装在计算机上的软件的安全补丁。如果替换旧补丁的新补丁已发布，那么，补丁评估将不会再检查旧补丁是否存在。只有新补丁会被评估。

什么是被替换的补丁？

如果某个软件商发布新的补丁用来替代较早的补丁，那么，新的补丁就称为替换补丁。较早的补丁被称为被替换的补丁。

Sophos 建议您安装替换补丁以保证计算机及时更新。

示例：如果您搜索病毒 X， 发现用于防范此病毒的补丁 P01已被补丁 P02 替换，那么，Sophos 建议您安装 P02。

7.7.2 关于补丁评估事件

当发生补丁评估事件时，例如，某计算机遗漏了某个补丁，该事件会被发送到 Enterprise Console 中，并且可以在 补丁评估 - 事件查看器 中查看它。

在 补丁评估 - 事件查看器 中，您可以使用筛选挑选仅仅显示您感兴趣的事件。您还可以将补丁评估事件列表导出到文件中。有关详细信息，请参见补丁评估事件 （第 164 页）和导出事件列表到文件中 （第 169 页）。

7.7.3 开启或关闭补丁评估

如果您使用基于角色的管理，那么：

- 您必须具备 策略设置 - 补丁 权限，才能配置补丁策略。
- 您不能编辑应用于您的活动子领域之外的策略。

要了解更多信息，请参阅 管理角色和子领域 （第 12 页）。

要开启或关闭补丁评估：

1. 请检查您想要配置的计算机组采用了哪个补丁策略。
   请参阅查看组采用的策略 （第 23 页）。
2. 在 策略 窗格板中，双击 补丁。然后，双击您想要更改的策略。
3. 在 补丁策略 对话框中，取消勾选 启用补丁评估 勾选框，并单击 确定。

7.7.4 选择补丁评估的频率

如果您使用基于角色的管理，那么：

- 您必须具备 策略设置 - 补丁 权限，才能配置补丁策略。
- 您不能编辑应用于您的活动子领域之外的策略。

要了解更多信息，请参阅 管理角色和子领域 （第 12 页）。

要设定补丁评估的频率：

1. 请检查您想要配置的计算机组采用了哪个补丁策略。
   请参阅查看组采用的策略 （第 23 页）。
2. 在 策略 窗格板中，双击 补丁。然后，双击您想要更改的策略。
3. 在 补丁策略 对话框中，单击 评估遗漏的补丁 栏中的下拉菜单，并选择相应的间隔。单击 确定。
   要按照此频率进行评估，必须在此策略中启用补丁评估。

7.8 网页控制策略

注释
此功能没有包括在所有的用户授权使用许可协议中。如果您想要使用它，您可能需要更改您的用户授权使用许可协议。要了解更多信息，请参见http://www.sophos.com/zh-cn/products/complete/comparison.aspx（英文）。

默认情况下，在 Enterprise Console 中网页控制策略会被关闭。选择 启用网页控制 将使您能够选择以下策略选项之一：

- 不合适的网站控制：此基本网页控制选项包括 14 种基本的网站分类。它的目的在于防止用户访问可能会使公司因此承担法律的责任的那些网站。要了解更多信息，请参见不合适的网站控制 （第 145 页）。
- 完全网页控制：此选项应用综合全面的策略，涵盖 50 多个网站分类。它要求 Sophos Web Appliance、Sophos Management Appliance 或者 Sophos UTM Appliance（9.2 版本或者更高）与终结点计算机进行同步，以便分发策略更新，以及收集网页活动数据。要了解更多信息，请参见完全网页控制 （第 149 页）。

在使用“不合适的网站控制”时，您既可以编辑现有的网页控制策略，也可以创建新的策略。要了解更多信息，请参见创建策略 （第 27 页）。您可以设置 “阻断，”“警告，” 或 “允许” 不同的网站类别。网页控制状态和网页事件显示会在 Enterprise Console 中。要了解更多有关网页事件的信息，请参见查看网页事件 （第 167 页）。

如果您使用的是“完全网页控制策略”，那么，Enterprise Console 则需要 Web、UTM、或 Management Appliance 的路径，完全的网页筛选策略将在那里配置，并且还配置共享密钥，以保证设备和 Enterprise Console 之间的安全通讯。在选择了“完整网页控制策略”后，大多数的报告和监控功能会被移至设备；不过，Sophos Endpoint Security and Control 的实时 URL 过滤机制（Web 保护 （第 85 页））扫描和评估的网站，会作为网页事件显示在 Enterprise Console 中。

要了解更多有关网页控制的信息，请参见Endpoint 网页控制概要指南。

注释
如果您使用基于角色的管理，那么：

- 您必须具备 策略设置 - 网页控制 权限，才能编辑网页控制策略。
- 您不能编辑应用于您的活动子领域之外的策略。

要了解更多有关基于角色的管理的信息，请参见管理角色和子领域 （第 12 页）。

7.8.1 不合适的网站控制

注释
此功能没有包括在所有的用户授权使用许可协议中。如果您想要使用它，您可能需要更改您的用户授权使用许可协议。要了解更多信息，请参见http://www.sophos.com/zh-cn/products/complete/comparison.aspx。

使用基本网页控制，您可以基于 14 种网站类别过滤用户的网页访问行为。针对每个类别，都有默认的措施（请见关于网站类别 （第 146 页）中的说明），但是，如果需要，您也可以按照选择网站类别措施 （第 148 页）中的说明，选择不同的措施。

用户访问受限制的网站时，可能被阻断。被引发的事件会向用户显示，并发送到Enterprise Console。

或者，当用户访问受控网站时，会收到警告；即使用户没有继续进行，仍然会引发警告事件。如果用户忽视警告，继续访问网站，那么，会引发第二个事件，并发送到 Enterprise Console。

注释
尽管 HTTP 协议和 HTTPS 协议的网站在所有受支持的网页浏览器中都受到过滤，但根据 URL 是 HTTP 协议还是 HTTPS 协议，用户收到的通告不同。如果是 HTTP 协议的网站，用户可以收到类别中的网站设置为 “阻断” 或 “警告”。如果是 HTTPS 协议的网站，用户仅能收到 “阻断” 通告，它们以气球状提示出现在 Windows 系统托盘中。HTTPS 协议网站的 “警告” 措施，既不会向用户显示，也不会记录在日志中。相反，用户会被允许继续访问所请求的网页，引发的事件会以“继续”措施被日志记录在 Enterprise Console 中。

如果您针对某个网站类别的选择是 “允许” 措施，用户则可以访问此类别中的所有网站，除非指定了网站例外。当选择了 不合适的网站控制 时，“允许” 措施将不会记录到日志中。

注释
被允许的网站仍然会被 Sophos Endpoint Security and Control 的实时 URL 过滤机制（网页保护）扫描和评估。

开启完全网站控制

执行以下步骤以开启 Enterprise Console 中的网页控制，并使用“不合适的网站控制”。

注释
如果您使用基于角色的管理，那么：

- 您必须具备 策略设置 - 网页控制 权限，才能编辑网页控制策略。
- 您不能编辑应用于您的活动子领域之外的策略。

要了解更多有关基于角色的管理的信息，请参见管理角色和子领域 （第 12 页）。

要开启不合适的网站控制：

1. 检查您想要配置的计算机组所采用的是哪个网页控制策略。要了解更多信息，请参阅 查看组采用的策略 （第 23 页）。
2. 在 策略 窗格板中，双击 网页控制。然后，双击您想要更改的策略。
   会出现 网页控制策略 对话框。
3. 在 常规 标签页中，选择 启用网页控制。
   会出现 不合适的网站控制 策略。尽管针对 14 种网站类别中的每个类别，都有默认的措施，您仍然可以设置不同的措施。要了解更多信息，请参见选择网站类别措施 （第 148 页）。

关于网站类别

通过选择 不合适的网站控制，您可以配置 14 种网站类别，控制用户可以通过网页浏览器访问的因特网内容。要了解更多信息，请参见不合适的网站控制 （第 145 页）。

以下描述的网站类别会被过滤。针对各个类别的默认措施，如括号内所示。每个类别可以被配置为 阻断，警告，或 允许。选择 允许 可以使用户能够访问类别中的所有网站。要更改措施，请参见选择网站类别措施 （第 148 页）。

- 成人内容/性暴露（阻断）：此类别中的网站包括成人产品；孩童色情，娈童；成人服务；黄色文字，露骨的性描写；性暴露的卡通和动画；在线色情论坛；以色情为目的的裸露人体网站；露骨

的性行为描绘或图片；色情暴力文字或图片；性游戏及癖好；裸体自然主义网站；露骨裸体刻画摄影。

注释
但不包括有关性健康，乳腺癌，或性传播疾病（除提供图片示例的网站以外）的网站。

- 酒精与烟草（警告）：此类别中包括促销或以免费或收费方式提供酒精或烟草的网站。
- 匿名代理服务器（阻断）：此类别中包括提供远程代理或匿名访问的网站，提供搜索引擎快照以绕开过滤的网站，以及绕开过滤的基于网页的翻译网站。
- 犯罪行为（阻断）：此类别中包括怂恿，教唆，指导违法行为的网站；提供逃避法律制裁的建议的网站；以及提供开锁和入室盗窃技巧的网站。
- 赌博（警告）：此类别中包括使用真实货币或虚拟货币的在线赌博，彩票网站；为参与彩票，赌博，数字抽奖等提供押注信息或建议的网站；虚拟赌场和离岸赌博活动的网站；体育抽奖和押注网站；押注金额巨大，高额回报的虚拟体育和虚拟联赛的网站。
- 黑客（阻断）：此类别中包括为使用可疑或非法设备获取密码，制造病毒，获取访问他人的计算机系统或计算机化的通讯系统，提供推广，指导，或建议的网站；为绕开过滤软件提供具体指导的网站；提供破解软件和破解信息的网站；提供 Warez 的网站；盗版软件和多媒体下载网站；以及计算机犯罪网站。
- 非法药品（阻断）：此类别中包括为制造非工业用目的的禁药/成分，提供配方，指导或工具的网站；美化，鼓励，或指导使用或掩盖使用酒精，烟草，禁药，或其它对未成年人视为非法的物品的网站；提供“合法兴奋药品”信息，包括吸胶毒，滥用处方药，或滥用其它合法物品的网站；免费或收费分发非法药品的网站；以及陈列，贩卖，或详细说明药物使用的网站。
- 狭隘与仇恨（阻断）：此类别包括主张或煽动羞辱或攻击基于某种联系（如：宗教，种族，国籍，性别，年龄，残障，或性向）而形成的人群或风俗的网站；宣传某种基于种族，宗教，国籍，性别，年龄，或性向等原因而排斥他人的，本质上是种族优越论的政治或社会主张的网站；否认纳粹大屠杀或为其翻案的网站，以及其它煽动仇恨的翻案者的网站；胁迫他人加入或招募成员加入帮会[1]或邪教[2] 的网站； 激进分子和极端分之的网站；提供肆无忌惮地，冷漠无情地冒犯他人的材料，包括不承认或不尊重不同意见和信仰的材料的网站。

  注释
  不包括可能符合上述标准的新闻，历史，媒体报道网站（以图片形式提供示例的除外）。

  [1]帮会是指以进行严重犯罪为基本活动的团体。它具有统一的名称，或识别符号，标志，其成员以帮会的名义单独或者共同实施犯罪活动。

  [2] 邪教是指其成员是受欺骗或被操纵加入，并且滞留其中深受影响，以至个性与行为方式均发生改变，而形成的团体。团体的上层权力无边，信奉独断专行，个人意愿服从于团体，而团体则独行与社会之外。
- 诱骗与诈骗（阻断）：此类别包括诱骗，电话诈骗，服务盗用建议网站，以及剽窃作弊网站，包括贩卖研究论文的网站。
- 垃圾邮件 URL（阻断）：此类别包括在垃圾邮件中发现的 URL，特别是有关：计算机，金融与股票，娱乐，游戏，健康与医药，幽默与小玩意，私人事宜与约会，产品与服务，购物，以及旅游。
- 间谍软件（阻断）：此类别包括帮助或从事在计算机终端用户或公司不知情，或不尽知情的情况下，收集或跟踪他们的信息的网站；带有恶意软件或病毒，第三方监控，以及其它不请自来的广告软件，间谍软件，以及恶意的“回叫”来电软件的网站。
- 庸俗与冒犯（警告）：此类别包括在提供的笑话，漫画，讽刺小品中充满粗言秽语，大不敬，或下流动作的网站。

- 暴力（警告）：此类别包括演示，描述或鼓励对人，动物进行肉体攻击的网站；渲染折磨，肢解，撕咬，或恐怖的死亡景象的网站；宣扬，鼓励，或者描述自虐，（包括通过饮食紊乱，成瘾等方式）自杀的网站；为制造炸弹，或制造其它以伤害或破坏为目的的设备提供指导，说明，或工具的网站；鼓吹恐怖行为的网站；以及极度暴力的体育运动或游戏（包括影像和在线游戏）。

  注释
  不包括可能符合上述标准的新闻，历史，媒体报道网站（以图片形式提供示例的除外）。

- 武器（警告）：此类别包括提供在线购买或订购武器信息（包括价目表和供应商地址）的网站；大量提供出售枪支弹药，或有毒物质的网站链接的网站；显示或详细说明如何使用枪支弹药，或有毒物质的网站；以及提供机关枪，自动步枪，其它攻击武器，和狙击手培训的俱乐部。

  注释
  武器的含义为可以用于伤害，击倒，毁灭他人的东西（如：棒球棒，刀具，或枪支等）。

选择网站类别措施

在开启了网页控制，并选择了 不合适的网站控制 策略，您可以配置针对各个网站类别的措施。您还可以创建基于默认策略的新策略。要了解更多信息，请参见创建策略 （第 27 页）。

要选择网站类别措施：

1. 在 常规 标签页中的您想要配置的网站类别旁的下拉菜单列表中，选择以下选项之一：
   - 阻断：防止用户访问此类别中的网站。如果被阻断的是 HTTP 网页，那么，会向用户显示阻断通告，解释为何网站会被阻断。如果被阻断的是 HTTPS 网页，那么，会在 Windows 系统托盘中向用户显示气球状提示。
   - 警告：警告用户他们可能违反公司的网站使用规定，但是允许他们继续。如果要访问的是 HTTP 网页，那么，会向用户显示警告通告，提醒他们小心访问此网站。如果要访问的是 HTTPS 网页，用户不会收到任何通告，将被允许继续访问此网站。此事件会在 Enterprise Console 中被日志记录为 “继续”。
   - 允许：允许用户访问此类别中的网站。此事件不会被日志记录。
2. 单击 确定。

管理网站例外

如果您已经选择了 不合适的网页控制 策略，您可以创建 “阻断” 和 “警告” 措施的例外。将网站添加到 “要允许的网站” 列表或 “要阻断的网站” 列表中，您可以使这些网站免除过滤机制的检查。条目可以使用 IP 地址或域名的形式。您也可以编辑现有的网站条目，将它们从列表中删除。

注释
如果在“阻断”和“允许”列表之间有冲突或重复的条目，那么，在“阻断”列表中的条目具有优先权。例如，如果在“阻断”列表和“允许”列表都包含一个相同的 IP 地址，那么，该网站将会被阻断。另外，如果某个域名包含在“阻断”列表中，但是它的子域名包含在“允许”列表中，那么，“允许”列表中的条目会被忽略，该域名及其所有子域名都将被阻断。

要添加网站例外：

1. 在 网站例外 标签页中，单击 要允许的网站 或 要阻断的网站 旁的 添加 按钮。
2. 在 添加允许的网站 对话框中，单击 主机名，带有子网掩码的 IP 地址，或 IP 地址。各种格式的示例，显示在相关的文本框的上方。

3. 在文本框中，输入您想要允许或阻断的网站的域名或 IP 地址。
4. 单击 确定。

如果您想编辑网站或从列表中删除网站，请勾选网站，并相应地单击 编辑 或 删除。

7.8.2 完全网页控制

注释
此功能没有包括在所有的用户授权使用许可协议中。如果您想要使用它，您可能需要更改您的用户授权使用许可协议。要了解更多信息，请参见http://www.sophos.com/zh-cn/products/complete/comparison.aspx。

如果您使用 Sophos Web Appliance、Sophos Management Appliance 或 Sophos UTM Appliance（9.2 版本或更高），那么，您可以通过 Enterprise Console 将基于设备的策略分布给用户。

终结点计算机与 Enterprise Console 的通讯，与选择“不合适网站控制”策略的通讯相同，但是网页过滤规则和网页活动日志记录则与您指定的设备进行同步化。此策略保存在终结点计算机上，并基于最新的 Sophos 数据进行应用。

根据网页控制策略，用户会被阻断，警告，以及允许。您可以使用 Web Appliance 或 Management Appliance 中的报告和搜索功能，或者 UTM 设备中的日志记录和报告 > 网页保护选项查看用户活动数据。所有网页控制事件均已记录在设备中；但是，被 Sophos Endpoint Security and Control 的实时 URL 过滤机制（网页保护）扫描和评估的网站被将作为网页事件记录在 Enterprise Console 中。

注释
尽管 HTTP 协议和 HTTPS 协议的网站在所有受支持的网页浏览器中都受到过滤，但是在 Web Appliance 或者 Management Appliance 中，根据 URL 是 HTTP 协议还是 HTTPS 协议，用户收到的通告不同。如果是 HTTP 协议的网站，用户可以收到类别中的网站设置为 “阻断” 或 “警告”。如果是 HTTPS 协议的网站，用户仅能收到 “阻断” 通告，它们以气球状提示出现在 Windows 系统托盘中。HTTPS 协议网站的 “警告” 措施，既不会向用户显示，也不会记录在日志中。相反，用户会被允许继续访问所请求的网页，引发的事件会以“继续”措施被日志记录在 Web Appliance 或 Management Appliance 中。

UTM 设备使用称为 Sophos LiveConnect 的中央云基服务来保护和监控终结点计算机。LiveConnect 允许您始终管理您所有的终结点计算机，无论它们是在您的本地网络、远程站点或是用于旅行用户——策略的更新文件都能够部署给用户，以及上传来自终结点计算机的报告数据（即使当用户没有连接在网络中时）。

使用 Management Appliance 或 Web Appliance 时，终结点计算机可直接或通过 Sophos LiveConnect 与该设备通讯。

在选择了 完全网页控制 的情况下，会应用功能完全的策略。根据您所使用的设备，与基本网页控制相比，完全网页控制提供更多的优点：

- 基于超过 50 种类别的 URL，用户得到警告或被阻断。
- 可以应用细分的 “特殊时间” 策略。
- 许许多多的附加策略，可以针对默认的和“特殊时间”的策略，用于单个用户例外或单个组例外。
- 在 Web Appliance、Management Appliance 或 UTM 设备上提供了详细的日志记录和报告。
- LiveConnect 使您能够部署策略更新和上传报告数据，即使用户使用的是远程连接。
- 用户可以提交有关处理被阻断的 URL 的反馈。
- 自定义显示给用户的通告页面，其中包括公司标识，以及与公司相关的文字陈述。要了解更多信息，请参见 Sophos Web Appliance 技术文档。

- 在启用了 SafeSearch 之后，用户会自动被限制浏览从流行的搜索引擎中获取的不合适的网站。

要了解更多有关配置完全Web Appliance策略的信息，请参见在http://wsa.sophos.com/docs/wsa/中提供的Sophos Web Appliance文档。

UTM Appliance 文档可以在 http://www.sophos.com/zh-cn/support/documentation/sophos-utm.aspx 中找到。

开启完全网页控制

注释
以下进行的步骤，假定您安装并配置了功能运作正常的 Sophos Web Appliance、Sophos Management Appliance 或 Sophos UTM 设备（9.2 版本或更高），并且使用 Endpoint Web Control。

依照默认值，网页控制策略会被关闭。执行以下步骤，以启用网页控制，并使用完全网页控制策略。

注释
如果您使用基于角色的管理，那么：

- 您必须具备 策略设置 - 网页控制 权限，才能编辑网页控制策略。
- 您不能编辑应用于您的活动子领域之外的策略。

要了解更多有关基于角色的管理的信息，请参见管理角色和子领域 （第 12 页）。

要开启“完全网页控制”：

1. 检查您想要配置的计算机组所采用的是哪个网页控制策略。要了解更多信息，请参阅 查看组采用的策略 （第 23 页）。
2. 在 策略 窗格板中，双击 网页控制。然后，双击您想要更改的策略。
   会出现 网页控制策略 对话框。
3. 在 常规 标签页中，单击 启用网页控制。
4. 选择 完全网页控制。
5. 在设置面板中，输入设备主机名和策略交换的安全密钥。
   - 对于 Web Appliance 或者 Management Appliance，您必须提供完全限定的主机名。该密钥必须与设备的 Endpoint Web Control 页面中显示的那个密钥匹配。
   - 对于 UTM，输入主机名和 UTM 所使用的 Sophos LiveConnect 代理的共享密钥。它们可在 SEC 信息下的Sophos LiveConnect - 注册一节中，终结点保护 > 计算机管理 > 高级选项卡中，UTM 管理界面 WebAdmin 中找到。

   有关更多信息，请参见 http://wsa.sophos.com/docs/wsa/ 的 Sophos Web Appliance 文档，或参见 http://www.sophos.com/zh-cn/support/documentation/sophos-utm.aspx 的 UTM 设备文档。
6. 或者，选择 如果无法确定网站的分类，则阻断浏览。如果终结点计算机无法获取网站类别的数据，那么，无法归类的 URL 会被阻断，直到获取网站类别的服务恢复为止。
   此勾选框不是默认的勾选项，它使得用户在网站归类服务失败的情况下，可以继续浏览网页。
7. 单击 确定。
   Enterprise Console 重新配置终结点计算机以与 Web Appliance、Management Appliance 或 UTM 所使用的 Sophos LiveConnect 代理通讯。

7.9 漏洞防御策略

注释
此功能没有包括在所有的用户授权使用许可协议中。如果您想要使用它，您可能需要更改您的用户授权使用许可协议。要了解更多信息，请参阅 http://www.sophos.com/zh-cn/products/complete/comparison.aspx。

漏洞防御可用于:

- 防止文档文件受到勒索软件的攻击(CryptoGuard)。
- 防止引导扇区受到攻击 (WipeGuard)。

  重要提示
  此功能当前对于服务器不可用。

- 保护Web浏览器的重要功能(安全浏览)。
- 缓解攻击。可以保护最容易受到恶意软件攻击的应用程序，如 Java 应用程序。
- 防止进程挖空攻击。
- 防止从不信任的文件夹加载.DLL文件。
- 防止处理器分支跟踪。

默认情况下，漏洞防御和所有漏洞防御选项均已开启。

重要提示
如果您升级许可证并将 Exploit Prevention 包括在内，它不会在您已经在管理的计算机上自动安装。您需要重新保护计算机以安装该组件。请参阅自动保护计算机 （第 39 页）。

您可以在漏洞防御中排除应用程序。请注意，它们仍然受到CryptoGuard和安全浏览保护。

要了解更多有关针对漏洞防御的建议设置，请参 Sophos Enterprise Console 策略设置指南。

注释
如果您使用基于角色的管理，那么：

- 您必须具备 策略设置 - 漏洞防御 权限，才能配置漏洞防御策略。
- 您不能编辑应用于您的活动子领域之外的策略。

要了解更多信息，请参阅 管理角色和子领域 （第 12 页）。

HitmanPro.Alert和策略更新

HitmanPro.Alert可在终结点检测需要保护的应用程序。其会将检测到的应用程序报告给Sophos Enterprise Console服务器。服务器对需要保护的应用程序进行整理，并以每120分钟的间隔将新的应用程序数据合并到策略中。服务器将更新后的策略分发到终结点，并提供需要保护的应用程序列表。

7.9.1 开启或关闭漏洞防御

若要使用基于角色的管理：

- 您必须具备 策略设置 - 漏洞防御 权限，才能配置漏洞防御策略。
- 您不能编辑应用于您的活动子领域之外的策略。

要了解更多信息，请参阅 管理角色和子领域 （第 12 页）。

注释
默认情况下，漏洞防御和所有漏洞防御选项均已开启。

如需开启或禁用漏洞防御：

1. 检查哪个漏洞防御策略被您想要配置的计算机组所采用了。
   请参阅查看组采用的策略 （第 23 页）。
2. 在 策略 窗格板中，双击 漏洞防御。然后，双击您想要更改的策略。
3. 在漏洞防御策略对话框的保护设置标签中，选择或清除启用漏洞防御复选框。
4. 选中或清除 防止文档文件受到勒索软件的攻击(CryptoGuard) 复选框。
   您还可以选择是否防范远程运行的勒索软件（仅在64位终结点）。
5. 选中或清除 磁盘和启动记录保护(WipeGuard) 复选框。
6. 选中或清除 保护Web浏览器的重要功能(安全浏览) 复选框。
7. 选中或清除 缓解易受攻击应用程序中发生的攻击 复选框。
   您还可以选择要保护的应用程序类型，例如Microsoft Office应用程序。
8. 选中或清除阻止进程挖空攻击 复选框。
9. 选中或清除 阻止从不信任的文件夹加载 DLL 复选框。
10. 选中或清除 CPU分支跟踪 复选框。
11. 单击 确定。

您可以在漏洞防御中排除应用程序。请注意，如果选择了这些选项，它们仍然受到CryptoGuard和安全浏览保护。请参阅在漏洞防御中排除应用程序 （第 152 页）。

您还可以在漏洞防御中排除攻击事件。请参阅在漏洞防御中排除攻击事件 （第 153 页）。

7.9.2 在漏洞防御中排除应用程序

若要使用基于角色的管理：

- 您必须具备 策略设置 - 漏洞防御 权限，才能配置漏洞防御策略。
- 您不能编辑应用于您的活动子领域之外的策略。

要了解更多信息，请参阅 管理角色和子领域 （第 12 页）。

重要提示
默认情况下，易受攻击的应用程序将受到保护。在漏洞防御中排除应用程序时需要非常小心。它们仍然受到 CryptoGuard 和安全浏览保护，请参见开启或关闭漏洞防御 （第 152 页）。

您可以在漏洞防御中排除应用程序。您也可以选择保护之前已被排除的应用程序。

如需排除应用程序：

1. 检查哪个漏洞防御策略被您想要配置的计算机组所采用了。
   请参阅查看组采用的策略 （第 23 页）。
2. 在 策略 窗格板中，双击 漏洞防御。然后，双击您想要更改的策略。
3. 在应用程序排除对话框的排除项目标签中，选择您想要在受保护的应用程序列表中排除的应用程序，然后单击排除。
   这将把选中的应用程序移动到排除的应用程序列表中。
4. 要保护当前不包括在检查中的应用程序，请转到排除的应用程序列表，选择应用程序，然后单击包括。
5. 单击 确定。

7.9.3 在漏洞防御中排除攻击事件

若要使用基于角色的管理：

- 您必须具备 策略设置 - 漏洞防御 权限，才能配置漏洞防御策略。
- 您不能编辑应用于您的活动子领域之外的策略。

要了解更多信息，请参阅 管理角色和子领域 （第 12 页）。

重要提示

- 如果您排除攻击事件，将只排除特定的漏洞，而不是整个应用程序。
- 如果攻击事件是已经排除的应用程序的一部分，则无需排除该攻击事件。

您可以在漏洞防御中排除攻击事件。您也可以选择保护之前已经排除的攻击事件。

要排除攻击事件：

1. 检查哪个漏洞防御策略被您想要配置的计算机组所采用了。
   请参阅查看组采用的策略 （第 23 页）。
2. 在 策略 窗格板中，双击 漏洞防御。然后，双击您想要更改的策略。
3. 在漏洞防御策略对话框的漏洞排除选项卡中，选择要在检测到的攻击事件列表中排除的攻击事件，然后单击排除。
   将把选定的攻击事件移入排除的攻击事件列表
4. 要保护当前不包括在检查中的攻击事件，请转到排除的攻击事件列表，选择事件，然后单击包括。
5. 单击确定。

8 设置警报和消息

在 Enterprise Console 中有数种发送警报的方法可供使用。

- 在控制台中显示的警报

  如果在计算机中发现了需要关注的项目，或者出现了错误，Sophos Endpoint Security and Control 会向 Enterprise Console 发送警报。在计算机列表中显示的警报。要了解更多有关软件预订的电子邮件警报的信息，请参见处置检测到项目的警报 （第 43 页）。

  这些警报总是会被显示。您不必设置它们。

- 在控制台中显示的事件。

  端点计算机上出现应用程序控制、防火墙、补丁评估、网页、数据控制、设备控制或防篡改保护事件时，如应用程序被防火墙阻止，该事件将发送到 Enterprise Console，并且可以在相应的事件查看器中查看。

- 控制台发送给您选择的收件人的警报和消息

  依照默认值，当某个项目在计算机中被发现时，消息会显示在计算机桌面上，会在 Windows 事件日志中添加有关条目。当发生应用程序控制，数据控制，或设备控制事件时，消息会显示在计算机桌面上。

  注释
  用户定义的可选桌面消息不会显示在运行 Windows 8 或以后版本的计算机上。

  您还可以为系统管理员设置电子邮件警报或 SNMP 消息。

  注释
  如果您想要使用经过验证的 SMTP 发送电子邮件警报，请参见Sophos 知识库文章 113780。

本节将说明怎样设置发送给您选择的收件人的警报。

8.1 设置软件预订警报

如果您使用基于角色的管理，那么，您必须具有 系统配置 权限，才能执行此任务。要了解更多信息，请参见管理角色和子领域 （第 12 页）。

Enterprise Console 会显示更新管理器在 更新管理器 视图的 警报 栏中给出的警报。如果您预订了固定版本的软件，当该版本即将淘汰或已淘汰时，会出现警报。如果您的产品的用户授权使用许可协议已更改，那么，会出现提示。

如果预订了固定版本的软件，同时选择了当 Sophos 不再支持该软件时自动升级固定版本软件，则您的预订将会自动升级。

如果您没有选择自动升级，您将被指导更改您的预订。

重要提示
运行不再支持的软件，将使您无法防范新出现的安全隐患。我们建议尽快更新到受支持的版本。

您还可以设置电子邮件警报，当您预订的产品的版本即将淘汰或已淘汰时，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。
   a) 在 服务器地址 文本框中，输入主机名或 SMTP 服务器的 IP 地址。
   b) 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。
   c) 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“软件预订”电子邮件警报。您可以预订三种警报：
   - 软件预订中包含很快就要被 Sophos 淘汰的产品版本
   - 软件预订中包含已被淘汰的产品版本。
     如果您预订的产品已被淘汰，或者，您的用户授权使用许可协议已更改，而新的用户授权使用许可协议中没有包含该产品，那么，警报就会被发出。
   - Sophos 用户授权使用许可协议已更新。产品的功能已更改。

8.2 设置防病毒和 HIPS 电子邮件警报

如果您使用基于角色的管理，那么：

- 您必须具备 策略设置 - 防病毒和 HIPS 权限，才能执行此任务。
- 您不能编辑应用于您的活动子领域之外的策略。

要了解更多信息，请参阅 管理角色和子领域 （第 12 页）。

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。

重要提示
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 对话框中，单击 消息发送。
3. 在 消息发送 对话框中的 电子邮件警报发送 标签页中，选择 启用电子邮件警报发送。
4. 在 要发送的消息 窗格板中，选择想要针对它发送电子邮件警报的事件。

   注释
   可疑行为检测，可疑文件检测，广告软件和可能不想安装的应用程序检测和清除，以及 其它错误 等的设置仅仅应用于 Windows 计算机。

5. 在 收件人 面板中，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。

重要提示
Mac OS X 计算机将只向列表中的第一个收件人发送邮件。

6. 单击 配置 SMTP，更改 SMTP 服务器和电子邮件警报语言的设置。
7. 在 配置 SMTP 设置 对话框中，按照以下说明输入详情。
   - 在 SMTP 服务器 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。
   - 在 SMTP 寄件人地址 文本框中，输入退回邮件和未送达报告将要寄往的地址。
   - 在 SMTP 回复地址 文本框中，您可以在文本框中，输入电子邮件警报的回复地址。电子邮件警报是从无人照管的邮箱发出的。
   - 在 语言 面板中，单击下拉箭头，然后选择寄送电子邮件警报所使用的语言。

8.3 设置防病毒和 HIPS SNMP 消息发送

如果您使用基于角色的管理，那么：

- 您必须具备 策略设置 - 防病毒和 HIPS 权限，才能执行此任务。
- 您不能编辑应用于您的活动子领域之外的策略。

要了解更多信息，请参阅 管理角色和子领域 （第 12 页）。

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 消息。

注释
这些设置仅应用于 Windows 计算机。

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 对话框中，单击 消息发送。
3. 在 消息发送 对话框中的 SNMP 消息发送 标签页中，选择 启用 SNMP 消息发送。
4. 在 要发送的消息 窗格板中，选择您想要 Sophos Endpoint Security and Control 针对它发送 SNMP 消息的事件类型。
5. 在 SNMP 陷阱目标 文本框中，输入收件人的 IP 地址。
6. 在 SNMP 团体名 文本框中，输入 SNMP 团体名。

8.4 配置防病毒和 HIPS 桌面消息发送

如果您使用基于角色的管理，那么：

- 您必须具备 策略设置 - 防病毒和 HIPS 权限，才能执行此任务。
- 您不能编辑应用于您的活动子领域之外的策略。

要了解更多信息，请参阅 管理角色和子领域 （第 12 页）。

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

1. 在 策略 窗格中，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。
   依照默认值，启用桌面消息发送 和 要发送的消息 窗格板中的所有选项都将被选择。如果需要，可以编辑这些设置。

   注释
   可疑行为检测，可疑文件检测，以及 广告软件和可能不想安装的应用程序检测 的设置仅应用于 Windows 计算机。

4. 在 用户自定义消息 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。

   注释
   用户定义的桌面消息不会显示在运行 Windows 8 及以后版本的计算机上。

8.5 设置应用程序控制警报和消息

如果您使用基于角色的管理，那么：

- 您必须具备 策略设置 - 应用程序控制 权限，才能配置应用程序控制策略。
- 您不能编辑应用于您的活动子领域之外的策略。

要了解更多信息，请参阅 管理角色和子领域 （第 12 页）。

当发现受控程序时，您可以向特定的用户发送消息。

1. 在 策略 窗格中，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 对话框的 消息发送 页中。
   消息发送 窗格板中的 启用桌面消息发送 复选框，依照默认值已被勾选。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。
3. 在 消息 文本框中，您可以输入一段消息文字，它会被添加到标准的桌面消息之后。

   注释
   用户定义的桌面消息不会显示在运行 Windows 8 及以后版本的计算机上。

4. 如果您想要发送有关检测到的受控程序的电子邮件警报，请选中 启用电子邮件警报发送 复选框。
5. 如果您想要发送 SNMP 消息，请选中 启用 SNMP 消息发送 复选框。

   注释
   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。要了解更多信息，请参见设置防病毒和 HIPS SNMP 消息发送 （第 156 页）。

8.6 设置数据控制警报和消息

如果您使用基于角色的管理，那么：

- 您必须具备 策略设置 - 数据控制 权限，才能配置数据控制策略。
- 您不能编辑应用于您的活动子领域之外的策略。

要了解更多信息，请参阅 管理角色和子领域 （第 12 页）。

Enterprise Console 使用事件和消息报告，检测到的或阻断的敏感数据传输。

要了解有关查看数据控制策略和事件的信息，请参见数据控制策略 （第 123 页）。

当数据控制启用时，依照默认值，以下事件和消息会记录在日志文件中，或者，会被显示：

- 数据控制事件会被记录在工作站计算机上的日志文件中。
- 数据控制事件会被发送到 Enterprise Console 中，可以通过 数据控制 - 事件查看器 查看它们。（要打开事件查看器，请在 事件 菜单中，单击 数据控制事件。）

  注释
  每个计算机每小时最多可以向 Enterprise Console 发送 50 个数据控制事件。

- 在最近七日之内，发生数据控制事件的数量超过了指定的级别的计算机，会显示在指标面板中。
- 桌面消息会显示在工作站计算机上。

您还可以配置 Enterprise Console 发送以下消息：

Email alerts	电子邮件消息会发送给您指定的收件人。
SNMP 消息	SNMP 消息会发送给您在“防病毒和 HIPS 策略”设置中指定的收件人。

要设置数据控制消息发送：

1. 请检查您想要配置的计算机组使用的是哪个数据控制策略。
   请参阅查看组采用的策略 （第 23 页）。
2. 在 策略 窗格板中，双击 数据控制。然后，双击您想要更改的策略。
   会出现 数据控制策略 对话框。
3. 在 数据控制策略 对话框中，转到 消息发送 标签页。桌面消息发送依照默认值是启用的，并且 在消息中包括匹配的规则 已被勾选。
4. 如果您愿意，请输入消息文字，它会被添加到标准的消息文字之后，供用户确认文件传输和阻断文件传输时使用。
   您输入的字符不能超过 100 个。您还可以为消息添加 HTML 链接，例如：About Sophos。

   注释
   用户定义的桌面消息不会显示在运行 Windows 8 及以后版本的计算机上。

5. 要启用电子邮件警报，请选中 启用电子邮件警报 复选框。在 电子邮件收件人 栏中，输入收件人的电子邮件地址。使用分号 (;) 分隔各个地址。
6. 要启用 SNMP 消息发送，请选中 启用 SNMP 消息发送 复选框。
   电子邮件服务器和 SNMP 陷阱的设置，是通过“防病毒和 HIPS 策略” 配置的。

8.7 设置设备控制警报和消息

如果您使用基于角色的管理，那么：

- 您必须具备 策略设置 - 设备控制 权限，才能编辑应用程序控制策略。

- 您不能编辑应用于您的活动子领域之外的策略。

要了解更多信息，请参阅 管理角色和子领域 （第 12 页）。

当检测到或已阻断受控设备时，Enterprise Console 通过事件和消息进行报告。

要了解有关查看设备控制事件的信息，请参见设备控制策略 （第 135 页）。

当设备控制启用时，依照默认值，以下事件和消息会记录在日志文件中，或者，会被显示：

- 设备控制事件会被记录在工作站计算机上的日志文件中。
- 设备控制事件会被发送到 Enterprise Console 中，可以通过 设备控制 - 事件查看器 查看它们。（要打开事件查看器，请在 事件 菜单中，单击 设备控制事件。）
- 在最近七日之内，发生设备控制事件的数量超过了指定的级别的计算机，会显示在指标面板中。
- 桌面消息会显示在工作站计算机上。

您还可以配置 Enterprise Console 发送以下消息：

Email alerts	电子邮件消息会发送给您指定的收件人。
SNMP 消息	SNMP 消息会发送给您在“防病毒和 HIPS 策略”设置中指定的收件人。

要设置设备控制消息发送：

1. 检查哪个设备控制策略被您想要配置的计算机组所采用了。
   请参阅查看组采用的策略 （第 23 页）。
2. 在 策略 窗格板中，双击 设备控制。然后，双击您想要更改的策略。
3. 在 设备控制策略 对话框的 消息发送 标签页中，依照默认值，桌面消息发送已启用。要进一步配置消息发送，请按照以下说明做：
   - 要为桌面消息发送输入消息文本，请在 消息文本 文本框中，输入将被添加到标准的消息文字之后的文字。

     您输入的字符不能超过 100 个。您还可以为消息添加 HTML 链接，例如：About Sophos。

     注释
     用户定义的桌面消息不会显示在运行 Windows 8 及以后版本的计算机上。

   - 要启用电子邮件警报，请选中 启用电子邮件警报 复选框。在 电子邮件收件人 栏中，输入收件人的电子邮件地址。使用分号 (;) 分隔各个地址。
   - 要启用 SNMP 消息发送，请选中 启用 SNMP 消息发送 复选框。

   电子邮件服务器和 SNMP 陷阱的设置，是通过“防病毒和 HIPS 策略” 配置的。

8.8 设置网络状态电子邮件警报

如果您使用基于角色的管理，那么，您必须具有 系统配置 权限，才能配置网络状态电子邮件警报。要了解更多信息，请参见管理角色和子领域 （第 12 页）。

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。

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

   b) 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。

   c) 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。

8.9 设置 Active Directory 同步化电子邮件警报

如果您使用基于角色的管理，那么，您必须具有 系统配置 权限，才能配置 Active Directory 同步化电子邮件警报。要了解更多信息，请参见管理角色和子领域 （第 12 页）。

您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。

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

   b) 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。

   c) 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：

   - 发现的新组
   - 发现的新计算机
   - 自动保护计算机失败

8.10 配置 Windows 事件日志记录

如果您使用基于角色的管理，那么：

- 您必须具备 策略设置 - 防病毒和 HIPS 权限，才能执行此任务。
- 您不能编辑应用于您的活动子领域之外的策略。

要了解更多信息，请参阅 管理角色和子领域 （第 12 页）。

依照默认值，当检测到或清除了病毒或间谍软件，检测到可疑行为，或检测到或清除了广告软件或可能不想安装的应用程序时，Sophos Endpoint Security and Control 会将警报添加到 Windows 的事件日志记录中。

要编辑这些设置：

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 对话框中，单击 消息发送。
3. 在 消息发送 对话框的 事件日志 标签页中。
   依照默认值，事件日志记录已启用。如果需要，可以编辑设置。
   扫描错误 中包括 Sophos Endpoint Security and Control 被拒绝访问试图扫描的项目的情况。

8.11 开启或关闭向 Sophos 发送反馈

如果您使用基于角色的管理，您必须具备系统配置权限，才能开启或关闭向 Sophos 发送反馈的功能。要了解更多信息，请参见管理角色和子领域 （第 12 页）。

Enterprise Console 将向Sophos定期发送报告。这些报告将帮助Sophos了解自家产品的使用情况，以改善我们的产品和服务。更多有关收集信息的类型和处理信息方式的详细信息，可参阅此处的 Sophos 最终用户授权使用许可协议（EULA）和 Sophos 隐私策略：http://www.sophos.com/legal。

一些报告的信息为可选，一些为强制要求，如最终用户许可协议和隐私策略中所述。可以通过更改反馈给 Sophos 设置，随时选择退出可选信息报表。

依照默认值，发送反馈给 Sophos 是启用的。在安装或更新控制台时，您有机会在 Sophos Enterprise Console 安装向导时，选择禁用该功能。

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

1. 在工具菜单中，单击反馈给 Sophos。
2. 在反馈给 Sophos 对话框中，您可以启用或禁用向 Sophos 发送反馈的功能。
   - 如果您想要启用向 Sophos 发送反馈功能，请阅读协议，如果您同意协议中的条款，选择我同意复选框。
   - 如果您想要禁用向 Sophos 发送反馈功能，请取消勾选我同意复选框。

9 查看事件

当某终结点计算机上出现应用程序控制，数据控制，设备控制，防火墙，补丁评估，介入防范，网页控制， 或漏洞防御事件时，例如，某应用程序已被防火墙阻断，该事件会被发送到 Enterprise Console，并且可以在相应的事件查看器中查看。

通过事件查看器，您可以调查发生在网络中的事件。您还可以基于您配置的过滤器生成事件列表，例如，某用户在过去7天中发生的所有数据控制事件的列表。

在最近七日之内，发生事件（除介入防范事件之外）的数量超过了指定的级别的计算机，会显示在指标面板中。要了解怎样设置级别的信息，请参见配置指标面板 （第 41 页）。

您还可以设置当发生事件时，向您选择的收件人发送警报。要了解更多信息，请参见管理角色和子领域 （第 12 页）。

9.1 查看应用程序控制事件

要查看应用程序控制事件：

1. 在 事件 菜单中，单击 应用程序控制事件。
   会出现 应用程序控制 - 事件查看器 对话框。
2. 在 搜索时间跨度 栏中，单击下拉箭头，并选择您想要显示的事件所在的时间跨度。
   您可以选择固定的时间跨度，如：24 小时内，或者，选择 自定义，通过选择开始日期和时间，以及结束日期和时间，来指定您自定义的时间跨度。
3. 如果您想查看某个用户或计算机的事件，请在相应的栏中输入名称。
   如果您保留这些栏为空，那么，将显示所有用户和计算机的事件。
   您在这些栏中使用通配符。使用 ？ 替代单个字符，以及使用 * 替代字符串。
4. 如果您想查看某个应用程序类型的事件，请单击 应用程序类型 栏上的下拉菜单，并选择应用程序类型。
   依照默认值，事件查看器会显示所有应用程序类型的事件。
5. 单击 搜索 可显示事件列表。

您可以将应用程序控制事件列表导出到文件中。有关详细信息，请参见导出事件列表到文件中 （第 169 页）。

9.2 查看数据控制事件

注释
如果您的用户授权使用许可协议中不包括数据控制功能，此功能将不可用。

如果您使用基于角色的管理，那么，您必须具备数据控制事件权限，才能查看 Enterprise Console 中的数据控制事件。要了解更多有关基于角色的管理的信息，请参见管理角色和子领域 （第 12 页）。

要查看数据控制事件：

1. 在 事件 菜单中，单击 数据控制事件。
   会出现 数据控制 - 事件查看器 对话框。
2. 在 搜索时间跨度 栏中，单击下拉箭头，并选择您想要显示的事件所在的时间跨度。

您可以选择固定的时间跨度，如：24 小时内，或者，选择 自定义，通过选择开始日期和时间，以及结束日期和时间，来指定您自定义的时间跨度。

3. 如果您想查看某个用户，计算机，或者，文件，请在相应的栏中输入名称。
   如果您保留这些栏为空，那么，将显示所有用户，计算机，和文件的事件。
   您在这些栏中使用通配符。使用 ？ 替代单个字符，以及使用 * 替代字符串。
4. 如果您想要查看针对某个规则的事件，请在 规则名称 栏，单击下拉箭头，并选择规则名称。
   依照默认值，事件查看器会显示针对所有规则的事件。
5. 如果您想查看某个文件类型的事件，请在 文件类型 栏中，单击下拉箭头，并选择文件类型。
   依照默认值，事件查看器会显示所有文件类型的事件。
6. 单击 搜索 可显示事件列表。

您可以将数据控制事件列表导出到文件中。有关详细信息，请参见导出事件列表到文件中 （第 169 页）。

9.3 查看设备控制事件

要查看设备控制事件：

1. 在 事件 菜单中，单击 设备控制事件。
   会出现 设备控制 - 事件查看器 对话框。
2. 在 搜索时间跨度 栏中，单击下拉箭头，并选择您想要显示的事件所在的时间跨度。
   您可以选择固定的时间跨度，如：24 小时内，或者，选择 自定义，通过选择开始日期和时间，以及结束日期和时间，来指定您自定义的时间跨度。
3. 如果您想查看某个设备类型的事件，请在 设备类型 栏中，单击下拉箭头，并选择设备类型。
   依照默认值，事件查看器会显示所有设备类型的事件。

   注释
   如果您将可选的磁盘驱动器设置为“只读”，这些设备的事件将不会显示在事件查看器中。

4. 如果您想查看某个用户或计算机的事件，请在相应的栏中输入名称。
   如果您保留这些栏为空，那么，将显示所有用户和计算机的事件。
   您在这些栏中使用通配符。使用 ？ 替代单个字符，以及使用 * 替代字符串。
5. 单击 搜索 可显示事件列表。

在 设备控制 - 事件查看器 对话框中，您可以从设备控制策略中免除设备。有关详细信息，请参见从所有策略中免除设备 （第 138 页）。

您可以将设备控制事件列表导出到文件中。有关详细信息，请参见导出事件列表到文件中 （第 169 页）。

9.4 查看防火墙事件

防火墙事件从终结点计算机到控制台只发送一次。来自不同的终结点计算机的相同的事件，在 防火墙 - 事件查看器 中会被放置在一起。在 计数 栏中，您可以看到某个事件被从不同的终结点计算机发送出来的总次数。

要查看防火墙事件：

1. 在 事件 菜单中，单击 防火墙事件。
   会出现 防火墙 - 事件查看器 对话框。

2. 在 搜索时间跨度 栏中，单击下拉箭头，并选择您想要显示的事件所在的时间跨度。
   您可以选择固定的时间跨度，如：24 小时内，或者，选择 自定义，通过选择开始日期和时间，以及结束日期和时间，来指定您自定义的时间跨度。
3. 如果您想查看某个类型的事件，请在 事件类型 栏中，单击下拉箭头，并选择事件类型。
   依照默认值，事件类型查看器会显示所有类型的事件。
4. 如果您想查看某个文件的事件，请在 文件名 栏中，输入文件名称。
   如果您保留此栏为空，所有文件的事件都会显示。
   您可以在此栏中使用通配符。使用 ？ 替代单个字符，以及使用 * 替代字符串。
5. 单击 搜索 可显示事件列表。

在防火墙 - 事件浏览器对话框中，您可以按照创建防火墙事件规则 （第 99 页）中的说明创建防火墙规则。

您可以将防火墙事件列表导出到文件中。有关详细信息，请参见导出事件列表到文件中 （第 169 页）。

9.5 查看介入防范事件

介入防范事件有两种类型：

- 顺利的介入防范验证事件，显示已验证的用户的名称，以及验证的时间。
- 不成功的介入尝试事件，显示涉及的 Sophos 软件产品或组件的名称，介入尝试的时间，以及进行介入尝试的用户的详情。

要查看介入防范事件：

1. 在 事件 菜单中，单击 介入防范事件。
   会出现 介入防范 - 事件查看器 对话框。
2. 在 搜索时间跨度 栏中，单击下拉箭头，并选择您想要显示的事件所在的时间跨度。
   您可以选择固定的时间跨度，如：24 小时内，或者，选择 自定义，通过选择开始日期和时间，以及结束日期和时间，来指定您自定义的时间跨度。
3. 如果您想要查看某个类型的事件，请在 事件类型 栏中，单击下拉箭头，并选择事件类型。
   依照默认值，事件查看器会显示所有类型的事件。
4. 如果您想查看某个用户或计算机的事件，请在相应的栏中输入名称。
   如果您保留这些栏为空，那么，将显示所有用户和计算机的事件。
   您在这些栏中使用通配符。使用 ？ 替代单个字符，以及使用 * 替代字符串。
5. 单击 搜索 可显示事件列表。

您可以将此列表导出到文件中。有关详细信息，请参见导出事件列表到文件中 （第 169 页）。

9.6 补丁评估事件

注释
如果您的用户授权使用许可协议中没有包括补丁评估功能，则该功能不可用。

补丁评估 - 事件查看器 中提供安全补丁和补丁评估结果的信息。

补丁更新 栏会显示补丁下载状态的信息。它会显示以下状态消息之一：

- 没有下载 表明补丁信息没有被下载，或者，您没有使用该补丁功能的用户授权使用许可协议。
- 正在下载 表明在安装之后进行的首次下载正在进行中。

- 确定 表明补丁信息已及时更新。
- 未及时更新 表明过去的 72 小时中没有顺利进行任何补丁数据的更新。通常，如果在 SEC 由于网络连接的原因，而没有及时更新时，就会显示此状态信息。如果您从含有该补丁功能的 SEC 的用户授权使用许可协议更换成了不含有该补丁的，那么，也会显示此状态信息。在只进行了部分更新的情况下，也可能出现此消息。

补丁评估 - 事件查看器 带有以下标签页：

按评级分类的补丁

此标签页将按照默认值，显示漏掉的补丁。每个补丁都会被显示，以及漏掉该补丁的计算机的总数，并且会显示与该补丁相关的安全隐患和安全漏洞的链接。您可以使用筛选功能，显示所有被支持的补丁的完整列表，并且显示漏掉这些补丁的相应的计算机的总数。

漏掉补丁的计算机

此标签页将按照计算机分类，显示补丁评估的状态。会出现每台计算机，并且会显示它遗漏的补丁。如果漏掉多个补丁，那么，计算机会多次被列示。

9.6.1 查看补丁评估事件

要查看补丁评估事件：

1. 在 事件 菜单中，单击 补丁评估事件。
   会出现 补丁评估 - 事件查看器 对话框。
2. 单击标签页 按照评级分类的补丁 或 遗漏补丁的计算机。要了解更多有关标签页的信息，请参见补丁评估事件 （第 164 页）。
3. 在“搜索”面板中，如果您想要根据名称，计算机，安全隐患，或安全漏洞针，对特定的补丁查看事件，请在相应的文本栏中输入信息。可用的标准则是基于标签页中显示的信息。
   如果您保留这些栏为空，那么，将显示所有基于补丁名称，补丁 ID，以及计算机名称的事件。
   您在这些栏中使用通配符。使用 ？ 替代单个字符，以及使用 * 替代字符串。
4. 如果您想要根据状态，评级，软件商，组，或发布时间，针对特定的补丁查看事件，请单击相应的栏目中的下拉箭头，并选择相应的选项。可用的标准则是基于标签页中显示的信息。
   依照默认值，事件查看器将显示安全隐患评级，软件商，组，安全隐患，以及漏掉的补丁的名称等事件。
5. 单击 搜索 可显示补丁评估事件列表。
   要了解更多有关显示的结果的信息，请参见搜索结果类别 （第 166 页）。

您可以右击单个的链接以复制它的名称，或者，可以使用 Ctrl+C 键，复制补丁评估事件行到“剪贴板”中。

您可以将补丁评估事件列表导出。有关详细信息，请参见导出事件列表到文件中 （第 169 页）。

单击所提供的链接，您可以查看指定的补丁的详情。要了解更多信息，请参见查看补丁，安全隐患，或者安全漏洞详情 （第 165 页）。

9.6.2 查看补丁，安全隐患，或者安全漏洞详情

要查看补丁，安全隐患，或者安全漏洞详情：

1. 在 事件 菜单中，单击 补丁评估事件。
   会出现 补丁评估 - 事件查看器 对话框。

2. 单击标签页 按照评级分类的补丁 或 遗漏补丁的计算机，勾选所要求的选项，然后，单击 搜索 以显示事件的列表。
   要了解更多有关显示的结果的信息，请参见搜索结果类别 （第 166 页）。
3. 单击您想要查看更多的详情的补丁的名称。
4. 在 补丁详情 对话框中，您可以查看补丁说明，以及有关它所针对的安全隐患和漏洞的信息。如果可能，您可以：
   - 单击补丁名称，开启网页浏览器，查看软件商提供的补丁信息。
   - 单击安全隐患，开启网页浏览器，查看 Sophos 安全隐患分析和建议。
   - 单击安全漏洞，开启网页浏览器，查看常见安全漏洞和潜在风险 (CVE) 的信息。
   - 单击 出处 栏中的补丁名称，可以打开网页浏览器，查看替代补丁的软件商的信息。

该列表按字母排序，然后，按安全漏洞排序。

9.6.3 搜索结果类别

搜索结果显示在基于标签页的不同的类别中：

- 按评级分类的补丁 （第 166 页）
- 漏掉补丁的计算机 （第 167 页）

按评级分类的补丁

搜索结果将根据以下类别显示：

- 安全隐患：安全隐患可能是病毒，特洛伊木马，蠕虫，间谍软件，恶意网站，以及广告和其它可能不想安装的应用程序。您可以单击安全隐患名称，在网页浏览器中查看 Sophos 安全隐患分析和建议。
- 安全漏洞：安全漏洞是可能被黑客利用的软件弱点。利用安全漏洞所能造成的损害，取决于安全漏洞的严重程度，以及受影响的软件本身。补丁用于修复安全漏洞，使其不能再被利用。您可以单击安全隐患名称，在网页浏览器中查看常见的安全漏洞和风险 (CVE)。
- 评级：补丁的评级，由 SophosLabs 提供。

  注释
  我们建议无论评级的高低，应用全部补丁。

  — 紧要：表明与此补丁相关的安全漏洞肯定会被利用。
  — 高：表明与此补丁相关的安全漏洞极有可能会被利用。
  — 中：表明与此补丁相关的安全漏洞可能会被利用。
  — 低：表明与此补丁相关的安全漏洞不大可能会被利用。
- 补丁名称：显示补丁的名称。您可以单击补丁名称，开启网页浏览器，查看软件商提供的补丁信息。
- 软件商：显示发布补丁的软件商的名称。
- 计算机：显示受影响的计算机的数量。如果一台或多台计算机受到了影响，您可以单击数字，在 遗漏补丁的计算机 标签页中，查看详情。如果出现 "-"，说明补丁没有被评估。
- 替换为：显示用来替换的补丁的名称。您可以单击补丁名称开启 补丁详情 对话框查看有关替代的补丁的信息。
- 发布日期：显示补丁发布的日期。

漏掉补丁的计算机

搜索结果将根据以下类别显示：

- 计算机：显示受影响的计算机的名称。
- 评级：补丁的评级，由 SophosLabs 提供。

  注释
  我们建议无论评级的高低，应用全部补丁。

  — 紧要：表明与此补丁相关的安全漏洞肯定会被利用。
  — 高：表明与此补丁相关的安全漏洞极有可能会被利用。
  — 中：表明与此补丁相关的安全漏洞可能会被利用。
  — 低：表明与此补丁相关的安全漏洞不大可能会被利用。
- 补丁名称：显示补丁的名称。您可以单击补丁名称，开启网页浏览器，查看软件商提供的补丁信息。
- 替换为：显示用来替换的补丁的名称。您可以单击补丁名称开启 补丁详情 对话框查看有关替代的补丁的信息。
- 前次评估：显示计算机前次评估漏掉的补丁的日期。
- 软件商：显示发布补丁的软件商的名称。
- 发布日期：显示补丁发布的日期。
- 组：显示计算机所在的组的名称。

9.7 查看网页事件

注释
如果您的用户使用权限许可协议中不包括网页控制，则此功能将不可用。

如果您使用基于角色的管理，那么，您必须具备网页事件权限，才能查看 Enterprise Console 中的网页事件。要了解更多有关基于角色的管理的信息，请参见管理角色和子领域 （第 12 页）。

您可以在“网页事件查看器”中查看以下网页事件：

- 防病毒和 HIPS 策略中的“网页保护”功能阻断的恶意网站。
- 网页控制事件，如果您使用了“网页控制”功能。

网页事件的显示会因所选择的网页控制策略的不同而不同。尽管“网页事件查看器”在两种策略模式中都可以使用，但显示的内容是不同的。

当选择了 不合适的网站控制 策略选项，您可以查看任何 “阻断” 和 “警告” 措施。访问了被归类为“警告”的 HTTPS 站点时，日志记录中会记为“继续”事件，因为，Sophos Endpoint Security and Control 对于 HTTPS 的回应不同（请参见不合适的网站控制 （第 145 页）中的说明）。

选择完全网页控制后，事件会显示在设备中。

- 对于 Sophos Web Appliance 或 Management Appliance，您可以使用报告和搜索功能查看浏览活动。“阻断，”“警告，”以及“允许”等措施会全部被显示。访问了被归类为“警告”的 HTTPS 站点时，日志记录中会显示为“继续”事件，因为，Sophos Endpoint Security and Control 对于 HTTPS 的回应不同（请参见完全网页控制 （第 149 页）中的说明）。

- 对于 UTM，使用日志记录和报告 > 网页保护 > 网页使用情况报告页面。在那里，您可以看到很多操作，显示：网站是否已经交付到客户端（通过），是否已经被应用程序控制规则阻止，或者用户是否使用略过阻止功能（重写）获得阻止页面的访问权限以及其他信息。

注释
无论您选择哪种策略，由 Sophos Endpoint Security and Control 的实时 URL 过滤机制（Web 保护 （第 85 页））扫描和评估的网站都会在 Enterprise Console 中显示为网页事件。

要查看网页事件：

1. 在 事件 菜单中，单击 网页事件。
   会出现 网页 - 事件查看器 对话框。
2. 在 搜索时间跨度 文本框中，单击下拉箭头，并选择您想要显示的事件所在的时间跨度。
   您可以选择固定的时间跨度，如：24 小时内，或者，选择 自定义，通过选择开始日期和时间，以及结束日期和时间，来指定您自定义的时间跨度。
3. 如果您想查看某个特定的用户或计算机的事件，请在相应的栏中输入名称。
   如果您保留这些栏为空，那么，将显示所有用户和计算机的事件。
   您在这些栏中使用通配符。使用 ？ 替代单个字符，以及使用 * 替代字符串。
4. 如果您想查看与某个措施相关的事件，请在 措施类型 栏中，单击下拉箭头，并选择措施类型。
5. 如果您想查看的事件与某个特定的域相关，请在 域 栏中输入域名。
6. 如果您想要查看由于某个特定的 原因 而引发的事件，请单击下拉箭头，并选择原因。
7. 单击 搜索 可显示事件列表。

您可以将网页事件列表导出到文件中。有关详细信息，请参见导出事件列表到文件中 （第 169 页）。

9.7.1 查看计算机上最新的网页事件

您可以查看针对终结点计算机的最近的10个采取了某种措施的事件，例如，最近阻断的网站。

要查看最新的网页事件：

1. 在 终结点 视图的计算机列表中，双击您想要查看活动的计算机。
2. 在 计算机详情 对话框中，下拉滚动条到 最近的网页事件 部分。

您还可以通过生成报告查看某个用户的事件的数量。要了解更多信息，请参阅 配置每个用户的事件的报告 （第 175 页）。

9.8 查看漏洞防御事件

注释
如果您的用户使用权限许可协议中不包括漏洞防御，则此功能将不可用。

如果您使用基于角色的管理，那么，您必须具备漏洞防御权限，才能查看 Enterprise Console 中的漏洞防御。要了解更多有关基于角色的管理的信息，请参见管理角色和子领域 （第 12 页）。

查看漏洞防御事件：

1. 在 事件 菜单中，单击 漏洞防御。
   会出现 漏洞防御 - 事件查看器 对话框。
2. 在 搜索时间跨度 文本框中，单击下拉箭头，并选择您想要显示的事件所在的时间跨度。

您可以选择固定的时间跨度，如：24 小时内，或者，选择 自定义，通过选择开始日期和时间，以及结束日期和时间，来指定您自定义的时间跨度。

3. 如果您想查看某个特定的用户或计算机的事件，请在相应的栏中输入名称。
   如果您保留这些栏为空，那么，将显示所有用户和计算机的事件。
   您在这些栏中使用通配符。使用 ？ 替代单个字符，以及使用 * 替代字符串。
4. 如果您想查看与某个措施相关的事件，请在 类型 栏中，单击下拉箭头，并选择类型。
5. 单击 搜索 可显示事件列表。

- 您可以将漏洞防御事件列表导出到文件中。有关详细信息，请参见导出事件列表到文件中 （第 169 页）。
- 您可以在漏洞防御中排除漏洞防御事件。请参阅在漏洞防御中排除事件 （第 169 页）。

9.9 导出事件列表到文件中

您可以将应用程序控制，数据控制，设备控制，防火墙，补丁评估，介入防范，网页事件，或漏洞防御事件列表导出到逗号分隔值 (CSV) 文件中。您还可以将补丁评估事件列表导出到 PDF 文件中。

1. 在 事件 菜单中，根据您想要导出的某种事件列表，单击该种“事件”选项。
   事件查看器 对话框会出现。
2. 如果您只想查看特定的事件，请在 搜索标准 窗格板中，设置合适的筛选项，然后，单击 搜索 按钮，以显示事件。
   要了解更多信息，请参见：
   - 查看应用程序控制事件 （第 162 页）
   - 关于数据控制事件 （第 127 页）
   - 关于设备控制事件 （第 135 页）
   - 查看防火墙事件 （第 163 页）
   - 补丁评估事件 （第 164 页）
   - 查看介入防范事件 （第 164 页）
   - 查看网页事件 （第 167 页）
   - 查看漏洞防御事件 （第 168 页）
3. 单击 导出。
4. 在 另存为 窗口中，浏览并选择保存文件的路径，在 文件名 对话框中输入文件名称，并在 另存为类型 对话框中选择文件类型。
5. 单击 保存。

9.10 在漏洞防御中排除事件

您可以在事件查看器中选择特定的事件，从漏洞防御中排除应用程序和漏洞防御事件。

1. 在 事件 菜单中，单击 漏洞防御事件。
   事件查看器 对话框会出现。
2. 如果您只想查看特定的事件，请在 搜索标准 窗格板中，设置合适的筛选项，然后，单击 搜索 按钮，以显示事件。
   要了解更多信息，请参见 查看漏洞防御事件 （第 168 页）。
3. 单击事件，然后单击排除。
   会出现 漏洞预防排除 对话框。

4. 单击要修改的策略。要修改所有策略的设置，请单击全选。
5. 在攻击事件或应用程序部分下面，单击排除
6. 单击确定。

漏洞防御事件或应用程序将从选定策略的漏洞防御中排除。

10 生成报告

报告可以提供有关您的网络安全状态的各个方面的文字和图形的信息。

报告是通过 报告管理器 提供的。使用 报告管理器，您可以基于现成的模板迅速创建报告，更改现有的报告的配置，以及计划安排报告按照固定的频率运行，并将报告以电子邮件附件的方式发送给您选择的收件人。您还可以打印报告，以及用多种格式导出报告。

Sophos 提供了一系列您可以现成使用的，或者，可以按照您的需要修改它们配置的各种报告。这些报告的种类有：

- 警报和事件历史
- 警报摘要
- 按照项目名称给出警报和事件
- 按照时间给出警报和事件
- 按照路径给出警报和事件
- 终结点策略非遵照
- 按用户排序的事件
- 受管理的终结点保护
- 更新层级

报告和基于角色的管理

如果您使用基于角色的管理，您必须具有 报告配置 权限，才能创建，编辑，或删除报告。如果您没有这样的权限，那么，您只能运行报告。要了解更多有关基于角色的管理的信息，请参见管理角色和子领域 （第 12 页）。

报告只能包含来自活动自领域中的数据。您不能在子领域之间共享报告。默认的报告不能从默认的子领域复制到您创建的新的子领域。

当您删除某个子领域时，该子领域中所有报告都会被删除。

10.1 创建新报告

如果您使用基于角色的管理，那么，您必须具有 报告配置 权限，才能执行此任务。要了解更多信息，请参见管理角色和子领域 （第 12 页）。

要创建报告：

1. 单击工具栏中的 报告 图标。
2. 在 报告管理器 对话框中，单击 创建。
3. 在 创建新报告 对话框中，选择某个报告模板，并单击 确定。

   会一个向导根据您选择的模板，指导您完成创建报告。

   如果您不想使用向导，请在 创建新报告 对话框中，取消勾选 使用向导创建报告 勾选框。然后，您可以在报告属性对话框中配置您的新建报告。要了解更多的信息，请参见有关配置相关报告的主题。

10.2 配置警报和事件历史报告

如果您使用基于角色的管理，那么，您必须具有 报告配置 权限，才能执行此任务。要了解更多信息，请参见管理角色和子领域 （第 12 页）。

警报和事件历史 报告显示每个特定的报告期间的警报和事件。

1. 单击工具栏中的 报告 图标。
2. 在 报告管理器 对话框中，选择 警报和事件历史，并单击 属性。
3. 在 警报和事件历史属性 对话框的 配置 标签页，设置您想要的选项。
   a) 在 报告详情 窗格板中，如果您愿意，可以编辑报告的名称和描述。
   b) 在 报告发送期间 窗格板的 时间跨度 文本框中，单击下拉箭头，并选择时间期间。
      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。
   c) 在 报告路径 窗格板中，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。
   d) 在 要包括的警报和事件类型 窗格板中，选择您想要包括在报告中的警报和事件类型。
      依照默认值，报告会显示所有警报和事件类型。
      或者，您可以配置报告，仅显示报告了特定的警报或事件的路径。要指定单个的警报或事件，请单击 高级，并单击列表中的警报或事件名称。要指定多个警报或事件，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。
4. 在 显示选项 标签页中，选择您想怎样排序警报和事件。
   依照默认值，警报和事件详情是按照 警报和事件名称 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。
5. 在 计划 标签中，如果您想要定期运行报告，并将报告结果以电子邮件附件的形式发送给您选择的收件人，请选择 计划此报告。输入起始日期和时间，以及生成报告的频率，指定输出文件的格式和语言，并输入报告收件人的电子邮件地址。

10.3 配置警报摘要报告

如果您使用基于角色的管理，那么，您必须具有 报告配置 权限，才能执行此任务。要了解更多信息，请参见管理角色和子领域 （第 12 页）。

警报摘要报告提供有关您的网络的状态和总体健康状况的统计数据。

1. 单击工具栏中的 报告 图标。
2. 在 报告管理器 对话框中，选择 警报摘要，并单击 属性。
3. 在 警报摘要属性 对话框的 配置 标签页中，设置您想要的选项。
   a) 在 报告详情 窗格板中，如果您愿意，可以编辑报告的名称和描述。
   b) 在 报告发送期间 窗格板的 时间跨度 文本框中，单击下拉箭头，并选择时间期间。
      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。
4. 在 显示选项 标签页中的 显示结果按照 下，指定测试非遵照的时间段， 如：每小时或每天，单击下拉箭头，并选择时间段。

5. 在 计划 标签中，如果您想要定期运行报告，并将报告结果以电子邮件附件的形式发送给您选择的收件人，请选择 计划此报告。输入起始日期和时间，以及生成报告的频率，指定输出文件的格式和语言，并输入报告收件人的电子邮件地址。

10.4 配置按照项目名称给出警报和事件的报告

如果您使用基于角色的管理，那么，您必须具有 报告配置 权限，才能执行此任务。要了解更多信息，请参见管理角色和子领域 （第 12 页）。

按照项目名称给出警报和事件 的报告，提供在所选择的报告期间，所有计算机上的所有警报和事件的统计摘要，以项目名称归类。

要配置报告：

1. 单击工具栏中的 报告 图标。
2. 在 报告管理器 对话框中，选择 按照项目名称给出警报和事件，并单击 属性。
3. 在 按照项目名称给出警报和事件属性 对话框的 配置 标签页中，设置您想要的选项。
   a) 在 报告详情 窗格板中，如果您愿意，可以编辑报告的名称和描述。
   b) 在 报告发送期间 窗格板的 时间跨度 文本框中，单击下拉箭头，并选择时间期间。
      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。
   c) 在 报告路径 窗格板中，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。
   d) 在 要包括的警报和事件类型 窗格板中，选择您想要包括在报告中的警报和事件类型。
      依照默认值，报告会显示所有警报和事件类型。
4. 在 显示选项 标签页的 显示 下，选择您想要在报告中显示的警报和事件。
   依照默认值，报告会显示所有的警报和事件，以及每个计算机合组中出现警报的次数。
   您还可以配置报告仅显示：
   - 前 n 个警报和事件（这里的 n 是您指定的数值），或者
   - 发生率不低于 m 的警报和事件（这里的 m 是您指定的数值）。
5. 在 排序依据 下，选择您想按照项目数还是警报和事件名称排序。
   依照默认值，报告列示的警报和事件，是按照警报数发生数，降序排列的。
6. 在 计划 标签中，如果您想要定期运行报告，并将报告结果以电子邮件附件的形式发送给您选择的收件人，请选择 计划此报告。输入起始日期和时间，以及生成报告的频率，指定输出文件的格式和语言，并输入报告收件人的电子邮件地址。

10.5 配置按照时间给出警报和事件的报告

如果您使用基于角色的管理，那么，您必须具有 报告配置 权限，才能执行此任务。要了解更多信息，请参见管理角色和子领域 （第 12 页）。

按照时间给出警报和事件 的报告显示在特定的时间段出现的警报和事件的摘要。

1. 单击工具栏中的 报告 图标。
2. 在 报告管理器 对话框中，选择 按照时间给出警报和事件，并单击 属性。
3. 在 按照时间给出警报和事件属性 对话框的 配置 标签中，设置您想要的选项。
   a) 在 报告详情 窗格板中，如果您愿意，可以编辑报告的名称和描述。
   b) 在 报告发送期间 窗格板的 时间跨度 文本框中，单击下拉箭头，并选择时间期间。

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。

c) 在 报告路径 窗格板中，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。

d) 在 要包括的警报和事件类型 窗格板中，选择您想要包括在报告中的警报和事件类型。

依照默认值，报告会显示所有警报和事件类型。

或者，您可以配置报告，仅显示报告了特定的警报或事件的路径。要指定单个的警报或事件，请单击 高级，并单击列表中的警报或事件名称。要指定多个警报或事件，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。

4. 在 显示选项 标签页中，指定测试警报和事件率的时间段，如：每小时或每天，单击下拉箭头，并选择时间段。
5. 在 计划 标签中，如果您想要定期运行报告，并将报告结果以电子邮件附件的形式发送给您选择的收件人，请选择 计划此报告。输入起始日期和时间，以及生成报告的频率，指定输出文件的格式和语言，并输入报告收件人的电子邮件地址。

10.6 配置按照路径排序的警报和事件的报告

如果您使用基于角色的管理，那么，您必须具有 报告配置 权限，才能执行此任务。要了解更多信息，请参见管理角色和子领域 （第 12 页）。

按照路径给出警报和事件的报告，提供在所选择的报告期间，所有计算机上的所有警报的统计摘要，以路径归类。

1. 单击工具栏中的 报告 图标。
2. 在 报告管理器 对话框中，选择 按照路径给出警报和事件，并单击 属性。
3. 在 按照路径给出警报和事件属性 对话框的 配置 标签中，设置您想要的选项。

a) 在 报告详情 窗格板中，如果您愿意，可以编辑报告的名称和描述。

b) 在 报告发送期间 窗格板的 时间跨度 文本框中，单击下拉箭头，并选择时间期间。

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。

c) 在 报告路径 窗格板中，单击 计算机 以显示每个计算机上的警报，或单击 组 以显示计算机上的各个组的警报。

d) 在 要包括的警报和事件类型 窗格板中，选择您想要包括在报告中的警报和事件类型。

依照默认值，报告会显示所有警报和事件类型。

或者，您可以配置报告，仅显示报告了特定的警报或事件的路径。要指定单个的警报或事件，请单击 高级，并单击列表中的警报或事件名称。要指定多个警报或事件，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。

4. 在 显示选项 标签页的 显示 下，选择您想要在报告中显示的警报。

依照默认值，报告会显示所有的计算机和组，以及每个计算机合组中出现警报的次数。您可以配置报告，仅显示：

- 前 n 个记录了最多次警报和事件的路径（这里的 n 是您指定的数值），或者
- 不少于 m 个警报和事件以上的路径（这里的 m 是您指定的数值）。

5. 在 排序依据 下，选择您想按照检测到的项目数还是警报名称排序。

依照默认值，报告列示的路径，是按照每一路径记录的警报和事件数，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。

6. 在 计划 标签中，如果您想要定期运行报告，并将报告结果以电子邮件附件的形式发送给您选择的收件人，请选择 计划此报告。输入起始日期和时间，以及生成报告的频率，指定输出文件的格式和语言，并输入报告收件人的电子邮件地址。

10.7 配置端点计算机策略非遵照报告

如果您使用基于角色的管理，那么，您必须具有 报告配置 权限，才能执行此任务。要了解更多信息，请参见管理角色和子领域 （第 12 页）。

终结点计算机策略非遵照 报告，显示在指定的时间段中，没有遵照所在的组的策略的计算机的百分比或数量。

1. 单击工具栏中的 报告 图标。
2. 在 报告管理器 对话框中，选择 终结点计算机策略非遵照，并单击 属性。
3. 在 终结点计算机策略非遵照属性 对话框的 配置 标签页中，设置您想要的选项。
   a) 在 报告详情 窗格板中，如果您愿意，可以编辑报告的名称和描述。
   b) 在 报告发送期间 窗格板的 时间跨度 文本框中，单击下拉箭头，并选择时间期间。
      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。
   c) 在 显示 窗格板中，选择您想要在报告中显示的策略。依照默认值，只有 防病毒和 HIPS 策略被选择。
4. 在 显示选项 标签页中的 显示结果按照 下，指定测试非遵照的时间段， 如：每小时或每天，单击下拉箭头，并选择时间段。
5. 在 显示结果为 下，选择您想要以百分比还是数字显示结果。
6. 在 计划 标签中，如果您想要定期运行报告，并将报告结果以电子邮件附件的形式发送给您选择的收件人，请选择 计划此报告。输入起始日期和时间，以及生成报告的频率，指定输出文件的格式和语言，并输入报告收件人的电子邮件地址。

10.8 配置每个用户的事件的报告

如果您使用基于角色的管理，那么，您必须具有 报告配置 权限，才能执行此任务。要了解更多信息，请参见管理角色和子领域 （第 12 页）。

每个用户的事件 的报告，显示应用程序控制，防火墙，数据控制，设备控制等事件，以及网页事件，并按照用户归类。

1. 单击工具栏中的 报告 图标。
2. 在 报告管理器 对话框中，选择 每个用户的事件，并单击 属性。
3. 在 每个用户的事件属性 对话框的 配置 标签页中，设置您想要的选项。
   a) 在 报告详情 窗格板中，如果您愿意，可以编辑报告的名称和描述。
   b) 在 报告发送期间 窗格板的 时间跨度 文本框中，单击下拉箭头，并选择时间期间。
      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。
   c) 在 要包括的事件类型 下，选择您想要显示事件的功能。
4. 在 显示选项 标签页的 显示 下，选择您想要在报告中显示的用户。

   依照默认值，报告会显示所有用户，以及每个用户的事件数量。您可以配置报告，仅显示：

   - 前 n 个记录了最多次事件的用户（这里的 n 是您指定的数值），或者
   - 不少于 m 个事件以上的用户（这里的 m 是您指定的数值）。

5. 在 排序依据 下，选择您想要按照发生的事件数还是名称排序用户。
   依照默认值，报告列示的用户，是按照每个用户发生的事件数，从高到低排列的。如果您想要它们以字母为序，按用户名称排列，请选择 用户。
6. 在 计划 标签中，如果您想要定期运行报告，并将报告结果以电子邮件附件的形式发送给您选择的收件人，请选择 计划此报告。输入起始日期和时间，以及生成报告的频率，指定输出文件的格式和语言，并输入报告收件人的电子邮件地址。

10.9 配置受管理的终结点保护的报告

如果您使用基于角色的管理，那么，您必须具有 报告配置 权限，才能执行此任务。要了解更多信息，请参见管理角色和子领域 （第 12 页）。

受管理的终结点保护 的报告，显示在指定的时间段中，受到保护的计算机的百分比或数量。

1. 单击工具栏中的 报告 图标。
2. 在 报告管理器 对话框中，选择 受管理的终结点保护，并单击 属性。
3. 在 受管理的终结点保护属性 对话框的 配置 标签页中，设置您想要的选项。
   a) 在 报告识别 窗格板中，如果您愿意，可以编辑报告的名称和描述。
   b) 在 报告发送期间 窗格板的 时间跨度 文本框中，单击下拉箭头，并选择时间期间。
      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。
   c) 在 显示 窗格板中，选择您想要在报告中显示的功能。
4. 在 显示选项 标签页中的 显示结果按照 下，指定测试非遵照的时间段， 如：每小时或每天，单击下拉箭头，并选择时间段。
5. 在 显示结果为 下，选择您想要以百分比还是数字显示结果。
6. 在 计划 标签中，如果您想要定期运行报告，并将报告结果以电子邮件附件的形式发送给您选择的收件人，请选择 计划此报告。输入起始日期和时间，以及生成报告的频率，指定输出文件的格式和语言，并输入报告收件人的电子邮件地址。

10.10 更新层级报告

更新层级 报告显示您的网络中的更新管理器，它们维护的更新共享，以及从这些共享进行更新的计算机。

您不能配置 更新层级 报告。您可以按照 运行报告 （第 177 页） 中的说明运行报告。

10.11 计划报告

如果您使用基于角色的管理，那么，您必须具有 报告配置 权限，才能执行此任务。要了解更多信息，请参见管理角色和子领域 （第 12 页）。

您可以计划安排定期运行报告，并将报告结果以电子邮件附件的形式发送给您选择的收件人。

1. 单击工具栏中的 报告 图标。
2. 在 报告管理器 对话中，选择您想要计划的报告，并单击 计划。
3. 在出现的对话框的 计划 标签中，选择 计划安排此报告。
4. 输入开始日期和时间，以及生成报告的频率。
5. 指定输出的文件的格式和语言。

6. 输入报告收件人的电子邮件地址。

10.12 运行报告

1. 单击工具栏中的 报告 图标。
2. 在 报告管理器 对话框中，选择您想要运行的报告，并单击 运行。
   显示报告的 报告发送 窗口会出现。

您可以更改报告的页面设置，并打印报告或导出报告到文件中。

10.13 查看图表形式的报告

有些报告可以同时以表的形式和图的形式查看。如果是这种情况，在出现在报告中的 报告发送 窗中，您将看到两个标签页，表 和 图。

1. 单击工具栏中的 报告 图标。
2. 在 报告管理器 对话框中，选择您想要运行的报告，如：按照每个路径提供警报和事件，然后，单击 运行。
   显示报告的 报告发送 窗口会出现。
3. 查看图表形式的报告，请转到相应的标签页。

10.14 打印报告

要打印报告，请单击报告顶端，工具栏上的 打印 图标。

10.15 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。
   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。

10.16 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。

11 审核

审核功能使您能够监控 Enterprise Console 的配置所发生的更改，以及其它用户和系统的操作行为。您可以在规范遵照和排疑解难时使用此（审核）信息，或者，在发生恶意入侵活动时，使用此信息进行证据采集与分析。

依照默认值，审核是禁用的。在启用了审核功能后，每当某些配置设置被更改时，或者，某些操作被执行时，都会有一条审核条目被写入审核数据库中。

注释
如果您使用基于角色的管理，那么，您必须具有 审核 权限，才能启用或禁用审核。要了解更多信息，请参见管理角色和子领域 （第 12 页）。

审核记录包括以下信息：

- 执行的操作
- 执行操作的用户
- 用户的计算机
- 用户的子领域
- 操作的日期和时间

无论是成功的操作，还是失败的操作，两者都会被审核，因此，审核记录会显示谁在系统中之行了操作，谁进行了最终没有成功的操作。

受审核的操作包括：

类别	操作
计算机操作	确认已知/处置警报和错误，保护计算机，更新计算机，删除计算机，在某个计算机上执行完整系统扫描
计算机组管理	创建组，删除组，移动组，重命名组，指派计算机到组
策略管理	创建策略，重命名策略，复制策略，编辑策略，指派策略到计算机，重置策略为厂商默认策略，删除策略
角色管理	创建角色，删除角色，重命名角色，复制角色，添加用户到角色，从角色中删除用户，添加权限到角色，从角色中删除权限
更新管理器管理	更新更新管理器，使更新管理器遵照配置，确认已知警报，删除更新管理器，配置更新管理器，添加新的软件预订，删除软件预订，重命名软件预订，编辑软件预订，复制软件预订
系统事件	启用审核，禁用审核

您可以使用第三方的软件，如：Microsoft Excel，Microsoft Access，Microsoft SQL Server Reporting Services，或者 Crystal Reports 等，访问和分析存储在审核数据库中的数据。要了解有关怎样查看审核条目的信息，请参见 Sophos Enterprise Console 审核用户指南。

11.1 启用或禁用审核

如果您使用基于角色的管理，那么，您必须具有 审核 权限，才能启用或禁用审核。要了解更多信息，请参见管理角色和子领域 （第 12 页）。

要启用或禁用审核：

1. 在 工具 菜单中，单击 管理审核。
2. 在 管理审核 对话框中，勾选或取消勾选 启用审核 勾选框，可以启用或禁用审核。此选项默认为禁用。

12 从 Enterprise Console 复制和打印数据

12.1 从计算机列表复制数据

您可以复制在计算机列表的 终结点 视图中中显示的数据，到“剪贴板”中，然后，可以将数据粘贴到“制表符分隔”格式的文档中。

1. 在 终结点 视图的 组 窗格板中，选择您想要复制数据的计算机组。
2. 在 查看 下拉列表中，选择您想要显示的计算机，例如，有潜在问题的计算机。
3. 如果该组含有子组，请选择您想显示的计算机是 仅在这一级 或在 在这一级，及以下级。
4. 在计算机列表中，在与您想要显示的内容相关的标签页中，例如，防病毒详情。
5. 单击计算机列表以激活它。
6. 在 编辑 菜单中，单击 复制 将数据复制到“剪贴板”中。

12.2 从计算机列表打印数据

您可以在 终结点 视图中打印显示在计算机列表中的信息。

1. 在 终结点 视图的 组 窗格板中，选择您想要打印数据的计算机组。
2. 在 查看 下拉列表中，选择您想要显示的计算机，例如，有潜在问题的计算机。
3. 如果该组含有子组，请选择您想显示的计算机是 仅在这一级 或在 在这一级，及以下级。
4. 在计算机列表中，在与您想要显示的内容相关的标签页中，例如，防病毒详情。
5. 单击计算机列表以激活它。
6. 在 文件 菜单中，单击 打印。

12.3 复制计算机详情

您可以从 计算机详情 对话框中复制信息到“剪贴板”中，然后，将它们粘贴到其它文档中。这些信息包括：计算机名称，计算机的操作系统，安装在计算机上的安全软件的版本，任何尚未处理的警报和错误，更新状态，等等。

1. 在 终结点 视图的计算机列表中，双击您想要复制数据的计算机。
2. 在 计算机详情 对话框中，单击 复制，复制数据到“剪贴板”中。

12.4 打印计算机详情

您可以从 计算机详情 对话框中打印信息。这些信息包括：计算机名称，计算机的操作系统，安装在计算机上的安全软件的版本，任何尚未处理的警报和错误，更新状态，等等。

1. 在 终结点 视图的计算机列表中，双击您想要打印的计算机。
2. 在 计算机详情 对话框中，单击 打印。

13 排疑解难

当您运行“保护计算机向导”时，由于以下几种原因，安全软件的安装可能会失败：

- 自动安装不能该操作系统的计算机上进行。执行手动安装。对于其他操作系统（如果您的许可证允许您保护它们），请参阅 安装指南（供 Linux 和 UNIX 用户使用）。
- 无法确定计算机的操作系统。这可能是因为在查找计算机时，您没有以“域名\用户名”的形式输入用户名。
- 防火墙规则阻止部署安全软件所需的访问。

13.1 计算机没有运行读写扫描

如果有计算机没有运行读写扫描：

1. 请检查这些计算机使用的防病毒和 HIPS 策略。
   有关详细信息，请参见查看组采用的策略 （第 23 页）。
2. 请确保已在该策略中启用了读写扫描，并且这些计算机已遵照此策略。
   有关详细信息，请参见开启或关闭读写扫描 （第 70 页）和使计算机采用组策略 （第 29 页）。

13.2 防火墙已禁用

如果有计算机上的防火墙已禁用：

1. 请检查这些防火墙使用的是哪个防火墙策略。
   有关详细信息，请参见查看组采用的策略 （第 23 页）。
2. 请确保已在该策略中启用了防火墙，并且这些计算机已遵照此策略。
   有关详细信息，请参见临时禁用防火墙 （第 100 页）和使计算机采用组策略 （第 29 页）。

13.3 防火墙未安装

注释
如果您使用基于角色的管理，那么，您必须具备 计算机搜索，保护和组 权限，才能安装防火墙。要了解更多信息，请参见管理角色和子领域 （第 12 页）。

在试图安装客户端防火墙到终结点计算机上之前，请检查终结点计算机上运行的不是服务器板的 Windows 操作系统。

注释
您无法在运行服务器操作系统，或者运行 Windows Vista Starter 的计算机上安装防火墙。

如果您想要在计算机上安装防火墙：

1. 请选择该计算机，单击鼠标右键，并选择 保护计算机。
   会出现 保护计算机向导。单击 下一步。
2. 当提示选择功能时，请选择 防火墙。结束向导。

如果问题继续存在，请联系 Sophos 技术支持。

13.4 具有未处置的警报的计算机

- 如果有计算机感染了病毒，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 （第 46 页）。
- 如果在计算机上检测到了您想要的广告软件或其他可能不想安装的应用程序，请参见批准广告软件和可能不想安装的应用程序 （第 91 页）。
- 如果有未及时更新的计算机，要获得有关诊断和解决问题的帮助，请参见更新未及时更新的计算机（第 65 页）。

注释
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 处置警报和错误。您必须具备 调整 - 清除 权限，才能确认已知（清空）警报和错误。

13.5 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。

注释
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（请参见管理角色和子领域 （第 12 页））。单击工具栏中的 发现计算机 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 组中。

如果某计算机没有被管理，有关它的详情，在 状态 标签页中会被灰白显示。

要开始管理未受管理的计算机：

1. 在 视图 下拉列表中，选择 未管理的计算机。
2. 执行下列操作之一：
   - 如果未受管理的计算机位于未指派组中，则选择这些计算机，将它们拖放到目标组中。启动的保护计算机向导可帮助您保护上述计算机。
   - 如果上述计算机已位于某一组中，则选择这些计算机，右击并选择保护计算机，以安装托管版 Sophos Endpoint Security and Control。
3. 如果有任何计算机，Enterprise Console 无法为其自动安装 Sophos Endpoint Security and Control，请进行 手动安装。

   使用保护计算机向导进行自动安装这一功能仅适用于 Windows 计算机。如需保护 Macs、Linux 或 UNIX 计算机，请手动安装软件。

   要了解手动保护 Macs 或 Windows 计算机的相关信息，请参见 Sophos Enterprise Console 高级启动指南。

   要了解保护 Linux 或 UNIX 的相关信息，请参见 Linux 和 UNIX 的 Sophos Enterprise Console 启动指南。

13.6 无法保护在“未指派”组中的计算机

未指派 组只用于放置尚未属于任何您创建的组的计算机，策略不能应用到此组中。直到将计算机放置到您创建的组中后，您才能保护它们。

13.7 Sophos Endpoint Security and Control 安装失败

如果 保护计算机向导 在计算机上安装 Sophos Endpoint Security and Control 失败，可能会是因为：

- Enterprise Console 不知道在计算机上运行的是哪个操作系统。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。
- 自动安装不能该操作系统的计算机上进行。执行手动安装。要了解具体的操作指导，请参见 Sophos Enterprise Console 高级安装指南。
- 计算机上正在运行防火墙。
- 在 Windows XP 计算机上的“简单文件共享”没有关闭。
- 在 Windows Vista 计算机，“简单文件共享”选项没有关闭。
- 计算机上的操作系统不支持您选择安装的功能。

要了解 Sophos Endpoint Security and Control 功能的系统要求的完整列表，请参见 Sophos 网站上的系统要求 (http://www.sophos.com/zh-cn/products/all-system-requirements)。

13.8 计算机未更新

要获得有关诊断和解决问题的帮助，请参见更新未及时更新的计算机 （第 65 页）。

13.9 防病毒设置在 Mac 计算机上不起作用

有些防病毒设置不能应用于 Mac 计算机。在这种情况下，在设置的页面中会出现警告文字。

更多有关适用于 Mac 的防病毒和 HIPS 策略设置的信息，请访问 Sophos 技术支持知识库文章 118859。

13.10 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，在设置的页面中会出现警告文字。

您可以按照 Sophos Anti-Virus for Linux configuration guide （英文） 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 configuration guide（英文）中的说明，使用 savscan 命令，更改 UNIX 计算机上的防病毒设置。

13.11 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。

13.12 在 Windows 计算机中出现未预期的新扫描

如果在 Windows 计算机上查看本地的 Sophos Endpoint Security and Control，您可能会看到有新的“可用扫描”列示出来，即使用户并没有创建新的扫描。

这个新扫描实际上是您从控制台中设置的计划扫描。您不应该删除它。

13.13 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 Endpoint Security and Control，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。

13.14 没有检测到广告软件和可能不想安装的应用程序 (PUA)

如果 没有检测到广告软件和其它可能不想安装的应用程序 (PUA)，那么，您应该检查：

- 检测是否已启用。请参阅配置读写扫描 （第 69 页）。
- 应用程序所运行的计算机运行的是 Windows 操作系统。

13.15 部分检测到项目

Sophos Endpoint Security and Control 可能会报告该项目（例如，特洛伊木马或可能不想安装的应用程序）为“部分检测到”。这说明它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 Windows 操作系统的计算机上，您可以通过选择计算机，右击并选择完整系统扫描来实现。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。请参阅 配置读写扫描 （第 69 页） 和 创建计划扫描 （第 74 页）。

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（参见从读写扫描中排除项目 （第 73 页））。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 Endpoint Security and Control 可能不能够彻底检测到或者删除，有组件安装在网络驱动器上的广告软件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。

13.16 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 Endpoint Security and Control 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：

- 禁用针对广告软件和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）。请参阅批准广告软件和可能不想安装的应用程序 （第 91 页）。
- 清除计算机，删除您没有批准的应用程序。请参阅立即清除计算机 （第 46 页）。

13.17 清除失败

如果 Sophos Endpoint Security and Control 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。请参阅立即扫描计算机 （第 45 页）。
- 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。检查是否有项目被排除在了扫描之外（参见从读写扫描中排除项目 （第 73 页））。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）。

13.18 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 查看安全信息。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。

13.19 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 Endpoint Security and Control 无法还原所有的设置。例如，某应用程序更改了浏览器的主页，而 Sophos Endpoint Security and Control 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 Endpoint Security and Control 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 查看安全信息。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和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。

13.20 数据控制不能检查通过嵌入式浏览器上传的文件

数据控制会介入通过独立使用的网页浏览器上传的文件。但它不会介入通过嵌入第三方应用程序（如：Lotus Notes）中浏览器上传的文件。如果您具有带有嵌入式浏览器的第三方应用程序，并且想要监控所有上传的文件，那么，您需要配置该应用程序启动外部的浏览器。

13.21 数据控制不扫描上传或附带的文件

如果数据控制不扫描使用受监控的应用程序（例如：电子邮件客户端，网页浏览器，或者，即时消息 (IM) 客户端）从网络路径中上传或附带的文件，那可能是因为您在“防病毒和 HIPS 策略”中将远程文件从读写扫描中排除了。这种情况下，数据控制使用 Sophos Anti-Virus 读写扫描器 (InterCheck™) 所使用的同一组排除文件，所以，如果禁用了远程文件扫描，那么，不会有任何远程文件发送给数据控制进行检查。

要了解更多有关配置读写扫描排除文件的信息，请参见从读写扫描中排除项目 （第 73 页）。

注释
使用 Windows 资源管理器复制或移动文件时，数据控制将不使用读写扫描排除项目。这种情况下，数据控制会介入从网络路径从向受监控的存储设备传输文件，例如：复制文件到可移动的存储设备，或者，烧录数据到光学介质上。

13.22 卸载了的更新管理器出现在控制台中

在您卸载了附加的更新管理器之后，它可能仍然出现在 Enterprise Console 的 更新管理器 视图中。

要从控制台中删除更新管理器，请选择它，单击鼠标右键，然后单击 删除。

14 用语表

Active Directory 同步化事件 (Active Directory synchroization event)	与 Active Directory 进行同步化时发生的事件。
活动子领域 (active sub-estate)	在组窗格板中显示的子领域。
高级内容控制列表编辑器 (advanced Content Control List editor)	一种编辑器，它使用户能够创建，由积分 (score)，最大计数 (maximum count)，正则表达式 (regular expression)，以及在匹配内容控制列表 (Content Control List) 之前必须达到的触发积分 (trigger score) 等，构成的一种自定义内容控制列表 (custom Content Control List)。
应用程序管理器 (Application manager)	一个对话框，它使您能够，针对被 Sophos Client Firewall 阻断的应用程序，允许或创建新规则。
审核 (auditing)	一种功能，它使您能够监控 Enterprise Console 的配置所发生的更改，以及其它用户和系统的操作行为。
自动保护	一旦安全软件完成了与 Enterprise Console 进行的同步化，就立即将安全软件部署（安装和策略强制实施）到某个 Active Directory 容器中的所有的计算机上。
种类 (category)	一种指定的标记，它用于根据类型 (type)，定义内容的正则 (regulation)，或所应用于的范围 (region)，来分类 SophosLabs 内容控制列表。
内容控制列表 (CCL) (Content Control List (CCL))	指定文件内容的一组条件，例如，与其它形式的个人识别信息在一起的信用卡或借记卡号码，或银行帐号详情。有两种类型的内容控制列表：SophosLabs 内容控制列表，和自定义内容控制列表。
内容规则 (content rule)	一种规则，它包括一个或多个内容控制列表，并指定，如果用户试图传输匹配了规则中的全部内容控制列表的数据到指定目标路径 (destination) 时，采取的措施。
受控程序 (controlled application)	公司想要检测或阻断的非恶意的应用程序，因为它们会影响工作或网络的运行效率。
受控数据 (controlled data)	满足数据控制条件的文件。
受控设备 (controlled device)	受到设备控制功能影响的设备。
紧要级 (critical level)	触发某个项目的安全状态转变为“紧要 (Critical)”的值。
自定义内容控制列表 (custom Content Control List)	由 Sophos 用户创建的内容控制列表。有两种方法可以创建自定义内容控制列表：创建带有特定的搜索条件（如：“所有这些搜索词”）的搜索词的简单列表；或者，使用高级内容控制列表编辑器。
指标面板 (Dashboard)	网络安全状态的一览图。

指标面板事件 (Dashboard event)	指标面板中的健康指标超过紧要级的事件。在指标面板事件发生时，会发出电子邮件警报。
数据控制	一种功能，用于减少从工作站计算机中意外丢失数据的机会。当工作站计算机的用户试图传输的文件，满足在数据控制策略和规则中定义的标准时，数据控制功能会采取相应的措施。例如，当某用户试图复制包含客户资料列表的电子表格文件到可移动的存储设备中时，或者，上传标记为机密的文档到 Webmail 帐户中时，数据控制功能会阻断此传输，如果事先的配置要求这样做。
数据丢失防护 (DLP)	请参阅数据控制。
数据库 (database)	Sophos Enterprise Console 组件，存储有关网络中的计算机的详情。
默认子领域 (Default sub-estate)	目录树的根在服务器的组树的根节点和 未指派 组中的子领域。当首次打开 Enterprise Console 时，它会作为默认值显示。
设备控制 (device control)	一种功能，用于减少从工作站计算机中意外丢失数据的机会，并且可以限制从网络外部引进和安装软件。当工作站计算机用户试图在他们的计算机上，使用某个未经批准的存储设备或网络设备时，该功能会采取措施。
下载信誉	从 Internet 下载的文件的信誉。信誉按文件的时间、来源、普遍性、深度内容分析和其他特征进行计算。它有助于确定文件是否安全或有潜在风险，以及如果下载是否会损坏用户的计算机。
领域 (estate)	请参阅 IT 领域 (IT estate)。
免除设备 (exempt device)	明确地从设备控制中排除的设备。
表达式 (expression)	请参阅正则表达式 (regular expression)。
文件匹配规则 (file matching rule)	一种规则，用于指定，如果用户试图传输带有特定的文件名或特定的文件类型的文件到特定的目标路径 (destination) 时，将要采取的措施，例如，阻断传输数据库到可移动的存储设备中。
组 (group)	在 Sophos Enterprise Console 中定义的受管理的计算机的组。
健康指标 (health indicator)	描述指标面板中某个部分或项目的安全状态，或者，描述网络的总体健康状态的，各种图标的总称。
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。
IT 领域 (IT estate)	公司的 IT 环境，包括计算机，网络，等等。
恶意数据流检测(Malicious Traffic Detection)	此功能可检测受影响的计算机和攻击者的命令和控制服务器之间的通信。
受管理的计算机 (managed computer)	安装了远程管理系统 (RMS) 的计算机，在该计算机上 Sophos Enterprise Console 可以报告，以及安装和更新软件。
管理控制台 (management console)	Sophos Enterprise Console 组件，使您能够保护和管理计算机。

管理服务器 (management server)	Sophos Enterprise Console 组件，处理更新和联网计算机之间的通讯。
最大计数 (maximum count)	可以计入到总积分中的，某正则表达式的匹配数目的最大值。
未及时更新的计算机 (out-of-date computer)	没有及时更新 Sophos 软件的计算机。
补丁评估	评估计算机上已安装的补丁，以及识别遗漏的补丁。
策略 (policy)	一组设置，例如：应用到某个组或多个组的计算机上的用于更新的一组设置。
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应用程序。
数量 (quantity)	在内容控制列表被匹配之前，必须在文件中找到的内容控制列表的主码数据类型 (key data type) 的数量。
数量主码 (quantity key)	在内容控制列表中定义的主码数据类型 (key type of data)，数量设置将应用于该主码数据类型。例如，对于某个包含信用卡或借记卡的号码的内容控制列表，数量指定，在内容控制列表被匹配之前，必须在文件中找到多少信用卡或借记卡的号码。
范围 (region)	SophosLabs 内容控制列表的范围。范围，要么指定内容控制列表（国家特定的内容控制列表）所应用的国家，要么显示为“全球”（应用于所有国家的全球内容控制列表）。
正则表达式 (regular expression)	一种搜索字符串，它使用指定的字符去匹配文件中的文本范式 (text pattern)。数据控制 (Data Control) 使用的是 Perl 5 正则表达式句法 (regular expression syntax)。
权限 (right)	在 Enterprise Console 中执行某种任务的许可的集合。
角色 (role)	决定访问 Enterprise Console 的权限的集合。
基于角色的管理 (role-based administration)	一种功能，它允许根据用户在公司中的角色，指定他们可以访问哪些计算机，以及可以执行哪些任务。
rootkit	一种特洛伊木马或类似的技术，它用来隐藏恶意的对象（进程，文件，注册键，或网络端口），避免计算机用户或系统管理员发现它们。
规则 (rule)	规则，用于指定如果某个文件满足了特定的条件时，所要采取的措施。有两种类型的数据控制规则：文件匹配规则和内容规则。
积分 (score)	当某个正则表达式被匹配时，加入到内容控制列表的总积分 (total score) 中的分数。
服务器根节点 (server root node)	在 组 窗格板中的组树中的最高层的节点，它包括未指派 组。
Sophos Live Protection	一种使用云计算技术的功能，它能不断地判断可疑文件是否成为安全隐患，并随时采取在 Sophos 防病毒保护配置中所指定的相应措施。

Sophos Update Manager (SUM)	一种程序，用于将 Sophos 安全软件和更新文件从 Sophos 或其它更新服务器上下载到共享的更新路径中。
Sophos 定义规则 (Sophos-defined rule)	由 Sophos 提供的作为范例的规则。Sophos 不更新 Sophos 定义规则。
SophosLabs 内容控制列表 (SophosLabs Content Control List)	由 Sophos 提供和管理的一种内容控制列表。Sophos 可以更新 SophosLabs 内容控制列表，或创建新的内容控制列表，并在 Enterprise Console 中提供这些列表。SophosLabs 内容控制列表中的内容无法被编辑。不过，可以为每个这样的内容控制列表设置数量 (quantity)。
子领域 (sub-estate)	IT 领域中某命名部分，包括计算机和组的子网。
子领域管理 (sub-estate administration)	一种功能，它可以限制在某些计算机和组上执行某些操作。
软件预订 (software subscription)	针对各种操作平台的各种软件集，由用户选择后，更新管理器会下载它们，并保持更新它们。可以为每个支持的平台指定一个版本（例如，为 Windows 指定“推荐”）。
可疑行为检测 (suspicious behavior detection)	对运行在系统中的所有程序的行为进行的动态分析，以检测和阻断可能的恶意活动。
可疑文件 (suspicious file)	一种文件，在文件中出现了病毒中普遍具有，但又不仅是病毒中才具有的一系列特征。
同步化间隔 (synchronization interval)	在 Enterprise Console 中同步化点与所选的 Active Directory 容器进行了同步化之后，到下一次进行同步化之间的时间间隔。
(针对 Active Directory 树的) 同步化点 (synchronization point (for an Active Directory tree))	一个 Sophos Enterprise Console 组，在该组中，所选的 Active Directory 容器（组和计算机，或者，只有组）里的内容，会被添加以进行同步化，它们的结构会保留不变。
与 Active Directory 同步化	Sophos Enterprise Console 组与 Active Directory 组织单元 (organizational unit)，或者容器进行的单向同步化。
已同步化的组 (synchronized group)	在同步化点下的任何组。
系统管理员 (System Administrator)	预置角色，具有管理网络中的 Sophos 安全软件，以及管理 Enterprise Console 中的角色的所有权限。 系统管理员 (System Administrator) 角色不能被删除，也不被更改名称或权限，并且 Sophos Full Administrators Windows 组不能从中被删除。其它的用户和组可以在角色中被添加或删除。
标记 (tag)	应用到 SophosLabs 内容控制列表中的一种标识符 (descriptor)，以识别内容控制列表的内容或范围。有三种类型的标记：类型 (type)，规定 (regulation)，范围 (region)。
介入防范 (tamper protection)	能够防范已知的恶意软件，以及防止未经授权的用户通过 Sophos Endpoint Security and Control 用户界面，卸载或禁用 Sophos 安全软件的一种功能。

指标级别 (threshold level)	触发某个项目的安全状态转变为“提醒 (Warning)”或“紧要 (Critical)”的值。
总积分 (total score)	按照已被满足的内容，某个内容控制列表所计的总积分。
触发积分 (trigger score)	在内容控制列表被匹配之前，正则表达式必须被匹配的次数。
真实文件类型 (true file type)	经过分析文件的结构，而不是通过文件的文件扩展名，而确认的文件类型。这是一种更加可靠的确认文件类型的方法。
类型 (type)	SophosLabs 内容控制列表分类所依据的标准，例如，某个内容控制列表定义的护照详情，邮寄地址，或者，电子邮件地址，属于个人识别信息类型 (Personally Identifiable Information type)。
更新管理器	请参阅 Sophos Update Manager。
提醒级 (warning level)	触发某个项目的安全状态转变为“提醒 (Warning)”的值。
网页控制 (web control)	使您能够设置和强制实施网页访问策略，并且可以查看网页浏览量报告的一种功能。您可以允许或阻断用户访问某些类别的网站，用户还会被提醒访问某个网站是否会违反公司规定。
Web 保护	可以检测网页中的安全隐患的功能。此功能可以阻断在过去用来发布恶意代码内容的网站，同时还会防止下载恶意代码。Web 保护是“防病毒和 HIPS 策略”的一部分。

15 技术支持

您可以通过以下各种方式获得 Sophos 产品的技术支持：

- 访问 community.sophos.com/ 的 Sophos Community 论坛，并搜索遇到相同问题的其它用户。
- 访问 www.sophos.com/zh-cn/support.aspx 的 Sophos 技术支持知识库。
- 在 www.sophos.com/zh-cn/support/documentation.aspx 中下载产品的技术文档。
- 访问 https://secure2.sophos.com/support/contact-support/support-query.aspx 联系我们的技术支持团队。

16 法律声明

索引

A

B

C

D

E

F

G

H

I

J

K

L

M

N

P

Q

R

S

T

U

W

X

Y

Z