

SOPHOS

Sophos Control Center 安装指南

产品版本：4.1

文档日期：2011 年 4 月



目录

1 关于本指南.....	3
2 系统要求.....	3
3 安装.....	4
4 保护联网计算机.....	7
5 检查计算机的保护状况.....	9
6 设置电子邮件警报.....	10
7 设置扫描可能不想安装的应用程序.....	11
8 处理病毒.....	13
9 设置防火墙.....	13
10 技术支持.....	16
11 版权所有.....	16

1 关于本指南

本指南将告诉您怎样保护您的联网计算机(包括 Windows 计算机和 Mac 计算机)，防范病毒(包括间谍软件)，可能不想安装的应用程序，以及其它安全隐患。

如果您有从不连接到网络中的计算机，请同时参见 *Sophos Endpoint Security and Control* 独立用户 (standalone) 安装指南。

如果您是从更早的版本 Sophos Control Center，请参见 *Sophos Control Center* 升级指南。

要了解本指南中没有提及的，所有 Sophos Control Center 的配置选项的详情，请参见 Sophos Control Center 帮助文件。

Sophos 文档均发布在 <http://cn.sophos.com/support/docs/>。

2 系统要求

要了解系统要求，请参见 Sophos 网站 <http://cn.sophos.com/products/all-sysreqs.html> 中的系统要求页面。

另外，您必须能够访问因特网，可以从 Sophos 网站下载软件。

Sophos Control Center 和服务器组件具有以下的其它要求：

- 您必须具有访问其它联网计算机的权限，同时它们也具有访问服务器的权限。
- 建议使用服务器操作系统，(如：Windows Server 2003，或 Windows Small Business Server 2011)。否则，Sophos Control Center 的运行效果将受到影响。

重要：如果您是在 Windows 2008 Small Business Server (SBS) 上安装 Sophos Control Center，那么，请确保在该计算机上没有安装 Windows Live OneCare。要卸载 Windows Live OneCare，请从 Windows 控制面板中，使用“添加/删除程序”来进行。

如果您要使用 SQL Server（而不是 Sophos 的其它产品所使用的 SQL Server Express 2005 Express），那么，请确保安装了 SQL Server，并创建了 SOPHOS 实例。要获得与此相关的帮助，请参见您的 SQL Server 技术文档，或者联系 Microsoft Technical Support 技术支持。

3 安装

3.1 准备安装 Sophos Control Center

在您安装 Sophos Control Center 之前，请确保：

- 您具有 Sophos 提供的用户名和密码。
- 在您想要安装 Sophos Control Center 的计算机上，根据情况，以系统管理员或域管理员的身份登录。

注：要保护在任何 Windows 操作系统中的工作组中的计算机，您必须首先执行在文章中提到的附加的步骤。

<http://cn.sophos.com/support/knowledgebase/article/29728.html>。

3.2 准备终结点计算机

在您将安全软件安装到终结点计算机上之前，请确保：

- 在您想要安装 Sophos Anti-Virus 的计算机上，已删除其它软件商的防病毒软件。
- 操作系统按照要求已配置。

3.2.1 Windows Vista 及以后

Sophos Anti-Virus 对 Windows Vista 及以后操作系统的计算机有以下额外的要求：

- 确保 **Remote Registry** 服务已启动，并且它的启动类型设置为 **自动**。在 Windows Vista 中该服务没有默认为开启状态。要开启该服务，可打开 **开始|控制面板|管理工具|服务**。滚动服务列表，双击 **Remote Registry** 服务。在 **Remote Registry** 属性对话框中的 **常规** 标签页中，在 **启动类型** 文本框中，单击下拉箭头，然后，选择 **自动**。单击 **应用**。单击 **开始**，并单击 **确定**。
- 关闭 **用户帐户控制**。这可以通过 **开始|控制面板|用户帐户|开启或关闭用户帐户控制** 来实现。在安装完成之后，您应该重新开启它。
- 打开 **高级安全 Windows 防火墙**。要开启该服务，可打开 **开始|控制面板|管理工具**。更改 **入站规则** 启动以下选项：

规则名称	配置文件
Remote Administration (NP-In)	域
Remote Administration (NP-In)	专有
Remote Administration (RPC)	域
Remote Administration (RPC)	专有
Remote Administration (RPC-EPMAP)	域
Remote Administration (RPC-EPMAP)	专有

注: 在安装完成之后, 您应该重新禁用它们。

3.2.2 Windows XP

您必须在所有 Windows XP 计算机上执行以下步骤:

- 在您想要安装 Sophos Client Firewall 的所有 Windows XP 计算机上, 删除 Windows Firewall 之外的, 任何其它软件商的防火墙软件。

- 禁用简单文件共享。

要了解怎样做到这一点, 请参见

<http://cn.sophos.com/support/knowledgebase/article/12837.html>。

Windows XP SP 2

在 Windows XP SP 2 的操作系统的计算机上, 如果 Windows Firewall 是开启的, 并且您并不打算在这些计算机上安装 Sophos Client Firewall, 那么, 您必须按照以下说明做:

- 为 Microsoft 网络启用文件和打印机共享。
- 添加以下的程序例外(program exception):

C:\Program Files\Sophos\Remote Management System\RouterNT.exe

要了解怎样做到这一点, 请参见

<http://cn.sophos.com/support/knowledgebase/article/11075.html>。

3.2.3 Windows Server 2003 SP1

如果 Windows Firewall 是开启的, 那么, 您必须完成以下事项:

- 为 Microsoft 网络启用文件和打印机共享。

- 添加以下的程序例外(program exception):

C:\Program Files\Sophos\Remote Management System\RouterNT.exe

要了解怎样做到这一点, 请参见

<http://cn.sophos.com/support/knowledgebase/article/11075.html>。

3.2.4 Windows 2000

- 在您想要安装 Sophos Client Firewall 的所有 Windows 2000 计算机上, 删除 Windows Firewall 之外的, 任何其它软件商的防火墙软件。

3.2.5 Windows 98 SE

- 删除任何现有的 Sophos Anti-Virus。要完成此项删除, 请通过 Windows 控制面板中的“添加/删除程序”来进行。

3.3 安装 Sophos Control Center

您首先要安装 Sophos Control Center, 它使您能够下载, 部署, 以及管理防病毒和防火墙软件。

1. 访问 <http://cn.sophos.com/support/updates> 中的 Sophos 产品下载页面, 输入 Sophos 提供的用户名和密码。

跟随链接下载您的 Sophos Small Business Solutions 安装程序, 然后, 运行它。

2. 在提取程序 (**Sophos Small Business Edition 安装程序**) 中确认放置所提取的安装文件的路径 (它必须在您安装 Sophos Control Center 的同一台计算机上), 然后, 单击 **安装**。
3. 在 **欢迎** 页面中, 单击 **下一步**。

会出现一个向导指导您完成安装过程。除了以下显示的以外, 接受默认选项。

4. 在 **设置类型** 页面中, 选择 **完整** 以安装所有的程序功能。

注: 如果您想要从别的计算机上管理安全软件, 您可以将安装程序复制到该计算机上, 运行安装程序, 并选择 **仅限 Management Console**。

单击 **下一步**, 然后, 继续再次进行此向导, 并接受默认选项。

5. 当安装结束后，单击 **完成** 以自动注销。如果您想要稍后再注销，请先取消勾选 **现在注销** 勾选框，再单击 **完成**。

有时，有必要重新启动 Windows 操作系统，而不是简单地注销。在这种情况下，不会出现勾选框，会接着出现消息框，询问您是否现在重新启动 Windows，或稍后再启动。

6. 当您再次登录时，请以同样的用户身份登录。Sophos 网络保护向导会自动启动。

要了解有关保护联网计算机的信息，请参见 [保护联网计算机](#)（第7页）。

4 保护联网计算机

当您在安装 Sophos Control Center 之后，首次登录到计算机时，Sophos Control Center 会自动打开，并出现 Sophos 网络保护向导。该向导使您能够保护联网的计算机。

1. 在 **欢迎** 页面中，单击 **下一步**。
2. 在 **Sophos 下载帐户详情** 页面中，请输入由 Sophos 提供给您的用户名和密码，并单击 **下一步**。

依照默认值，Sophos Control Center 会将软件下载到您当前正在使用的计算机上的 C:\Program Files\Sophos\SCC\Library 文件夹中，然后，从该文件夹中，将所下载的软件分发给其它的计算机。路径会因操作系统的不同而不同：

- Windows 2000/XP/2003:
C:\Documents and Settings\All Users\Application Data\Sophos\Update Manager\Update Manager\CIDs\
- Windows Vista 及以后：
C:\ProgramData\Sophos\Update Manager\Update Manager\CIDs\

如果您使用代理服务器连接到因特网，请勾选 **通过代理服务器访问 Sophos**，然后，输入代理服务器。

3. 在 **操作平台选择** 页面中，请选择针对在您的计算机上运行的操作系统的软件。
 - **Windows 2000 及以后** 是默认选项。
 - 如果使用 Mac OS X 计算机，请选择 **Mac OS X** 勾选框。这将使您稍后能够在这些计算机上安装防病毒软件。
4. 在 **正在下载软件** 页面中，会出现进度条。Sophos Control Center 会下载软件。当下载完成后，单击 **下一步**。

5. 在 **Windows 用户帐户详情** 页面中，输入对于所有联网计算机都有效的，具有管理权限的帐户的详情，以便可以将软件安装在这些计算机上。该帐户不同于您早先使用的 Sophos 帐户。在许多情况下，您可以使用在开始进行安装时，登录计算机的帐户。

6. 在 **保护计算机** 页面中，向导会搜索能够自动安装软件的计算机。

因为不能在 Windows 98 或 Mac 计算机上进行自动安装，只有 Windows 2000 及以后的计算机才会被列示在此页中。

依照默认值，所有的计算机都选择为需要提供保护。您可以取消勾选您不需要提供保护的计算机旁的勾选框。要选择或取消勾选列表中的所有 **保护** 勾选框，请勾选或取消勾选 **保护** 栏目标题旁的勾选框。

7. 在 **选择功能** 页面中，选择您想要安装的功能：

- 防病毒保护（默认选择）。
- Sophos Client Firewall 保护（如果您的用户授权使用许可协议包括）。

注：您必须重新启动安装了 Sophos Client Firewall 的各台计算机，以激活防火墙。

- 同类软件产品删除工具。

单击 **下一步**。

8. 如果在 **必须手动保护的计算机** 页中有计算机的列表，单击 **打印** 可以将这些计算机的列表打印出来，单击 **另存为** 可以保存该列表，或者，可以记下这些计算机。单击 **下一步**，并跟随向导。

Sophos Control Center 会在您所选择的计算机上自动安装软件。

一旦防病毒和防火墙保护应用到了各台计算机上，就会在计算机名称旁显示一个蓝色的计算机图标，并在 **是否及时更新** 栏中显示 **是** 字样。

要了解怎样手动保护计算机的信息，请参见 [手动保护联网计算机](#)（第8页）。

4.1 手动保护联网计算机

您可以手动保护联网计算机。

1. 到您打印出来，或保存下来的计算机列表中的各台计算机上。浏览找到 Sophos Control Center 用来提供防病毒和防火墙软件和更新文件的那个文件夹。依照默认值，该文件夹是：

操作系统	文件夹
Windows 2000 和以后	\\[server name]\sophosUpdate\CIDs\Sxxx\EECSXP
Windows 98	\\[server name]\sophosUpdate\CIDs\Sxxx\ES9X
Mac OS X	smb://[server name]/sophosUpdate/CIDs/Sxxx/ESCOSX

这里：

[server name] 是您安装了 Sophos Control Center 的那台计算机的名称。

[Sxxx] 代表在进行下载时，生成的数字，如：S000\369。

2. 双击 setup.exe (在 Windows 计算机中) 或 Sophos Anti-Virus.mpkg (在 Mac OS X 计算机中)。

如果您是在 Mac OS X 10.2 或以后的计算机上安装，您必须将 Sophos Anti-Virus.mpkg 复制到该 Mac 计算机上，然后，在那里执行安装。

您还可以保护并不总是联网的计算机（[保护有时连接到网络中的计算机](#)（第 9 页））。

4.2 保护有时连接到网络中的计算机

有时连接到网络中的计算机（例如：不在办公室使用的笔记本型电脑，但有时会带到办公室连接到网络中），可以在没有连接到网络中时，也受到保护。

您安装了防病毒和防火墙软件的所有计算机，已经被配置为，当没有连接到网络中时，可以直接从 Sophos 下载防病毒和防火墙的更新文件。

如果有计算机有时会连接到您的网络中，而您尚未在这些计算机上安装防病毒或防火墙软件，那么，您应该在它们下一次连接到网络中时，为它们提供保护。在 Sophos Control Center 帮助文件中，有关保护新的计算机部分，对此进行了说明。

5 检查计算机的保护状况

通过指标面板，您可以检查计算机是否已受到保护，防范安全隐患。

指标面板提供网络安全状态的“一览图”。您可以配置级别值，以便当达到该值时，指标面板会发出警告，并发送警报信息。

要显示或隐藏指标面板，请单击工具栏上的 **指标面板** 按钮。

要了解怎样配置指标面板，以及所显示的图标和它们的状态的完整列表，请参见 Sophos Control Center 帮助文件。

6 设置电子邮件警报

依照默认值，桌面消息警报只在发现了安全隐患的计算机上出现。您可以配置 Sophos Control Center，使您选择的用户在有安全隐患被发现时，也能够收到电子邮件警报。

要配置关于安全隐患的电子邮件警报：

1. 在左手边的窗格板的 **配置** 下，单击 **配置扫描**。
2. 在 **配置扫描** 对话框中，单击 **消息发送**。

会出现 **消息发送** 对话框。

3. 单击 **电子邮件警报发送** 标签页，选择 **启用电子邮件警报发送** 以接收电子邮件发送的警报。
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：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和清除的设置仅应用于 Windows 2000 及以后。“其它错误”的设置只应用于 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。

注：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。

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

- 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。

您还可以配置 Sophos Control Center，就基于指标面板中的指标级别的网络状态，发送电子邮件警报，相关信息请参见 Sophos Control Center 帮助文件中的“管理通告”部分。

7 设置扫描可能不想安装的应用程序

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

注: 此选项仅应用于运行在 Windows 2000 或以后的计算机上的 Sophos Anti-Virus 中。

Sophos 建议您在开始时，使用计划扫描检测可能不想安装的应用程序。这样使您能够安全地处理已经在您的网络中运行的那些应用程序。在这之后，您可以启用读写扫描可能不想安装的应用程序来保护您的计算机。

7.1 在计算机上运行计划扫描

1. 在左手边的窗格板的 **配置** 下，单击 **配置扫描**。
2. 在 **配置扫描** 对话框中，在 **计划扫描** 面板中，单击 **添加** 创建新扫描，或在列表中选择某个扫描，并单击 **编辑** 以编辑它。
3. 在 **计划扫描** 对话框中，单击 **配置** (在页面底部)。
4. 在 **扫描和清除设置** 对话框中，单击 **扫描** 标签。在 **扫描选项** 面板中，勾选 **扫描广告软件和可能不想安装的应用程序** 勾选框，并单击 **确定**。

当进行扫描时，Sophos Anti-Virus 可能会报告发现某些可能不想安装的应用程序。您既可以批准这些应用程序，也可以从计算机中删除这些程序。

7.2 批准您想要使用的应用程序

您可以选择批准在计划扫描的过程中，被检测为广告软件/可能不想安装的应用程序的应用程序。

要批准某个应用程序：

1. 在左手边的窗格板的 **配置** 下，单击 **配置扫描**。
2. 在 **配置扫描** 对话框中，单击 **批准**。

3. 在 **批准管理器** 对话框中，按照以下说明做：
 - 选择您想要批准的应用程序。单击 **添加**，添加它到已批准的应用程序列表中。
 - 如果您不能找到该应用程序，请单击 **新项目**。在开启的对话框中，根据链接进入 Sophos 的可能不想安装的应用程序的列表。找到您想要批准的应用程序，并将它的名称输入 **名称** 文本框中。

7.3 清除您不想使用的应用程序

您可以清除在计划扫描期间检测到广告软件/可能不想安装的应用程序。

要清除应用程序：

1. 在左手边的窗格板的 **操作** 下，单击 **处置警报和错误**。
会出现 **处置警报和错误** 对话框。
2. 勾选您想要删除的各个应用程序的勾选框，或者，单击 **全选**，然后，单击 **清除**。

这将从所选的计算机中，删除所选择的应用程序的所有已知的组件。清除过程可能会花费一些时间。

注：有些应用程序，您将无法使用 Sophos Control Center 清除它们。出现这种情况时，请到相应的计算机上，使用 Sophos Anti-Virus 来清除这些应用程序。

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

要在 Sophos 网站中了解更多的有关某个应用程序的信息，请在 **处置警报和错误** 对话框中，单击该应用程序的名称。

如果您单击 **确认已知**，所选的应用程序将从列表中删除。不过，它们并没有被清除，也没有被批准。

7.4 启用读写扫描广告软件和可能不想安装的应用程序

1. 在左手边的窗格板的 **配置** 下，单击 **配置扫描**。
会出现 **配置扫描** 对话框。

2. 单击 **读写扫描**。

会出现 **读写扫描设置** 对话框。

3. 在 **扫描选项** 面板中，勾选 **扫描广告软件和可能不想安装的应用程序** 勾选框。单击 **确定**。

有一些应用程序会“监控”文件，并试图频繁地读写文件。如果您已启动了读写扫描，它会检测到每一次读写活动，并发出多个警报。

8 处理病毒

您可以按照以下说明清除病毒。

1. 在 Sophos Control Center 中的 **指标面板** 上单击 **病毒/间谍软件** 链接。

在 **处置警报和错误** 对话框中，会显示被感染的计算机的列表，并带有病毒详情。

2. 选择您想要清除的病毒，并单击 **清除**。

这将从被感染的文件或引导区中清除病毒。不过，清除文档文件中的病毒，并不会修复病毒已经在文档中进行的更改，清除程序文件中的病毒应该只作为暂时的措施：您应该接下来用原始安装盘，或清洁的备份中程序文件，替换被感染过的程序文件。清除过程可能会花费一些时间。

有某些病毒，您将无法使用 Sophos Control Center 清除它们。出现这种情况时，请到相应的计算机上，使用 Sophos Anti-Virus 来清除这些病毒。

Sophos 建议您在试图从计算机上清除多组件的安全隐患之前，在计算机上运行一次完全的计划扫描，以便检测到多组件安全隐患的所有组件。

要在 Sophos 网站中了解更多的有关某个病毒的信息，请在 **处置警报和错误** 对话框中，单击该病毒的名称。

9 设置防火墙

当您首次安装 Sophos Client Firewall 时，它会被设置允许必要的流入和流出通讯流。

注：Sophos Client Firewall 不支持 IPv6。版本 1 会让 IPv6 数据包通过；版本 1.5 和 2.0 会根据配置，要么阻断全部，要么允许全部 IPv6 数据包。

9.1 配置防火墙

您可以配置防火墙按照要求允许或阻断通讯流。依照默认值，防火墙设置为允许必要的流入通讯流和所有的流出通讯流。

要配置防火墙：

1. 在左手边的窗格板的 **配置** 下，单击 **配置防火墙**。
2. 在防火墙配置向导中，单击 **下一步**。
3. 在 **配置防火墙** 页面中，选择以下任何选项：

- **单一路径**

为总是在网络中的计算机，例如，台式机，选择此选项。

- **双重路径**

如果您想要根据计算机所在的路径，例如，在办公室（在网络中），不在办公室，而使用不同的设置，选择此选项。您可能会想为笔记型电脑设置双重路径。

- **允许所有通讯流**

如果您想要关闭防火墙，允许所有通讯流，选择此选项。

4. 如果您在先前的页面中选择了 **双重路径**，请在 **网络识别** 页面中，配置您的网络的 DNS 或 网关识别。

注：网络识别 页面只会在您选择 **双重路径** 时，才出现。

然后，Sophos Control Center 将根据它们是否在网络中，来应用不同的防火墙设置。

5. 在 **操作模式** 页中，选择防火墙应该怎样处置流入和流出通讯流的模式。

■ **阻断入站的通讯流，并允许出站的通讯流。**

这将只允许必要的通讯流从您的计算机访问网络和因特网，但是阻断任何流入通讯流。在此模式中不会验证应用程序。

■ **阻断入站和出站的通讯流。**

如果您选择此模式，防火墙将阻断，除了您指定的通讯流之外的，所有的流出通讯流。单击此选项右边的 **信任** 按钮，以添加应用程序。对于“信任的”应用程序，会被允许进行所有的网络活动。

■ **监控**

此模式将应用任何指定的规则到计算机上，同时将允许所有通讯流访问网络和因特网。此模式会向控制台报告信息。使用此模式可以搜集网络信息以创建适当的规则。

■ **自定义**

这将允许您应用自定义配置。单击 **高级** 按钮，以打开防火墙的高级配置。

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

要了解更多有关高级防火墙的配置，请参见 *Sophos Endpoint Security and Control* 帮助文件。

6. 在 **文件和打印共享** 页中，如果您想要允许局域网中的其它计算机访问打印机，以及您计算机上的共享文件夹，请选择 **允许文件和打印共享**。

7. 如果您选择了 **双重路径**，您会被提示为副路径（不在网络中）设置操作模式，以及文件和打印机共享（如步骤 5 和步骤 6 所述）。

如果您稍后要修改任何设置，您可以选择再次运行向导。

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）。要了解更多的信息，请参见 *Sophos Control Center* 帮助文件。

9.2 处理被防火墙阻断的项目

Sophos Control Center 可能会阻断您想要运行的应用程序或进程。如果出现这样的情况，请按照以下的说明做：

1. 在 Sophos Control Center 中的 **指标面板** 上单击 **防火墙** 链接。
2. 在 **防火墙 - 事件查看器** 对话框中，选择想要允许它，或者为它创建规则的应用程序条目。单击 **创建规则**。

3. 在出现的对话框中，选择是否允许该应用程序，或者，使用现有的预设为它创建规则。

10 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 <http://community.sophos.com/> 中的 SophosTalk 论坛，并搜索遇到相同问题的其它用户。
- 访问 <http://www.sophos.com/support/> 的 Sophos 技术支持知识库。
- 在 <http://www.sophos.com/support/docs/> 中下载产品的技术文档。
- 发送电子邮件至：support@sophos.com，提供您的 Sophos 软件的版本号，计算机的操作系统，补丁级别，以及任何出错信息的原文。

11 版权所有

版权所有 © 2011 Sophos Limited。保留一切权利。本出版物的任何部分，都不得被以电子的、机械的、复印的、记录的或其它的一切手段或形式，再生，存储到检索系统中，或者传输。除非您是有效的被授权用户，并且根据您的用户授权使用许可协议中的条件，您可以再生本文档；或者，除非您事先已经获得了版权所有者的书面许可。

Sophos 和 Sophos Anti-Virus 都是 Sophos Limited 的注册商标。所有其它提及的产品和公司的名称都是其所有者的商标或注册商标。

The Sophos software that is described in this document includes or may include some software programs that are licensed (or sublicensed) to the user under the Common Public License (CPL), which, among other rights, permits the user to have access to the source code. The CPL requires for any software licensed under the terms of the CPL, which is distributed in object code form, that the source code for such software also be made available to the users of the object code form. For any such software covered under the CPL, the source code is available via mail order by submitting a request to Sophos; via email to support@sophos.com or via the web at <http://www.sophos.com/support/queries/enterprise.html>. A copy of the license agreement for any such included software can be found at <http://opensource.org/licenses/cpl1.0.php>

ACE™, TAO™, CIAO™, and CoSMIC™

ACE¹, TAO², CIAO³, and CoSMIC⁴ (henceforth referred to as “DOC software”) are copyrighted by Douglas C. Schmidt⁵ and his research group⁶ at Washington University⁷, University of California⁸, Irvine, and Vanderbilt University⁹, Copyright © 1993 – 2005, all rights reserved.

Since DOC software is open-source, free software, you are free to use, modify, copy, and distribute perpetually and irrevocably the DOC software source code and object code produced from the source, as well as copy and distribute modified versions of this software. You must, however, include this copyright statement along with code built using DOC software.

You can use DOC software in commercial and/or binary software releases and are under no obligation to redistribute any of your source code that is built using DOC software. Note, however, that you may not do anything to the DOC software code, such as copyrighting it yourself or claiming authorship of the DOC software code, that will prevent DOC software from being distributed freely using an open-source development model. You needn't inform anyone that you're using DOC software in your software, though we encourage you to let us¹⁰ know so we can promote your project in the DOC software success stories¹¹.

DOC software is provided as is with no warranties of any kind, including the warranties of design, merchantability, and fitness for a particular purpose, noninfringement, or arising from a course of dealing, usage or trade practice. Moreover, DOC software is provided with no support and without any obligation on the part of Washington University, UC Irvine, Vanderbilt University, their employees, or students to assist in its use, correction, modification, or enhancement. A number of companies¹² around the world provide commercial support for DOC software, however. DOC software is Y2K-compliant, as long as the underlying OS platform is Y2K-compliant.

Washington University, UC Irvine, Vanderbilt University, their employees, and students shall have no liability with respect to the infringement of copyrights, trade secrets or any patents by DOC software or any part thereof. Moreover, in no event will Washington University, UC Irvine, or Vanderbilt University, their employees, or students be liable for any lost revenue or profits or other special, indirect and consequential damages.

The ACE¹³, TAO¹⁴, CIAO¹⁵, and CoSMIC¹⁶ web sites are maintained by the DOC Group¹⁷ at the Institute for Software Integrated Systems (ISIS)¹⁸ and the Center for Distributed Object Computing of Washington University, St. Louis¹⁹ for the development of open-source software as part of the open-source software community²⁰. By submitting comments, suggestions, code, code snippets, techniques (including that of usage), and algorithms, submitters acknowledge that they have the right to do so, that any such submissions are given freely and unreservedly, and that they waive any claims to copyright or ownership. In addition, submitters acknowledge that any such submission might become part of the copyright maintained on the overall body of code, which comprises the DOC software. By making a submission, submitter agree to these terms. Furthermore, submitters acknowledge that the incorporation or modification of such submissions is entirely at the discretion of the moderators of the open-source DOC software projects or their designees.

The names ACE, TAO, CIAO, CoSMIC, Washington University, UC Irvine, and Vanderbilt University, may not be used to endorse or promote products or services derived from this source without express written permission from Washington

University, UC Irvine, or Vanderbilt University. Further, products or services derived from this source may not be called ACE, TAO, CIAO, or CoSMIC nor may the name Washington University, UC Irvine, or Vanderbilt University appear in their names, without express written permission from Washington University, UC Irvine, and Vanderbilt University.

If you have any suggestions, additions, comments, or questions, please let me²¹ know.

Douglas C. Schmidt²²

References

1. <http://www.cs.wustl.edu/~schmidt/ACE.html>
2. <http://www.cs.wustl.edu/~schmidt/TAO.html>
3. <http://www.dre.vanderbilt.edu/CIAO/>
4. <http://www.dre.vanderbilt.edu/cosmic/>
5. <http://www.dre.vanderbilt.edu/~schmidt/>
6. <http://www.cs.wustl.edu/~schmidt/ACE-members.html>
7. <http://www.wustl.edu/>
8. <http://www.uci.edu/>
9. <http://www.vanderbilt.edu/>
10. mailto:doc_group@cs.wustl.edu
11. <http://www.cs.wustl.edu/~schmidt/ACE-users.html>
12. <http://www.cs.wustl.edu/~schmidt/TAO.html>
13. <http://www.cs.wustl.edu/~schmidt/ACE.html>
14. <http://www.cs.wustl.edu/~schmidt/TAO.html>
15. <http://www.dre.vanderbilt.edu/CIAO/>
16. <http://www.dre.vanderbilt.edu/cosmic/>
17. <http://www.dre.vanderbilt.edu>
18. <http://www.isis.vanderbilt.edu/>
19. <http://www.cs.wustl.edu/~schmidt/doc-center.html>
20. <http://www.opensource.org/>
21. <mailto:d.schmidt@vanderbilt.edu>
22. <http://www.dre.vanderbilt.edu/~schmidt/>

iMatix SFL

This product uses parts of the iMatix SFL, Copyright © 1991-2000 iMatix Corporation <<http://www.imatix.com>>.