

# SOPHOS

## Sophos Control Center 4.1 升级指南

产品版本：4.1

文档日期：2011 年 4 月



# 目录

1 关于本指南.....	3
2 Sophos Control Center 4 中的新内容.....	3
3 系统要求.....	4
4 准备升级.....	5
5 升级 Sophos Control Center.....	6
6 检查计算机的保护状况.....	7
7 设置防火墙.....	7
8 设置应用程序控制.....	7
9 设置设备控制.....	8
10 技术支持.....	11
11 版权所有.....	11

## 1 关于本指南

本 Sophos Control Center 4.1 升级指南将说明怎样：

- 从 Sophos Control Center 版本 2.0/ 2.5 升级到 Sophos Control Center 版本 4.1。
- 从 Sophos Anti-Virus 和 Sophos Client Firewall（如果您的用户授权使用许可协议中包括防火墙产品）升级到 Sophos Endpoint Security and Control。

如果您使用先前版本的 Sophos PureMessage，并且您的用户授权使用许可协议包括升级到最版的 Sophos PureMessage，要了解怎样升级，请参见 *Sophos PureMessage Upgrade Guide*。

- 设置新的安全功能。

在 *Sophos Control Center* 帮助文件中，您可以找到本指南中没有提及的，Sophos Control Center 的所有其它配置选项的详情。

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

## 2 Sophos Control Center 4 中的新内容

新版的 Sophos Control Center 具有以下重要功能：

### Sophos Control Center 4.1

#### 操作系统兼容性

Sophos Control Center 4.1 只与以下操作系统兼容：

- Windows Server 2008 R2，
- Windows 7。

**注：**Sophos Control Center 4.0 与更早的 Windows 操作系统兼容。有关完整的系统要求的信息，请参见以下章节，[系统要求](#)（第4页）。

### Sophos Control Center 4.0

#### 支持最新的终结点安全软件

新版本的 Sophos Control Center 使您能够使用 Sophos Endpoint Security and Control 为终结点计算机提供 Windows 2000 及以后的最新版的防病毒和防火墙软件。

#### 指标面板

Sophos Control Center 界面现在可以使用指标面板，使您能够获得网络安全状态的“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。要了解怎样配置指标面板的信息，请参见 Sophos Control Center 帮助文件。

### 应用程序控制

Sophos Control Center 使您能够检测和阻断您认为不适合在办公环境中使用的应用程序。要了解更多有关应用程序控制的信息，请参见 [设置应用程序控制](#)（第7页）。

### 设备控制

设备控制可以使您防止用户在他们的计算机上，使用未经授权的外部硬件设备，移动存储介质，以及无线连接技术。要了解更多有关设备控制的信息，请参见 [设置设备控制](#)（第8页）。

### 启动 Sophos PureMessage 和 Sophos for Microsoft SharePoint

如果 Sophos PureMessage 或 Sophos for Microsoft SharePoint 控制台安装在 Sophos Control Center 所在的计算机上，那么，您可以从 Sophos Control Center 控制台启动它们。

## 3 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。

## 4 准备升级

注:

- 建议您在升级之前，备份现有版本的 Sophos Control Center。
- 在完成 Sophos Control Center 安装向导之后，您需要从您升级 Sophos Control Center 的计算机上注销，然后再重新登录，或者，您需要重新计算机。
- 如果您选择安装 Sophos Client Firewall（如果您的用户授权使用许可协议中包括它），您必须重新启动每一台您已经安装了防火墙的计算机，以激活防火墙。

在先前版本的 Sophos Control Center 中生成防火墙警报无法在您升级到 Sophos Control Center 4.0 之后使用。Sophos 建议在升级之前，处置所有的防火墙警报。

### 4.1 前提条件

在您升级 Sophos Control Center，接着将软件升级到它所管理的网络中的计算机上之前，请确保您满足了以下条件：

- 您已经满足在 [系统要求](#)（第4页）中所列的所有硬件和软件要求。
- 您应该以系统管理员的身份登录到您将要升级 Sophos Control Center 的计算机上。

为 **Windows** 操作系统的终结点计算机做好准备。

对于 Windows 操作系统的终结点计算机，您必须做到：

- 禁用所有 Windows XP 计算机上的简单文件共享。

要了解怎样做到这一点，请参见

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

- 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。

为您不想安装 **Sophos Client Firewall** 的终结点计算机做准备。

如果您有 Windows XP SP 2 工作站计算机，或者，Windows Server 2003 SP1 计算机，而您不想在这些计算机上安装 Sophos Client Firewall，并且，在这些计算机上 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。

要了解怎样做到这一点，请参见

<http://cn.sophos.com/support/knowledgebase/article/11738.html>。

- 确保开启了TCP 端口 8192，8193 以及 8194。
- 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>。

- 重新启动计算机，以使更改生效。

## 5 升级 Sophos Control Center

要升级 Sophos Control Center 保留您的设置，在安装了先前版本的 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，并按照以下说明做：

1. 如果有开启的 Sophos 应用程序，请全部关闭它们。
2. 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 Control Center 安装程序，然后，运行它。

3. 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**。
4. 在 **欢迎** 页面中，单击 **下一步**。

安装程序向导会指导您完成安装过程。接受默认选项。

5. 当升级结束后，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。

在 Sophos Control Center 的安装完成之后，终结点计算机会在新的终结点软件版本下载完毕时，立即进行自动更新。

**注：**在 Windows 98，以及 Mac OS X 操作系统的终结点计算机上，您只能手动升级 Sophos Anti-Virus。要了解更多有关手动保护计算机的信息，请参见 *Sophos Control Center 安装指南*。

## 6 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。

## 7 设置防火墙

当您首次安装 *Sophos Client Firewall* 时，它会被配置为允许所有通讯流。您可以配置它仅按照要求允许或阻断通讯流。

如果您是首次设置防火墙，要了解怎样配置防火墙的信息，请参见 *Sophos Control Center* 帮助文件。

**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。

## 8 设置应用程序控制

*Sophos Control Center* 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：** 此选项只应用于 *Sophos Endpoint Security and Control for Windows 2000* 及以后。

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* 技术支持知识库文章 35330 (<http://www.sophos.com/support/knowledgebase/article/35330.html>)。

要了解有关应用程序控制事件的信息，请参见 *Sophos Control Center* 帮助文件。

### 8.1 设置应用程序控制

您可以配置 *Sophos Control Center* 读写扫描您想在网络中控制的应用程序。

1. 在左手边的窗格板的 **配置** 下，单击 **配置应用程序控制**。  
会出现 **配置应用程序控制** 对话框。
2. 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：**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）。
3. 单击 **批准** 标签，并选择您想要控制的应用程序。  
要了解更多信息怎样选择应用程序的信息，请参见 [选择要控制的应用程序](#)（第 8 页）。

## 8.2 选择要控制的应用程序

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

1. 在左手边的窗格板的 **配置** 下，单击 **配置应用程序控制**。
2. 在 **配置应用程序控制** 对话框，单击 **批准** 标签页。
3. 选择 **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 **已批准** 列表中。
  - 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。



要了解怎样卸载受控程序的信息，请参见 Sophos Control Center 帮助文件。

## 9 设置设备控制

**重要：**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。

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，Sophos 建议您：

- 选择要控制的设备类型。
- 检测但不阻断它们。
- 设置设备控制警报。
- 检测并阻断设备，或者，允许只读访问存储设备。

要了解有关设备控制事件的信息，请参见 Sophos Control Center 帮助文件。

## 9.1 可以控制哪些类型的设备

设备控制可以使您阻断三种类型的设备：存储，网络，以及短距 (*short range*)。

### 存储

- 可移动存储设备（如：USB 闪存，PC 读卡器，以及外置硬盘）
- 光盘驱动器（CD-ROM/DVD/Blu-ray 驱动器）
- 软盘驱动器
- 安全的可移动存储设备（例如，SanDisk Cruzer Enterprise，SanDisk Cruzer Enterprise FIPS Edition，Kingston Data Traveler Vault - Privacy Edition，Kingston Data Traveler BlackBox，以及具有硬件加密的 IronKey Enterprise Basic Edition USB 闪存）

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。要了解最新的受到支持的安全的可移动存储设备列表，请访问 Sophos 网站 ([www.sophos.com](http://www.sophos.com))。

### 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，您可以为“阻断桥接”模式设置附加的访问级别。当计算机与物理网络断开连接时，它会启用网络设备（如：Wi-Fi 适配器）。在为网络设备设置访问级别时，可以选择“阻断桥接”选项。

**注：**“阻断桥接”模式可以避免网络桥接，例如，在公司网络和非公司网络之间。此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。

### 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，阻断蓝牙接口将会阻断：

- 计算机中内建的蓝牙接口和
- 任何通过 USB 接入计算机的蓝牙适配器。

## 9.2 设置设备控制

您可以配置 Sophos Control Center 读写扫描您想在网络中控制的设备。

1. 在左手边的窗格板的 **配置** 下，单击 **配置设备控制**。

**设备控制策略** 对话框。

2. 在 **配置** 标签中，按照以下说明设置选项：

- 要启用设备控制，请勾选 **启用设备控制扫描** 勾选框。如果您只想要检测设备，但是不想阻断它们，请勾选 **检测但不阻断设备** 勾选框。
- 要为每个类型的设备设置访问级别，请单击设备类型旁的 **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”。

要了解有关怎样设置设备控制警报的信息，请参见 Sophos Control Center 帮助文件。

## 9.3 免除设备

您可以从设备控制策略中免除某个设备。

您可以免除设备实体（“仅限此设备”）或者，免除设备型号（“此型号的所有设备”）。不要同时设置免除型号和设备实体。如果同时定义了两者，那么，设备实体的设置将优先。

要免除设备：

1. 在 **查看** 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。
3. 选择您想要免除的设备条目，然后，单击 **免除设备**。  
会出现 **免除设备** 对话框。在 **设备详情** 中，您可以看到设备类型，型号，和 ID。

## 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](mailto: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](mailto: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™**

ACE<sup>1</sup>, TAO<sup>2</sup>, CIAO<sup>3</sup>, and CoSMIC<sup>4</sup> (henceforth referred to as “DOC software” ) are copyrighted by Douglas C. Schmidt<sup>5</sup> and his research group<sup>6</sup> at Washington University<sup>7</sup>, University of California<sup>8</sup>, Irvine, and Vanderbilt University<sup>9</sup>, 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 us<sup>10</sup> know so we can promote your project in the DOC software success stories<sup>11</sup>.

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 companies<sup>12</sup> 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 ACE<sup>13</sup>, TAO<sup>14</sup>, CIAO<sup>15</sup>, and CoSMIC<sup>16</sup> web sites are maintained by the DOC Group<sup>17</sup> at the Institute for Software Integrated Systems (ISIS)<sup>18</sup> and the Center for Distributed Object Computing of Washington University, St. Louis<sup>19</sup> for the development of open-source software as part of the open-source software community<sup>20</sup>. 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 me<sup>21</sup> know.

Douglas C. Schmidt<sup>22</sup>

## 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](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/>