

Sophos Endpoint Security and Control 9.5 快速安装指南

文档日期: 2010年6月



目录

1	关于本指南3
2	安装什么?
3	哪些主要步骤?
4	检查系统要求4
5	做好安装准备5
6	下载安装程序
7	安装 Enterprise Console6
8	下载安全软件7
9	安装 NAC Manager7
10	创建计算机组
11	设置安全策略
12	查找计算机9
13	保护计算机9
14	检查网络的健康状况11
15	排疑解难12
16	就通常的任务获得帮助12
17	技术支持13
18	法律声明13

1 关于本指南

本指南将告诉您怎样使用 Sophos 安全软件保护您的网络。

如果您是首次安装 Sophos 软件,请阅读本指南。

如果您在进行升级,请转到 *http://cn.sophos.com/support/upgrades*/ 中的 **Endpoint** Security and Control 9.5 Upgrade Center 。

注: 如果您具有大型的网络,您可能会考虑 Sophos Endpoint Security and Control 高级安装指南中说明的各种安装选项。

2 安装什么?

您将安装两个管理工具:

- Sophos Enterprise Console。它使您能够在计算机上安装和管理安全软件。
- Sophos NAC Manager。它使您能够使用 "网络访问控制", 防止未经授权的计算机,或者,没有遵照您的安全标准的计算机,访问您的网络。

安装 NAC Manager 是选项。

注: 您将使用不同的安装程序, 分别安装这两种工具。

注:您可以在同一台服务器上同时安装这两种工具。不过,如果您拥有超过 1,000的计算机,那么,您应该将这两种工具安装到不同的服务器上。安装的 过程是相同的。

3 哪些主要步骤?

您要进行这些主要步骤:

- 检查系统要求。
- 做好安装准备。
- 下载安装程序。
- 安装 Enterprise Console。
- 下载安全软件
- 安装 NAC Manager。
- 创建计算机组

- 设置安全策略
- 查找计算机。
- 保护计算机。
- 检查网络的健康状况。

4 检查系统要求

在开始安装之前,请检查硬件,操作系统,以及系统软件是否符合要求。

4.1 硬件和操作系统

系统要求取决于您将安装的工具。

以下所显示的是建议的要求。这些要求假定管理工具都安装在一台服务器上, 并且网络中的计算机不超过1,000台。

所有情况都要求能够访问因特网。

注: 这里的要求只列示服务器版的操作系统。如果您需要了解详细的要求,请访问 *http://cn.sophos.com/products/all-sysreqs.html*。

仅限 Enterprise Console

处理器	磁盘空间	内存	操作系统
2 GHz Pentium 或同等处理能力	最多2GB数据 库	512 MB	Windows Server 2008 R2 Windows Server 2008 (32 or 64 bit) Windows Server 2008 Hyper-V Windows Server 2003 R2 Windows Server 2003 SP1+ (32 位或 64 位) VMWAre ESX 3.0/3.5 VMWare Workstation 6.5

Enterprise Console 和 NAC Manager

处理器	磁盘空间	内存	操作系统
2 GHz Pentium 或同等处理能力	至多3GB供 数据库使用	1 GB	Windows Server 2008 R2 Windows Server 2008 (32 位或 62 位) Windows Server 2003 R2 Windows Server 2003 SP1+ (32 位或 64 位)

4.2 Microsoft 系统软件

必须安装以下 Microsoft 系统软件,以便能够运行 Enterprise Console 安装程序:

- Microsoft Windows Installer 4.5 按照 KB958655 更新补丁
- Security Update for Microsoft XML Core Services 6.0
- Microsoft .NET Framework 3.5 SP1
- Microsoft SQL Server 2005 Express

如果您没有这些(或更高)的版本的 Microsoft 系统软件, Enterprise Console 安装程序将会为您安装它们。

注:

安装程序将安装 SQL Server 2008 Express,除非您已经安装了 SQL Server 2005 Express 或以后。SQL Server 2008 Express 与 Windows Server 2003 SP1 或 Windows Essential Business Server 2008 不兼容。

安装程序不能安装 .NET Framework 3.5 到运行 Windows Server 2008 R2 的计算 机上。您必须从 Server Manager 的 Features 部分中添加它。

在安装了所要求的系统软件之后,您需要重新启动计算机。要了解更多有关计 算机重新启动要求的信息,请参见 Sophos 技术支持库文章 65190 (http://cn.sophos.com/support/knowledgebase/article/65190.html)。

5 做好安装准备

转到符合系统要求的服务器上,并且按照下面的说明做好准备:

- 确保已连接到了因特网中。
- 确保您准备了 Windows 操作系统 CD,及其全部的 Service Pack CD。在安装的过程中,您可能会被提示使用它们。

- 如果您具有的 Microsoft SQL Server 2000/MSDE 2000 的数据库实例不是 "SOPHOS", 那么,请将它升级到 Microsoft SQL Server 2005。
- 如果该服务器上运行的是 Windows Server 2008 或以后,那么,请关闭"用 户帐户控制 (UAC)",并重新启动该服务器。

注: 在完成了安装,并且下载了安全软件之后,您可以重新开启 UAC。

6 下载安装程序

将 Sophos 安装程序下载到您想要安装管理工具的那台服务器上。

- 1. 转到 http://cn.sophos.com/support/updates/。
- 2. 输入您的 MySophos 用户名和密码。
- 3. 在下载 Endpoint Security and Data Protection 的网页中,您应该:
 - 下载 Enterprise Console 安装程序。
 - 如果您想要使用 NAC Manager,请下载 Sophos NAC 安装程序。

如果您想要将 NAC Manager 安装到与 Enterprise Console 所在的服务器不同 的服务器上,那么,您应该将安装程序下载到那台不同的服务器上。

7 安装 Enterprise Console

要安装 Enterprise Console:

- 1. 以管理员身份登录:
 - 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。
- 2. 找到您先前下载的 Enterprise Console 安装程序。

提示:该安装程序的文件名中包括 "sec" 字样。

- 3. 双击该安装程序文件。
- 4. 在 Sophos Endpoint Security and Control 9.5 network installer 对话框中,单击 Install。

安装文件会被复制到计算机上,并且安装向导会启动。

5. 在 Sophos Enterprise Console 对话框中,单击下一步。

6. 会出现一个向导指导您完成安装过程。您按照以下说明做:

a) 尽量接受默认值。

b) 选择 **完整** 安装。

7. 当安装完成后,会提示您重新启动计算机。单击确定或完成。

8 下载安全软件

在您首次安装之后,重新注销再登录(或重新启动)之后,Enterprise Console 会自动开启,并且会有一个向导出现。

注: 如果您使用了 Remote Desktop 进行安装,则控制台不会自动开启。请从 "开始"菜单打开它。

该向导将指导您选择和下载安全软件。您按照以下说明做:

- 在 Sophos 下载帐户详情页面中,输入在您的用户授权使用许可协议的条款 中提供的用户名和密码。如果您是通过代理服务器访问因特网的,请勾选 通过代理服务器访问 Sophos 勾选框。
- 2. 在操作平台选择页面中,只勾选您当前需要保护的操作平台。

在您单击下一步后, Enterprise Console 会开始下载您的软件。

- 3. 在 正在下载软件 页面中, 会出现下载进程。随时单击 下一步。
- 4. 在 从 Active Directory 导入计算机 页面中,如果您想要 Enterprise Console 使 用您现有的 Active Directory 计算机组,请勾选 为计算机设置组。

如果您在安装之前关闭了"用户帐户控制",您现在可以重新开启它。

9 安装 NAC Manager

确保您准备了 Windows 操作系统 CD,及其全部的 Service Pack CD。在安装的 过程中,您可能会被提示使用它们。

注: 如果您要从 NAC Manager 安装 Enterprise Console 到不同的服务器上,那 么,您必须首先手动安装 SQL Server 2005 或以后版本的数据。

- 1. 以管理员身份登录。
 - 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。

2. 找到您先前下载的 Sophos NAC 安装程序。

提示:该安装程序的文件名中包括 "nac" 字样。

- 3. 双击该安装程序文件。
- 4. 在 Sophos NAC Manager 对话框中,单击 安装。
- 5. 会出现一个向导指导您完成安装过程。

10 创建计算机组

如果您使用了**下载安全软件向导**设置您的计算机组(基于您的Active Directory 组),那么,可以跳过本节。转到设置安全策略(第8页)。

在您能够保护和管理计算机之前,您需要为它们创建组。

- 1. 如果 Enterprise Console 尚未开启,请开启它。
- 在 组 窗格板(位于控制台的左手边)中,确保勾选了在上方显示的服务器 的名称。
- 3. 在工具栏中,单击 创建组 图标。

在列表中会添加一个"新组",组名会高亮显示。

4. 请为该组输入一个名称。

要进一步创建组,请到左手边的窗格板中。如果您要创建另一个第一级的组, 请选择在第一级所显示的服务器。如果您要在某个组中创建次组,请选择该 组。然后,创建并命名该组,方法同前。

11 设置安全策略

Enterprise Console 会应用"默认的"安全策略到您的计算机组中。如果您不想更改这些策略,您完全可以不更改它们,除非:

- 您现在必须设置防火墙策略。
- 如果您想要使用这些功能,您必须编辑网络访问控制,应用程序控制,数据 控制,或设备控制策略。您可以随时进行上述任务。

11.1 设置防火墙策略

注: 在安装防火墙期间,网络适配器会暂时断开连接。这种情况会导致联网的 应用程序,如:远程桌面等,断开连接。 依照默认值,防火墙将阻断所有可有可无的连接。因此您必须在保护计算机之前,配置防火墙。

- 1. 在策略窗格板中,双击防火墙。
- 2. 双击 默认策略 以编辑它。会出现一个向导。
- 3. 在 防火墙策略向导 中, 我们建议您作出以下选择。
 - a) 在 配置防火墙 页面中,选择 单一路径,除非您想要防火墙根据您使用它的路径来使用不同的设置。
 - b) 在 操作模式 页面中,选择 选择 阻断流入的通讯流,并允许流出的通讯 流。
 - c) 在 文件和打印共享 页面中,选择 允许文件和打印共享。

12 查找计算机

在 Enterprise Console 能够保护和管理计算机之前,您必须先在网络中搜索到这些计算机。

- 1. 在工具栏上,单击查找新计算机图标。
- 2. 选择您想要查找计算机的方式。
- 3. 请输入帐户详情,并在必要时指定您想在何处查找。

如果您使用查找选项之一,那么,计算机会被放置到未指派文件夹中。

13 保护计算机

要保护计算机,您需要:

- 准备计算机
- 自动保护 Windows 计算机。
- 手动保护 Windows 或 Mac OS X 计算机。

13.1 保护计算机的准备

在您保护计算机之前,请按照以下说明做:

删除第三方软件的准备

如果您想要 Sophos 安装程序删除任何先前安装的安全软件,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。

如果计算机使用的是其它软件商的更新工具,您可能想要删除它。请参见 EnterpriseConsole帮助文件中,"保护计算机"一节中的"删除第三方软件"。

检查您是否具有可以用于安装软件的帐户

您会被提示输入帐户的详情,以便用于安装安全软件。该帐户通常会是一个域 系统管理员帐户。它必须:

- 拥有您要保护的计算机的本地管理员权限。
- 能够登录到您安装了 Enterprise Console 的计算机上。
- 能够读访问计算机将要从中进行更新的那个路径。要查看该路径,请在 策略 窗格板中,双击 更新,然后,双击 默认值。

安装网络访问控制的准备

在安装网络访问控制到计算机上时,您必须:

■ 指定您安装了 NAC Manager 的计算机所在的 URL 地址。在 Enterprise Console 中,选择 工具 > 配置 NAC URL.

13.2 自动保护 Windows 计算机

要保护计算机,请按照以下说明做。

- 1. 选择您想要保护的计算机。
- 2. 单击鼠标右键,并选择保护计算机。

注:如果计算机在未指派组中,只需简单地将其拖放您所选择的组中。

- 3. 会有一个向导, 指导您完成安装 Sophos 的安全软件。您按照以下说明做:
 - a) 在 选择功能 页面中,您可以安装可选的功能。如果您想使用网络访问控制,请选择 Compliance Control。
 - b) 在保护摘要页面中,检查是否存在任何安装问题。需要帮助,请参见排 疑解难(第12页)。
 - c) 在 认证资料 页面中, 输入能够用于安装软件的帐户的详情。

由于安装是交错进行的,所以在所有计算机上完成安装过程,需要有一段时间。

在安装结束后,请再次查看计算机列表。在 **读写扫描** 栏中, "**活动中"**的字 样,表明该计算机正在运行病毒读写扫描。

13.3 手动保护 Windows 或 Mac OS X 计算机

如果您具有无法自动保护的计算机,那么,您可以通过从某个中央安装目录运 行某些安装程序的方法,来保护这些计算机。

要找到这些安装程序所在的中央安装目录,请开启 Enterprise Console 并选择 查看 > 引导路径。

- 1. 到各计算机上以本地管理员权限登录。
- 2. 在中央安装目录中找到安装文件,然后双击它。
 - 对 Windows 操作系统而言,这些程序是 setup.exe 文件。
 - 对 Mac OS X 操作系统而言,这些程序是 Sophos Anti-Virus.mpkg 文件。
- 3. 会出现一个向导指导您完成安装过程。

14 检查网络的健康状况

要从 Enterprise Console 检查网络的健康状况,请按照以下说明做。

- 在菜单栏中,单击指标面板图标(如果指标面板未显示)。 指标面板中向您显示,有多少计算机:
 - 检测到了安全隐患。
 - 未及时更新。
 - 未遵照策略。

- 2. 如果您使用 NAC, 您还可以:
 - a) 选择 File > Open > NAC。
 - b) 在 NAC Manager 中,选择 报告 > 遵照。
 - 这将向您显示计算机是否遵照了 NAC。

15 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:

- 在某操作系统的计算机中无法进行自动安装。执行手动安装。请参见手动保护 Windows 或 Mac OS X 计算机(第11页).要了解其它操作系统的信息,请参见 Sophos Endpoint Security and Control 高级安装指南。
- 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。
- 此计算机上正在运行防火墙。

16 就通常的任务获得帮助

本节将告诉您,在那里可以找到有关怎样完成通常的任务的信息。

SESC = Sophos Endpoint Security and Control

任务	文档
保护 Linux 计算机	SESC 9.5 安装指南 供 Linux, NetWare 和 UNIX 使用: "保护 Linux 计算机"
保护独立用户 (standalone) 计算机	SESC 9.5 高级安装指南: "保护独立用户 (standalone)的计算机"
配置防病毒和 HIPS	Enterprise Console帮助文件: "配置防病毒和 HIPS 策略"
配置应用程序控制	Enterprise Console 帮助文件: "配置应用程序控制 策略"
配置数据控制	Enterprise Console 帮助文件: "配置数据控制策略"

任务	文档
配置设备控制	Enterprise Console 帮助文件: "配置设备控制策略"
配置介入防范	Enterprise Console 帮助文件: "配置介入防范策略"
配置 NAC	NAC Manager 帮助文件: "管理概览"
使来宾用户能够访问网络	Sophos Compliance Agent 配置指南: "Dissolvable agent"
处置警报	Enterprise Console帮助文件: "处置警报和错误"
清除计算机	Enterprise Console 帮助文件: "清除计算机"
生成 SEC 报告	Enterprise Console 帮助文件: "生成报告"
生成 NAC 报告	NAC Manager 帮助文件: "报告概览"

17 技术支持

要获得此 Beta 发布的技术支持:

- 请(通过 Sophos 寄发给您的提供下载指导说明的电子邮件),访问您专用 的在线反馈表,填写完成相关的详情,然后,将表格直接提交给我们的技术 支持团队。
- 2. 请(通过 Sophos 寄发给您的提供下载指导说明的电子邮件),访问 Sophos Beta 论坛,并搜索遇到相同问题的其它 Beta 用户。
- 3. 如果您在进行上述操作时,遇到任何问题,请发送电子邮件至: betaprogram@sophos.com 我们的 Beta 团队的成员将会与您联系。

18 法律声明

版权所有 © 2010 Sophos Group。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 Plc and Sophos Group 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://cn.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*