System Center

Endpoint Protection 适用于 Mac

安装手册和用户指南

Microsoft

目录

System Center Endpoint Protection

随着基于 Unix 的操作系统越来越受欢迎，恶意软件作者正在开发针对 Mac 用户的威胁。System Center Endpoint Protection 提供对这些新兴威胁的强大而高效的防护。System Center Endpoint Protection 具有阻止 Windows 威胁的能力，从而在 Mac 用户与 Windows 用户交互（反之亦然）时保护他们。虽然 Windows 恶意软件不会导致对 Mac 的直接威胁，但禁用已感染 Mac 计算机的恶意软件将阻止它通过本地网络或 Internet 扩散到基于 Windows 的计算机。

系统要求

要使 System Center Endpoint Protection 实现最佳性能，系统应满足以下硬件和软件要求：

System Center Endpoint Protection:

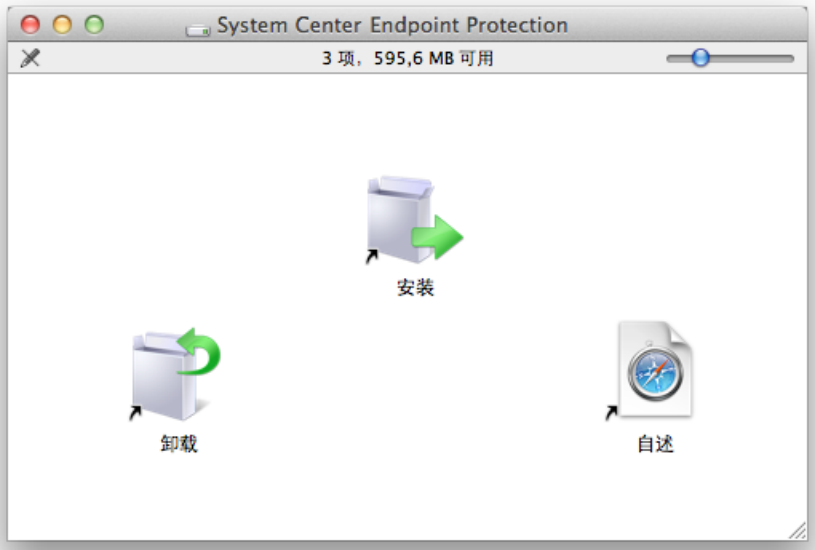
	系统要求
处理器结构	32 位、64 位 Intel
操作系统	Mac OS X 10.6 及更高版本
内存	512 MB
可用磁盘空间	100 MB

安装

在开始安装过程之前，请关闭计算机上所有打开的程序。System Center Endpoint Protection 包含可能会与您的计算机上已安装的其他病毒防护程序相冲突的组件。强烈建议移除任何其他病毒防护程序以避免潜在问题。您可以从安装 CD/DVD 或从我们网站下载的文件来安装 System Center Endpoint Protection。

要启动安装向导，请执行以下其中一项操作：

- 如果从安装 CD/DVD 安装，请将光盘插入计算机中，从桌面或 Finder 窗口打开，然后双击**安装**图标。
- 如果从下载的文件安装，则打开下载的文件，然后双击**安装**图标。



启动安装程序，安装向导将引导您完成基本设置。在同意软件许可协议并阅读隐私声明后，您可以选择以下安装类型：

- 典型 4
- 自定义 4

典型安装

典型安装模式包括适合于大多数用户的配置选项。这些设置提供最高安全性和最出色的系统性能。典型安装是默认选项，如果您对特定设置没有特别要求，建议使用此选项。

选择**典型**安装模式后，配置**潜在不受欢迎应用程序的检测**。潜在不受欢迎的应用程序未必是恶意的，但可能对操作系统的运行产生不良影响。这些应用程序通常与其他程序捆绑在一起，在安装过程中不容易引起注意。虽然这些应用程序在安装过程中通常会显示通知，但它们无需您的同意即可轻易安装。

安装 System Center Endpoint Protection 后，您应扫描计算机中的恶意代码。在主程序窗口中，单击**计算机扫描**，然后单击**智能扫描**。有关手动计算机扫描的更多信息，请参见手动计算机扫描 10 部分。

自定义安装

自定义安装模式是为想要在安装过程中修改高级设置的有经验的用户设计的。

选择**自定义**安装模式后，系统将提示您配置**代理服务器**设置。如果使用代理服务器，可以通过选择**我使用代理服务器**选项定义其参数。在**地址**字段中输入代理服务器的 IP 地址或 URL。在端口字段中指定代理服务器接受连接的端口（默认情况下使用 3128 端口）。如果代理服务器要求验证，则输入有效的**用户名**和**密码**，才能访问代理服务器。如果确定没有使用代理服务器，则选择**我不使用代理服务器**选项。如果不确定，可以通过选择**使用系统设置（建议）**使用当前系统设置。

在下一步中，可以**定义授权用户**，这些用户能够编辑程序配置。从左侧的用户列表中，选择用户并将其**添加**至**授权用户**列表。要显示所有系统用户，则选择**显示所有用户**选项。

安装过程的下一步是配置**潜在不受欢迎的应用程序检测**。潜在不受欢迎的应用程序未必是恶意的，但可能对操作系统的运行产生不良影响。这些应用程序通常与其他程序捆绑在一起，在安装过程中不容易引起注意。虽然这些应用程序在安装过程中通常会显示通知，但它们无需您的同意即可轻易安装。

安装 System Center Endpoint Protection 后，您应扫描计算机中的恶意代码。在主程序窗口中，单击**计算机扫描**，然后单击**智能扫描**。有关手动计算机扫描的更多信息，请参见手动计算机扫描 10 部分。

卸载

如果要从计算机卸载 System Center Endpoint Protection，请执行以下操作之一：

- 将 System Center Endpoint Protection 安装 CD/DVD 插入计算机中，从桌面或 Finder 窗口打开，然后双击**卸载**图标，
- 打开 System Center Endpoint Protection 安装文件 (.dmg)，双击**卸载**图标，或
- 启动 Finder，打开硬盘驱动器上的**应用程序**文件夹，按住 ctrl 单击 System Center Endpoint Protection 图标，选择**显示程序包内容**选项。打开Contents > Helpers文件夹，双击Uninstaller图标。

入门指南

本章提供对 System Center Endpoint Protection 及其基本设置的初步概述。

用户界面

System Center Endpoint Protection 的主程序窗口分为两个主要部分。右侧的主窗口显示与左侧的主菜单中选定选项相关的信息。

以下是主菜单中选项的说明：

- **防护状态** - 提供有关 System Center Endpoint Protection 的防护状态的信息。如果**高级模式**被激活，则显示**统计**子菜单。
- **计算机扫描** - 此选项允许您配置和启动手动扫描计算机。
- **更新** - 显示有关病毒库更新的信息。
- **设置** - 选择此选项可调整计算机的安全等级。如果**高级模式**被激活，则显示**病毒和间谍软件防护**子菜单。
- **工具** - 提供对**日志文件**？**隔离**和**计划任务**的访问。此选项仅显示在**高级模式**中。
- **帮助** - 提供程序信息和对帮助文件的访问。

System Center Endpoint Protection 用户界面允许用户在 标准 和 高级 模式间切换。标准模式提供对一般操作所需功能的访问。不会显示任何高级选项。要在两种模式间切换，单击主程序窗口左下角**激活高级模式/激活标准模式**旁边的加号图标 (+) 或按 cmd+M。

切换到高级模式会在主菜单中添加**工具**选项。**工具**选项允许您访问**日志文件**？**隔离**和**计划任务**的子菜单。

注意： 本指南中的所有其他说明都将出现在**高级模式**中。

检查系统操作

要查看**防护状态**，请单击主菜单的顶部选项。有关 System Center Endpoint Protection 操作的状态摘要显示在主窗口和**统计**子菜单中。选择它以查看有关系统上已执行的计算机扫描的更详细信息和统计信息。 统计 窗口仅在高级模式下可用。

程序工作不正常时如何应对

如果启用的模块正常工作，则会带有一个绿色对号图标。如果工作不正常，则显示红色惊叹号或橙色通知图标，有关模块的其他信息显示在窗口的上半部分。同时还显示修复该模块的建议解决方案。要更改单个模块的状态，请在主菜单中单击**设置**，然后单击所需模块。

使用 System Center Endpoint Protection

病毒和间谍软件防护

病毒防护通过修改可能导致潜在威胁的文件防止恶意系统攻击。如果检测到带有恶意代码的威胁，则病毒防护模块可以通过阻止它，然后将其清除、删除或移至隔离区，来消除威胁。

实时文件系统防护

文件系统实时防护控制系统中所有与病毒防护相关的事件。在计算机上打开、创建或运行任何文件时，都将扫描该文件是否带有恶意代码。文件系统实时防护在系统启动时启动。

实时防护设置

文件系统实时防护检查所有类型的介质，并根据各种事件触发扫描。文件系统实时防护对新创建的文件和现有文件区别对待。对于新创建的文件，可以应用更深的控制级别。

默认情况下，实时防护在系统启动时启动，并提供不间断的扫描。特殊情况下（例如，如果与其他实时扫描程序冲突），可通过单击位于菜单栏（屏幕顶部）中的 System Center Endpoint Protection 图标，然后选择**禁用文件系统实时防护**选项来终止实时防护。还可以从主程序窗口（**设置** > **病毒和间谍软件防护** > **禁用**）终止实时防护。

要修改实时防护的高级设置，请转至**设置** > **进入应用程序首选项...**> **防护** > **实时防护**并单击**设置...**按钮，该按钮位于**高级选项**（在标题为高级扫描选项 8的部分中有描述）的旁边。

运行扫描于（事件触发式扫描）

默认情况下，所有文件都会在**文件打开**？**文件创建**或**文件执行**时扫描。建议您保留默认设置，因为默认设置可为计算机提供最高级别的实时防护。

高级扫描选项

在此窗口中，可以定义要由扫描引擎扫描的对象类型、启用/禁用**高级启发式扫描**以及修改压缩文件和文件缓存的设置。

不建议更改在**默认压缩文件设置**部分中的默认值，除非需要解决特定问题，因为较高的压缩嵌套值可能阻碍系统性能。

通过在每个相应的引擎参数部分单击**高级启发式扫描**复选框，可以分别切换已执行文件、已创建文件和已修改文件的高级启发式扫描。

为了在使用实时防护时提供最小的系统占用空间，可以定义优化缓存的大小。当您使用**启用清除文件缓存**选项时，此行为处于活动状态。如果禁用，则在每次访问文件时都扫描该文件。文件缓存达到已定义的缓存大小之后不会重复扫描这些文件（除非它们已被修改）。每次病毒库更新后立刻重新扫描文件。

单击**启用清除文件缓存**来启用/禁用此功能。要设置要缓存的文件量，只要在**缓存大小**旁边的输入字段中输入想要的值即可。

其他扫描参数可以在**引擎设置**窗口中设置。您可以为文件系统实时防护定义应扫描哪种类型的**对象**、使用哪些**选项**和**清除**级别，以及定义**扩展名**和文件大小**限制**。您可以通过在 高级设置 窗口中单击**引擎**旁边的**设置...**按钮，进入引擎设置窗口。有关引擎参数的更多详细信息，请参见引擎参数设置 12。

扫描排除项

本节提供如何将特定文件和文件夹排除在扫描之外的信息。

- **路径** - 被排除文件和文件夹的路径
- **威胁** - 如果已排除文件旁有一个威胁的名称，则表示该文件仅对给定威胁排除，并不是全部排除。因此，如果该文件稍后被其他恶意软件感染，病毒防护模块将会检测到。
- **添加...** - 选择不予检测的对象。输入对象的路径（也可以使用通配符 * 和 ?）或从树结构选择文件夹或文件。
- **编辑...** - 使您能够编辑选择的条目
- **删除** - 除去选择的条目
- **默认** - 取消所有排除项。

何时修改实时防护配置

实时防护是维护系统安全的最重要的组件。修改实时防护参数时要小心。建议您仅在特定情况下修改这些参数。例如，与某个应用程序或另一个病毒防护程序的实时扫描程序发生冲突时。

安装 System Center Endpoint Protection 后，所有设置都会得到优化以便为用户提供最高级别的系统安全性。要恢复默认设置，请单击**默认**按钮，它位于**实时防护**窗口（**设置** > **进入应用程序首选项...**> **防护** > **实时防护**）的左下角。

检查实时防护

要验证实时防护是否工作，是否在检测病毒，请使用测试文件 eicar.com。此文件是一个可供所有病毒防护程序检测的特殊无害文件。此文件由 EICAR 协会（欧洲计算机病毒防护研究协会）创建，用于测试病毒防护程序的功能。

要远程检查实时防护的状态，请使用**终端**连接到客户端计算机并执行以下命令：
`/Applications/.scep/Contents/MacOS/scep_daemon --status`

实时扫描程序的状态将显示为 `RTPStatus=Enabled` 或 `RTPStatus=Disabled`。

终端 BASH 的输出还包含以下状态：

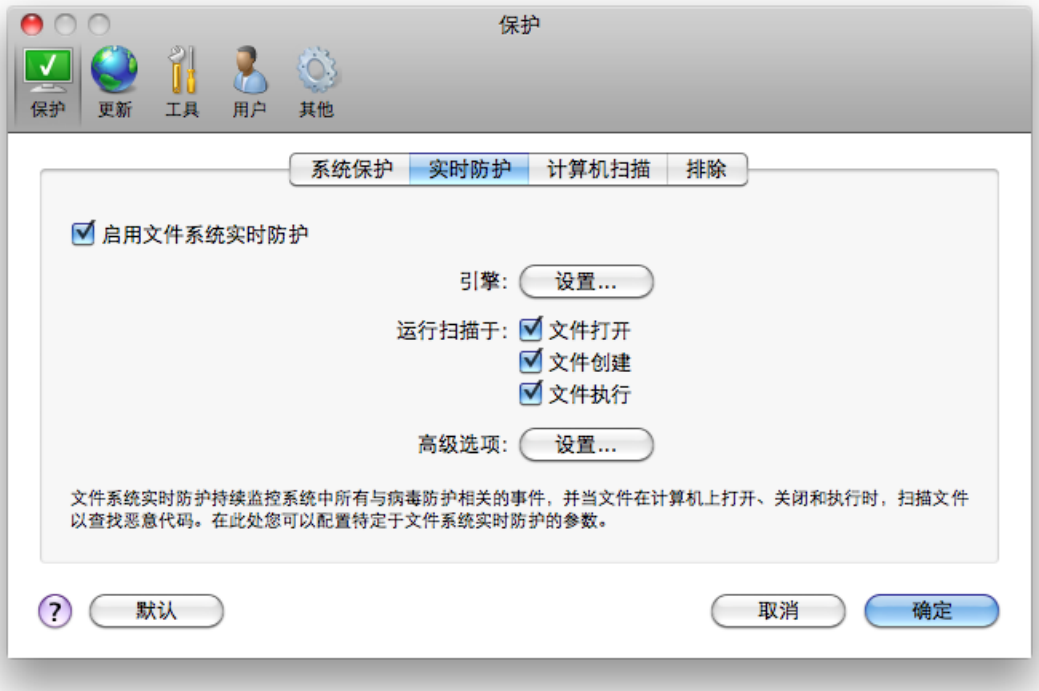
- 客户端计算机上安装的 System Center Endpoint Protection 版本
- 病毒库的日期和版本
- 更新服务器的路径

注意： 仅推荐高级用户使用 终端 ”。

实时防护不工作时如何应对

在本章中，我们将介绍使用实时防护时可能出现的问题场景，以及如何排除这些故障。

实时防护被禁用
如果用户无意中禁用了实时防护，则需要重新启用它。要重新启用实时防护，请浏览至**设置** > **病毒和间谍软件防护**并在主程序窗口中（在右侧）单击**启用文件系统实时防护**链接。或者，您可以在**防护** > **实时防护**下的 高级设置 窗口中，选择**启用文件系统实时防护**选项，来启用文件系统实时防护。



实时防护功能不检测和清除威胁

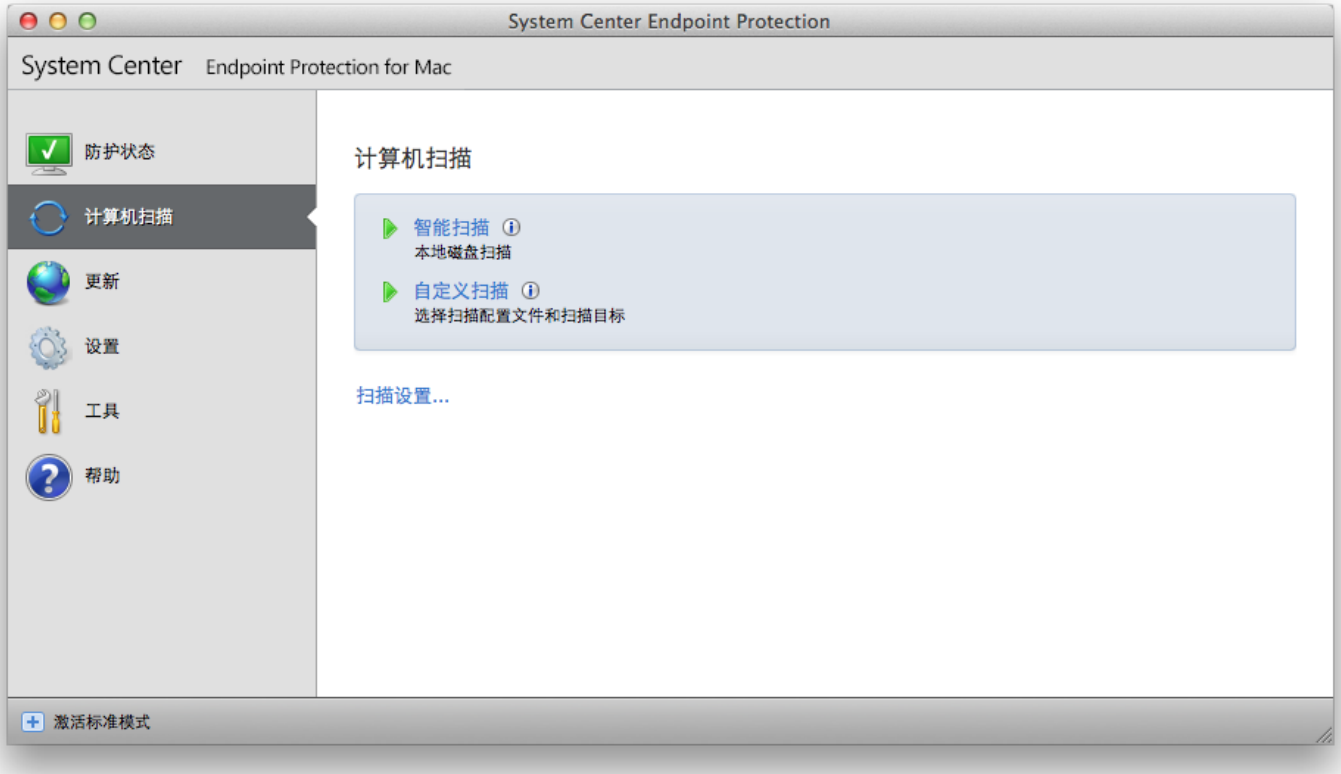
请确保您的计算机上没有安装其他病毒防护程序。如果同时启用两种实时防护，它们可能互相冲突。建议您卸载系统上可能存在的任何其他病毒防护程序。

实时防护不启动
如果系统启动时实时防护未启动，可能是因为与其他程序发生冲突。如果是这种情况，请咨询客户服务专家。

手动扫描计算机

如果您怀疑计算机受到感染（行为不正常），请运行**计算机扫描** > **智能扫描**，以检查计算机是否存在威胁。为了得到最大防护，计算机扫描应作为日常安全手段的一部分定期运行，而不应仅在怀疑有威胁时运行。定期扫描能够检测到威胁，这些威胁在保存到磁盘时未被实时扫描程序发现。如果计算机被感染时实时扫描程序已被禁用，或者病毒库过期，就会出现这种情况。

我们建议您每月至少运行一次手动扫描计算机。在**工具** > **计划任务**下可以将扫描配置为计划任务。



您还可以将所选文件和文件夹从桌面或 Finder 窗口拖放到 System Center Endpoint Protection 主屏幕、平台图标、菜单栏图标（屏幕顶部）或应用程序图标（位于 /Applications 文件夹中）。

扫描类型

有两种类型的手动扫描计算机可用。**智能扫描**快速扫描系统，无需进一步配置扫描参数。**自定义扫描**允许您选择任意预定义的扫描配置文件以及选择特定扫描目标。

智能扫描

智能扫描允许您快速启动计算机扫描和清除被感染文件而无需用户干预。其主要优势在于操作方便，没有复杂的扫描配置。智能扫描检查所有文件夹中的所有文件并自动清除或删除检测到的威胁。清除级别被自动设置为默认值。有关清除类型的更多详细信息，请参见清除[13]部分。

自定义扫描

如果您要指定扫描参数（如扫描目标和扫描方法等），**自定义扫描**是最佳选择。运行自定义扫描的优点在于能够详细配置参数。不同的配置可以保存为用户定义的扫描配置文件中，这在使用相同的参数重复扫描时非常有用。

要选择扫描目标，请选择**计算机扫描** > **自定义扫描**，并从树结构中选择特定的**扫描目标**。也可以通过输入要包括的文件或文件夹路径，更精确地指定扫描目标。如果您仅想扫描系统而不进行附加的清除操作，则选择**扫描但不清除**选项。此外，还可以通过单击**设置...**> **清除**，从三种清除级别中进行选择。

对于有病毒防护程序使用经验的高级用户，建议使用自定义扫描执行计算机扫描。

扫描目标

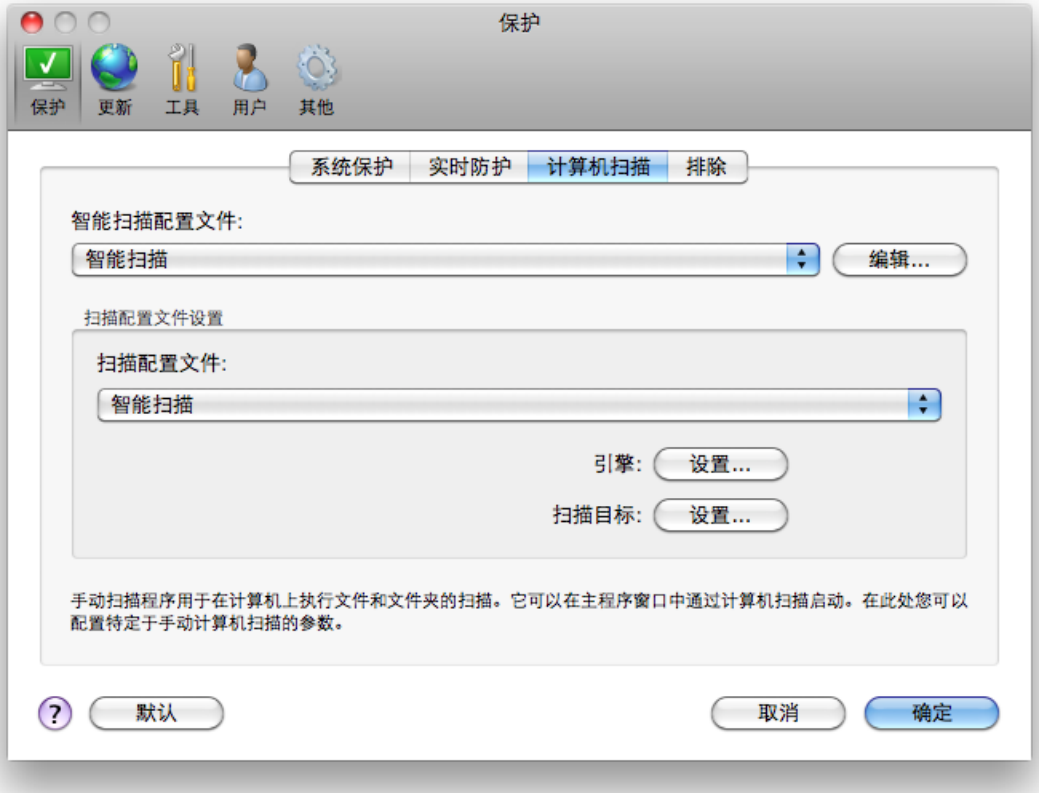
扫描目标树结构允许您选择要进行病毒扫描的文件和文件夹。也可以根据配置文件的设置选择文件夹。

还可以通过输入要扫描的文件或文件夹路径，更精确地定义扫描目标。从列有计算机上所有可用文件夹的树结构中选择目标。

扫描配置文件

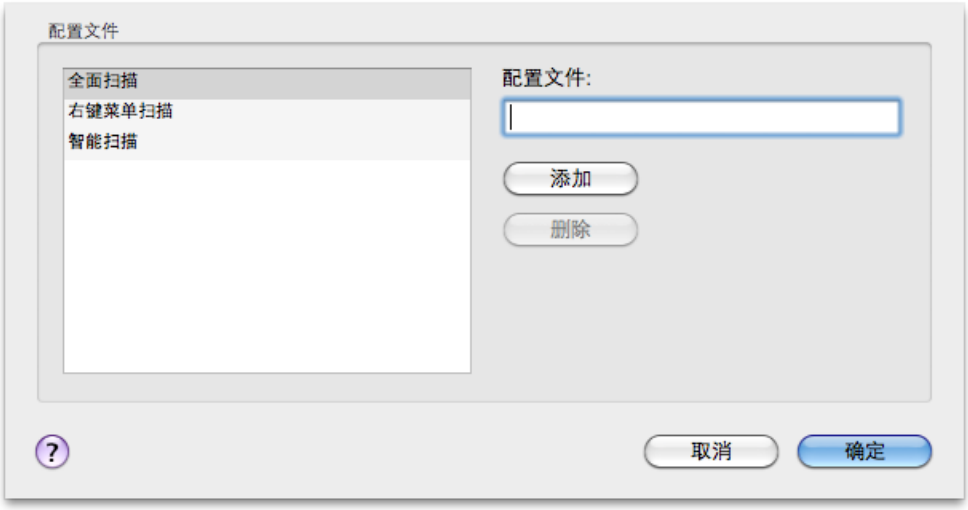
可以保存您的首选扫描设置以用于将来的扫描。建议您创建不同的配置文件（带有各种扫描目标、扫描方法和其他参数）用于每次定期扫描。

要创建新的配置文件，请转至**设置** > **进入应用程序首选项...**> **防护** > **计算机扫描**并单击当前配置文件列表旁边的**编辑...**。



为了帮助您创建适合您需求的扫描配置文件，请参见引擎参数设置[12]部分，查看扫描设置中每个参数的描述。

示例：假设您想要创建自己的扫描配置文件而且智能扫描配置部分适用，但您不希望扫描加壳程序或潜在不安全的应用程序，并且还希望应用严格清除。在**手动扫描程序配置文件列表**窗口，键入配置文件名称，单击**添加**按钮并通过单击**确定**进行确认。然后通过设置**引擎**和**扫描目标**调整参数以使其满足您的需求。



引擎参数设置

System Center Endpoint Protection 中使用的扫描技术具有主动防护功能，也就是说，它可在新威胁开始传播的较早阶段提供防护。该技术采用了多种方法（代码分析、代码仿真、一般的识别码、病毒库等），可显著提高系统安全性。扫描引擎可同时控制多个数据流，最大限度地提高效率和检测速度。此技术还可成功阻止 Rootkit。

引擎技术设置选项允许您指定若干扫描参数：

- 要扫描的文件类型和扩展名
- 不同检测方法的组合
- 清除级别等。

要进入设置窗口，请单击**设置** > **病毒和间谍软件防护** > **高级病毒和间谍软件防护设置**，然后单击**设置...**按钮，它位于**系统防护**？**实时防护**和**计算机扫描**通配符中。不同的安全情形可能要求不同的配置。请记住，可针对下列防护模块单独配置引擎参数：

- **系统防护** > 自动启动文件检查
- **实时防护** > 文件系统实时防护
- **计算机扫描** > 手动计算机扫描

引擎参数已针对每个模块进行了特定优化，对其进行修改可能会明显影响系统操作。例如，将设置更改为始终扫描加壳程序，或在文件系统实时防护模块中启用高级启发式扫描，可能会造成系统性能下降。因此，建议您保留所有模块（ 计算机扫描 除外）的默认引擎参数。

对象

对象部分允许您定义将扫描威胁的计算机文件。

- **文件** –提供对所有常见文件类型（程序、图片、音频、视频文件、数据库文件等）的扫描。
- **符号链接** -（仅手动扫描程序）扫描特殊文件类型，这些文件包含被操作系统当作和用作另一个文件或目录的路径的文本字符串。
- **电子邮件文件** -（在实时防护中不可用）扫描包含电子邮件的特殊文件。
- **邮箱** -（在实时防护中不可用）扫描系统中的用户邮箱。误用此选项可能导致与电子邮件客户端的冲突。
- **压缩文件** -（在实时防护中不可用）提供对压缩文件（.rar、.zip、.arj、.tar 等）中被压缩的文件的扫描。
- **自解压文件** -（在实时防护中不可用）扫描包含在自解压文件中的文件。
- **加壳程序** –除了标准静态加壳程序（UPX、yoda、ASPack、FGS 等），还有在内存中解压的加壳程序（和标准压缩类型不同）。

选项

在**选项**部分，可以选择在系统扫描威胁期间所用的方法。可用选项包括：

- **启发式扫描** - 启发式扫描是一种分析程序（恶意）行为的算法。启发式检测的主要优点是能够检测到以前不存在或已知病毒列表（病毒库）中没有的新恶意软件。
- **高级启发式扫描** - 高级启发式扫描具有一种独特的启发式扫描算法，它使用高级编程语言编写而成，针对检测计算机蠕虫和木马进行优化。有了高级启发式扫描，程序的检测能力显著提高。

- **潜在的不受欢迎应用程序** - 这些应用程序未必是恶意的，但可能会对计算机的性能产生不利影响。此类应用程序通常会在安装前提请用户同意。如果计算机上安装了这类程序，系统运行（与这些应用程序安装前的行为方式相比）会有所不同。最显著的变化包括会出现不受欢迎的弹出窗口、启动和运行隐藏进程、系统资源消耗增加、更改搜索结果以及应用程序与远程服务器的通信。
- **潜在的不安全应用程序** - 这些应用程序是指合法的商业软件，如果在用户不知情时安装了它们，可能会被攻击者滥用。此类别包括类似远程访问工具这样的程序，这就是默认禁用此选项的原因。

清除

清除设置确定扫描程序清除被感染文件的方式。共有 3 个清除级别：

- **不清除** - 被感染文件不会被自动清除。程序会显示一个警告窗口，允许您选择操作。
- **标准清除** - 程序将尝试自动清除或删除被感染文件。如果无法自动选择正确操作，程序将提供一组后续操作供选择。如果无法完成预定义的动作，也将显示后续操作选择。
- **严格清除** - 程序将清除或删除所有被感染文件（包括压缩文件）。唯一例外的是系统文件。如果无法清除文件，将弹出一个警告窗口，其中为您提供了操作选项。

警告： 在默认标准清除模式下，仅当压缩文件中的所有文件都被感染时，才会删除整个压缩文件。如果压缩文件还包含合法文件，则不删除。如果严格清除模式下检测到被感染的压缩文件，即使其中包含干净的文件，也会删除整个压缩文件。

扩展名

扩展名是用句点分隔的文件名的一部分。扩展名定义文件的类型和内容。引擎参数设置的此部分允许您定义不想扫描的文件类型。

默认情况下程序扫描所有文件，无论其扩展名是什么。可将任何扩展名添加到不扫描的文件列表中。使用**添加**和**删除**按钮，可以启用或禁用对所需扩展名的扫描。

如果扫描特定文件类型会妨碍程序正常工作，有时候需要不扫描这些文件。例如，建议排除 .log? .cfg 和 .tmp 扩展名。

限制

限制部分允许您指定要扫描的对象的最大大小和嵌套压缩文件的层数：

- **最大大小:**定义要扫描的对象的最大大小。病毒防护模块则仅扫描小于指定大小的对象。不建议更改默认值，因为通常无需修改它。此选项应仅由具有从扫描中排除大型对象的特定原因的高级用户更改。
- **最长扫描时间:**定义为扫描对象分配的最长时间。如果在此输入用户定义的值，时间用完后病毒防护模块将停止扫描对象，不管扫描是否完成。
- **最大嵌套层数:**指定压缩文件扫描的最大深度。不建议更改默认值 10，正常情况下无需修改它。如果扫描因嵌套压缩文件的数量而提前终止，则压缩文件仍将处于未选中状态。
- **最大文件大小:**此选项允许您指定要扫描的压缩文件（当解压缩时）中所包含文件的最大文件大小。如果因此限制而提前终止扫描，则压缩文件仍将处于未选中状态。

其他

启用智能优化后，使用最优化的设置可确保最高效的扫描级别，同时可保持最高的扫描速度。各种保护模块可进行智能化扫描，在将它们应用到特定的文件类型时使用不同的扫描方法。智能优化在该产品中未严格定义。我们的开发团队不断进行新更改，然后将这些更改通过定期更新集成到您的 System Center Endpoint Protection。如果禁用了智能优化，则在执行扫描时仅应用特定模块的引擎核心中用户定义的设置。

扫描交换数据流（仅手动扫描程序）
文件系统使用的交换数据流（资源/数据派生) 是对普通扫描技术不可见的文件和文件夹关联。许多渗透试图通过伪装成交换数据流来避开检测。

检测到渗透

渗透可通过各种渠道进入系统：网页、共享文件夹、电子邮件或可移动计算机设备（USB、外部磁盘、CD、DVD、软盘等）。

如果您的计算机有被恶意软件感染的迹象，例如速度下降、常常停止响应等，建议您遵循以下步骤：

1. 打开 System Center Endpoint Protection 并单击**计算机扫描**。
2. 单击**智能扫描**（更多信息，请参见智能扫描 10 部分）。
3. 扫描完成后，查看日志中已扫描文件、被感染文件和已清除文件的数量。

如果您只希望扫描磁盘的某一部分，请单击**自定义扫描**，然后选择扫描目标。

以下为 System Center Endpoint Protection 如何处理威胁的一般示例，假设使用默认清除级别的实时文件系统监视程序检测到了威胁。它将尝试清除或删除该文件。如果实时防护模块没有预定义操作，程序将显示一个警报窗口，要求您从中选择一个选项。一般会有**清除**？**删除**和**不操作**等选项。建议您不要选择**不操作**，因为这样将不对被感染文件采取任何操作。除非您确信该文件无害，只是检测失误所致。

清除和删除 - 如果文件遭到了病毒攻击（该病毒在被文件上附加了恶意代码），请应用清除。如果是这种情况，请首先尝试清除被感染文件，使其恢复到初始状态。如果文件全部由恶意代码组成，将删除该文件。

删除压缩文件中的文件 - 在默认清除模式下，仅当压缩文件只包含被感染文件而没有干净文件时，才会删除整个压缩文件。换言之，如果还包含无害的干净文件，就不会删除压缩文件。但是，执行**严格清除**扫描时请小心 - 使用严格清除时，即使压缩文件只包含一个被感染文件，无论压缩文件中其他文件的状态如何，都将删除该压缩文件。

更新程序

定期更新 System Center Endpoint Protection 对于保持最高级别的安全性很有必要。 更新 模块通过下载最新病毒库确保程序始终为最新。

通过在主菜单中单击**更新**，可以查看当前更新状态，包括上一次成功更新的日期和时间以及是否需要更新。要手动开始更新过程，请单击**更新病毒库**。

一般环境下，当正常下载更新时，将在 更新 窗口中显示消息*无需进行更新 - 所安装的病毒库为当前版本*。

更新 窗口还包含有关病毒库版本的信息。此数值指示符是指向网站的活动链接，其中列有给定更新期间添加的所有病毒库。

更新设置

要启用测试模式（下载测试模式），请单击**高级选项**旁边的**设置...**按钮，并选择**启用测试模式**复选框。要在每次成功更新后禁用系统托盘通知显示，则选择**不显示关于成功更新的通知**复选框。

要删除所有临时存储的更新数据，请单击**清除更新缓存**旁边的**清除**按钮。如果您在更新时遇到困难，则使用此选项。

如何创建更新任务

更新可以手动方式触发，方法是在主菜单中单击**更新**，在显示的主窗口中单击**更新病毒库**。

更新还可以作为计划任务运行。要配置计划任务，请单击**工具** > **计划任务**。默认情况下，在 System Center Endpoint Protection 中会启用以下任务：

- **定期自动更新**
- **用户登录后自动更新**

可以修改每个更新任务以满足您的需要。除了默认更新任务外，您还可以使用用户定义的配置创建新更新任务。有关创建和配置更新任务的更多详细信息，请参见计划任务 16 部分。

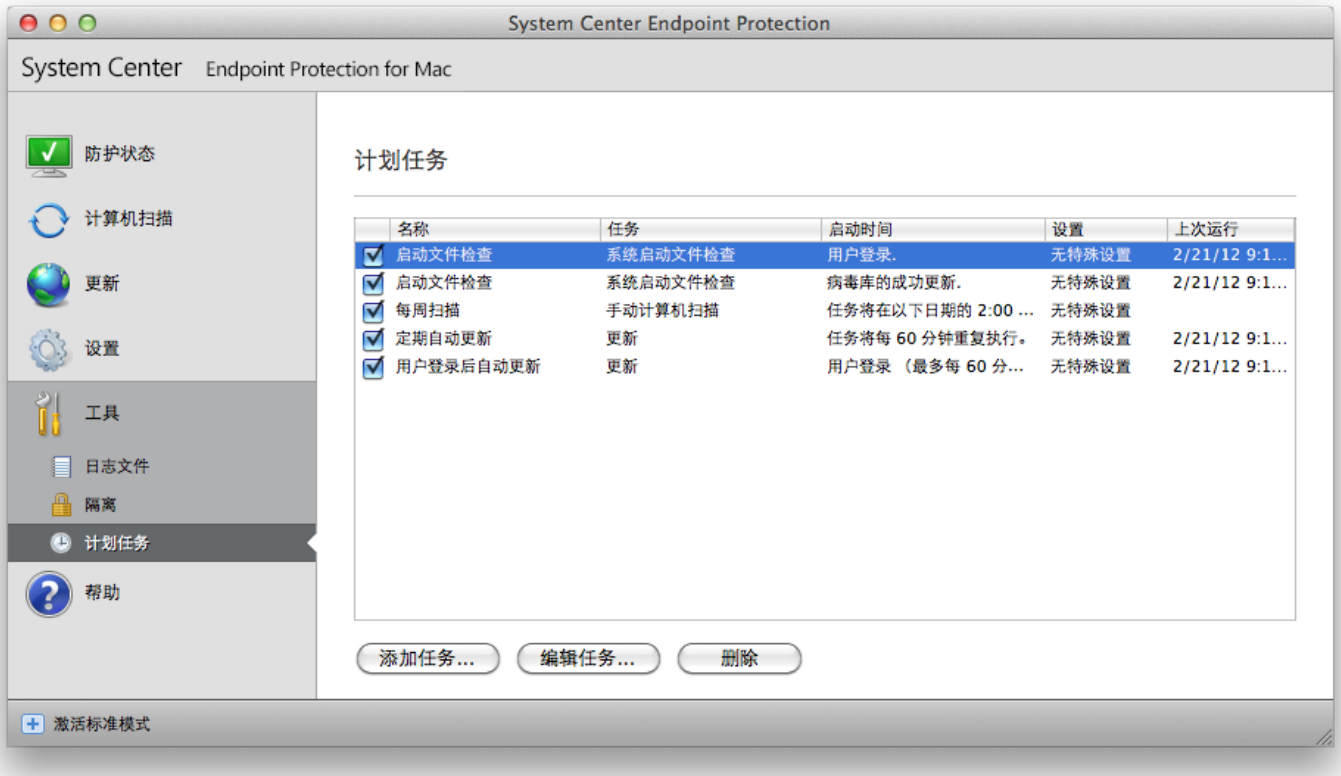
升级到新版本

为了得到最大防护，使用 System Center Endpoint Protection 的最新版本很重要。要查看是否有新版本，请从左侧的主菜单中单击**更新**。如果有新版本可用，则会在窗口底部显示消息 *产品有新版本可用*。”单击**了解详细信息...**，显示一个新窗口，其中包含新版本的版本号和变更日志。

单击**下载**，下载最新的版本。单击**关闭**，关闭窗口并在以后下载升级。

计划任务

如果在 System Center Endpoint Protection 中激活了高级模式，则**计划任务**可用。 计划任务 位于 System Center Endpoint Protection 主菜单中的**工具**下。**计划任务**包含所有计划任务和配置属性的列表，如预定义的日期、时间和使用的扫描配置文件。



默认情况下，计划任务中显示以下计划任务：

- 定期自动更新
- 用户登录后自动更新
- 用户登录后启动文件检查
- 成功更新病毒库后进行启动文件检查
- 日志维护（在计划任务设置中启用**显示系统任务**选项后）
- 每周扫描

要编辑现有计划任务（包括默认和用户定义的）的配置，请按 ctrl 单击要修改的任务然后单击**编辑...**，或选择任务然后单击**编辑任务...**按钮。

计划任务的目的

计划任务管理和启动具有预定义配置和属性的计划任务。配置和属性包含日期和时间等信息以及执行任务期间使用的指定配置文件。

创建新任务

要在计划任务中创建新任务，请单击**添加任务...**按钮或按 ctrl 单击空白字段，并从右键菜单中选择**添加...**。共有 5 种类型的计划任务：

- **运行应用程序**
- **更新**
- **日志维护**
- **手动扫描计算机**
- **系统启动文件检查**

因为 '更新 '是最常用的计划任务之一，所以我们将解释如何添加新的更新任务。

从**计划任务**下拉菜单中选择**更新**。将任务名称输入到**任务名称**字段。从**运行任务**下拉菜单中选择任务频率。可用选项包括：**用户定义的**？**一次**？**重复**？**每日**？**每周**和**由事件触发**。将根据选定的频率为您提供不同的更新参数。

如果选择**用户定义**，将提示您以 cron 格式指定日期/时间（参见创建用户定义的任务[17]一节了解更多详细信息）。

在下一步中，定义无法在计划时间执行或完成任务时要采取的操作。有以下三个选项可用：

- **延至下次预定时间**
- **尽快运行任务**
- **如果自上次执行任务至今已超过指定时间间隔则立即执行任务**（可以使用**任务最短时间间隔**选项定义该时间间隔）

在下一步中，显示包含有关当前计划任务信息的摘要窗口。单击**完成**按钮。

新的计划任务将添加到当前计划任务列表。

默认情况下，系统包含必要的计划任务以确保产品功能正常。这些任务不能改变，且默认情况下处于隐藏状态。要更改此选项并使这些任务可见，请进入**设置** > **进入应用程序首选项...**> **工具** > **计划任务**并选择**显示系统任务**选项。

创建用户定义的任务

用户定义的任务的日期和时间必须以年扩展 cron 格式输入（白空格分隔的 6 字段组成的字符串）：
`分钟(0-59) 小时(0-23) 日期(1-31) 月份(1-12) 年份(1970-2099) 星期几(0-7)(周日 = 0 或 7)`

示例：
`30 6 22 3 2012 4`

cron 表达式支持的特殊字符：
- 星号 (*) - 表达式匹配字段的所有值；例如，第 3 个字段（日期）中的星号表示每一天
- 连字符 (-) - 定义范围；例如 `3-9`
- 逗号 (,) - 分隔列表项；例如 `1,3,7,8`
- 斜杠 (/) - 定义范围增量；例如`3-28/5` 在第 3 个字段（日期）中表示每月第 3 天以及以后依次增加 5 天。

不支持日期名称（周一-周日）和月份名称（1 月-12 月）。

注意： 如果定义日期和星期几，则仅当两个字段匹配时才会执行命令。

隔离

隔离的主要任务是安全储存被感染文件。隔离文件的前提是文件出现以下情况：无法清除、不安全或被建议删除，或被 System Center Endpoint Protection 错误检测。

您可以选择隔离任何文件。如果文件行为可疑但未被病毒防护扫描程序检测到，建议采取隔离措施。

可在表格中查看储存在隔离区文件夹中的文件，表格中显示隔离的日期和时间、被感染文件原始位置的路径、文件大小（字节数）、原因（例如，由用户添加…）以及威胁数量（例如，是否为包含多个威胁的压缩文件）等。即使在卸载 System Center Endpoint Protection 后，带隔离文件的隔离文件夹 (/Library/Application Support/Microsoft/scep/cache/quarantine) 仍保留在系统内。隔离的文件以安全的加密形式存储，在安装 System Center Endpoint Protection 后可再次恢复。

隔离文件

System Center Endpoint Protection 自动隔离被删除的文件（如果您尚未在警报窗口中取消该选项）。如果需要，您可以手动隔离任何可疑文件，方法是单击**隔离...**按钮。也可以通过右键菜单来实现此目的 –按 ctrl 单击空白字段，选择**隔离...**，选择想要隔离的文件并单击**打开**按钮。

从隔离恢复

隔离的文件还可以恢复到其初始位置。使用**恢复**按钮可达到此目的。按 ctrl 单击**隔离**窗口中的给定文件，然后单击**恢复**，也可以从右键菜单访问恢复功能。右键菜单还提供**恢复至...**选项，使用此选项可将文件恢复到其被删除时位置之外的其他位置。

日志文件

日志文件包含所有已发生的重要程序事件的信息，并提供检测到的威胁的概要信息。日志记录是系统分析、威胁检测以及故障排除的必要工具。日志记录在后台主动执行，无需用户交互。对信息的记录是根据当前日志级别设置进行的。可以直接从 System Center Endpoint Protection 环境以及归档日志中查看文本消息和日志。

日志文件可从 System Center Endpoint Protection 主菜单中访问，方法是单击**工具** > **日志文件**。使用窗口顶部的**日志**下拉菜单选择所需日志类型。可用日志包括：

1. **检测到的威胁** - 使用此选项可以查看与威胁检测相关的所有事件信息。
2. **事件** - 此选项用于帮助系统管理员和用户解决问题。System Center Endpoint Protection 执行的所有重要操作都记录在事件日志中。
3. **计算机扫描** - 所有已完成的扫描的结果显示在此窗口中。双击任意条目可查看相应手动计算机扫描的详细信息。

在每一部分中，显示的信息都可以直接复制到剪贴板，方法是选择条目并单击**复制**按钮。

日志维护

可从主程序窗口访问 System Center Endpoint Protection 的日志记录配置。单击**设置** > **进入应用程序首选项...**> **工具** > **日志文件**。您可以为日志文件指定以下选项：

- **自动删除旧日志记录** - 自动删除指定天数以前的日志条目。
- **自动优化日志文件** - 如果未用记录百分比超过指定值，则启用日志文件的自动碎片整理。

图形用户界面、威胁和事件消息上显示的所有相关信息都可以采用人类可阅读的文本格式（如纯文本或 CSV（用逗号分隔的值））存储。如果您要使这些文件可使用第三方工具处理，请选中**启用日志记录到文本文件**旁的复选框。

若要定义日志文件将保存到的目标文件夹，请单击**高级设置**旁的**设置...**。

根据在**文本日志文件:** 的**编辑**下选中的选项，您可以保存写入了以下信息的日志：

- 由启动扫描程序、实时防护或计算机扫描检测到的威胁将存储在名为 threatslog.txt 的文件中。
- *用户名和密码无效*和*无法更新病毒库*等事件将写入 eventslog.txt 文件。
- 所有已完成扫描的结果都将采用 scanlog.NUMBER.txt 格式保存。

要配置**默认计算机扫描日志记录**的过滤器，请单击该选项旁边的**编辑...**按钮，并根据需要选择/取消选择日志类型。可以在本章中 18找到对这些日志类型的进一步说明。

日志过滤

有关重要系统事件的日志存储信息。日志过滤功能允许您显示有关特定类型事件的记录。

下面列出了最常用的日志类型：

- **严重警告** - 严重系统错误（例如，病毒防护未能启动）
- **错误** - 诸如 *"下载文件时出错"*之类的错误消息和严重错误
- **警告** - 警告消息
- **信息性记录** - 包括成功更新、警报等的信息性消息
- **诊断记录** - 微调程序所需要的信息以及上述所有记录。

用户界面

System Center Endpoint Protection 中的用户界面配置选项允许您调整工作环境以符合您的需要。这些配置选项可从**设置** > **进入应用程序首选项...**> **用户** > **界面**进行访问。

在此部分中，用户可通过 高级模式 选项切换到高级模式。高级模式显示更详细的设置和 System Center Endpoint Protection 的其他控件。

要启用启动初始屏幕功能，请选择**在启动时显示启动画面**选项。

在**使用标准菜单**部分，可以选择**以标准模式/以高级模式**选项， 以在相应的显示模式下在主程序窗口中使用标准菜单。

要启用工具提示，请选择**显示工具提示**选项。**显示隐藏文件**选项允许您查看并选择在**计算机扫描**的**扫描目标**设置中的隐藏文件。

警报和通知

警报和通知部分允许您配置在 System Center Endpoint Protection 中处理威胁警报和系统通知的方式。

禁用**显示警报**选项将取消所有警报窗口，而且仅在特定情况下适用。对于大多数用户，我们建议保留该选项的默认设置（启用）。

选择**在桌面上显示通知**选项将使不需要用户交互的警报窗口显示在桌面上（默认情况下，在屏幕的右上角）。 通过调整在 X **秒后自动关闭通知**一值，可以定义通知显示的时长。

警报和通知高级设置

仅显示需要用户交互的通知
使用此选项可切换需要用户交互的消息的显示。

在全屏模式下运行应用程序时，仅显示需要用户交互的通知
在进行幻灯片演示或需要全屏的其他操作时，此选项很有用。

权限

System Center Endpoint Protection 设置对您的组织安全策略非常重要。未经授权的更改可能会破坏系统的稳定和防护。最终，您可以选择哪些用户具有编辑程序配置的权限。

要指定授权用户，请进入**设置** > **进入应用程序首选项...**> **用户** > **权限**。

为最大限度地保障系统安全，必须正确配置程序。未经授权的修改可能导致丢失重要数据。要设置授权用户列表，只要从左侧的**用户**列表选择用户并单击**添加**按钮即可。要除去用户，只要从右侧的**授权用户**列表选择他们的名称并单击**删除**即可。

注意： 如果授权用户列表为空，系统的所有用户都将具有编辑程序设置的权限。

右键菜单

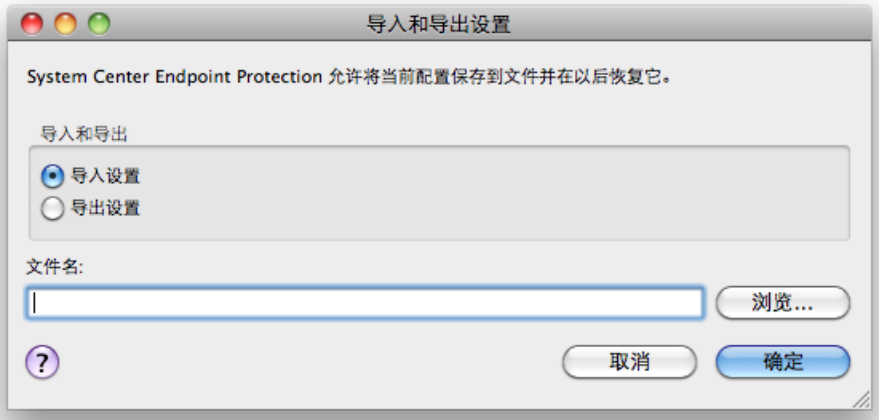
右键菜单集成可以通过在**设置** > **进入应用程序首选项...**> **用户** > **右键菜单**部分启用**集成到右键菜单**复选框来启用。

高级用户

导入和导出设置

System Center Endpoint Protection 的导入和导出配置可在**设置**下的高级模式中找到。

导入和导出都使用压缩文件来存储配置。如果需要备份 System Center Endpoint Protection 的当前配置以便在将来使用，导入和导出会很有用。对于想要在多个系统上使用其首选 System Center Endpoint Protection 配置的用户，导出设置选项也很便利，因为他们可以方便地导入配置文件来传输想要的设置。



导入设置

导入配置非常简单。在主菜单中，单击**设置** > **导入和导出设置...**，然后选择**导入设置**选项。输入配置文件的名称，或单击**浏览...**按钮来找到想要导入的配置文件。

导出设置

导出配置的步骤非常相似。在主菜单中，单击**设置** > **导入和导出设置...**选择**导出设置**选项并输入配置文件的名称。使用浏览器在计算机上选择要保存配置文件的位置。

代理服务器设置

代理服务器设置可以在**其他** > **代理服务器**下配置。在此级别指定的代理服务器定义了所有 System Center Endpoint Protection 功能的全局代理服务器设置。此处的参数将用于需要连接到 Internet 的所有模块。

要指定此级别的代理服务器设置，请选中**使用代理服务器**复选框，然后在**代理服务器**字段中输入代理服务器的 IP 地址或 URL。在端口字段中指定代理服务器接受连接的端口（默认情况下使用 3128 端口）。如果与代理服务器的通信需要验证，请选中**代理服务器需要验证**复选框，然后在相应字段中输入有效**用户名**和**密码**。

可移动磁盘阻止

可移动磁盘（例如 CD 或 USB 磁盘）可能包含恶意代码，从而威胁您的计算机。若要阻止可移动磁盘，请选中**启用可移动磁盘阻止**旁的复选框。若要允许访问特定类型的磁盘，请取消选中要允许的磁盘类型旁的复选框。

如果您要将这些设置应用到 CD、DVD、FireWire 或 USB 之外的磁盘类型，请选中**其他**旁的复选框。该设置将特别应用于任何通过 Thunderbolt 端口连接到您的计算机的外围设备。

词汇表

渗透类型

渗透是一种试图进入和/或损坏用户计算机的恶意软件。

病毒

计算机病毒是破坏计算机上现有文件的渗透。计算机病毒之所以用生物学上的 "病毒 "一词命名，是因为它们使用类似手法在计算机之间传播。

计算机病毒主要攻击可执行文件、脚本和文档。为了进行复制，病毒将 "本体 "附加在目标文件末尾。计算机病毒的工作方式可简述如下：执行被感染文件后，病毒（在原始应用程序之前）自我启动并执行其预定义的任务。只有在此之后，原始应用程序才开始运行。除非用户自己（意外或故意）运行或打开恶意程序，否则病毒无法感染计算机。

计算机病毒的目的和严重性各有不同。其中有些病毒非常危险，因为它们会故意删除硬盘驱动器上的文件。另一方面，一些病毒不造成任何破坏，它们只是骚扰用户，展示其作者的技术技巧。

必须注意，病毒（与木马或间谍软件相比）正越来越少见，因为它们对恶意软件作者的商业吸引力不足。而且，"病毒 "一词常常被误用来涵盖所有类型的渗透。这种用法正在逐渐改变，而由新的、更为准确的术语 "恶意软件 "所取代。

如果您的计算机感染了病毒，必须将被感染文件恢复为初始状态，即通过使用病毒防护程序清除它们。

病毒示例包括：OneHalf? Tenga 和 Yankee Doodle。

蠕虫

计算机蠕虫是包含可通过网络攻击主机并传播的恶意代码的程序。病毒和蠕虫的基本区别在于蠕虫具有自我复制和传播的能力，它们不依赖主机文件（或引导区）。蠕虫通过联系人列表中的电子邮件地址或利用网络应用程序中的安全漏洞进行传播。

因此，蠕虫的生存能力远超计算机病毒。由于 Internet 的广泛应用，它们可以在发布后数小时内传播到世界各地 - 在某些情况下，甚至只需数分钟。这种独立快速复制的能力使得它们比其他类型恶意软件更加危险。

在系统中激活的蠕虫会带来多种不便：它可以删除文件、降低系统性能，甚至停止程序。计算机蠕虫的特性使其适合作为其他类型渗透的 "传输手段"。

如果您的计算机感染了蠕虫，建议您删除被感染文件，因为它们可能包含恶意代码。

著名的蠕虫示例包括：Lovsan/Blaster? Stration/Warezov? Bagle 和 Netsky。

木马

历史上对计算机木马的定义是，试图以有用程序的假面具欺骗用户允许其运行的一类威胁。现在，木马已无需伪装自己。它们唯一的目的就是尽可能轻松地渗透并达到其恶意目的。 "木马 "已成为一个通用词，用来形容不属于任何特定类别的所有渗透。

由于其涵盖范围非常广，因此常被分为许多子类别：

- Downloader –一种能够从 Internet 下载其他威胁的恶意程序。
- Dropper –一种设计用于将其他类型恶意软件放入所破坏的计算机中的木马。
- Backdoor - 一种与远程攻击者通信，允许其获得系统访问权并控制系统的应用程序。
- Keylogger –（按键记录程序），一种记录用户键入的每个按键并将信息发送给远程攻击者的程序。
- Dialer - 是用于连接附加计费号码的程序。用户几乎无法注意到新连接的创建。Dialer 只能对使用拨号调制解调器（现在已很少使用）的用户造成破坏。
- 木马通常采用可执行文件形式。如果计算机上的文件被检测为木马，建议您将其删除，因为它极有可能包含恶意代码。

著名木马示例包括：NetBus? Trojandownloader.Small.ZL 和 Slapper。

广告软件

广告软件是可支持广告宣传的软件的简称。显示广告资料的程序便属于这一类别。广告软件应用程序通常会在 Internet 浏览器中自动打开一个包含广告的新弹出窗口，或者更改浏览器主页。广告软件经常与免费软件程序捆绑在一起，以填补免费软件程序开发人员开发应用程序（通常为有用程序）的成本。

广告软件本身并不危险 –用户可能只是受到广告的干扰。广告软件的危险在于它也可能执行跟踪功能（和间谍软件一样）。

如果您决定使用免费软件产品，请特别注意安装程序。安装程序大多会通知您将要安装附加的广告软件程序。通常您可以取消它，安装不带有广告软件的程序。

如果不安装广告软件，某些程序可能无法安装，或者功能受到限制。这意味着，广告软件可能常常以 "合法 "方式访问系统，因为用户已同意安装它。在这种情况下，与其事后追悔莫及，不如事前稳妥行事。如果计算机上的某个文件被检测为广告软件，我们建议您删除它，因为该软件极有可能包含恶意代码。

间谍软件

此类别包括所有在未经用户同意/了解的情况下发送私人信息的应用程序。间谍软件使用跟踪功能发送各种统计数据，例如所访问网站的列表、用户联系人列表中的电子邮件地址或记录按键的列表。

间谍软件的作者宣称，这些技术旨在更好地了解用户需求和兴趣，从而使广告更有针对性。问题在于，有用和恶意的应用程序之间并没有明显的差别，任何人都无法确保检索到的信息不会被滥用。间谍软件应用程序获得的数据可能包括安全代码、PIN、银行帐号等。程序的作者通常将间谍软件与其免费版本程序捆绑，以获取收益或促使用户购买软件。通常情况下，程序在安装时会告知用户存在间谍软件，以促使其将软件升级为不带间谍软件的付费版本。

比如 P2P（点对点）网络客户端应用程序就是著名的捆绑了间谍软件的免费软件产品。Spyfalcon 或 Spy Sheriff（以及更多）属于特定的间谍软件子类别 –它们看上去象间谍软件防护程序，实际上其本身就是间谍软件程序。

如果计算机上的某个文件被检测为间谍软件，我们建议您删除它，因为该软件极有可能包含恶意代码。

潜在的不安全应用程序

许多合法程序可用于简化联网计算机的管理。然而，不法之徒可能将其滥用为恶意目的。System Center Endpoint Protection 提供检测此类威胁的选项。

"潜在的不安全应用程序 "是指用于商业目的的合法软件。其中包括远程访问工具、密码破解应用程序以及按键记录器（用于记录用户键盘输入信息）等程序。

如果您发现计算机上存在且正在运行潜在的不安全应用程序（而您并没有安装它），请咨询您的网络管理员或删除该应用程序。

潜在的不受欢迎应用程序

潜在的不受欢迎应用程序未必是恶意的，但可能会对计算机性能造成负面影响。此类应用程序通常会在安装前提请用户同意。如果计算机上安装了这类程序，系统运行（与安装前的行为方式相比）会有所不同。其中最显著的变化是：

- 系统会打开以前没见过的新窗口
- 启动并运行隐藏的进程
- 系统资源的使用增加
- 搜索结果发生改变
- 应用程序会与远程服务器通信。