System Center Endpoint Protection

安装手册和用户指南

Red Hat Enterprise Linux Server 5, 6
SUSE Linux Enterprise 10, 11
CentOS 5, 6
Debian Linux 5, 6
Ubuntu Linux 10.04, 12.04
Oracle Linux 5, 6

Microsoft

Microsoft® System Center Endpoint Protection

目录

介绍

感谢您使用 System Center Endpoint Protection。Microsoft 先进的扫描引擎具有无与伦比的扫描速度和检测率以及极低系统资源，是适合任何 Linux OS 服务器的理想选择。

主要功能

手动扫描程序

特权用户（通常是系统管理员）可以通过命令行界面、Web 界面或操作系统的自动计划任务工具（例如 cron），启动手动扫描程序。*手动*指按用户或系统需要扫描文件系统对象。

实时防护

当用户和 *或*操作系统尝试访问文件系统对象时，调用实时防护。这也是*自动*的含义；因为扫描由访问文件系统对象的尝试触发。

系统主要功能

高级引擎算法

Microsoft 病毒防护扫描引擎算法提供最高检测率和最快扫描时间。

多处理

System Center Endpoint Protection 开发可在单处理器和多处理器设备上运营。

高级启发式扫描

System Center Endpoint Protection 具有用于 Win32 蠕虫、后门感染和其他形式恶意软件的独特高级启发式扫描。

内置功能

内置压缩工具可解压缩压缩对象，无需任何外部程序。

速度和效率

为增加系统速度和效率，System Center Endpoint Protection 架构基于运行的后台程序（常驻程序），从该后台程序发送所有扫描请求。

提高安全

所有执行后台程序（scep_dac 除外）在非特权用户帐户下运行以提高安全。

有选择性的配置

系统支持根据用户或客户端 服务器有选择性的配置。

多日志记录级别

可以配置多日志记录级别以获得关于系统活动和渗透的信息。

Web 界面

通过直观且用户友好的 Web 界面提供配置和管理。

无外部库

System Center Endpoint Protection 安装不需要外部库或 LIBC 以外的程序。

用户指定的通知

可以配置系统在检测到渗透或其他重要事件时通知特定用户。

低系统要求

要高效运行，System Center Endpoint Protection 只需 16MB 硬盘空间和 32MB RAM。它在 2.2.x、2.4.x 和 2.6.x Linux OS 内核版本下流畅运行。

性能和可扩展性

从低性能小型办公服务器到具有数千用户的企业级 ISP 服务器，除了 Microsoft 安全产品无比的安全性，System Center Endpoint Protection 还提供您希望从 UNIX 解决方案获得的性能和可扩展性。

术语与缩写

在本节中我们将回顾本文档中使用的术语与缩写。注意，粗体对产品组件名称和新定义的术语与缩写保留。本章中定义的术语与缩写以后将扩展至本文档。

SCEP

SCEP 是 Microsoft 为 Linux 操作系统开发的安全产品的标准缩写。它还是包含产品的软件包的名称。

SCEP daemon

主要 SCEP 系统控制和扫描后台程序： *scep_daemon*.

SCEP 基础目录

存储包含病毒库的 SCEP 可加载模块的目录。缩写 *@BASEDIR@* 未来将用于指此目录。下面列出 *@BASEDIR@* 值（取决于操作系统）：

```
Linux: /var/opt/microsoft/scep/lib
```

SCEP 配置目录

存储 System Center Endpoint Protection 配置所有相关文件的目录。缩写 *@ETCDIR@* 未来将用于指此目录。下面列出 *@ETCDIR@* 值（取决于操作系统）：

```
Linux: /etc/opt/microsoft/scep
```

SCEP 配置文件

主要 System Center Endpoint Protection 配置文件。文件的绝对路径如下：

@ETCDIR@/scep.cfg

SCEP 二进制文件目录

存储相关 System Center Endpoint Protection 二进制文件的目录。缩写 *@BINDIR@* 未来将用于指此目录。下面列出 *@BINDIR@* 值（取决于操作系统）：

```
Linux: /opt/microsoft/scep/bin
```

SCEP 系统二进制文件目录

存储相关 System Center Endpoint Protection 系统二进制文件的目录。缩写 *@SBINDIR@* 未来将用于指此目录。下面列出 *@SBINDIR@* 值（取决于操作系统）：

```
Linux: /opt/microsoft/scep/sbin
```

SCEP 对象文件目录

存储相关 System Center Endpoint Protection 对象文件和库的目录。缩写 *@LIBDIR@* 未来将用于指此目录。下面列出 *@LIBDIR@* 值（取决于操作系统）：

```
Linux: /opt/microsoft/scep/lib
```

安装

System Center Endpoint Protection 作为二进制文件分发：

```
scep.i386.ext.bin
```

在上面显示的二进制文件中，*'ext'* 是取决于 Linux 操作系统分发的后缀， "deb 表示 Debian， "rpm 表示 RedHat 和 SuSE， "tgz 表示其他 Linux OS 分发。

要安装或升级产品，使用以下命令：

```
sh ./scep.i386.ext.bin
```

显示产品的用户许可证接受协议。确认接受协议后，将安装包放入当前工作目录，并在屏幕上显示程序包安装、卸载或升级的相关信息。

安装程序包后，可以使用以下命令检验主 SCEP 服务是否运行：

```
ps -C scep_daemon
```

按 ENTER 后，您应看到以下（或类似）消息：

```
 PID TTY TIME CMD
2226 ? 00:00:00 scep_daemon
2229 ? 00:00:00 scep_daemon
```

至少两个 SCEP 后台程序进程在后台运行。第一个 PID 表示系统的进程和线程管理器。另一个表示 SCEP 扫描进程。

安装语言包

要安装 System Center Endpoint Protection 所需的语言包，使用以下命令：

```
sh ./scep-lang.lng.bin
```

其中 *'lng'* 需要替换为要导入的文件的语言代码。

Installation completed successfully 通知显示后，相应更新 LANG 系统变量并根据需要更新环境。这包括语言包安装。

每个语言包包括以下内容：

- 本地化 Web 界面
- 本地化 SCEP 代理和命令控制台输出
- 本地化 PDF 文档

架构概述

成功安装 System Center Endpoint Protection 后，您应熟悉其架构。

系统包括以下部分：

核心

System Center Endpoint Protection 的核心是 SCEP 后台程序 (scep_daemon)。后台程序使用 SCEP API 库 libscep.so 和 SCEP 加载模块 em00X_xx.dat 提供基础系统任务，如扫描、维护代理后台程序进程，维护样本提交系统，日志记录，通知等。请参考 *scep_daemon(8)* 主页了解详细信息。

代理

SCEP 代理模块的用途是将 SCEP 与 Linux 服务器环境集成。

实用工具

实用工具模块提供简单有效的系统管理。它们负责隔离管理、系统设置和更新等系统任务。

配置

正确的配置是安全系统最重要的部分；本章其余部分专门解释所有相关部分。我们还强烈建议您对 *scep.cfg* 文件有全面深入的了解，因为其中包含勒对 System Center Endpoint Protection 配置至关重要的信息。

成功安装产品后，所有配置组件存储在 SCEP 配置目录中。目录包含以下文件：

@ETCDIR@/scep.cfg

这是最重要的配置文件，因为它控制产品功能的所有主要方面。scep.cfg 文件包含多个部分，每部分包含不同参数。文件包含一个 global 和多个 'agent 部分，在方括号中包含所有部分名称。global 部分的参数用于定义 SCEP 后台程序的配置选项，以及 SCEP 扫描引擎配置的默认值。agent 部分的参数用于定义用于拦截计算机和 /或其邻居中各种数据流类型并准扫描的模块配置选项。注意，除了用于系统配置的各种参数，还有规则规定文件的组织。有关组织此文件的最有效方式的详细信息，请参考 *scep.cfg(5)* 和 *scep_daemon(8)* 主页以及所有相关代理的主页。

@ETCDIR@/certs

此目录用于存储 SCEP Web 界面身份验证使用的证书。请参见 *scep_wwwi(8)* 主页了解详细信息。

@ETCDIR@/scripts/daemon_notification_script

如果脚本通过 SCEP 配置文件参数 *'exec_script'* 而得以启用，则当病毒防护程序检测到渗透时，将执行此脚本。它用于向系统管理员发送关于事件的电子邮件通知。

与文件系统集成

本章介绍可提供对病毒和蠕虫文件系统感染最有效防护的手动和实时防护配置。System Center Endpoint Protection 的扫描能力来自手动扫描程序命令 *'scep_scan'* 和自动扫描程序命令 *'scep_dac'*。Linux 版本的 System Center Endpoint Protection 提供额外自动扫描程序技术，使用预加载的库模块 *libscep_pac.so*。以下章节中介绍所有这些命令。

手动扫描程序

特权用户（通常是系统管理员）可以通过命令行界面、Web 界面或操作系统的自动计划任务工具（例如 cron），启动手动扫描程序。*手动*指按用户或系统需要扫描文件系统对象。

手动扫描程序不要求特别配置即可运行。正确安装 SCEP 包后，可以使用命令行界面或计划任务工具直接运行手动扫描程序。要从命令行运行手动扫描程序，使用以下语法：

```
@SBINDIR@/scep_scan [option(s)] FILES
```

其中 FILES 是要扫描的目录和 *或*文件列表。

使用 SCEP 手动扫描程序可以使用多个命令行选项。要查看选项完整列表，请参见 *scep_scan(8)* 主页。

Dazuko 支持的实时防护

：

用户和 *或*操作系统对文件系统对象的访问调用实时防护。这也是*自动*的含义；扫描程序由访问所选文件系统对象触发。

SCEP 自动扫描程序使用的技术由 Dazuko (da-tzu-ko) 内核模块支持，以拦截内核调用为基础。Dazuko 项目是开放源，这意味着免费分发其源代码。这样允许用户为自己的自定义内核编译内核模块。注意 Dazuko 内核模块不属于任何 SCEP 产品，在使用自动扫描命令 *scep_dac* 前必须编译它并安装在内核中。Dazuko 技术使自动扫描不依赖使用的文件系统类型。它还适合通过 Network File System (NFS)、Nettalk 和 Samba 扫描文件系统对象。

重要信息 提供与自动扫描程序配置和使用有关的详细信息前，应注意，扫描程序主要开发和测试用于保护外部装载的文件系统。如果有多个未外部装载的文件系统，您需要从文件访问控制中排除它们以防止系统挂起。要排除的典型目录示例包括 *'/dev'* 目录和 SCEP 使用的任何目录。

工作原理

实时防护 *scep_dac* (SCEP Dazuko-powered file Access Controller) 是提供对文件系统持续监测和控制的常驻程序。每个文件系统对象都根据可自定义的文件访问事件类型进行扫描。当前版本支持以下事件类型：

Open 事件

要启动此文件访问类型，将 scep.cfg 文件的 **[fac]** 部分的 *'event_mask'* 参数设置为 open。这样将启用 Dazuko 访问掩码的 ON_OPEN 位。

Close 事件

要启动此文件访问类型，将 scep.cfg 文件的 **[fac]** 部分的 *'event_mask'* 参数设置为 close。这样将启用 Dazuko 访问掩码的 ON_OPEN 位。这样将启用 Dazuko 访问掩码的 ON_CLOSE 和 ON_CLOSE_MODIFIED 位。

注意： 一些操作系统内核版本不支持拦截 ON_CLOSE 事件。在这些情况下，*scep_dac* 将不监测 close 事件。

Exec 事件

要启动此文件访问类型，将 scep.cfg 文件的 **[fac]** 部分的 *'event_mask'* 参数设置为 exec。这样将启用 Dazuko 访问掩码的 ON_EXEC 位。

实时防护确保 *scep_daemon* 首先扫描所有打开、关闭和执行的文件中的病毒。根据扫描结果，拒绝或允许对特定文件的访问。

安装和配置

初始化 *scep_dac* 前，必须编译 Dazuko 内核模块并安装在运行的内核中。有关如何编译和安装 Dazuko 的详细信息，请参见：

http://www.dazuko.org

安装 Dazuko 后，检查并编辑 SCEP 配置文件 (scep.cfg) 的 **[global]** 和 **[fac]** 部分。注意，要使实时防护正确工作，取决于此文件的 **[fac]** 部分中的 *'agent_type'* 选项配置。此外，您必须定义由实时防护监测的文件系统对象（如目录和文件）。定义 *'ctl_incl'* 和 *'ctl_excl'* 选项的参数可以实现这一点，这些参数也在 **[fac]** 部分中。更改 scep.cfg 文件后，您可以重新加载 SCEP 后台程序，强制重新读取新创建的配置。

提示

!

要确保初始化 *scep_dac* 后台程序前 Dazuko 模块加载，请遵循以下步骤：

将 Dazuko 模块的副本放在为内核模块保留的以下任一目录中：

```
/lib/modules
```

或

```
/modules
```

使用内核实用程序 'depmod' 和 'modprobe'（对于 BSD OS，使用 'kldconfig' 和 'kldload'）处理依赖项并成功初始化新添加的 Dazuko 模块。

在 scep_daemon 初始化脚本 '/etc/init.d/scep_daemon' 中的后台程序初始化声明前插入以下语句：

```
/sbin/modprobe dazuko
```

对于 BSD OS，行

```
/sbin/kldconfig dazuko
```

必须插入在 '/usr/local/etc/rc.d/scep_daemon.sh' 脚本中。

警告 完全按照给定顺序执行这些步骤非常重要。如果内核模块不在内核模块目录中，将不会正确加载，导致系统挂起。

使用预加载 LIBC 库的实时防护

在前面的章节中，我们介绍了 Dazuko 支持的实时防护与 Linux/BSD 文件系统服务的集成。不是所有情况下都适合使用 Dazuko，包括以下情况下维护关键系统的系统管理员：

- 与运行内核有关的源代码和 /或配置文件不可用，
- 内核更多倾向单片集成，而不是模块化，
- Dazuko 模块不支持给定操作系统。

在任意这些情况下，应使用基于预加载 LIBC 库的自动扫描技术。参见本节以下主题了解详细信息。请注意本节只与 Linux OS 用户有关，包含使用预加载库 *'libscep_pac.so'* 的自动扫描程序的操作、安装和配置信息。

工作原理

实时防护 *libscep_pac.so* (SCEP Preload library based file Access Controller) 是在系统开机时启动的共享对象库。此库供文件系统服务器（如 FTP 服务器、Samba 服务器等）用于 LIBC 调用。根据可执行文件访问事件类型扫描每个文件系统对象。当前版本支持以下事件类型：

Open 事件

如果 *'open'* 字样位于 esest.cfg 文件（**[fac]** 部分）的 *'event_mask'* 参数中，则启动此文件访问类型。

Close 事件

如果 *'close'* 字样位于 scep.cfg 文件（**[fac]** 部分）的 *'event_mask'* 参数中，则启动此文件访问类型。在此情况下，拦截 LIBC 的所有文件描述符和文件流关闭功能。

Exec 事件

如果 *'exec'* 字样位于 scep.cfg (**[fac]** 部分）的 *'event_mask'* 参数中，则启动此文件访问类型。在此情况下，拦截 LIBC 的所有可执行功能。

SCEP 后台程序扫描所有打开、关闭和执行的文件中是否存在病毒。根据扫描结果，拒绝或允许对给定文件的访问。

安装和配置

libscep_pac.so 库模块使用预加载库的标准安装机制进行安装。您需要用指向 *libscep_pac.so* 库的绝对路径定义环境变量 *'LD_PRELOAD'*。有关更多信息，请参考 *ld.so(8)* 主页。

注意： 务必注意，*'LD_PRELOAD'* 环境变量只对将在实时防护控制下的网络服务器后台程序进程（ftp、Samba 等）定义。通常不建议对所有操作系统进程进行预加载 LIBC 调用，因为这样会显著降低系统性能或甚至导致系统挂起。从这个角度来说，不应使用 '/etc/ld.so.preload' 文件，或将 'LD_PRELOAD' 环境变量全局导出。两者都会覆盖所有相关 LIBC 调用，导致系统在初始化时挂起。

为确保仅拦截给定文件系统中的相关文件访问调用，使用下面一行可以覆盖可执行语句：

```
LD_PRELOAD=@LIBDIR@/libscep_pac.so COMMAND COMMAND-ARGUMENTS
```

其中 'COMMAND COMMAND-ARGUMENTS' 是原始可执行语句。

检查并编辑 SCEP 配置文件 (scep.cfg) 的 **[global]** 和 **[fac]** 部分。要使自动扫描程序正确工作，您必须定义需要在预加载库控制下的文件系统对象（即目录和文件）可以通过在 SCEP 配置文件的 **[fac]** 部分中定义 *'ctl_incl'* 和 *'ctl_excl'* 选项的参数来实现这一点。更改 scep.cfg 文件后，您可以重新加载 SCEP 后台程序，强制重新读取新创建的配置。

提示

要在文件系统启动后立刻启动实时防护，必须在相应网络文件服务器初始化脚本中定义 *'LD_PRELOAD'* 环境变量。

示例 假定我们希望自动扫描程序在启动 Samba 服务器后立刻监视所有文件系统访问事件。在 Samba 后台程序初始化脚本 (/etc/init.d/smb) 中，我们将语句

```
daemon /usr/sbin/smbd $SMBDOPTIONS
```

替换为下面一行：

```
LD_PRELOAD=@LIBDIR@/libscep_pac.so daemon /usr/sbin/smbd $SMBDOPTIONS
```

这样，将在系统启动时扫描 Samba 控制的所选文件系统对象。

重要 SCEP 机制

处理对象策略

处理对象策略机制根据状态筛选扫描的对象。此功能以下面的配置选项为基础：

- action_av
- action_av_infected
- action_av_notscanned
- action_av_deleted

有关这些选项的详细信息，请参考 *scep.cfg(5)* 主页。

首先根据 *'action_av'* 选项的配置处理每个处理的对象。如果此选项设置 *'accept'*（或 *'defer'*? *'discard'*? *'reject'*），则接受（推迟、放弃、拒绝）该对象。如果选项设置为 *'scan'*，则扫描对象的病毒定义，如果 *'av_clean_mode'* 选项设置为 *'yes'*，则还清除对象。此外，考虑配置选项 *'action_av_infected'*? *'action_av_notscanned'* 和 *'action_av_deleted'* 以进一步评估对象处理。如果因这三个操作选项采取 *'accept'* 操作，则接受对象。否则拒绝对象。

用户特定配置

用户特定配置机制的用途是提供更高水平的自定义和功能。它允许系统管理员根据访问文件系统对象的用户定义 SCEP 病毒防护扫描程序参数。

scep.cfg(5) 主页提供该功能的详细书面。在本节中我们将仅提供用户特定配置的简短示例。

在此示例中，目的是使用 *scep_dac* 模块控制 ON_OPEN 和 ON_EXEC 对 /home 目录下装载的某个外部磁盘的访问事件。可以在 SCEP 配置文件的 **[fac]** 部分配置模块。参见下面：

```
[fac]
agent_type = "dazuko"
event_mask = "open"
ctl_incl = "/home"
action_av = "scan"
```

要为单个用户指定扫描设置，*'user_config'* 参数必须指定将存储个人扫描规则的特殊配置文件名。在此处显示的示例中，特殊配置文件称为 *'scep_dac_spec.cfg'*，位于 SCEP 配置目录中（此目录基于您的操作系统。请参见术语与缩写页）。

```
[fac]
agent_type = "dazuko"
event_mask = "open"
ctl_incl = "/home"
action_av = "scan"
user_config = "scep_dac_spec.cfg"
```

在 **[fac]** 部分中指定 *'user_config'* 文件参数后，必须在 SCEP 配置目录中创建 *'scep_dac_spec.cfg'* 文件。最后添加所需的扫描规则。

```
[username]
action_av = "reject"
```

在特殊部分的顶部，输入将应用个人规则的用户名。此配置将允许所有其他尝试访问文件系统的用户正常处理，即将扫描其他用户访问的所有系统对象中的渗透，但用户 *'username'* 除外，将拒绝（阻止）他的访问。

计划任务

计划任务的功能包括在指定时间或指定事件时运行计划的任务，用预定义的配置和属性管理和启动任务等。任务配置和属性可以用于影响启动日期和时间，也可以通过在任务执行时引入自定义配置文件使用，扩展任务的应用。

'scheduler_tasks' 选项默认备注，导致应用默认计划任务配置。在 SCEP 配置文件中，所有参数和任务用分号分隔。任何其他分号（和反斜杠）必须用反斜杠进行转义。每个任务具有 6 个参数，语法如下：

- id - 唯一标识符。
- name - 任务说明。
- flags - 这是可以设置用于禁用指定计划任务的特殊标志。
- failstart - 指示在计划日期无法运行任务时如何操作。
- datespec - 常规日期指定，具有 6 个（crontab 类似年扩展）字段，重复日期或事件名称选项。
- command - 可以是命令的绝对路径，后接参数或具有 @' 前缀的特殊命令名称（例如病毒防护更新： *@update*).

```
#scheduler_tasks = "id;name;flags;failstart;datespec;command;id2;name2;...";
```

可以使用以下事件名称代替 datespec 选项：

- start - 后台程序启动。
- startonce - 后台程序每天最多启动一次。
- engine - 成功引擎更新。
- login - Web 界面登录启动。
- threat - 检测到威胁。
- notscanned - 未扫描的文件。

要显示当前计划任务配置，请使用 Web 界面或运行以下命令：

```
cat @ETCDIR@/scep.cfg | grep scheduler_tasks
```

有关计划任务及其参数的完整说明，请参考 *scep_daemon(8)* 主页的计划任务部分。

Web 界面

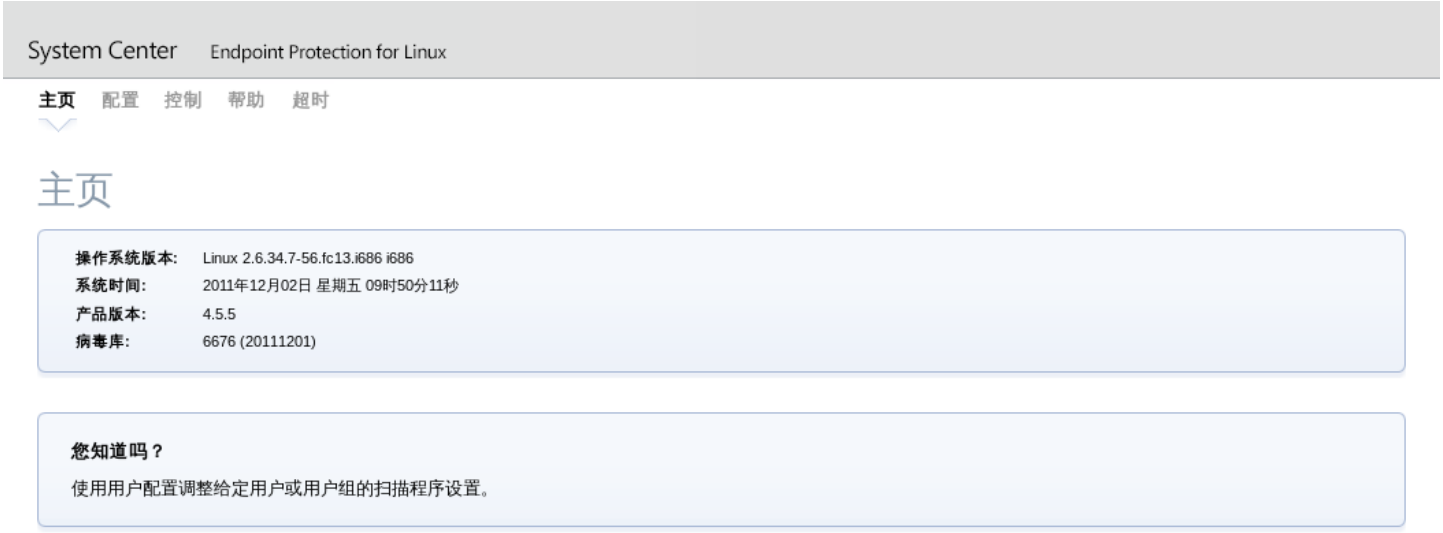
Web 界面允许用户友好地配置和管理 SCEP 安全系统。此模块是一个单独代理，必须明确启用。要快速配置 *Web 界面*，请设置 SCEP 配置文件中的以下选项并重新启动 SCEP 后台程序：

```
[wwwi]
agent_enabled = yes
listen_addr = address
listen_port = port
username = name
password = pass
```

将斜体文本替换为您自己的值，并将浏览器指向 *'https://address:port'*（注意是 https）。用 *'username/password'* 登录。帮助页面中可找到基本使用说明，*scep_wwwi* 的技术详细信息可在 *scep_wwwi(1)* 主页中找到。

Web 界面允许您远程访问 SCEP 后台程序并轻松部署。此功能强大的实用程序方便读写配置值。

图 6-1. System Center Endpoint Protection - 主屏幕。



System Center Endpoint Protection 的 Web 界面窗口分为两个主要部分。主窗口，用于显示所选菜单选项和主菜单的内容。顶部的水平条用于在以下主要选项之间浏览：

- **主屏幕** - 提供基本系统和 Microsoft 产品信息
- **配置** - 可以在这里更改 System Center Endpoint Protection 系统配置
- **控制** - 允许您运行简单任务和查看关于 scep_daemon 处理的对象的全局统计信息。
- **帮助** - 提供 System Center Endpoint Protection Web 界面的详细使用说明
- **注销** - 用于结束当前会话

重要信息： 确保在对 Web 界面的**配置**部分进行任何更改后单击**保存更改**按钮以保存您的新设置。要应用设置，需要单击左窗格的**应用更改**重新启动 SCEP 后台程序。

实时防护配置示例

配置 SCEP 有两种方法。在我们的示例中，我们将演示如何使用它们设置 Access Controller 模块，使用预加载的 LIBC 库的实时防护一章中对此有所介绍。您可以选择最适合的选项。

- 使用 SCEP 配置文件：

```
[fac]
agent_type = "preload"
event_mask = "open"
ctl_incl = "/home"
action_av_deleted = "reject"
action_av = "scan"
action_av_infected = "reject"
```

- 使用 Web 界面：

图 6-3. SCEP - 配置 > 自动扫描程序。

更改 Web 界面中的设置时，始终记住单击**保存更改**保存您的配置。要应用新更改，请单击**配置**部分面板中的**应用更改**。

手动扫描程序

本节包含一个关于如何使用手动扫描程序扫描病毒的示例：

- 导航至**控制 > 手动扫描**
- 输入要扫描的目录路径
- 单击**扫描文件**按钮执行命令行扫描程序

图 6-4. SCEP - 控制 > 手动扫描程序。

Microsoft 命令行扫描程序将自动在后台运行。要查看扫描进度，请单击**查看**链接。将打开一个新浏览器窗口。

计划任务

您可以通过 SCEP 配置文件（参见章节计划任务）或使用 Web 界面管理计划任务。

图 6-5. SCEP - 全局 > 计划任务。

单击复选框启用 禁用计划任务。默认显示以下计划任务：

- **日志维护** - 程序自动删除旧的日志以节省硬盘空间。计划任务将开始整理日志碎片。此过程中将删除所有空白日志条目。这样将提高处理日志时的速度。尤其在日志包含大量条目数时，可以感受到这种提高。
- **启动文件检查** - 成功更新病毒库后扫描内存和运行的服务。
- **每周扫描** - 每周一次扫描整个文件系统（默认周一早上 2:00）。用户可以自定义此任务。
- **定期自动更新** - 定期更新 System Center Endpoint Protection 是保持计算机最高安全级别的最佳方法。参见 SCEP 更新工具了解更多信息。
- **威胁通知** - 默认每个威胁将记录在 syslog 中。此外，可以配置 SCEP 运行外部（通知）脚本，通过电子邮件通知系统管理员威胁检测。

统计信息

您可以在这里查看所有活跃 SCEP 代理的统计信息。**统计信息**总结每 10 秒刷新一次。

图 6-6. SCEP - 控制 > 统计信息。

日志记录

：

SCEP 通过 syslog 记录系统后台程序日志。*Syslog* 是记录程序消息的标准，可以用于记录网络和安全事件等系统事件。

消息指向工具：

```
auth, authpriv, daemon, cron, ftp, lpr, kern, mail, ..., local0, ..., local7
```

消息发件人为消息分配优先级 级别：

```
Error, Warning, Summall, Summ, Partall, Part, Info, Debug
```

本节介绍如何配置和读取 syslog 的日志记录输出。*'syslog_facility'* 选项（默认值 *'daemon'*）定义用于日志记录的 syslog 工具。要修改 syslog 设置，请编辑 SCEP 配置文件或使用 Web 界面。修改 *'syslog_class'* 参数值以更改日志记录类别。我们建议仅当您熟悉 syslog 时修改这些设置。有关 syslog 配置示例，参见下文：

```
syslog_facility = "daemon"
syslog_class = "error:warning:summall"
```

日志文件的名称和位置取决于 syslog 安装和配置（例如 rsyslog、syslog-ng 等）。syslog 输出文件的标准文件名示例包括 *'syslog'*？ *'daemon.log'* 等。要跟踪 syslog 活动，在控制运行以下命令：

```
tail -f /var/log/syslog
tail -100 /var/log/syslog | less
cat /var/log/syslog | grep scep | less
```

重要信息 必须先在 SCEP 配置文件中或通过 SCEP Web 界面启用使用 System Center Operations Manager 监测 Linux SCEP 产品，才能正常工作。请确保上述配置文件中的 *'scom_enabled'* 参数设置为 *'scom_enabled = yes'*，或在 Web 界面的 **配置** > **全局** > **后台程序选项** > **启用 SCOM** 下更改相应设置。

SCEP Security 系统更新

SCEP 更新实用程序

为保持 System Center Endpoint Protection 的效果，病毒库必须保持是最新的。*scep_update* 实用程序专为此用途开发。参见 *scep_update(8)* 主页了解详细信息。如果服务器通过 HTTP 代理服务器访问 Internet，还必须额外定义配置选项 *'proxy_addr'*? *'proxy_port'*。如果访问 HTTP 代理服务器需要用户名和密码，必须在此部分中定义 *'proxy_username'* 和 *'proxy_password'* 选项。要启动更新，请输入以下命令：

@SBINDIR@/scep_update

为了给最终用户提供最高安全水平，Microsoft 团队不断从世界各地收集病毒定义文件 -以极短间隔向病毒库加入新模式。因此，我们建议定期启动更新。要指定更新频率，您需要在 SCEP 配置文件的 **[global]** 部分配置 *'scheduler_tasks'* 选项的 *'@update'* 任务。您也可以使用计划任务设置更新频率。SCEP 后台程序必须启动和运行才能成功更新病毒库。

SCEP 更新过程说明

更新过程包含两个阶段：首先从 Microsoft 服务器下载预编译的更新模块。

更新过程的第二个阶段是编译本地镜像中存储的可供 System Center Endpoint Protection 扫描程序加载的模块。通常创建以下 SCEP 加载模块：加载程序模块 (em000.dat)、扫描程序模块 (em001.dat)、病毒库模块 (em002.dat)、压缩文件支持模块 (em003.dat)、高级启发式扫描模块 (em004.dat) 等。模块在以下目录中创建：

@BASEDIR@

告诉我们

我们希望本指南帮助您彻底了解 System Center Endpoint Protection 安装、配置和维护的要求。但我们的目标是持续提高文档的质量和效率。如果您认为本指南中任何章节不清楚或不完整，请联系客户支持部门告诉我们：

support.microsoft.com

我们致力于提供最高水平支持，并希望在您遇到本产品任何问题时帮助您。

附录 A. PHP 许可证

Redistribution and use in source and binary forms, with or without modification, is permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. The name "PHP" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact group@php.net.
4. Products derived from this software may not be called "PHP", nor may "PHP" appear in their name, without prior written permission from group@php.net. You may indicate that your software works in conjunction with PHP by saying "Foo for PHP" instead of calling it "PHP Foo" or "phpfoo"
5. The PHP Group may publish revised and/or new versions of the license from time to time. Each version will be given a distinguishing version number. Once covered code has been published under a particular version of the license, you may always continue to use it under the terms of that version. You may also choose to use such covered code under the terms of any subsequent version of the license published by the PHP Group. No one other than the PHP Group has the right to modify the terms applicable to covered code created under this License.
6. Redistributions of any form whatsoever must retain the following acknowledgment: "This product includes PHP software, freely available from <http://www.php.net/software/>".

THIS SOFTWARE IS PROVIDED BY THE PHP DEVELOPMENT TEAM "AS IS" AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE PHP DEVELOPMENT TEAM OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.