思科安全管理器 4.7 版本说明

最初发布日期：2014 年 8 月 21 日
最后更新日期：2016 年 3 月 30 日

安全管理器 4.7 现已推出。SMARTnet 注册用户转至 http://www.cisco.com/go/csmanager，在“支持”(Support) 下点击**下载此产品的软件 (Download Software for this Product)** 即可从思科支持网站上获取 4.7 版本。

本文档包含以下主题：

简介

注 请将本文档与产品文档，第 27 页中指出的文档结合使用。另外，用户文档的在线版本在初始发布后有时会有更新。因此，如果 Cisco.com 上的思科安全管理器最终用户指南中包含的信息与产品上下文相关帮助中包含的任何信息不一致，应以前者为准。

本文档包含以下产品的版本说明信息：

- **思科安全管理器 4.7** - 您可以利用思科安全管理器管理思科安全设备上的安全策略。安全管理器支持集中调配防火墙、VPN 和 IPS 服务，范围覆盖 IOS 路由器、PIX 和 ASA 安全设备、IPS 传感器和模块、Catalyst 6500 和 7600 系列 ASA 服务模块 (ASA-SM)，以及 Catalyst 交换机和部分路由器的许多其他服务模块。（要查看完整设备支持信息，请转至 Cisco.com 参阅思科安全管理器兼容性信息。）另外，安全管理器还支持调配许多针对特定平台的设置，例如接口、路由、身份、QoS、日志记录等。

  从仅有几台设备的小型网络到容纳数千台设备的大型网络，安全管理器均可高效地管理各种规模的网络。安全管理器之所以能实现这样的可扩展性，是因为在设备分组能力方面拥有丰富的功能集合，以及拥有可共享的对象和政策。

- **Auto Update Server 4.7** - Auto Update Server (AUS) 是一个用于升级 PIX 安全设备软件映像、ASA 软件映像、PIX 设备管理器 (PDM) 映像、自适应安全设备管理器 (ASDM) 映像，以及 PIX 安全设备和 ASA 配置文件的工具。使用自动更新功能，并且采用动态 IP 地址的安全设备会定期连接 AUS，以升级设备配置文件和传送设备与状态信息。

注 在使用思科安全管理器 4.7 之前，我们建议您先通读本文档。另外，在安装思科安全管理器 4.7 之前，请务必先阅读重要说明，第 11 页、安装说明，第 6 页和 *“Installation Guide for Cisco Security Manager 4.7”*（思科安全管理器 4.7 安装指南）。

本文档中列出了可能对产品操作产生影响的问题的 ID 号码和标题。另外，本文档中还列出了一些已解决的问题。如果您在 Cisco.com 上访问本文档，则点击任何 ID 号码即可转至思科缺陷搜索工具 (BST) 中的版本说明文档。版本说明文档中包含问题的症状、状态和解决办法信息。

支持的组件版本和相关软件

思科安全管理应用套件包含许多组件应用，以及一些可与组件应用结合使用的相关应用。下表列出了组件应用、相关应用，以及这些应用可以与此版本套件配合使用的版本。有关这些应用的说明，请参阅 *“Installation Guide for Cisco Security Manager 4.7”*（思科安全管理器 4.7 安装指南）。

注 有关可以使用思科安全管理器管理的受支持软件和硬件的详情，请转至 Cisco.com，参阅思科安全管理器兼容性信息下的在线文档 *“Supported Devices and Software Versions for Cisco Security Manager”*（思科安全管理器支持的设备和软件版本）。

表 1　　受支持的组件应用和相关应用版本

应用	支持版本
组件应用	
思科安全管理器	4.7
自动更新服务器	4.7
CiscoWorks Common Services	4.2.2
相关应用	
Cisco Security Monitoring, Analysis and Response System (CS-MARS)	6.0.7、6.1.1

表 1　　受支持的组件应用和相关应用版本（续）

应用	支持版本
适用于 Windows 的思科安全访问控制服务器 (ACS) **说明** • 也支持思科安全 ACS 解决方案引擎 4.1(4)。 • 支持使用思科安全 ACS 5.x 进行身份验证。 • 您可以使用其他版本思科安全 ACS，不过要将它们配置为非 ACS TACACS+ 服务器。在 ACS 模式下配置服务器可提供精细控制，而非 ACS 配置则无法提供此种精细控制。	4.2(0)、5.x
思科配置引擎	3.5、3.5(1)

新增内容

思科安全管理器 4.7 服务包 3

安全管理器 4.7 服务包 3 修复了许多问题。有关详细信息，请参阅已解决的警告 - 版本 4.7 服务包 3，第 21 页。

除了解决下面列出的漏洞之外，此服务包还提供对互联网控制消息协议 (ICMP) 的 IPv6 支持和数据包跟踪器功能。

思科安全管理器 4.7 服务包 2

安全管理器 4.7 服务包 2 修复了许多问题。有关详细信息，请参阅已解决的警告 - 版本 4.7 服务包 2，第 22 页。

另外，该服务包还支持在运行 ASA 软件 8.2(2) 或更高版本的设备上将 IPv6 地址配置用作故障转移接口。

思科安全管理器 4.7 服务包 1

安全管理器 4.7 服务包 1 修复了许多问题。有关详细信息，请参阅已解决的警告 - 版本 4.7 服务包 1，第 22 页。

此服务包还支持以下内容：

- ASA 软件版本 9.2(3)
- ISE 版本 1.3
- TLS 版本 1.2

思科安全管理器 4.7

除了已经解决的警告问题之外，本版本还包含以下新功能和增强功能：

- 支持更多设备（有关兼容性的详细信息，请参阅 *“Supported Devices and Software Versions for Cisco Security Manager 4.7”* [思科安全管理器 4.7 支持的设备和软件版本]）：
  - ASA 9.1(5)、ASA 9.2(1)、ASA 9.2(2) 和 ASA 9.3(1)
  - ASA 9.2(1)+ 上的思科虚拟安全设备 (ASAv)
  - IPS 7.3(2)

- 为安装了 FirePOWER 模块的 ASA 交叉启动至 FireSIGHT 管理中心。除了 Prime 安全管理器外，单点登录配置的 GUI 元素现在扩展至 FireSIGHT 管理中心。
- 支持检测 ASA 设备上安装的 ASA FirePOWER 模块。
- 安全管理器 4.7 版本中首次推出了新带外重新同步工具，能够帮助您重新同步或协调带外数据。该带外重新同步工具是对安全管理器 4.6 及更早版本中带外检测工具的扩展，4.7 版本保留了这一工具。带外重新同步工具的作用是，自动执行将设备上的带外数据传入安全管理器安装这一流程，同时保留您之前建立的策略结构。
- 在“报告管理器”(Report Manager) 内，“系统报告”(System Reports) >“VPN”文件夹中新增了“连接配置文件报告”(Connection Profile Report)。
- 另外，“报告管理器”(Report Manager) 内的“用户名”(Username) 过滤器现在支持区分大小写，并且可以使用通配符和执行“NOT”运算。
- “精简诊断”(Light Diagnostics) 支持 - 自 4.7 版本起，安全管理器开始支持一种新的精简诊断变体；这种“精简诊断”(Light Diagnostics) 变体只收集基本信息；因此，诊断文件变得更小，诊断速度变得更快。在 4.7 版本中，现有的“一般诊断”(General Diagnostics) 变体与在 4.6 版本及更早版本中相同。
- “共享策略分配”设备过滤器 - 在 4.7 版本中，思科安全管理器为“设备过滤器”(Device Filter) 添加了一个新的可用过滤选项。利用这个新选项，可以过滤应用了共享策略的设备。
- 在安全管理器 4.6 及更早版本的“运行状况与性能监控器”(Health and Performance Monitor) 中，当为 ASA、IPS 和 VPN 生成 HPM 警报时，系统会向用户发送邮件通知。此框架在 4.7 版本中得到增强，它还会发送 SNMP 陷阱通知。
- 具有写入权限的 API 现已推出。要了解此 API 的规格，请参阅 http://www.cisco.com/c/en/us/support/security/security-manager/products-user-guide-list.html。
- 从版本 4.7 开始，虚拟自适应安全设备（虚拟 ASA）可支持安全管理器提供的所有 VPN 功能。
- 加密图 - 自版本 4.7 开始，安全管理器允许在 VPN 拓扑中为每台对等设备手动配置加密图名称和加密 ACL 名称。此功能仅在规则 IPsec 拓扑中受支持。
- 支持 ASA 版本 9.2.1 - 在安全管理器 4.7 中，您可以允许部分无客户端 SSL VPN 和 AnyConnect 用户不必在 VPN 隧道组中运行思科安全桌面软件。
- 支持 ASA 版本 9.3.1 自定义策略属性 - 安全管理器 4.7 能够在动态接入策略中配置自定义属性。AnyConnect 自定义属性支持 ASA 为添加新客户端控制项提供通用支持，而无需对 ASA 软件进行升级，从而加快新终端功能的交付和部署速度。从版本 4.7 开始，安全管理器允许您为现有自定义属性类型添加自定义属性数据。
- 支持 AnyConnect 版本 3.2 - 安全管理器版本 4.7 为 AnyConnect 版本 3.2 中的 ISE 安全评估提供支持。您可以使用 ISE 编辑器配置 ISE 配置文件。
- 在安全管理器版本 4.7 中，您可以创建智能隧道网络对象，并定义是通过隧道传输所有流量，还是允许或禁止通过特定网络传输流量。
- 利用安全管理器版本 4.7，您可以定义一个用于从证书映射用户名的脚本。此映射用于指定数字证书中供提取用户名之用的字段。您可以指定脚本参数，也可以配置自定义 LUA 脚本。
- 安全管理器版本 4.7 填补了动态接入策略中的空白，所支持的一些功能可以与自适应安全设备管理器软件和托管设备提供的功能相当。在此版本中，得到增强的属性包括 AAA、LDAP、Device、File、Always-on VPN 和 Session Action 属性。
- 安全管理器版本 4.7 填补了以下组策略空白：
  - 允许 AnyConnect 在用户登录计算机后立即自动建立 VPN 会话。
  - 允许在连接至公司网络时按需要配置最终用户的浏览器的代理设置，并在断开连接后自动恢复为原始配置。

- 支持在 ASA 9.2(1)+ 上使用边界网关协议 (BGP)。BGP 是一种自治系统间路由协议。BGP 用于交换互联网的路由信息，并且是互联网运营商 (ISP) 之间所使用的协议。

  对于 ASA 9.3(1)+，BGP 在 L2（EtherChannel 类型）和 L3（单个接口类型）集群模式下受支持。

- 支持以下 ASA 路由策略对象：路由映射、策略列表、前缀列表、AS 路径和社区列表。

注 对于安全管理器 4.7，路由映射对象只能与 BGP、OSPF 和 OSPFv3 路由协议配合使用。

- 对于 ASA 9.2(1)+，OSPF 现在支持 Fast Hello 数据包功能，从而形成在 OSPF 网络中实现更快融合的配置。
- 对于 ASA 9.2(1)+，OSPF 接口间隔和虚拟链路间隔值的有效范围已更新。
- 对于 ASA 9.2(1)+，添加了新 OSPF 计时器；弃用了旧 OSPF 计时器。
- 对于 ASA 9.2(1)+，现在支持使用 ACL 过滤路由。
- 对于 ASA 9.2(1)+，添加了 OSPF 重新分发功能。
- 支持静态 Null0 路由配置。静态 Null0 路由用于将不必要或不想要的流量转发到黑洞。
- 对于 ASA 9.3(1)+，为 BGP、OSPFv2 和 OSPFv3 添加了对不间断转发的支持。
- 支持在 ASA 9.2(1)+ 上使用嵌入式事件管理器 (EEM)。EEM 功能使您可以调试问题并提供用于故障排除的通用日志记录。EEM 通过执行操作对 EEM 系统中的事件作出响应。其中涉及两个组件：EEM 触发的事件；用于定义操作的事件管理器小应用程序。您可以为每个事件管理器小应用程序添加多个事件，从而触发小应用程序调用配置的操作。
- 对于 ASA 9.2(1)+ 上的 AAA 服务器组，支持 RADIUS 动态授权变更 (CoA) 服务。
- 在 ASA 9.2(1)+ 设备上使用 RADIUS 协议时，您可以允许生成 RADIUS interim-accounting-update 消息。目前，仅当 VPN 隧道连接添加至无客户端 VPN 会话时，才会生成这些消息。发生此情况时，将生成记帐更新，以便将新分配的 IP 地址通知给 RADIUS 服务器。
- 在 ASA 9.2(1)+ 设备上使用 RADIUS 协议时，您可以为 RADIUS 服务器组启用“仅授权”模式。启用此模式后，为各台 AAA 服务器配置的通用密码将不再是必需的，您可以不配置该密码。
- 对于运行 9.1(5) 或更高版本的 ASA 设备，您现在最多可以配置 128 台 SNMP 主机。
- 添加了对启用 EXEC shell 访问授权的支持。
- 添加了对自动启用 AAA 授权的支持。有足够授权权限的管理员可以通过输入自己的身份验证凭证一次进入特权 EXEC 模式。
- 从 ASA 9.1(5) 开始，您可以将规则引擎配置为在实施规则更改时使用交易模式。在交易模式中，在编译并准备好使用新规则之前，ASA 可以继续使用旧规则。使用交易模式时，性能不应在规则编译期间降低。您可以为访问组规则、NAT 规则启用交易模式或为两者均启用交易模式。
- 在 ASA 9.1(5)+ 中支持 URL 规范化。URL 规范化是包括路径规范化、大小写规范化和方案规范化在内的一项额外安全功能。系统在比较 URL 之前，会先对在 ACE 和门户地址栏中指定的 URL 进行规范化；在过滤 webvpn 流量时，会以规范化 URL 比较结果为依据。
- 您可以使用“CLI 提示”(CLI Prompt) 页面自定义 ASA 7.2(1)+ 设备在 CLI 会话期间使用的提示。
- 支持对重新定向至安装于 ASA 中的 FirePOWER 模块的流量进行配置。仅适用于使用版本 9.2(1)+ 的 ASA 55xx-X 设备。
- 支持挂载点。挂载点让安全设备可访问通用互联网文件系统 (CIFS) 或文件传输协议 (FTP)。
- 支持配置虚拟 HTTP 服务器和虚拟 Telnet 服务器。

- 有些交换机不支持 LACP 动态端口优先级（活动链路和备用链路）。从 ASA 9.2(1) 开始，您可以禁用动态端口优先级，使跨网络 EtherChannel 具有更高兼容性。
- 对于 ASA 9.2(1)+，EtherChannel 现在最多可支持 16 条活动链路。

安装说明

有关具体安装说明和客户端与服务器要求方面的信息，请参阅 *“Installation Guide for Cisco Security Manager 4.7”*（思科安全管理器 4.7 安装指南）。在安装思科安全管理器 4.7 之前，请务必阅读本节列出的说明以及重要说明，第 11 页。

- 您可以根据安装指南中“Licensing”（许可）一章的内容确定自己所需的许可证。（需要怎样的许可证取决于您要执行是全新安装，还是从某个旧版本升级。）该章还包含对各种可用许可证（例如，标准、专业和评估版本许可证）的介绍。本章网址为：http://www.cisco.com/c/en/us/td/docs/security/security_management/cisco_security_manager/security_manager/4-7/installation/guide/IG/licensing.html。
- STD-TO-PRO（标准至专业）升级会将 ST25 许可证转换为 PRO50 许可证，从而能够为 50 台设备提供支持。若要为更多设备提供支持，您需要购买必要的增量许可证。
- 思科从安全管理器版本 4.7 开始为 API 提供临时许可证。
- 从安全管理器版本 4.7 开始，您可以为安全管理器许可证的评估版本应用增量许可证。
- 请勿修改在产品安装期间建立的 casuser（默认服务帐户）或目录权限。进行上述修改会导致您无法执行以下操作：
  - 登录 Web 服务器
  - 登录客户端
  - 成功备份所有数据库
- 有关服务器要求、服务器配置和安装后任务方面的重要信息，请参阅 *“Installation Guide for Cisco Security Manager 4.7”*（思科安全管理器 4.7 安装指南）。
- 另外，*“Installation Guide for Cisco Security Manager 4.7”*（思科安全管理器 4.7 安装指南）还提供与操作系统和浏览器支持相关的重要信息。以下几条列出了在这方面最重要的新支持信息。
- 服务器设备支持的操作系统如下：
  - Microsoft Windows Server 2008 R2 with SP1 Enterprise - 64 位
  - Microsoft Windows Server 2012 Standard - 64 位
  - Microsoft Windows Server 2012 Datacenter - 64 位
- 客户端设备支持的操作系统如下：
  - Microsoft Windows 7 SP1 Enterprise - 64 位和 32 位
  - Microsoft Windows 8.1 Enterprise Edition - 64 位和 32 位
  - Microsoft Windows Server 2008 R2 with SP1 Enterprise - 64 位
  - Microsoft Windows Server 2012 Standard - 64 位
  - Microsoft Windows Server 2012 Datacenter - 64 位
- 服务器设备和客户端设备支持的浏览器相同，具体如下：
  - Internet Explorer 8.x、9.x 或 10.x（但仅限兼容性视图）
  - 支持 Firefox 15.0.1 及更高版本（推荐）

- 您可以直接安装安全管理器服务器软件，也可以在安装了安全管理器的服务器上升级软件。本版本产品的 *"Installation Guide for Cisco Security Manager"*（思科安全管理器安装指南）介绍了支持对哪些旧版本安全管理器进行升级，并提供了与服务器要求、服务器配置和安装后任务相关的重要信息。
- 您必须先确保安全管理器数据库中不包含任何待处理数据（也就是说，尚未提交至数据库的数据），然后才能成功从旧版本安全管理器升级至安全管理器 4.7。如果安全管理器数据库中包含待处理数据，您必须在执行之前提交或舍弃所有未提交的更改，然后对数据库进行备份。本版本产品的 *"Installation Guide for Cisco Security Manager"*（思科安全管理器安装指南）包含对数据库执行升级准备工作的完整步骤说明。
- 我们不支持在运行任何其他 Web 服务器或数据库服务器（例如，IIS 或 MS-SQL）的服务器上安装安全管理器。如果您执意在上述服务器上安装安全管理器，可能会因非预期错误导致无法登录或使用思科安全管理器。
- 在升级之前，请注意以下重要事项：
  - 确保您要升级的所有应用目前均运行正常，并且您可以创建有效备份（即可正常完成备份流程且备份期间不出现任何错误）。如果应用在升级前运行不正常，则在升级后也可能无法正常运行。

注 思科注意到，有些用户对系统进行了不正规且不受支持的修改，从而导致备份流程未能备份已安装的所有 CiscoWorks 应用。安装指南中记载的升级流程假设您未破坏系统的预期功能。如果您要创建的备份不能涵盖所有数据，则在执行更新之前，您有责任确保已掌握所需的所有备份数据。我们强烈建议您撤消这些不受支持的修改。否则，您最好不要尝试进行将产品与旧版本安装到相同服务器上的内嵌升级；正确做法是将更新的应用安装到全新的"干净"服务器上并恢复数据库备份。

- 如果您登录的安全管理器服务器的版本比您运行的客户端高，则系统会显示一条通知并为您提供下载相应客户端版本的选项。
- 从安全管理器 4.4 开始，AUS 和安全管理器以并行方式安装，从而加快安装速度。
- 在您安装安全管理器或 AUS 时，系统会自动安装 CiscoWorks Common Services 4.2.2。
- 当出现任何数据库迁移错误时，系统会弹出错误消息；出现这种情况时，安装可在不停止的情况下继续进行。
- 为取得最佳性能，建议以 50 GB 的磁盘大小增加幅度解除磁盘分区。

注意 不过，频繁解除分区可能会造成坏扇区，最终导致磁盘故障。

- 从版本 4.4 开始，安全管理器在服务器安装程序中添加了 Windows 防火墙配置脚本。此脚本能够自动执行打开和关闭必要端口的过程，从而确保 Windows 防火墙工作的准确性和安全性；采用此脚本的目的在于增强安全管理器服务器的稳健性。

服务包 1 下载和安装说明

要下载和安装服务包 1，请按以下步骤操作：

注 在应用此服务包之前，您必须先在服务器上安装思科安全管理器 4.7 FCS 版本。

注意 在安装此服务包之前，请先备份以下文件：

MDC\ips\etc\sensorupdate.properties
MDC\eventing\config\communication.properties

如果您之前修改过这些文件，则安装完服务包后应重新配置这些文件。

步骤 1 转到 http://www.cisco.com/go/csmanager，然后在屏幕右侧的“支持”(Support) 标题下点击**下载此产品的软件 (Download Software for this Product)**。

步骤 2 输入用户名和密码，登录 Cisco.com。

步骤 3 在最右侧一列中点击**安全管理器 4.7 (Security Manager 4.7)**。

步骤 4 点击**安全管理器 (CSM) 软件 (Security Manager [CSM] Software)**，然后在**最新 (Latest)** 下点击 **4.7sp1**。

步骤 5 下载文件 fcs-csm-470-sp1-win-k9.exe。

步骤 6 要安装服务包，请关闭所有打开的应用（包括思科安全管理器客户端）。

步骤 7 如果服务器上已安装思科安全代理，应依次点击**开始 > 设置 > 控制面板 > 管理工具 > 服务**，然后手动停止思科安全代理服务。

步骤 8 运行先前下载的 fcs-csm-470-sp1-win-k9.exe 文件。

步骤 9 在“安装思科安全管理器 4.7 服务包 1”(Install Cisco Security Manager 4.7 Service Pack 1) 对话框中，点击**下一步 (Next)**，然后在下一屏中点击**安装 (Install)**。

步骤 10 安装完更新的文件后，点击**完成 (Finish)** 以完成安装。

步骤 11 在用于连接安全管理器服务器的每台客户端设备上，您必须先通过执行以下步骤来应用服务包，才能使用该客户端连接服务器：

a. 如果客户端上已安装思科安全代理，应依次点击**开始 > 设置 > 控制面板 > 管理工具 > 服务**，然后手动停止思科安全代理服务。

b. 启动安全管理器客户端。

系统将提示您“下载服务包”(Download Service Pack)。

c. 下载服务包，然后启动下载的文件以应用服务包。

步骤 12 （可选）转到客户端安装目录并清空缓存，例如 <客户端安装目录>/cache。

步骤 13 （可选）为 Open SSL 配置 SSL 证书或自签证书：

a. 停止 CSM 后台守护程序服务 [net stop crmdmgtd]

b. 如果您已自己配置了 SSL 证书，可以按照以下链接中所述的步骤重新配置证书：

http://www.cisco.com/c/en/us/td/docs/net_mgmt/ciscoworks_lan_management_solution/4-2/user/guide/admin/admin/appendixcli.html#wp1016314

c. 对于自签证书，请利用命令提示符导航至 <CSCOpx>\MDC\Apache 目录，然后执行 gencert.bat 文件
（其中的 <CSCOpx> 是您的安装目录）

d. 启动 CSM 后台守护程序服务 [net start crmdmgtd]

服务包 2 下载和安装说明

要下载和安装服务包 2，请按以下步骤操作：

注 在应用此服务包之前，您必须先在服务器上安装思科安全管理器 4.7 FCS 版本。

注意 在安装此服务包之前，必须先备份以下文件：

MDC\ips\etc\sensorupdate.properties
MDC\eventing\config\communication.properties

如果您之前修改过这些文件，则安装完服务包后应重新配置这些文件。

注 在恢复数据库备份时，请不要在安装 4.7 SP2 过程中直接从安全管理器版本 4.7 或 4.7 SP1 版本恢复数据库备份。正确做法是，将数据库恢复至提取备份时所用的相应版本，然后安装版本 4.7 SP2。

步骤 1 转到 http://www.cisco.com/go/csmanager，然后在屏幕右侧的“支持”(Support) 标题下点击**下载此产品的软件 (Download Software for this Product)**。

步骤 2 输入用户名和密码，登录 Cisco.com。

步骤 3 在最右侧一列中点击**安全管理器 4.7 (Security Manager 4.7)**。

步骤 4 点击**安全管理器 (CSM) 软件 (Security Manager [CSM] Software)**，然后在**最新 (Latest)** 下点击 **4.7sp2**。

步骤 5 下载文件 fcs-csm-470-sp2-win-k9.exe。

步骤 6 要安装服务包，请关闭所有打开的应用（包括思科安全管理器客户端）。

步骤 7 如果服务器上已安装思科安全代理，应依次点击**开始 > 设置 > 控制面板 > 管理工具 > 服务**，然后手动停止思科安全代理服务。

步骤 8 运行先前下载的 fcs-csm-470-sp2-win-k9.exe 文件。

步骤 9 在“安装思科安全管理器 4.7 服务包 2”(Install Cisco Security Manager 4.7 Service Pack 2) 对话框中，点击**下一步 (Next)**，然后在下一屏中点击**安装 (Install)**。

步骤 10 安装完更新的文件后，点击**完成 (Finish)** 以完成安装。

步骤 11 在用于连接安全管理器服务器的每台客户端设备上，您必须先通过执行以下步骤来应用服务包，才能使用该客户端连接服务器：

a. 如果客户端上已安装思科安全代理，应依次点击**开始 > 设置 > 控制面板 > 管理工具 > 服务**，然后手动停止思科安全代理服务。

b. 启动安全管理器客户端。

系统将提示您“下载服务包”(Download Service Pack)。

c. 下载服务包，然后启动下载的文件以应用服务包。

步骤 12 （可选）转到客户端安装目录并清空缓存，例如 <客户端安装目录>/cache。

步骤 13 （可选）为 Open SSL 配置 SSL 证书或自签证书：

a. 停止 CSM 后台守护程序服务 [net stop crmdmgtd]

b. 如果您已自己配置了 SSL 证书，可以按照以下链接中所述的步骤重新配置证书：

http://www.cisco.com/c/en/us/td/docs/net_mgmt/ciscoworks_lan_management_solution/4-2/user/guide/admin/admin/appendixcli.html#wp1016314

c. 对于自签证书，请利用命令提示符导航至 <CSCOpx>\MDC\Apache 目录，然后执行 gencert.bat 文件
（其中的 <CSCOpx> 是您的安装目录）

d. 启动 CSM 后台守护程序服务 [net start crmdmgtd]

服务包 3 下载和安装说明

要下载和安装服务包 3，请按以下步骤操作：

注 在应用此服务包之前，您必须先在服务器上安装思科安全管理器 4.7 FCS 版本。

注意 在安装此服务包之前，必须先备份以下文件：

MDC\ips\etc\sensorupdate.properties
MDC\eventing\config\communication.properties

如果您之前修改过这些文件，则安装完服务包后应重新配置这些文件。

注 在恢复数据库备份时，请不要在安装 4.7 SP3 过程中直接从安全管理器版本 4.7 或 4.7 SP2 版本恢复数据库备份。正确做法是，将数据库恢复至提取备份时所用的相应版本，然后安装版本 4.7 SP3。

步骤 1 转到 http://www.cisco.com/go/csmanager，然后在屏幕右侧的“支持”(Support) 标题下点击**下载此产品的软件 (Download Software for this Product)**。

步骤 2 输入用户名和密码，登录 Cisco.com。

步骤 3 在最右侧一列中点击**安全管理器 4.7 (Security Manager 4.7)**。

步骤 4 点击**安全管理器 (CSM) 软件 (Security Manager [CSM] Software)**，然后在**最新 (Latest)** 下点击 **4.7sp3**。

步骤 5 下载文件 fcs-csm-470-sp3-win-k9.exe。

步骤 6 要安装服务包，请关闭所有打开的应用（包括思科安全管理器客户端）。

步骤 7 如果服务器上已安装思科安全代理，应依次点击**开始 > 设置 > 控制面板 > 管理工具 > 服务**，然后手动停止思科安全代理服务。

步骤 8 运行先前下载的 fcs-csm-470-sp3-win-k9.exe 文件。

步骤 9 在“安装思科安全管理器 4.7 服务包 3”(Install Cisco Security Manager 4.7 Service Pack 3) 对话框中，点击**下一步 (Next)**，然后在下一屏中点击**安装 (Install)**。

步骤 10 安装完更新的文件后，点击**完成 (Finish)** 以完成安装。

步骤 11 在用于连接安全管理器服务器的每台客户端设备上，您必须先通过执行以下步骤来应用服务包，才能使用该客户端连接服务器：

a. 如果客户端上已安装思科安全代理，应依次点击**开始 > 设置 > 控制面板 > 管理工具 > 服务**，然后手动停止思科安全代理服务。

b. 启动安全管理器客户端。

系统将提示您“下载服务包”(Download Service Pack)。

c. 下载服务包，然后启动下载的文件以应用服务包。

步骤 12 （可选）转到客户端安装目录并清空缓存，例如 <客户端安装目录>/cache。

步骤 13 （可选）为 Open SSL 配置 SSL 证书或自签证书：

a. 停止 CSM 后台守护程序服务 [net stop crmdmgtd]

b. 如果您已自己配置了 SSL 证书，可以按照以下链接中所述的步骤重新配置证书：

http://www.cisco.com/c/en/us/td/docs/net_mgmt/ciscoworks_lan_management_solution/4-2/user/guide/admin/admin/appendixcli.html#wp1016314

c. 对于自签证书，请利用命令提示符导航至 <CSCOpx>\MDC\Apache 目录，然后执行 gencert.bat 文件
（其中的 <CSCOpx> 是您的安装目录）

d. 启动 CSM 后台守护程序服务 [net start crmdmgtd]

重要说明

安全管理器 4.7 服务包 1

以下说明和修复适用于安全管理器 4.7 服务包 1 版本：

- 为遵守某些国家/地区的进口法规，Oracle 实施提供了一个默认的加密管辖范围策略文件，用于对加密算法的强度加以限制。如果设备上需要配置或已配置强度更高的算法（例如，将 AES 配置为 256 位密钥，将 DH 组配置为 5、14、24），请按以下步骤操作：

  a. 访问 http://www.oracle.com/technetwork/，依次点击“下载”(Downloads) >“Java SE”>“适用于 JDK/JRE 7 的 Java 加密扩展 (JCE) 无限强度管辖范围策略文件”(Java Cryptography Extension [JCE] Unlimited Strength Jurisdiction Policy Files for JDK/JRE 7)，下载无限强度加密策略 .jar 文件。（点击“下载”[Download] 按钮并接受许可协议即可下载文件。）

  b. 在 CSCOpx\MDC\vms\jre\lib\security 文件夹中，替换安全管理器服务器的 local_policy.jar 和 US_export_policy.jar 文件。

  c. 重新启动安全管理器服务器。

- **CSCuh52092** - 发布此修复后，您可以配置 HTML 和 PDF 报告，并通过设置超时时间，让系统在超过预设时间后退出报告生成进程。您可以配置以下属性：
  - #generate_activity_report_timeout=10
  - #generate_activity_pdf_report=true
  - #generate_activity_html_report=false

请按以下步骤操作：

a. 在文本编辑器（例如，记事本）中打开 $NMSROOT\MDC\athena\config\ 子目录中的 csm.properties 文件。（$NMSROOT 是 Common Services 安装目录的完整路径名称 [默认路径为 C:\Program Files (x86)\CSCOpx]）。

b. 在 csm.properties 文件中搜索上述属性。

c. 删除代码行开头的 # 字符，启用特定属性。

d. 超时 (generate_activity_report_timeout) 是 PDF 和 HTML 报告生成中的常见设置。启用并设置超时后，报告生成进程会在设定的时间后停止并释放所有资源。设置超时（以分钟为单位）时，应以生成报告的平均用时为依据。我们建议将超时设置为 10 分钟。

e. 启用 generate_activity_pdf_report 或 generate_activity_html_report，并根据需要将启用的属性设置为“true”。如果两个属性均设置为“true”，安全管理器会生成 PDF 格式的报告。

f. 要禁用某个属性，在该属性代码行开头添加 # 字符即可。

g. 保存并关闭 csm.properties 文件。

h. 依次点击“开始”>“程序”>“管理工具”>“服务”，重新启动思科安全管理器后台守护程序管理器服务。

- **CSCup28957** - 此修复发布之后，您可以在“活动更改”(Activity Change) 报告中排除所有适用策略的操作列表行。
  - 排除的操作必须以英文逗号分隔，并且值为空或代码行包含注释时，应包含所有操作。
  - 排除的操作包括“添加”(Add)、“删除”(Delete)、“修改”(Modify)、“移动”(Move)、“重新排序”(ReOrder)、“分配”(Assign) 和“取消分配”(UnAssign)。您不得修改这些操作名称，这些名称应原封不动。

  默认情况下，这些操作的值为空，如果您要排除特定操作，请执行以下步骤：

a. 在文本编辑器（例如，记事本）中打开 $NMSROOT\MDC\athena\config\ 子目录中的 csm.properties 文件。（$NMSROOT 是 Common Services 安装目录的完整路径名称 [默认路径为 C:\Program Files (x86)\CSCOpx]）。

b. 搜索 ActChangeReport.excludedOperations=

c. 使用任意可用选项，添加所需的排除操作：例如：
   - ActChangeReport.excludedOperations=ReOrder
   - ActChangeReport.excludedOperations=Add,ReOrder
   - ActChangeReport.excludedOperations=Add,Modify,Move,ReOrder

d. 保存并关闭 csm.properties 文件。

e. 依次点击“开始”>“程序”>“管理工具”>“服务”，重新启动思科安全管理器后台守护程序管理器服务。

安全管理器 4.7

以下说明适用于安全管理器 4.7 版本：

- ASA 9.x 支持远程接入 VPN 使用 IPv6，但是 4.10 之前的安全管理器版本不支持远程接入 VPN 使用 IPv6。因此，4.10 之前的安全管理器版本发现不了远程接入 VPN IPv6 配置。
- 安全管理器不支持 IPv6 互联网控制消息协议 (ICMP) 地址。它仅支持 IPv4 ICMP 地址。
- 安全管理器仅将有差别的配置发送给配置引擎并供特定设备获取。配置引擎并不会向设备推送完整配置。因此，设备的 OSPF、VLAN 和故障转移会产生以下行为。
  - 适用于 IOS 路由器的 OSPF - 安全管理器支持运行 IOS 软件 12.2 和更高版本的路由器上的 OSPF 策略。不过，安全管理器不支持 Catalyst 设备上的 OSPF 策略。因此，当您配置 Catalyst 设备中的 OSPF 策略并在安全管理器中执行发现操作时，发现操作会从完整配置中删除 ‘no passive-interface <*interface number*>’ 命令。因此，您会发现安全管理器生成的配置与设备上的配置存在差异。
  - VLAN - 安全管理器支持发现 IOS 设备中的 VLAN 命令，但是不支持 VLAN 命令的动态行为。如果 VLAN 策略中存在由用户造成的更改，安全管理器生成命令时会采用差量配置或完整配置。换句话说，在普通预览或部署中，安全管理器不会采用完整配置生成 VLAN 命令。因此，您会发现安全管理器生成的配置与设备上的配置存在差异。
  - 适用于防火墙设备（例如，ASA 和 FWSM）和 IOS 设备的故障转移策略 - 安全管理器不支持故障转移设备的动态行为。也就是说，HA 中的主设备采用 ‘failover lan unit primary’ 命令，而辅助设备采用 ‘failover lan unit secondary’ 命令。发生状态切换时，安全管理器会尝试比较 ‘failover lan unit primary’ 并生成差量配置。这会导致部署失败。

  注 安全管理器不支持“动态”CLI 命令。如果 CLI 命令的语法被修改（例如，由 ‘primary’ 关键字改为 ‘secondary’），安全管理器将不再支持该命令。

- 对于集群模式下的 ASA 设备，安全管理器将整个集群视为一个节点，并使用主集群 IP 地址管理集群。集群的主集群 IP 地址是集群的固定地址，始终属于当前的主设备。如果主节点更改，集群的 SNMP 引擎 ID 也会随之更改。在发生这种情况时，安全管理器会为使用明文密码配置的所有 SNMP 服务器用户重新生成 CLI。安全管理器不会为使用加密密码配置的用户重新生成 CLI。

  您可以使用 SNMP 页面上的“获取 SNMP 引擎 ID”(Get SNMP Engine ID) 按钮从当前的集群主设备取回引擎 ID。

- 如果您使用 **password encryption aes** 命令启用了密码加密，则将无法使用安全管理器管理 IOS 或 ASA 8.3+ 设备。您必须关闭密码加密，然后才能将设备添加至安全管理器资产。
- 如果您将由安全管理器管理的 ASA 由 8.2(x) 或更低版本升级至 8.3(x) 或更高版本，则您必须使用 NAT 重新发现选项重新发现 NAT 策略（右键单击设备、选择“发现设备上的策略”[Discover Policies on Device(s)]，然后仅选择“NAT 策略”[NAT Policies] 作为要发现的策略类型）。此选项将升级安全管理器配置，在实现与设备配置相符的同时，保留所有现有的共享策略、继承配置、Flex 配置等。

  ASA 设备由 8.4.x 升级至 9.0.1 时，设备策略将转换为统一格式。您可以使用 NAT 重新发现选项重新发现统一 NAT 规则，或者借助安全管理器中的规则转换器，将现有 NAT 策略转换为统一 NAT 策略。有关详细信息，请参阅 http://www.cisco.com/c/en/us/td/docs/security/security_management/cisco_security_manager/security_manager/4-6/user/guide/CSMUserGuide/porules.html#pgfId-161507 或在线帮助中的“Converting IPv4 Rules to Unified Rules”（将 IPv4 规则转换为统一规则）主题。

  如果要以统一的防火墙规则格式管理这些策略，您也可以使用适用于其他防火墙规则（例如，访问规则、AAA 规则和检测规则）的规则转换器。

- ASA 8.3 ACL 使用设备的实际 IP 地址，而非转换的 (NAT) 地址。在升级期间，规则会转换为使用实际 IP 地址。所以其他设备类型及较旧 ASA 版本使用 ACL 中的 NAT 地址。
- ASA 8.3 对设备内存的要求比旧 ASA 版本高。在升级之前，确保设备满足 ASA 文档中规定的最低内存要求。安全管理器将阻止向不满足最低要求的设备进行部署。
- 如果从安全管理器 4.6 升级至 4.7，安全管理器 4.7 将增加对以下 ASA 策略的支持：
  - 路由映射
  - CLI 提示符
  - 虚拟访问
  - AAA Exec 授权

  如果您的设备在旧版安全管理器中使用了不受支持的命令，则这些命令不会随此版本安全管理器的升级自动移到安全管理器。如果恢复设备的部署，这些命令会从设备中删除，因为它们不属于安全管理器中配置的目标策略。我们建议您为安全管理器中新添加的属性设置正确的值，从而确保下次部署时能正确调配这些命令。您也可以在设备中重新发现平台设置；不过，您必须执行必要步骤来保存和恢复分配给设备的所有已共享安全管理器策略。

注 如果在 ASA 上配置了路由映射，并且 OSPF 策略中使用与此相同的路由映射，则由安全管理器 4.6 升级至安全管理器 4.7 后，OSPF 页面上会显示红色横幅。要解决此问题，您必须重新发现 ASA。

- 如果您的设备在旧版安全管理器中使用了不受支持的命令，则这些命令不会随此版本安全管理器的升级自动移到安全管理器。如果恢复设备的部署，这些命令会从设备中删除，因为它们不属于安全管理器中配置的目标策略。我们建议您为安全管理器中新添加的属性设置正确的值，从而确保下次部署时能正确调配这些命令。您也可以在设备中重新发现平台设置；不过，您必须执行必要步骤来保存和恢复分配给设备的所有已共享安全管理器策略。
- 安全管理器 4.7 不支持 Common Services 中的设备和凭证存储库 (DCR) 功能。
- IPS 4500 设备系列不支持 LACP 配置。
- 在 IPS 5.x+ 设备、Catalyst 和 ASA 服务模块以及路由器网络模块上，安装和签名更新需要 Cisco Services for IPS 服务许可证。
- 不要直接连接数据库，因为这样做会造成性能降低和导致系统异常行为。
- 不要对数据库执行 SQL 查询。
- 如果在线帮助页面在浏览器视图中显示空白，请刷新浏览器。
- 安全管理器 4.7 仅支持思科安全 ACS 5.x 用于身份验证。实现身份验证和授权必须使用 ACS 4.1(3)、4.1(4) 或 4.2(0)。
- 如果您不管理 IPS 设备，请考虑执行以下性能调整步骤。在 *$NMSROOT*\MDC\ips\etc\sensorupdate.properties 中，将 packageMonitorInterval 的值由初始默认值 30,000 毫秒改为 600,000 毫秒，从而降低频率。执行此步骤能够在一定程度上提升性能。[*$NMSROOT* 是 Common Services 安装目录的完整路径名称，默认路径为 C:\Program Files (x86)\CSCOpx。]
- 安全管理器随附的 IPS 软件包不包含更新 IPS 设备所需的软件包文件。在应用任何更新之前，您必须先从 Cisco.com 或本地更新服务器下载 IPS 软件包。下载的版本包含所有必需软件包文件，并会替换安全管理器初始安装中包含的不完整文件。
- 删除了 CiscoWorks Common Services 主页上的“许可证管理”(License Management) 链接。
- CsmReportServer 和 CsmHPMServer 现在支持 64 位 JRE。
- “rsh”服务已改为手动启动模式。您可以根据需要启动该服务。

警告

本节介绍与此版本相关的未解决警告和已解决警告。

为便于您使用思科缺陷搜索工具 (BST) 寻找警告，本节中的警告标题均直接提取自缺陷搜索工具数据库。由于标题字段长度有限，因此警告标题不一定是完整句子。为尽可能完整简洁地说明问题，警告标题截短了部分用词或标点。本文对这些标题仅做如下修改：

- 规范产品名称和缩略词的使用。
- 更正拼写错误和错别字。

注 如果您是 cisco.com 注册用户，转至 https://tools.cisco.com/bugsearch 即可在 cisco.com 上访问思科缺陷搜索工具。有关缺陷搜索工具的更多信息，请访问帮助页面：http://www.cisco.com/web/applicat/cbsshelp/help.html。

如果您不是 cisco.com 注册用户，可以转至以下网站注册：http://tools.cisco.com/RPF/register/register.do

本节包含以下主题：

未解决警告 - 版本 4.7

以下警告对此版本有影响并且涵盖在安全管理器 4.7 之中。

注 有些情况下，已知问题可能会不止在一个方面造成影响，例如，PIX 设备可能会在部署期间遇到问题。如果您在某个表中找不到有关特定问题的警告，应将搜索范围扩大至涵盖其他表。在前述示例中，已知问题可能在“部署”或“PIX/ASA/FWSM 配置”表中列出。

表 2 思科 IOS 路由器设备警告

参考编号	说明
CSCth95357	XE: Deploy Fails when Memory Critical Notifications are Changed（XE：内存告急通知更改时，部署失败）
CSCti15944	CLI: “dot1x pae authenticator” generated after deployment of 802.1x（CLI：部署 802.1x 后生成“dot1x pae authenticator”）
CSCtq12795	Generic Router : AAA rules getting negated.（通用路由器：AAA 规则被否定。）

表 3 思科 IPS 与 IOS IPS 设备警告

参考编号	说明
CSCtk36259	MU-IPS Licensing page taking too long for Refresh / CCO Update operation（在多用户 IPS 许可页面上，刷新/CCO 更新操作耗时过长）
CSCug68487	CSM isn't closing all the HTTPS session as part of config deployment（CSM 未在配置部署中关闭所有 HTTPS 会话）
CSCum79301	TP tunings are not applied when sig is tuned other than status fields（调整签名而非状态字段时，未应用 TP 调整）

表 4 客户端和服务器安装警告

参考编号	说明
CSCtq99125	Installation: Evaluation and Licensing options get enabled simultaneous（安装：评估和许可选项同时启用）
CSCtr71792	ETSGJ-CH:CSM Launch Icons Missing on XP JOS Client（ETSGJ-CH：XP JOS 客户端上缺少 CSM 启动图标）
CSCtr72248	ETSGJ-CH:Not able to proceed with install if going back to previous page（ETSGJ-CH：返回前页后无法继续安装）
CSCuj65797	CSM 4.5 Security Tools page UI launching Issues on Win 7 32 bit client（CSM 4.5 安全工具页面 UI 在 Win 7 32 位客户端上存在启动问题）

表 5 设备管理、发现和部署警告

参考编号	说明
CSCub81927	Scal Testing: DB error during deployment（SCAL 测试：部署期间出现数据库错误）
CSCuc13848	Getting error while submitting a ticket for Validation.（提交待验证申请单时出错。）
CSCup91317	ASAv:Rediscovery fails after OOB image Upgrade（ASAv：OOB 映像升级后，重新发现失败）

表 6　事件查看器警告

参考编号	说明
CSCtg57676	Internal error thrown when portlist is used in service object filter.（服务对象过滤器中使用端口列表时，抛出内部错误。）
CSCtg57745	Filtering does not work when only protocol name is used in service obj.（服务对象中仅使用协议名称时，无法正常进行过滤。）
CSCtg57839	Results not correct when network obj with non-contiguous mask is used.（使用非邻接掩码网络对象时，结果不正确。）
CSCua81392	CSM 4.2 - Eventing directory does not get deleted（CSM 4.2 - 无法删除事件目录）
CSCuh16940	IPS subscription is not getting closed when unmonitoring the device（未监控设备时，IPS 订阅不会关闭）
CSCuh38244	P2E: Events are not filtered properly if ACE has muliple services（P2E：ACE 有多个服务时，事件无法得到正确过滤）
CSCui01213	Changing “Time field” by highlighting the value is not inserting properly（通过突出显示值更改“时间字段”时无法正确插入）

表 7　防火墙服务警告

参考编号	说明
CSCtf32208	Deployment fails with ACE edit in ACL BB（在 ACL BB 中修改 ACE 时，部署失败）
CSCtg80500	Manual-NAT: need validation for “neq” operator in static NAT（手动 NAT：需要验证静态 NAT 中的“neq”运算符）
CSCti08077	system context Config file discovery fails with ASA 5580 platform（在使用 ASA 5580 平台时，系统情境配置文件发现失败）
CSCtl10613	Int: ASA 5580/85 should support max 1034 int allocation to context（接口：ASA 5580/85 最多支持向情境分配 1034 个接口）
CSCto67515	ASA/ASASM Failover commands not negated（ASA/ASASM 故障转移命令未被否定）
CSCto80002	UID: Deployment fails when domain is used in ACL and is deleted（UID：当域在 ACL 中使用并被删除时，部署失败）
CSCtq04794	NAT: Deployment is failing for object NAT for Translate DNS rule（NAT：使用转换 DNS 规则时，对象 NAT 部署失败）
CSCtq20997	NAT:Subnet Can not be used as mapped Source in Dynamic NAT policy（NAT：子网无法在动态 NAT 策略中用作映射来源）
CSCtq24069	UID: repeated ACL delta with ACL match protocol inspection（UID：使用 ACL 匹配协议检测时，出现重复 ACL 差量）
CSCtq36739	NAT: Same Mapped address cannot be used to perform both NAT and PAT（NAT：相同映射地址无法同时用于执行 NAT 和 PAT）
CSCtq63721	UID: order of AAA server negation/appending _1 on discovery should modify（UID：应修改 AAA 服务器否定/附加 _1 的顺序）

表 7　　防火墙服务警告（续）

参考编号	说明
CSCtq82588	Discovery fails for device with scan safe AAA in CSM 4.1（CSM 4.1 中，采用 ScanSafe AAA 配置的设备发现失败）
CSCtr12016	ETSGJ-CH:Japanese User not displayed in Identity UserGroup UI（ETSGJ-CH：身份用户组 UI 中不显示日语用户）
CSCtr12155	ETSGJ-CH:Japanese User Group shows Name as Square blocks in JOS Client（ETSGJ-CH：日语用户组名称在 JOS 客户的中显示为方块）
CSCtr25092	ETSGJ-CH:Pop-up for wrong bind in Identity needs to be revisited（ETSGJ-CH：弹出窗口要求重新访问错误捆绑的身份）
CSCtr25195	ETSGJ-CH:Domain name with special characters are permitted（ETSGJ-CH：允许使用包含特殊字符的域名）
CSCtr30676	Deployment fails when http accounting banner from file is configured（配置来自文件的 http 记帐横幅时，部署失败）
CSCtr71998	ETSGJ-CH:Incremental pop-up for a wrong MAC in Cat6k ASA-SM Failover（ETSGJ-CH：因 Cat6k ASA-SM 故障转移中错误 MAC 而显示的弹出窗口增多）
CSCts25221	Edit ACL in Identity Policy-CSM generates incorrect order of cli（编辑身份策略中的 ACL - CSM 产生的 cli 顺序错误）
CSCtw48451	Override BB are not mapping with BBs used in import rules（覆盖 BB 与导入规则中使用的 BB 不对应）
CSCty77037	Remove unreferenced Object-Group option can cause deployment error（删除未参考的对象组选项导致部署出错）
CSCud37752	ASA Image Downgrade From 9.0 to 8.4.4 Contain Xlate Rules in Preview（从 9.0 降级至 8.4.4 的 ASA 映像在预览中包含 Xlate 规则）
CSCuj99884	Global search does not display default inspection rule present in device（全局搜索不显示设备中存在的默认检测规则）
CSCuo15620	WebACL: URL Validation is not happening with the added ACL object（WebACL：添加的 ACL 对象无法进行 URL 验证）
CSCup33218	[OOB]Avoid Rule Splitting during OOB Re-synch（[OOB]在 OOB 重新同步期间避免规则分割）
CSCup76874	[OOB]Change In Section Structure After Re-Synch for Modified ACL（[OOB]修改的 ACL 重新同步后，节结构改变）
CSCup77926	Red banner Error in asa 921 post upgrade from csm 4.5（从 CSM 4.5 升级后，ASA 921 中出现红色横幅错误）
CSCuq19631	Route Map edit is not working properly.（无法正确编辑路由映射。）
CSCuq23825	Prefix-list/As-Path modification and route-map delete not in one activity（前缀列表/AS 路径修改和路由映射删除不位于一个活动中）

表 8　运行状况和性能监控警告

参考编号	说明
CSCtt95667	FW: Certificates should be displayed as part of Non VPN Views（FW：证书应显示为非 VPN 视图的一部分）
CSCtx48130	VPN: SitetoSite VPN tunnel details not proper with dynamic cryptomap 8.4（VPN：使用动态加密图 8.4，站到站 VPN 隧道详情不正确）
CSCue50284	Tunnel Alerts: Traps Not Processed if the Remote Subnet is a Host（隧道警报：远程子网为主机时，不处理陷阱）
CSCuo10773	Perf : HPM Client Lag Issue after leaving it idle for long time（性能：HPM 客户端长时间闲置后发生延迟问题）

表 9　映像管理警告

参考编号	说明
CSCup89988	ASAv: Image Upgrade Fails for Virtual ASA（ASAv：虚拟 ASA 映像升级失败）
CSCuq01829	ReloadWait: Image loading failing from IM with an active VPN tunnel（重新加载等待：使用主动 VPN 隧道从 IM 加载映像失败）

表 10　其他警告

参考编号	说明
CSCtq99617	CSM UI unresponsive for a long period in MU testing（CSM UI 在 MU 测试中长时间无响应）
CSCuh86712	Device state is not changed as rediscovering the changes（重新发现更改后，设备状态不改变）
CSCui32627	Adding IP to cluster pool is not getting updated in logrelay filter（添加到集群池的 IP 在 logrelay 过滤器中未更新）
CSCui78433	Flickering issue : IP Intel and View Statistics refresh/other flows（闪烁问题：IP 智能窗口和查看统计数据刷新/其他流程）
CSCuj25254	Not able to crosslaunch frm CSM-PRSM if username starts with bold letter（用户名以粗体字母开头时，无法交叉启动 frm CSM-PRSM）
CSCuj50087	Image is removing from the list after viewing the config file（查看配置文件后，映像文件从列表中删除）
CSCuj60513	Logrelay:Warning can be given when one user changes impacting other user（Logrelay：一个用户所做的更改对其他用户产生影响时，可能会显示警告）
CSCul96498	Device Status view is not getting autorefreshed when in undock view（在非固定视图中，设备状态视图不自动刷新）
CSCul97177	Device filter is not working in OOB detection window（设备过滤器在 OOB 检测窗口中无法正常使用）
CSCun70866	Discrepancy in displaying Geoip Schedule download timings（显示 Geoip 计划下载时间时出现差异）

表 10 其他警告（续）

参考编号	说明
CSCuo06326	Cross launch to DC with IPv6 address does not work with 2 browsers（使用 2 个浏览器时，无法通过 IPv6 地址交叉启动 DC）
CSCuo29366	Need proper validation error message with invalid data for BB（BB 数据无效时，显示“需要适当验证”错误消息）

表 11 策略管理警告

参考编号	说明
CSCud86519	CSM deployment error with an Object（对象 CSM 部署错误）
CSCuh40492	Configuration differences in OOB detection not shown exactly（未精确显示 OOB 检测中的配置差异）
CSCun24271	Mutual usage of PB in multiuser scenario showing exceptions in message（在多用户情景中，多用户使用策略包在消息中显示例外）
CSCup00905	Smart Tunnel Network List BB: Overriden Values Not Imported（智能隧道网络列表 BB：未导入覆盖的值）

表 12 报告管理器警告

参考编号	说明
CSCuo48915	VPN User rpt:Couldn't do the column sorting based on login / logout time（VPN 用户 RPT：无法根据登录/注销时间对列排序）
CSCuq28564	Upgrade: Issue in showing pre upgrade data in VPN User report（升级：在 VPN 用户报告中显示升级前数据存在问题）

表 13 VPN 设备和配置支持警告

参考编号	说明
CSCtq67354	preview fails,rule name(SSLVPN->othersett->content rewrite) having space（预览失败，规则名称 [SSLVPN->othersett->content rewrite] 含空格）
CSCtq86149	deployment fails:existing Virtual Template int with type serial - Ezvpn（部署失败：现有虚拟模板接口采用串行类型 - Ezvpn）
CSCtr06681	preview fails : if SSO name is given with spaces（预览失败：提供的 SSO 名称含空格）
CSCtr28222	IPSec Proposal is not discovered, if DVTI/VRF is configured in ISR（如果在 ISR 中配置 DVTI/VRF，无法发现 IPSec 提案）
CSCts30832	Preview failed due to FQDN acl BB used in group policy.（因为在组策略中使用 FQDN acl BB，预览失败。）
CSCub82270	CSM deletes the existing ACL when changing protected nw/Spk2Spk connecti（更改受保护 nw/Spk2Spk 连接时，CSM 删除现有 ACL）
CSCub89125	PKI node under Remote Access VPN to be enabled（远程接入 VPN 下的 PKI 节点启用）

表 13　　VPN 设备和配置支持警告（续）

参考编号	说明
CSCud61707	PKI deployment failed with trustpoint not enrolled error for ASA 9.0（PKI 部署失败，ASA 9.0 信任点未注册错误）
CSCum00081	Discovery issue for IKEv2 Auth policy when changed from PSK to PKI（由 PSK 改为 PKI 时，IKEv2 身份验证策略存在发现问题）
CSCun33192	IOS SSL VPN:negation of ssl trustpoint cli（IOS SSL VPN：否定 SSL 信任点 cli）
CSCun52538	existing IPsec proposals are deleted when anew tungrp is created via wiz（通过向导创建新隧道组时，现有 IPsec 提案被删除）
CSCup04598	Device has to be redeployed to change Crypto Map on Multi Topology（必须重新部署设备，以更改多拓扑上的加密图）
CSCup95990	Browser proxy:Incorrect cli when removing entry from the exception list（浏览器代理：从例外列表删除条目时，cli 出错）
CSCuq25585	Activity Validation For Different Crypto Map Name of Multi Topology（多拓扑不同加密图名称的活动验证）

已解决的警告 - 版本 4.7 服务包 3

思科安全管理器 4.7 服务包 3 中已解决了客户发现或之前版本说明中存在的以下警告。

参考编号	说明
CSCut29478	CSM client memory leakage in javaw.exe process（javaw.exe 进程中 CSM 客户端内存泄漏）
CSCuv35928	CSM - Error "Parent policy is locked" when modifying inherited policies（CSM - 修改继承策略时出现“父策略已锁定”错误）
CSCuv39677	Translated source shows ",0" value in Activity Report（转换后来源在活动报告中显示“,0”值）
CSCuu43022	CSM - Flex Config permissions with Terminal Services（CSM - 终端服务中的 Flex 配置权限）
CSCut87333	CSM 4.7cp2 ICMP does not support IPv6 Addressses（CSM 4.7cp2 ICMP 不支持 IPv6 地址）
CSCut65297	CSM - unable to do packet-tracer with IPv6 addresses（CSM - 无法对 IPv6 地址进行数据包跟踪）
CSCuu12847	CSM - ICMP IPv6 Support（CSM - ICMP IPv6 支持）
CSCuu18236	CSM - ICMP IPv6 warning commands to line up with ASA（CSM - 与 ASA 结合的 ICMP IPv6 警告命令）
CSCuv26167	Evaluation of vms for OpenSSL July 2015 vulnerability（针对 OpenSSL 2015 年 7 月漏洞对 VMS 的评估）

已解决的警告 - 版本 4.7 服务包 2

思科安全管理器 4.7 服务包 2 中已解决了客户发现或之前版本说明中存在的以下警告。

参考编号	说明
CSCub97603	CSM should allow configuring a secondary IPv6 address on ASA interface（CSM 应允许在 ASA 接口上配置一个辅助 IPv6 地址）
CSCur23742	CSM fails to deploy class-map when access-list is used（使用访问列表时，CMS 无法部署类别图）
CSCut76507	CSM 4.8 CSM fails to deploy class-map when access-list is used（使用访问列表时，CSM 4.8 CSM 无法部署类别图）
CSCut59655	Multi-context ASA discovery failing on 4.7（多情境 ASA 发现功能在 4.7 上失败）
CSCus59205	CSM: IPS Licenses show "Nonretrievable - Invalid username and password"（CSM：IPS 许可证显示“无法获取 - 用户名和密码无效”）
CSCuq26685	Not able to edit a specific object-group in the CSM v 4.5（无法编辑 CSM v 4.5 中的特定对象组）
CSCut07447	CSM 4.7 CP2: CSM sending "no speed nonegotiate" for fiber interface（CSM 4.7 CP2：CSM 向光纤接口发送“无速度协商”）
CSCus42723 (CSCut45947)	OpenSSL PSIRT
CSCut22499	Incorrect delta changes for CSM deployment to ASR（CSM 向 ASR 部署的错误差量更改）
CSCut60126	Re-discovery fails on CSM after upgrade of ASA to 9.2(2)（ASA 升级到 9.2(2) 后，在 CSM 上重新发现失败）
CSCut03558	CSM 4.7: Preview configuration fails while parsing group-object（CSM 4.7：解析组对象时，预览配置失败）

已解决的警告 - 版本 4.7 服务包 1

思科安全管理器 4.7 服务包 1 中已解决了客户发现或之前版本说明中存在的以下警告。

参考编号	说明
CSCud11355	CSM Server needs to support TLS v1.2（CSM 服务器需要支持 TLS v1.2）
CSCus82037	Support for "http-only-cookie" cli for ASA 9.2(3)（支持 9.2(3) 的“仅 http cookie”cli）
CSCur29069	Cisco Security Manager : evaluation of SSLv3 POODLE vulnerability（思科安全管理器：评估 SSLv3 POODLE 漏洞）
CSCus88379	CSM:- Import/Export perl script not working on non default HTTPS port（CSM：无法通过非默认 HTTPS 端口导入/导出 perl 脚本）
CSCus12592	CSM 4.7 support for ISE 1.3（CSM 4.7 支持 ISE 1.3）

参考编号	说明
CSCuq75832	CSM 4.7 Editing OSPF interfaces in device view（CSM 4.7 在设备视图中编辑 OSPF 接口）
CSCup63069	CSM 4.6 Event Manager 'go to policy' fails for none Unified ACLs ASA 9.x（对于非统一 ACL ASA 9.x，CSM 4.6 事件管理器“转至策略”失败）
CSCuq30700	CSM pushing "management-only" on interfaces with a "management" alias（CSM 使用“管理”别名在接口上推送“仅管理”）
CSCup58780	CSM: Event Management/Viewer [PartitionPurgeRoutine] - Failed to delete（CSM：事件管理器/查看器 [PartitionPurgeRoutine] - 无法删除）
CSCup91495	CSM 4.6 HPM startup issue when VPN alerting is enabled（启用 VPN 警报时，CSM 4.6 HPM 出现启动问题）
CSCuq01831	CSM: Event Viewer Error "This operation cannot be performed"（CSM：事件查看器错误“无法执行此操作”）
CSCul51205	Image Manager not using correct user credentials（映像管理器使用的用户凭证不正确）
CSCup91522	CSM 4.6 Additional Tunnels displayed when SNMP query to device fails（SNMP 对设备的查询失败后，显示 CSM 4.6 额外隧道）
CSCuh52092	CSM 4.3SP1 : tomcat.exe spikes during change report generation（CSM 4.3SP1：tomcat.exe 在生成更改报告期间产生尖峰）
CSCup70309	CSM Inconsistency in shared policy access-rules.（共享策略访问规则中 CSM 不一致。）
CSCup28957	Ability to exclude line number changes from Activity Report（可以从活动报告排除行号更改）
CSCur13055	CSM 4.7 removes ospf hello-interval and dead-interval settings（CSM 4.7 删除 OSPF hello 间隔和 dead 间隔）
CSCup70029	CSM: Inspection Rule policy for Scansafe has no HTTPS（CSM：Scansafe 的检测规则策略没有 HTTPS）
CSCup70098	CSM: Scansafe Inspection Rule policy have no changes in delta config（CSM：Scansafe 检测规则策略在差量配置中无变化）
CSCuq64605	Event viewer shows incorrect event if sorts event（在对事件排序时，事件查看器显示错误事件）
CSCup91482	ASA/FWSM:IPV6 ACL Removed on Discovery（ASA/FWSM：IPV6 ACL 在发现时被删除）
CSCur08936	Unable to import policies in CSM 4.6（无法在 CSM 4.6 中导入策略）
CSCul96691	Cmf Database engine service was disabled after a failed scheduled backup（计划的备份失败后，Cmf 数据库引擎服务被禁用）
CSCuq52900	CSM 4.6 SP1 Deploys wrong SNMPv3 password（CSM 4.6 SP1 部署错误的 SNMPv3 密码）
CSCur54703	csm 4.7 and ospf redistribute static and metric-type 1（csm 4.7 和 ospf 静态重新分发和指标类型 1）
CSCup02863	CSM Preview config fails with "network-object object null" exception（CSM 预览配置失败，出现“network-object object null”例外）
CSCur82360	CSM: Unable to generate VPN reports after the upgrade（CSM：升级后无法生成 VPN 报告）

参考编号	说明
CSCur76940	Deployment report can't be generated in HTML format（无法生成 HTML 格式的部署报告）
CSCus14411	Validation error while applying interface role with override（通过覆盖应用接口角色时出现验证错误）
CSCus19784	CSM deploys management-only under non-management interface（CSM 在非管理接口下部署“仅管理”）
CSCur89878	CSM: ZBF deployment fails due to invalid access-group used in class-map.（CSM：因为在类别图中使用的访问组无效，ZBF 部署失败。）
CSCus43939	NoValueNetworkBBValidationLevel property throws error for unified rules（NoValueNetworkBBValidationLevel 属性对统一规则抛出错误）
CSCuq56721	media-type does not exist in show run, causing CSM deployments to fail（show run 中不存在媒体类型，导致 CSM 部署失败）
CSCuq21511	Username From CertScript Policy View does not show the scripts properly（证书脚本策略视图中的用户名显示的脚本不正确）

已解决的警告 - 版本 4.7

本版本中已解决了客户发现或之前版本说明中存在的以下警告。

参考编号	说明
CSCse93193	Add VPN-PKI enhancement for terminal enrollment（为终端注册添加 VPN-PKI 增强功能）
CSCsl42198	address-pool under ASA user-group is not supported + other enhancements（不支持 ASK 用户组下的地址池 + 其他增强功能）
CSCsy95299	Banner motd first empty line can not be removed（不能删除问候报文横幅第一行空行）
CSCtb17772	CSM: ENH To detect changes and import just the changes.（CSM：增强更改检测功能，并且仅导入更改。）
CSCtb68104	ENH: Notify user when they modify a shared object in CSM（增强：用户修改了 CSM 中的共享对象后，向用户发送通知）
CSCtg54222	Eventing Restore: Restore failing or partially succeeding in some cases（事件恢复：恢复失败，有时仅部分事件恢复成功）
CSCud93498	CSM 4.3-SSLVPN Missing the option to configure the parameters for SSO（CSM 4.3 - SSLVPN 缺少为 SSO 配置参数的选项）
CSCud93515	CSM 4.3 - VPN - ip/network missing for smart tunneled application config（CSM 4.3 - VPN - 缺少智能隧道应用可配置的 ip/网络）
CSCuh31093	ENH: CSM needs to be able to create "username_from_cert.xml" file（增强：CSM 需要能够创建“username_from_cert.xml”文件）
CSCuh53309	dmgtd.exe causes bluescreen on the CSM Server（dmgtd.exe 导致 CSM 服务器蓝屏）
CSCui60252	CSM 4.3 Misleading Information in Common Services（CSM 4.3 在 Common Services 中显示误导性信息）

参考编号	说明
CSCui94177	CSM 4.4 does not support "time-range"（CSM 4.4 不支持“时间范围”）
CSCuj59706	CSM 4.4 deploys IOS NTP configuration in worng command order（CSM 4.4 以错误的命令顺序部署 IOS NTP 配置）
CSCuj65553	CSM 4.5 Installation Command Buttons appear garbled（CSM 4.5 安装命令按钮显示乱码）
CSCuj65593	CSM 4.5 Installation Button Appears Garbled（CSM 4.5 安装按钮显示乱码）
CSCul70104	CSM does not properly disable isakmp keepalives（CSM 未能正确禁用 isakmp keepalive 功能）
CSCum03347	CSM: Deployment Validation Fails if ASA nameif Contains "(" or ")" Chars（CSM： ASA nameif 包含“(”或“)”字符时，部署验证失败）
CSCum61701	CSM 4.4 Activity and Ticket field cannot be altered independently（在 CSM 4.4 中，无法独立更改活动和申请单字段）
CSCum87972	Can't execute backup on CSM4.4SP1（无法在 CSM4.4SP1 上执行备份）
CSCum91828	Security Notification:Event Archival-Event data deleted before archival（安全通知：事件归档 - 归档前删除事件数据）
CSCum92428	CSM should handle NPE in ServiceSplitter.java（CSM 应在 ServiceSplitter.java 中处理 NPE）
CSCun00643	CSM reports hitcounts not for all ACE in FWSM（CSM 报告的命中计数不涵盖 FWSM 中的所有 ACE）
CSCun04177	CSM 4.5 does not report hitcount for some ACE with obj-group on ASA（CSM 4.5 不报告 ASA 上某些有对象组的 ACE 的命中计数）
CSCun05594	HPM statuses not showing proper device states in Config Manager（HPM 状态在配置管理器中显示错误设备状态）
CSCun06578	CSM Event Viewer hangs for several hours.（CSM 事件查看器挂起数小时。）
CSCun13807	CSM trying to negate unmanaged VPN config（CSM 尝试否定未受管理的 VPN 配置）
CSCun14649	OSPFv3: Add Range and Virtual Link Table Empty on GUI（OSPFv3：在 GUI 上添加空范围和虚拟链路表）
CSCun29381	CSM 4.5: Raw ACE table content does not match with the selected ACL（CSM 4.5：原始 ACE 表内容与所选的 ACL 不符）
CSCun36357	CSM: Cannot Login to Client App After Upgrading to 4.5+（CSM：升级到 4.5+ 后，无法登录客户端应用）
CSCun48049	Support of dhcprelay server per interface on ASA（在 ASA 上支持 dhcprelay server per interface）
CSCun55888	CSM does not deploy changed Network object name in Shared policy（CSM 在共享策略中未部署更改的网络对象名称）
CSCun65303	CSM 4.5 - Warnings related to IOSMethodType when deploying on ASA（CSM 4.5 - 在 ASA 上部署时，与 IOSMethodType 相关的警告）
CSCun94866	Security Manager: CSM fails to find unused objects for all policy types.（安全管理器：CSM 无法找到所有策略类型未使用的对象。）
CSCuo03654	CSM 4.5 Wrong src/dst address ACEs show up in "Show HitCount Details"（“显示命中计数”中显示错误的来源/目标地址 ACE）
CSCuo18730	CSM backup scheduler script generates wrong batch file for backup（CSM 备份安排程序脚本生成错误的批处理备份文件）

参考编号	说明
CSCuo19842	CSM 4.5 CP02 Deploys "no mop enabled" under IOS 15.2 Interfaces（CSM 4.5 CP02 在 IOS 15.2 接口下部署“no mop enabled”）
CSCuo20820	Unable to install 3rd party Base64 encoded X.509 certificate on CSM 4.5（无法在 CSM 4.5 上安装第三方 Base64 编码 X.509 证书）
CSCuo30084	307CSM: ASA child NAT moved out to be parent（307CSM：ASA 子项 NAT 移至父项）
CSCuo54170	CSM deploys management-only to ASA management port-channel sub-interface（CSM 为 ASA 管理端口通道子接口部署“仅管理”）
CSCuo54275	CSM remove router ACL rules with nested service object-group（CSM 删除含嵌套服务对象组的 ACL 规则）
CSCuo55452	CSM4.6 fails to parse interface-specific dhcprelay config on ASASM（CSM4.6 无法解析 ASASM 上针对特定接口的 dhcprelay 配置）
CSCuo55556	CSM fails to validate identity user group with a space in between（CSM 无法验证含空格的身份用户组）
CSCuo56467	Cisco Security Manager wrongly negates 'mac-address auto' command on ASA（思科安全管理器在 ASA 上错误否定“mac-address auto”命令）
CSCuo66187	CSM approving activity cause Server Busy or Unavailable（CSM 批准活动导致服务器忙碌或不可用）
CSCuo73552	Security Manager doesn't allow user to configure asymmetric vpn keys（安全管理器不允许用户配置不对称 VPN 密钥）
CSCuo79712	CSM: original custom signature is deleted after save button（CSM：按“保存”按钮后，原始自定义签名被删除）
CSCup01683	CSM 4.6 incorrectly requires cluster IP pool for spanned-etherchannel（在 CSM 4.6 中，跨网络 EtherChannel 错误地要求集群 IP 池）
CSCup02800	CSM 4.5 : Deployment failing due to java.lang.NullPointerException（CSM 4.5：java.lang.NullPointerException 导致部署失败）
CSCup10456	DOC-CSM Run CSM client with "run as administrator" when UAC is enabled（文档 - CSM：在启用 UAC 时，“以管理员身份运行”CSM 客户端）
CSCup13423	CSM usage of DM_INLINE_NETWORK_ objects（CSM 使用 DM_INLINE_NETWORK_ 对象）
CSCup44842	CSM: CsmReportServer Process Maximum Heap Size Info Incorrect in Doc（CSM：文档中的 CsmReportServer 进程最大堆大小信息不正确）
CSCup67375	CSM - Cannot Edit NTP Server Configuration for ASA after Policy Creation（CSM - 创建策略后，无法为 ASA 编辑 NTP 服务器配置）
CSCup93631	DOC : CSM reports OOB even if the order of config changes（文档：即使配置顺序更改，CSM 仍报告 OOB）
CSCuq02522	CSM: 5515-IPS 7.3.2 discovery fails with Signature Threat Profile Error（CSM：5515-IPS 7.3.2 发现失败，出现签名威胁配置文件错误）

已解决的警告 - 4.7 之前版本

要获取之前版本解决的警告的列表，请参阅以下文档：

- http://www.cisco.com/c/en/us/support/security/security-manager/products-release-notes-list.html

后续操作

如果要：	执行以下操作：
安装安全管理器服务器或客户端软件。	参阅 *“Installation Guide for Cisco Security Manager 4.7”*（思科安全管理器 4.7 安装指南）。
了解基础知识。	参阅在启动安全管理器时自动打开的交互式 JumpStart 指南。
快速启动并开始使用产品。	参阅在线帮助中的“Getting Started with Security Manager”（安全管理器入门），或参阅 *《User Guide for Cisco Security Manager 4.7》*（思科安全管理器 4.7 用户指南）第 1 章。
完成产品配置。	参阅在线帮助中的“Completing the Initial Security Manager Configuration”（完成安全管理器初始配置），或参阅 *“User Guide for Cisco Security Manager 4.7”*（思科安全管理器 4.7 用户指南）第 1 章。
管理用户身份验证和授权。	参阅在线帮助中的以下主题，或参阅 *“Installation Guide for Cisco Security Manager 4.7”*（思科安全管理器 4.7 安装指南）第 7 章。 • 设置用户权限 • 安全管理器与思科安全 ACS 集成
独立管理设备。	参阅在线帮助中的“Preparing Devices for Management”（准备要管理的设备），或参阅 *“User Guide for Cisco Security Manager 4.7”*（思科安全管理器 4.7 用户指南）第 2 章。

产品文档

有关本版本支持文档的完整列表，请参与针对本版本的文档导读：

- *Guide to User Documentation for Cisco Security Manager（思科安全管理器用户文档导读）*

  http://www.cisco.com/c/en/us/support/security/security-manager/products-documentation-roadmaps-list.html

  其中归纳了本版本安全管理器的支持文档集合，并提供对各文档内容的摘要。
- 有关一般产品信息，请参阅：

  http://www.cisco.com/go/csmanager

获取文档和提交服务请求

要了解如何获取文档、使用思科漏洞搜索工具 (BST)、提交服务请求和收集其他信息，请参阅 *“What's New in Cisco Product Documentation”*（思科产品文档中的新内容）。

如果您订阅思科产品文档中的新内容 RSS 源，最新的和修订后的思科技术内容将直接送到您面前。RSS 源是一种免费服务。

本文档需结合“产品文档”一节中列出的文档共同使用。