FireSIGHT 系统版本说明

版本 5.3.1.6
首次出版：2015 年 9 月 28 日

即使您熟悉更新过程，也请务必通读并理解这些版本说明。这些版本说明描述了受支持的平台、新增功能和更改的功能、已知问题和已解决的问题，以及产品和网络浏览器的兼容性。它们还包含有关以下设备的先决条件、警告以及具体安装和卸载说明的详细信息：

- 系列 3 防御中心（DC750、DC1500 和 DC3500）
- 64 位虚拟防御中心
- 具备 FirePOWER 服务的思科 ASA （ASA5512-X、ASA5515-X、ASA5525-X、ASA5545-X、ASA5555-X、ASA5585-X-SSP-10、ASA5585-X-SSP-20、ASA5585-X-SSP-40 和 ASA5585-X-SSP-60）

注意 此更新**仅**适用于防御中心和具备 FirePOWER 服务的思科 ASA。物理或虚拟受管设备和 X-Series 专用 Sourcefire 软件**不**支持此更新。

提示 有关 FireSIGHT 系统的详细信息，请参阅联机帮助或从支持站点下载*《FireSIGHT 系统用户指南》*。

这些版本说明适用于版本 5.3.1.6 FireSIGHT 系统。您可以将运行至少 5.3.1 版 FireSIGHT 系统的设备更新至版本 5.3.1.6。

有关详细信息，请参阅以下各节：

思科系统公司
www.cisco.com

更改的功能

版本 5.3.1.6 的功能无任何更改。

早期版本添加的特性和功能

有关详细信息，请参阅《*FireSIGHT 系统用户指南*》、《*FireSIGHT 系统安装指南*》。

具备 FirePOWER 服务的思科 ASA 管理

5.3.1 版本引入了如下功能：使用 FireSIGHT 防御中心管理具备 FirePOWER 服务的思科 ASA（ASA FirePOWER 设备）。运行 5.3.1 版本的防御中心可以在以下 ASA 设备上管理 ASA FirePOWER 模块：

- ASA5512-X
- ASA5515-X
- ASA5525-X
- ASA5545-X
- ASA5555-X
- ASA5585-X-SSP-10、ASA5585-X-SSP-20、ASA5585-X-SSP-40 和 ASA5585-X-SSP-60

由防御中心版本 5.3.1.1 管理的 ASA FirePOWER 模块**必须**是版本 5.3.1。ASA FirePOWER 模块**只能**安装在运行 9.2.2 版或更高版本 ASA 软件的上述平台上。

具备 FirePOWER 服务的思科 ASA 的功能限制

如果使用防御中心管理具备 FirePOWER 服务的思科 ASA 设备，ASA FirePOWER 模块会提供最重要的系统策略，并将流量传送到 FireSIGHT 系统，以便进行访问控制、入侵检测和防御、发现以及高级恶意软件保护。

无论安装和应用了何种许可证，ASA FirePOWER 设备都无法通过 FireSIGHT 系统支持以下任何功能：

- ASA FirePOWER 设备**不**支持基于硬件的 FireSIGHT 系统功能，包括集群、堆叠、交换、路由、虚拟专用网络 (VPN) 和网络地址转换 (NAT)。

注意 ASA 平台提供上述功能，可通过 ASA 命令行界面 (CLI) 和自适应安全设备管理器 (ASDM) 配置这些功能。有关详细信息，请参阅 ASA FirePOWER 模块文档。

- **不能**使用防御中心的网络界面配置 ASA FirePOWER 接口。
- **不能**使用防御中心来关闭、重新启动或管理 ASA FirePOWER 进程。
- **不能**使用防御中心从 ASA FirePOWER 设备创建备份，或者从备份还原这些设备。
- **不能**使用 VLAN 标记条件编写用于匹配流量的访问控制规则。

ASA FirePOWER 设备**没有** FireSIGHT 网络界面。但是，它有软件和一个 ASA 平台专属的 CLI。使用这些特定于 ASA 的工具可安装系统以及执行其他特定于平台的管理任务。有关详细信息，请参阅 ASA FirePOWER 模块文档。

请注意，如果编辑 ASA FirePOWER 设备并从多情境模式切换到单情境模式（反之亦然），则设备会重命名其所有接口。您**必须**重新配置所有 FireSIGHT 系统安全区域、关联规则以及相关的配置，才能使用更新的 ASA FirePOWER 接口名称。

注意 如果 ASA FirePOWER 设备是在 SPAN 端口模式下部署的，防御中心**不会**显示 ASA 接口。

术语

5.3.1 版引入了通过 FireSIGHT 防御中心管理具备 FirePOWER 服务的思科 ASA 功能。如果您参阅版本 5.3 或版本 5.3.0.1 的相应文档，可能会注意到这些文档中使用的术语与版本 5.3.1 文档中的术语有所不同。

表 1　　术语更改

5.3.1 版本术语	说明
Cisco	原称为 *Sourcefire*
FireSIGHT 系统	原称为 *Sourcefire 3D 系统*
防御中心 FireSIGHT 防御中心 Cisco FireSIGHT 管理中心	原称为 *Sourcefire 防御中心*
受管设备	以前是 *Sourcefire 受管设备*
FireSIGHT 受管设备	是指 FireSIGHT 防御中心管理的所有设备（受管设备和 ASA 设备）
思科自适应安全设备 (ASA) ASA 设备	是指 Cisco ASA 硬件
具备 FirePOWER 服务的思科 ASA	是指安装了 ASA FirePOWER 模块的 ASA 设备
ASA FirePOWER 模块	是指安装在兼容 ASA 设备上的硬件和软件模块
ASA 软件	是指安装在思科 ASA 设备上的基本软件

提示 Cisco 文档可能会将防御中心称为 FireSIGHT 管理中心，防御中心和 FireSIGHT 管理中心是同一个设备。

早期版本引入的功能

早期版本中介绍的功能可能被其他新功能取代，或者通过已解决问题进行更新。

版本 5.3.1.3 引入了以下功能：

- 版本 5.3.1.3 不再提供默认关联策略。您必须创建自定义策略和规则。

版本 5.3.1.1 引入了以下特性和功能：

- 您现在可以使用 **GRE 47** 端口条件配置访问控制规则。
- 您现在可以使用防御中心代理服务器与 Cisco 安全管理器 (CSM) 通信。

- 您可以在“对象管理”(Object Management) 页面编辑设备集群、堆栈或集群堆栈的安全区列表后，在“设备管理”(Device Management) 页面（**设备 [Devices] > 设备管理 [Device Management]**）选择设备变更应用图标重新应用设备配置。
- 您现在可以通过“设备管理”(Device Management) 页面（**设备 [Devices] > 设备管理 [Devices Management]**）高级选项卡上的高级选项配置已注册的 ASA FirePOWER 设备。

文档更新

为版本 5.3.1.6 提供的文档包含如下错误的表述：

- *《FireSIGHT 系统用户指南》*包含如下错误的表述：在您无法登录设备管理界面的时候，您可以在不登录的情况下通过 LAN 上串行 (SOL) 连接在默认 (eth0) 管理接口上使用无人值守管理 (LOM) 来远程监控或管理系列 3 设备。(CSCuu17674)
- *《FireSIGHT 系统用户指南》*对于堆栈中设备有如下错误的表述：如果辅助设备发生故障，主设备会继续检测流量，生成警报，并将流量发送到所有辅助设备。在发生故障的辅助设备上，流量会被丢弃。系统会生成指示链路丢失的运行状况警报。

  该文档应指明：默认情况下，如果堆栈中的辅助设备出现故障，启用了可配置旁路的内联集将会在主设备上进入旁路模式。对于所有其他配置，系统会继续将均衡流量加载到发生故障的辅助设备。无论是哪一种情况，系统都会生成指示链路丢失的运行状况警报。（122708/CSCze88292、123380/CSCze88692 和 138433/CSCze91099）
- *《FireSIGHT 系统联机帮助》*未反映出以下情况：

  原始客户端 IP 地址提取自 X-Forwarded-For (XFF)、True-Client-IP 或自定义 HTTP 信头。要显示此字段的值，必须在网络分析策略中启用 HTTP 预处理程序“提取原始客户端 IP 地址”(Extract Original Client IP Address) 选项。或者，在网络分析策略的同一区域，还可以指定最多六个自定义客户端 IP 报头，并设置系统选择“原始客户端 IP 事件”(Original Client IP event) 字段值的优先顺序。请参阅第 25-33 页 *《FireSIGHT 系统用户指南》*的*选择服务器级 HTTP 标准化选项*部分，以了解更多信息。

  启用“提取原始客户端 IP 地址”(Extract Original Client IP Address) 后，请指定系统处理原始客户端 IP HTTP 信头的顺序。如果在受监控网络上您想要遇到除 X-Forwarded-For (XFF) 或 True-Client-IP 以外的原始客户端 IP 地址信头，则可以点击 “添加”(Add) 在优先级列表中添加最多 6 个额外的客户端 IP 信头名称。请注意，如果 HTTP 请求中出现多个 XFF 信头，“原始客户端 IP 事件”(Original Client IP event) 字段的值为优先级最高的信头。您可以使用每种信头类型旁边的向上和向下箭头图标调整其优先级。（139492/CSCze91210、141233/CSCze92868 和 144139/CSCze95050）
- *《FireSIGHT 系统联机帮助》*未反映出以下情况：如果修改 ASA 设备的安全情境，并从单情境模式切换到多情境模式，或从多情境模式切换到单情境模式，系统会从安全区配置中移除接口。（141050/CSCze92286、141064/CSCze92547）
- 交付时配有适用于版本 5.3.1 的 *《FireSIGHT 系统联机帮助》*的设备将系列 2、系列 3、虚拟和 X 系列设备列为支持的设备。而并不支持这些设备。（144113/CSCze95418）
- *《FireSIGHT 系统用户指南》*未反映出以下情况：如果您向防御中心注册设备集群、堆栈或集群堆栈，则必须手动重新应用设备配置。（142411/CSCze92729、141602/CSCze92992）
- *《FireSIGHT 系统联机帮助》*未反映出以下情况：使用 NT LAN Manager (NTLM) 身份验证的代理无法与综合安全情报云通信以接收信息。如果要使用基于云的功能，请确保为您的代理配置不同的身份验证。(143613/CSCze94827)

- *《FireSIGHT 系统用户指南》*未反映出以下情况：

  防御中心完成云查找后，首次检测到的文件将分配有一个处置结果。除非文件立即分配有一个处置结果，否则系统将生成一个文件事件，但是**无法**存储文件。

  如果之前未检测到的文件与具有阻止恶意软件操作的文件规则相匹配，则随后的云查找将立即返回性质，从而使系统可以存储文件并生成事件。

  如果之前未检测到文件与具有恶意软件云查找操作的文件规则相匹配，则系统将生成文件事件，但需要额外的时间执行云查找并返回性质。由于这种延迟，系统无法存储与具有恶意软件云查找操作的文件规则想匹配的文件，直到在网络上第二次看到这些文件。（143973/CSCze95101、144180/CSCze94566）
- *《FireSIGHT 系统用户指南》*未反映出以下情况：您现在可以选择是否在策略应用过程中检测流量。在重负载系统中，在策略应用过程中检测流量会影响网络吞吐量和延迟。如果该负面影响对于您的网络设置不太理想且连接比检测更重要，取消勾选该复选框会在策略应用过程中临时禁用检测，并可确保在该过程中不会丢失任何数据包。在策略应用成功之后，检测会恢复正常。(144574/CSCze95159)
- *《FireSIGHT 系统用户指南》*包含如下错误的表述：在配置管理外壳访问时，外壳用户可以使用由小写、大写或大小写混合的字母组成的用户名登录。正确的表述应该是：外壳用户可以使用由小写字母组成的用户名登录。(144936/CSCze95327)
- *《FireSIGHT 系统用户指南》*包含对于 5.3.1 STIG 版本说明的错误引用。适用于版本 5.3 的 STIG 版本说明应同时用于版本 5.3.1。有关 5.3 STIG 版本说明，请联系支持人员。(CSCur79089)
- 关于使用用户名“admin”以及在部署安装向导中指定的新管理员帐户密码在 VMware 控制台登录虚拟设备，*《FireSIGHT 系统虚拟安装指南》*包含如下错误的表述：如果您没有使用向导更改密码，或者正在使用 ESXi OVF 模板进行部署，请使用“Cisco”作为密码。正确的表述应该是：如果您没有使用向导更改密码，或者正在使用 ESXi OVF 模板进行部署，请使用 Sourcefire 作为密码。(CSCut77002)

准备工作：重要更新和兼容性说明

在开始版本 5.3.1.6 的更新过程之前，您应熟悉更新过程中的系统行为，以及任何兼容性问题或者更新前后需要进行的配置更改。

注意 Cisco 强烈建议您在维护时间段、或在中断对部署影响最小的时间段执行更新。

有关详细信息，请参阅以下各节：

配置和事件备份准则

在您开始更新之前，Cisco 强烈建议删除或移动设备上的所有备份文件，然后将当前的事件和配置数据备份到外部位置。

可使用防御中心为防御中心本身及其管理的设备备份事件和配置数据。有关备份和还原功能的详细信息，请参阅*《FireSIGHT 系统用户指南》*。

注意 防御中心会清除来自以前的更新的本地存储备份。要保留存档的备份，请将备份存储到外部。

更新期间的流量和检查

更新过程（以及卸载更新）会重启 ASA FirePOWER 设备。取决于设备的配置和部署方式，以下功能会受到影响：

- 流量检查，包括应用感知和控制、URL 过滤、安全情报、入侵检测和防御以及连接日志记录
- 链路状态

流量检查和链路状态

在内联部署中，ASA FirePOWER （取决于型号）可通过应用控制、用户控制、URL 过滤、安全情报和入侵防御，在被动部署中，您可以执行入侵检测和收集发现数据，而不会影响网络流量。有关设备功能的详细信息，请参阅*《FireSIGHT 系统安装指南》*。

下表提供了有关流量、检查和链路状态在更新时会受到何种影响（取决于部署）的详细信息。

表 2　网络流量中断

部署	网络流量是否被中断？
线内	在整个更新过程中，网络流量会被阻止。
被动	在更新过程中，网络流量不会中断，但也不会对其进行检查。

更新过程中的审计日志记录

在更新具有网络界面的设备时，系统完成其更新前任务之后，简化的更新界面页面将会显示。直到更新过程完成和设备重新启动之后，对设备的登录尝试才会反映在审核日志中。

更新至版本 5.3.1.6 的版本要求

要将设备更新至版本 5.3.1.6，防御中心必须至少运行 5.3.0.1 版本。如果运行的是较低版本，可从支持站点获取更新。

注意 受管设备或 X-Series 专用 Sourcefire 软件不支持此更新。

设备的当前版本与发行版本（版本 5.3.1.6）越接近，更新所需的时间就越少。

更新版本 5.3.1.6 的时间和磁盘空间要求

下表提供了版本 5.3.1.6 更新的磁盘空间和时间准则。请注意，使用防御中心更新 ASA FirePOWER 设备时，防御中心的 `/Volume` 分区需要有额外的磁盘空间。

注意 在更新过程中的任何时候都**不得**重新开始更新或重新启动设备。Cisco 提供的时间预估仅供参考，实际更新时间因设备型号、部署和配置而异。请注意，在更新的预先检查部分和重启后，系统可能会呈非活动状态；这是预期的行为。

更新的重新启动部分包括数据库检查。如果在数据库检查过程中发现错误，更新需要更长时间才能完成。与数据库交互的系统后台守护程序，在数据库检查和修复期间不会运行。

如果遇到更新进度方面的问题，请联系支持部门。

表 3　　时间和磁盘空间要求

设备	/上的空间	/Volume 上的空间	管理器中的/Volume 上的空间	Time
系列 3 防御中心	232 MB	6150 MB	n/a	107 分钟
虚拟防御中心	232 MB	6150 MB	n/a	因硬件而异
具备 FirePOWER 服务的思科 ASA	69 MB	5344 MB	899 MB	63 分钟

更新至版本 5.3.1.6 后的产品兼容性

必须使用版本至少为 5.3.0.1 版本的防御中心来管理运行版本 5.3.1.6 的设备。运行版本 5.3.1.6 的防御中心可管理安装在 ASA 设备上的 ASA FirePOWER 模块。防御中心管理的设备必须至少运行下表中确定的版本。

表 4　　管理版本要求

设备	要运行版本 5.3.1.6 的防御中心管理必须达到的最低版本
物理和虚拟受管设备	FireSIGHT 系统 5.3 版本
ASA FirePOWER 模块	FireSIGHT 系统 5.3.1 版本

操作系统兼容性

您可以在以下托管环境中托管 64 位虚拟设备：

- VMware vSphere 虚拟机监控程序/VMware ESXi 5.0
- VMware vSphere 虚拟机监控程序/VMware ESXi 5.1
- VMware vCloud Director 5.1

您可以在运行 9.2.2 版或更高版本的以下 ASA 平台上更新 FireSIGHT 系统：

- ASA5512-X
- ASA5515-X
- ASA5525-X
- ASA5545-X

- ASA5555-X
- ASA5585-X-SSP-10、ASA5585-X-SSP-20、ASA5585-X-SSP-40 和 ASA5585-X-SSP-60

有关详细信息，请参阅*《FireSIGHT 系统安装指南》*或*《FireSIGHT 系统虚拟安装指南》*。

网络浏览器兼容性

用于 FireSIGHT 系统的版本 5.3.1.6 网络界面在下表所列的浏览器上进行过测试。

表 5　　受支持的网络浏览器

浏览器	需要启用的选项和设置
Chrome 45	JavaScript、Cookie
Firefox 40	JavaScript、Cookie、安全套接字层 (SSL) v3
Microsoft Internet Explorer 9、10 和 11	JavaScript、Cookie、安全套接字层 (SSL) v3、128 位加密、**活动脚本**安全设置、兼容性视图、将**检查存储网页的较新版本**设置为**自动**

注意　在使用 Microsoft Internet Explorer 11 上传文件到服务器时，版本 5.3.1.1 和更高版本当前不支持包含本地目录路径。思科建议在 Internet Explorer **工具 (Tools) > Internet 选项 (Internet Options) > 安全 (Security) > 自定义级别 (Custom level)** 页面禁用**将文件上传到服务器时包含本地目录路径 (Include local directory path when uploading files to server)** 选项。

屏幕分辨率兼容性

Cisco 建议，至少选择 1280 像素宽的屏幕分辨率。用户界面兼容低分辨率，但高分辨率可优化显示效果。

安装更新

在您开始更新之前，必须通读和理解这些版本说明，特别是准备工作：重要更新和兼容性说明（第 5 页）。

要将至少运行 5.3.0.1 版本 FireSIGHT 系统的设备更新至版本 5.3.1.6，请参阅以下概述的准则和操作步骤：

- 更新防御中心（第 9 页）
- 更新具备 FirePOWER 服务的思科 ASA（第 11 页）

注意　物理或虚拟受管设备和 X-Series 专用 Sourcefire 软件**不**支持此更新。

注意　请**不要**在更新期间重新启动或关闭设备，直至看到登录提示。系统在更新的预先检查部分可能呈非活动状态，这是预期的行为，不需要您重新启动或关闭设备。

何时执行更新

由于更新过程可能会影响流量检查、流量和链路状态，Cisco **强烈**建议您在维护时段或者在中断对部署影响最小的时间执行更新。

安装方法

使用防御中心的网络界面执行更新。先更新防御中心，然后用它更新其管理的设备。

安装顺序

先更新防御中心，再更新其管理的设备。

在成对的防御中心上安装更新

开始更新高可用性对中的一个防御中心时，如果它尚未就绪，另一个防御中心将会变为主防御中心。此外，成对的防御中心将会停止共享配置信息。成对的防御中心在常规同步过程中**不会**接收软件更新。

为确保操作的连续性，请**不要**同时更新成对的防御中心。应先完成辅助防御中心的更新操作步骤，然后再更新主防御中心。

安装后

当您在防御中心或受管设备上执行更新后，**必须**重新应用设备配置和访问控制策略。应用访问控制策略可能会导致流量和处理的短时间暂停，还可能会导致一些数据包未经检查地通过。有关详细信息，请参阅*《FireSIGHT 系统用户指南》*。

您还应执行多个额外的更新后步骤，以确保部署可正常执行。其中包括：

- 验证更新是否已成功
- 确保部署中的所有设备都能够成功通信
- 更新至版本 5.3.1.6 的最新补丁（如有），以利用最新的增强功能和安全修复程序
- 或者，更新入侵规则和漏洞数据库 (VDB)，并重新应用访问控制策略
- 根据更改的功能（第 2 页）中的信息，进行必要的配置更改

以下各节不仅包括有关执行更新的详细说明，还包括有关完成任何更新后步骤的详细说明，确保完成所有列出的任务。

更新防御中心

按照本节所述的操作步骤更新防御中心（包括虚拟防御中心）。对于版本 5.3.1.6 更新，防御中心会重启。

注意 在您更新防御中心之前，请将访问控制策略重新应用至所有受管设备。否则，对受管设备的最终更新可能会失败。

注意 更新期间，在看到登录提示之前，请**不要**再重新启动或关闭设备。系统在更新的预先检查部分可能呈非活动状态，这是预期的行为，不需要您重新启动或关闭设备。

注意 将防御中心更新至版本 5.3.1.6，会从设备中移除现有的卸载程序。

要更新防御中心，请执行以下操作：

步骤 1 阅读这些版本说明，并完成必要的更新前任务。

有关详细信息，请参阅准备工作：重要更新和兼容性说明（第 5 页）。

步骤 2 从支持站点下载更新：

- 对于系列 3 和虚拟防御中心：

  `Sourcefire_3D_Defense_Center_S3_修补-5.3.1.6-16.sh`

注意 直接从支持站点下载更新。如果通过邮件传输更新文件，可能会损坏该文件。

步骤 3 选择**系统 (System) > 更新 (Updates)**，然后在**产品更新 (Product Updates)** 选项卡中点击**上传更新 (Upload Update)**，将更新上传到防御中心。浏览到更新并点击**上传 (Upload)**。

更新将会上传到防御中心。网络界面会显示您上传的更新的类型、其版本号以及生成更新的日期和时间。

步骤 4 确保部署中的设备能够成功通信，并且运行状况监控器未报告任何问题。

步骤 5 查看任务队列（**系统 [System] > 监控 [Monitoring] > 任务状态 [Task Status]**），确保没有正在进行的任务。

正在运行的任务会在更新开始时停止，成为失败的任务，并且不能恢复，您必须在更新完成后，将其从任务队列中手动删除。任务队列每 10 秒自动刷新一次，**必须**等到所有长时间运行的任务都完成后，才能开始更新。

步骤 6 选择**系统 (System) > 更新 (Updates)**。

系统将显示“产品更新”(Product Updates) 选项卡。

步骤 7 点击上传的更新旁边的安装图标。

系统将显示“安装更新”(Install Update) 页面。

步骤 8 选择防御中心并点击 **Install**。确认要安装更新并重新启动防御中心。

更新过程将会开始。可以开始在任务队列（**系统 (System) > 监控 (Monitoring) > 任务状态 (Task Status)**）中监控更新进度。但是，在防御中心完成其必要的更新前检查后，系统会使您注销。当您重新登录时，系统会显示“更新状态”(Upgrade Status) 页面。“更新状态”(Upgrade Status) 页面会显示进度条，提供当前正在运行的脚本的相关详细信息。

如果更新由于任何原因而失败，该页面会显示错误消息，其中指明失败的时间和日期、更新失败时正在运行的脚本，并提供有关如何联系支持部门的说明。请**不要**重新开始更新。

注意 如果更新出现任何其他问题（例如，手动刷新“更新状态”(Upgrade Status) 页面后，几分钟都没有显示进度），请**不要**重新开始更新，而应联系支持部门。

更新完成后，防御中心会显示成功消息，并重新启动。

更新过程将会开始。您可以在任务队列中监控更新进度（**系统 [System] > 监控 [Monitoring] > 任务状态 [Task Status]**）。

注意 在更新完成并且防御中心重新启动之前，请**不要**使用网络界面执行任何其他任务。在更新完成之前，网络界面可能会变得不可用，并且防御中心可能会使您注销。这是预期的行为，重新登录便可查看任务队列。如果更新仍在运行，请**不要**使用网络界面，直到更新完成。如果更新出现问题（例如，如果任务队列指示更新已失败，或者手动刷新任务队列后，几分钟都没有显示进度），请**不要**重新开始更新，而应联系支持部门。

步骤 9 在更新完成后，应清除浏览器缓存，并强制要求浏览器重新加载。否则，用户界面可能会出现意外行为。

步骤 10 登录至防御中心。

步骤 11 审阅并接受《最终用户许可协议 (EULA)》。请注意，如果不接受 EULA，您将从设备注销。

步骤 12 选择**帮助 (Help) > 关于 (About)**，确认软件版本是否已正确列出：版本 5.3.1.6。另请注意，防御中心上的规则更新和 VDB 的版本，您随后会需要这些信息。

步骤 13 确保部署中的设备能够成功通信，并且运行状况监控器未报告任何问题。

步骤 14 如果支持站点上的可用规则更新比防御中心上的规则要新，请导入较新的规则。

有关规则更新的详细信息，请参阅*《FireSIGHT 系统用户指南》*。

步骤 15 如果支持站点上的可用 VDB 比防御中心上的 VDB 要新，请安装最新的 VDB。

安装 VDB 更新会导致流量和处理的短时间暂停，还可能会导致一些数据包未经检查地通过。有关详细信息，请参阅*《FireSIGHT 系统用户指南》*。

步骤 16 将设备配置重新应用到所有设备。

要重新激活灰显的**应用 (Apply)** 按钮，请在设备配置中编辑任意接口，然后在不进行更改的情况下，点击**保存 (Save)**。

步骤 17 将访问控制策略重新应用到所有设备。

注意 请**不要**单独重新应用入侵策略，必须全面重新应用所有访问控制策略。

应用访问控制策略可能会导致流量和处理的短时间暂停，还可能会导致一些数据包未经检查地通过。有关详细信息，请参阅*《FireSIGHT 系统用户指南》*。

步骤 18 如果支持站点提供了版本 5.3.1.6 的补丁，请按照该版本的《*FireSIGHT 系统版本说明*》所述，应用最新的补丁。**必须**更新至最新补丁才可利用最新增强功能和安全修复程序。

注意 请注意在更新完防御中心后，设备变更的应用图标会启用，并显示为绿色，表明需要将变更重新应用到您的注册设备。

更新具备 FirePOWER 服务的思科 ASA

将防御中心更新至版本 5.3.1.6 后，可以使用它们来更新其管理的 ASA FirePOWER 设备。

防御中心必须运行 5.3.0.1 或更高版本才能将其 ASA FirePOWER 设备更新至版本 5.3.1.6。

更新 ASA FirePOWER 设备分两步进行。首先，从支持站点下载更新，并将其上传到管理防御中心。接着，安装软件。可一次对多台 ASA FirePOWER 设备进行更新，但这些设备必须都使用同一个更新文件。

对于版本 5.3.1.6 更新，所有 ASA FirePOWER 设备都会重新启动。更新过程还可能会影响流量和链路状态，具体取决于 ASA FirePOWER 设备的配置和部署。有关详细信息，请参阅更新期间的流量和检查（第 6 页）。

注意 在更新 ASA FirePOWER 设备之前，请使用其管理防御中心将适当的访问控制策略重新应用至 ASA FirePOWER 设备。否则，ASA FirePOWER 设备的更新可能会失败。

注意 更新期间，在看到登录提示之前，请**不要**再重新启动或关闭设备。系统在更新的预先检查部分可能呈非活动状态，这是预期的行为，不需要您重新启动或关闭设备。

要更新具备 FirePOWER 服务的思科 ASA：

步骤 1 阅读这些版本说明，并完成必要的更新前任务。

有关详细信息，请参阅准备工作：重要更新和兼容性说明（第 5 页）。

步骤 2 更新 ASA FirePOWER 设备的管理防御中心上的软件，请参阅更新防御中心（第 9 页）。

步骤 3 从支持站点下载更新：

```
Cisco_Network_Sensor_Patch-5.3.1.6-16.sh
```

注意 直接从支持站点下载更新。如果通过邮件传输更新文件，可能会损坏该文件。

步骤 4 要将更新上传至防御中心，请选择**系统 (System) > 更新 (Updates)**，然后点击“产品更新”(Product Updates) 选项卡中的**上传更新 (Upload Update)**。浏览到更新并点击**上传 (Upload)**。

更新将会上传到防御中心。网络界面会显示您上传的更新的类型、其版本号以及生成更新的日期和时间。该页面还会指明在更新过程中是否需要重新启动。

步骤 5 确保部署中的设备能够成功通信，并且运行状况监控器未报告任何问题。

步骤 6 点击要安装的更新旁边的安装图标。

系统将显示“安装更新”(Install Update) 页面。

步骤 7 选择要安装更新的 ASA FirePOWER 设备。

步骤 8 点击**安装**。确认要安装更新，并重新启动 ASA FirePOWER 设备。

步骤 9 更新过程将会开始。可在防御中心的任务队列（**系统 [System] > 监控 ([Monitoring] > 任务状态 [Task Status]**）中监控更新进度。

请注意，在更新过程中，ASA FirePOWER 设备可能会重新启动两次，这是预期的行为。

注意 如果更新出现问题（例如，如果任务队列指示更新已失败，或者手动刷新任务队列后，几分钟都没有显示进度），请不要重新开始更新，而应联系支持部门。

步骤 10 选择**设备 (Devices) > 设备管理 (Device Management)**，并确认更新的 ASA FirePOWER 是否具有正确的软件版本：版本 5.3.1.6。

步骤 11 确保部署中的设备能够成功通信，并且运行状况监控器未报告任何问题。

步骤 12 将设备配置重新应用到所有 ASA FirePOWER 设备。

提示 要重新激活灰显的**应用 (Apply)** 按钮，请在设备配置中编辑任意接口，然后在不进行更改的情况下，点击**保存 (Save)**。

步骤 13 将访问控制策略重新应用到所有 ASA FirePOWER 设备。

应用访问控制策略可能会导致流量和处理的短时间暂停，还可能会导致一些数据包未经检查地通过。有关详细信息，请参阅《*FireSIGHT 系统用户指南*》。

步骤 14 如果支持站点提供了版本 5.3.1.6 的补丁，请按照该版本的《*FireSIGHT 系统版本说明*》所述，应用最新的补丁。**必须**更新至最新补丁才可利用最新增强功能和安全修复程序。

卸载更新

以下各节帮助您从设备卸载版本 5.3.1.6 更新：

计划卸载

在您卸载更新之前，必须通读并理解以下各节。

卸载方法

必须在本地卸载更新。**不能**使用防御中心从 ASA FirePOWER 设备卸载更新。

对于所有物理设备和虚拟防御中心，请使用本地网络界面卸载更新。由于具备 FirePOWER 服务的思科 ASA 没有网络界面，因此，**必须**使用 bash 外壳卸载更新。

卸载顺序

卸载更新与安装更新的顺序相反。也就是说，应先从 ASA FirePOWER 设备卸载更新，然后再从防御中心进行卸载。

从内联部署的设备卸载更新

在卸载更新时，ASA FirePOWER 设备**不会**执行流量检查、交换、路由或相关功能。卸载过程还可能会影响流量和链路状态，具体取决于设备的配置和部署。有关详细信息，请参阅更新期间的流量和检查（第 6 页）。

卸载更新和联机帮助

卸载版本 5.3.1.6 更新**不会**将联机帮助还原到其上一版本。如果联机帮助的版本与 FireSIGHT 系统软件版本不匹配，则联机帮助中可能包含不可用功能的文档，并且可能存在情景敏感性和链接功能方面的问题。

卸载后

卸载更新后，应执行多个步骤来确保部署正常运行。这些步骤包括验证卸载是否成功，以及验证部署中的所有设备是否能够成功地进行通信。

以下各节不仅包括有关执行更新的详细说明，还包括有关完成任何更新后步骤的详细说明。确保完成所有列出的任务。

从 ASA FirePOWER 设备卸载更新

以下操作步骤说明如何从 ASA FirePOWER 设备卸载版本 5.3.1.6 更新。**不能**使用防御中心从 ASA FirePOWER 设备卸载更新。

卸载版本 5.3.1.6 更新会导致设备运行版本 5.3.1.5。有关卸载旧版本的信息，请参阅该版本的 *FireSIGHT 系统版本说明*。

卸载版本 5.3.1.6 更新会重新启动设备。ASA FirePOWER 设备在更新过程中，**不会**执行流量检查或相关功能。更新过程还可能会影响流量，具体取决于设备的配置和部署。有关详细信息，请参阅更新期间的流量和检查（第 6 页）。

要从 ASA FirePOWER 设备卸载更新，请执行以下操作：

步骤 1 阅读并理解计划卸载（第 13 页）。

步骤 2 通过 SSH 或虚拟控制台，以管理员身份登录至设备。

步骤 3 在 CLI 提示符后，键入 `expert` 以访问 bash 外壳。

步骤 4 在 bash 外壳提示符后，键入 `sudo su -`。

步骤 5 键入管理员密码继续以根权限执行此过程。

步骤 6 在提示符后，在一行中输入以下内容：

```
install_update.pl /var/sf/updates/Cisco_Network_Sensor_Patch_Uninstaller-5.3.1.6-16.sh
```

卸载过程将会开始。

注意 如果卸载出现问题，请不要重新开始卸载，而应联系支持部门。

步骤 7 在卸载完成后，应清除浏览器缓存，并强制要求浏览器重新加载。否则，用户界面可能会出现意外行为。

步骤 8 登录防御中心。

步骤 9 选择**帮助 (Help) > 关于 (About)**，确认软件版本是否已正确列出：5.3.1 版。

步骤 10 确保部署中的设备能够成功通信，并且运行状况监控器未报告任何问题。

从防御中心卸载更新

使用以下步骤从防御中心和虚拟防御中心卸载版本 5.3.1.6 更新。注意卸载过程会重新启动防御中心。

卸载版本 5.3.1.6 更新会导致防御中心运行5.3.0.1 版本。有关卸载旧版本的信息，请参阅该版本的 *FireSIGHT 系统版本说明*。

要从防御中心卸载更新，请执行以下操作：

步骤 1 阅读并理解计划卸载（第 13 页）。

步骤 2 确保部署中的设备能够成功通信，并且运行状况监控器未报告任何问题。

步骤 3 查看任务队列（**系统 [System] > 监控 [Monitoring] > 任务状态 [Task Status]**），确保没有正在进行的任务。

正在运行的任务会在卸载开始时停止，成为失败的任务，并且不能恢复。您必须在卸载完成后，将其从任务队列中手动删除。任务队列每 10 秒自动刷新一次，**必须**等到所有长时间运行的任务都完成后，才能开始卸载。

步骤 4 选择**系统 (System) > 更新 (Updates)**。

系统将显示“产品更新”(Product Updates) 选项卡。

步骤 5 点击与要移除的更新匹配的卸载程序旁边的安装图标。

系统将显示“安装更新”(Install Update) 页面。

步骤 6 选择防御中心并点击 **Install**，然后确认要卸载该更新并重新启动设备。

卸载过程将会开始。您可以在任务队列中监控卸载进度（**系统 [System] > 监控 [Monitoring] > 任务状态 [Task Status]**）。

注意 在卸载完成并且防御中心重新启动之前，请**不要**使用网络界面执行任何其他任务。在卸载完成之前，网络界面可能变得不可用，并且防御中心可能会使您注销。这是预期的行为；重新登录便可查看任务队列。如果卸载仍在运行，请**不要**使用网络界面，直至卸载完成。如果卸载出现问题（例如，如果任务队列指示更新已失败，或者手动刷新任务队列后，几分钟都没有显示进度），请**不要**重新开始卸载，而应联系支持部门。

步骤 7 在卸载完成后，应清除浏览器缓存，并强制要求浏览器重新加载。否则，用户界面可能会出现意外行为。

步骤 8 登录防御中心。

步骤 9 选择**帮助 (Help) > 关于 (About)**，确认软件版本是否已正确列出：5.3.1 版。

步骤 10 确保部署中的设备能够成功通信，并且运行状况监控器未报告任何问题。

已解决的问题

您可以使用 Cisco 漏洞搜索工具 (https://tools.cisco.com/bugsearch/) 跟踪此版本解决的缺陷。以下各节列出了版本 5.3.1.6 更新中已解决的问题。

版本 5.3.1.6 中已解决的问题：

- 安全问题解决了会使客户端连接遭到外部攻击的多个 SSLv3 漏洞，如 CVE-2014-8275 和 CVE-2015-0204 中所述。
- 安全问题解决了 Linux、NTP 及其他第三方的多个漏洞问题，如 CVE-2011-2699、CVE-2011-4131、CVE-2012-3400、CVE-2013-1944、CVE-22013-4545、CVE-22013-21944 和 CVE-22014-29296。
- 安全问题解决了一个随机脚本注入漏洞，该漏洞使未经身份验证的远程攻击者可以攻击 GNU C 函数库的 DNS 解析功能，如 CVE-2013-7423 中所述。
- 解决了以下问题：当防御中心更新访问控制策略在应用策略时所引用的大型安全情报源时，受管设备停止处理流量。(CSCus19921)
- 解决了以下问题：在注册到防御中心（至少运行版本 5.4 ）的设备（至少运行版本 5.3）上运行 `sudo ips_profile` 外壳命令，会导致规则分析脚本失败。(CSCuu02211)
- 解决了思科云不断检测更新下载且导致系统问题的问题。(CSCuu04844)
- 解决了以下问题：如果您将设为**阻止**（默认操作）的访问控制策略应用到 ASA FirePOWER 设备，系统错误地将策略的默认操作还原到**重置**而不是**阻止**。(CSCuu60713)
- 解决了以下问题：系统不会正确地将新添加的注释的编辑项编码至访问控制策略规则。(CSCus83065)
- 解决了以下问题：如果您创建产品图集和**添加固定图**，系统不会在供应商下拉菜单中生成供应商列表。(CSCuu79373)
- 解决了以下问题：如果您生成了一个报告，离开“报告模板”(Report Templates) 选项卡，然后生成另一个报告，**发送电子邮件 (Send email)** 复选框无法保持选定状态。(CSCuu97750)
- 解决了以下问题：即使存在 URL 过滤许可证，“产品许可”(Product Licensing) 控制面板构件未列出任何 URL 过滤许可证。(CSCuu97762)
- 解决了以下问题：如果您添加一个以上的许可证至 3D8250 设备并添加一个许可至另一台系列 3 设备，“许可证”(License) 页面错误地在错误设备下列出许可证。(CSCuu99789)

版本 5.3.1.5 解决的问题：

- 安全问题解决了 HTTP 连接处理漏洞，该漏洞允许用户被重定向到恶意网站，如 CVE-2015-0706 中所述。
- 安全问题解决了 Linux 及其他第三方的多个漏洞问题，如 CVE-2011-1927、CVE-2012-2744 和 CVE-2015-1781 中所述。
- 安全问题解决了跨站脚本 (XSS) 漏洞问题，如 CVE-2015-0707 中所述。
- 解决了以下问题：生成的事件错误地将文件威胁级别报告为数字而不是**低**、**中等**、**高**或**非常高**。(142290/CSCze93722)
- 改善了 URL 拦截和 URL 过滤问题。(144198/CSCze94590)
- 解决了以下问题：如果您在“对象管理”(Object Management) 页面中编辑了接口安全区，当堆栈设备配置不是最新版本时，它仍显示为最新版本。(144626/CSCze94847)
- 解决了以下问题：如果您在“入侵规则编辑器”(Intrusion rule Editor) 页面编辑了一个本地规则，系统在查看规则文档而不是触发事件的规则配置时，系统显示已生成的事件数据的当前本地规则配置。(145118/CSCze95346)
- 解决了以下问题：如果您在防御中心上启用了远程存储并安排了邮件警报响应，安排程序禁用远程存储，而且远程存储备份失败。(145288/CSCze95993)
- 解决了以下问题：如果您导入引用了共享层的策略，导入策略会失败。(144946/CSCze96151)
- 解决了以下问题：如果您创建了一条关联规则，将它配置为当**发生入侵事件**或**发生连接事件**时，并选择**入口安全区域**、**出口安全区域**、**入接口**或**出接口**作为条件，系统无法识别规则，并且未触发与规则匹配的流量。(CSCur59840)
- 解决了以下问题：如果已注册 ASA FirePOWER 设备的密码包含不受支持的字符，系统会生成`内部服务器错误 (Internal Server Error)`消息。(CSCus68604)
- 解决了以下问题：如果您的系统在安装了 VDB 后重启，而且您的访问策略中**应用策略时检查流量 (Inspect Traffic During Policy Apply)** 选项已取消选中，您的系统上的网络连接断开。(CSCut08225)
- 解决了以下问题：如果您编辑了一个包含多个 URL 类别条件的访问控制规则并尝试删除其中某个条件，Web 管理接口仅删除所列的第一个类别条件。(CSCut25082)
- 当 CPU 利用率从高级变为正常状态时，系统会对所有 CPU 上报恢复事件。(CSCut27600)
- 解决了以下问题：当网络中只有一个子集受到监控，系统不会显示主机配置文件中的某些 Web 应用信息。（解决了以下问题：当网络中只有一个子集受到监控，系统不会显示主机配置文件中的某些 Web 应用信息。(CSCut36536)）
- 解决了以下问题：如果您为生成的事件创建并编辑一个搜索，然后在搜索开始之前取消搜索，系统会将您重定向至与含错误搜索名称的搜索相关的事件页面。(CSCut63265)
- 如果由于您当前配置存在问题，导致网络轨迹文件不可用，系统生成`基于可配置的最大值，由于相关文件事件被修剪，网络文件轨迹对恶意软件事件不可用`消息。(CSCut63362)
- 解决了以下问题：如果在不重启 SFR5585X 服务卡的情况下重启配置有大量子接口的 ASA5585X 设备，SFR5585X 服务卡出现故障。(CSCut89619)
- 解决了以下问题：如果您将以 Cisco 开头的 RPM 文件，RPM 页面管理器 (RPM) 安装历史记录无法正确重置。(CSCut98525)
- 解决了以下问题：运行版本 5.4.1 的防御中心无法将策略应用于运行版本 5.3.1.5 的设备。(CSCuu16406)
- 解决了以下问题：如果您将系统的时区改为 UTC 东部的一个时区并添加一个包含至少一个非活动周期的关联规则至关联策略，策略应用会失败。(CSCuu37600)
- 解决了以下问题：如果您创建一个包含地理定位条件的访问控制策略，本应该匹配条件的流量不匹配条件。(CSCuu48800)

- 提高了 SFDataCorrelator 的稳定性。(CSCuu53215)
- 解决了以下问题：如果您在启用了 IPv6 地址的情况下将防御中心配置为使用静态 IPv4 地址，并使用 IPv6 地址访问防御中心的接口，访问控制策略编辑器页面没有加载。(CSCuu83933)

版本 5.3.1.4 解决的问题：

- 安全问题解决了多个跨站脚本 (XSS) 漏洞。（CSCur25518、CSCus07858、CSCus07875）
- 安全问题解决了会使客户端连接遭到外部攻击的多个 SSLv3 漏洞，如 CVE-2014-3569、CVE-2014-3570、CVE-2014-3572、CVE-2015-0204、CVE-2015-0286、CVE-2015-0287、CVE-2015-0289、CVE-2015-0292 和 CVE-2015-0293 中所述。
- 改善了数据修剪的功能。(141894/ CSCze92576)
- 解决了以下问题：防御中心或受管设备生成非受管磁盘利用率高的运行状况警报。(145221/CSCze95877)
- 改善了多个控制面板构件。(CSCus11068)
- 解决了以下问题：如果您将访问控制策略应用到集群设备，即使操作队列任务已成功完成，访问控制策略页面依然显示策略应用状态为待处理 (pending)。(CSCus86011)

版本 5.3.1.3 解决的问题：

- 安全问题解决了一个随机脚本注入漏洞，该漏洞使未经身份验证的远程攻击者可以攻击 GNU C 函数库。CVE-2015-0235 对该问题进行了修复。
- 安全问题解决了会使客户端连接遭到外部攻击的多个 SSLv3 漏洞。CVE-2014-3566 对该问题进行了修复。
- 安全问题解决了多个注入漏洞，如 CVE-2007-6750 中所述。
- 安全问题解决了多个跨站脚本 (XSS) 漏洞。
- 安全问题解决了通用唯一标识符 (UUID) 处理方面的未经授权访问漏洞。
- 根据 *FireSIGHT 系统联机帮助*记录，HTTP X-Forwarded-For (XFF) 报头在入侵策略规则编辑器中现为可配置选项。（139492/CSCze91210、141233/CSCze92868）
- 根据 *FireSIGHT 系统联机帮助*记录，在“设备管理”(Device Management) 页面（**设备 [Devices] > 设备管理 [Device Management]**）中，当过时的设备配置策略需要重新应用时，设备更改应用图标激活并变为绿色。(144142/CSCze95449)
- 解决了以下问题：注册至防御中心（至少运行版本 5.3.1）的 3D9900 设备（运行版本 5.3.0.3 以前的版本）不生成入侵事件。(144171/CSCze94677)
- 提高了 URL 信誉和检测功能的可靠性。(144196/CSCze94549)
- 解决了以下问题：系统将 DNS 流量作为 OpenVPN、QQ 和 Viber 流量进行处理。(144546/CSCze95528)
- 解决以下问题：在某些情况下，系统错误地将 SMTP 流量识别为 FTP 流量，对误报的 FTP 命令生成入侵事件。(144591/CSCze95154)
- 解决了以下问题：如果您将一个设备堆栈添加至组，然后将该组添加至您的目标列表，系统会显示该组中的堆栈为两个目标而不是一个目标。(145008/CSCze95316)
- 解决了以下问题：如果您尝试在管理 X-系列设备的同时下载更新，自动更新会失败。(145045/CSCze95716)
- 解决了以下问题：运行 5.3 版本系统错误地报告大于 32767 的端口号。(145183/CSCze95390)
- 解决了以下问题：防御中心或受管设备生成非受管磁盘利用率高的运行状况警报。(145221/CSCze9587)

- 解决了以下问题：如果您尝试使用**产品更新 (Product Updates)** 页面（**系统 [System] > 更新 [Updates]**）中的**下载更新 (Download Updates)** 按钮更新您的系统，系统会提供一个错误的补丁版本。(145172/CSCze95369)
- 解决了以下问题：系统不提供 URL 类别或信誉信息。(CSCur38971)
- 解决了以下问题：由启用了预处理程序选项的入侵规则生成的事件的系统日志警报消息是 Snort 警报消息而不是自定义消息。(CSCur40263)
- 解决了以下问题：主机配置文件错误地显示单台受管设备有多个 IP 地址。（CSCur42027、CSCur59486）
- 解决了以下问题：如果您创建一个自定义工作流程并尝试打开入侵事件的数据包视图，系统会打开错误入侵事件的数据包视图。(CSCur48743)
- 解决了以下问题：如果您创建一个安装最新数据库版本 (VDB) 的计划任务而且防御中心已经安装了 VDB，系统会在每次任务执行时从主用模式切换至备用模式。(CSCur59252)
- 解决了以下问题：如果根据客户端应用从漏洞网络图展开漏洞，系统不会显示关联的主机。(CSCur86191)
- 改善了某些事件工作流程的优化问题。(CSCus52203
- 改善了故障排除功能。(CSCut12157)
- 改善了 SFDataCorrelator 功能。(CSCut23688)
- 解决了以下问题：当处理流量时，系统会忽略源网络访问控制规则条件。(CSCut23929)
- 故障生成的故障排除现包含 IPv6 信息。(CSCut48083)

由于您可以将设备从 5.3.1 版更新至版本 5.3.1.6，此更新还包括版本 5.3.1.6 到版本 5.3.1 的所有更新中的更改。之前解决的问题按版本列出。

版本 5.3.1.1 解决的问题：

- 安全问题解决了多个跨站脚本 (XSS) 漏洞。
- 安全问题解决了多个跨站请求伪造 (CSRF) 漏洞。
- 安全问题解决了多个 HTML 注入漏洞。
- 安全问题解决了多个拒绝服务 (DoS) 漏洞，如 CVE-2014-0196 和 CVE-2014-3153 中所述。
- 解决了以下问题：如果您将当前访问控制策略所针对的一组堆叠设备添加到防御中心，然后重新应用策略，系统会在“设备管理”(Device Management) 页面中错误地显示受管设备列表并阻止您编辑所列的设备。(140710/CSCze92390)
- 解决了以下问题：将单个运行状况策略应用于 100 台或更多的受管设备会导致系统问题。(140977/CSCze92388)
- 解决了以下问题：如果您注册一台 ASA FirePOWER 设备到高可用性配置环境中的一对防御中心，在“用户管理”(User Management) 页面中（**系统 [System] > 本地 [Local] > 用户管理 [User Management]**），辅助防御中心不显示“CSM 单点登录”(CSM Single Sign-On) 选项卡。(141150/CSCze92615)
- 解决了以下问题：当系统日志警报作为入侵事件通知发送时，该警报包含错误的入侵规则分类数据。（141213/CSCze92467、141216/CSCze92474、141220/CSCze92639）
- 解决了以下问题：如果您将网络变量（如 `$HOME_NET`）作为用于网络设置的值，自适应配置文件未能生效。(141225/CSCze92611)
- 解决了以下问题：如果创建仅包含配置的备份，备份文件会包含无关的发现事件数据。(141246/CSCze92508)
- 解决了以下问题：如果您创建使用 VLAN 标记对象的已保存的搜索，系统会在您使用该 VLAN 标记对象的字段中，以值 `0` 保存该搜索。(141330/CSCze92734)

- 解决了以下问题：如果您创建包含大量页面的自定义工作流程，时间窗会遮挡通向该工作流程的最终页面的链接。(141336/CSCze92873)
- 解决了以下问题：在极少数情况下，当重新应用设备配置失败时，系统不生成运行状况警报。（141625/CSCze93130、141628/CSCze93009）
- 解决了以下问题：在安装了漏洞数据库 (VDB) 后，受管设备上的一个或多个无响应的检测资源导致系统问题。(141758CSCze93100)
- 解决了以下问题：在极少数情况下，当收到服务器发出的 TCP 会话的第一个未记录出接口的数据包时，系统会触发警报。(141817/CSCze93047)
- 解决了以下问题：在极少数情况下，应用多个访问控制策略会导致系统问题并生成非受管磁盘利用率高的运行状况警报。(141830/CSCze92990)
- 解决了第三方 OpenSSL 漏洞，如 CVE-2-014-0224 所述。(141901/CSCze93310)
- 提高了 SMB 和 DCE/RPC 预处理程序的稳定性。(142199/CSCze93232)
- 解决了以下问题：如果您编辑了访问控制策略，然后策略应用失败，尝试应用的策略中的策略更改不会恢复至之前已应用的策略。(142907/CSCze94256)
- 以下 CVE 解决了第三方 Java 漏洞：CVE-2014-0429、CVE-2013-5907、CVE-2013-5782、CVE-2013-5830、CVE-2013-1537、CVE-2013-0437、CVE-2013-1478、CVE-2013-1480、CVE-2012-5083、CVE-2012-1531、CVE-2012-1713、CVE-2014-0385、CVE-2013-5802、CVE-2013-2461、CVE-2013-2467、CVE-2013-2407、CVE-2014-0460、CVE-2014-0423、CVE-2013-5905、CVE-2013-5906、CVE-2014-4264、CVE-2013-6954、CVE-2013-6629、CVE-2013-5825、CVE-2013-4002、CVE-2013-5823、CVE-2013-2457、CVE-2013-0440、CVE-2013-5780、CVE-2014-4244、CVE-2014-4263、CVE-2014-0453、CVE-2014-0411、CVE-2013-0443、CVE-2013-2451、CVE-2013-5803、CVE-2013-2415、CVE-2013-1489、CVE-2012-5085。(143620/CSCze94657)
- 解决了以下问题：如果系统从文件流量生成文件事件，系统错误地截短网络界面多个页面上带冒号的文件事件文件名。(143666/CSCze94954)
- 解决了以下问题：如果系统生成与规则匹配的入侵事件，且该规则含有的生成器 ID (GID) 不是 1 或 3，系统日志警报包含错误的消息。(143725/CSCze94300)
- 解决了以下问题：如果您禁用的访问控制规则包含入侵策略或与任何已启用的规则和访问控制策略的默认操作不同的变量集，访问控制策略应用会失败且系统会遇到问题。(143870/CSCze94942)
- 解决了一个随机注入漏洞，该漏洞使未经身份验证的远程攻击者可以通过 bash 执行命令这解决了 CVE-2014-6271 和 CVE-2014-7169 中所述的问题。有关更多信息，请参阅思科安全咨询页面，网址为 http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20140926-bash。（144863/CSCze95512、144942/CSCze95480、144949/CSCze96202）

5.3.1 版中解决的问题：

- 解决了以下问题：在某些情况下，入侵事件数据包视图显示的规则消息与生成事件的规则不匹配。(138208/CSCze90592)
- 解决了以下问题：不能导入引用自定义变量的入侵规则。(138211/CSCze90499)
- 解决了以下问题：如果在思科 IOS 空路由补救模块上启用 Telnet，并配置思科 IOS 实例的用户名，以便在思科 IOS 路由器上默认启用，会导致思科 IOS 空路由补救在防御中心上失败。(139506/CSCze91607)
- 解决了以下问题：系统不会阻止创建带有被排除网络值的网络变量，而该网络值排除了所有 (any) 网络。(139510/CSCze91770)

已知问题

版本 5.3.1.6 中报告了以下已知问题：

- 在某些情况下，如果您以管理员用户的身份登录您的系统，并编辑所应用的入侵策略的基本层，系统会错误地标记**管理员**更新的基本策略（以及子策略，如有配置）。(CSCur79437)
- 在某些情况下，如果您在“用户首选项”(User Preferences) 页面（**管理员 [Admin] > 用户首选项 [User Preferences] > 时区首选项 [Time Zone Preference]**）中的“时区首选项”(Time Zone Preference) 选项卡中更改所选的时区，则系统可能不会纳入夏令时，且可能显示错误的时间。(CSCur92028)
- (CSCus45769)
- 在某些情况下，如果您禁用引用入侵策略的访问控制规则，在访问控制策略成功重新应用后，“访问控制策略”(Access Control Policy) 页面（**策略 [Policies] > 访问控制 [Access Control]**）会将入侵策略错误地显示为过时状态。“入侵策略”(Intrusion Policy) 页面（**策略 [Policies] > 入侵 [Intrusion] > 入侵策略 [Intrusion Policy]**）会显示正确的策略状态。(CSCuu15483)
- 在某些情况下，如果您创建文件策略和 NAT 策略，并启用带有 HTTP 端口号的 TCP 流预处理程序规则，但该端口并非网络访问策略的 HTTP 预处理程序配置页面上可用的端口，系统不会检测与所配置文件策略操作匹配的流量中的恶意软件，并会异常地下载恶意软件内容。(CSCuu24472)
- 在某些情况下，如果您将系统策略配置为使用远程 NTP 服务器，以便与使用注册的 ASA 5500-X 设备、系列 2 设备或运行版本 5.4 以前的版本的系列 3 设备的系统实现时间同步，当遇到闰秒问题时，系统可能会占用大量 CPU。(CSCuv11738)

早期版本中报告了以下已知问题：

- 在某些情况下，应用您的访问控制策略、入侵策略、网络发现策略或设备配置中的更改，或安装漏洞数据库 (VDB) 的入侵规则更新时，在快速模式下使用链路汇聚控制协议 (LACP) 的流量会出现中断。对此的解决方法是，配置缓慢模式下的 LACP 链路。(112070/CSCze87966)
- 如果系统生成 **Destination Port/ICMP Code** 为 `0` 的入侵事件，则“入侵事件统计”(Intrusion Event Statistics) 页面（**概述 [Overview] > 摘要 [Summary] > 入侵事件统计 [Intrusion Event Statistics]**）的“前 10 个目标端口”(Top 10 Destination Ports) 部分会在显示中遗漏端口号。(125581/CSCze88014)
- 防御中心本地配置 (**System > Local > Configuration**) 在高可用性对等体之间**不会被**同步。您必须在所有防御中心，而不仅仅是主设备上编辑和应用更改。（130612/CSCze89250、130652）
- 在某些情况下，如果在系统开始修剪之前，磁盘空间使用率超过磁盘空间阈值，则大型系统备份可能会失败。(132501/CSCze88368)
- 在某些情况下，使用 RunQuery 工具执行 `SHOW TABLES` 命令，可能会导致查询失败。为避免查询失败，请仅使用 RunQuery 应用重新以交互方式运行该查询。(132685/CSCze89153)
- 如果您删除了之前导入的本地入侵规则，您无法重新导入被删除的规则。(132865/CSCze88250)
- 在极少数情况下，系统可能不为入侵规则 141:7 或 142:7 生成事件。(132973/CSCze89252)
- 在某些情况下，受管设备的远程备份包括无关的统一文件，在防御中心上生成大型备份文件。(133040/CSCze89204)
- 必须使用设备的 CLI 或外壳，编辑防御中心或受管设备上的最大传输单位 (MTU)。不能通过用户界面编辑 MTU。(133802/CSCze89748)
- 如果在 URL 中创建带星号 (`*`) 的 URL 对象，对于包含引用该对象的规则的访问控制策略，系统不会为其生成被抢占的规则的警告。请**不要**在 URL 对象 URL 中使用星号 (`*`)。（134095/CSCze88837、134097/CSCze88846）
- 如果将入侵策略配置为生成入侵事件系统日志警报，由启用了预处理程序选项的入侵规则生成的入侵事件系统日志警报消息是 `Snort 警报`，而不是自定义消息。(134270/CSCze88831)

- 如果堆栈中的辅助设备生成入侵事件，系统不会使用安全区域数据填充入侵事件的表视图。(134402/CSCze88843)
- 如果在启用**快速端口扫描 (Fast Port Scan)** 选项的情况下配置 Nmap 扫描补救，Nmap 补救会失败。对此的解决方法是，禁用**快速端口扫描 (Fast Port Scan)** 选项。(134499/CSCze88810)
- 如果根据连接事件表保存的搜索，生成包含连接事件摘要数据的报告，关于该表的报告中将不会填充任何数据。(134541/CSCze89348)
- 安排和运行并行的系统备份任务，会对系统性能造成负面影响。对此的解决方法是，错开安排的任务，每次仅运行一个备份。(134575/CSCze89679)
- 如果编辑之前配置的，并且启用了用户和组访问控制参数的 LDAP 连接，点击**取出组 (Fetch Groups)** 不会填充“可用组”(Available Groups) 框。在编辑 LDAP 连接时，必须重新输入密码，以提取可用组。(134872/CSCze89834)
- 在某些情况下，如果在“事件视图设置”(Event View Settings) 页面的**事件首选项 (Event Preferences)** 部分中，启用**解析 IP 地址 (Resolve IP Addresses)**，则与 IPv6 地址关联的主机名，在控制面板或事件视图中可能无法如预期解析。(135182/CSCze90155)
- 对于恶意软件云查找，不支持通过消息摘要 5 (MD5) 密码加密配置代理服务器来进行身份验证。(135279/CSCze89442)
- 创建 LDAP 身份验证对象时，在**基本过滤器 (Base Filter)** 字段中输入的字符数不能超过 450 个。(135314/CSCze89081)
- 有某些情况下，如果您在使用夏令时 (DST) 时安排任务，所安排的任务在您不使用 DST 的时段不会运行。对此的解决方法是，在“时区首选项”Time Zone Preference 页面 （**管理员 [Admin] > 用户首选项 [User Preferences]**） 中选择**欧洲，伦敦 (Europe, London)** 作为本地时区，并在不使用 DST 的时段重新创建任务。(135480)
- 为进行数据库检查，系统需要额外时间来重新启动运行版本 5.3 或更高版本的设备或 ASA FirePOWER 设备。如果在数据库检查过程中发现错误，重新启动需要额外时间来修复数据库。（135564、136439）
- 在某些情况下，系统可能对 SSH 预处理程序规则 128:1 生成误报。(135567/CSCze89434)
- 如果应用其中包含规则（已启用**提取原始客户端 IP 地址 [Extract Original Client IP Address]**“HTTP 预处理程序”[HTTP preprocessor] 选项）的入侵策略，当流量通过专用代理服务器时，系统可能会在**原始客户端 IP (Original Client IP)** 字段中，使用不正确的数据填充入侵事件。(135651/CSCze89056)
- 如果安排以 **报告 (Report)** 为作业类型的任务，系统不会将该报告附加到通过邮件发送的状态报告。(136026/CSCze90265)
- 如果将访问控制策略应用到多台设备，防御中心将在网络界面的“任务状态”(Task Status) 页面、“访问控制策略”(Access Control policy) 页面和“设备管理”(Device Management) 页面上以不同方式显示任务状态。“设备管理”(Device Management) 页面（**设备 [Devices] > 设备管理 [Device Management]**）上的任务状态正确。（136364/CSCze87068、136614/CSCze89936）
- 在某些情况下，如果根据运行状况事件表创建自定义工作流程，防御中心将在事件查看器中显示冲突的数据。(136419/CSCze90336)
- 如果将自定义入侵规则作为 `.rtf` 文件导入，系统不会发出有关该 `.rtf` 文件类型不受支持的警告。(136500/CSCze89991)
- 如果配置安全情报源，并指定在运行 WINDOWS 操作系统的计算机上创建的**源 URL**，系统将不会在“安全情报”(Security Intelligence) 选项卡上的工具提示中，显示正确数量的已提交 IP 地址。对此的解决方法是，使用 `dos2unix` 命令将文件从 WINDOWS 编码转换为 Unix 编码，然后点击“安全情报”(Security Intelligence) 页面上的**更新源 (Update Feeds)**。(136557/CSCze89888)
- 如果禁用物理接口，与其关联的逻辑接口也会被禁用，但对于该受管设备，这些逻辑接口在设备编辑器的“界面”(Interfaces) 选项卡上仍显示为绿色。(136560/CSCze89894)

- 如果基于捕获的文件表创建自定义表，系统将生成一条错误消息。系统不支持基于捕获的文件表创建自定义表。(136844/CSCze89977)
- 如果使用超过 40 个字符的主机名注册受管设备，设备注册将会失败。(137235/CSCze90144)
- 在某些情况下，如果在过滤条件中包括任何以下特殊字符，系统将不会按照预期在对象管理器中过滤对象：美元符号 ($)、脱字号 (^)、星号 (*)、方括号 ([ ])、竖线 (|)、正斜杠 (\)、句点 (.) 和问号 (?)。(137493/CSCze90413)
- 在某些情况下，如果在系统策略中启用简单网络管理协议 (SNMP) 轮询，则在某个集群受管设备上修改高可用性 (HA) 链路接口配置，将会导致系统生成错误的 SNMP 轮询请求。(137546/CSCze90000)
- 在某些情况下，如果将访问控制策略配置为，将已列入黑名单的连接记录到系统日志或 SNMP 陷阱服务器，则会导致系统问题。(137952)
- 在某些情况下，如果系统收到错序 DNS 或 NTP 数据包，操作系统摘要工作流程会显示不正确的 DNS 服务器计数、NTP 服务器计数和 DNS 端口计数。(138047/CSCze90930)
- 文件事件的表视图似乎支持查看不合格文件事件的文件轨迹。仅可查看含有计算出 SHA-256 值的文件的文件轨迹。(138155/CSCze90676)
- 如果生成一个 HTML 或 PDF 格式的报告，且该报告含有以 x-axis 作为**文件名**的表格，系统不会在 x-axis 文件名中显示 UTF-8 字符。(138297/CSCze90799)
- 在极少数情况下，如果使用防御中心管理过多台设备，系统将在控制面板显示不正确的入侵事件计数。(138298)
- 在极少数情况下，编辑并重新应用入侵策略几百次，将会导致入侵规则更新和系统更新需要超过 24 小时才能完成。(138333/CSCze90747)
- 如果防御中心安装了地理位置数据库 (GeoDB) 的最新版本，当您尝试使用相同版本更新 GeoDB 时，系统将生成一条错误消息。(138348/CSCze90813)
- 记录到系统日志或 SNMP 陷阱服务器的连接事件的 **URL Reputation** 值可能不正确。（138504/CSCze91066、139466/CSCze91510）
- 在某些情况下，如果在部署中应用多个访问控制策略，搜索与特定访问控制规则匹配的入侵或连接事件（**分析 [Analysis] > 搜索 [Search]**），可能会检索到其他策略中不相关的规则生成的事件。(138542/CSCze91690)
- 不能在策略之间剪切并粘贴访问控制规则。(138713/CSCze91012)
- 在安全情报源/目标元数据 (rec_type:281) 中，eStreamer 服务器将源标识为目标，将目标标识为源。(138740/CSCze91402)
- 在访问控制策略中，系统会在处理策略的安全情报黑名单之前，处理某些信任规则。可在黑明单之前处理位于第一监控规则前的或位于含有应用、URL、用户或基于地理位置的网络条件的规则前的信任规则。也就是说，靠近访问控制策略顶部附近的信任规则（编号小的规则），或者在简单策略中使用的信任规则，允许本应列入黑名单的流量，未经检查地通过。（138743、139017）
- 如果在入侵策略中禁用**在内联模式下丢弃**，内联标准化将会停止修改流量中发现的数据包，并且系统不会指示要修改哪些流量。在某些情况下,重新启用**在内联模式下丢弃**之后,网络上的其他设备或应用的工作方式可能会有改变。（139174/CSCze91149、139177/CSCze91163）
- 已知安全问题 Sourcefire 可察觉到智能平台管理接口 (IPMI) 标准 (CVE-2013-4786) 中固有的漏洞。在设备上启用远端控制管理 (LOM) 可暴露该漏洞。为了缓解该漏洞，请将设备部署在仅供可信用户访问的安全管理网络上。为了防止暴露该漏洞，请不要启用 LOM。(139286/CSCze91556)
- 在极少数情况下，“任务状态”(Task Status) 页面 （**系统 [System] > 监控 [Monitory] > 任务状态 [Task Status]**）会将失败的系统策略错误地报告为已成功应用。(139428/CSCze92142)

- 如果配置并保存通过其基本策略彼此引用的三个或更多的入侵策略，系统将不会更新“入侵策略”(Intrusion Policy) 页面（**策略 [Policies] > 入侵 [Intrusion] > 入侵策略 [Intrusion Policy]**）上所有策略的最后修改日期。对此的解决方法是，等待 5 到 10 分钟，然后刷新“入侵策略”(Intrusion Policy) 页面。(139647/CSCze91353)
- 在某些情况下，如果在高可用性配置的主防御中心上创建系统策略，然后手动同步到辅助防御中心，系统会生成一条 `错误 500 内部服务器错误` 消息。(139685/CSCze95818)
- 在某些情况下，如果配置并保存一份报告，该报告带有一个包含从使用夏令时 (DST) 过渡到不使用 DST 的过渡日的时间窗，系统会将该时间窗调整为比指定时间提前 1 小时开始。对此的解决方法是，将时间窗设置为在 1 小时后开始。(139713/CSCze91697)
- 如果通过防御中心网络界面的“对象管理器”(Object Manager) 页面从全局白名单移除 IP 地址，防御中心上的命令行界面 (CLI) 将不会反映此更改。(139784/CSCze91728)
- 如果通过在“产品更新”(Product Updates) 页面（**系统 [System] > 更新 [Updates]**）上点击**下载更新 (Download Updates)** 自动下载补丁更新，防御中心可能会下载不正确的补丁。对此的解决方法是，通过在“产品更新”(Product Updates) 页面上点击**上传更新 (Upload Update)** 手动下载补丁更新。(141056/CSCze92845)
- 如果使用 Internet Explorer 11 将报告参数添加到报告部分标题栏，同时创建新的报告模板（**概述 [Overview] > 报告 [Reporting] > 报告模板 [Report Templates]**），报告字段不会被添加到该模板。对此的解决方法是，安装并使用 Internet Explorer 10。(142950/CSCze94011)
- 在某些情况下，从受管设备看到的系统日志输出会将 `SNORT 警报` 报告为签名 ID，而非从防御中心看到的系统日志输出所报告的签名 ID。(CSCur40263)
- 在某些情况下，如果防御中心的文件列表中含有 **SHA-256** 文件条目，此时在高可用性配置中添加防御中心，则高可用性配置中的辅助防御中心会删除现有文件列表数据。(CSCur57708)
- 在某些情况下，如果创建包含静态时间窗的新报告模板，系统保存的时间可能会不正确。(CSCur61984)
- 无法将系统提供的安全情报对象导入一个已包含系统提供的安全情报对象的设备。(CSCur78753)
- 解决了以下问题：在 Snort 重新启动期间，带有非被动接口的设备可能会出现延迟问题。(CSCus13247)
- 系统不支持在 ASA5585-X 设备上重置管理员用户的密码。(CSCus17991)
- 如果在启用服务器消息块 (SMB) 协议的情况下，从“报告”(Reports) 页面（**概述 [Overview] > 报告[Reporting] > 报告[Reports]**）选择**启用远程报告存储 (Enable Remote Storage of Reports)**，则`$ 用户，主机报告：$ 主机、攻击报告：$ 攻击 SID` 和 `Sourcefire FireSIGHT 报告：$ 客户名称`模板将会因不支持报告名称中的字符而无法生成报告。(CSCus21871)
- 在某些情况下，如果创建包含 Web 应用类别和阻止恶意软件规则的文件策略，当阻止恶意软件规则位于 Web 应用类别之后时，系统不会阻止被识别为恶意软件的文件。对此的解决方法是，将阻止恶意软件规则置于 Web 应用类别之前。(CSCus64526)
- 在某些情况下，如果将引用文件策略的访问控制规则置于带有 Web 应用的访问控制规则之后，就不会识别出与文件策略匹配的流量。对此的解决方法是，将包含文件策略的规则置于带有 Web 应用的的规则之前。（CSCus64393、CSCus64526）
- 在某些情况下，如果在“剪贴板”(Clipboard) 页面存储详细信息并创建事件，然后**将所有信息添加至事件 (Add all to incident)**，再从新的事件中生成报告，然后尝试创建新的事件，可将以前的剪切板内容添加到新的事件中，即使“事件”(Incidents) 页面（**分析 [Analysis] > 入侵 [Intrusion] > 事件 [Incidents]**）的**剪切板中的事件 (Events in your clipboard)** 部分是空的。(CSCus67128)
- 在某些情况下，如果系统包含 SSL 可视性设备 (SSLVA) 设备，在创建包含 Web 应用类别和阻止恶意软件规则的文件策略时，首次尝试通过 HTTPS 下载文件可能会失败。对此的解决方法是，禁用文件策略。(CSCus72505)

- 在某些情况下，如果创建含有规则集的访问控制策略来拦截包含 URL 的对象组，系统不会拦截与所含 URL 对象相关的流量。对此的解决方法是，把要拦截的 URL 作为单个 URL 对象纳入访问控制规则而不是对象组。(CSCus77551)
- 在某些情况下，如果将一个访问控制策略应用至多个受管设备，系统会将策略状态错误地显示为待定，而实际上策略应用是成功的。对此的解决方法是，编辑并保存策略，然后重新应用。(CSCus86011)
- 在某些情况下，如果创建用户角色，系统可能不会启用某些复选框，但会启用禁用复选框下的可用选项。(CSCus87248)
- 如果从 ASA5585 设备的顶部刀片删除 LSI RegEx 卡，则无法安装 ASA FirePOWER 模块。(CSCus89754)
- 在某些情况下，如果防御中心遇到大量数据，对备份进行还原可能会失败。(CSCus91552)
- 在某些情况下，如果系统在策略应用过程中遇到网络中断，稍后尝试停用“应用检测器”(Application Detector) 页面（**策略 [Policies] > 应用检测器 [Application Detectors]**）上未使用的检测器时,系统会生成一个 无法停用 1 检测器，因其正在对已应用的访问控制策略所使用的应用进行检测错误。(CSCus91892)
- 在某些情况下，如果尝试还原位于 WINDOWS 网络文件服务器 (NFS) 的备份存档，则备份还原会失败。对此的解决方法是，通过 WinSCP 手动传输存档文件。(CSCut08317)
- 您无法拦截未分类的或未分配信誉分数的 URL。(CSCut17683)
- 在某些情况下，如果防御中心数据库遇到系统问题，您可能会丢失访问控制策略，或者您的访问控制策略可能会丢失规则。如果遇到访问控制策略丢失规则问题，请联系支持部门。(CSCut30047)
- 访问控制规则当前不支持包含37个及其以上字符数的 LDAP 组名称。(CSCut34003)
- **受管设备备份 (Managed Device Backup)**页面（**系统 [System] > 工具 [Tools] > 备份/还原 [Backup/Restore] > 受管设备备份 [Managed Device Backup]**）的“备份管理”(Backup Management) 选项卡未将注册的 ASA55X5 或 ASA55X5-SSP-XX 设备纳入作为选项。(CSCut41338)
- 在某些情况下，如果创建访问控制策略，该策略引用网络规则集来拦截所有包含 ：：/0 的 IPv6 地址或引用网络规则集来拦截所有包含 0.0.0.0/0 的 IPv4 地址，系统会错误地拦截所有流量。(CSCut58667)
- 在某些情况下，如果系统尝试查询未知 URL，云查找运行状况模块会生成误报警报。(CSCut77594)
- 由于一个无效符号链接，防御中心上的 /var/home 目录显示为空白。(CSCut80381)
- 如果编辑包含多个类别条件的访问控制规则并尝试删除某个条件，则网络管理界面仅删除列出的第一个类别条件，不受已选条件影响。(CSCuu00585)
- 在某些情况下，如果从刚创建的 FireSIGHT 报告中复制顶级入侵事件表，则生成表中的字段行不包含数据。对此的解决方法是，手动填充复制表字段行的数据。(CSCuu01020)
- 在某些情况下，系统会出现问题，云会对已更新的下载持续进行检查。(CSCuu04844)
- 系统在“内存”(Memory) 页面（**概述 [Overview] > 控制面板 [Dashboards] > 摘要控制面板 [Summary Dashboard] > 状态 [Status] > 系统负载 [System load] > 内存 [Memory]**）上显示不正确的内存使用量。对此的解决方法是，通过“内存使用率”(Memory Usage) 页面（**运行状况 [Health] > 运行状况监控器 [Health Monitor]**）的“内存测试”(Memory Test) 选项查看正确的内存使用率。(CSCuu19742)
- 在某些情况下，如果创建和删除一个自定义用户角色或多次停用并重新激活一个用户角色，系统将在网络浏览器中生成无关的选项卡。(CSCuu31584)
- 在某些情况下，如果将系统的时区改为 UTC 东部的一个时区并将包含至少一个非活动周期的关联规则添加至一个关联策略，策略应用失败。对此的解决方法是，删除旧的关联规则并将时区暂时设置为 UTC。然后重新创建包含非活动周期的关联规则并应用策略，然后重新设置时区并重新应用策略。(CSCuu37600)

- 系统不包含以 `<script>alert(1)</script>` 作为用户名的登录尝试的审核日志条目。（CSCuu39516、CSCuu39521）
- 在某些情况下，如果系统长时间积聚大量流量，Snort 可能会遇到延迟问题，同时您可能会遇到流量中断问题。(CSCuu52545)
- 如果设备在从版本 5.3.1 更新为版本 5.3.1.4 或更高版本时出现错误或故障，请联系支持部门。(CSCuu54653)
- 如果您在 ASA FirePOWER 设备上应用了一条设置为**拦截**的访问控制策略，系统会错误地重置会话。(CSCuu60713)
- 在某些情况下，如果设备似乎未应用“设备管理”(Device Management) 页面（**设备 [Devices] > 设备管理 [Device Management]**）上的更改，而您**应用更改 [Apply Changes]**，然后点击**查看更改 [View Changes]** 链接，则系统会生成入侵策略比较查看器，而正常情况下，是不应该生成的。(CSCuu88332)
- 在某些情况下，如果在“安排”(Scheduling) 页面（**系统 [System] > 工具 [Tools] > 安排 [Scheduling]**）创建新的任务并选择以备份配置文件形式提供的链接，则网页会生成为 `HTTP 错误 500 内部服务器`错误页面。(CSCuv22624)

帮助

所有新的支持申诉必须通过电话、网络或电子邮件使用 Cisco 技术支持中心 (TAC) 提出。要在线提出 TAC 申诉，您必须拥有 Cisco.com 用户 ID 和合同编号。如果需要提出申诉方面的帮助，请拨打以下号码致电 Cisco TAC：800-553-2447。

Cisco 支持

有关获取文档、使用 Cisco 漏洞搜索工具 (BST)、提交服务请求和收集 Cisco ASA 设备其他相关信息的内容，请参阅*《思科产品新特性文档》*，网址为：http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html。

请订阅 *Cisco 产品新特性文档*，该内容以 RSS 源的形式列出所有新的和经过修订的 Cisco 技术文档，并通过阅读器应用程序直接将内容提供至您的桌面。RSS 源是一种免费服务。

如果有任何疑问或者需要 Cisco ASA 设备方面的帮助，请通过以下方式联系 Cisco 支持部门：

- 请访问 Cisco 支持站点，网址为：http://support.cisco.com/。
- 向 Cisco 支持部门发送邮件，邮箱为：tac@cisco.com。
- 致电 Cisco 支持部门，电话号码为：1.408.526.7209 或 1.800.553.2447。