# FireSIGHT 系统版本说明

**5.3.1 版本**
**首次出版日期：2014 年 7 月 17 日**
**上次更新日期：2015 年 1 月 21 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、警告以及具体安装说明的详细信息：

- 2 系列和 3 系列防御中心 （DC500、 DC750、 DC1000、 DC1500、 DC3000 和 DC3500）
- 64 位虚拟防御中心

**注** 此更新**仅**适用于防御中心。物理或虚拟受管设备和用于 X 系列的 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 5.3.1 版本 FireSIGHT 系统。您可以将运行至少 5.3.0.1 版本 FireSIGHT 系统的设备更新至 5.3.1 版本。

有关详细信息，请参阅以下各节：

# 新功能

版本说明的这一节汇总了 5.3.1 版本 FireSIGHT 系统中的新功能和经过更新的功能：



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

## 管理具备 FirePOWER 服务的思科 ASA

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

运行 5.3.1 版本的防御中心管理的 ASA FirePOWER 模块**必须**运行 5.3.1 版本。ASA FirePOWER 模块**只能**安装在运行 9.2.2 版本或更高版本 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防护。

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** 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。这些 ASA 专属工具可用于安装系统，并执行其他平台专属的管理任务。有关详细信息，请参阅 ASA FirePOWER 模块文档。

**注** 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 版本引入了使用 FireSIGHT 防御中心来管理具备 FirePOWER 服务的思科 ASA 的功能。如果您参阅 5.3 版本或 5.3.0.1 版本的相应文档，可能会注意到这些文档中使用的术语与 5.3.1 版本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 |
|---|---|
| 思科 | 以前是 *Sourcefire* |
| FireSIGHT 系统 | 以前是 *Sourcefire 3D 系统* |
| 防御中心<br>FireSIGHT 防御中心<br>思科 FireSIGHT 管理中心 | 以前是 *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)<br>ASA 设备 | 是指思科 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** 思科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。

# 文档更新

您可以从支持站点下载所有更新的文档。在 5.3.1 版本中，以下文档进行了更新，以反映功能的新增和更改，并且解决报告的文档问题：

- 《FireSIGHT 系统*联机帮助*》
- *《FireSIGHT 系统用户指南》*
- *《FireSIGHT 系统安装指南》*
- *《FireSIGHT 系统虚拟安装指南》*
- *《FireSIGHT 系统 eStreamer 集成指南》*
- *《FireSIGHT 系统数据库访问指南》*

更新后的 5.3.1 版本文档包含以下错误：

- 该文档对于堆栈中设备的以下陈述有误：**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：如果堆栈中的辅助设备出现故障，默认情况下，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、123380、 138433）
- 该文档没有反映以下方面：如果修改 ASA 设备的安全情景，并从单情景模式切换到多情景模式，或从多情景模式切换到单情景模式，系统会从安全区域配置中移除接口。（141050、 141064）

# 准备工作：重要更新和兼容性说明

在开始 5.3.1 版本的更新过程之前，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** 思科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，第 5 页
- 更新过程中的审计日志记录，第 5 页
- 更新至 5.3.1 版本的版本要求，第 5 页
- 更新 5.3.1 版本的时间和磁盘空间要求，第 5 页
- 更新至 5.3.1 版本后的产品兼容性，第 6 页
- 还原为上一版本，第 7 页

# 配置和事件备份准则

在您开始更新之前，思科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** 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计日志中。

# 更新至 5.3.1 版本的版本要求

要更新至 5.3.1 版本，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** 受管设备或 用于 X 系列的 Sourcefire 软件**不**支持此更新。

设备的当前版本与发行版本 （5.3.1 版本）越接近，更新所需的时间就越少。

# 更新 5.3.1 版本的时间和磁盘空间要求

下表提供了 5.3.1 版本更新的磁盘空间和时间准则。请注意，使用防御中心更新受管设备时，防御中心需要其 `/Volume` 分区有额外的磁盘空间。

**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。思科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新启动后，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 2 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 | 时间 |
|---|---|---|---|---|
| 2 系列防御中心 | 0 MB | 2.16 GB | 不适用 | 55 - 70 分钟 |
| 3 系列防御中心 | 0 MB | 2.2 GB | 不适用 | 50 - 65 分钟 |
| 虚拟防御中心 | 0 MB | 2.2 GB | 不适用 | 因硬件而异 |

# 更新至 5.3.1 版本后的产品兼容性

运行 5.3.1 版本的防御中心可以管理安装在 ASA 上的受管设备和 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 3　　管理版本要求*

| 设备 | 要由运行 5.3.1 版本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 5.2 版本 |
| 用于 X 系列的 Sourcefire 软件 | 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

您可以在运行 9.2.2 版本或更高版本的以下 ASA 平台上安装 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

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 5.3.1 版本网络界面在下表所列的浏览器上进行过测试。

*表 4　　受支持的网络浏览器*

| 浏览器 | 需要启用的选项和设置 |
|---|---|
| Chrome 34 | JavaScript、 Cookie |
| Firefox 29 | 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** |

### 屏幕分辨率兼容性

思科建议，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。

# 还原为上一版本

如果您由于某种原因，需要将设备还原为 FireSIGHT 系统的上一版本，请联系支持部门，以便了解详细信息。

# 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 4 页。

要将至少运行 5.3.0.1 版本 FireSIGHT 系统的设备更新至 5.3.1 版本，请参阅以下概述的准则和操作步骤：

- 更新防御中心，第 8 页
- 使用外壳执行更新，第 9 页

**注** 物理或虚拟受管设备和用于 X 系列的 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，思科**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。

### 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

您在防御中心上执行更新后，**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。这些步骤包括：

- 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 5.3.1 版本的最新补丁 （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
- 根据新功能，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

运用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 5.3.1 版本更新，防御中心会重新启动。

**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** 将防御中心更新至 5.3.1 版本，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 4 页。

**步骤 2** 从支持站点下载更新：

- 对于 2 系列防御中心：

  `Sourcefire_3D_Defense_Center_Patch-5.3.1-152.sh`
- 对于 3 系列和虚拟防御中心：

  `Sourcefire_3D_Defense_Center_S3_Patch-5.3.1-152.sh`

**注** 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 **System > Updates**，然后在 **Product Updates** 选项卡中点击 **Upload Update**，将更新上传到防御中心。浏览到更新并点击 **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 (**System > Monitoring > 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 **System > Updates**。

系统将显示 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 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 (**System > Monitoring > 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 Upgrade Status 页面。 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 Update 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。

**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 **Help > About**，确认软件版本是否已正确列出：5.3.1 版本。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受管设备。

要重新激活灰显的 **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 **Save**。

**步骤 17** 将访问控制策略重新应用到所有受管设备。

**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 5.3.1 版本的补丁，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** 如果防御中心在从 5.3 版本更新至 5.3.1 版本时，发生 FSIC 故障，请先安装 5.3.0.2 版本，然后再更新至 5.3.1 版本。

# 使用外壳执行更新

虽然思科建议在防御中心上使用网络界面执行更新，但在极少数情况下，可能需要使用 bash 外壳来更新设备。

对于 5.3.1 版本更新，所有设备都会重新启动。有关详细信息，请参阅更新过程中的审计日志记录，第 5 页。

**要使用外壳安装更新，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 4 页。

**步骤 2** 从支持站点下载适当的更新：

- 对于 2 系列防御中心：

  `Sourcefire_3D_Defense_Center_Patch-5.3.1-152.sh`
- 对于 3 系列和虚拟防御中心：

  `Sourcefire_3D_Defense_Center_S3_Patch-5.3.1-152.sh`

**注** 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** 使用具有管理员权限的帐户，登录至设备的外壳。

对于虚拟设备，可以使用 VMware vSphere 客户端中的虚拟控制台登录。

**步骤 4** 在提示符后，以根用户身份运行更新，在出现提示时提供您的密码：

```
sudo install_update.pl /var/sf/updates/update_name
```

其中，*update_name* 是您之前下载的更新的文件名。

更新过程将会开始。

**步骤 5** 更新完成后，设备会重新启动。可以监控更新，并按照以下各节所述，完成所有更新后步骤

- 更新防御中心，第 8 页

**注** 如果防御中心在从 5.3 版本更新至 5.3.1 版本时发生 FSIC 故障，请先安装 5.3.0.2 版本，然后再更新至 5.3.1 版本。

# 已解决的问题

以下各节列出了 5.3.1 版本更新中已解决的问题。

### 5.3.1 版本中已解决的问题

- 解决了如下问题：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)
- 解决了如下问题：不能导入引用自定义变量的入侵规则。 (138211)
- 解决了如下问题：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)
- 解决了如下问题：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)

# 已知问题

5.3.1 版本中报告了以下已知问题：

- 由于数据库检查，系统需要额外时间来重新启动运行 5.3 版本或更高版本的设备或 ASA FirePOWER 模块。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）
- 不能创建带有 GRE 47 端口条件的访问控制规则。（140642、 140644、 140646、 140648、 140650）
- 如果您从防御中心删除某台受管设备，添加另一台设备，然后重新应用带有与默认操作关联的入侵策略的访问控制策略，系统会指出该入侵策略已在多于防御中心当前管理的设备上过时。 (140705)
- 如果您向设备组添加设备堆栈，并编辑应用的访问控制策略，系统会从该策略移除所有目标设备，阻止您添加新设备并破坏策略名称。对此的解决办法是，从设备组中移除设备堆栈，并分别以独立设备、设备堆栈和设备组为目标。 (140710)
- 如果您在防御中心上配置代理和单点登录 (SSO)，而代理无法访问思科安全管理器 (CSM) 服务器，则 SSO 尝试将会超时并失败。 (140897)
- 在极少数情况下，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。对此的解决办法是，减少应用运行状况策略的受管设备的数量。 (140977)
- 如果通过在 Product Updates 页面 (**System > Updates**) 上点击 **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。对此的解决办法是，通过在 Product Updates 页面上点击 **Upload Update** 手动下载补丁更新。 (141056)
- 如果未使用防御中心的网络界面向防御中心注册 ASA 设备，将不能使用该网络界面配置单点登录 (SSO)。要在高可用性 (HA) 对中的防御中心上配置 SSO，思科建议向这两个防御中心都注册 ASA 设备，然后从主防御中心配置 SSO。 (141150)
- 在某些情况下，作为入侵事件通知发送的系统日志警报，可能包含不正确的入侵规则分类数据。（141213、 141216、 141220）
- 如果 eStreamer 检索大量文件事件，系统会出现内存问题。 (141222)
- 如果在配置自适应配置文件时将网络变量用作 **Networks** 值，自适应配置文件将会失败。解决方法是，显式指定 IP 地址或地址块。 (141225)
- 如果您创建阻止流量的访问控制规则或入侵规则，然后将该访问控制规则或入侵规则应用至使用内联接口集的虚拟受管设备，则流量会中断，直至您重新启动设备。 (141230)
- 如果创建仅包含配置的备份，备份文件将会包含无关的发现事件数据。 (141246)
- 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)
- 如果您创建包含大量页面的自定义工作流程，页面右上部分的时间窗口，可能会遮挡通向该工作流程的最终页面的链接。 (141336)
- 在极少数情况下，如果向某个安全区域添加多个被动接口，然后在受管设备配置中引用该安全区域，配置应用将会失败，而且系统会出现检测中断。（141625、 141628）
- 在某些情况下，如果一个或多个检测资源在受管设备上无响应，安装漏洞数据库 (VDB) 更新会导致系统问题。 (141758)
- 在极少数情况下，如果完成大量访问控制策略应用，系统会出现内存问题，且可能会生成多个 **High unmanaged disk usage** 运行状况警报。 (141830)

早期版本中报告了以下已知问题：

- 如果系统生成 **Destination Port/ICMP Code** 为 0 的入侵事件，则 Intrusion Event Statistics 页面 (**Overview > Summary > Intrusion Event Statistics**) 的 Top 10 Destination Ports 部分会在显示中遗漏端口号。 (125581)
- 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、 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)
- 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)
- 如果删除了之前导入的本地入侵规则，将无法重新导入被删除的规则。 (132865)
- 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)
- 在某些情况下，受管设备的远程备份包括无关的统一文件，从而导致防御中心上生成大型备份文件。 (133040)
- 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)
- 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、 134097）
- 如果将入侵策略配置为生成入侵事件系统日志警报，由启用了预处理器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)
- 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)
- 如果配置启用了 **Fast Port Scan** 选项的 Nmap 扫描补救， Nmap 补救将会失败。对此的解决办法是，禁用 **Fast Port Scan** 选项。 (134499)
- 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)
- 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。对此的解决办法是，错开安排的任务，每次仅运行一个备份。 (134575)
- 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 **Fetch Groups** 不会填充 Available Groups 框。在编辑 LDAP 连接以提取可用组时，您必须重新输入密码。 (134872)
- 在某些情况下，如果在 Event View Settings 页面的 **Event Preferences** 部分中，启用 **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)
- 创建 LDAP 身份验证对象时，在 **Base Filter** 字段中不能输入超过 450 个字符。 (135314)
- 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。对此的解决办法是，在 Time Zone Preference 页面 (**Admin > User Preferences**) 中选择 **Europe, London** 作为本地时区，并在不使用 DST 的时段重新创建任务。 (135480)
- 在某些情况下，系统可能对 SSH 预处理器规则 128:1 生成误报。 (135567)
- 如果应用其中包含规则 （已启用 **Extract Original Client IP Address** 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 **Original Client IP** 字段中，使用不正确的数据填充入侵事件。 (135651)

- 如果安排以 **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)
- 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 Task Status 页面、 Access Control policy 页面和 Device Management 页面上以不同方式显示任务状态。 Device Management 页面 (**Devices > Device Management**) 上的任务状态正确。（136364、 136614）
- 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)
- 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)
- 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 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。对此的解决办法是，使用 `dos2unix` 命令将文件从 Windows 编码转换为 Unix 编码，然后点击 Security Intelligence 页面上的 **Update Feeds**。 (136557)
- 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 Interfaces 选项卡上仍显示为绿色。 (136560)
- 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)
- 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)
- 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)
- 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)
- 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)
- 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。您只能查看具有已计算 SHA-256 值的文件的文件轨迹。 (138155)
- 如果生成包含以 **File Name** 为 X 轴的图表的 HTML 或 PDF 格式的报告，系统将不会在 X 轴文件名中显示 UTF-8 字符。 (138297)
- 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)
- 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)
- 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、139466）
- 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 (**Analysis > Search**)，可能会检索到其他策略中不相关的规则生成的事件。 (138542)
- 不能在策略之间剪切并粘贴访问控制规则。 (138713)
- 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)

- 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。放置在第一个监控规则之前，或者具有应用、 URL、用户或基于地理定位的网络条件的规则之前的信任规则，将在黑名单之前处理。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 **Drop When Inline**，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 **Drop When Inline** 后，网络上其他设备或应用的工作方式可能会有所改变。（139174、 139177）
- 已知安全问题 Sourcefire 有一个已知的智能平台管理接口 (IPMI) 标准 (CVE-2013-4786) 固有漏洞。在设备上启用无人值守管理 (LOM) 会暴露该漏洞。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)
- 在极少数情况下，Task Status 页面 (**System > Monitory > Task Status**) 会将失败的系统策略错误地报告为已成功应用。 (139428)
- 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 Intrusion Polycy 页面 (**Policies > Intrusion > Intrusion Policy**) 上所有策略的 Last Modified 日期。对此的解决办法是，等待 5 到 10 分钟，然后刷新 Intrusion Policy 页面。 (139647)
- 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 的过渡日的时段，系统会将该时段调整为比指定时间提前 1 小时开始。对此的解决办法是，将时段设置为在 1 小时后开始。 (139713)
- 如果通过防御中心网络界面的 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)

# 获取帮助

感谢您选用 FireSIGHT 系统。

### Sourcefire 支持

如果您是新客户，请访问 https://support.sourcefire.com/ 下载 Sourcefire 支持欢迎套件，该文档有助于您快速了解 Sourcefire 支持，并设置客户中心帐户。

如果有任何疑问，想要下载经过更新的文档，或者需要 Sourcefire 防御中心方面的帮助，请联系 Sourcefire 支持部门：

- 请访问 Sourcefire 支持站点，网址为：https://support.sourcefire.com/。
- 向 Sourcefire 支持部门发送邮件，邮箱为：support@sourcefire.com。
- 致电 Sourcefire 支持部门，电话号码为：410.423.1901 或 1.800.917.4134。

### 思科支持

有关获取文档、使用思科漏洞搜索工具 (BST)、提交服务请求和收集思科 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 *《思科产品新特性文档》*，该内容以 RSS 源的形式列出所有新的和经过修订的思科技术文档，并通过阅读器应用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思科 ASA 设备方面的帮助，请通过以下方式联系思科支持部门：

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